REVISTA IBEROAMERICANA DE DERECHO INFORMÁTICO
(SEGUNDA ÉPOCA)

FEDERACIÓN IBEROAMERICANA DE ASOCIACIONES
DE DERECHO E INFORMÁTICA

ISSN 2530-4496 – AÑO 2, N.º 11, 2021, PP. 101-176

NEUROTECNOLOGÍA: INTERFAZ CEREBRO-COMPUTADOR Y PROTECCIÓN DE DATOS CEREBRALES O NEURODATOS EN EL CONTEXTO DEL TRATAMIENTO DE DATOS PERSONALES EN LA UNIÓN EUROPEA

NEUROTECHNOLOGY: BRAIN-COMPUTER INTERFACE AND PROTECTION OF BRAIN DATA OR NEURODATA IN THE CONTEXT OF THE PROCESSING OF PERSONAL DATA IN THE EUROPEAN UNION

Yasna Vanessa Bastidas Cid[1]

1 Investigadora del Instituto de Derecho Informático, Región de los Ríos, Chile. Abogada por la Excelentísima Corte Suprema de Chile; Máster en protección de datos y Máster en propiedad intelectual y derecho de las nuevas tecnologías, ambos por la Universidad Internacional de la Rioja- UNIR; Investigadora becaria del Grupo de Investigación TREs-i "Trabajo líquido y riesgos emergentes en la sociedad de la información" de la Universidad Internacional de la Rioja-UNIR; y PhD (c) en derecho de la Universidad Carlos III de Madrid.

Resumen ejecutivo

El objetivo general de este trabajo consiste en analizar los desafíos a los que se enfrentan las neurotecnologías, en particular, la interfaz cerebro-computador (en adelante, BCI) de cara al cumplimiento de las condiciones para el tratamiento de datos personales establecidas en el Reglamento General de protección de datos (UE) (en adelante RGPD). Los objetivos específicos consisten en analizar la relación entre neurotecnologías, neuroderechos humanos y privacidad mental; determinar y categorizar la tipología de datos que recogen las BCI; y estudiar las diferentes medidas técnicas y organizativas destinadas a garantizar el adecuado tratamiento de datos en proyectos BCI.

El desarrollo de las neurotecnologías ha impulsado de sobremanera la investigación sanitaria. La investigación en BCI basada en el análisis de electroencefalograma es la más prometedora en el área de la medicina curativa y de las neurociencias. Los recientes avances en neurotecnología e inteligencia artificial están permitiendo un acceso mayor y más rápido a la información acumulada en el cerebro de las personas otorgándole capacidad a las máquinas de leer nuestros impulsos mentales, procesarlos, interpretarlos y manipularlos, pudiendo alterar, incluso nuestro concepto de ser humano. Este nuevo ecosistema neurotecnológico genera el escenario perfecto para el acceso a una ingente cantidad de información de carácter sensible, datos neurales vinculados a la salud como también a los pensamientos más íntimos y privados de las personas.

Para conseguir nuestros objetivos el presente trabajo se ha divido en 3 capítulos de estudio: el primer capítulo está destinado a introducirnos en los conceptos básicos de las neurotecnologías, su funcionamiento y aplicaciones más relevantes, y sus implicancias técnicas y ético jurídicas. Estas últimas de especial relevancia porque traen aparejadas el nacimiento de nuevos derechos y libertades fundamentales para los individuos y la necesidad de protegerlos y garantizarlos, los nuevos "neuroderechos humanos". El capítulo segundo nos sumerge en los desafíos que nos plantean las interfaces cerebro-computador en cuanto a la privacidad y protección de los datos cerebrales que recogen, registran e interpretan. Así, analizaremos el concepto de dato cerebral o neurodato, determinando su significado legal, su naturaleza jurídica y su categorización dentro de alguno de los grupos de datos personales protegidos y garantizados por RGPD. Cerraremos el estudio de esta sección con las condiciones que debe cumplir el consentimiento del interesado en entornos BCI. Y, en el tercer y último capítulo enfocamos el estudio a dos grandes principios establecidos en el RGPD que irradian de manera transversal las operaciones de tratamiento de datos personales: el principio de responsabilidad proactiva y el enfoque de riesgo. De tal manera que, gestionamos su cumplimiento, determinando los riesgos específicos a los que están expuestos los datos en proyectos BCI y las medidas técnicas y organizativas que nos ofrece el RGPD para garantizar un nivel adecuado de neuroprotección.

De esta manera logramos delinear el impacto de las nuevas neurotecnologías avanzadas en los derechos y libertades fundamentales de las personas, en especial, en el derecho a la privacidad mental. Esbozamos un concepto jurídico

de dato cerebral o neurodato tanto en sentido amplio como restringido y determinamos su naturaleza jurídica, categorización, tipología y condiciones para un tratamiento válido, ético y justo a la vista del RGPD.

Así, la contribución principal de este trabajo ha sido aportar una solución a los agentes de la ciencia y el derecho, que, obnubilados por la disyuntiva entre la naturaleza biológica o jurídica de los impulsos eléctricos registrados en entornos BCI, y por la rápida evolución de la tecnología -que siempre va un paso más adelante que el derecho- no han logrado determinar un concepto jurídico para dichos datos y se han cuestionado si se deben o no aplicar en las operaciones de tratamiento de los neurodatos, los principios, condiciones y garantías que prescribe el RGPD para el tratamiento de los datos personales, sembrando una duda respecto a si el RGPD ha sido preparado y diseñado para afrontar los cambios tecnológicos constantes de la revolución informática de la última era promovida por la Internet y el proceso de globalización.

Con la aprobación y vigencia del RGPD se ha reformado de manera sustancial el panorama europeo relativo a la protección de datos personales. El actual RGPD está pensado para afrontar los problemas que suponen las nuevas tecnologías en el ámbito de la privacidad, siendo aplicable no solo a la motorización de los comportamientos mostrados en internet; sino también a cualquier motorización realizada por cualquier medio destinado para ello. Sin embargo, el aumento exponencial de la información que se envía por Red debe ser respaldado por la concienciación, educación y por la elaboración de nuevas leyes y estándares internacionales donde todos los sujetos que son parte de aquellos países que no forman parte de la Unión Europea ni del Espacio Económico Europeo también puedan participar, comprometerse y ser sujetos de obligaciones y derechos. De tal manera que, unidas esas regulaciones al RGPD contribuyan con la privacidad y seguridad necesaria de la información y la garantía y protección de los nuevos neuroderechos humanos.

Índice

Abreviaturas y acrónimos

AC Autoridad de Control
BCI Interfaz cerebro-computador
CEPD Comité Europeo de Protección de datos
CPR Constitución Política de la República de Chile
DPD Delegado de protección de datos
DPO *Data Protection Officer*
EEG Electroencefalograma
EIPD Evaluación de impacto en protección de datos
GT 29 Grupo de trabajo del artículo 29
IA Inteligencia Artificial
IdT Internet del Todo
IoB *Internet of Bodies*
IoT *Internet of Things*
PbD *Privacy by Design* / Privacidad desde el diseño
RAT Registro de actividades de tratamiento
RGPD 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).

Glosario reglamento (UE) 2016/679

1. **Datos personales:** toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.
2. **Tratamiento:** cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.
3. **Responsable del tratamiento o responsable:** la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros.
4. **Encargado del tratamiento o encargadoespecífica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen."** : la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.
5. **Consentimiento del interesadoespecífica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen."** : toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.
6. **Violación de la seguridad de los datos personales:** toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.
7. **Datos relativos a la salud:** datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.
8. **Interesado:** persona física a quien corresponde la titularidad de los datos personales que se tratan.

Introducción

El desarrollo de las neurotecnologías ha impulsado de sobremanera la investigación sanitaria. La investigación en interfaz cerebro computador (en adelante, BCI) basada en el análisis de electroencefalograma es la más prometedora en el área de la medicina curativa y de las neurociencias.

Con el fin de permitir a las personas con limitaciones motrices severas comunicarse con una neuroprótesis o programas de selección de palabras de comunicación básicas, los sistemas de BCI descifran la intención del usuario a través de señales eléctricas neuronales que incluyen potenciales corticales lentos, potenciales evocados visuales, potencial P300, ritmos *beta* o *mu* registrados sobre el cuero cabelludo, así como la actividad neural cortical registrada mediante electrodos implantados.

El poder comunicarse con el entorno y con las personas, es una necesidad esencial de los seres humanos. Las personas con discapacidades motoras encuentran en los sistemas BCI una oportunidad para mejorar su calidad de vida y recuperar su autoestima y sobre todo su autonomía.

Sin embargo, precisamente uno de los aspectos más debatidos en los últimos tiempos es si esa autonomía es verdadera o real o en la medida que los individuos se someten a los procedimientos en vez de ganar autonomía la van cediendo y adquieren solo una ficción de existencia de la misma.

Podemos encontrar miles de artículos y libros publicados que tienen como óbice el impacto de las nuevas tecnologías y los avances científicos en la condición humana. Los recientes avances en neurotecnología e inteligencia artificial están permitiendo un acceso mayor y más rápido a la información acumulada en el cerebro de las personas otorgándole capacidad a las máquinas de leer nuestros procesos mentales, procesarlos, interpretarlos y manipularlos, pudiendo alterar, incluso nuestro concepto de ser humano.

Este nuevo ecosistema neurotecnológico genera el escenario perfecto para el acceso a una ingente cantidad de información de carácter sensible, datos neurales vinculados a la salud como también a los pensamientos más íntimos y privados de las personas.

El objetivo general de este trabajo consiste en analizar los desafíos a los que se enfrentan las neurotecnologías, en particular, la interfaz cerebro-computador de cara al cumplimiento de las condiciones para el tratamiento de datos personales establecidas en el Reglamento General de protección de datos (UE) (en adelante RGPD). Los objetivos específicos consisten en analizar la relación entre neurotecnologías, neuroderechos humanos y privacidad mental; Determinar y categorizar la tipología de datos que recogen las BCI; y estudiar las diferentes medidas técnicas y organizativas destinadas a garantizar el adecuado tratamiento de datos en proyectos BCI.

Para lograr estos objetivos el presente trabajo se ha divido 3 capítulos de estudio:

El primer capítulo está destinado a introducirnos en los conceptos básicos de las neurotecnologías, su funcionamiento y aplicaciones más relevantes, y

sus implicancias técnicas y ético jurídicas. Estas últimas de especial relevancia porque traen aparejadas el nacimiento de nuevos derechos y libertades fundamentales para los individuos y la necesidad de protegerlos y garantizarlos, los nuevos "neuroderechos humanos".

El capítulo segundo nos sumerge en los desafíos que nos plantean las interfaces cerebro-computador en cuanto a la privacidad y protección de los datos cerebrales que recogen, registran e interpretan. Así, analizaremos el concepto de dato cerebral o neurodato, determinando su significado legal, su naturaleza jurídica y su categorización dentro de alguno de los grupos de datos personales protegidos y garantizados por el RGPD. Cerraremos el estudio de esta sección con las condiciones que debe cumplir el consentimiento del interesado en entornos BCI.

En el tercer y último capítulo nos centraremos en dos grandes principios establecidos en el RGPD que irradian de manera transversal las operaciones de tratamiento de datos personales: el principio de responsabilidad proactiva y el enfoque de riesgo. De tal manera que, gestionaremos su cumplimiento, determinando los riesgos específicos a los que están expuestos los datos en proyectos BCI y las medidas técnicas y organizativas que nos ofrece el RGPD para garantizar un nivel adecuado de neuroprotección.

Capítulo I
Las nuevas neurotecnologías: dimensión técnica y ético-jurídica

1. Definiendo las nuevas neurotecnologías

Eaton e Illes en la revista *Nature Biothecnology* de 2007, definen la neurotecnología como todo desarrollo que permite monitorear o modificar el funcionamiento cerebral[2]. De tal manera, la neurotecnología deriva en un conjunto de herramientas que sirven para manipular, registrar, medir y obtener información del cerebro, con el fin de analizar e influir sobre el sistema nervioso del ser humano.

Existen neurotecnologías que permiten la manipulación de la actividad del cerebro con precisión celular, donde se utiliza la bioingeniería para insertar información genética de proteínas sensibles a la luz en las células cerebrales, generando así, cambios genéticos en las neuronas que las hacen fotosensibles, un claro ejemplo lo encontramos en la optogenética[3]. De igual manera, existen neurotecnologías que registran la actividad del cerebro y a partir de sistemas computarizados trasladan esta información para controlar prótesis o sistemas robóticos periféricos, los denominados, dispositivos para la estimulación cerebral

2 EATON, M. L., & ILLES, J. (2007). *Commercializing cognitive neurotechnology—the ethical terrain. Nature Biotechnology*, 25(4), pp. 393-397.

3 SALIN-PASCUAL, (2015). Optogenética: la luz como una herramienta para el estudio del funcionamiento cerebral en los mecanismos del sueño-vigilia y la conducta alimentaria. Revista Mexicana de Neurocienicas. 16(3), pp. 39-51.

profunda o interfaces cerebro ordenador, que son utilizados para el tratamiento de múltiples enfermedades[4].

De esta forma, confluyen en la minuciosa área de las neurociencias las tecnologías como la inteligencia artificial, el *big data*, la realidad virtual, la nanotecnología y las interfaces cerebro-computador, entre otros. Sus aplicaciones son fenomenales en el área de la salud. La inteligencia artificial (en adelante, IA) unida al *big data* destaca por su capacidad de ayudar a los expertos en la personalización de los tratamientos. Gracias al análisis de datos por parte de la IA se puede aprender de cada paciente en concreto. Las propuestas más innovadoras respecto a la Inteligencia Artificial están intentando ir más allá del uso del *machine learning* para analizar cantidades ingentes de información y se están aventurando en la investigación de los aspectos más humanos de la Inteligencia Artificial. Un ejemplo claro es el diseño de máquinas que sean capaces de sentir emociones o ser conscientes de su propia existencia[5].

Por su parte, la realidad virtual, mediante un cúmulo de técnicas informáticas permite crear imágenes y espacios simulados computarizados en los que una persona, mediante un dispositivo visual, tiene la sensación de estar y poder desenvolverse dentro de ellos. Esta valiosa técnica **no solo es utilizada con fines de esparcimiento y entretención, sino que, además,** puede aportar mucha información social relacionada con el comportamiento de las personas en situaciones determinadas. Capturando los micromovimientos de las personas, se puede lograr entender algunas de las dinámicas interpersonales más básicas, pero también, se puede definir cómo funcionan los grupos de gente en conjunto. De esta forma, se vuelve una herramienta tecnológica poderosa en la intervención de pacientes con trastorno del espectro autista, adicciones, etc[6].

Ser capaces de manejar una máquina con nuestro cerebro hoy es posible gracias al uso extendido de las interfaces cerebro-máquina. Se trata de un dispositivo que se basa en la adquisición de ondas cerebrales para luego ser procesadas, interpretadas y decodificadas por un algoritmo en una máquina u ordenador en tiempo real, y que, en función del modo de aplicación de la tecnología pueden dividirse en invasivas y no invasivas. Las primeras requieren de la cirugía para incorporar receptores o emisores cerca o junto a áreas del cerebro o terminaciones nerviosas que van a ser afectadas. Un buen ejemplo de estos, son los implantes cerebrales microtecnológicos o nanotecnológicos normalmente introducidos en el córtex cerebral de una persona en el tratamiento de enfermedades como el Parkinson o la epilepsia. En general, lo que se busca es reconstruir movimientos intencionales desde patrones de disparo neuronal. Las segundas no requieren de cirugía eliminando los inconvenientes derivados de la intervención quirúrgica. Estas últimas utilizan emisores y receptores que envían o captan señales alterando o recopilando los estados sensoriales característicos del cerebro

4 LEBEDEV, M., & NICOLELIS, M. (2017). *Brain-Machine Interfaces: From Basic Science to Neuroprostheses and Neurorehabilitation. Physiological Reviews*, 97(2), pp.767-837.

5 VADILLO BUENO, (2020). Futuros de la Inteligencia Artificial. Revista Digital Universitaria. 21(1) pp.1-12.

6 FUNDACIÓN INNOVACIÓN BANKINTER. (2019). Neurociencias: Más allá del cerebro. FUTURE TRENDS FORUM, PP.15-33.

o el sistema nervioso. Un gran ejemplo de estos, son los electroencefalogramas (EEG), estudio que detecta la actividad eléctrica del cerebro mediante pequeños discos metálicos con cables delgados (electrodos) colocados sobre el cuero cabelludo y que envían señales a una computadora para registrar los resultados[7].

También pone a disposición su sello innovador la nanotecnología. Veníamos comentando que, las últimas técnicas en las interfaces cerebro-computador permiten la instalación de electrodos en el cerebro para restaurar sentidos como la vista o el oído, frenar los temblores de la enfermedad de Párkinson. Sin embargo, el método utilizado, es decir romper el cráneo, daña tejidos cerebrales sanos, crea un riesgo de infección y deja cables que sobresalen de su cabeza, que, a lo largo del tiempo, desarrollan tejidos de cicatriz alrededor de los electrodos, aislándoles del tejido cerebral activo. La nanotecnología ha permitido incursionar en el desarrollo un nuevo procedimiento para llegar al cerebro sin tocar el cráneo. Se trata de un método para conectar los electrodos a pequeñas agrupaciones de células cerebrales o incluso neuronas individuales, utilizando el sistema cardiovascular como el conducto por el que se hilan los nanocables[8].

En suma, las neurotecnologías resultan de una combinación sinérgica, particularmente de las nuevas tecnologías avanzadas, que, aplicadas a la salud y las capacidades físicas de las personas tienen como consecuencia, la respuesta a un sinnúmero de necesidades humanas básicas.

2. Una nueva dimensión: del Internet de las Cosas (IoT) al Internet de los Cuerpos (IoB)

Vivimos en un mundo conectado, cada vez más objetos están siendo integrados con sensores, ganando capacidad de comunicación, y con ello las barreras que separan el mundo real del virtual se difuminan. El mundo se está convirtiendo en un campo de información global y la cantidad de datos que circulan por las redes está creciendo exponencialmente.

Este concepto, mundialmente conocido como el «Internet de las Cosas» («*The Internet of Things*» en adelante IoT), consiste en que los objetos puedan conectarse a Internet en cualquier momento y lugar. El término IoT fue empleado por primera vez en 1999 por el pionero británico Kevin Ashton para describir un sistema en el cual los objetos del mundo físico se podían conectar a Internet por medio de sensores. Ashton acuñó este término para ilustrar el poder de conectar a Internet las etiquetas de identificación por radiofrecuencia (RFID) que se utilizaban en las cadenas de suministro corporativas para contar y realizar un seguimiento de las mercancías sin necesidad de intervención humana[9].

7 LUCERO, B., & MUÑOZ-QUEZADA, M. T. (2014). Sistemas de interfaz neuronal y su desarrollo en las neurociencias: revisión bibliográfica sistemática acerca de su aplicación en personas con parálisis. Revista Ciencias Psicológicas, 8(2).

8 KUNO, N., (2016). La nanotecnología cobra vida con dispositivos de interfaz humana basados en agujas. News Center Latam. [en línea] Recuperado el 28 de octubre de 2020.

9 ROSE, K., ELDRIDGE, S., & CHAPIN, L. (2015). La Internet de las Cosas- Una breve reseña para entender mejor los problemas y desafíos de un mundo más conectado. Internet Society, pp.13-16.

El fenómeno del IoT ha irrumpido a nuestro alrededor, dando vida a objetos cotidianos que se interconectan gracias a la Red y que constituyen fuentes inagotables de información. Para ello, ha sido necesaria la conjunción de tres fenómenos que posibilitan el empleo del IoT por los usuarios. Primero, la miniaturización por la cual los componentes de los ordenadores son cada vez más pequeños, lo que facilita que se pueda conectar prácticamente cualquier cosa, desde cualquier sitio, en cualquier momento. Segundo, la superación de la limitación de la infraestructura de telefonía móvil. Y, tercero, la proliferación de las aplicaciones y los servicios que ponen en uso la gran cantidad de información creada a partir del IoT[10].

El hecho de que Internet esté presente al mismo tiempo en todas partes permite la construcción de entornos inteligentes, de esta manera, cada vez estamos más interconectados y las personas y objetos pueden interactuar de manera completamente distinta.

Esta nueva era del IoT está produciendo un impacto social en los seres humanos, muchos de estos objetos conectados están sustituyendo a los actuales dispositivos por terminales insertados en el cuerpo humano. Por ello, se puede afirmar, que en la evolución del llamado IoT el mismo se está moviendo hacia y dentro del cuerpo humano, convirtiéndose en el Internet de los cuerpos (en adelante, IoB).

La relación entre el cuerpo humano y la tecnología es cada vez más habitual, aunque no podemos desconocer que se lleva explorando desde hace muchos años. Esto demuestra el interés del ser humano, como colectivo, en mejorar nuestras capacidades a través de tecnología. Ya en 1961 había sido creado el primer ordenador para vestir. Inventado por los matemáticos *Edward O. Thorpe y Claude Shannon*, era un zapato que contenía un pequeño dispositivo capaz de calcular las posibilidades de dónde caería la bola en la ruleta –tenía un índice de acierto del 44%- y lo enviaba por radio al apostador. Otros aparatos similares aparecieron más adelante, hasta el punto que en 1985 el estado de Nevada los prohibió. Justo un año antes de la creación de este dispositivo los científicos *Manfred E.Clynes y Nathan S.Kline* habían inventado el término "**cyborg**" para referirse a una criatura compuesta de elementos orgánicos y dispositivos cibernéticos generalmente con la intención de mejorar las capacidades de la parte orgánica mediante el uso de tecnología[11].

De esta forma, en los últimos años han surgido personas que se definen a sí mismas como **cyborg**. Un caso muy conocido es el de Neil Harbisson, artista que cuenta con **una antena en la cabeza** que le permite ver y percibir colores incluso invisibles para el ojo humano a través de frecuencias de sonido. Harbisson decidió implantarse este sistema para compensar su acromatopsia, enfermedad que le impide ver los distintos tonos de colores[12].

10 FUNDACIÓN DE LA INNOVACIÓN BANKINTER. (2011). El Internet de la Cosas. En un mundo conectado de objetos inteligentes. pp.9-10.

11 ELÍO, J. (25 de septiembre de 2016). elespañol.com.

12 ORFILA, M. (16 de marzo de 2019). elobservador.com.

Así, este ámbito de la tecnología del Internet de los cuerpos (IoB), nos remite al estudio de la relación de los dispositivos y nuestro cuerpo, es decir, aparatos conectados fuera de nosotros y que llevamos en nuestro exterior (relojes inteligentes); o aparatos que albergamos temporal o permanentemente dentro de nuestro cuerpo (cápsulas con microcámaras para hacer endoscopias o marcapasos inteligentes); o aquellos dispositivos que fusionan la mente humana con computadoras externas e internet.

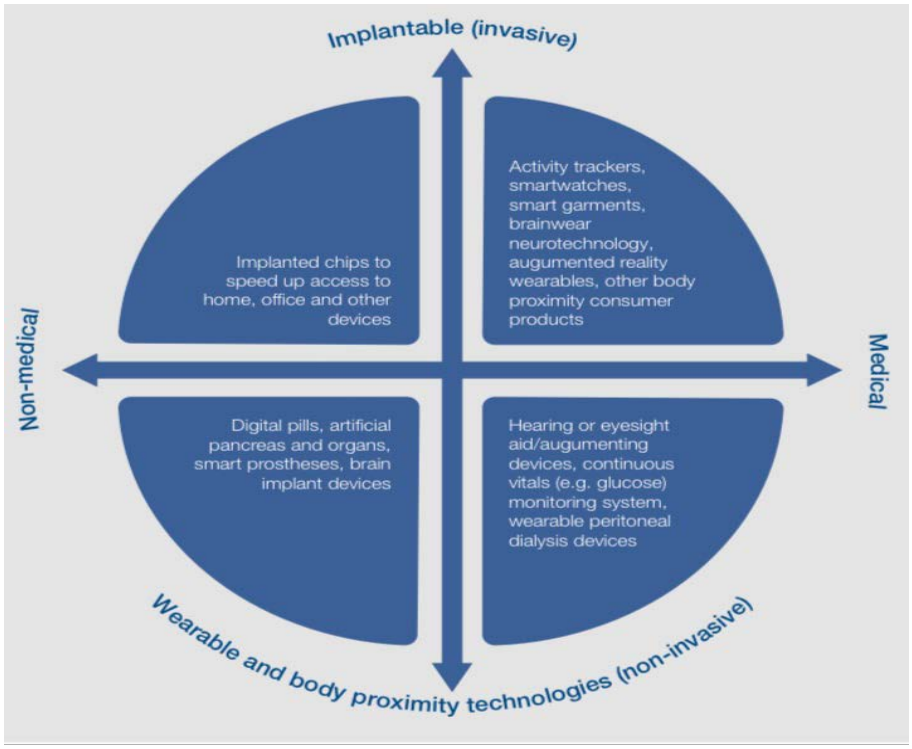

Figura 1: Internet of Bodies technologies. (Xiao Lu y Jeff Merritt, 2020)[13]

Según *Andrea M. Matwyshyn* podemos clasificar el IoB en tres generaciones[14]:

a) *IoB de primera generación. Cuerpo externo:* Son dispositivos ponibles que, ubicados junto a la piel proporcionan una visión en datos corporales. Estos dispositivos son aparentemente ubicuos, y abarcan tres categorías de productos externos al cuerpo: dispositivos médicos; dispositivos de bienestar general que presentan bajo riesgo y promueven un de estilo de vida saludable; y varios otros dispositivos corporales no relacionados con la salud, educativos y recreativos que se conectan a Internet, directamente o indirectamente. Los dispositivos médicos de IoB de primera generación incluyen dispositivos como máquinas de cirugía robótica con acceso a Internet y prótesis conectadas que un paciente maneja desde un teléfo-

13 LU, X., & MERRITT, J. (2020). *Shaping the future of the Internet of Bodies: New challanges of technology governance. World Economic Forum*, p.7.

14 MATWYSHYN, A. M. (2019). *The Internet of Bodies. William & Mary Law Review,* 61(77), pp.89-115.

no móvil. En comparación, la categoría de IoB de primera generación de "bienestar y estilo de vida general" abarca dispositivos familiares como los rastreadores de actividad física y relojes "inteligentes" con capacidad de seguimiento del estilo de vida. Ejemplos de la última categoría de estos dispositivos IoB de primera generación son, las gafas conectadas y los cascos que ofrecen regularmente la información de los trabajadores en tiempo real en entornos empresariales y los proyectos de exoesqueletos para soldados que ofrecen nuevas capacidades de combate.

b) *IoB de segunda generación. Cuerpo interno:* Se refiere a dispositivos donde una parte del mismo reside dentro del cuerpo o accede al cuerpo rompiendo la piel. Por ejemplo, los marcapasos y los implantes cocleares que ahora incluyen funcionalidad dependiente de Bluetooth o pastillas digitales que se basan en un circuito impreso en 3D y un transmisor dentro de una cápsula. De manera similar, varias compañías están compitiendo actualmente para traer un "páncreas" artificial implantable conectado a Internet, gestionado por un software y una aplicación de teléfono móvil.

c) *IoB de tercera generación*. Cuerpo fusionado: Los dispositivos IoB de tercera generación fusionan la mente humana con computadoras externas e Internet. Como se conceptualiza actualmente, estos dispositivos involucran principalmente interfaces cerebrales informáticas inyectadas o implantadas que actúan de manera bidireccional de lectura / escritura. En otras palabras, extienden y exteriorizan funcionalmente porciones de la mente humana. Por lo tanto, uno de los objetivos de IoB de tercera generación es la mejora cognitiva de seres humanos (sanos en principio) con la ayuda de computadoras y vínculos con implantes cerebrales. Se han aplicado principalmente en pacientes con la enfermedad de Parkinson. Unida a la robótica también destacan en el tratamiento de pacientes con nula movilidad o movilidad reducida. Actualmente, los esfuerzos se han concentrado en utilizar estas técnicas para descubrir las causas del Alzheimer y proceder a su tratamiento.

En consecuencia, la convergencia tecnológica actual descansa, principalmente, en la IoT y la IoB, por lo tanto, no es muy difícil convenir en que es la Internet el punto de encuentro entre la neurociencia y la tecnología, de tal manera, ambas se encuentran unidas por una relación bidireccional habiendo entre ellas una retroalimentación constante.

3. Una visión panorámica de los neuroriesgos y neurodesafíos.

Junto a los beneficios sociales y las innovaciones mencionadas en los párrafos anteriores, la gran variedad y cantidad de datos recopilados a través de tecnologías IoB hacen surgir nuevos riesgos y desafíos de cara a las implicaciones técnicas, éticas, legales y políticas de usar el cuerpo como una plataforma tecnológica[15].

Con millones de dispositivos en el ecosistema de salud desplegados para monitorear el cuerpo humano, desde la cama del hospital hasta cualquier lugar, y la recogida de diferentes tipos de datos de una amplia gama de fuentes para

15 *Ídem*

mejorar la atención médica y la investigación, parece evidente que el primer problema que se puede presentar es el de la estandarización de datos e interoperabilidad de las tecnologías. La falta de una plataforma estandarizada para extraer flujos continuos de datos de diferentes dispositivos, restringe el uso de esos datos, ya que estos no son capaces de ofrecer información precisa y mucho menos indubitada salvo que todas las fuentes de datos formen parte de dispositivos interoperables. El primer requisito de la conectividad a Internet es que los sistemas "conectados" deben poder "hablar el mismo idioma" en cuanto a protocolos y codificaciones[16].

Por otra parte, no obstante existir una mayor conciencia de la vulnerabilidad de los wearables y dispositivos IoB a los ciberataques, la ciberseguridad y privacidad siguen siendo un gran desafío. Por ejemplo, en las interfaces cerebro-ordenador es posible el riesgo de *brainhacking* o *brainjacking*. Tanto el *brainhacking* como el *brainjacking* suponen una brecha de seguridad en el software de control. El *brainhacking* implica interrumpir el correcto funcionamiento del algoritmo detrás de las operaciones de una neurotecnología o dispositivo IoB de tercera generación, como por ejemplo las interfaces cerebro-ordenador. El *brainjacking* supone el control remoto de la neurotecnología pudiendo repercutir en el control de un dispositivo tecnológico periférico como una silla de ruedas, implante cerebral, medicamento digital, etc[17].

En medio del brote de COVID-19, con el registro de datos para el seguimiento del coronavirus y la relajación e implantación de aplicaciones de datos sanitarios a nivel mundial, la privacidad de los datos de salud ha generado serias preocupaciones. El equilibrio entre la privacidad de los datos, la transparencia requerida, el nivel de las medidas de seguridad implantadas para hacer frente a una emergencia de salud pública sigue siendo un tema polémico a nivel técnico-jurídico. Los usuarios deben poder confiar en que los dispositivos de la IoB y los servicios de datos relacionados serán seguros y estarán libres de vulnerabilidades, especialmente a medida que esta tecnología sea más difundida y se integre a nuestra vida diaria. Esto significa que los derechos de privacidad y las expectativas con respeto a la privacidad de los usuarios son esenciales para asegurar la confianza de los usuarios en Internet, en los dispositivos conectados y en los servicios relacionados. Huelga mencionar, que cada dispositivo mal asegurado conectado a Internet podría afectar la seguridad y la resistencia de Internet a nivel global[18].

Asimismo, la analítica algorítmica utilizada para tomar decisiones importantes en áreas como seguros, empleo, finanzas, educación, justicia penal, servicios sociales y la asignación de recursos sociales junto con el perfilado desarrollado en relación a datos inexactos o incompletos, datos proxy y generación de datos sensibles de inferencias, todos basados en datos derivados de dispositivos IoB, puede resultar en políticas sesgadas y toma de decisiones que afectan no solo a

16 LU & MERRITT, *Op. Cit.* p. 10.

17 AUSÍN, T., MORTE, R., & MONASTERIO, A. (8 de octubre de 2020). Neuroderechos: Derechos humanos para las neurotecnologías. Diario La Ley (43), pp.1-7.

18 LU & MERRITT, *Op. Cit.* p. 10.

las personas, sino también, a grupos y poblaciones vulnerables, incluso cuando los procesadores de datos y tomadores de decisiones no logren darse cuenta del sesgo implícito o daño potencial. Arrojando como consecuencia, riesgos de discriminación y falta de equidad en el análisis de datos[19].

El uso de dispositivos de IoB plantea nuevas cuestiones reglamentarias y legales y también amplifica los problemas legales que ya existen en torno a Internet. Estas cuestiones son de amplio alcance y muchas veces el rápido ritmo con el que avanza la tecnología supera la capacidad de adaptación de las estructuras políticas, legales y reglamentarias asociadas. De tal manera, que la jurisprudencia y la doctrina se enfrentan a diario con el problema de la interpretación de las normas jurídicas y la idea de hacer del derecho una ciencia adaptable a los cambios tecnológicos. Sin embargo, debemos reconocer que la tecnología siempre irá varios escalones más adelante que la ley[20].

En definitiva, se trata de tecnologías disruptivas, capaces de influir en el desarrollo de nuestra personalidad, de cambiar el concepto de dignidad humana y de modificar el ejercicio de nuestros derechos y libertades fundamentales. En este sentido los desafíos decantan en un cúmulo de responsabilidades que abarcan desde la gestión de los datos, la implantación de medidas de seguridad, el respeto por la privacidad, la mitigación de riesgos de los sesgos discriminatorios, el resguardo de la autonomía, la conservación de la identidad personal, la evaluación de los efectos psico-sociales, y la diligencia en el acceso no consentido a datos cerebrales hasta la prevención de los neurocrímenes, suplantación de identidad, robo y descubrimiento de información sensible de patologías y manipulación cognitiva[21].

4. El nacimiento de una nueva categoría de derechos: los neuroderechos humanos

Proteger a las personas de los abusos que se pudieran realizar con la utilización de las nuevas técnicas de neurotecnología e inteligencia artificial es fundamental para la preservación de la dignidad humana y el libre desarrollo de la personalidad. Con el fin de ir resolviendo los neurodesafíos normativos se ha acuñado por la ciencia una nueva categoría de derechos humanos: los neuroderechos humanos[22].

La tecnología en principio es neutra, se puede utilizar para bien o para mal. Según Rafael Yuste[23]:

> Los métodos de **neurotecnología** que tienen que ver con la **lectura y el cambio de la actividad cerebral**, en realidad nos llevan a la **manipulación de la esencia del ser humano**. Nosotros somos una especie definida

19 *Ibídem,* p. 11.

20 ROSE, ELDRIDGE, & CHAPIN, *Op. Cit*. p. 57.

21 AUSÍN, MORTE, & MONASTERIO, Op. Cit. p.4.

22 YUSTE, R. (2019). Las nuevas neurotecnologías y su impacto en la ciencia, medicina y sociedad. La Lección Cajal, p. 37.

23 *Ibídem*, p. 25.

> por la mente y esta surge del cerebro, entonces si cambias el cerebro estarías cambiando la mente y la base de lo que es ese ser.

Rafael Yuste, neurocientífico y catedrático de la Universidad de Columbia es el impulsor de *Brain Research Through Advancing Innovative Neurotechnologies,* iniciativa de investigación colaborativa que nació en Estados Unidos durante el gobierno del expresidente Barack Obama. En un lapso de 15 años, y con un método de trabajo similar al utilizado en el Proyecto de Genoma Humano, investigadores de diferentes lugares del mundo están desarrollando técnicas para registrar y también manipular la actividad cerebral.

Por esta razón, Rafael Yuste firmó en 2017 junto a otros 25 destacados científicos un artículo en la Revista *Nature* titulado "Cuatro prioridades éticas para las neurotecnologías e Inteligencia Artificial". En dicho artículo proponen una modificación a la Declaración Universal de los Derechos Humanos de 1948 y la incorporación de los nuevos neuroderechos humanos, como un resguardo ante la mala utilización de los avances científicos y tecnológicos.

Cuando se adoptó la Declaración Universal de Derechos Humanos en 1948, los retos futuros de la Neurotecnología y la Inteligencia Artificial apenas podían imaginarse. En consecuencia, no existen disposiciones en el documento de derechos humanos para abordar los nuevos riesgos producidos por las innovaciones tecnológicas. Derechos que antes se daban por sentados, como la privacidad mental o la autonomía cognitiva, han caído en peligro con el advenimiento de las neurotecnologías.

Así, los neuroderechos humanos se concentrarían en 4 categorías: derecho a la privacidad y al consentimiento; derecho a la identidad y a la toma de decisiones (agencia); derecho al aumento cognitivo justo y equitativo; y derecho a la ausencia de sesgos[24].

4.1 Derecho a la privacidad mental y al consentimiento:

La confidencialidad es un principio bioético central que rige la relación proveedor-paciente. Desde Hipócrates, las nuevas leyes lo han interpretado para la era de la medicina de precisión y los registros médicos electrónicos. Más allá del deber moral reconocido de proteger la información médica de los pacientes, los médicos y científicos deberían ahora defender un derecho básico a la privacidad como un medio para salvaguardar los datos cerebrales de los pacientes con el fin de prevenir su uso abusivo y comercial[25].

Esta protección debería cubrir cualquier tipo de información obtenida del cerebro por medio de las neurotecnologías y distribuida por medios digitales. En esta línea, Rafael Yuste señala que:

> Todos tenemos muy presente el problema que existe con la privacidad de los datos (por ejemplo, en nuestros teléfonos móviles). Antes o después vamos a descifrar los patrones cerebrales y vamos a poder entender el pensamiento de las personas. Esto no es ciencia ficción, es algo que se empieza a hacer ya.

24 Ídem.

25 ABOUJAOUDE, Op. Cit. pp. 604-607.

> De hecho, las compañías tecnológicas están muy interesadas en utilizar estas tecnologías. Los algoritmos utilizados por el mejor buscador del mundo son primitivos comparados con nuestro cerebro. Entender cómo pensamos sería un paso de gigante, y tal vez definitivo, para el desarrollo de la inteligencia artificial. Por ejemplo, Facebook tiene un programa de unos cuarenta millones de dólares para conseguir con electrodos no invasivos convertir en texto lo que está pensando una persona, para no tener que utilizar los dedos. Pero eso significa que se podría descifrar lo que uno está pensando, y eso implica una privacidad mucho mayor que la privacidad de los datos, porque los pensamientos, la actividad mental, define quiénes somos. Esto es la máxima privacidad que existe, quiénes somos. El problema es aún peor, porque se puede llegar a descifrar lo que tenemos dentro, el subconsciente, y lo que no sabemos que pensamos. Esta es una situación que debe tener su propio Derecho Humano Universal: el derecho a la privacidad mental, el derecho a que no se pueda comerciar con los datos mentales. Que haya una barrera, que todo lo que tenga que ver con la privacidad mental sea intocable.

En este sentido, el derecho a la privacidad mental y al consentimiento se traduce, por una parte, en proteger a las personas frente al uso ilegítimo y no consentido de su información cerebral o actividad neuronal (su mente y sus pensamientos), implementando todas las medidas técnicas y organizativas destinadas a evitar posibles brechas de seguridad o filtraciones de estos datos. Y, por otra parte, en garantizar a la persona un poder de control sobre sus neurodatos o información cerebral, sobre sus usos y destinos, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y demás derechos del afectado.

4.2 Derecho a la identidad y a la toma de decisiones (agencia):

La omnipresencia de las tecnologías de la información y de la comunicación y la digitalización junto con el creciente desarrollo de la biotecnología, y la automatización y la robótica, en nuestra sociedad, comportan un impacto directo en nuestra identidad. Las amenazas a nuestra identidad, sea por hackers o por errores humanos nos pueden desestabilizar, generando inseguridad y sentimiento de impotencia.

Aunque aún creamos que es ficción y que esto solo ocurre en la película "Matrix" ya en la actualidad numerosas partes de nuestro cuerpo pueden ser reemplazadas y funciones de nuestros órganos pueden ser externalizadas o incorporadas. Las neurotecnologías pueden ser utilizadas para monitorear las señales del cerebro, así como para estimular o modular las funciones cerebrales. El trasplante de órganos son ya un clásico, las prótesis, la bomba de insulina, la hemodiálisis, la mejora de la visión con chips implantados en el cerebro, o el exoesqueleto para pacientes con lesiones modulares, son unos ejemplos. La estimulación puede, como consecuencia, crear cambios en los estados mentales críticos para la personalidad. En el futuro cercano habrá más tecnologías que permitirán mejorar determinadas limitaciones físicas mediante chips integrados en el cuerpo o elementos nanotecnológicos que podrán circular por nuestro cuerpo informando del estado de determinados procesos fisiológicos, generando un impacto en la continuidad psicológica de la persona y cómo la misma se perciba[26].

26 CORNET I PRAT, J. (17 de diciembre de 2017). [en línea] Communityofinsurance.es.

Rafael Yuste incluso señala que la Universidad de Washington ha ido más allá de los simples ejemplos anteriores:

> se ha conectado a tres personas con electrodos de superficie para que realicen juntos una tarea mental común. Estamos en una situación en la que es técnicamente posible conectar a personas, incluso gente que no está en la misma habitación. Puedes conectarte con una persona que está en la otra parte del mundo. Pero cuando estás conectado, ¿quién eres tú? Si fusionas tu cerebro con el cerebro de otra persona o con una máquina, pierdes la identidad personal.

De tal manera que, este derecho a la identidad personal implica la protección al concepto de continuidad psicológica, a la percepción del "yo" tal y como la persona se ha conocido y reconocido a lo largo de su vida, la protección de la continuidad del comportamiento personal y su rol en la sociedad, del cómo los demás le han percibido hasta hoy, frente a modificaciones no consensuadas por terceros. Por lo que, en palabras de Yuste "se vuelve un derecho intocable de la humanidad".

De igual manera, las personas deben ostentar el poder en sus propias decisiones y ser libres para ejercitar dicho poder. Hoy el asunto se ha vuelto más relevante a partir del vertiginoso desarrollo que han alcanzado las nuevas tecnologías. Sabemos que nuestro libre albedrío está condicionado por nuestros genes y nuestros "memes" y hoy debemos añadirle los algoritmos[27].

Al respecto Yuste señala que:

> Si en un futuro estamos conectados a computadoras a través de sistemas no invasivos, que no necesiten introducir electrodos dentro del cerebro, se podrá registrar la actividad mental. Actualmente hay docenas de compañías en Silicon Valley que están desarrollando estos sistemas. Los algoritmos podrán influir en la toma de decisión de las personas y, cuanto más conectados estemos, menos independientes seremos. Eso significa que el libre albedrío en la toma de decisiones nos va a venir de fuera, a través de un algoritmo de inteligencia artificial que puede controlar lo que hacemos. Podrá hacerlo igual o mejor que nosotros, pero ya no seremos nosotros (…)

Todo sistema normativo debe presuponer y garantizar la capacidad de los seres humanos de controlar voluntariamente su comportamiento o en cierta medida de influirlo, incluso cuando sea cuestionable la existencia de libre albedrío cuando aquello que la persona experimenta como una elección libre es el resultado de interacciones electroquímicas en el cerebro y una suerte de programa biológico para la toma de decisión modelada por la evolución.

4.3 Derecho al aumento cognitivo justo y equitativo:

El desarrollo cognitivo es un campo de estudio de la neurociencia y la psicología que se centra en los procedimientos intelectuales y en las conductas que emanan de estos procesos. En otras palabras, el desarrollo cognitivo es el conjunto de

27 Respecto al término "meme", este fue acunado por Richard Dawkins, para referirse a nuestras unidades mínimas de herencia social o unidades de transmisión cultural.

transformaciones que se producen en las características y capacidades de pensar y comprender en el transcurso de la vida[28].

Las investigaciones neurocientíficas han develado que es posible la creación de programas positivos y eficaces de entrenamiento cerebral personalizado a las necesidades de un individuo determinado. Un ejemplo lo encontramos en la innovadora tecnología desarrollada y patentada por *CogniFit,* empresa del sector de la salud e investigación, fundada en el año 1999 por el profesor *Shlomo Breznitz. CogniFit* automatiza la evaluación del perfil cognitivo de cada usuario y genera un programa de entrenamiento cerebral específico que está optimizado para adaptarse a ese perfil en concreto. El "Sistema de Entrenamiento Individualizado" (ITS™) es una patentada aplicación en tiempo real y tecnológicamente avanzada que gestiona la experiencia de cada usuario durante el entrenamiento. Utilizando sofisticados algoritmos en los datos proporcionados por la evaluación, configura un programa de entrenamiento individualizado con un equilibrio óptimo entre las tareas y los niveles de dificultad para que coincida con el perfil cognitivo del usuario, garantizando así su desarrollo cognitivo[29].

Estas tecnologías en sí implican unos costos elevados, pensar que todas las personas podrán acceder a ellas no resulta lógico, por el contrario, los sectores más vulnerables de la población siguen siendo los más afectados y con menos posibilidad de acceso.

En este aspecto, Yuste coincide en que[30]:

> (…) Tiene que haber un sistema justo y equitativo. Creemos que el derecho equitativo a la "aumentación" debe ser un derecho universal, que no provoque la creación de una sociedad en la que cierto grupo de personas se conviertan en una especie de superhumanos, que evidentemente tendrán muchísimas más oportunidades económicas y vitales, y que dejen atrás a otro tipo de población que no pueda permitirse el lujo de aumentarse cognitivamente.

Por esta razón, se vuelve fundamental establecer unos estándares o directrices tanto nacionales como internacionales que regulen el desarrollo y aplicaciones de estas neurotecnologías determinando sus objetivos y fines, límites y alcances. De manera que, se logre garantizar un acceso justo, equitativo, igualitario y no discriminatorio de toda la población (en cuanto sea de vital importancia para los interesados) a estos procedimientos.

4.4 Derecho a la ausencia de sesgos:

Las neurotecnologías deben empoderar a todos e involucrar a la gente. Deben tratar a todas las personas de manera justa. Los sistemas de procesamiento de datos son puramente lógicos y, en teoría, no están sujetos a la conciencia o prejuicios inconscientes que inevitablemente influyen en la toma de decisiones. Sin embargo, debido a que los sistemas de procesamiento de datos, en general,

28 ALBORNOZ ZAMORA, E. J., & GUZMÁN, M. (diciembre de 2016). Desarrollo cognitivo mediante estimulación en niños de 3 años. Revista Científica Multidisciplinar de la Universidad de Cienfuegos, 8(4), pp.186-192.

29 BREZNITZ, S. (2019). [en línea] cognifit.com.

30 YUSTE, 2019. *Op.Cit.* pp. 28-29.

basados en algoritmos de inteligencia artificial (en adelante IA) están diseñados por los seres humanos y los sistemas se entrenan utilizando datos que refleja el mundo imperfecto en el que vivimos, la IA puede operar injustamente sin una planificación cuidadosa[31].

Cabe destacar, además, la existencia de algoritmos de IA que pueden mostrar la conciencia del usuario al confirmar o rechazar una acción y, según sea necesario, corregir la comprensión de la intención del usuario, reconociendo y ajustándose a las personas, lugares y eventos que son más importantes para los usuarios. Ante tal situación, es fundamental y debe convertirse en una obligación, proporcionar información que ayude a las personas a comprender qué inferencias el sistema está haciendo sobre ellos. Tal información hará más fácil identificar y crear conciencia sobre posibles sesgos, errores y resultados no deseados.

Respecto de la IA, Yuste ha señalado que[32]:

> La inteligencia artificial lleva en sus algoritmos unos sesgos que discriminan a ciertos grupos de la población (mujeres, minorías raciales, minorías religiosas o étnicas) porque los algoritmos no tienen ninguna ética, escogen entre probabilidades. Optimizan la solución del problema que se les propone y aumentan las tendencias que se observan en la base de datos que reflejan de una manera algo exagerada, igual que ocurre en el mundo. Y, en muchas ocasiones, esto provoca que los sesgos estén metidos en los algoritmos. Por esta razón, a pesar de nuestro ahínco para hacer una sociedad más equitativa y justa, con estas tecnologías estamos haciendo lo contrario. Tenemos una muestra de lo que puede venir en la utilización de las redes sociales, que, en vez de generar una sociedad más democrática, generan lo contrario. Estamos viendo cómo, a menudo, aumentan los sesgos y desequilibran la opinión pública de una manera que puede tener consecuencias políticas importantes (…)

Para asegurarnos de que las tecnologías involucradas en las neurotecnologías, en particular, la IA, beneficien y potencien a todos, deben incorporar y abordar una amplia gama de las necesidades y experiencias humanas. Las prácticas de diseño inclusivas ayudarán a los desarrolladores de sistemas a comprender y abordar barreras potenciales en un producto o entorno que podrían excluir involuntariamente a las personas. Esto significa que los sistemas neurotecnológicos basados en IA deben estar diseñado para comprender el contexto, las necesidades y expectativas de las personas que las utilizan.

Finalmente, además de las buenas prácticas y recomendaciones anteriores, se vuelve indispensable legislar estableciendo una capacidad de control de las personas respecto a la ausencia de sesgos.

Por el momento, esta propuesta de reconocimiento de los nuevos neuroderechos humanos abre un debate absolutamente necesario sobre el creciente papel de las neurotecnologías en nuestra sociedad y su enorme potencial disruptivo, hasta el punto de poder transformar la forma en que nos percibimos y cómo el mundo nos percibe e identifica. Parece prudente establecer salvaguardas básicas

31 SMITH, B., & SHUM, H. (2018). *The Future Computed Artificial Intelligence and its role in society. Microsoft Corporation,* pp. 57-73.

32 YUSTE, *Op. Cit.* pp. 29-30.

y universales, en términos de derechos humanos, que establezcan un marco normativo para estas tecnologías y que puedan ser incorporadas en los diferentes ordenamientos jurídicos en materia de derechos y garantías fundamentales.

5. La regulación de los neuroderechos humanos en marcha: Chile, primer país en presentar al mundo dos iniciativas legislativas frente a los riesgos de las neurotecnologías.

"No hay ninguna Constitución, ninguna ley en el mundo que hable de la privacidad mental. No hay precedentes y hay que definir legalmente la privacidad mental por primera vez, y para ello estoy trabajando con los abogados del Senado de Chile"

Rafael Yuste

Finalmente, el trabajo de Rafael Yuste en Chile dio sus primeros frutos el día 07 de octubre de 2020, cuando los Honorables Senadores Guido Girardi, Carolina Goic, Francisco Chahuán, Juan Antonio Coloma y Alfonso De Urresti, presentaron dos iniciativas legislativas ante el Congreso de Chile: el Proyecto de Reforma Constitucional Boletín N°13827-19, que modifica el artículo 19, número 1°, de la Carta Fundamental, para proteger la integridad y la indemnidad mental con relación al avance de las neurotecnologías; y el Proyecto de Ley Boletín N°13828-19, sobre protección de los neuroderechos y la integridad mental, y el desarrollo de la investigación y las neurotecnologías. Ambos proyectos se encuentran en el Primer Trámite Constitucional.

El proyecto de Reforma Constitucional, establecido en el Boletín N°13827-19 tiene como objeto la incorporación de un nuevo inciso en el artículo 19 de la Constitución Política de Chile de 1980 (en adelante CPR), estableciendo en el texto constitucional algunos elementos esenciales para la debida protección de los derechos humanos ante el desarrollo de la neurotecnología, constituyéndose así las ideas matrices del proyecto.

Reza el artículo 19 número 1 de la CPR[33]:

> Artículo 19.- La Constitución asegura a todas las personas:
> 1º.- El derecho a la vida y a la integridad y psíquica de la persona.
> La ley protege la vida del que está por nacer.
> La pena de muerte sólo podrá establecerse por delito contemplado en ley aprobada con quórum calificado.
> Se prohíbe la aplicación de todo apremio ilegítimo;

El actual proyecto de Reforma Constitucional prescribe[34]:

> Artículo Único: Intercálese el siguiente inciso segundo en el artículo 19 Numeral 1° de la Constitución Política del Estado, pasando el actual inciso segundo a ser tercero y así sucesivamente.
> "La integridad física y psíquica permite a las personas gozar plenamente de su identidad individual y de su libertad. Ninguna autoridad o individuo

33 Artículo 19 N° 1, de la Constitución Política de Chile de 1980.

34 Proyecto de Reforma Constitucional Boletín N° 13827, de 7 de octubre de 2020.

> podrá, por medio de cualquier mecanismo tecnológico, aumentar, disminuir o perturbar dicha integridad individual sin el debido consentimiento. Sólo la ley podrá establecer los requisitos para limitar este derecho, y los requisitos que debe cumplir el consentimiento en estos casos."

Se desprende de esta iniciativa legislativa el fin último de garantía y protección de la dignidad humana, presupuesto básico para el libre desarrollo de la personalidad y autodeterminación de los seres humanos, y que, encierra en su seno, un haz o conjunto de prerrogativas que, por una parte, se traduce en poderes invocables por las personas frente a ataques o transgresiones arbitrarias, y que, por otra, demanda de acciones positivas por parte del Estado enderezadas a brindar dicha protección.

La regla general que incorpora el nuevo inciso es la prohibición por parte de cualquier autoridad o individuo y por medio de cualquier mecanismo tecnológico de aumentar, disminuir o perturbar dicha integridad individual. Aquella integridad individual tiene una doble dimensión, por un lado, está compuesta por los datos cerebrales, mentales o neurodatos, y de otro lado, acuña los derechos de privacidad de la información producida por la actividad cerebral y el consentimiento; el derecho a la identidad personal y la autodeterminación; el derecho a la igualdad frente al aumento de capacidad cerebral; y el derecho al control de los sesgos algorítmicos.

Apostilla, además, que el tratamiento de los neurodatos requerirá como base única de legitimación el "consentimiento del afectado". Prescribiendo que, solo la ley podrá establecer los requisitos que debe cumplir el consentimiento, y solo la ley podrá limitar el ejercicio de este derecho de neuroprotección.

Por otra parte, el proyecto de Ley establecido en el Boletín N°13828-19 pretende introducir al ordenamiento jurídico chileno una especial protección de la "identidad mental", un reconocimiento como nuevo derecho humano del cerebro y su funcionalidad como núcleo del libre albedrío, pensamientos y emociones que caracterizan y diferencian a la especie humana[35].

El proyecto consta de 2 artículos: Artículo primero y Artículo segundo.

El Artículo primero, establece la ley sobre la neuroprotección y que regula el desarrollo de la investigación y el avance de las neurotecnologías. Está compuesto por 3 Títulos y 10 artículos.

El Título I establece las disposiciones generales. Lo componen los artículos 1 y 2 del proyecto, y en ellos se plasman los objetivos de la ley y algunas definiciones elementales.

El Título II instituye las medidas para proteger la integridad y la privacidad mental. Lo componen los artículos del 3 al 7 del proyecto, y en ellos se prescriben y categorizan, en general, los requisitos del tratamiento de los neurodatos o datos cerebrales.

El Título III, regula el desarrollo de la investigación y el avance de las neurotecnologías. Lo componen los artículos del 8 al 10 del proyecto, y en ellos se

35 Proyecto de Ley Boletín N°13828-19, de 7 de octubre de 2020.

manifiesta el rol garantista del Estado frente al derecho a la neuroprotección y las limitaciones a la actividad científica.

Por otro lado, el Artículo segundo, establece un mandato al legislador prescribiendo la modificación del Código Sanitario.

El objetivo de este proyecto es regular el contenido del derecho a la neuroprotección o neuroderechos establecido en la reforma constitucional correspondiente establecida en el Boletín N° 13827-19. Para ello, el presente proyecto de ley posee un marcado anclaje en la dignidad humana como meta principio subyacente al que debe siempre mirar la neurotecnología, incorporando, además, un elemento de igualdad de acceso frente al desarrollo de la técnica, que se materializa a través del igual acceso al aumento de la capacidad mental, para evitar cualquier atisbo de diferenciaciones arbitrarias, e ilícitas.

Asimismo, se establecen catálogo de definiciones, avanzando hacia un marco conceptual sobre la materia, es por ello que se definen conceptos como "neurotecnología", "interfaz cebero computadora" y "datos neuronales". Además, se establecen disposiciones para proteger los neuroderechos y la integridad mental, estableciendo como norma eje, la prohibición de cualquier forma de intervención de conexiones neuronales o cualquier forma de intrusión a nivel cerebral mediante el uso de neurotecnología, interfaz cerebro computadora o cualquier otro sistema o dispositivo, sin contar con el consentimiento libre, expreso e informado, de la persona o usuario del dispositivo, inclusive en circunstancias médicas. Aun cuando la neurotecnología posea la capacidad de intervenir en ausencia de la conciencia misma de la persona.

Finalmente, el proyecto establece reglas mínimas a la que deben sujetarse las investigaciones en el campo de la neurotecnología, estableciendo siempre como norte el respeto por la dignidad humana, estableciéndose, además, el deber en el Estado de fomentar las investigaciones y garantizar el acceso igualitario a los avances de la ciencia.

A nivel internacional, algunos países ya cuentan con normas regulatorias. Francia, por ejemplo, incorporó en su Código Civil una modificación a su legislación en bioética para regular el uso de la información cerebral como pruebas periciales. El Parlamento Europeo, en 2017 aprobó las "Normas de Derecho civil sobre robótica" una de las primeras acciones concretas en regulación, en este caso con recomendaciones a la Comisión Europea sobre normas de Derecho Civil sobre robótica[36]. Actualmente, con fecha 20 de octubre de 2020, el Parlamento aprobó tres informes que estudian cómo regular la inteligencia artificial para impulsar la innovación, el respeto de estándares éticos y la confianza en la tecnología. Los eurodiputados quieren que las normas contemplen el respeto a la intervención y la supervisión humana. El proyecto de informe centrado en las cuestiones éticas propone cómo garantizar la seguridad, la transparencia y la responsabilidad para evitar cualquier forma de sesgo y discriminación, así como el respeto de los derechos fundamentales. "El ciudadano es el centro de la

36 FUENTES, R., HIDALGO, M. C., & YUSTE, R. (2019). Neurotecnologías: los desafíos de conectar el cerebro humano y computadores. Santiago: Biblioteca del Congreso Nacional de Chile. p. 6.

propuesta", reconoce en una rueda de prensa el ponente del informe, el eurodiputado socialista español Ibán García del Blanco.

En Estados Unidos (en adelante, EE.UU), Los estudios jurídicos muestran dos ámbitos de emprendimiento regulatorio. El primero se vincula al manual *Law and Neuroscience* (de la Red de Investigación en Legislación y Neurociencias de la Fundación MacArthur de Estados Unidos), que comprende como temas prioritarios para legislar: el acrecentamiento artificial de la capacidad cognitiva, las interfaces cerebro-computadores y la inteligencia artificial[37]. El segundo se centra en la supervisión regulatoria que ha recaído sobre los dispositivos IoB de primera generación, y que, se ha dividido principalmente entre *la Food and Drug Administration (FDA) y la Federal Trade Commission (FTC)*[38]. Con el objetivo de mejorar la calidad del software integrados en dispositivos médicos, incluidos los dispositivos médicos IoB, la FDA ha publicado dos documentos de orientación sobre seguridad. El primero es titulado "Contenido de las presentaciones previas a la comercialización para la gestión de Ciberseguridad y dispositivos médicos: orientación para la industria y Personal de la Administración de Alimentos y Medicamentos", de fecha 2 de octubre de 2014, y proporciona orientación sobre los tipos de consideraciones de seguridad médicas que los fabricantes de dispositivos deben incorporar y divulgar al desarrollar sus dispositivos[39]. La segunda guía se titula "Gestión posmercado de la ciberseguridad en los dispositivos médicos: guía para la industria y personal de la Administración de Alimentos y Medicamentos, emitido el 28 de diciembre de 2016, y crea deberes de cuidado continuos para garantizar la seguridad de dispositivos en el mercado[40].

Como se explicó en secciones anteriores, los dispositivos IoB de primera generación son aquellos considerados como bienestar general y dispositivos de estilo de vida saludable en lugar de dispositivos médicos. En EE.UU, su principal regulador se convirtió en la FTC. Respecto de los dispositivos médicos, la actuación de la FTC se limita principalmente a la vigilancia policial de las declaraciones falsas, injustas o engañosas de las propiedades saludables en anuncios y marketing. En otras palabras, si el dispositivo está clasificado por la FDA como

37 MATWYSHYN, *Op.Cit.* pp. 132-148.

38 La Administración de Medicamentos y Alimentos (*Food and Drug Administration*, FDA) o Administración de Alimentos y Medicamentos) es la agencia del gobierno de los Estados Unidos responsable de la regulación de alimentos (tanto para personas como para animales), medicamentos (humanos y veterinarios), cosméticos, aparatos médicos (humanos y animales), productos biológicos y derivados sanguíneos.

Disponible en: https://es.wikipedia.org/wiki/Administraci%C3%B3n_de_Medicamentos_y_Alimentos

La FTC o Comisión Federal de Comercio es una agencia independiente del gobierno de los Estados Unidos, establecida en 1914 por el Acta de la Comisión Federal de Comercio. Su misión principal es promover los derechos de los consumidores y la eliminación y prevención de prácticas que atentan contra la libre competencia.

Disponible en: https://es.wikipedia.org/wiki/Comisi%C3%B3n_Federal_de_Comercio

39 U.S FOOD & DRUG ADMINISTRATION, 2018. Content of Premarket Submissions for Management of Cybersecurity in Medical Devices. [en línea]

40 U.S . FOOD & DRUG ADMINISTRATION, 2016. Postmarket Management of Cybersecurity in Medical Devices. [en línea]

médico o de "estilo de vida saludable" / recreativo tiene un impacto directo en el alcance jurisdiccional de la FTC.

Las próximas generaciones de IoB (cerebro-computador) probablemente requerirán un mayor nivel de participación regulatoria, no solo de esas dos agencias, sino también de la Comisión de Seguridad de Productos de Consumo (CPSC), la Oficina de Protección Financiera del Consumidor (CFPB) y la Comisión Federal de Comunicaciones (FCC), entre otros.

En Latinoamérica, México, permite el uso de neurotecnologías como pruebas judiciales[41].

Sin embargo, es menester destacar que, la iniciativa de Chile es pionera a nivel mundial. Propone regular de manera específica los efectos de las nuevas neurotecnologías en los derechos fundamentales de las personas, en especial, en la identidad individual. Proteger la esencia del ser humano ante la utilización de las neurotecnologías fuera del campo de la medicina curativa. Establecer limitaciones en aquellos procedimientos que se usan para predecir, anular o manipular el comportamiento del ser humano y controlar sus decisiones. Y, por último, restringir el uso de dispositivos tecnológicos neuronales para mejorar las capacidades intelectuales, con el fin de evitar las brechas o inequidades respecto de quienes no poseen los medios económicos o físicos para acceder a estos adelantos.

Capítulo II
La interfaz cerebro computadora a la luz del RGPD

1. Entendiendo la Interfaz Cerebro Computadora

Como seres vivos, las personas deben ser capaces de responder a los estímulos del ambiente para poder subsistir. En la vida diaria, esta respuesta se logra a través de dos vías esenciales: modificando el entorno en forma directa a través de los mecanismos musculares, o manifestando su pensamiento (comunicación), ya sea expresando sus sentimientos, deseos y/o ideas. No obstante, en algunos casos las funciones motrices se ven comprometidas debido a enfermedades como las lesiones medulares, infarto cerebral, esclerosis lateral amiotrófica, esclerosis múltiple, distrofia muscular, tumores o accidentes; por lo que sufren daños parciales o totales en subsistemas del cuerpo, lo que provoca perdida de la capacidad de respuesta natural (parcial o total) al entorno. Este tipo de discapacidad dio lugar al desarrollo de las tecnologías de Interfaz cerebro computadora[42].

La Interfaz Cerebro Computadora (BCI por su acrónimo en inglés) es una interfaz asistida por computador que permite la interacción directa entre el cerebro y el entorno de un sujeto, a través de actuadores enlazados al computador. Este tipo de interfaz surge de la necesidad de establecer un nuevo canal de comunicación entre un sujeto y su entorno; que no dependa de sus vías nerviosas

41 PARLAMENTO EUROPEO. (21 de octubre de 2020). euoparl.europa.eu. [en línea]

42 MORENO, I., SERRACÍN, J., SERRACÍN, S., & QUINTERO, J. (2019). Los sistemas de interfaz cerebro-computadora basado en EEG: características y aplicaciones. Revista de I+D Tecnológico, 15(2), p. 13. [en línea].

o musculares. Estas interfaces se basan en la captación de señales asociadas a procesos mentales, aplicadas para la resolución de problemas de comunicación en pacientes, registrando señales neurofisiológicas adquiridas a través de electroencefalografía (EEG por su acrónimo en inglés), magnetoencefalografía (MEG por su acrónimo en inglés), imagen por resonancia magnética funcional (fMRI por su acrónimo en inglés), el electrocorticograma (ECoG), la actividad de una sola neurona (SUA, del inglés *single unit activity*), entre otras; facilitando con ello la interacción con el entorno a personas con discapacidades motrices severas[43] .

Con independencia de la técnica de adquisición de señal encefalográfica utilizada, la BCI vista como máquina que traduce intenciones humanas en acciones tiene al menos tres partes bien diferenciadas: 1. Sensor: es el encargado de recoger la actividad cerebral. La gran mayoría de modalidades sensoriales utilizadas en BCI provienen de aplicaciones clínicas, como son el electroencefalograma, la imagen por resonancia magnética funcional, etc.; 2. Motor de Procesamiento de Señal: este módulo recoge la señal resultado de medir la actividad cerebral y aplica unos filtros para decodificar el proceso neurofisiológico que refleja la intención del usuario; y 3. Aplicación: es el módulo de interacción con el entorno y da forma a la aplicación final de la BCI. Puede ser mover una silla de ruedas o escribir con el pensamiento en una pantalla de ordenador, o mover un brazo robótico[44].

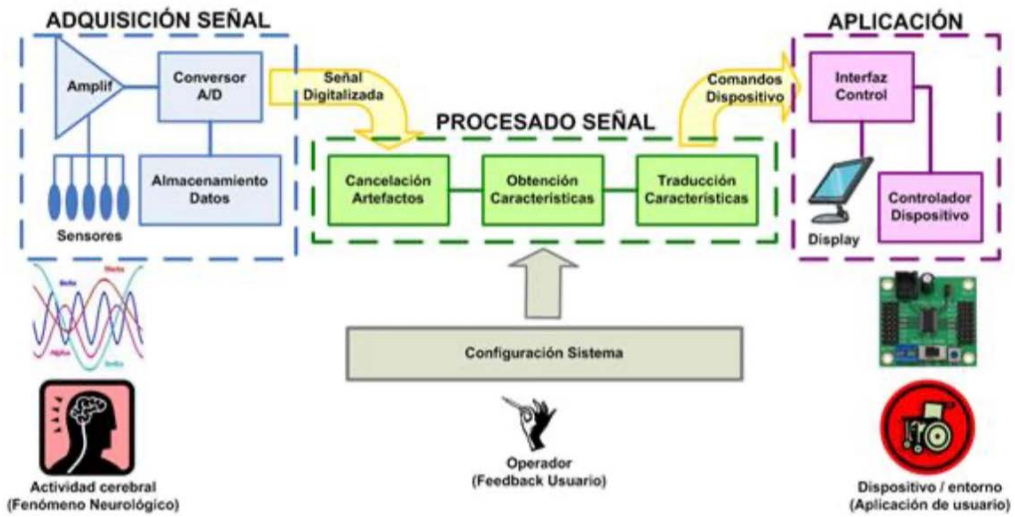

Figura 2. Diagrama de bloques de un sistema BCI: sensado de la señal, procesamiento de la misma y controlador del dispositivo (o aplicación)[45]

43 *Ídem.*

44 MINGUEZ, J. (s.f.). Tecnología de interfaz cerebro-computador. Departamento de informática e ingeniería de sistemas, p. 3. [en línea]

45 GALINDO, M. D. (2008). Introducción a los sistemas Brain Computer Interface. (F. Telefónica, Editor) [en línea]

La interfaz cerebro computador por la naturaleza de su método de adquisición de señales puede ser de tipo invasiva: mediante electrodos implantados en la superficie de la corteza cerebral o en su interior; o no invasiva: mediante electrodos ubicados en la superficie del cuero cabelludo[46].

Es importante señalar en este punto que se entiende por BCI a una interfaz hombre-máquina que utiliza para su funcionamiento únicamente información obtenida del sistema nervioso central y en particular del cerebro (es decir, actividad puramente cerebral). Por tanto, quedan excluidas todas las interfaces que utilicen de forma implícita o explícita información eléctrica resultante del movimiento muscular (que usualmente se denominan artefactos en el entorno de EEG). Un aspecto fundamental entonces es entender la generación del proceso de actividad cerebral y la modalidad elegida para medirla[47].

2. Privacidad y protección de datos en entornos de BCI

Actualmente, se encuentra vigente desde el 25 de mayo de 2018, el 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 (en adelante, RGPD)[48].

El texto constituye el marco general de regulación del tratamiento de datos de carácter personal en la Unión Europea, indica, además, que cualquier referencia que se contenga a la citada Directiva que se deroga, se entenderá hecha a dicho RGPD. De la misma manera, cualquier referencia al Grupo de protección de las personas en lo que refiere al tratamiento de datos personales establecido por el artículo 29 de la Directiva 95/46/CE se tiene que entender hecha al Comité Europeo de Protección de Datos establecido por este RGPD[49].

En cuanto a los objetivos de la reforma, podemos desprenderlos del título del cuerpo normativo. Por un lado, la regulación del derecho fundamental a la protección de datos y por otro, garantizar la libre circulación de los datos. Y por otro, la homogeneización del nivel de protección de datos en los distintos Estados de la Unión y adaptar la normativa de protección de datos al nuevo entorno tecnológico determinado por la expansión de internet y las redes sociales[50].

Al tratarse de un Reglamento, esta norma es directamente aplicable y no precisa ni admite transposición por parte de los Estados Miembros. De la misma forma que la normativa anterior, este Reglamento es aplicable al tratamiento de datos de personas físicas, no jurídicas.

46 Véase Capítulo I, apartado 1, párrafo 5°, del presente trabajo.

47 MINGUEZ, *Op. Cit.* p. 3.

48 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. DUOE número 119. [en línea]

49 Artículo 94, del RGPD.

50 Considerando 10, del RGPD.

El gran reto que nos trae este cuerpo normativo para la interfaz cerebro-computador será determinar si dentro de los grandes volúmenes de información procesada a través de dicha neurotecnología, se puede identificar a una persona; y, por ende, si se está ante un tratamiento de datos personales, actividad estrictamente regulada por el RGPD.

En consecuencia, para concluir si un procedimiento basado en BCI se debe adecuar a la normativa de privacidad, analizaremos qué tipo de datos se recolectan, si contienen información de carácter personal, y pueden ser identificativos de una persona natural.

2.1 Determinando el concepto de datos cerebrales o neurodatos.

No existe ningún ordenamiento jurídico que disponga de una definición o concepto de dato cerebral en sus leyes vigentes. No existe, actualmente, una definición jurídica o legal de dato cerebral o neurodato. Sin embargo, debemos reconocer que la definición dada por Chile en la iniciativa legal N°13828-19, puede ser una primera aproximación al concepto.

Reza el artículo 2 del Proyecto de Ley del Estado de Chile[51]:

> Se considerará para efectos de esta ley (…) C) Datos neuronales: Aquella información obtenida, directa o indirectamente, a través de los patrones de actividades de las neuronas, cuyo acceso está dado por neurotecnología avanzada, incluyendo sistemas de registro cerebrales tanto invasivos como no invasivos. Estos datos contienen una representación de la actividad psíquica, tanto consciente como subconsciente, y que corresponden al más íntimo aspecto de la privacidad humana.

En el área de la neurociencia, el neurobiólogo español Rafael Yuste se ha referido a los neurodatos como "otro órgano del cuerpo, no físico, sino que mental y sería el más importante de todos los órganos porque es el cual nos define como somos", enfatiza[52].

En biología, un órgano (del latín "organum", que significa un instrumento o herramienta) es una colección de tejidos que estructuralmente forman una unidad funcional diferenciada y especializada para realizar una función determinada. Su corazón, los riñones y los pulmones son ejemplos de órganos[53].

Los órganos generalmente funcionan dentro de sistemas o aparatos, es decir, compenetrados con otros órganos para la realización de una función. Así, en el aparato digestivo tenemos el hígado, el estómago o el intestino, a cada uno de los cuales corresponde una función.

Un sistema es un conjunto de órganos y estructuras que trabajan en conjunto para cumplir alguna función fisiológica en un ser vivo. El cuerpo humano posee más de cincuenta billones de células. Estas se agrupan en tejidos, los cuales

51 Proyecto de Ley Boletín N° 13.828-19, *Op. Cit*.

52 SENADO DE CHILE. (2019). Inteligencia Artificial y neuroderechos: la protección de nuestro cerebro podría quedar consagrado en la Constitución.

53 AMAT, A., MARTÍ, J., & DARNÉ, I. (2018). Investigamos cómo funciona el cuerpo humano. *Petit Talent Cientifics*, pp. 63-70.

se organizan en órganos y estos en aparatos o sistemas. Dentro de estos sistemas encontramos el sistema nervioso[54].

La función del sistema nervioso consiste en recibir los estímulos que le llegan tanto del medio externo como interno del organismo, organizar esta información y hacer que se produzca la respuesta adecuada. Los estímulos procedentes del medio externo son recibidos por los receptores situados en la piel, destinados a captar sensaciones generales como el dolor, tacto, presión y temperatura, y por los receptores que captan sensaciones especiales como el gusto, la vista, el olfato, el oído, la posición y el movimiento. Las señales (o impulsos) que llegan al sistema nervioso periférico, se transmiten a partir de estos receptores al sistema nervioso central, donde la información es registrada y procesada convenientemente. Una vez registradas y procesadas, las señales son enviadas desde el sistema nervioso central a los distintos órganos a fin de proporcionar las respuestas adecuadas. Desde un punto de vista funcional el sistema nervioso se divide en tres partes, sistema nervioso central, sistema nervioso periférico, y sistema nervioso autónomo[55].

Una enfermedad del sistema nervioso central puede afectar la médula espinal (mielopatía) o bien el cerebro (encefalopatía), los cuales son parte del sistema nervioso central. Cualquier enfermedad o lesión que afecte la médula espinal, desde la vértebra dorsal hacia abajo, puede causar una paraplejia, ya que esta estructura transmite las "instrucciones" del movimiento desde el cerebro a los órganos efectores y las sensaciones en sentido opuesto (temperatura, dolor, posición de los miembros, sensibilidad, etc.). Mientras que algunas personas que padecen de paraplejía pueden caminar hasta cierto punto, la mayoría dependen de una silla de ruedas, prótesis o de otros dispositivos para disponer de movilidad[56].

La ciencia y la tecnología van avanzando con descubrimientos que permiten hacer cosas que antes eran inimaginables. Su aplicación al cuerpo humano está modificando la forma en que entendemos y valoramos el cuerpo humano.

Nuestro cerebro produce impulsos eléctricos (potenciales de acción) que viajan a través de nuestras neuronas. Estos impulsos eléctricos producen ritmos que son conocidos como ondas cerebrales. Los impulsos eléctricos son información que viaja de neurona a neurona haciendo uso de cientos de miles de ellas para lograr transportarse y ejecutar una función determinada. La actividad de las ondas cerebrales puede ser observada a través de un EEG[57].

Las Interfaces Cerebro-Computadora intentan proveer al cerebro de un nuevo canal, no muscular, de comunicación y control para transmitir mensajes y comandos al mundo exterior.

De forma general, una BCI puede ser vista como un sistema de reconocimiento de patrones, donde el EEG es utilizado como la fuente primaria de

54 *Ídem*.

55 *Ídem*.

56 NIETO-SANPEDRO, M., GUDIÑO-CABRERA, G., TAYLOR, J., & VERDÚ, E. (2002). Trauma en el sistema nervioso central y su reparación. Revisiones en Neurociencia, pp. 34-35.

57 AZNAR CASANOVA, J. A. (2017). ub.edu. [en línea] Recuperado el 31 de octubre de 2020.

información. Los algoritmos de aprendizaje computacional son utilizados para aprender una función de inferencia a partir de dicha información, y los algoritmos ya entrenados pueden decodificar las señales de EEG en comandos a ejecutar por un dispositivo electro-mecánico. Algunas de las aplicaciones más comunes de la investigación en BCI están dirigidas a asistir a las personas con discapacidad motriz severa[58].

En este nuevo contexto "cuerpo humano-tecnología", el cuerpo humano ya no estaría compuesto tan solo de órganos biológicos tangibles, sino que formarían parte de él las diferentes técnicas de captación de señales neurofisiológicas (EEG / MEG / fMRI / ECoG / SUA) y un órgano mental, intangible, los "neurodatos" o impulsos eléctricos procesados y decodificados a través de una BCI. Dando origen de esta manera a un nuevo tipo de sistema nervioso, el "sistema neuro-tecnológico humano" el cual tiene como función sustituir las funciones desarrolladas por un órgano del sistema nervioso central y que han desaparecido producto de un daño o lesión.

Pero esto no termina aquí. Si volvemos al ejemplo de la película "Matrix", precisamente a la escena donde el protagonista aprende Kung fu mediante estimulación cerebral, permitiéndole dominar las artes marciales a pesar de nunca haberlas practicado antes en su vida, nos damos cuenta que existe un futuro distópico al que podríamos estar sometidos antes de lo imaginado.

La principal limitación de la inteligencia humana es la "cantidad de datos" que nuestra memoria puede manejar, ¿hemos imaginado alguna vez no tener esa limitación? ¿podría ocurrir que no solo sea posible comunicarse con dispositivos periféricos a través de la actividad del cerebro, sino que cierta información pueda ser introducida en el cerebro y en lugar de "leer la mente", que se pueda "escribir la mente"? ¿qué calificación tendrían esos datos?

Rafael Yuste, en comunión con otros profesionales del área de la neurociencia, está dando los primeros pasos hacia la posibilidad de "leer" y "escribir" la mente[59].

Ahora bien, del análisis de los antecedentes anteriores intentaremos construir jurídicamente un concepto de "datos cerebrales o neurodatos".

En sentido estricto, neurodato o dato cerebral es "toda información captada directa o indirectamente de un patrón de actividad neuronal a través de la utilización de neurotecnologías, incluyendo las técnicas de captación de señales neurofisiológicas, tanto invasivas como no invasivas. Dicha información decodificada representa la actividad psíquica consciente o subconsciente y forma parte del aspecto más intrínseco de la persona humana, la privacidad mental".

Si embargo, debido al rápido perfeccionamiento de la tecnología y de las oportunidades de manipulación del cuerpo humano que se generan, por ejemplo, la estimulación cerebral directa a partir de un aprendizaje asociativo, se vuelve indispensable ampliar el concepto jurídico de neurodato con el fin de prevenir

58 TORRES GARCÍA, 2016. *Op. Cit.* p. 19.

59 YUSTE, R., & DUPRE, C. (2017). *Non-overlapping Neural Networks in Hydra vulgaris. Current Biology,* 27(8), pp.1084-1096.

futuras vulneraciones del neuroderecho a la privacidad mental. De tal manera que, el concepto dado a los neurodatos en sentido estricto se ve complementado "con toda aquella información que no solo es captada, sino que también es incorporada al cerebro humano a través de neurotecnologías avanzadas".

2.2 La naturaleza jurídica de los datos cerebrales o neurodatos según el RGPD

Para determinar si los datos cerebrales o neurodatos pueden ser considerados un dato personal en los términos descritos por el RGPD, centraremos el análisis sobre los datos aportados por una BCI no invasiva, en este caso utilizaremos únicamente señales adquiridas mediante EEG, ya sea tomada de bases de datos preexistentes como tomando datos nuevos mediante un dispositivo adquirido.

Se ha optado por datos aportados por una BCI no invasiva, porque los resultados pueden ser extendidos a los datos que pudiera aportar una BCI invasiva, ya que estas últimas permiten obtener diagnósticos aún más precisos. Se ha elegido el EEG, porque es una técnica de exploración funcional del sistema nervioso central *ab antiquo*, mediante la cual se obtiene el registro de la actividad cerebral eléctrica en tiempo real[60].

El EEG mide la actividad eléctrica del cerebro mediante la colocación de electrodos sobre la superficie del cuero cabelludo. El número de electrodos o canales del EEG puede ser variable, desde unos cuantos hasta 256 canales. Los electrodos se colocan sobre el cuero cabelludo en posiciones establecidas por la federación internacional de sociedades de electroencefalografía y neurofisiología clínica, de acuerdo al Sistema Internacional 10-20. El nombre 10-20 indica el hecho de que los electrodos son ubicados a lo largo de la línea media en 10, 20, 20, 20, 20, y 10 % del total de la distancia *nasión* - *inión* (el *nasión* es la unión de los huesos de la nariz y el frontal, y el *inión* es la parte más prominente del occipital). El EEG es diariamente utilizado para el diagnóstico médico de patologías (por ejemplo, la epilepsia), el reconocimiento de emociones; y la interacción con dispositivos[61].

La señal del EEG es resultado de la interacción de un sinnúmero de procesos entre cientos de millones de neuronas organizadas en determinados grupos neuronales. Por ejemplo, procesos de control fisiológico, procesos de pensamiento y estímulos externos generan potenciales corticales en las correspondientes partes del cerebro que pueden ser registradas en el cuero cabelludo usando electrodos de superficie. Específicamente, los potenciales corticales son generados debido a potenciales post-sinápticos (excitatorios e inhibitorios) realizados por los cuerpos de célula y las dendritas de neuronas piramidales. De aquí que, el EEG sea un promedio de las múltiples actividades de muchas pequeñas zonas de la superficie cortical por debajo del electrodo; Las amplitudes de la señal del EEG están

60 RAMOS ARGÜELLES, F., MORALES, G., EGOZCUE, S., PABÓN, R. M., & ALONSO, M. T. (2009). Técnicas básicas de electroencefalografía: principios y aplicaciones clínicas. Anales Sistema Sanitario Navarra, 32(Supl.3), p. 70.

61 TORRES GARCÍA, A. (2016). Análisis y clasificación de electroencefalogramas (EEG) registrados durante el habla imaginada. (tesis doctoral) Instituto Nacional de Astrofísica, Óptica y Electrónica, pp. 16-18.

normalmente en un rango de 30 a 100 μV. La actividad rítmica del cerebro en un sujeto sano está caracterizada principalmente por los siguientes tipos de onda: delta δ (0-4 Hz.), theta θ (4-8 Hz.), alfa α (8-12 Hz.), beta ß (12 a 30 Hz.), y gamma γ (30-60 Hz.). Además, las señales EEG están clasificadas como no estacionarias, es decir, que son señales que presentan una frecuencia variable en el tiempo.

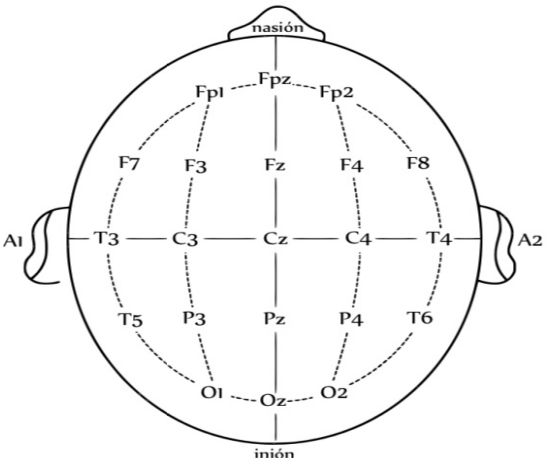

Figura 3: Posiciones estándares de los electrodos de acuerdo al Sistema Internacional 10-20. Acotaciones de las etiquetas de los canales: fp- pre-frontal, ffrontal, p- parietal, c- central, o- occipital, t- temporal, z- línea media, a-auricular; los números impares están sobre el lado izquierdo y, los números pares están sobre el lado derecho del individuo[62].

La actividad eléctrica, generada por el cerebro y que registra un EEG, varía dependiendo de diversos factores internos (edad, sexo, vigilia-sueño, estado psicoafectivo, factores metabólicos, patológicos) y externos (ambientales, toma de fármacos, procedimientos de activación, hiperventilación, estimulación luminosa), que actúan sobre una determinada base genética[63].

De esta forma, el **EEG del niño** y del recién nacido difiere significativamente del EEG del adulto. El proceso de crecimiento, maduración y desarrollo cerebral desde el nacimiento hasta la edad adulta se acompaña de cambios progresivos en la actividad electroencefalográfica, por lo que la variabilidad de la actividad eléctrica cerebral en el niño es mayor que en el adulto. Así, por ejemplo, un EEG normal en la actividad de fondo en vigilia en un **recién nacido a término,** la actividad de fondo es predominantemente continua e irregular. Está constituida fundamentalmente por frecuencias theta y delta de amplitud variable. Pueden verse ondas agudas frontales bifásicas, en ocasiones asíncronas. La simetría interhemisférica alcanza aproximadamente el 80% a las 36 semanas y el 100% a las 43 semanas. En tanto que, en un adolescente de entre **13 a 19 años,** el ritmo alfa está bien definido y alcanza una frecuencia de 9-11 Hz. Ocasionalmente la frecuencia del ritmo posterior puede alcanzar incluso los

62 GUTIERREZ, J. (2001). Análisis de señales en el neuromonitoreo. Revista Mexicana de Ingeniería Biomédica, 22(2), pp. 66-67.

63 ALONSO, X. (2015). Encefalografía en el niño. [en línea] Recuperado el 31 de octubre de 2020.

12-13 Hz. Hay una disminución progresiva de la proporción de ondas lentas posteriores de la juventud. Es común la presencia de ritmo mu y ondas lambda. Desde un punto de vista técnico, el registro EEG del niño también difiere del registro EEG del adulto, ya que existen diferencias anatómicas, fisiológicas y de capacidad de colaboración[64].

Además, existen enfermedades neurológicas específicas de la edad pediátrica que no están presentes en la edad adulta o enfermedades que solo puede padecer un género determinado. Ejemplo de esto último es el Síndrome de Rett, constituye una de las causas más frecuentes de retardo mental en mujeres. Es transmitida genéticamente, ligada al cromosoma "X" en forma dominante, y clínicamente asocia deterioro cognitivo progresivo, microcefalia adquirida y retardo mental severo con pérdida del uso pragmático de las manos y aparición de su signo más característico, que es el movimiento estereotipado en forma de "lavado de manos"[65].

Como mencionábamos en la sección anterior, en las BCIs basadas en EEG, a los mecanismos neurológicos o procesos empleados para generar las señales de control, se les denomina fuentes electrofisiológicas (neuromecanismo o estrategia mental). Las más utilizadas son, los potenciales corticales lentos, los potenciales P300, las imágenes motoras (ritmos sensoriales motrices mu y beta) y los potenciales evocados visuales. Para no profundizar en el tema, ya que no es el objetivo de este trabajo, solo mencionaremos un ejemplo de información neurofisiológica que nos puede aportar una fuente electrofisiológica. Los potenciales evocados visuales (PEV) son una fuente electrofisiológica, definida como la respuesta eléctrica generada por las células del córtex occipital ante un estímulo de la vía visual. La respuesta es registrada posicionando electrodos sobre el cráneo, y representa una medida objetiva y reproducible del funcionamiento de la vía visual completa, desde la mácula, los fotorreceptores, las células bipolares y ganglionares, hasta el córtex occipital. Comúnmente se realiza mediante la estimulación con damero del campo visual completo. La activación del estímulo puede ser de los tipos patrón-reverso (blanco-negro), patrón *ON/OFF* (blanco-gris-negro-gris) o *flash*. La característica principal de los PEV es que aporta datos fisiológicos cuantificables de latencia y amplitud. La duración típica de los registros es de 250 ms a partir del estímulo. Para cada tipo de estimulación, existe un patrón de respuesta definido por ondas positivas y negativas, de las cuales se mide su amplitud y su latencia. Estas características morfológicas permiten identificar determinadas disfunciones en la vía visual, orientando si predominan los fenómenos desmielinizantes, con retraso de los potenciales (aumento de latencia) o si predomina degeneración axonal en la vía visual (reducción de amplitud). Por otro lado, permiten realizar un seguimiento evolutivo, evaluando la posible eficacia de un tratamiento, o la progresión de una enfermedad[66].

64 ALONSO, *Op. Cit*.

65 Durante un tiempo se creyó que solamente se producía en mujeres. Sin embargo, ello no es así. Los casos de Síndrome de Rett en varones son escasos, mortal en la mayor parte antes de nacer o antes de cumplir el año de vida.

66 DE SANTIAGO RODRIGO, L. (2016). Análisis avanzado de señales potenciales evocados multifocales aplicados al diagnóstico de neuropatías ópticas (tesis doctoral). Universidad

Teniendo en cuenta lo descrito anteriormente, vamos a revisar lo que nos prescribe el RGPD respecto de lo que debemos entender por dato personal.

El artículo 4.1 del RGPD, define los "datos personales" como:

> Toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;

De esta definición se desprende que se ha adoptado un concepto amplio de dato personal ("toda información") y que para que un dato personal goce de protección jurídica es necesario, además de que se refiera a una persona física, que la identifique o la haga identificable. Por tanto, a los datos anónimos (cualquier información relativa a una persona física que no permita su identificación por el responsable del tratamiento de los datos o por cualquier otra persona, teniendo en cuenta el conjunto de medios que puedan razonablemente ser utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona) y a los datos convertidos en anónimos (es decir, datos que anonimizados no permitan la reidentificación del interesado) no se les aplican los principios de la protección de datos personales[67].

El Dictamen 4/2007 del Grupo de Trabajo del artículo 29 (actualmente, Comité Europeo de Protección de Datos), desglosó el concepto de datos de carácter personal que proporcionaba la Directiva en cuatro elementos: "toda información", "sobre", "persona física identificada o identificable" y "persona física", y los analizó por separado[68].

"Toda información", es una expresión que requiere una interpretación en sentido amplio y que el GT29 analizó desde 3 puntos de vista distintos: (i) la naturaleza, (ii) el contenido y (iii) el formato o soporte.

1. Desde la naturaleza: la expresión incluye todo tipo de afirmaciones sobre una persona, ya sean objetivas (un dato fisiológico) o subjetiva (una opinión).
2. Desde el contenido: incluye todos los datos con independencia de su contenido. Por ejemplo, datos sensibles, personales *strictu sensu* y familiares o de vida privada.
3. Desde el formato o soporte: incluye la información disponible en cualquier forma, por ejemplo, alfabética, numérica, gráfica, fotográfica o sonora. Desde este punto de vista, el concepto incluye la información conservada en papel, así como la información almacenada en una memoria de ordenador, utilizando un código binario, o en una cinta de video, por ejemplo. En particular, los datos que consisten en sonidos e imágenes están calificados como datos

de Alcalá, pp. 18-19.

67 Considerando 26, del RGPD.

68 Grupo del Trabajo del Artículo 29 [GT29], 2007, sobre el concepto de datos personales, pp. 6-26.

personales desde este punto de vista, en la medida en que pueden contener información sobre una persona.

"Sobre", por lo general, se entiende que la información versa sobre sobre una persona cuando se refiere a ella, si bien la información también puede referirse a un objeto o a un proceso y solo indirectamente a una persona. Para el GT29, (actualmente, Comité Europeo de Protección de Datos (CEPD), una información se refiere a una persona cuando exista un elemento "contenido" o un elemento "finalidad" o un elemento "resultado":

- Contenido: el elemento contenido está presente cuando se proporciona una información sobre una persona concreta, circunstancia que debe ser evaluada caso por caso y sin tener en consideración ni el propósito que pueda abrigar el responsable del tratamiento o un tercero, ni la repercusión que pueda tener sobre el interesado.
- Finalidad: Si el elemento "contenido" puede existir indistintamente del tratamiento que el responsable o el encargado pretenden realizar, no ocurre lo mismo con el elemento "finalidad", que sí depende del tratamiento en cuestión, considerándose que existe "*cuando los datos se utilizan o es probable que se utilicen, teniendo en cuenta todas las circunstancias que rodean el caso concreto, con la finalidad de evaluar, tratar de determinada manera o influir en la situación o el comportamiento de una persona*".
- Resultado: Finalmente, también debe entenderse que los datos versan "sobre" una persona en esas situaciones en que, "*teniendo en cuenta todas las circunstancias que rodean el caso concreto, es probable que su uso repercuta en los derechos y los intereses de determinada persona*".

Los tres elementos son independientes, *ergo* para considerar que la información versa "sobre" una persona, no es necesario que concurran los tres elementos simultáneamente, sino que bastará con que exista uno de ellos. Además, es posible que una misma información se refiera al mismo tiempo a diversas personas, porque en esa información concurra más de un elemento y uno se refiera a una persona y otro a otra.

"Persona física identificada o identificable", se considera que una persona física está "identificada" cuando, dentro de un grupo de personas, se la puede distinguir de los demás miembros del grupo. Por consiguiente, la persona física será "identificable" cuando, aunque no se la haya identificado todavía, sea posible hacerlo.

Por lo general, se entiende que una persona está directamente identificada cuando conoces su "nombre y apellidos", pues es el identificador más común y al que a menudo nos referimos. No obstante, en ocasiones el nombre y apellidos pueden no ser suficiente para identificar a una persona y deberán de combinarse con otros datos, como una dirección, una foto de perfil o un número de teléfono, que permitan identificar a la persona indirectamente.

"Persona física", el RGPD establece en el considerando 14 que «la protección otorgada por el presente Reglamento debe aplicarse a las personas físicas, independientemente de su nacionalidad o de su lugar de residencia, en relación con

el tratamiento de sus datos personales». Se trata, por lo tanto, de un derecho universal de las personas físicas que no se circunscribe a los nacionales o residentes de un determinado país.

El RGPD limita su protección a las personas físicas vivas, excluyendo a las **personas fallecidas**[69]. Tampoco se aplicará el Reglamento a los datos relativos a las **personas jurídicas**[70].

Ahora bien, el considerando 26 del RGPD al referirse al término «identificable» es decir, para determinar si una persona es identificable, señala que, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona. Esto significa que la mera e hipotética posibilidad de singularizar a un individuo no es suficiente para considerar a la persona como «identificable». Si, teniendo en cuenta «el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona», no existe esa posibilidad o es insignificante, la persona no debe ser considerada como «identificable» y la información no debe catalogarse como «datos personales»[71].

Según el GT29, el criterio del «conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona» debe tener especialmente en cuenta todos los factores en juego. Lo costoso de la identificación es un factor, pero no el único. La finalidad del tratamiento, la manera en que el tratamiento está estructurado, el rédito que espera obtener el responsable del tratamiento, los intereses individuales en juego, así como el riesgo de que se produzcan disfunciones organizativas (por ejemplo, un quebrantamiento del deber de confidencialidad) y los fracasos técnicos son todos ellos elementos que deben tenerse en cuenta.

Por otra parte, se desprende del RGPD que el tratamiento de los datos se refiere a cualquier operación o conjunto de operaciones efectuadas sobre datos personales o conjunto de datos personales, mediante procedimientos manuales o automatizados relacionadas con la recogida, el registro, la organización, la estructuración, la conservación, la adaptación o modificación, la extracción, la consulta, la utilización, la comunicación por transmisión, la difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción[72].

En consecuencia, los impulsos eléctricos *per se* conocidos como ondas cerebrales no necesariamente recogen una información que, entendida en los términos del RGPD permita identificar indiscutiblemente a la persona física de donde surgen. Sin embargo, el GT29 ha señalado que, en particular, los datos que consisten en sonidos e imágenes están calificados como datos personales en

69 Considerando 27, del RGPD.

70 Considerando 14, del RGPD.

71 GT29, *Op. Cit*. pp. 16-17.

72 Artículo 4.2 del RGPD.

la medida en que pueden contener información sobre una persona[73]. En este sentido, los impulsos eléctricos registrados en un EEG, procesados y decodificados, se traducen en datos fisiológicos, que, unidos a otras características personales internas o externas como la edad, sexo, historial clínico, patologías, información relacionada con factores de carácter psicológico, información de ficheros automatizados o manuales, entre otros, permiten determinar la identidad del titular de los datos. Por lo tanto, en todos esos casos en que los identificadores de que dispone el responsable del tratamiento o cualquier otra persona, que no permiten singularizar a una persona determinada, pero al combinarlos con otros datos (tanto se tenga conocimiento de su existencia como si no) es posible distinguir a la persona de otras, debe entenderse que la persona es identificable indirectamente. Por lo tanto, estamos frente a un dato personal cuyo tratamiento queda sometido a la normativa sobre protección de datos personales.

2.3 Categorizando los neurodatos en el RGPD.

En general en el ámbito de la salud, de acuerdo con Pila León Sanz, hay un solapamiento en cuanto al origen de los datos, y todos ellos pueden tener interés (en el ámbito sanitario) en función de la aplicación de los algoritmos que su utilicen para su análisis; unos proceden de la asistencia médica, otros de la investigáión, otros del área de la salud pública, o del ámbito administrativo, o simplemente son incorporados como consecuencia del registro de actividades sociales[74].

Como datos sensibles contienen todos los aspectos fisiológicos que nos conforman como seres humanos y que son el núcleo de la personalidad.

No todos los datos personales, tienen la categoría de sensibles. Serán considerados datos personales si se revelan aspecto de nuestra vida privada, pero, serán considerados datos sensibles si son datos que revelan aspectos íntimos de las personas.

El artículo 9.1 del RGPD califica como categorías especiales de datos personales aquellas 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".

Además, el GT29 ha señalado que[75]:

> Esta definición también se aplica a los datos personales cuando tienen una relación clara y estrecha con la descripción del estado de salud de una

73 GT29, *Op. Cit.* p. 8.

74 LEÓN SANZ, P. (2016). Bioética y explotación de grandes conjuntos de datos. En A. ANDÉREZ GONZALES, J. DÍAZ GARCÍA, F. ESCOLAR CASTELLÓN, & P. LEÓN SANZ, LA EXPLOTACIÓN DE DATOS DE SALUD. Retos, oportunidades y límites (pág. p.25). Sociedad Española de Informática y Salud.

75 GT29*, Op. Cit*. pp. 7-8.

> persona: los datos sobre el consumo de medicamentos, alcohol o drogas, así como los datos genéticos, son sin duda "datos personales sobre la salud", especialmente si están incluidos en un expediente médico. También habrá que considerar sensibles otros datos - por ejemplo, los datos administrativos (número de seguridad social, fecha de ingreso en un hospital, etc.) - contenidos en la documentación médica relativa al tratamiento de un paciente: si no fueran pertinentes en el contexto del tratamiento del paciente, no se habrían incluido, ni deberían haberse incluido, en un expediente médico.

Por consiguiente, indica el GT29, que todos los datos contenidos en documentos médicos, en historiales médicos y en sistemas de historial médico electrónico (HME) son datos personales sensibles.

En consecuencia, cuando estamos frente a un dato cerebral o neuronal que ha sido recogido en un documento médico (por ejemplo, un EEG) o en una historia clínica no automatizada o por un sistema HME, su tratamiento no solo está sujetos a todas las normas generales sobre protección de datos del RGPD, sino también a las normas particulares que rigen la protección de datos sensibles contenidas en el artículo 9 del RGPD[76].

2.4 Los "datos cerebrales o neurodatos" como dato de salud.

Dentro de los considerados datos sensibles o categorías especiales de datos establecidas en el artículo 9.1 del RGPD, encuentran especial atención los datos de salud.

El RGPD define en su artículo 4.15 como datos personales relacionados con la salud aquellos "relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud".

Por su parte, el Considerando 35 del RGPD apostilla:

> Entre los datos personales relativos a la salud se deben incluir todos los datos relativos al estado de salud del interesado que dan información sobre su estado de salud física o mental pasado, presente o futuro. Se incluye la información sobre la persona física recogida con ocasión de su inscripción a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia, de conformidad con la Directiva 2011/24/UE del Parlamento Europeo y del Consejo (9); todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su

76 Entendido el "dato cerebral o neuronal" en el sentido jurídico estricto, como "toda información captada directa o indirectamente de un patrón de actividad neuronal a través de la utilización de neurotecnologías, incluyendo las técnicas de captación de señales neurofisiológicas, tanto invasivas como no invasivas. Dicha información decodificada representa la actividad psíquica consciente o subconsciente y forma parte del aspecto más intrínseco de la persona humana, la privacidad mental".

fuente, por ejemplo un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro.

La definición de "datos de salud" se refiere a la información sobre la salud pasada, presente o futura de una persona sana o enferma, con enfermedades de carácter físico o psicológico, incluidas las adicciones en general y la información de los datos genéticos. Abarca, por tanto, los datos de carácter médico (aquellos que se refieran a enfermedades o problemas de salud, como aquellos datos que indiquen un buen nivel de salud) como aquellos otros que guarden relación con la salud (un tratamiento clínico o un historial médico)[77].

La doctrina ha manifestado que la definición que ha hecho el RGPD es amplia porque se ha basado en la opinión del GT29 que ha analizado la información que captan o procesan distintos dispositivos móviles, que antes no eran tenidos en cuenta a nivel de salud, pero que registran nuestros pasos, nuestro ritmo cardíaco, las calorías consumidas, etc. El GT29 determinó, en su documento de asesoramiento que, debido a la amplia gama de datos personales que pueden pertenecen a la categoría de datos de salud, esta categoría representa una de las áreas más complejas de datos y en el que los Estados miembros muestran una gran diversidad e inseguridad jurídica. que han de tener consideración de datos de salud[78]:

a) En este sentido los datos personales que se relacionan con la salud deberían incluir en particular todos los datos que pertenecen al estado de salud de un sujeto de datos, información sobre el registro de un individuo para la provisión de la Seguridad Social, información sobre pagos o elegibilidad para asistencia médica en lo que concierne al individuo, un número, símbolo en particular asignado a un individuo para únicamente identificar al individuo para objetivos de salud, cualquier información que sobre el individuo se reunió en el curso de la provisión de la Seguridad Social al individuo, la información sacada de las pruebas o exámenes del cuerpo o la sustancia corporal, incluyendo muestras biológicas, identificación de una persona como proveedor de asistencia médica al individuo, o cualquier información sobre, por ejemplo, una enfermedad, incapacidad, riesgo de enfermedad, HC, tratamiento clínico, o el estado real fisiológico o biomédico del sujeto de datos independiente de su fuente, como por ejemplo, de un médico o profesional de la salud, un hospital, un dispositivo médico, o una prueba in vitro diagnóstica.
b) Al respecto el GT29 señala que los datos de salud, abarcan un concepto mucho más amplio que el término médico. Asimismo, han concluido que la información como el hecho que una mujer ha roto su pierna (caso Lindqvist), que una persona lleva anteojos o lentes de contacto, datos sobre la capacidad intelectual o emocional de una persona, la información sobre los hábitos de fumar o consumo de alcohol, datos sobre alergias reveladas a entidades privadas (como las líneas aéreas) o a cuerpos públicos, cons-

77 MURILLO DE LA CUEVA, P. L. (2000). La publicidad de los archivos judiciales y la confidencialidad de los datos sanitarios. VII Congreso Nacional de Derecho Sanitario. Madrid: Fundación Mapfre Medicina.

78 GT29, 2015. *ANNEX - Health data in apps and devices,* pp. 1-2.

tituyen todos ellos datos sobre la salud. datos sobre las condiciones de salud utilizado en una emergencia (por ejemplo, información de que un niño que participa en un campamento de verano o similar evento sufre de asma); membresía de un individuo en un grupo de apoyo para pacientes (por ejemplo, cáncer grupo de apoyo), *Weight Watchers*, Alcohólicos Anónimos u otros grupos de autoayuda y apoyo con un objetivo relacionado con la salud; y la mera mención del hecho de que alguien está enfermo en un empleo contexto son todos los datos relacionados con la salud de los interesados individuales. Conclusiones sobre el estado de salud o riesgo de salud de una persona -con independencia de que estas conclusiones resulten o no certeras, legítimas u oportunas-.

c) También el GT29, asume que hay una categoría de datos personales generados por el modo de vivir de la sociedad a través de la utilización de las apps y dispositivos en general, que no será considerado como dato de salud. Esto concierne a los datos de los cuales no pueden obtenerse conclusiones razonables sobre el estado de salud de una persona, por ejemplo, si una aplicación solo contaría el número de pasos durante una sola caminata, sin poder combinar esos datos con otros datos de y sobre el mismo interesado, y en ausencia de un contexto médico específico en qué datos de la aplicación se utilizarán, no es probable que los datos recopilados tengan un impacto significativo en el privacidad del interesado y no requieren la protección adicional de la categoría especial de salud datos. Son solo datos personales sin procesar (estilo de vida de impacto relativamente bajo) (siempre que la aplicación no procesar datos de ubicación), no información a partir de la cual el conocimiento sobre la salud de esa persona pueda ser inferido.

En este sentido, por la generalidad y amplitud con que han sido tratados los datos de salud tanto en la normativa como en la doctrina, podemos entender comprendidos en ellos a los "datos cerebrales o neurodatos".

2.5 El consentimiento explícito como supuesto de tratamiento de los neurodatos en entornos BCI.

El artículo 4, apartado 11, del RGPD define el consentimiento como "toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen".

El artículo 7 del RGPD regula las condiciones para el consentimiento. Así, el numeral 1 del artículo 7 del RGPD señala que "cuando el tratamiento se base en el consentimiento de interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales".

Seguidamente, el consentimiento debe ser libre de manera que el consentimiento no es una base jurídica válida cuando existe un desequilibrio entre el interesado y el responsable del tratamiento. De tal manera, si el sujeto no es realmente libre para elegir, se siente obligado a dar su consentimiento o sufrirá consecuencias negativas si no lo da, entonces el consentimiento no puede considerarse válido. Si el consentimiento está incluido como una parte no negociable de las condiciones generales se asume que no se ha dado libremente. En

consecuencia, no se considerará que el consentimiento se ha prestado libremente si el interesado no puede negar o retirar su consentimiento sin perjuicio[79].

Que el consentimiento deba ser específico, quiere decir, que los datos se tratarán de modo leal y para fines concretos, distinguiendo el consentimiento otorgado para el tratamiento determinado de cualquier otra manifestación de voluntad destinada a otro asunto. En este sentido el artículo 7.2 del RGPD señala que "si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud del consentimiento se presentará de forma que se distinga claramente de los demás asuntos". El requisito de que el consentimiento deba ser «específico» tiene por objeto garantizar un nivel de control y transparencia para el interesado[80].

En la misma línea el Considerando 32 del RGPD prescribe que "el consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos".

Además, el GT29, ha señalado que de conformidad con el artículo 5 del RGPD, el requisito de transparencia es uno de los principios fundamentales, estrechamente relacionado con los principios de lealtad y licitud. Facilitar información a los interesados antes de obtener su consentimiento es esencial para que puedan tomar decisiones informadas, comprender qué es lo que están autorizando y, por ejemplo, ejercer su derecho a retirar su consentimiento. Si el responsable no proporciona información accesible, el control del usuario será ilusorio y el consentimiento no constituirá una base válida para el tratamiento de los datos[81].

Se deberá informar sobre:

✓ La identidad y los datos de contacto del responsable y del delegado de protección de datos, si cabe. ✓ Los derechos de los interesados. ✓ El derecho del interesado a retirar su consentimiento. ✓ Los fines y la base jurídica del tratamiento de los datos. ✓ El interés legítimo del responsable. ✓ Los destinatarios de los datos personales. ✓ El derecho a presentar una reclamación.	✓ Requisito legal o contractual que obliga a la comunicación de datos, y las consecuencias de no facilitar los datos pedidos. ✓ Si se va a proyectar un fin ulterior distinto del fin inicial, se informará antes del nuevo tratamiento. ✓ La transferencia de datos a un tercer país o a una organización internacional. ✓ El plazo de conservación de los datos personales. ✓ Decisiones automatizadas, como la elaboración de perfiles.

79 GT29, 2017. Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, revisadas por última vez y adoptadas el 10 de abril de 2018, pp. 5-33.

80 *Ídem*.

81 Artículos 13 y 14 del RGPD.

El RGPD establece claramente que el consentimiento debe ser inequívoco, es decir, requiere una declaración del interesado o una clara acción afirmativa, lo que significa que siempre debe darse el consentimiento mediante una acción o declaración. Debe resultar evidente que el interesado ha dado su consentimiento a una operación concreta de tratamiento de datos. El GT29 manifiesta que una "clara acción afirmativa" significa que el interesado debe haber actuado de forma deliberada para dar su consentimiento a ese tratamiento en particular y que, en cualquier caso, el consentimiento siempre debe obtenerse antes de que el responsable del tratamiento comience a tratar datos personales para los que se requiere consentimiento[82].

Por otra parte, el artículo 7.2 del RGPD mandata que la solicitud de consentimiento se presentará "de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo"

Finalmente, dispone el numeral 3 del artículo 7 del RGPD "el interesado tendrá derecho a retirar su consentimiento en cualquier momento". La retirada del consentimiento, por ejemplo, en el ámbito de la investigación no afectará a la licitud del tratamiento basado en el consentimiento hasta ese momento.

Estas condiciones, también deben entenderse aplicable al consentimiento explícito requerido en el tratamiento de datos relativos a la salud.

El artículo 9.1 RGPD califica los datos de salud como una categoría especial de datos personales, prohibiendo su tratamiento como regla general. No puede ser de otra manera pues los datos de salud se sitúan en la esfera más íntima de la persona, particularmente, aquellos datos que su conocimiento por otros puede menoscabar el desarrollo de la personalidad. Su tratamiento puede provocar que el responsable o un tercero que ha accedido a los datos vulnere derechos fundamentales del titular de los datos, particularmente, el derecho a la no discriminación. De ahí que los datos de salud disfruten de un estatuto jurídico particular dada su calificación como categoría especial de dato.

Dentro de los supuestos descritos en el artículo 9.2 del RGPD que legitiman el tratamiento de las categorías especiales de datos del interesado se encuentra "su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados". Este supuesto de legitimidad del tratamiento de categorías especiales de datos personales, está también previsto en la Carta de los Derechos fundamentales de la Unión Europea que señala que los datos se tratarán «sobre la base del consentimiento de la persona afectada».

La diferencia con el consentimiento como criterio de licitud del tratamiento de las categorías generales de datos personales, es la exigencia añadida de que el consentimiento sea explícito. Por tanto, para que el tratamiento de categorías especiales de datos personales sea lícito, no es suficiente la obtención del consentimiento , entendido este último en los términos del artículo 4.11 del RGPD, es decir, "toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen", pues esta

82 *Ídem*

definición reconoce el consentimiento implícito como válido para las categorías generales de datos personales pero dicho consentimiento resulta insuficiente en el tratamiento de las categorías especiales de datos personales.

El consentimiento explícito que da el interesado es para el tratamiento de categorías especiales de datos personales «con uno o más de los fines especificados». De forma que, cuando el tratamiento es para varios fines, debe darse el consentimiento explícito para todos ellos.

Según el GT29, el término explícito se refiere a la manera en que el interesado expresa el consentimiento. Significa que el interesado debe realizar una declaración expresa de consentimiento confirmando dicho consentimiento en una declaración escrita y firmada del interesado. Por lo tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. En el entorno digital, un interesado puede emitir su consentimiento explícito, rellenando un impreso electrónico, enviando un correo electrónico, cargando un documento escaneado con su firma o utilizando una firma electrónica. También las declaraciones verbales pueden ser una forma lo suficientemente manifiesta de expresar el consentimiento explícito, sin embargo, puede resultar difícil para el responsable del tratamiento demostrar que se cumplieron todas las condiciones para el consentimiento explícito válido cuando se grabó la declaración[83].

El consentimiento del menor para tratar datos personales los consentimientos dados por pacientes que tengan 16 años, son plenamente válidos. No obstante, lo anterior, los Estados Miembros de la Unión Europea pueden establecer una edad inferior siempre que no sea inferior a 13 años[84].

Además, el responsable deberá ser capaz de demostrar en todo momento que el titular de los datos otorgó en su momento el consentimiento de tratamiento de datos. Esta obligación implica conservar y/o registrar la cláusula informativa junto con la declaración afirmativa del titular (firma del documento físico o registro del clicado en la página web, por ejemplo).

No obstante, el supuesto de legitimidad del tratamiento de categorías especiales de datos personales en virtud del consentimiento explícito contenida en el artículo 9.2 letra a) del RGPD no es una regla absoluta desde el momento en que la norma establece que este consentimiento explícito puede ser limitado en virtud del Derecho de la Unión o de los Estados miembros, que podrán prescribir, que la regla general de prohibición de tratamiento de categorías especiales de datos establecida en el artículo 9.1 del RGPD no pueda ser levantada por el consentimiento del interesado.

Además, el RGPD establece algunas excepciones al "consentimiento explícito" y señala que podrán tratarse los datos de salud sin el consentimiento explícito del interesado en los siguientes casos[85]:

i. Por razones médicas, si el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del traba-

83 *Ídem*.

84 Artículo 8.1 del RGPD.

85 Artículo 9.1 letras h), i) j) del RGPD.

jador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social.

ii. Por razones de salud pública, si el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional.

iii. Por razones de investigación científica o estadística, si el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

Finalmente, el RGPD señala que el tratamiento de las categorías especiales de datos personales, como los datos de salud, debe ser realizado "por un profesional sujeto a la obligación de secreto profesional o bajo su responsabilidad"[86].

Capítulo III
Responsabilidad proactiva (accountability) y enfoque de riesgo en entornos BCI

1. El principio de responsabilidad proactiva o *Accountability*

Una de las novedades más relevantes del RGPD es la inclusión del principio de responsabilidad proactiva o *accountability*. Así, el apartado segundo del artículo 5 establece que "el responsable del tratamiento será responsable del cumplimiento de los principios relativos al mismo y capaz de demostrarlo".

Este principio se encuentra desarrollado en el artículo 24 del RGPD al establecer la obligación general del responsable del tratamiento de aplicar las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el reglamento, teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas.

Este principio requiere que el responsable del tratamiento realice un análisis de los datos que trata y de las demás circunstancias que rodean el tratamiento para después adoptar las medidas reales y eficaces que garanticen que el mismo cumple los requisitos legales. Para ello deberá tener en cuenta "la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa

86 Artículo 9.3 RGPD.

probabilidad y gravedad para los derechos y libertades de las personas físicas". estas medidas habrán de revisarse y actualizarse siempre que sea necesario.

Cabe indicar que el GT29 en su dictamen 3/2010 sobre el principio de responsabilidad explicaba su significado y alcance[87].

El GT29 señalaba que "proviene del mundo anglosajón donde es de uso general y donde se da una comprensión ampliamente compartida de su significado, aunque la definición exacta de "responsabilidad" resulta compleja en la práctica". Y también que "el término apunta sobre todo al modo en que se ejercen las competencias y al modo en que esto puede comprobarse".

Así, al hablar de Responsabilidad proactiva o *accountability* debemos considerar dos elementos:

a) La necesidad de que el responsable del tratamiento adopte medidas adecuadas y eficaces para aplicar los principios de protección de datos.

b) La necesidad de demostrar, si así se requiere, que se han adoptado las medidas adecuadas y eficaces.

El GT29 considera, por ejemplo, que se podrían aplicar medidas revisión interna, evaluación, establecimiento de políticas escritas y vinculantes de protección de datos para asegurar el cumplimiento de los criterios de calidad de datos; establecimiento de procedimientos que garanticen la identificación correcta de todas las operaciones de tratamiento de datos y el mantenimiento de un inventario de operaciones de tratamiento; nombramiento de un responsable de protección de datos o delegado de protección de datos; realización de evaluaciones de impacto sobre la privacidad en circunstancias específicas; formación a los miembros del personal, en especial a los directores de recursos humanos y a los administradores de tecnologías de la información; establecimiento de un mecanismo interno de tratamiento de quejas; etc.[88]

En este sentido el Considerando 74 del RGPD explica que:

> Debe quedar establecida la responsabilidad del responsable del tratamiento por cualquier tratamiento de datos personales realizado por él mismo o por su cuenta. En particular, el responsable debe estar obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el presente Reglamento, incluida la eficacia de las medidas. Dichas medidas deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como el riesgo para los derechos y libertades de las personas físicas.

De esta forma, el simple cumplimiento normativo es condición necesaria, pero no suficiente.

2. El enfoque de riesgo.

Para el cumplimiento del principio de "*Responsabilidad Proactiva"* el responsable y encargado de tratamiento deberán previamente realizar un análisis

87 GT 29, 2010. Opinión 3/2010 on the principle of accountability (WP 173).

88 *Ídem*.

y **estudio del cumplimiento en materia de protección de datos basado en el riesgo**. Es decir, deberán analizar qué medidas de protección de datos son necesarias implantar para garantizar el cumplimiento del RGPD, en función de naturaleza, alcance, contexto y finalidades del tratamiento de datos que realicen, así como de los riesgos o probabilidades de intromisión en los Derechos y libertades de los interesados.

El enfoque de aproximación al Riesgo se recoge en el art. 24 y en los considerandos 75 a 77 del RGPD.

El riesgo es un elemento con el que convivimos habitualmente, cualquier actividad que realizamos tiene implícito un riesgo. Las modalidades del riesgo son tan variadas como nuestra propia actividad, algunos de los riesgos que habitualmente son analizados pueden ser: de negocio, laborales, corporativos, de salud, medioambientales, riesgos para la seguridad de la información, etc. A esta variedad de riesgos cabría añadir una nueva vertiente: los riesgos para los derechos y libertades de las personas derivados de los tratamientos de datos personales.

Con el objeto de poder tener una idea aproximada de lo que debe de ser considerado como riesgo, el considerando 75 del RGPD enumera aquellos **tratamientos de datos que pueden ser considerados de riesgo para los derechos y libertades de los interesados**:

i. Tratamiento que puede dar lugar problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo;

ii. Tratamiento que pueda privar a los interesados de sus derechos y libertades o impedirles ejercer el control sobre sus datos personales;

iii. Tratamiento de datos personales sensibles que revelen origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas;

iv. Tratamiento en la elaboración de perfiles, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales;

v. Tratamiento de datos personales de personas físicas vulnerables, en particular de niños;

vi. Tratamiento que implica una gran cantidad de datos personales y que afecta a un gran número de interesados.

Por otro lado, y según el considerando 76, dicho riesgo deberá ponderarse en algunos casos y evaluarse de forma objetiva en otros para determinar si existe un "riesgo" o un "riesgo alto".

Por último, dado que el RGPD puede introducir situaciones de indeterminación en cuanto al riesgo a considerar en el tratamiento de datos, el considerando 77 establece que podrá proporcionarse más orientación sobre la identificación y evaluación de los riesgos del tratamiento de datos, y sobre la identificación de enfoques de mejores prácticas para mitigar esos riesgos, a través de códigos de conducta, certificaciones y directrices aprobadas por Comité el Grupo de Trabajo del artículo 29, o incluso por el propio Delegado de Protección de Datos de la Organización.

El análisis de riesgos en sistemas de gestión de seguridad de la información, en concreto de los datos personales, nos permite el estudio y la evaluación del riesgo asociado a los activos de la organización en cuestión, se basa en el análisis de las vulnerabilidades en la gestión y tratamiento de datos personales, cuyos resultados le ayudarán al responsable del tratamiento a la toma de las mejores decisiones respecto de la seguridad en el tratamiento de datos personales.

Las normas ISO 31000 y 31010 han establecido que todas las actividades de una organización, implican un riesgo de todos los tipos y tamaños, tanto internos como externos, y en concreto la norma ISO 27001:2005 nos define "análisis de riesgo", como la utilización sistemática de la información disponible para identificar peligros y estimar riegos[89].

A modo de ejemplo, la norma ISO 31000 define el proceso del análisis y la gestión de riesgos en cuatro fases:

i. Diseño y definición del marco de trabajo

ii. Implementar y gestionar el riesgo

iii. Verificar los resultados mediante procesos de auditoría

iv. Añadir mejoras al marco inicial del trabajo

La propuesta de esta norma, similar a cualquier metodología de análisis y gestión del riesgo, se basa en un sistema de mejora continua de la calidad. Un sistema en permanente evolución que técnicamente se conoce como ciclo PDCA o ciclo de Deming[90]:

89 ISO 31000. (2018). Gestión del riesgo. [en línea] Recuperado el 02 de noviembre de 2020.

90 El ciclo de Deming (de Edwards Deming), también conocido como ciclo PDCA (del inglés *Plan-Do-Check-Act*) o PHVA (de la traducción oficial al español como Planificar-Hacer-Verificar-Actuar) o *espiral de mejora continua*, es una estrategia basada en la mejora continua de la calidad, en cuatro pasos, según el concepto ideado por Walter A. Shewhart, amigo y mentor de William E. Deming que lo enseñó en el Japón de los años 1950. A veces también es, por ello, denominado *Ciclo Deming-Shewhart.(Véase, https://es.wikipedia.org/wiki/Ciclo_de_Deming)*

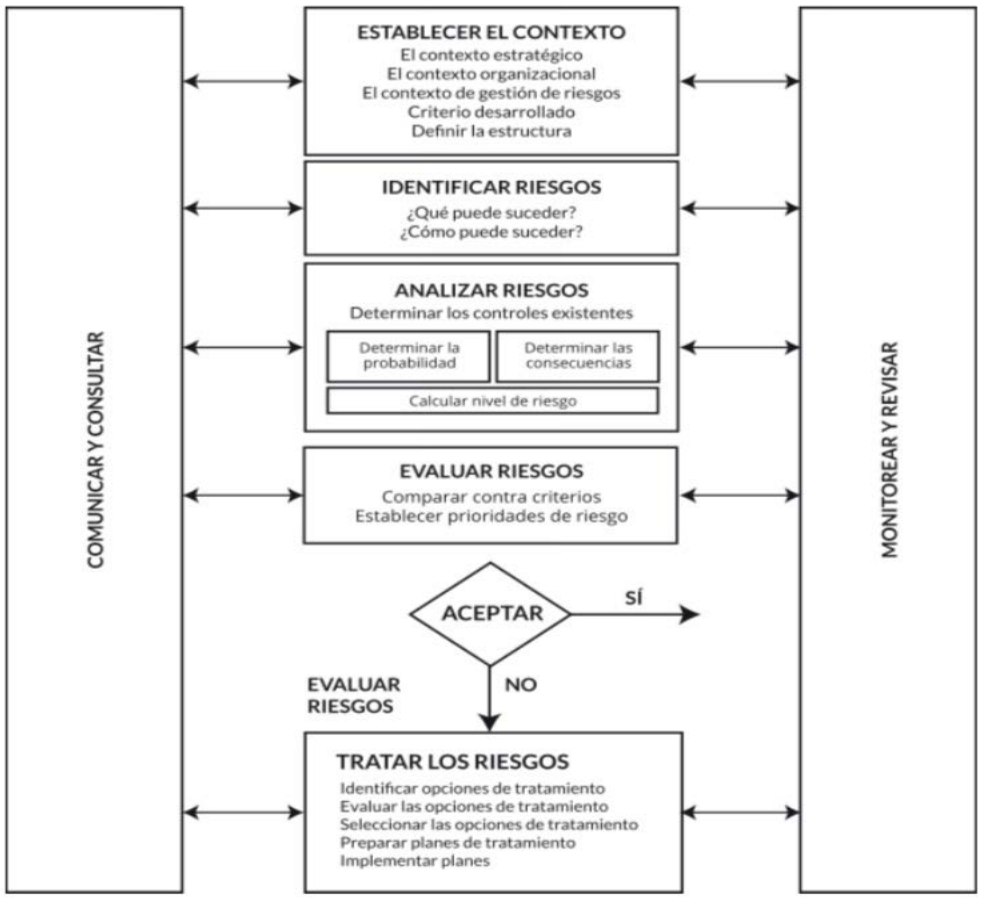

Figura 4: Pasos básicos en la gestión de riegos[91]

En otros términos, podemos decir que el riesgo es cambiante según el entorno (marco físico, tecnológico, intervención humana, etc.) y la adecuación de las medidas para paliar riesgos también debe de ser cambiante y en permanente adecuación y revisión. El proceso por el que se revisan las medidas para paliar los riesgos se denomina auditoría y es un mecanismo básico y necesario para garantizar la efectividad de las medidas para la seguridad de los tratamientos de datos y garantizar los derechos y libertades de las personas[92].

En el ámbito europeo, el legislador ha tenido en consideración estos precedentes en los Estándares Internacionales de Calidad para mejorar la salvaguardia y seguridad de la protección de datos personales a la hora de elaborar el RGPD y en específico señala en el Considerando 83:

91 ISOTOOLS EXCELLENCE. (2018). isotools.org. [en línea] Recuperado el 02 de noviembre de 2020.

92 La AEPD tiene publicada una guía de análisis de riesgos que facilitará la labor a los responsables del tratamiento www.agpd.es

> A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales.

De esta forma, todo tratamiento de datos requerirá un análisis general previo de los riesgos, que no debe confundirse con la EIPD propiamente tal. El análisis de riesgo previo forma parte de la EIPD, por lo tanto, si a partir de este análisis se determina que no es obligatoria la realización de una EIPD, sólo tendremos la obligación de gestionar los riesgos del tratamiento a través de un análisis de riesgos preliminar[93]. Si la evaluación preliminar general de riesgos indica que una operación concreta o un grupo de operaciones de tratamiento de datos personales plantea un probable «alto riesgo» o se ha producido un cambio en los riesgos en las operaciones que ya iniciaron, el responsable deberá llevar a cabo una Evaluación de impacto de protección de datos antes de continuar con la operación u operaciones. El RGPD aclara que esto podría ser, en especial, cuando la operación se realiza con el apoyo de las nuevas tecnologías[94].

93 Al respecto el artículo 32 del RGPD señala: Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo (…)

94 El GT29 en sus directrices sobre la EIPD, aprobadas por el CEPD, estableció nueve criterios que debían tenerse en cuenta para determinar si una operación de tratamiento puede dar lugar a un «alto riesgo»: 1. Evaluación o puntuación, incluida la elaboración de perfiles y la predicción, especialmente de «aspectos relacionados con el rendimiento en el trabajo, la situación económica, la salud, las preferencias o intereses personales, la fiabilidad o el comportamiento, la situación o los movimientos del interesado» (considerandos 71 y 91). Algunos ejemplos de esto podrán incluir a una institución financiera que investigue a sus clientes en una base de datos de referencia de crédito o en una base de datos contra el blanqueo de capitales y la financiación del terrorismo o sobre fraudes, o a una empresa de biotecnología que ofrezca pruebas genéticas directamente a los consumidores para evaluar y predecir los riesgos de enfermedad/salud, o a una empresa que elabore perfiles de comportamiento o de mercadotecnia basados en el uso o navegación en su sitio web. 2. Toma de decisiones automatizada con efecto jurídico significativo o similar: tratamiento destinado a tomar decisiones sobre los interesados que produce «efectos jurídicos para las personas físicas» o que les afectan «significativamente de modo similar» [artículo 35, apartado 3, letra a)]. Por ejemplo, el tratamiento puede provocar exclusión o discriminación contra las personas. El tratamiento con poco o ningún efecto sobre las personas no coincide con este criterio específico. Las futuras directrices sobre elaboración de perfiles del GT29 contendrán más explicaciones sobre estas nociones. 3. Observación sistemática: tratamiento usado para observar, supervisar y controlar a los interesados, incluidos los datos recogidos a través de redes u «observación sistemática [...] de una zona de acceso

público» [artículo 35, apartado 3, letra c)]. Este tipo de observación representa un criterio porque los datos personales pueden ser recogidos en circunstancias en las que los interesados pueden no ser conscientes de quién está recopilando sus datos y cómo se usarán. Además, puede resultar imposible para las personas evitar ser objeto de este tipo de tratamiento en espacios públicos (o espacios de acceso público). 4. Datos sensibles o datos muy personales: esto incluye las categorías especiales de datos personales definidas en el artículo 9 (por ejemplo, información sobre las opiniones políticas de las personas), así como datos personales relativos a condenas e infracciones penales según la definición del artículo 10. Un ejemplo sería un hospital general que guarda historiales médicos de pacientes o un investigador privado que guarda datos de delincuentes. Más allá de estas disposiciones del RGPD, puede considerarse que algunas categorías de datos aumentan el posible riesgo para los derechos y libertades de las personas. Estos datos personales se consideran sensibles (dado que este término es de uso común) porque están vinculados a hogares y actividades privadas (como comunicaciones electrónicas cuya confidencialidad debe ser protegida), porque afectan al ejercicio de un derecho fundamental (como datos de localización cuya recogida compromete la libertad de circulación) o porque su violación implica claramente graves repercusiones en la vida cotidiana del interesado (como datos financieros que podrían usarse para cometer fraude en los pagos). En este sentido, puede resultar relevante que los datos ya se hayan hecho públicos por el interesado o por terceras personas. El hecho de que los datos personales sean de acceso público puede considerarse un factor en la evaluación si estaba previsto que estos se usaran para ciertos fines. Este criterio también puede incluir datos tales como documentos personales, correos electrónicos, diarios, notas de lectores de libros electrónicos equipados con opciones para tomar notas e información muy personal incluida en aplicaciones de registro de actividades vitales. 5. Tratamiento de datos a gran escala: el RGPD no define qué se entiende por gran escala, aunque el considerando 91 ofrece alguna orientación. En cualquier caso, el GT29 recomienda que se tengan en cuenta los siguientes factores, en particular, a la hora de determinar si el tratamiento se realiza a gran escala: a. el número de interesados afectados, bien como cifra concreta o como proporción de la población correspondiente; b. el volumen de datos o la variedad de elementos de datos distintos que se procesan; c. la duración, o permanencia, de la actividad de tratamiento de datos; d. el alcance geográfico de la actividad de tratamiento. 6. Asociación o combinación de conjuntos de datos, por ejemplo, procedentes de dos o más operaciones de tratamiento de datos realizadas para distintos fines o por responsables del tratamiento distintos de una manera que exceda las expectativas razonables del interesado. 7. Datos relativos a interesados vulnerables (considerando 75): El tratamiento de este tipo de datos representa un criterio debido al aumento del desequilibrio de poder entre los interesados y el responsable del tratamiento, lo cual implica que las personas pueden ser incapaces de autorizar o denegar el tratamiento de sus datos, o de ejercer sus derechos. Entre los interesados vulnerables puede incluirse a niños (se considera que no son capaces de denegar o autorizar consciente y responsablemente el tratamiento de sus datos), empleados, segmentos más vulnerables de la población que necesitan una especial protección (personas con enfermedades mentales, solicitantes de asilo, personas mayores, pacientes, etc.), y cualquier caso en el que se pueda identificar un desequilibrio en la relación entre la posición del interesado y el responsable del tratamiento. 8. Uso innovador o aplicación de nuevas soluciones tecnológicas u organizativas, como combinar el uso de huella dactilar y reconocimiento facial para mejorar el control físico de acceso, etc. El RGPD deja claro (artículo 35, apartado 1, y considerandos 89 y 91) que el uso de una nueva tecnología, definida «en función del nivel de conocimientos técnicos alcanzado» (considerando 91), puede hacer necesario realizar una EIPD. Esto es debido a que el uso de dicha tecnología puede implicar nuevas formas de recogida y utilización de datos, posiblemente con un alto riesgo para los derechos y libertades de las personas. De hecho, las consecuencias personales y sociales del despliegue de una nueva tecnología pueden ser desconocidas. Una EIPD ayudará al responsable del tratamiento a entender y abordar tales riesgos. Por ejemplo, algunas aplicaciones del

3. Riesgos específicos de privacidad y seguridad de los neurodatos en BCI

La interfaz cerebro-computador es una neurotecnología avanzada que tiene acceso a los **datos neurales o cerebrales de una persona**, una información extremadamente sensible tanto por su carácter vinculado a salud, como por el vinculado a los pensamientos íntimos y privados de la persona.

Podemos estudiar los impactos de las BCI en las personas en 3 escenarios diferentes, cuya principal técnica de captura de señales eléctricas es el EEG[95]:

a) **Monitorización**: abarca todo el abanico de aplicaciones relacionadas con recoger la actividad del cerebro de forma pasiva para identificar patrones relacionados con nuestra actividad cognitiva, emocional o motora. Las BCI pasivas permiten una adaptación al entorno al considerar el estado mental o la percepción del usuario. Por ejemplo, los datos que estiman la carga de trabajo mental de los estudiantes mediante la monitorización de su EEG se pueden usar para optimizar el aprendizaje, ajustando el nivel de dificultad y repitiendo el contenido que puede no haberse entendido bien. una de las aplicaciones más extendidas es el *Neurofeedback*. Este tipo de terapia permite a los pacientes aprender a regular la actividad de ciertas ondas en su cerebro, mediante la retroalimentación basada en estímulos visuales, auditivos o táctiles. Así, se expone al paciente a una pantalla cuya imagen se nubla o aclara en función de la regulación que este haga de sus ondas cerebrales. De esta forma, se consigue un entrenamiento en el control de dichas ondas. Esta técnica se utiliza en padecimientos como el trastorno por déficit de atención e hiperactividad.

b) **Evaluación/Diagnóstico**: procesar la actividad cerebral para poder evaluar capacidades cognitivas o emocionales en base a patrones cerebrales. Además, también se pueden identificar patrones anormales relacionados con patologías mentales como puede ser la depresión o la epilepsia. **Actualmente, existen sistemas de EEG Portátiles,** que pueden grabar estudios hasta por meses.

c) **Interacción/Intervención**: procesar la actividad cerebral en tiempo real para interaccionar con un dispositivo como puede ser un teclado en la pantalla. Cuando esta interacción tiene un objetivo de rehabilitación se suele hablar de **intervención**.

«Internet de las cosas» podrían tener un impacto significativo sobre la vida diaria y la privacidad de las personas y, por tanto, requieren una EIPD. 9. Cuando el propio tratamiento «impida a los interesados ejercer un derecho o utilizar un servicio o ejecutar un contrato» (artículo 22 y considerando 91). Esto incluye operaciones de tratamiento destinadas a permitir, modificar o denegar el acceso de los interesados a un servicio o a un contrato. Un ejemplo de esto sería cuando un banco investiga a sus clientes en una base de datos de referencia de crédito con el fin de decidir si les ofrece un préstamo. (GT29, 2017. Directrices sobre la evaluación de impacto relativa a la protección de datos [EIPD] y para determinar si el tratamiento "entraña probablemente un alto riesgo" a efectos del Reglamento 2016/679, págs. 10-12)

95 BALLARIN USIETO, P., & MINGUEZ, J. (s.f.). La importancia de la ciberseguridad en *brain-computer interfaces.* [en línea] Recuperado el 02 de noviembre de 2020

Por consiguiente, en un tratamiento de datos personales en entornos BCI los riesgos para el interesado son principalmente los que puedan afectar a sus derechos y libertades relacionados con 3 aspectos fundamentales:

a) La naturaleza de los datos registrados en un EEG
b) El uso de inteligencia artificial en el procesamiento de los datos.
c) El desarrollo de nuevos canales de comunicación con el cuerpo a través de los cuales se puedan generar ataques contra el usuario.

En cuanto a la naturaleza de los datos, la situación es crítica principalmente en los procesos de monitorización de la actividad cerebral del usuario y de diagnóstico. En el procedimiento de monitorización, el EEG se utiliza de forma controlada para conocer las reacciones emocionales o cognitivas de las personas. Determinados marcadores en el EEG como la asimetría en alfa, o los N100, P200, N200, P300, pueden permitir conocer las emociones, preferencias o gustos de una persona hacia opciones políticas, orientación sexual, consumo, etc; o incluso acceder a sus capacidades cognitivas como la memoria, aprendizaje, o resolución de problemas, entre otras[96].

En aplicaciones de diagnóstico, los resultados de un EEG pueden detectar comportamientos anómalos del cerebro como epilepsia, hemorragias, desórdenes del sueño, encefalitis, tumores, migrañas, o el abuso de drogas o alcohol. En algunos casos, se trata de información de la cual ni siquiera el propio usuario tiene por qué ser consciente de ella. Esta información podría ser procesada para obtener, con algoritmos de predicción, la probabilidad de que elabore ciertos sentimientos o pueda desarrollar ciertas enfermedades[97].

Por otro lado, los datos brutos reales generados por los dispositivos de EEG son fundamentales para optimizar los algoritmos de Inteligencia Artificial en los que se basa la interfaz cerebro-computador. La problemática en torno a la IA pivota en la inexistencia de la ética algorítmica, y la facilidad con que se produce el sesgo algorítmico. Debemos tener presente que los humanos dirigen todo el ciclo de vida de la IA. Dado que los humanos tenemos sesgos, estos pueden trasladarse con gran facilidad a la IA en todo ese ciclo de vida. El reto es que son muy difíciles de identificar y más aún de corregir[98].

Es tan fundamental el uso ético de los algoritmos para los derechos fundamentales de los afectados que con fecha 20 de octubre de 2020, la Eurocámara aprobó el primer informe sobre IA. El texto aboga por la creación de un marco regulatorio de principios éticos que sea de obligado cumplimiento para los softwares, algoritmos y datos incluidos en la inteligencia artificial, la robótica y las tecnologías conexas que se desarrollen, se distribuyan o se usen en la Unión Europea. El eurodiputado García del Blanco ha enfatizado que "todos ellos deberán

96 *Ídem.*

97 *Ídem.*

98 MONASTERIO ASTOBIZA, A. (2017). Ética algorítmica: Implicaciones éticas de una sociedad cada vez más gobernada por algoritmos. Dilemata (24), 186-204.

respetar la dignidad humana, el cumplimiento de los derechos fundamentales y la legalidad de la Unión. Si no, no podrán operar en Europa"[99].

En el texto, García del Blanco propuso también la creación de una Agencia Europea para la Inteligencia Artificial (IA), que coordine la acción de los estados en este ámbito. El informe propone "una perspectiva humano céntrica en el desarrollo de la tecnología, que sirva a los intereses de la ciudadanía y permita el control humano durante todo el proceso de desarrollo y uso, lo que conllevaría la habilitación de un *botón rojo* de parada por si fuera necesario. Al mismo tiempo, nuestra regulación debe garantizar un equilibrio entre la protección de los derechos de los ciudadanos y la eliminación de complejidad burocrática para la investigación, desarrollo e implementación"[100].

Además, propone definir como "de alto riesgo" las tecnologías "que conlleven un riesgo significativo de quiebra de estos principios éticos; garantizar que las tecnologías se desarrollen, implementen y utilicen de manera segura, transparente y responsable; y asegurar que los datos usados o producidos por ellas respetan el valor de la dignidad humana y evitan el sesgo y la discriminación".

En relación con la privacidad, García del Blanco recordó que "tanto el Reglamento General de Protección de Datos como la Carta de Derechos Fundamentales son plenamente de aplicación" en este campo.

En cuanto a los riesgos del procesamiento de datos basados en IA en relación a la seguridad de la información en BCI, generalmente las amenazas ocurren en escenarios donde el atacante logra acceder temporalmente a la diadema (EEG) e introduce contenido malicioso en el firmware, este malware puede crear y enviar datos EEG manipulados. La consecuencia que deriva de esta brecha de seguridad, es el robo de datos con fines de extorción o venta a terceros y la posible manipulación de los datos enviados al dispositivo de control cercano, por lo que la aplicación no lleva a cabo su objetivo, o peor, lleva a cabo un objetivo lucrativo para el atacante. Otros ejemplos de riesgos de interacción máquina-cuerpo humano, es la posibilidad de envían estímulos al usuario y estudiar la respuesta cerebral no consciente para obtener información privada, verbigracia, gustos, preferencias, PIN de tarjetas, entre otros[101].

Elevada importancia en este ámbito ha desarrollado la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, autoridad de control que se caracteriza por una participación activa, normativa y colaborativa. En el mes de febrero de 2020 publicó una Guía de adecuación al RGPD de tratamientos que incorporan inteligencia artificial dando a conocer una serie de recomendaciones para los productos y servicios que emplean distintas técnicas, entre ellas, el aprendizaje

99 GARCÍA DEL BLANCO, "Hemos marcado el camino para que la inteligencia artificial en la UE sirva para mejorar nuestras vidas y nuestro entorno", [en línea) Recuperado el 20 de octubre de 2020.

100 PARLAMENTO EUROPEO, 2020. *DRAFT REPORT with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies*. pp.1-34 [en línea] Recuperado el 02 de noviembre de 2020.

101 *Ídem*.

automático. En la referida guía también aborda las amenazas específicas en los componentes IA y ha señalado que[102]:

> Existen tipologías estudiadas de ataque y defensa a componentes de IA. Entre las medidas de seguridad, se recomienda prestar especial atención a aquellas que gestionen estos tipos de amenazas:
>
> - ✓ Acceso y manipulación del conjunto de datos de entrenamiento, previo a la configuración del modelo, por ejemplo, mediante técnicas de envenenamiento con patrones adversos.
> - ✓ Inclusión de troyanos y puertas traseras durante el proceso de desarrollo de la IA, bien en el propio código o en las herramientas de desarrollo.
> - ✓ Manipulación de la API de usuario para realizar accesos al modelo, tanto a nivel de caja negra como de caja blanca, para la manipulación de parámetros del modelo, filtrado del modelo a terceros, ataques a la integridad o disponibilidad de las inferencias.
> - ✓ Ataques por "adversarial machine learning" por lo que sería necesario un análisis de la robustez y control de la alimentación con datos al modelo.
> - ✓ Ataques por imitación de patrones que se conoce serán admitidos por el sistema.
> - ✓ Reidentificación de los datos personales incluidos en el modelo (inferencia de pertenencia o inversión del modelo) por parte de usuarios internos y externos.
> - ✓ Fraude o engaño a la IA por parte de los interesados, especialmente en casos que puedan suponer un perjuicio para otros interesados, lo que implica la necesidad de realizar un análisis de la robustez ante dichas actuaciones y la realización de auditorías.
> - ✓ Filtrado a terceros de resultados de perfilado o decisiones inferidas por la IA (también relacionado con las API's de usuario).
> - ✓ Filtrado o acceso a los logs resultado de las inferencias generadas en la interacción con los interesados.

De otro lado, en cuanto al desarrollo de nuevos canales de comunicación con el cuerpo, generalmente estos riesgos están asociados a las aplicaciones de las BCI en contexto de interacción/intervención máquina/usuario, y suponen nuevos escenarios de riesgos debido al crecimiento exponencial de los dispositivos conectados, la seguridad poco adecuada de los mismos y el desconocimiento de las medidas básicas de seguridad por parte de los usuarios. En los escenarios de usuarios con discapacidad motora, los riesgo relacionados con la privacidad proceden del uso secundario de los datos procedentes de la actividad cerebral del

102 AEPD, (2020). Adecuación al RGPD de tratamientos que incorporan Inteligencia artificial. Una introducción. pp.42-43.

usuario, de los cuales se pueden obtener, no solamente la condición de discapacidad por degeneración de la actividad de la corteza motora, sino también otra información relativa a enfermedades mentales. Además, la actividad cerebral es monitorizada durante varias horas continuadas de uso del dispositivo, por lo que potencialmente puede obtenerse información relativa a sus emociones y motivaciones durante todas las actividades que realiza en su día a día, por ejemplo, la interacción con otras personas, visualización de la televisión, etc.[103]

Sobra decir, que los fabricantes de estas nuevas tecnologías tienen a su disposición millones de muestras de información de EEG en sus servidores en la nube generados por miles de usuarios cada vez que usan la diadema. Estos datos se pueden usar tanto para impulsar la investigación interna como para su comercialización dentro de un mercado muy lucrativo[104]. En estas circunstancias, no parece raro imaginar la cantidad de empresas que recogen información de los usuarios, crean perfiles lo más concretos posibles y venden todo ello a terceros sin el consentimiento del afectado. De hecho, en el mundo cibernético aquellas entidades ya poseen nombre y apellido, los *"data brokers"*[105].

4. Medidas de seguridad adecuadas para la protección de los neurodatos en entornos BCI

El artículo 32 del RGPD establece que las medidas técnicas y organizativas apropiadas para garantizar el nivel de seguridad adecuado al riesgo se definen en función del estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas. No se establecen medidas de seguridad estáticas, corresponderá al responsable determinar aquellas medidas de seguridad que son necesarias para garantizar la confidencialidad, la integridad y la disponibilidad de los datos personales, por lo tanto, un mismo tratamiento de datos puede implicar medidas de seguridad distintas en función de las especificidades concretas en las que tiene lugar dicho tratamiento de datos.

Cuando nos referimos a confidencialidad nos referimos a cualquier medida que impida el acceso no autorizado a los datos personales, mecanismos para evitar la vulneración del deber de secreto o medidas encaminadas para garantizar los privilegios de acceso a la información o los datos personales. Por ejemplo, hablamos de medidas por la que se conceden o deniegan los permisos para acceder a un sistema de información o la gestión de las altas y bajas del personal de una organización. En seguridad se viene refiriendo a la confidencialidad con el principio de la "necesidad de saber" *("need to know")* principio mediante el cual

103 BALLARIN USIETO & MINGUEZ, *Op. Cit.*

104 *Ídem.*

105 Se denominan Data Brokers, a las empresas que recopilan información ,incluida información personal sobre consumidores, de una amplia variedad de fuentes con el fin de revender dicha información a sus clientes, que incluyen tanto empresas del sector privado como agencias gubernamentales. (Véase, https://en.wikipedia.org/wiki/Information_broker)

únicamente deben acceder a la información aquellas personas que lo precisen en virtud de las funciones que deben desempeñar en su trabajo o su cargo[106].

La integridad de los datos personales o de la información se relaciona con el principio de exactitud o de calidad de los datos. De acuerdo con este principio, el responsable del tratamiento de los datos debe garantizar que aquellos datos que vienen siendo tratados son acordes a la realidad o veraces y adecuados a la finalidad para la que fueron obtenidos y, además, se garantiza su inalterabilidad[107].

La disponibilidad es la característica de la seguridad por la que se intenta mantener los datos accesibles para su consulta, localización y rectificación cuando sea necesario. Dicho de otra forma, esta característica garantiza los derechos de acceso, rectificación, supresión, derecho de limitación del tratamiento, derecho a la portabilidad de los datos, y el derecho a la portabilidad de los datos. En definitiva, se trata de una característica de la seguridad estrechamente vinculada a los derechos de los interesados[108].

Para garantizar estos tres factores de la seguridad son necesarias medidas tanto de índole técnica como de índole organizativo, sobre todo en entornos de BCI donde nos enfrentamos a una categoría especial de datos que requieren "el nivel más alto" de protección. A continuación, analizaremos cada una de las medidas que nos ofrece el RGPD.

4.1 Neutralidad tecnológica y Privacidad desde el diseño (PbD) y por defecto

El Considerando 15 del RGPD establece que "a fin de evitar que haya un grave riesgo de elusión, la protección de las personas físicas debe ser tecnológicamente neutra y no debe depender de las técnicas utilizadas"[109]

Por su parte el Considerando 78 del Reglamento, afirma que "la protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos del presente Reglamento"[110]

La neutralidad tecnológica, comúnmente definida como "la libertad de los individuos y las organizaciones de elegir la tecnología más apropiada y adecuada a sus necesidades y requerimientos para el desarrollo, adquisición, utilización o comercialización, sin dependencias de conocimiento implicadas como la información o los datos»[111], está íntimamente relacionada con el principio de privacidad desde el diseño y por defecto.

106 INSTITUTO NACIONAL DE CIBERSEGURIDAD [INCIBE]. (s.f.). incibe.es. pp.6-7. [en línea] Recuperado el 02 de noviembre de 2020,

107 *Ídem*.

108 *Ídem*.

109 Considerando 15 RGPD.

110 Considerando 78 RGPD.

111 Neutralidad tecnológica. (2018). *Wikipedia, La enciclopedia libre*. (Disponible en https://es.wikipedia.org/w/index.php?title=Neutralidad_tecnol%C3%B3gica&oldid=105001172, fecha última consulta: 03.10.2020)

Por su parte, el concepto protección de datos desde el diseño y por defecto, recogido en el artículo 25 del RGPD, consiste en incorporar, desde las primeras fases de todo proyecto, medidas técnicas y organizativas apropiadas, teniendo en cuenta factores como el estado de la técnica, el coste de la aplicación, la naturaleza, ámbito, contexto y fines del tratamiento o los riesgos del tratamiento para los derechos y libertades de los afectados, aquellas medidas permitirán cumplir los requisitos del Reglamento y proteger los derechos de los interesados, produciéndose una relación integral entre las nuevas tecnologías y la protección de datos personales[112].

En palabras de *Ann Cavoukian,* los principios de Privacidad por Diseño pueden ser aplicados a todos los tipos de información personal, pero deben ser aplicadas con vigor especial a datos delicados tales como información médica y datos financieros. La robustez de las medidas de privacidad tiende a ser correspondiente con la sensibilidad de los datos. Así, para cumplir con la privacidad desde el diseño se deben practicar 7 principios fundamentales[113]:

i. Proactivo, no Reactivo; Preventivo no Correctivo El enfoque de Privacidad por Diseño (PbD por sus siglas en inglés) está caracterizado por medidas proactivas, en vez de reactivas. Anticipa y previene eventos de invasión de privacidad antes de que estos ocurran. PbD no espera a que los riesgos se materialicen, ni ofrece remedios para resolver infracciones de privacidad una vez que ya ocurrieron – su finalidad es prevenir que ocurran. En resumen, Privacidad por Diseño llega antes del suceso, no después.

ii. Privacidad como la Configuración Predeterminada Todos podemos estar seguros de una cosa – ¡Lo predeterminado es lo que manda! La Privacidad por Diseño busca entregar el máximo grado de privacidad asegurándose de que los datos personales estén protegidos automáticamente en cualquier sistema de IT dado o en cualquier práctica de negocios. Si una la persona no toma una acción, aun así la privacidad se mantiene intacta. No se requiere acción alguna de parte de la persona para proteger la privacidad – está interconstruida en el sistema, como una configuración predeterminada.

iii. Privacidad Incrustada en el Diseño La Privacidad por Diseño está incrustada en el diseño y la arquitectura de los sistemas de Tecnologías de Información y en las prácticas de negocios. No está colgada como un suplemento, después del suceso. El resultado es que la privacidad se convierte en un componente esencial de la funcionalidad central que está siendo entregada. La privacidad es parte integral del sistema, sin disminuir su funcionalidad.

112 Agencia Española de Protección de Datos y a la Asociación Española para el Fomento de la Seguridad de la Información, ISMS *Forum Spain,* (2016). *Código de buenas prácticas en protección de datos en proyectos de Big Data,* p. 20.

113 CAVOUKIAN, A. (2016). Privacidad por diseño los 7 principios fundamentales. Mediascope. pp.1-2 [en línea] Recuperado el 03 de noviembre de 2020.

iv. Funcionalidad Total – "Todos ganan", no "Si alguien gana, otro pierde" Privacidad por Diseño busca acomodar todos los intereses y objetivos legítimos de una forma "ganar-ganar", no a través de un método anticuado de "si alguien gana, otro pierde", donde se realizan concesiones innecesarias. Privacidad por Diseño evita la hipocresía de las falsas dualidades, tales como privacidad versus seguridad, demostrando que sí es posible tener ambas al mismo tiempo.

v. Seguridad Extremo-a-Extremo – Protección de Ciclo de Vida Completo Habiendo sido incrustada en el sistema antes de que el primer elemento de información haya sido recolectado, la Privacidad por Diseño se extiende con seguridad a través del ciclo de vida completo de los datos involucrados – las medidas de seguridad robustas son esenciales para la privacidad, de inicio a fin. Esto garantiza que todos los datos son retenidos con seguridad, y luego destruidos con seguridad al final del proceso, sin demoras. Por lo tanto, la Privacidad por Diseño garantiza una administración segura del ciclo de vida de la información, desde la cuna hasta la tumba, desde un extremo hacia el otro.

vi. Visibilidad y Transparencia – Mantenerlo Abierto Privacidad por Diseño busca asegurar a todos los involucrados que cualquiera que sea la práctica de negocios o tecnología involucrada, esta en realidad esté operando de acuerdo a las promesas y objetivos declarados, sujeta a verificación independiente. Sus partes componentes y operaciones permanecen visibles y transparentes, a usuarios y a proveedores. Recuerde, confíe, pero verifique.

vii. Respeto por la Privacidad de los Usuarios – Mantener un Enfoque Centrado en el Usuario Por encima de todo, la Privacidad por Diseño requiere que los arquitectos y operadores mantengan en una posición superior los intereses de las personas, ofreciendo medidas tales como predefinidos de privacidad robustos, notificación apropiada, y facultando opciones amigables para el usuario. Hay que mantener al usuario en el centro de las prioridades.

A su vez, la privacidad por defecto implica la adopción de medidas técnicas y organizativas cuya finalidad es garantizar que por defecto sólo se traten aquellos datos que sean necesarios para los fines del tratamiento[114]. Entre las estrategias básicas que permiten implementar la privacidad por defecto tenemos:

i. Recogida de datos: analizar los tipos de datos que se recaban con un criterio de minimización en función de los productos y servicios seleccionados por el usuario;

ii. Tratamiento de los datos: analizar los procesos asociados a dichos tratamientos para que se acceda a los mínimos datos personales necesarios para ejecutarlos;

114 Ídem.

iii. Conservación: implementar una política de conservación de datos que permita, con un criterio restrictivo, eliminar aquellos datos que no sean estrictamente necesarios;

iv. Accesibilidad: limitar el acceso por parte de terceros a dichos datos personales.

4.2 Evaluación de Impacto (EIPD): Privacy Impact Assessments (PIA)

Una segunda herramienta que nos proporciona el RGPD para hacer frente a los riesgos que producen las tecnologías de la información en la protección de datos, como es el caso de un planteamiento de trabajo en entornos de *BCI* está establecida en su artículo 35.1 que reza:

> Cuando sea probable que un tipo de tratamiento, en particular si utiliza 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 de 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[115]

En términos simples, podemos definir una EIPD como un análisis de los riesgos que un producto o servicio puede entrañar para la protección de datos de los afectados teniendo en consideración la categoría de los datos objeto del tratamiento, la finalidad del mismo, la necesidad de su realización y las tecnologías utilizadas. El objetivo principal de ese análisis, es la gestión de dichos riesgos mediante la adopción de las medidas necesarias para eliminarlos o mitigarlos[116].

En entornos de *BCI*, no solo es necesaria una EIPD, sino que es una obligación legal, y es así, no solo por las tecnologías que se utilizan o las categorías de datos que se tratan, sino porque ese tratamiento de datos personales está destinado a ser una actividad constante y sistemática destinada a obtener ciertos resultados que lleven a decisiones directamente aplicables a los individuos titulares de dichos datos[117].

El contenido esencial de una EIPD viene determinado por el artículo 35.7 del RGPD, lo explicaremos en términos simples, para que sea mejor comprendido[118]:

i. Operaciones de tratamiento previstas y de los fines de tratamiento: Es básicamente una lista detallada del tratamiento de datos, incluyendo: los datos que usa, los detalles de sus responsables y encargados, la base legal o los períodos de retención aplicados a los datos.

ii. Evaluación de la necesidad y la proporcionalidad: Se debe incluir una evaluación de la necesidad y la proporcionalidad de las operacio-

115 Artículo 35.1 RGPD.

116 AEPD, *Op. Cit.* p. 22.

117 Artículo 35.3 RGPD.

118 Artículo 35.7 RGPD.

nes de tratamiento con respecto a su finalidad superando el juicio de proporcionalidad.

iii. Evaluación de los riesgos: Por ejemplo, dificultad para obtener el consentimiento expreso para datos especialmente protegidos, violaciones de confidencialidad, falta de diligencia por parte del encargado, y la dificultad o imposibilidad del ejercicio de los derechos, violaciones de seguridad, etc.

iv. Medidas preventivas: Se establecerán las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

La AEPD también ha dado su opinión en relación a la EIPD en aquellos tratamientos que incorporan tecnologías basadas en IA. La cuestión es interesante debido a que la BCI mantiene una relación bidireccional de funcionamiento y retroalimentación en base a IA. De esta forma, la AEPD ha señalado que una EIPD ha de concretarse en la adopción de una serie de medidas específicas y concretas para la gestión del riesgo, algunas de ellas orientadas a reforzar las obligaciones de cumplimiento en función de dicho riesgo y que afectan a[119]:

i. La concepción del tratamiento, en sus fases, procedimientos, tecnologías y extensión.

ii. La incorporación de medidas de privacidad por defecto y desde el diseño en el tratamiento y que sigan los principios de:

- ✓ Minimizar la cantidad de datos que son tratados, tanto en volumen de información recopilada como en el tamaño de la población de estudio, así como a lo largo de las diferentes fases del tratamiento.
- ✓ Agregar los datos personales en la medida de lo posible para reducir al máximo el nivel de detalle que es posible obtener.
- ✓ Ocultar los datos personales y sus interrelaciones para limitar su exposición y que no sean visibles por partes no interesadas.
- ✓ Separar los contextos de tratamiento para dificultar la correlación de fuentes de información independientes, así como la posibilidad de inferir información.
- ✓ Mejorar la Información a los interesados, en tiempo y forma, de las características y bases jurídicas de su tratamiento para fomentar la transparencia y permitir a los interesados tomar decisiones informadas sobre el tratamiento de sus datos.
- ✓ Proporcionar medios a interesados para que puedan controlar cómo sus datos son recogidos, tratados, usados y comunicados a terceras partes mediante la implementación de mecanismos

119 AEPD, (2020)., Op. Cit. pp. 32-33.

adaptados al nivel de riesgo que les permita realizar el ejercicio de sus derechos en materia de protección de datos.

- ✓ Cumplir con una política de privacidad compatible con las obligaciones y requisitos legales impuestos por la normativa.
- ✓ Demostrar, en aplicación del principio de responsabilidad proactiva, el cumplimiento de la política de protección de datos que esté aplicando, así como del resto de requisitos y obligaciones legales impuestos por el Reglamento, tanto a los interesados como a las autoridades de control. Esto implica auditar dinámicamente el resultado/ las conclusiones de los tratamientos, evaluando las divergencias o desviaciones sobre los inicialmente previstos o evaluados como previsibles, incluidos los algoritmos ejecutados, para adoptar, en su caso, medidas correctivas, incluida, la supresión de la información y documentar detalladamente el análisis realizado y las medidas adoptadas.

iii. La identificación de requisitos de seguridad que minimicen el riesgo para la privacidad.

iv. La adopción de medidas específicas dirigidas a implementar un sistema de gobernanza de los datos personales que permitan demostrar el cumplimiento de principios, derechos y garantías para gestionar el riesgo de los tratamientos realizados.

La AEPD, además, proporciona guías para abordar los aspectos anteriores de forma concreta para cualquier tipo de tratamiento genérico, destacando la Guía práctica para las evaluaciones de impacto en la protección de datos personales, la Guía de Privacidad desde el Diseño, Modelo de informe de Evaluación de Impacto en la Protección de Datos para Administraciones Públicas, así como herramientas que ayudan a realizar la EIPD, como GESTIONA.

El modelo de evaluación del impacto sobre la protección de datos es necesario para brindar a los responsables del tratamiento de datos pautas suficientemente específicas, útiles y claras para el cumplimiento de los principios del tratamiento de datos[120].

4.3 Adopción de medidas de seguridad adecuadas.

El artículo 32 del RGPD establece que "teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo […]".

Una de las medidas que pueden contribuir a reducir el nivel del riesgo es la seudonimización. La seudonimización o disociación de los datos personales, supone eliminar aquellos datos que a priori permiten una identificación de los interesados, dejando accesibles aquellos datos o información personal que se

120 AEPD, *Op. Cit.* pp. 23-24.

necesita para el tratamiento. Cuando hablamos de seudonimización siempre hay que tener en cuenta que se trata de un mecanismo que oculta la identidad de los interesados, pero este ocultamiento de la identidad es reversible y siempre podremos reidentificar a las personas. Frente a la seudonimización hablamos de anonimización cuando el procedimiento para disociar la información está diseñado para evitar la reidentificación de los interesados e interesadas, sin embargo, el propio RGPD también pone de manifiesto los límites de la anonimización de forma que en ningún caso podremos hablar en términos absolutos de datos anónimos, siempre existirá un riesgo de reidentificación de las personas[121].

Además, el RGPD, en su artículo 32.3 permite a los responsables de los tratamientos la posibilidad de utilizar mecanismos de certificación para garantizar y demostrar el cumplimiento de los requisitos de seguridad, o la adopción de un código de conducta. Mediante un mecanismo de certificación, un tercero examina las medidas de seguridad implantadas por el responsable del tratamiento y evalúa los riesgos con el fin de determinar si dichas medidas de seguridad son acordes a los riesgos implícitos en el tratamiento. La certificación y los códigos de conducta pueden ser herramientas útiles para el cumplimiento de lo previsto en el RGPD en cuanto a medidas de seguridad, pero no exime a los responsables del enfoque de riesgo[122].

Otro ejemplo de medida de seguridad es el establecimiento de un sistema de control de accesos. Identificar usuarios implica gestionar la identidad digital de forma diligente. Es decir, cada usuario debe estar perfectamente registrado en el sistema, disponer de credenciales únicas y tener los privilegios de acceso definidos y delimitados.

Una estrategia técnica de uso generalizado son los cortafuegos o firewall. Una buena manera de asegurar que sólo las personas y archivos adecuados están recibiendo nuestros datos es mediante firewalls. Software o hardware diseñado con un conjunto de reglas para bloquear el acceso a la red de usuarios no autorizados. Son líneas de defensa para evitar la interceptación de datos y bloquear el malware que intenta entrar en la red, y también evitan que la información importante salga, tales como contraseñas o datos confidenciales.

Es recomendable, también, incorporar un sistema de trazabilidad debido que, la eficacia en la protección de datos sensibles pasa por la monitorización del acceso y el uso que se da a los sistemas, pero también de la política que se ha implantado para conseguirlo. Es decir, que un seguimiento apropiado permite saber si realmente esa política está funcionando o si, por el contrario, es necesario adaptarla a nuevas circunstancias.

De forma transversal, se podrían implementar otro tipo de soluciones de privacidad orientadas a proteger los datos como el *Blockchain,* las cuales permiten hacer seguimiento y auditorías de los datos. Configurada como una **base de datos distribuida formada por cadenas de bloques diseñadas para evitar su modificación una vez que un dato ha sido publicado** usando un sellado de tiempo confiable (o *trusted timestamping*) y enlazando a un bloque

121 GT29, 2014. Sobre técnicas de anonimización, p. 5-28.

122 Artículo 40 del RGPD.

anterior. Esta configuración la traduce en una **herramienta de incalculable valor para la seguridad**, pero también sirve para tareas como el almacenamiento de datos o su confirmación empleando la "minería de datos"[123].

4.4 Designar un delegado de protección de datos (DPO, por su acrónimo en inglés)

Esta figura resulta esencial en entornos de BCI, ya que, el tratamiento de los neurodatos implica un alto riesgo para los derechos y libertades fundamentales de las personas.

De acuerdo al artículo 39.2 del RGPD, el DPO debe desempeñar sus funciones prestando la debida atención a los riesgos teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

Además, según especifica el artículo 39 del RGPD, esta figura tiene entre sus funciones informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen de la gestión de las obligaciones que les incumben en virtud del reglamento; supervisar el cumplimiento de lo dispuesto en el RGPD, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento. Por otro lado, el RGPD insiste en la importancia de que el DPO coopere siempre con la autoridad de control y actúe como punto de contacto del regulador para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto. El delegado de protección de datos debe ser nombrado atendiendo a sus cualificaciones profesionales y, en particular, a su conocimiento de la legislación y la práctica de la protección de datos.

En definitiva, es sabido que el fenómeno del BCI supone la gestión y tratamiento de ingentes cantidades de datos personales sensibles que pueden brindar grandes ventajas y beneficios a las organizaciones públicas y privadas y a la sociedad en general. Pero, no es menos cierto que también conlleva altos riesgos en materia de privacidad. Por ello, es importante que cada entidad tenga una postura definida y ordenada en cuanto a los procedimientos y estrategias a seguir destinadas al cumplimiento de los principios del tratamiento en este entorno tecnológico.

4.5 Llevar un Registro de Actividades de Tratamiento (RAT)

Una de las obligaciones principales del nuevo RGPD es la de crear un registro de actividades de tratamiento. Dicho registro sustituye a la obligación anterior de inscribir los ficheros, y aparece regulada en el artículo 30 del Reglamento General de Protección de Datos. Cada responsable debe llevar un registro de actividades de tratamiento en el que se contenga la siguiente información[124]:

i. Nombre y datos de contacto del responsable

ii. Fines del tratamiento

123 PALOMO-ZURDO, (2018). Blockchain: la descentralización del poder y su aplicación en la defensa. Documento Opinión, Instituto Español de Estudios Estratégicos. pp. 1-30.

124 Artículo 30 RGPD.

iii. Descripción de los interesados (clientes, proveedores, usuarios etc.)
iv. Categorías de datos (datos identificativos, datos fiscales, datos sensibles, etc.)
v. Categorías de destinatarios a quienes se comunicarán los datos
vi. Transferencias internacionales previstas
vii. Medidas técnicas y organizativas de seguridad
viii. Plazos de supresión para las diferentes categorías de datos

Este Registro de actividades de tratamiento es un documento interno de cada responsable que debe estar a disposición de la Autoridad de Control en caso de que haya una inspección. Es un documento que debe ser modificado cuando existan cambios, como puede ser ampliar a otras categorías de datos nuestro tratamiento.

Se exige que conste por escrito, inclusive en formato electrónico[125]. Y se establece que esta obligación no se aplicará a ninguna empresa que emplee a menos de 250 personas, a menos que el tratamiento que se realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales (como en el caso de los EEG) indicadas en el artículo 9, apartado 1, o datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10[126].

4.6 Notificación de las brechas de seguridad

La notificación de las violaciones de seguridad es una obligación del responsable del tratamiento, y también del encargado, establecida en los artículos 33 y 34 del RGPD. El artículo 33 se refiere a las obligaciones de notificación del responsable a la Autoridad de Control y del encargado al responsable, mientras que el artículo 34 se refiere a las obligaciones de notificación al interesado.

Se trata de una obligación más amplia para el responsable. Se emplaza al responsable para que implemente un procedimiento de gestión de incidentes de seguridad que afecten a datos de carácter personal, cuyo resultado visible al exterior son las notificaciones tanto de las brechas seguridad como de las acciones y decisiones relativas a dichas violaciones. Además, establece una obligación para la Autoridad de Control, que es la de, si lo estima oportuno, intervenir de conformidad con las funciones y poderes establecidos en RGPD.

El RGPD define el concepto de "violación de seguridad" en su artículo 4.12 como:

> Toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos;

El RGPD es muy riguroso y establece un plazo de 72 horas después de que el responsable del tratamiento haya tenido constancia de la violación de seguridad

125 Artículo 30.3 RGPD.

126 Artículo 30.5 RGPD.

de los datos personales, para notificar de esta circunstancia a la Autoridad de Control competente. En caso de que el encargado del tratamiento sufra una violación de seguridad, éste debe notificar sin dilación al responsable la existencia de la misma[127].

El responsable debe notificar la violación de seguridad a la autoridad competente y los interesados, cuando esta entrañe un alto riesgo para los derechos y libertades del mismo. Esta comunicación debe realizarse en un lenguaje claro y sencillo, describiendo la naturaleza de la violación de seguridad de los datos personales y contendrá como mínimo la información del nombre y los datos del Delegado de Protección de Datos o de otro punto de contacto en el que pueda obtenerse información, la descripción de las posibles consecuencias de la violación de seguridad, la descripción de las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos[128].

El 34.3 del RGPD establece una serie de excepciones a la necesidad de comunicar la violación a los interesados, y son las que siguen:

i. Que el responsable del tratamiento haya adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como puede ser el caso de que los datos estén cifrado.

ii. El responsable ha tomado medidas ulteriores que garanticen que ya no existe la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado.

iii. Que el realizar esa comunicación suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados Hay que tener en cuenta que la decisión del responsable de no notificar a los interesados puede ser revocada por la Autoridad de Control y ésta exigir que dicha notificación se ejecute.

Hay que tener en cuenta que la decisión del responsable de no notificar a los interesados puede ser revocada por la Autoridad de Control y ésta exigir que dicha notificación se ejecute.

4.7 Mantener relaciones con la autoridad de control

Las autoridades de control nacional, se erigen como el ente fundamental en la fiscalización y garantía del cumplimiento de los principios y derechos

127 Artículo 33.1 RGPD.

128 Artículo 33 letras b), c) y d) del RGPD.

establecidos por el Reglamento europeo en relación con el tratamiento de datos personales y los titulares de estos últimos[129].

Por este motivo, cuando un responsable de tratamiento pretende realizar un tratamiento de datos de salud en entornos de BCI, éste debe contemplar en caso necesario la interrelación con la correspondiente autoridad de control en todas las etapas del proyecto que se proponga.

De esta manera, deberá considerar los siguientes aspectos:

i. Consulta previa a la autoridad de control en base a los resultados de la Evaluación de Impacto en la Protección de Datos que se realice[130].

ii. El responsable del tratamiento además de planificar y adoptar las medidas técnicas u organizativas con miras a garantizar la seguridad del tratamiento, en el marco de la consulta previa a la que alude el apartado anterior, debería informar la autoridad de control sobre las concretas medidas y garantías que estime adoptar en proyectos BCI, debiendo la autoridad de control instruir y asesorar al responsable en caso de que considere que éste no ha identificado o mitigado suficientemente el riesgo con las medidas que haya proyectado[131].

iii. Especial importancia tiene el deber de colaborar con la autoridad de control en el correcto ejercicio de sus competencias, operando este deber como una garantía general en favor de la protección de la privacidad de los neurodatos de las personas físicas en proyectos BCI.

Por último, debemos aclarar que los recursos ofrecidos por la nueva normativa europea, tienen como objetivo facilitar el tratamiento de datos personales en una sociedad cada vez más tecno-dirigida. De tal manera que, el RGPD no debe apreciarse como un límite para los responsables y encargados del tratamiento de datos, sino como un documento de apoyo que establece las directrices indispensables para un desarrollo lícito de dicha actividad.

Conclusiones

1. Del Internet de las Cosas al Internet de los Cuerpos, un paso al Internet del Todo. El Internet del Todo (IdT), no debe ser visto como un fenómeno futuro, ya está aquí y debemos concienciar sobre su uso y riesgos a todos los agentes de la sociedad. Una de las cuestiones que genera más debate en la doctrina es la seguridad y privacidad de la información personal que está constantemente disponible en la red. Una frase común de escuchar en un ámbito de tecnologías de la información es "Si se puede programar se puede hackear". Es alarmante saber que toda nuestra información personal, el registro de lo que hacemos, de nuestras preferencias, de nuestra ideología política, de nuestra sexualidad, de nuestros momentos de esparcimiento, sea accesible

129 Artículo 47, Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. BOE número 294.

130 Artículo 35 RGPD.

131 Artículo 57.1 RGPD.

a cualquier persona que pueda hackear nuestros dispositivos conectados a internet.

2. Con la aprobación y vigencia del RGPD se ha reformado de manera sustancial el panorama europeo relativo a la protección de datos personales. El actual RGPD está pensado para afrontar los problemas que suponen las nuevas tecnologías en el ámbito de la privacidad. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa y el legislador europeo ha observado los problemas y limitaciones que generaba la Directiva 95/46, y ha asegurado la protección de los datos personales de sus ciudadanos, incluso más allá de los límites territoriales, incluso más allá del *big data* y del *cloud computing*, incluso más allá de la inteligencia artificial y de las neurotecnologías en general. Verbigracia, el Considerando 24 manifiesta que "(…) Para determinar si se puede considerar que una actividad de tratamiento controla el comportamiento de los interesados, debe evaluarse si las personas físicas son objeto de un seguimiento en internet, inclusive el potencial uso posterior de técnicas de tratamiento de datos personales que consistan en la elaboración de un perfil de una persona física con el fin, en particular, de adoptar decisiones sobre él o de analizar o predecir sus preferencias personales, comportamientos y actitudes. Unido este Considerando al artículo 3.2 del RGPD nos permite concluir que, el RGPD es aplicable no solo a la monitorización de los comportamientos mostrados en internet; sino también a cualquier monitorización realizada por cualquier medio destinado para ello.
3. Sin embargo, el aumento exponencial de la información que se envía por Red debe ser respaldado por la elaboración de nuevas leyes y estándares internacionales donde aquellos países que no forman parte de la Unión Europea ni del Espacio Económico Europeo también puedan participar, comprometerse y ser sujetos de obligaciones. De tal manera, que unidas esas regulaciones al RGPD contribuyan con la privacidad y seguridad necesaria de la información. Regular es fundamental si queremos establecer la obligatoriedad de implantar unas salvaguardas tecnológicas mínimas y evitar la vulneración de los derechos y libertades de los individuos, en particular, de la privacidad e integridad mental y corporal, la identidad individual, la capacidad de elegir las propias acciones y de controlar nuestra información, es decir de los "neuorderechos humanos".
4. También nos parece prudente acompañar la nueva relación humano-máquina de un cambio legislativo con otros ajustes al unísono, tales como la redefinición del concepto de persona; y los efectos patrimoniales y de familia que de suyo podría generar una persona con "neuromejoras" o "mejores capacidades cognitivas". Se debe monitorizar y cuantificar el impacto moral y jurídico de los algoritmos en la vida de las personas. Prohibiendo las decisiones basadas en algoritmos que discriminen arbitrariamente a los individuos, produciendo indefensión y abuso de poder. Aunque en la actualidad existen diversos grupos de investigación que trabajan para integrar algoritmos éticos y justos en agentes artificiales, uno de los mayores obstáculos es que todavía no sabemos cómo se da exactamente el proceso de evaluar y tomar decisiones éticas en los propios seres humanos. Todavía falta mucho

por delimitar en la ética si pretendemos que la transformación tecnológica y digital sea más justa, noble y amable con las personas.

5. El Neuroderecho, como disciplina que se aboca al estudio de las relaciones entre el derecho, la neurociencia y las neurotecnologías avanzadas, busca visibilizar un realismo jurídico que propone sentar las primeras bases para una regulación de los problemas y efectos que se desprenden del uso de las neurotecnologías e inteligencia artificial en los seres humanos. Pone sobre el escenario jurídico una nueva realidad de la especie humana; probablemente desde el transhumanismo, de la relación biológico-artificial, nos propone plantearnos hasta qué punto seguiremos siendo humanos. Nos propone enfrentarnos a un cambio de paradigma en que la neuroprotección se vuelve un principio fundamental.

Bibliografía

ABOUJAOUDE, E. (2019). Protecting privacy to protect mental health: the new ethical imperative. *Journal of Medical Ethics*(45), pp.604-607. Recuperado el 27 de octubre de 2020, de https://jme.bmj.com/content/45/9/604

ALBORNOZ ZAMORA, E. J., & GUZMÁN, M. (diciembre de 2016). Desarrollo cognitivo mediante estimulación en niños de 3 años. *Revista Científica Multidisciplinar de la Universidad de Cienfuegos, 8*(4), pp.186-192. Recuperado el 28 de octubre de 2020, de http://scielo.sld.cu/pdf/rus/v8n4/rus25416.pdf

ALONSO, X. (2015). *Encefalografía en el niño*. Recuperado el 31 de octubre de 2020, de http://neuropedwikia.es/content/electroencefalografia-en-el-nino

AMAT, A., MARTÍ, J., & DARNÉ, I. (2018). Investigamos cómo funciona el cuerpo humano. *Petit Talent Cientifics*, pp.63-70. Recuperado el 31 de octubre de 2020, de file:///C:/Users/Alumno/Downloads/Investigamos-como-funciona-el-cuerpo-humano-WEB.pdf

AUSÍN, T., MORTE, R., & MONASTERIO, A. (8 de octubre de 2020). Neuroderechos: Derechos humanos para las neurotecnologías. *Diario La Ley*(43), pp.1-7. Recuperado el 27 de octubre de 2020, de https://globernance.org/wp-content/uploads/2020/04/20201008-Neuroderechos-_Derechos_....pdf

AZNAR CASANOVA, J. A. (2017). *ub.edu*. Recuperado el 31 de octubre de 2020, de http://www.ub.edu/pa1/node/130

BALLARIN USIETO, P., & MINGUEZ, J. (s.f.). *La importancia de la ciberseguridad en brain-computer interfaces*. Recuperado el 02 de noviembre de 2020, de https://www.bitbrain.com/es/blog/ciberseguridad-cerebro-computadora

BREZNITZ, S. (2019). *cognifit.com*. Recuperado el 28 de octubre de 2020, de https://www.cognifit.com/es/que-es-cognifit

CAVOUKIAN, A. (2016). Privacidad por diseño los 7 principios fundamentales. *Mediascope*. Recuperado el 03 de noviembre de 2020, de https://www.mediascope.es/wp-content/uploads/2016/10/privacidad-por-disen%CC%83o-1.pdf

CORNETIPRAT, J. (17 de diciembre de 2017). *Communityofinsurance.es*. Recuperado el 28 de octubre de 2020, de https://communityofinsurance.es/2017/12/17/las-nuevas-tecnologias-y-los-retos-para-la-identidad-personal/

DE SANTIAGO RODRIGO, L. (2016). Análisis avanzado de señales potenciales evocados multifocales aplicados al diagnótico de neuropatías ópticas (tesis doctoral). *Universidad de Alcalá*, pp.18-19. Recuperado el 31 de octubre de 2020, de https://ebuah.uah.es/dspace/bitstream/handle/10017/29264/Tesis%20Luis%20de%20Santiago%20Rodrigo.pdf?sequence=1&isAllowed=y

EATON, M. L., & ILLES, J. (2007). Commercializing cognitive neurotechnology—the ethical terrain. *Nature Biotechnology, 25*(4), pp.393-397. Recuperado el 26 de octubre de 2020, de https://www.researchgate.net/publication/6401449_Commercializing_cognitive_neurotechnology_-_The_ethical_terrain

ELÍO, J. (25 de septiembre de 2016). *elespañol.com*. Recuperado el 27 de octubre de 2020, de https://elandroidelibre.elespanol.com/2016/09/historia-de-los-wearables.html

FUENTES, R., HIDALGO, M. C., & YUSTE, R. (2019). *Neurotecnologías: los desafíos de conectar el cerebro humano y computadores*. Santiago: Biblioteca del Congreso Nacional de Chile. Recuperado el 29 de octubre de 2020, de https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/27272/1/If01_Neurotecnologias_BCN_final.pdf

FUNDACIÓN DE LA INNOVACIÓN BANKINTER. (2011). El Internet de la Cosas. En un mundo conectado de objetos inteligentes. pp.9-10. Recuperado el 28 de octubre de 2020, de https://www.fundacionbankinter.org/documents/20183/137558/RE+PDF+ES+FTF_IOT.pdf/379ba7dd-711c-419c-a105-59e6693f502a

FUNDACIÓN INNOVACIÓN BANKINTER. (2019). Neurociencias: Más allá del cerebro. *FUTURE TRENDS FORUM*, PP.15-33. Recuperado el 27 de octubre de 2020, de https://www.fundacionbankinter.org/documents/20183/376572/Neurociencia+Informe+completo/0f567df1-ad0b-4cb2-b0d6-534908efba13

GALINDO, M. D. (2008). *Introducción a los sistemas Brain Computer Interface*. (F. Telefónica, Editor) Recuperado el 30 de octubre de 2020, de https://lacofa.fundaciontelefonica.com/general/

GARCÍA DEL BLANCO, I. (20 de octubre de 2020). García del Blanco: "Hemos marcado el camino para que la inteligencia artificial en la UE sirva para mejorar nuestras vidas y nuestro entorno". (S. E. Europeo, Entrevistador) Recuperado el 02 de noviembre de 2020, de http://www.socialistas-parlamentoeuropeo.eu/garcia-del-blanco-marcado-camino-la-inteligencia-artificial-la-ue-sirva-mejorar-nuestras-vidas-entorno/

GUTIERREZ, J. (2001). Análisis de señales en el neuromonitoreo. *Revista Mexicana de Ingeniería Biomédica, 22*(2), pp.66-67. Recuperado el 31 de octubre de 2020

INSTITUTO NACIONAL DE CIBERSEGURIDAD [INCIBE]. (s.f.). *incibe.es*. Recuperado el 02 de noviembre de 2020, de https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_proteccion-de-la-informacion.pdf

ISO 31000. (2018). *Gestión del riesgo.* Recuperado el 02 de noviembre de 2020, de https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es

ISOTOOLS EXCELLENCE. (2018). *isotools.org.* Recuperado el 02 de noviembre de 2020, de https://www.isotools.org/pdfs-pro/ebook-iso-31000-gestion-riesgos-organizaciones.pdf

KUNO, N. (2016). La nanotecnología cobra vida con dispositivos de interfaz humana basados en agujas. *News Center Latam*. Recuperado el 28 de octubre de 2020, de https://news.microsoft.com/es-xl/la-nanotecnologia-cobra-vida-con-dispositivos-de-interfaz-humana-basados-en-agujas/

LEBEDEV, M., & NICOLELIS, M. (2017). Brain-Machine Interfaces: From Basic Science to Neuroprostheses and Neurorehabilitation. *Physiological Reviews, 97*(2), pp.767-837. Recuperado el 26 de octubre de 2020, de https://journals.physiology.org/doi/pdf/10.1152/physrev.00027.2016

LEÓN SANZ, P. (2016). Bioética y explotación de grandes conjuntos de datos. En A. ANDÉREZ GONZALES, J. DÍAZ GARCÍA, F. ESCOLAR CASTELLÓN, & P. LEÓN SANZ, *LA EXPLOTACIÓN DE DATOS DE SALUD. Retos, oportunidades y límites* (pág. p.25). Sociedad Española de Informática y Salud. Obtenido de https://seis.es/wp-content/uploads/2018/02/LA-EXPLOTACI%C3%93N-DE-DATOS-DE-SALUD.pdf

LU, X., & MERRITT, J. (2020). Shaping the future of the Internet of Bodies: New challanges of technology governance. *World Economic Forum*, p.7. Recuperado el 28 de octubre de 2020, de http://www3.weforum.org/docs/WEF_IoB_briefing_paper_2020.pdf

LUCERO, B., & MUÑOZ-QUEZADA, M. T. (2014). Sistemas de interfaz neuronal y su desarrollo en las neurociencias: revisión bibliográfica sistemática acerca de su aplicación en personas con parálisis. *Revista Ciencias Psicológicas, 8*(2). Recuperado el 27 de octubre de 2020, de http://www.scielo.edu.uy/scielo.php?script=sci_arttext&pid=S1688-42212014000200008

MATWYSHYN, A. M. (2019). The Internet of Bodies. *William & Mary Law Review, 61*(77), pp.89-115. Recuperado el 27 de octubre de 2020, de https://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=3827&context=wmlr

MINGUEZ, J. (s.f.). Tecnología de interfaz cerebro-computador. *Departamento de informática e ingeniería de sistemas*, p.3. Recuperado el 30 de octubre de 2020, de https://webdiis.unizar.es/~jminguez/Sesion001_UJI.pdf

MONASTERIO ASTOBIZA, A. (2017). Ética algorítmica: Implicaciones éticas de una sociedad cada vez más gobernada por algoritmos. *Dilemata*(24), 186-204. Recuperado el 03 de noviembre de 2020, de file:///C:/Users/Alumno/Downloads/412000107-Texto%20del%20art%C3%ADculo-1994-1-10-20170530%20(1).pdf

MORENO, I., SERRACÍN, J., SERRACÍN, S., & QUINTERO, J. (2019). Los sistemas de interfaz cerebro-computadora basado en EEG: características y aplicaciones. *Revista de I+D Tecnológico, 15*(2), p.13. Recuperado el 30 de octubre de 2020, de file:///C:/Users/Alumno/Downloads/2230-Textodelartculo-11319-1-10-20190730.pdf

MURILLO DE LA CUEVA, P. L. (2000). La publicidad de los archivos judiciales y la confidencialidad de los datos sanitarios. *VII Congreso Nacional de Derecho Sanitario.* Madrid: Fundación Mapfre Medicina.

NIETO-SANPEDRO, M., GUDIÑO-CABRERA, G., TAYLOR, J., & VERDÚ, E. (2002). Trauma en el sistema nervioso central y su reparación. *Revisiones en Neurociencia*, pp.34-35. Recuperado el 31 de octubre de 2020, de file:///C:/Users/Alumno/Downloads/NietoSampedroRev.Neurol.2002.pdf

ORFILA, M. (16 de marzo de 2019). *elobservador.com*. Recuperado el 27 de octubre de 2020, de https://www.elobservador.com.uy/nota/de-humano-a-cyborg-la-historia-de-neil-harbisson-el-primer-cyborg-de-la-historia-201931595557

PALOMO-ZURDO, R. (2018). Blockchain: descentralización del poder y su aplicación en la defensa. *Documento Opinión*, pp.3-20. Recuperado el 04 de noviembre de 2020, de http://www.ieee.es/en/Galerias/fichero/docs_opinion/2018/DIEEEO70-2018_Blockchain_PalomoZurdo.pdf

PARLAMENTO EUROPEO. (21 de octubre de 2020). *euoparl.europa.eu*. Recuperado el 29 de octubre de 2020, de https://www.europarl.europa.eu/news/es/headlines/society/20201015STO89417/regulacion-de-la-inteligencia-artificial-en-la-ue-la-propuesta-del-parlamento

PONCE, P., MOLINA, A., BALDERAS, D. C., & GRAMMATIKOU, D. (2014). Brain Computer Interfaces for Cerebral Palsy, Cerebral Palsy-Challanges for the Future, Emira Svraka. *IntechOpen.* doi:10.5772/57084

RAMOS ARGÜELLES, F., MORALES, G., EGOZCUE, S., PABÓN, R. M., & ALONSO, M. T. (2009). Técnicas básicas de electroencefalografía: principios y aplicaciones clínicas. *Anales Sistema Sanitario Navarra, 32*(Supl.3), p.70. Recuperado el 31 de octubre de 2020, de http://scielo.isciii.es/pdf/asisna/v32s3/original6.pdf

ROSE, K., ELDRIDGE, S., & CHAPIN, L. (2015). La Internet de las Cosas- Una breve reseña para entender mejor los problemas y desafíos de un mundo más conectado. *Internet Society*, pp.13-16. Recuperado el 28 de octubre de 2020, de https://www.internetsociety.org/wp-content/uploads/2017/09/report-InternetOfThings-20160817-es-1.pdf

SALIN-PASCUAL, R. J. (2015). Optogenética: la luz como una herramienta para el estudio del funcionamiento cerebral en los mecanismos del sueño-vigilia y la conducta alimentaria. *Revista mexicana de neurociencias, 16*(3), p.39-51. Recuperado el 25 de octubre de 2020, de file:///C:/Users/Alumno/Downloads/RevMexNeuroci-No-3-May-Jun-2015-39-51R%20(1).pdf

SENADO DE CHILE. (2019). *Inteligencia Artificial y neuroderechos: la protección de nuestro cerebro podría quedar consagrado en la Constitución*. Recuperado el 31 de octubre de 2020, de https://www.senado.cl/inteligencia-artificial-y-neuroderechos-la-proteccion-de-nuestro/senado/2019-05-28/132221.html

SMITH, B., & SHUM, H. (2018). The Future Computed Artificial Intelligence and its role in society. *Microsoft Corporation*, pp.57-73. Recuperado el 28 de octubre de 2020, de https://news.microsoft.com/uploads/2018/02/The-Future-Computed_2.8.18.pdf?ranMID=24542&ranEAID=je6NUbpObpQ&ranSiteID=je6NUbpObpQ-sUXneKUeZh08LEknB4PaTg&epi=je6NUbpObpQ-sUXneKUeZh08LEknB4PaTg&irgwc=1&OCID=AID2000142_aff_7593_1243925&tduid=%28ir__gqmcfps6r0

TORRES GARCÍA, A. (2016). Análisis y clasificación de electroencefalogramas (EEG) registrados durante el habla imaginada. *(tesis doctoral) Insituto Nacional de Astrofísica, Óptica y Electrónica*, pp.16-18. Recuperado el 31 de octubre de 2020, de file:///C:/Users/Alumno/Downloads/TorresGaAA%20(1).pdf

U.S . FOOD & DRUG ADMINISTRATION. (2016). Postmarket Management of Cybersecurity in Medical Devices. Recuperado el 28 de octubre de 2020, de https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices

U.S FOOD & DRUG ADMINISTRATION. (octubre de 2018). Content of Premarket Submissions for Management of Cybersecurity in Medical Devices. Recuperado el 28 de octubre de 2020, de Disponible en: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/content-premarket-submissions-management-cybersecurity-medical-devices

VADILLO BUENO, G. (2020). Futuros de la Inteligencia Artificial. *Revista Digital Universitaria, 21*(1), pp.1-12. Recuperado el 27 de octubre de 2020, de https://www.revista.unam.mx/wp-content/uploads/v21_n1_a3.pdf

YUSTE, R. (2019). Las nuevas neurotecnologías y su impacto en la ciencia, medicina y sociedad. *La Lección Cajal*, (pág. 37). Zaragoza. Recuperado el 28 de octubre de 2020, de https://zaguan.unizar.es/record/86978/files/BOOK-2020-001.pdf

YUSTE, R., & DUPRE, C. (2017). Non-overlapping Neural Networks in Hydra vulgaris. *Current Biology, 27*(8), pp.1084-1096. Recuperado el 31 de octubre de 2020, de https://www.cell.com/current-biology/pdfExtended/S0960-9822(17)30220-8

Referencias normativas

Unión Europea

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. DUOE número 119. (s.f.). Obtenido de https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807

España

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. (2018). Recuperado el 20 de enero de 2020, de https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673&p=20181206&tn=2

Chile

CONSTITUCIÓN POLÍTICA DE CHILE. (1980). *Artículo 19 número 1.* Recuperado el 29 de octubre de 2020, de https://www.bcn.cl/leychile/navegar?idNorma=242302

PROYECTO DE REFORMA CONSTITUCIONAL BOLETÍN N°13827. (de 7 de octubre de 2020). Recuperado el 29 de octubre de 2020, de Disponible en: http://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=13827-19

PROYECTO DE LEY BOLETÍN N°13828-19. (de 7 de octubre de 2020). Recuperado el 29 de octubre de 2020, de Disponible en: http://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=13828-19

Otros documentos

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS [AEPD]. (2017). *Códigos de buenas prácticas en protección de datos para proyectos Big Data.* Recuperado el 20 de noviembre de 2020, de https://www.bigdatius.com/wp-content/uploads/2017/05/Guia_Big_Data_AEPD-ISMS_Forum.pdf

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, (2020). Adecuación al RGPD de tratamientos que incorporan Inteligencia artificial. Una introducción. pp.42-43. Recuperado el 25 de octubre de 2020, de https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf

EUROPEAN PARLIAMENT. (2020). *DRAFT REPORT with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies.* Recuperado el 02 de noviembre de 2020, de https://ibangarciadb.eu/wp-content/uploads/REPORT-Ethical-AI_final_XM.pdf

GRUPO DE TRABAJO DEL ARTÍCULO 29 [GT 29]. (2010). *Opinión 3/2010 on the principle of accountability (WP 173).* Recuperado el 01 de noviembre de 2020, de https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm

GRUPO DE TRABAJO DEL ARTÍCULO 29 [GT29]. (2007). Documento de trabajo sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos (HME). pp.7-8. Recuperado el 01 de noviembre de 2020, de https://www.apda.ad/sites/default/files/2018-10/wp131_es.pdf

GRUPO DE TRABAJO DEL ARTÍCULO 29 [GT29]. (2014). Dictamen 5/2014 sobre técnicas de anonimización. pp.5-28. Recuperado el 02 de noviembre de 2020, de https://www.aepd.es/sites/default/files/2019-12/wp216-es.pdf

GRUPO DE TRABAJO DEL ARTÍCULO 29 [GT29]. (2017). Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, revisadas por última vez y adoptadas el 10 de abril de 2018. pp.5-33. Recuperado el 01 de noviembre de 2020, de https://www.euskadi.eus/contenidos/informacion/20161118/es_def/adjuntos/wp259rev01__es20180709.pdf

GRUPO DE TRABAJO DEL ARTÍCULO 29 [GT29]. (5 de febrero de 2015). ANNEX - Health data in apps and devices. pp.1-8. Recuperado el 01 de noviembre de 2020, de https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf

GRUPO DEL TRABAJO DEL ARTÍCULO 29 [GT29]. (2007). *Dictamen 4/2007 sobre el concepto de datos personales.* Recuperado el 31 de octubre de 2020, de https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf