CENTRO DE INVESTIGACIÓN Y DOCENCIA ECONÓMICAS, A.C.

NEURODERECHO A LA PRIVACIDAD MENTAL: ANÁLISIS DEL GDPR

TESINA

QUE PARA OBTENER EL TÍTULO DE

LICENCIADA EN DERECHO

PRESENTA

DALIA STOFENMACHER MARCUSHAMER

DIRECTORA DE LA TESINA: DRA. MARÍA SOLANGE MAQUEO RAMÍREZ

CIUDAD DE MÉXICO 2023

Mis más profundos agradecimientos,

A mi directora de tesis, la Dra. María Solange Maqueo Ramírez, por compartir su conocimiento, sabiduría y consejos invaluables. Gracias por guiarme en este camino.

A mis profesores del CIDE por enseñarme lo que saben y hacerme una mejor abogada y persona.

A mis papás, Noemi y David, y mis hermanos, Ronit y Bernardo, por estar ahí siempre. Los amo.

A mis abuelos, Erika y Bernardo z'l, Raquel y Marcos, por siempre creer en mí. A toda mi familia, por su apoyo.

A Andrea y Romina, por compartir un solo cerebro conmigo toda la carrera. No estaría aquí si no fuera por ustedes.

A mis amigxs y compañerxs del CIDE y de la vida, gracias por compartir esta vida conmigo.

Al Dr. Manuel Sierra Beltran y a Abhayadipa Ruelas, por ayudarme a curar mi cuerpo y mente.

A Hershey y a Nessie, por existir y acompañarme.

Resumen

El objetivo de esta investigación es analizar si el marco normativo de la Unión Europea en materia de privacidad y protección de datos personales, a través del GDPR (Reglamento General de Protección de Datos de la Unión Europea), protege el neuroderecho a la privacidad mental. Los neuroderechos se pueden definir como las normas o principios que buscan la protección y preservación del cerebro y la mente humana, incluyendo el derecho a la privacidad mental. Para determinar si el régimen de la Unión Europea protege este derecho, se explora el estado, capacidad y posible futuro de la tecnología existente (neurotecnología e inteligencia artificial). Adémas, se analiza el sistema de protección de datos personaless de la Unión Europea, su impacto a nivel global y la forma en la que el GDPR regula los datos personales y los datos personales sensibles. Despúes, se examina la naturaleza de los datos mentales y su relación con las categorías preexistentes de datos personales. Por último, se concluye que una interpretación expansiva del GDPR permite proteger una parte importante de los datos mentales, pero que la regulación actual no es suficiente para garantizar de manera comprensiva este derecho.

Lista de Abreviaturas y Acrónimos

BCI: Interfaces Cerebro-Computadora

Convenio 108: Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal

Derechos ARCO: Acceso, Rectificación, Cancelación y Oposición

DNN: Redes Neuronales Profundas O *Deep Neuronal Networks*

DPIAs: Evaluación de Impacto de la Protección de Datos

DPOs: Delegados de Protección De Datos

EEG: Electroencefalografía

ELA: Esclerosis Latera Amiotrófica

fMRI: Resonancia Magnética Funcional

GDPR: Reglamento General de Protección de Datos de la Unión Europe

ÍNDICE

Introducción

"Es una verdad universalmente reconocida que un hombre soltero, poseedor de una gran fortuna, está en búsqueda de una esposa."[1] Así empieza la famosa novela de Jane Austen, *Orgullo y Prejuicio.* A pesar de que la autora inicia la historia con una verdad aparentemente universal, lo que es subjetivo, son los pensamientos y sentimientos de los personajes. Los protagonistas, Elizabeth Bennet y Fitzwilliam Darcy, están tan inmersos en sus propios prejuicios y experiencias, que no se dan cuenta de que están enamorados, el uno del otro, hasta el final.[2]

La trama de este libro no parece ser una historia muy diferente a lo que pasa hoy en día. Las personas se siguen entendiendo y desentendiendo, enamorándose o desenamorándose en el proceso. Sin embargo, ¿qué pasaría si esta forma de comunicarse cambiara y fuera posible leer los pensamientos y emociones de otra persona? Esto no es una situación hipotética de un futuro lejano, sino, una realidad del aquí y el ahora. Ya existe tecnología que puede leer la mente y potencialmente cambiar el comportamiento[3] y la memoria humana.[4] Este es un fenómeno que avanza con una velocidad acelerada.

Tecnología que puede leer la mente humana ya existe y cada vez se está desarrollando más. En los últimos años se han invertido más de 19 billones de dólares en 200 compañías de neurotecnología.[5] Algunas de estas compañías intentan responder a la pregunta de ¿cómo se pueden leer los pensamientos humanos?

Este avance tecnológico hace que inevitablemente surjan nuevos desafíos con los que hay que lidiar como humanidad. Si la información mental de las personas puede ser accedida por terceros, la autonomía personal y la misma concepción del "yo" se puede diluir. Además, las intenciones de comportamiento futuro pueden ser predichos a pesar de no haber sucedido

[1] Jane Austen *Pride and Prejudice* (Harlow, England: Pearson Education Limited, 2019). (traducción de la autora).
[2] Ibidem.
[3] Melissa Heikkilä, "Machines Can Read Your Brain. There's Little That Can Stop Them," POLITICO, 1 de Septiembre, 2021. https://www.politico.eu/article/machines-brain-neurotechnology-neuroscience-privacy-neurorights-protection/#:~:text=Inception,brain%20activity%20and%20external%20circumstances.
[4] Meg Tirrell. "Defense Department Developing a 'Prosthetic Memory'," CNBC. CNBC, 25 de Mayo, 2016. https://www.cnbc.com/2016/05/24/defense-department-developing-a-prosthetic-memory.html.
[5] Rafael Yuste, Jared Genser y Stephanie Herrmann, "It's Time for Neuro-Rights," *Horizons,* Volumen 18 (Invierno 2021). https://www.cirsd.org/files/000/000/008/47/7dc9d3b6165ee497761b0abe69612108833b5cff.pdf

aún.[6] Algunas de las preguntas que surgen de esta situación son las siguientes: ¿las empresas y los gobiernos deberían ser capaces de predecir o saber los pensamientos y comportamientos de las personas? En caso afirmativo ¿hasta qué punto? ¿La población debería tener acceso a esta tecnología? En caso de que sí, ¿cómo se debería distribuir y quién debería poder acceder a ellas? ¿Cuáles son los riesgos que representa esta tecnología para la democracia? ¿Cuáles son los beneficios de usar esta tecnología? y ¿qué problemas puede resolver?

Con estos dilemas (y muchos otros) en mente se inventó el término neuroderechos. Los *neuroderechos* son las normas o principios que buscan la "protección y preservación del cerebro y la mente humana."[7] Con la neurotecnología, entra en cuestión algo que nunca antes la humanidad había tenido que preguntarse ¿todos los pensamientos deberían ser privados? Y ¿cómo proteger la privacidad de los pensamientos? Cuando un aspecto de la vida, que solía ser completamente privado, se vuelve potencialmente parte del dominio público, hay que considerar si la normativa vigente es suficiente para protegerlo. Esta investigación busca responder a la siguiente pregunta, ¿es suficiente la regulación de datos personales y datos personales sensibles de la Unión Europea para proteger el neuroderecho a la privacidad mental? La hipótesis de este trabajo es que una interpretación expansiva del Reglamento General de Protección de Datos de la Unión Europea (GDPR, por sus siglas en inglés) permite proteger una parte importante de los datos mentales, sin embargo, la regulación actual no es suficiente para garantizar de manera comprensiva este derecho. Para responder a la pregunta que se plantea en este trabajo se hará un análisis documental, bibliográfico y normativo del sistema europeo de protección de datos personales (principalmente plasmados en el GDPR -).

Este trabajo analiza los neuroderechos bajo el principio de *neutralidad tecnológica*. El investigador Bert-Jaar Koops sugiere tres formas distintas de usar este término. La primera está basada en el análisis del resultado. Por eso escribe "[L]a regulación no debe regular la tecnología en sí, sino sólo los efectos del uso de esta."[8] Por lo mismo, el autor dice que, bajo este enfoque, sólo se puede discriminar entre diferentes tipos de tecnología cuando los efectos de cada una de

[6] Marcello Ienca y Gianclaudio Malgieri, "Mental Data Protection and the GDPR," *Journal of Law and the Biosciences*, (5 de Mayo, 2021). http://dx.doi.org/10.2139/ssrn.3840403
[7] Marcello Ienca, "On Neurorights," pág 1. (traducción por la autora).
[8] Koops, Bert-Jaap, Miriam Lips, Corien Prins & Maurice Schellekens, "Should ICT Regulation Be Technology-Neutral?"

ellas sean distintos. Por ejemplo, se asume que recibir llamadas publicitarias no deseadas es más molesto que recibir la misma información por correo electrónico. Esto justificaría que se regule el uso de cada tecnología de manera desigual.[9]

El segundo significado dice que, en vez de enfocarse en el propósito de la tecnología, hay que limitar los efectos negativos que esta podría tener. En esencia, intentar evitar las consecuencias no deseadas (independientemente del tipo de tecnología).[10] El tercer y último significado habla del hecho que la tecnología avanza más rápido que la creación de las leyes.

Esta investigación tiene como propósito estudiar el marco normativo de la Unión Europea en materia de privacidad y protección de datos personales. La razón por la que se analiza este sistema no es por una pretensión de que a nivel sustantivo es superior a otros sistemas jurídicos en esta materia, sino que tiene que ver con el impacto material que estas regulaciones tienen a nivel mundial. Los reglamentos de la Unión Europea tienen un efecto extraterritorial muy importante y además han sido la base o inspiración de múltiples legislaciones alrededor del mundo.

El capítulo primero de esta investigación se enfoca en explorar el marco conceptual y un breve análisis del desarrollo histórico de los neuroderechos, con especial énfasis en el neuroderecho a la privacidad mental. El capítulo segundo explica la tecnología que puede descifrar la mente humana. Para esto, se describen las dos formas más comunes de hacerlo: la neurotecnología y la inteligencia artificial. El capítulo tercero explora el sistema de protección de datos personales de la Unión Europea, sus características principales, su impacto a nivel global, su importancia en este tema y la razón por la que se analiza. El capítulo cuarto analiza cómo regula el sistema de la Unión Europea los datos personales y datos personales sensibles, dentro de todas sus distintas categorías y analiza sus excepciones. Por último, el capítulo quinto busca contestar ¿son los datos mentales datos personales? Y en caso de serlo ¿son datos personales sensibles? Con esto, se busca entender si la privacidad mental está protegida por el régimen más estricto de datos personales sensibles. Al final, se presentan las conclusiones y recomendaciones de la investigación.

[9] Ibidem
[10] Ibidem

Capítulo Primero: Neuroderecho a la Privacidad Mental

1. Neuroderechos

Es importante precisar las definiciones de ciertos conceptos clave y su uso en la comunidad legal. *Neurotecnología* se refiere al conjunto de métodos, sistemas e instrumentos que crean una conexión con el cerebro humano. Al mismo tiempo, esta conexión tiene que poder registrar o influenciar la actividad neuronal. Esta tecnología generalmente proviene de las neurociencias o la neuroingeniería.[11] Otra definición propuesta es "[C]ualquier tecnología que registre o interfiera en la actividad cerebral."[12]

Neuroética, como su nombre denota, analiza la ética detrás de la *neurotecnología*. En el 2002 el escritor William Safire definió la *neuroética* como "la examinación de lo que está bien y lo que está mal sobre el tratamiento, la perfección o la invasión no deseada y manipulación preocupante del cerebro humano."[13] Por otra parte, *neuroley* (o neurolaw en inglés) habla de la intersección entre la neurociencia y la ley.[14]

En el último tiempo, una nueva rama dentro de la *neuroética* y la *neuroley* ha surgido. Esta busca generar principios normativos generales que resuelvan los retos éticos y jurídicos de la neurociencia y la neurotecnología. Con esto en mente, se inventó el término *neuroderechos*. Los *neuroderechos* son las normas o principios que buscan la "protección y preservación del cerebro y la mente humana."[15]

El término *neuroderechos* fue introducido por Marcello Ienca y Roberto Andorno en el 2017. Este término surgió de un análisis normativo de instrumentos de protección de Derechos Humanos como la Declaración Universal de Derechos Humanos (1948), la Carta de los Derechos Fundamentales de la Unión Europea (2000) y la Declaración Universal sobre Bioética y Derechos Humanos de la UNESCO (2005). El estudio de estos instrumentos, comparado con el avance de la neurotecnología, llevó a los autores a concluir que los derechos humanos

[11] Marcello Ienca, "On Neurorights."
[12] "Mission." The Neurorights Foundation. Accedido el 3 de Diciembre de 2022. https://neurorightsfoundation.org/mission.
[13] William Safire, "Visions for a new field of neuroethics," *Neuroethics: Mapping the Field, Conference Proceedings, May 13-14, 2002*, (San Francisco: The Dana Press), 4–9. https://dana.org/wp-content/uploads/2022/05/neuroethics-mapping-the-field.pdf
[14] Marcello Ienca, "On Neurorights."
[15] Ibidem

existentes son necesarios, pero no son suficientes para enfrentarse a los nuevos retos planteados por la neurotecnología.[16]

Ienca y Andorno proponen la conceptualización de cuatro *neuroderechos.* Estos son el derecho a la libertad cognitiva, a la privacidad mental, a la integridad mental y a la continuidad psicológica.[17] El derecho a la libertad cognitiva busca proteger a los individuos del uso coercitivo y no consensuado de la neurotecnología. En esencia, les da a las personas el derecho a elegir de manera informada si desean usar cierta neurotecnología y cómo usarla. El derecho a la privacidad mental protege a las personas de la intromisión sin consentimiento de su información cerebral, así como la recolección sin autorización de estos datos. El derecho a la integridad mental busca garantizar que no se manipule de manera no consensuada o perjudicial la actividad mental de las personas. Por último, el derecho a la continuidad psicológica busca preservar la identidad de las personas y protegerlas de alteración sin consentimiento por terceras personas.[18]

La *Neurorights Foundation* (Fundación de Neuroderechos), es una organización fundada por Rafael Yuste, profesor de la Universidad de Columbia y director del Centro de Neurotecnología de esta Universidad.[19] Además, Yuste, fue uno de los ideólogos detrás del proyecto BRAIN (Brain Research through Advancing Innovative Neurotechnologies o Investigación del Cerebro a través del Avance de Neurotecnologías Innovadoras), un proyecto fundado por el gobierno de Estados Unidos en el 2014.[20] El entonces presidente Barack Obama dijo de este proyecto: "[T]enemos la oportunidad de mejorar la vida no sólo de millones, sino de miles de millones de personas en este planeta a través de la investigación que se lleva a cabo en esta Iniciativa BRAIN".[21]

---

[16] Marcello Ienca y Roberto Andorno, "Towards new human rights in the age of neuroscience and neurotechnology," *Life Sciences, Society and Policy,* Volumen 13, Artículo 5 (Abril 2017). https://lsspjournal.biomedcentral.com/articles/10.1186/s40504-017-0050-1

[17] Ibidem

[18] Ibidem

[19] "Meet our people." The Neurorights Foundation. Accedido el 3 de Diciembre, 2022. https://neurorightsfoundation.org/mission.

[20] Juanjo Becerra, "Rafael Yuste, ideólogo del proyecto Brain: "La humanidad se subirá a la chepa de la inteligencia artificial," *El Mundo,* 26 del 2023 https://www.elmundo.es/tecnologia/innovacion/working-progress/2023/03/26/641dc4e221efa078638b45d5.html

[21] "The BRAIN Initiative," The White House, accedido el 1 de Junio del 2023, https://obamawhitehouse.archives.gov/BRAIN

La Fundación de Neuroderechos busca proteger los derechos humanos de las personas frente a estas nuevas tecnologías. Por lo tanto, propone cinco derechos que considera fundamentales: el libre albedrío, el acceso equitativo a las tecnologías de mejora, la identidad personal, la protección de sesgos y la privacidad mental.[22] Con esto, se agrega un neuroderecho que no había sido previamente considerado, el de acceso equitativo a las tecnologías de mejora.

Sin embargo, esta es solo una propuesta de cuáles deben ser los neuroderechos. Hasta ahora no hay un consenso internacional en qué consisten estos derechos.[23] Otras propuestas de cuáles deben ser los neuroderechos incluyen el derecho a la autonomía personal. Este incluye tanto el derecho al consentimiento informado del uso de la neurotecnología, pero también a la preservación de la libre voluntad de las personas, sin interferencia de terceros. Otros temas que se proponen que los neuroderechos resuelvan son la protección de la alteración neuronal, dimensión o continuidad sin consentimiento (integridad mental e identidad personal) y protección de sesgos algorítmicos.[24] La autora considera que la creación de neuroderechos específicos tienen que ver con las necesidades históricas del momento y lugar que los creen o regulen. Sin embargo, esta investigación se enfoca analizar el neuroderecho a la privacidad mental. Por una parte, de los neuroderechos propuestos y revisados anteriormente, el único en el que tanto Ienca y Andorno coinciden con Yuste,[25] indicando que estos investigadores (como la autora), consideran que un derecho importante por explorar. Además, es el único neuroderecho que está contemplado y protegido, explícita o implícitamente en Latinoamérica.[26]

El ejemplo más notable es que en el 2021, Chile hizo una reforma constitucional para proteger este neuroderecho. Esta propuesta puso en su carta magna el siguiente texto "[E]l desarrollo científico estará al servicio de las personas y se llevará a cabo con respeto a la vida y su integridad física y síquica. La ley establecerá los requisitos, condiciones y restricciones para su uso en las personas, debiendo resguardar especialmente la actividad cerebral e información

[22] "Mission." The Neurorights Foundation. Accedido el 3 de Diciembre de 2022. https://neurorightsfoundation.org/mission.
[23] Rafael Yuste, Jared Genser y Stephanie Herrmann, "It's Time for Neuro-Rights."
[24] Karen Herrera-Ferrá, José M. Muñoz, Humberto Nicolini, Garbiñe Saruwatari Zavala y Víctor Manuel Martínez Bullé Goyri, "Contextual and Cultural Perspectives on Neurorights: Reflections Toward an International Consensus," *AJOB Neuroscience* (2022), 10.1080/21507740.2022.2048722
[25] Eric García-López, José M. Muñoz y Roberto Andorno, "Editorial: Neurorights and Mental Freedom: Emerging Challenges to Debates on Human Dignity and Neurotechnologies," *Frontiers in Human Neuroscience,* volumen 15 (Diciembre 2021). https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8727361/
[26] Karen Herrera-Ferrá, *et al*, "Contextual and Cultural Perspectives on Neurorights."

de ella".[27] Como se dijo en la discusión en el senado chileno, la intención de aprobar esta iniciativa es "generar un nuevo derecho humano que busca garantizar la integridad física y síquica". [28] En agosto del 2023, la Suprema Corte de Chile tuvo la oportunidad de proteger este derecho. En una sentencia en contra de Emotiv, una empresa que estadounidense que almacena la información cerebral de los usuarios. En esta sentencia, la Suprema Corte afirmo que esta compañía vulnera las garantías constitucionales que corresponden a la integridad física y psíquica, así como el derecho a la privacidad.[29]

Por otro lado, en España se creó la Carta de Derechos Digitales. Este es un documento que busca proteger los derechos y libertades de las personas de las personas en entornos digitales y ante nuevas tecnologías. Esta Carta protege el neuroderecho a la privacidad mental en su artículo 26. Este dice que "[L]as condiciones, límites y garantías de implantación y empleo en las personas de las neurotecnologías podrán ser reguladas por la ley con la finalidad de: c) Asegurar la confidencialidad y seguridad de los datos obtenidos o relativos a sus procesos cerebrales y el pleno dominio y disposición sobre los mismos."[30] Sin embargo, en distinción como se buscaba hacer en Chile, "[L]a Carta no tiene carácter normativo, sino que su objetivo es reconocer los novísimos retos de aplicación e interpretación que la adaptación de los derechos al entorno digital plantea, así como sugerir principios y políticas referidas a ellos en el citado contexto."[31] Además, ellos señalan que no se están generando nuevos derechos humanos. Como mencionan en las consideraciones previas "[la carta] no trata de crear nuevos derechos fundamentales si no de perfilar los más relevantes en el entorno y los espacios digitales o describir derechos instrumentales o auxiliares de los primeros."[32]

---

[27] Decreto núm 43,086-B del 2021 [con fuerza de ley]. Por medio del cual se modifica la Carta Fundamental, para establecer el desarrollo científico y tecnológico al servicio de las personas (Ley núm. 21,383). Diario Oficial de la República de Chile, 25 de Octubre del 2021.

[28] "Histórica Aprobación: Información Cerebral Estará Protegida En La Constitución - Senado - República De Chile." Senado. Accedido el 6 de Junio, 2022. https://www.senado.cl/noticias/neuroderechos/historica-aprobacion-informacion-cerebral-estara-protegida-en-la.

[29] Francisco Corvalán, "Neuroderechos: Corte Suprema acogió recurso contra empresa que almacena datos cerebrales," *LaTercera*, 11 de agosto del 2023. https://www.latercera.com/que-pasa/noticia/neuroderechos-corte-suprema-acogio-recurso-contra-empresa-que-almacena-datos-cerebrales/GX3KDMHC6NDUVCNHGIKBF4AOWI/

[30] Carta de Derechos Digitales del Reino de España. Artículo 26, 14 de julio del 2021. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf

[31] Ibidem

[32] Ibidem

2. Privacidad

Para entender el neuroderecho a la privacidad mental, primero hay que dar un paso atrás y ver el derecho a la privacidad. Una de las primeras menciones de privacidad en el sistema jurídico moderno fue la concepción que hizo el juez de la Suprema Corte de Estados Unidos, Louis Brandeis en la década de los 1890. Brandeis argumentaba que la privacidad es el "derecho a ser dejado en paz" y que debe ser una de las libertades más importantes en una democracia.[33] Más tarde, a mediados del siglo XX, Alan Westin fue uno de los investigadores más importantes del concepto de la privacidad.[34] El definió la privacidad como "la capacidad de un individuo de determinar qué información sobre sí mismo pueden conocer los demás."[43] Además, menciona que existe un conflicto continuo entre tres grupos de intereses y orientaciones ideológicas. La primera, una posición de alta privacidad, tiene más desconfianza de las organizaciones y busca intervenciones que protejan la privacidad a través de leyes. La segunda, una posición de privacidad limitada, piensa que los reclamos de privacidad son menos importantes que la eficiencia de los negocios y de los intereses de la sociedad. Además, tiende a tener más confianza en las instituciones y a oponerse a nuevas intervenciones regulatorias. La tercera, una posición de privacidad balanceada, valora la privacidad al mismo tiempo que busca intervenciones legales contra abusos y promueve elecciones de privacidad individual.[35]

[33] Jedidiah Bracy, "Westin's Privacy Scholarship, Research Influenced a Generation," *The Privacy Advisor*, 1 de marzo del 2013, https://web.archive.org/web/20130622195347/https:/www.privacyassociation.org/publications/2013_02_19_westins_privacy_scholarship_research_influenced_a_generation

[34] Ibidem

[35] lan Westin, Social and Political Dimensions of Privacy *Journal of Social Issues, Vol. 59, No. 2, 2003, pp. 431--453,* traducción de la autora.

Capítulo Segundo: ¿Cómo se pueden leer los pensamientos?

a. Formas de descifrar la actividad neuronal

Hay dos formas principales de descifrar la actividad neuronal, la primera es con métodos no invasivos y la segunda es con métodos invasivos. Ejemplos de la primera forma son la electroencefalografía (EEG), la resonancia magnética funcional (fMRI) y la espectroscopia del infrarrojo cercano.[36] Usando señales del fMRI se puede recrear la imagen visual de una persona.[37] Incluso, con estas tecnologías, investigadores se han podido comunicar con personas en un estado vegetativo o mínimamente conscientes.[38]

Una limitación de usar fMRI es que las personas tienen que estar dentro del escáner. Por lo mismo, la investigación de métodos invasivos ha aumentado y con eso la creación de interfaces cerebro-computadora (BCI por sus siglas en inglés). Entre otras cosas, estas interfaces permiten que, a través de una operación o procedimiento cerebral, electrodos puedan decodificar las intenciones de una persona. Esto ha ayudado a que individuos paralizados puedan manejar desde su mente brazos robóticos[39] o incluso volver a tener movimiento en sus manos.[40] En el 2022, la compañía Synchron, fue la primera en Estados Unidos en poner un implante cerebral en un paciente con ELA (esclerosis lateral amiotrófica) que le permite usar el internet y mandar mensajes con solo pensar. Este implante (con una cirugía mínimamente invasiva) traduce sus pensamientos en instrucciones para la computadora.[41]

---

[36] Pieter R. Roelfsema, Damiaan Deys, P. Christian Klink, "Mind Reading and Writing: The Future of Neurotechnology," *Trends in Cognitive Sciences,* Volumen 22, Número 7 (Julio 2018): 598-610. https://doi.org/10.1016/j.tics.2018.04.001

[37] Xiaogang Chen, Yijun wang, Masaki Nakanishi and Shangkai Gao, "High-speed spelling with a noninvasive brain–computer interface," *Proceedings of the National Academy of Sciences of the United States of America (PNAS)* (19 de Octubre del 2015). https://doi.org/10.1073/pnas.1508080112

[38] Adrian M. Owen, Martin R. Coleman, Melanie Boly, Matthew H. Davis, Steven Laureys, John D. Pickar,"Detecting awareness in the vegetative state." *Science* (8 de Septiembre del 2006). https://www.science.org/doi/10.1126/science.1130197

[39] Leigh R. Hochberg, Daniel Bacher, Beata Jarosiewicz, Nicolas Y. Masse, *et al, "*Reach and grasp by people with tetraplegia using a neurally controlled robotic arm." *Nature*, 485 (2012): pp. 372-375. https://www.nature.com/articles/nature11076

[40] Chad E. Bouton, Ammar Shaikhouni, Nicholas V Annetta, Marcia A Bockbrader, *et al,* "Restoring cortical control of functional movement in a human with quadriplegia." *Nature,* (Mayo del 2016). https://pubmed.ncbi.nlm.nih.gov/27074513/

[41] Ashlee Vance, "Brain-Computer Interface Company Implants New Type of Device," *Bloomberg*, Julio 18, 2022, https://www.bloomberg.com/news/articles/2022-07-18/brain-computer-interface-company-implants-new-type-of-device?leadSource=uverify wall.

La interpretación de distintos patrones neuronales busca extraer información de la actividad cerebral y predecir qué acción se llevará a cabo o reconstruir los eventos y estímulos que causaron tal actividad.[42] La decodificación lineal tradicional ha llevado a muy buenos resultados, sin embargo, la combinación con ciencias informáticas lo ha llevado al siguiente nivel.[43]

b. Inteligencia Artificial

Una de las tecnologías informáticas que ha tenido mucho impacto en el campo de la biotecnología (y en el mundo en general) es la inteligencia artificial. La inteligencia artificial son las técnicas que permiten que las computadoras imiten el comportamiento humano para resolver tareas complejas. La inteligencia artificial contiene modelos analíticos que buscan generar reglas, respuestas, predicciones, etc. Al principio, esta tecnología requería que las personas escribieran código del cual la computadora pudiera hacer inferencias lógicas. Sin embargo, este método tenía la limitación de que a los humanos se les dificulta codificar el conocimiento tácito requerido para realizar tareas complejas.[44]

Con la intención de solucionar el problema anterior y de automatizar la inteligencia artificial, se creó un método llamado *machine learning* (aprendizaje automático). Este fenómeno sucede cuando "[E]n vez de codificar el conocimiento en las computadoras, el machine learning busca aprender automáticamente, relaciones importantes y patrones a través de ejemplos y observaciones".[45] Por ejemplo, en vez de definir en una computadora, a través de código, qué es una princesa, se le da a la máquina muchos ejemplos de princesas para que esta reconozca el patrón existente entre ellas y llegue a su propia conclusión. Esto ha llevado al crecimiento de sistemas inteligentes que parecen replicar la cognición humana y en ciertos casos, rebasarla, al

[42] Pieter R. Roelfsema, Damiaan Deys, P. Christian Klink, "Mind Reading and Writing: The Future of Neurotechnology," *Trends in Cognitive Sciences,* Volumen 22, Número 7 (Julio 2018): 598-610. https://doi.org/10.1016/j.tics.2018.04.001
[43] Ari S. Benjamin, Hugo L. Fernandes, Tucker Tomlinson, Pavan Ramkumar, Chris Ver Steeg, Lee Miller, Konrad Paul Kording, "Modern Machine Learning as a Benchmark for Fitting Neural Responses," Frontiers in Computational Neuroscience (Julio del 2018). https://doi.org/10.3389/fncom.2018.00056
[44] Christian Janiesch, Philipp Zschech, y Katharina Heinrich. 2021. "Machine learning and deep learning." *Electron Markets*31 (3): 685-695. https://doi.org/10.1007/s12525-021-00475-2.
[45] Ibidem

encontrar patrones complejos y aparentemente escondidos, a pesar de no haber sido explícitamente programados para buscarlos.[46]

c. Machine learning

Con ayuda del *machine learning* se ha avanzado mucho en la interpretación de patrones de la actividad neuronal. La decodificación neuronal (*neural decoding)* busca reconstruir los estímulos que causan cierta actividad neuronal o intentar predecir las acciones que van a surgir después de tal actividad.[47] En otras palabras, busca encontrar cómo las neuronas procesan la información.[48] Cualquier aplicación que busca interpretar cómo funciona el cerebro necesita tener parte del código neuronal. Para funciones más sencillas, como la generación de movimiento o la percepción, ya se conoce gran parte del código neuronal. Sin embargo, para funciones más complejas como el pensamiento abstracto y la memoria es mucho más difícil descifrar este código. Los métodos de decodificación lineal tradicional han tenido resultados exitosos, sin embargo, no son capaces de interpretar tanta información a la vez. Con ayuda del *machine learning* se han creado métodos de decodificación mucho más efectivos. A través del análisis de redes neuronales profundas (*deep neuronal networks* o *DNN* por sus siglas en inglés) el *machine learning* puede interpretar patrones de actividad mucho más complejos. Incluso, es posible que con esta tecnología sea posible entender la actividad cerebral sin conocimiento explícito del código neuronal.[49]

Sin embargo, esta no es la única aplicación del *machine learning* relacionada con este tema. A través del *machine learning* (aprendizaje automático) las computadoras pueden hacer correlaciones entre circunstancias externas y la actividad cerebral. Esta combinación lleva a que realicen predicciones altamente precisas de los pensamientos y las motivaciones humanas.[50] Un reporte del Derecho a la Privacidad en la Era Digital del Alto Comisionado de las Naciones Unidas para el Consejo de Derechos Humanos dice que la inteligencia artificial puede hacer

[46] Christian Janiesch, Philipp Zschech, y Katharina Heinrich. 2021. "Machine learning and deep learning."
[47] Pieter R. Roelfsema, Damiaan Deys, P. Christian Klink, “Mind Reading and Writing”.
[48] S.H. Scott, "Neural Coding in Primary Motor Cortex," in *Encyclopedia of Neuroscience*, edited by Larry R. Squire (Academic Press, 2009), 105-115, https://doi.org/10.1016/B978-008045046-9.01322-X.
[49] Pieter R. Roelfsema, Damiaan Deys, P.Christian Klink, “Mind Reading and Writing”.
[50] Melissa Heikkilä, “Machines Can Read Your Brain. There's Little That Can Stop Them.”

inferencias de gran alcance acerca de la condición mental y física de los individuos. Además, puede establecer la probabilidad de comportamiento futuro.[51]

La inteligencia artificial no solo busca predecir comportamientos futuros, sino, también "leer" lo que ya está en la mente humana. Investigadores han logrado inferir los números de una tarjeta de crédito a través de la actividad cerebral de una persona. Otro estudio publicado en la revista *Nature* detalla un experimento donde se escaneó el cerebro de los participantes mientras veían imágenes de distintas caras. A través del análisis de las imágenes cerebrales hechas en un fMRI, esta inteligencia artificial logró recrear casi perfectamente las caras que veían los participantes en la computadora.[52]

c. Computación cuántica

Esta es la situación tecnológica en el presente. Sin embargo, expertos creen que el uso de la computación cuántica podría llevar el uso de la inteligencia artificial y el *machine learning* al siguiente nivel. Una computadora cuántica tiene el poder de desempeñar muchas tareas de manera simultánea. Esto está basado en el concepto de la mecánica cuántica llamado superposición. Esto quiere decir que se puede existir en múltiples estados al mismo tiempo, pero que la observación va a causar que se tome un estado en específico. Una forma de entenderlo es un experimento mental que se ha hecho famoso en la cultura popular, el llamado cato de Schrödinger.[53]

La diferencia entre una computadora como la conocemos actualmente y una computadora cuantica, es que las primeras funcionan a través de la manipulación de números binarios, que existen en dos estados, ceros y unos. Por otro lado, las computadoras cuánticas

[51] Michelle Bachelet, "La inteligencia artificial plantea riesgos para la privacidad y exige una acción urgente, dice Bachelet", comunicado de prensa, Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, 15 de septiembre de 2021, https://www.ohchr.org/es/press-releases/2021/09/artificial-intelligence-risks-privacy-demand-urgent-action-bachelet.
[52] Thirza Dado, Yağmur Güçlütürk, Luca Ambrogioni, Gabriëlle Ras, Sander Bosch, Marcel van Gerven y Umut Güçlü. "Hyperrealistic neural decoding for reconstructing faces from fMRI activations via the GAN latent space". *Scientific Reports* 12, Artículo número: 141 (2022), https://doi.org/10.1038/s41598-021-03938-w
[53] Molly Ruby, "Quantum Computers in the Revolution of Artificial Intelligence and Machine Learning." *Medium,* 18 de marzo del 2023. https://towardsdatascience.com/quantum-computers-in-the-revolution-of-artificial-intelligence-and-machine-learning-c5b0356903f3

existen en superposición. Están al mismo tiempo combinaciones de ceros y unos. Esto permite que puedan procesar millones de algoritmos de manera simultánea. Esto haría que las capacidades de la inteligencia artificial avancen exponencialmente.[54]

A pesar de la promesa de esta nueva tecnología, la computación cuántica no ha llegado a manifestar todo su potencial. En el 2019, científicos en Google declararon que habían logrado la *supremacía cuántica.* Sin embargo, expertos aseguran que esta afirmación es una exageración y que todavía la humanidad no está en esa era. En el 2023, el equipo cuántico de IBM presento sus nuevos hallazgos y dijo que estaban entrando en la era de la *utilidad* cuántica. Estas computadoras logran hacer calculaciones que en una computadora normal no podrían hacerse. Sin embargo, todavía hay mucho por trabajarse, sobre todo en el área de corrección y mitigación de errores, para el que se necesitan procesadores mucho más poderosos de los que se tienen actualmente.[55]

La intención de este capítulo fue detallar la situación tecnológica y describir los conceptos técnicos. En los capítulos posteriores se busca analizar los desafíos legales y regulatorios que presentan estas tecnologías. En específico, el neuroderecho a la privacidad mental.

[54] Ibidem.
[55] Kenneth Chang, "*Quantum Computing Advance Begins New Era, IBM Says," New York Times,* 14 de junio del 2023. https://www.nytimes.com/2023/06/14/science/ibm-quantum-computing.html

Capítulo Tercero: Sistema de la Unión Europea

a. Contexto histórico: Protección de datos personales y el Holocausto Nazi

El origen de las leyes de protección de datos personales tiene muchas explicaciones. Sin embargo, algunos expertos piensan que una de las causas históricas fue lo sucedido en Alemania durante las Segunda Guerra Mundial. Una revisión de la historia de episodios recientes de genocidio y abuso de derechos humanos están relacionados con el uso de recabar información personal de la población y tratarla con herramientas tecnológicas. Uno de los casos más famosos es el ocurrido en el Holocausto Nazi. En el libro Protección de la Privacidad en Sociedades de Vigilancia, el autor David Flaherty establece que "[L]as leyes de protección de datos incluyen la agenda oculta de desalentar una repetición de los esfuerzos Nazis y de la Gestapo por controlar a la población, y por tanto buscan evitar la reaparición de una burocracia opresiva que podría utilizar los datos existentes para fines nefastos. Esta preocupación es un fundamento tan vital de la actual legislación [de protección de datos] que rara vez se expresa en los debates formales. ... Así, los legisladores europeos han reflejado un miedo real al Gran Hermano basado en la experiencia común de la destructividad potencial de la vigilancia mediante el mantenimiento de registros. Ninguno[56] desea repetir las experiencias sufridas bajo los Nazis durante la Segunda Guerra Mundial."[57] Es fundamental entender que el desarrollo de las leyes de protección de datos en Europa está inmerso en este pasado histórico y por lo mismo va a tener características distintas a las normativas desarrolladas en otros lugares. Sin embargo, es importante entender que esta narrativa histórica no siempre avanza hacia "delante". Un ejemplo de esto es la propuesta de un ministro italiano de hacer un censo a las personas de origen romaní en el 2018.[58]

b. GDPR

El Reglamento General de Protección de Datos de la Unión Europea (GDPR, por sus siglas en inglés) es considerado como el catalizador de uno de los cambios más importantes en

[56] Esta sección busca explicar el pasado historico en el que esta inmersa la región que se analiza. Sin embargo, no se busca asegurar que todos los Estados miembros de la Unión Europea estan dispuestos a no cometer los mismos errores historicos.
[57] David Flaherty, *Surveillance Societies* (Oxford: ABC-CLIO, 1989).
[58] Redacción, "Italia prepara un censo de gitanos para expulsar a los irregulares." *La vanguardia, 18 de junio del 2018.* https://www.lavanguardia.com/internacional/20180618/45226771012/italia-censo-gitanos-salvini.html

materia de protección de datos de los últimos 20 años.[59] Desde el 2018, el GDPR es aplicable a cualquier organización que recolecta y procesa información de ciudadanos de la Unión Europea, dentro y fuera de esta.[60] Los siete principios por los que se rige el GDPR son los siguientes: Legalidad, equidad y transparencia; Limitación del propósito; Minimización de datos; Exactitud; Limitaciones de almacenamiento; Integridad y confidencialidad; y Responsabilidad.[61]

El primer principio, legalidad, equidad y transparencia, establece que los datos personales deben ser procesados de manera legal, equitativa y transparente. El segundo principio, limitación del propósito, dice que los datos personales deben ser recolectados para un fin específico y legítimo. Además, estos datos no pueden ser usados para un fin distinto al que fueron recolectados (excepto si es con fines de interés público, científico, histórico o estadístico). El tercer principio, minimización de datos, busca que solo se recolectan los datos personales relevantes y adecuados conectados con el fin que se propone. El cuarto principio, exactitud, indica que se tienen que tomar todos los pasos posibles para asegurarse que los datos guardados sean exactos y que no estén, por ejemplo, expirados. El quinto principio, limitaciones de almacenamiento, establece que los datos personales sólo pueden ser almacenados por el tiempo que sea necesario para cumplir los propósitos con los que se recolectaron. El sexto principio, integridad y confidencialidad, dice que los datos se tienen que guardar de manera segura y con suficiente protección contra intrusiones ajenas. El séptimo principio, responsabilidad, establece que quien controla los datos personales debe demostrar que cumple con todos los principios anteriores.

c. Impacto Global del GDPR

A pesar de que el GDPR es legislación de la Unión Europea, este ha tenido un impacto global muy grande, ya que obliga a cualquier organización que procese datos de ciudadanos europeos, independientemente de su localización.[62] Muchas compañías (sobre todo las corporaciones multinacionales), tienden a crear regulaciones internas basadas en el estándar

[59] Razieh Nokhbeh Zaeem and K. Suzanne Barber. 2020. "The Effect of the GDPR on Privacy Policies: Recent Progress and Future Promise." *ACM Trans. Manage. Inf. Syst.* 12, no. 1, Articulo 2 (Marzo 2021): 20, https://doi.org/10.1145/3389685.
[60] Ibidem
[61] Ibidem
[62] Ibidem

internacional más estricto para reducir el costo de cumplir con distintas formas de regular. Por lo mismo, tales compañías tienden a tener una sola política de protección de datos personales, y esta es la de la Unión Europea. El impacto extraterritorial del GDPR depende tanto del cumplimiento voluntario de ciertas corporaciones y del poder coercitivo que puedan tener tribunales de la Unión Europea para hacer cumplir a aquellas compañías que traten datos personales de ciudadanos de la Unión.[63]

Sin embargo, esta no es la única forma en que el GDPR tiene un impacto global. Muchos países alrededor del mundo han decidido adaptar su sistema normativo al planteado por este reglamento. Esto significa que ha habido una *difusión política* exitosa de esta normativa de protección de datos personales. La *difusión política* es cuando un proceso proveniente de una situación política o jurídica de un tiempo y lugar en específico es adoptado en otro lugar. Hay dos razones principales por las que existe este fenómeno, determinantes internos y externos. Los determinantes internos tienen que ver con la búsqueda de legitimidad por parte de la comunidad internacional y la expectativa de que la legislación adoptada puede resolver un problema interno. Los determinantes externos tienen que ver con la presión de organizaciones internacionales o supranacionales imponiendo ciertas regulaciones a los Estados miembros de sus organizaciones. Otras razones tienen que ver con proximidad geográfica, conexión con comunidades de conocimiento y competencia, nexos económicos y comerciales.[64]

Con relación a la *difusión política* externa, muchos países que no son miembros de la Unión Europea adoptan estándares del GDPR para asegurar su competitividad y atraer más inversión extranjera. Una de las razones es que los procesos de integración económica de la Unión Europea permiten que los países miembros actúen como un bloque dándole más fuerza a sus normas supranacionales. Además, los países que están altamente integrados con la economía de la Unión Europea tienen muchos incentivos para adoptar los estándares del GDPR.[65] Algunos ejemplos de países, no miembros de la Unión Europea, que han adoptado legislaciones parecidas al GDPR son Australia, Brasil, Canadá, Chile, China, Egipto, India, Israel, Japón, Nueva Zelanda, Nigeria, Sudáfrica, Corea del Sur, Suiza, Tailandia y Turquía.[66]

---

[63] Ivy Hu, "Economic, Social and Cultural Rights in the Digital Age: The Case of Privacy and Data Protection."
[64] Ibidem
[65] Ibidem
[66] "Countries with GDPR-like Data Privacy Laws," Comfort Insights, accedido Julio 25, 2022, https://insights.comforte.com/countries-with-gdpr-like-data-privacy-laws.

d. ¿Por qué se analiza el GDPR?

La intención de este trabajo no es analizar el GDPR por sus méritos sustantivos. Con esto, no se pretende asegurar que esta es la mejor regulación a nivel mundial para proteger datos personales. A pesar de esto, se reconoce su tratamiento innovador e integral de la materia. La razón por la que se analiza el GDPR es por el impacto material que este reglamento tiene en el mundo. Estudiosos del derecho han llegado a la conclusión que el GDPR ha evolucionado a ser un *estándar de oro* a nivel mundial. Esto tiene que ver con el llamado *Efecto Bruselas.*[67]

La profesora de Columbia, Anu Bradford, ha definido el *Efecto Bruselas*, como el poder unilateral que tiene Europa para regular el mercado global. Ella explica que la Unión logra hacer esto a través del uso de mecanismos de mercado y plantea dos maneras principales, *de facto* y *de jure.* Por mecanismos *de facto*, se refiere a la adopción de sus estándares regulatorios por compañías orientadas a la exportación de sus productos y servicios. Por mecanismos *de jure*, se habla de la promulgación de leyes por otras legislaturas en jurisdicciones con motivaciones parecidas. Otros juristas, como Paul Schwartz, de la Universidad de Berkley, vislumbran un modelo más complejo. Él dice que, sobre todo en materia de privacidad de datos, la Unión Europea, utiliza estrategias de negociación, además de haber creado un modelo legal muy trasplantable a otras jurisdicciones.[68]

e. GDPR en México

A pesar de que el foco de este trabajo no es analizar la normativa mexicana, no queda de más subrayar el impacto que ha tenido el GDPR en México y como este ha afectado el tratamiento de datos personales en el país. La protección de datos personales en México es un derecho humano que está consagrado en la Constitución Mexicana. El artículo 16 constitucional establece que "[T]oda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público,

[67] Arturo Carajillo y Matías Jackson "Follow the Leader? A Comparative Law Study of the EU's General Data Protection Regulation's Impact in Latin America," *ICL Journal, Volumen* 16, número 2, https://www.degruyter.com/document/doi/10.1515/icl-2021-0037/html
[68] Ibidem

seguridad y salud públicas o para proteger los derechos de terceros."[69] En esencia, este artículo busca limitar el uso indiscriminado de los datos personales y asimismo, dar a los titulares de los datos personales, derechos ARCO (acceso, rectificación, cancelación y oposición).

Por otro lado, en el 2018 México se adhirió al Convenio 108 de la Unión Europea (Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal).[70] Un año antes, en el 2017, México expidió la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.[71] Ésta impuso responsabilidades de protección en materia de datos personales a las autoridades públicas y entidades gubernamentales. La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados incorporó muchos elementos del GDPR. Entre ellos se encuentran la portabilidad de datos, los DPOs y los DPIAs. Por portabilidad de datos se habla del derecho de los titulares de datos personales de obtener o transferir los datos que han dado a cierta entidad. Además, cada entidad debe tener una manera mecánica y automática de proporcionar dichos datos. Los DPOs (por sus siglas en inglés) son los delegados de protección de datos que se encargan de garantizar un buen tratamiento de esta información. El DPIAs (por sus siglas en inglés) es la evaluación de impacto de la protección de datos. Esta busca analizar de manera automatizada los procesos necesarios para evaluar los riesgos asociados con el tratamiento de datos personales. Además, la ley, al igual que el GDPR, impone bastantes obligaciones tanto en los encargados como en los responsables de datos (a pesar de que los encargados tienen más obligaciones).[72]

A pesar de que hay muchas similitudes entre la Ley General de Datos Personales en Posesión de Sujetos Obligados y el GDPR, también hay muchas disparidades. La principal tiene que ver con la forma única en la que México decidió regular esta materia. A diferencia de otros países de Latinoamérica y Europa, México tiene una aproximación dual a la protección de datos personales. Esto significa que regula de manera distinta el tratamiento que deben tener los

[69] Constitución Política de los Estados Unidos Mexicanos, art. 16, Diario Oficial de la Federación, 5 de febrero de 1917. https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf

[70] OF. "DECRETO Promulgatorio del Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, hecho en Estrasburgo, Francia, el veintiocho de enero de mil novecientos ochenta y uno.", 28 de septiembre de 2018, Diario Oficial de la Federación, última modificación 28 de septiembre de 2018,

[71] Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), 5 de julio del 2010, México.https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

[72] Arturo Carajillo y Matías Jackson "Follow the Leader? A Comparative Law Study of the EU's General Data Protection Regulation's Impact in Latin America."

actores públicos y privados. Esto hace que se complique la comparación con el GDPR, ya que por definición la Ley del sector público mexicana sólo regula a los sujetos obligados. Por lo mismo es difícil examinar el impacto extraterritorial de la ley de la misma forma en la que se analiza el GDPR. Otra diferencia que hay entre el GDPR y la Ley General de Datos Personales en Posesión de Sujetos Obligados es que esta segunda solo incorporó de manera implícita el derecho a ser olvidado.[73] El derecho a ser olvidado establece la posibilidad de los titulares de datos de pedirle a ciertas organizaciones borrar sus datos personales.

El propósito de los siguientes capítulos es explorar la incidencia del GDPR en los neuroderechos. En específico, analiza la relación entre este Reglamento y el neuroderecho a la privacidad mental que es el enfoque de esta investigación.

[73] Ibidem

Capítulo Cuarto: Datos personales y datos personales sensibles

a. Datos personales

Este capítulo se enfoca en analizar las categorías de datos personales dentro del GDPR, para en capítulos posteriores establecer una relación con los datos mentales y por lo tanto poder visualizar si estos pueden proteger el neuroderecho a la privacidad mental. El GDPR define establece dos elementos para definir a los datos personales. El primero es el objeto y el segundo el sujeto. Como objeto se habla de la información sobre una persona física identificada (se sabe quién es) o identificable (es posible saber quién es). Como se sujetó se habla del "interesado" que es la persona física identificable. Para calificar como tal, su identidad debe poder determinarse, directa o indirectamente por un identificador particular. El GDPR pone como ejemplos de identificadores un "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." [74]

Si existen datos personales seudonomizados (con un seudónimo) pero con uso de información adicional sería posible identificar a la persona física, debe considerarse como información sobre una persona física identificable. Para saber si esta persona es identificable, debe determinarse si se puede singularizar de manera razonable y tomar en cuenta los factores objetivos como el coste, cantidad de tiempo y tecnología disponible para hacerlo. Por lo mismo, la información que no tenga relación con una persona física identificada o identificable o que haya sido hecha anónima, y que no se pueda singularizar a la persona, no está regulada bajo el

[74] GDPR. Artículo 7. Sección 1. A efectos del presente Reglamento se entenderá por: 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.

GDPR.[75] Además, no entran dentro de este reglamento los datos personales sobre personas que han muerto.[76]

Algo que es fundamental recalcar es que el GDPR protege los datos personales de las personas físicas no de las personas jurídicas. Es por eso por lo que los datos personales (para efectos de este reglamento) se definen como información sobre personas físicas únicamente. Esta clasificación no es aplicable para regular el tratamiento de datos personales de personas jurídicas como podrían ser el nombre, la forma de la persona jurídica y datos de contacto de empresas u otras personas jurídicas.[77]

Además, la protección de las personas físicas es tecnológicamente neutra. Esto quiere decir que la protección de los datos personales no depende de la técnica utilizada y debe aplicarse tanto al tratamiento manual, como al automatizado.[78] Por otra parte, el GDPR no se aplica al tratamiento de datos personales que tiene una persona física en una actividad que sea exclusivamente personal o doméstica. Esto quiere decir, que no tenga una conexión profesional o comercial. Ejemplos de estas actividades son la correspondencia personal, tener un directorio de direcciones, el uso de redes sociales y del internet para llevar a cabo las actividades anteriores.

---

[75] GDPR. Consideraciones. Parrafo 26. Los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable. Los datos personales seudonimizados, que cabría atribuir a una persona física mediante la utilización de información adicional, deben considerarse información sobre una persona física identi- ficable. Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física. Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos. Por lo tanto los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo. En consecuencia, el presente Reglamento no afecta al tratamiento de dicha información anónima, inclusive con fines estadísticos o de investigación.

[76] GDPR. Consideraciones. Parrafo 27. El presente Reglamento no se aplica a la protección de datos personales de personas fallecidas. Los Estados miembros son competentes para establecer normas relativas al tratamiento de los datos personales de estas.

[77] GDPR. Consideraciones. Parrafo 14. 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. El presente Reglamento no regula el tratamiento de datos personales relativos a personas jurídicas y en particular a empresas constituidas como personas jurídicas, incluido el nombre y la forma de la persona jurídica y sus datos de contacto.

[78] GDPR. Consideraciones. Parrafo 15. 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. La protección de las personas físicas debe aplicarse al tratamiento automatizado de datos personales, así como a su tratamiento manual, cuando los datos personales figuren en un fichero o estén destinados a ser incluidos en él. Los ficheros o conjuntos de ficheros, así como sus portadas, que no estén estructurados con arreglo a criterios específicos, no deben entrar en el ámbito de aplicación del presente Reglamento.

Sin embargo, este Reglamento su regula a los responsables o encargados que proporcionen los medios para llevar a cabo actividades personales y domésticas.[79]

b. Excepciones a la regulación de datos personales

El GDPR no debe aplicarse al tratamiento de datos personales por parte de las autoridades competentes cuando se trate de amenazas contra la seguridad pública y cuestiones penales como la prevención, investigación, detección enjuiciamiento de infracciones penales y ejecución de sentencias penales. Todo lo anterior debe regirse por la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo. [80]

El GDPR si regula el tratamiento de datos personales por parte de tribunales y otras autoridades judiciales. Sin embargo, para proteger la independencia judicial, cuando se trate del tratamiento de datos personales en el ejercicio de la función judicial, tendrá que haber un órgano independiente establecido por el sistema judicial del Estado miembro.[81]

---

[79] GDPR. Consideraciones. Parrafo 18. El presente Reglamento no se aplica al tratamiento de datos de carácter personal por una persona física en el curso de una actividad exclusivamente personal o doméstica y, por tanto, sin conexión alguna con una actividad profesional o comercial. Entre las actividades personales o domésticas cabe incluir la correspondencia y la llevanza de un repertorio de direcciones, o la actividad en las redes sociales y la actividad en línea realizada en el contexto de las citadas actividades. No obstante, el presente Reglamento se aplica a los responsables o encargados del tratamiento que proporcionen los medios para tratar datos personales relacionados con tales actividades personales o domésticas.

[80] GDPR. Consideraciones. Parrafo 19. La protección de las personas físicas en lo que respecta al tratamiento de datos de carácter personal por parte de las autoridades competentes a efectos de la prevención, investigación, detección o enjuiciamiento de infracciones penales o de la ejecución de sanciones penales, incluida la protección frente a las amenazas contra la seguridad pública y la libre circulación de estos datos y su prevención, es objeto de un acto jurídico específico a nivel de la Unión. El presente Reglamento no debe, por lo tanto, aplicarse a las actividades de tratamiento destinadas a tales fines. No obstante, los datos personales tratados por las autoridades públicas en aplicación del presente Reglamento deben, si se destinan a tales fines, regirse por un acto jurídico de la Unión más específico, concre- tamente la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo (1). Los Estados miembros pueden encomendar a las autoridades competentes, tal como se definen en la Directiva (UE) 2016/680, funciones que no se lleven a cabo necesariamente con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o ejecución de sanciones penales, incluida la protección frente a las amenazas a la seguridad pública y su prevención, de tal forma que el tratamiento de datos personales para estos otros fines, en la medida en que esté incluido en el ámbito del Derecho de la Unión, entra en el ámbito de aplicación del presente Reglamento.

[81] GDPR. Consideraciones. Parrafo 20. Aunque el presente Reglamento se aplica, entre otras, a las actividades de los tribunales y otras autoridades judiciales, en virtud del Derecho de la Unión o de los Estados miembros pueden especificarse las operaciones de tratamiento y los procedimientos de tratamiento en relación con el tratamiento de datos personales por los tribunales y otras autoridades judiciales. A fin de preservar la independencia del poder judicial en el desempeño de sus funciones, incluida la toma de decisiones, la competencia de las autoridades de control no debe abarcar el tratamiento de datos personales cuando los tribunales actúen en ejercicio de su función judicial. El control de esas operaciones de tratamiento de datos ha de poder encomendarse a organismos específicos establecidos dentro del sistema judicial del Estado miembro, los cuales deben, en particular, garantizar el cumplimiento de las normas del presente Reglamento, concienciar más a los miembros del poder judicial acerca de

c. Consentimiento para el tratamiento de datos personales

Para que haya consentimiento para el uso de datos personales la voluntad se tiene que manifestar con los siguientes elementos: tiene que ser libre, especifica, informada e inequívoca. Formas para expresar la voluntad incluyen una declaración por escrito, en medios electrónicos o de manera verbal. Un ejemplo muy común de esto es marcar una casilla en un sitio web. Algo que es de suma importancia considerar es que el silencio, las casillas ya marcadas o la falta de acción no son consideradas como consentimiento. Si el tratamiento de datos tiene muchos fines, se tiene que otorgar consentimiento para cada uno de ellos.[82]

Una excepción a esto, son los datos que se utilizan con fines de investigación científica. A veces es difícil saber *a priori* cual será la finalidad del tratamiento de esos datos. Por eso los interesados pueden consentir a dar sus datos para un ámbito general de la investigación científica.[83]

Los niños tienen una protección especial de sus datos personales ya que pueden ser menos conscientes de los riesgos implícitos o de los derechos que tienen para defenderlos. Por eso a menos que sea un servicio preventivo o de asesoramiento especialmente dirigido a niños, los titulares de la patria potestad o tutela deben otorgar su consentimiento.[84]

---

sus obligaciones en virtud de este y atender las reclamaciones en relación con tales operaciones de tratamiento de datos.

[82]GDPR. Consideraciones. Parrafo 32. El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. Esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. 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. Si el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta.

[83] GDPR. Consideraciones. Parrafo 33. Con frecuencia no es posible determinar totalmente la finalidad del tratamiento de los datos personales con fines de investigación científica en el momento de su recogida. Por consiguiente, debe permitirse a los interesados dar su consentimiento para determinados ámbitos de investigación científica que respeten las normas éticas reconocidas para la investigación científica. Los interesados deben tener la oportunidad de dar su consentimiento solamente para determinadas áreas de investigación o partes de proyectos de investigación, en la medida en que lo permita la finalidad perseguida.

[84] GDPR. Consideraciones. Parrafo 38. Los niños merecen una protección específica de sus datos personales, ya que pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales. Dicha protección específica debe aplicarse en particular, a la utilización de datos personales de niños con fines de mercadotecnia o elaboración de perfiles de personalidad o de usuario, y a la obtención de datos personales relativos a niños cuando se utilicen servicios ofrecidos directamente a un niño. El consentimiento

d. Definición de datos personales sensibles

Los datos personales sensibles son definidos en el GDPR en él sus Consideraciones en el párrafo 51. Este dice que merecen especial protección los datos que pueden entrañar riesgos para los derechos y libertades fundamentales. Como regla general está prohibido el tratamiento de datos personas que revelen la siguiente información de las personas: su origen étnico, racial, sus opiniones políticas, creencias filosóficas o religiosas, afiliación sindical. También está prohibido el tratamiento de datos genéticos y biométricos que quieran identificar de manera inequívoca a una persona física y los datos de la vida u orientación sexual de una persona.[85] Las fotografías no son automáticamente datos personales sensibles, solo cuando permiten identificar de manera inequívoca a la persona física.

Lo más importantes, es que estos datos no deben ser tratados excepto en los casos específicos permitidos por el reglamento. A pesar de esto los Estados miembros pueden establecer disposiciones específicas. Además de los requisitos específicos se tiene que aplicar los otros principios y normas, en especial condiciones de licitud del tratamiento. Puede haber excepciones para el tratamiento de estos datos cuando el interesado de su consentimiento explicito o en necesidades específicas (siempre a la luz de proteger los derechos y libertades fundamentales).[86]

---

del titular de la patria potestad o tutela no debe ser necesario en el contexto de los servicios preventivos o de asesoramiento ofrecidos directamente a los niños.

[85]. GDPR. Artículo 9. Quedan prohibidos el tratamiento de datos personales 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.

[86] GDPR. Consideraciones. Parrafo 51. Especial protección merecen los datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales. Debe incluirse entre tales datos personales los datos de carácter personal que revelen el origen racial o étnico, entendiéndose que el uso del término «origen racial» en el presente Reglamento no implica la aceptación por parte de la Unión de teorías que traten de determinar la existencia de razas humanas separadas. El tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física. Tales datos personales no deben ser tratados, a menos que se permita su tratamiento en situaciones específicas contempladas en el presente Reglamento, habida cuenta de que los Estados miembros pueden establecer disposiciones específicas sobre protección de datos con objeto de adaptar la aplicación de las normas del presente Reglamento al cumplimiento de una obligación legal o al cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Además de los requisitos específicos de ese tratamiento, deben aplicarse los principios generales y otras normas del presente Reglamento, sobre todo en lo que se refiere a las condiciones de licitud del tratamiento. Se deben establecer de forma explícita excepciones a la prohibición general de tratamiento de esas categorías especiales de datos personales, entre otras cosas cuando el interesado dé su

d. Subtipos de datos personales sensibles

Un tipo de datos personales son los datos personales genéticos. Estos son definidos como los datos que estén relacionados con características genéticas. Estas pueden ser heredadas o adquiridas y tienen que venir del análisis biológico de una persona física. El análisis biológico se refiere a un análisis del ADN, ARN u otro elemento que pueda obtener información que sea equivalente.[87]

Otro tipo de datos, son los datos relativos a la salud. Estos se refieren a aquellos que den información sobre el estado de la salud física o mental del interesado, independientemente si es del pasado, presente o futura. [88]

Por último, están los datos biométricos. Estos son los datos que son obtenidos a través de un tratamiento técnico especifico que captura datos o características físicas, fisiológicas o conductuales de las personas. Ejemplos de esto son imágenes faciales o huellas dactilares.[89]

consentimiento explícito o tratándose de necesidades específicas, en particular cuando el tratamiento sea realizado en el marco de actividades legítimas por determinadas asociaciones o fundaciones cuyo objetivo sea permitir el ejercicio de las libertades fundamentales.

[87] GDPR. Consideraciones. Parrafo 34. Debe entenderse por datos genéticos los datos personales relacionados con características genéticas, heredadas o adquiridas, de una persona física, provenientes del análisis de una muestra biológica de la persona física en cuestión, en particular a través de un análisis cromosómico, un análisis del ácido desoxirribonucleico (ADN) o del ácido ribonucleico (ARN), o del análisis de cualquier otro elemento que permita obtener información equivalente.

[88] GDPR. Consideraciones. Parrafo 35. 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 (1); 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 fuente, por ejemplo un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro.

[89] GDPR. Artículo 7. Sección 14. A efectos del presente Reglamento se entenderá por: 14. «datos biométricos»: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las caracte- rísticas físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.

b. Excepciones generales a la prohibición del tratamiento de datos personales sensibles

El párrafo 52 de las Consideraciones GDPR habla acerca de las excepciones especificas a la prohibición del tratamiento de datos personales sensibles. La primera es cuando lo establezca el derecho de la unión o los estados miembros, si existen las garantías apropiadas. La segunda es cuando sea en interés público, sobre todo en temas de: legislación laboral, protección social, supervisión y alerta sanitaria, prevención o control de enfermedades transmisibles y amenazas graves a la salud. Esa excepción también aplica para fines de salud incluyendo la sanidad pública, sobre todo para garantizar los seguros médicos, para archivos de interés público, investigación científica, histórica y/o fines estadísticos (más adelante se ahondará más en excepciones relacionadas con salud. La última excepción que menciona este artículo es para el uso de estos datos personales sensibles en un procedimiento judicial, administrativo o extrajudicial.[90]

Por otro lado, el GDPR permite que se traten estos datos por autoridades públicas cuando se quieran alcanzar los objetivos (partes del derecho consuetudinario o internacional publico) de asociaciones religiosas que están reconocidas de manera oficial.[91] Además, en actividades electorales se les puede permitir a los partidos políticos recopilar datos personas sensibles sobre opiniones políticas siempre y cuando sea por razones de interés público y se ofrezcan garantías adecuadas.[92]

[90] GDPR. Consideraciones. Parrafo 52. Asimismo deben autorizarse excepciones a la prohibición de tratar categorías especiales de datos personales cuando lo establezca el Derecho de la Unión o de los Estados miembros y siempre que se den las garantías apropiadas, a fin de proteger datos personales y otros derechos fundamentales, cuando sea en interés público, en particular el tratamiento de datos personales en el ámbito de la legislación laboral, la legislación sobre protección social, incluidas las pensiones y con fines de seguridad, supervisión y alerta sanitaria, la prevención o control de enfermedades transmisibles y otras amenazas graves para la salud. Tal excepción es posible para fines en el ámbito de la salud, incluidas la sanidad pública y la gestión de los servicios de asistencia sanitaria, especialmente con el fin de garantizar la calidad y la rentabilidad de los procedimientos utilizados para resolver las reclama- ciones de prestaciones y de servicios en el régimen del seguro de enfermedad, o con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos. Debe autorizarse asimismo a título excepcional el tratamiento de dichos datos personales cuando sea necesario para la formulación, el ejercicio o la defensa de reclamaciones, ya sea por un procedimiento judicial o un procedimiento administrativo o extrajudicial.

[91] GDPR. Consideraciones. Parrafo 55. Se realiza además por razones de interés público el tratamiento de datos personales por las autoridades públicas con el fin de alcanzar los objetivos, establecidos en el Derecho constitucional o en el Derecho internacional público, de asociaciones religiosas reconocidas oficialmente.

[92] GDPR. Consideraciones. Parrafo 56. Si, en el marco de actividades electorales, el funcionamiento del sistema democrático exige en un Estado miembro que los partidos políticos recopilen datos personales sobre las opiniones políticas de las personas, puede autorizarse el tratamiento de estos datos por razones de interés público, siempre que se ofrezcan garantías adecuadas.

c. Excepciones en temas de salud a la prohibición del tratamiento de datos personales sensibles

Hay excepciones a la prohibición de uso de datos personales sensibles en ciertos temas relacionados con la salud. El GDPR dice que estos datos solo pueden usarse con fines relacionados con la salud cuando sea necesario para el bienestar de las personas físicas y de la sociedad. Sobre todo, para garantizar que siga habiendo asistencia sanitaria, protección social, asistencia sanitaria transfronteriza, fines de seguridad, supervisión y alerta sanitaria. También para archivos con interés público, para investigaciones científicas, históricas o estadísticas.

Sin embargo, tiene que haber condiciones específicas cuando estos datos son tratados en temas de salud por personas que tienen la obligación de respetar el secreto profesional. Además, los estados miembros pueden introducir otras condiciones o limitaciones cuando se trate de datos genéticos, biométricos o relativos a la salud siempre y cuando este no sea un obstáculo para la libre de circulación de datos personales dentro de la Unión Europea.[93]Además, los datos personales sensibles solo se pueden usar sin consentimiento del interesado por razones de interés público en salud pública. Sin embargo, su tratamiento tiene que estar sujeto a medidas que protejan los derechos y libertades de las personas físicas. Terceros (empresarios, seguros, o bancos) no pueden usar estos datos para otros fines. 94

[93] GDPR. Consideraciones. Parrafo 53. Las categorías especiales de datos personales que merecen mayor protección únicamente deben tratarse con fines relacionados con la salud cuando sea necesario para lograr dichos fines en beneficio de las personas físicas y de la sociedad en su conjunto, en particular en el contexto de la gestión de los servicios y sistemas sanitarios o de protección social, incluido el tratamiento de esos datos por las autoridades gestoras de la sanidad y las autoridades sanitarias nacionales centrales con fines de control de calidad, gestión de la información y supervisión general nacional y local del sistema sanitario o de protección social, y garantía de la continuidad de la asistencia sanitaria o la protección social y la asistencia sanitaria transfronteriza o fines de seguridad, supervisión y alerta sanitaria, o con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, basados en el Derecho de la Unión o del Estado miembro que ha de cumplir un objetivo de interés público, así como para estudios realizados en interés público en el ámbito de la salud pública. Por tanto, el presente Reglamento debe establecer condiciones armonizadas para el tratamiento de categorías especiales de datos personales relativos a la salud, en relación con necesidades específicas, en particular si el tratamiento de esos datos lo realizan, con fines relacionados con la salud, personas sujetas a la obligación legal de secreto profesional. El Derecho de la Unión o de los Estados miembros debe establecer medidas específicas y adecuadas para proteger los derechos fundamentales y los datos personales de las personas físicas. Los Estados miembros deben estar facultados para mantener o introducir otras condiciones, incluidas limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud. No obstante, esto no ha de suponer un obstáculo para la libre circulación de datos personales dentro de la Unión cuando tales condiciones se apliquen al tratamiento transfronterizo de esos datos.

[94] GDPR. Consideraciones. Parrafo 54. El tratamiento de categorías especiales de datos personales, sin el consentimiento del interesado, puede ser necesario por razones de interés público en el ámbito de la salud pública. Ese tratamiento debe estar sujeto a medidas adecuadas y específicas a fin de proteger los derechos y libertades de las personas físicas. En ese contexto, «salud pública» debe interpretarse en la definición del Reglamento (CE) n.o 1338/2008 del Parlamento Europeo y del Consejo (1), es decir, todos los elementos relacionados con la salud,

CAPITULO QUINTO: DATOS MENTALES

a. Datos Mentales

Este trabajo busca responder la pregunta de si ¿es suficiente la regulación de datos personales y datos personales sensibles de la Unión Europea para proteger el neuroderecho a la privacidad mental? Para poder determinar si la legislación actual protege o no los datos mentales, hay que definir en qué consiste esta información y si es diferente de los datos personales y los datos personales sensibles. En esencia, lo que se busca responder a continuación es si ¿la información mental es una categoría distinta dentro de los datos personales?

Hay varias preguntas que se van a hacer en esta sección para poder contestar esta pregunta general. La primera es ¿qué son los datos mentales? La segunda es ¿son los datos mentales datos personales? La tercera es ¿son los datos mentales datos personales sensibles? Por último ¿la categoría de datos personales sensibles protege los datos mentales?

Ienca y Malgieri definen los datos mentales como "cualquier dato que pueda organizarse y procesarse para inferir los estados mentales de una persona, incluidos sus estados cognitivos, afectivos y de conciencia."[95] Para que un dato mental sea considerado un dato personal dentro del GDPR tiene que haber una conexión entre el objeto (el dato) y el sujeto (la persona física). En otras palabras, el dato tiene que ser un identificador de la persona. De esto se puede concluir que un dato mental es un dato personal cuando este permite identificar a la persona física. Por ejemplo, una emoción o un pensamiento, que no es posible saber quién lo siente o lo piensa, no es un dato personal.

b. ¿Son los datos mentales datos personales sensibles?

Para saber si los datos mentales son datos personales sensibles, hay dos formas de hacer un análisis. La primera es por el contenido del dato personal. La segunda es si en esencia, los

concretamente el estado de salud, con inclusión de la morbilidad y la discapacidad, los determinantes que influyen en dicho estado de salud, las necesidades de asistencia sanitaria, los recursos asignados a la asistencia sanitaria, la puesta a disposición de asistencia sanitaria y el acceso universal a ella, así como los gastos y la financiación de la asistencia sanitaria, y las causas de mortalidad. Este tratamiento de datos relativos a la salud por razones de interés público no debe dar lugar a que terceros, como empresarios, compañías de seguros o entidades bancarias, traten los datos personales con otros fines.

[95] Marcello Ienca y Gianclaudio Malgieri, "Mental Data Protection and the GDPR," *Journal of Law and the Biosciences*, (5 de Mayo, 2021). http://dx.doi.org/10.2139/ssrn.3840403

datos mentales son datos personales sensibles, independientemente de su contenido. Resulta bastante obvio que un dato mental que tenga un contenido que entre dentro de los supuestos marcados por el GDPR como datos personales sensibles será uno de estos. Esto quiere decir que cualquier dato mental que permita saber el origen étnico, racial, las opiniones políticas, creencias filosóficas o religiosas, afiliación sindical, la vida sexual, orientación sexual, datos genéticos o biométricos califica como un dato personal sensible.[96]

Por el otro lado, cabe analizar si los datos mentales son datos sensibles *per se.* Hay dos categorías de datos sensibles dentro de los que los datos mentales podrían caber. La primera tiene que ver con la definición de datos relativos a la salud. La segunda con los datos biométricos.

c. ¿Son los datos mentales datos personales relativos a la salud?

Algunos autores, como Ienca *et al.* y Yuste *et al.* argumentan que los datos mentales tienen la habilidad de conocer y predecir el estatus de salud presente y futuro de una persona.[97] El GDPR define a los datos relacionados con la salud como la información sobre el estado de la salud física o mental de la persona física, en el pasado, presente o futura.

Ienca propone que el término salud mental debe interpretarse de manera expansiva. Por eso se refiere a que parámetros biológicos que serían capaces de determinar una patología de la mente, deben ser considerados como datos mentales sensibles, incluso en la ausencia de tal patología.[98] Por ejemplo, si se puede acceder a información mental que podría determinar si una persona sufre de depresión, incluso en la ausencia de esa enfermedad mental, la información que podría decir si se tiene depresión o no, también debe considerarse como datos personales sensibles. La autora de este trabajo quisiera agregar que toda la información, que podría llegar a la misma conclusión, aunque se esté usando con una finalidad distinta, también debería ser considerada como datos personales sensibles.

[96] GDPR. Artículo 9. Quedan prohibidos el tratamiento de datos personales 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.
[97] Marcello Ienca y Giancluadio Malgieri, "Mental data protection and the GDPR" y Rafael Yuste, Jared Genser y Stephanie Herrmann, "It's Time for Neuro-Rights."
[98] Marcello Ienca y Giancluadio Malgieri, "Mental data protection and the GDPR."

Sin embargo, incluso con esta interpretación expansiva, no toda la información mental cabría dentro de esta categoría. Ejemplos de categorías que no entran sería emociones no relacionadas con cierta patología y la mayoría de los pensamientos, preferencias o memorias. Con el resto de los datos mentales hay dos posibles interpretaciones. Por una parte, considerar que todos los datos mentales por naturaleza son datos relativos a la salud y por lo tanto datos sensibles. La segunda opción es determinar que no son datos relativos a la salud. Dentro de la definición de datos relativos a la salud se incluye "cualquier información relativa […] [al] estado fisiológico o biomédico del interesado."[99]

Ienca y Malgieri concluyen que los datos personales no son por naturaleza datos relativos a la salud. Ellos establecen que "[P]or lo que concierne a los datos que revelan información relacionada con los pensamientos o memorias de los interesados, estos datos no son automáticamente datos sensibles por el mero hecho de referirse a la 'esfera mental' del sujeto."[100]

Este trabajo argumenta que sería posible hacer una interpretación más amplia de los datos relativos a la salud para incluir a los datos mentales.[101] El GDPR define a los datos relacionados con la salud como la información sobre el estado de la salud física o mental de la persona física, en el pasado, presente o futura. Dentro de esta parte de la definición no entran muchos datos mentales, ya que no todos son capaces de determinar el estado de salud de una persona física.

La parte de la definición donde podrían hacerse una interpretación más amplia es la siguiente: "[los datos relativos a la salud son] cualquier información relativa […] [al] estado fisiológico o biomédico del interesado."[102] Aquí resulta necesario hacerse una pregunta técnica:

---

[99] GDPR. Consideraciones. Parrafo 35. 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 (1); 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 fuente, por ejemplo un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro.

[100] Marcello Ienca y Giancluadio Malgieri, "Mental data protection and the GDPR."

[101] Marcello Ienca y Giancluadio Malgieri, "Mental data protection and the GDPR."

[102] GDPR. Consideraciones. Parrafo 35. 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

¿son los datos mentales datos sobre el estado fisiologico o biomedico de las personas físicas? Ienca y Malgieri argumentan que hay una diferencia fundamental entre la mente y el cerebro, y por lo tanto una diferencia entre los datos cerebrales y los datos mentales. Ellos establecen que los datos cerebrales son mediciones directas del cerebro humano, su estructura, función y actividad. Además, presentan dos razones por las que los datos mentales deberían estar separados de los datos cerebrales.

Primero, argumentan que no todos los datos mentales son datos cerebrales, ya que mucha de la información acerca del estado mental puede inferirse de otros tipos de datos, por ejemplo, información acerca del comportamiento de las personas (*behavioural data)*. Segundo, dicen que no todos los datos cerebrales son datos mentales ya que la información cerebral puede ser procesada para buscar cosas distintas al estado mental, como la anatomía o fisiología del cerebro.[103]

Los argumentos presentados anteriormente plantean una interpretación posible. Sin embargo, la autora de este trabajo propone una interpretación alternativa. Primero, a pesar de que no necesariamente se necesitan datos neuronales para saber que pasa por la mente de una persona, estas predicciones buscan inferir la conclusión a la que la actividad neuronal llegará. Por lo mismo, busca recrear de manera artificial lo que el cerebro hizo o hará de manera natural. Por lo tanto, de alguna manera, busca conocer el estado fisiológico o biomédico del interesado. Y segundo, sería posible simplemente considerar a los los datos mentales como una subclasificación de los datos cerebrales. Esto quiere decir que mientras no todos los datos cerebrales son mentales, todos los datos mentales podrían considerarse como datos cerebrales.

d. ¿Son los datos mentales datos biométricos?

El GDPR define a los datos biométricos como los datos que son obtenidos a través de un tratamiento técnico especifico que captura datos o características físicas, fisiológicas o

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

[103] Marcello Ienca y Giancluadio Malgieri, "Mental data protection and the GDPR"

conductuales de las personas y que permitan confirmar la identidad de una persona.[104] Un artículo publicado por el MIT Science Policy Review establece que hay dos tipos de datos biométricos. Los primeros, llamados biometría de primera generación, se enfocan en la identificación de personas a través de herramientas como la geometría facial y las huellas dactilares. Tradicionalmente, estos son los que han sido regulados. La segunda generación, o biométrica de comportamiento, están siendo desarrollados. Este tipo de biometría "[…] incluye la voz, la marcha, las expresiones faciales, la frecuencia cardíaca y la actividad cerebral, se utiliza cada vez más para detectar estados emocionales y cognitivos momentáneos, como el estrés y la fatiga, y para clasificar características mentales más estables, como las intenciones, las preferencias y el estado de salud."[105]

Bajo esta definición, los datos mentales que identifican la actividad cerebral con técnicas biométricas si son datos personales sensibles. Sin embargo, como observan Ienca y Malgieri, "[…] es difícil considerar sensibles los datos relacionados con las emociones detectados mediante métodos no biométricos (por ejemplo, texto escrito o registros de voz)."[106] Esto quiere decir que no todos los datos mentales serían datos biométricos de manera automática y por lo tanto no todos estarían protegidos bajo el régimen de datos personales sensibles.

[104] GDPR. Artículo 7. Sección 14. A efectos del presente Reglamento se entenderá por: 14. «datos biométricos»: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las caracte- rísticas físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.

[105] Constanza M. Vidal Bustamante, Karolina Alama-Maruta, Carmen Ng y Daniel D.L. Coppersmith, "Should machines be allowed to 'read our minds'? Uses and regulation of biometric techniques that attempt to infer mental states," *MIT Science Policy Review* (2022), https://sciencepolicyreview.org/wp-content/uploads/securepdfs/2022/08/MITSPR-v3-191618003010.pdf

[106] Marcello Ienca y Giancluadio Malgieri, "Mental data protection and the GDPR." Y Rafael Yuste, Jared Genser y Stephanie Herrmann, "It's Time for Neuro-Rights."

Conclusiones

Este trabajo se enfoco en explorar la relación del derecho a la privacidad mental en el contexto de la regulación de la Unión Europea, en especifico el GDPR. Para hacer este analisis se examino la naturaleza de los datos mentales y su relación con las categorías pre existentes de datos personales y datos personales sensibles.

Para esto, se definio a los datos mentales como los datos que puedan ser procesados para inferir los estados mentales de las mentales, incluyendo sus estados cognitivos, afectivos y de conciencia. Además, se ha establecido que un dato mental se considera un dato personal cuando puede identificar a una persona física. Para examinar si los datos mentales se pueden categorizar como datos personales sensibles se examino el contenido y la naturaleza instrinsica de este tipo de datos. Aquí se concluyo que si un dato mental tiene un contenido protegido bajo esta categoría se considera un dato personal sensible. Sin embargo, sigue la pregunta de si los datos mentales son datos personales sensibles *per se,* independientemente de su contenido. Este trabajo argumenta que sería posible hacer una interpretación más amplia de los datos relativos a la salud, una sub-categoría de los datos personales sensibles, para incluir a los datos mentales. Sin embargo, respecto la sub-categoría de datos biometricos como datos personales sensibles, no se puede decir que no todos los datos mentales serían datos biométricos de manera automática.

En conclusión, hay una relación compleja entre el neruoderecho a la privacidad mental y la regulación del GDPR, se necesita una mayor claridad y debate en este ambito para poder proteger este derecho de mejor manera. Por lo mismo, la autora propone las siguientes recomendaciones.

Como se exploró en este trabajo, de hacerse una interpretación amplia del GDPR, sobre todo en la regulación de datos sensibles, se podrían proteger los datos mentales. Sin embargo, esto requiere la aceptación de varias de las interpretaciones planteadas, algo que no puede asegurarse. Además, hace que sea difícil que los obligados de cumplir el Reglamento, o los interesados en proteger sus derechos, sepan cómo tratar o proteger los datos mentales. Esto presenta un riesgo para la certeza jurídica.

El GDPR dice en sus consideraciones "[E]l tratamiento de datos personales debe estar concebido para servir a la humanidad."[107] De ser así, sería bueno recordar las palabras de Joseph Michel Servan, un abogado francés, que ya en el siglo XVIII habia dicho: "[S]obre las flojas fibras del cerebro se asienta la base inquebrantable de los imperios más sólidos." La protección de los datos mentales es uno de los retos más importantes de los siguientes años. Quién tenga en su poseción el conocimiento sobre lo que hay en la mente de otros tiene un enorme poder. Tal vez un poder que no se ha visto nunca antes. El uso de esta tecnología puede ser de enorme beneficio para la humanidad. Ayudar a personas con paralisis, Alzheimers y Estrés Postraumatico. Cambiar la forma en que se trabaja, en que las personas se relacionan con la tecnología y con el Otro.

Sin embargo, como cualquier herramienta, tiene el potencial de dañar y causar sufrimiento. Un cuchillo puede usarse como bisturí para salvar o como navaja para asesinar. Es deber de la comunidad decidir que forma es aceptable y como se debe regular. Este trabajo propone que dentro del GDPR debería estar regulado los datos mentales como una sub categoría de los datos sensibles y por lo tanto gozar del estandar más elevado que requiere su tratamiento. Esto es un primer paso necesario que cabe dentro del marco actual para la protección de datos. Sería positivo que trabajos susbecuentes investiguen si el régimen de datos personales sensibles y el mismo GDPR son la mejor forma de proteger el neuroderecho a la privacidad mental.

[107] GDPR. Consideraciones. Parrafo 4. El tratamiento de datos personales debe estar concebido para servir a la humanidad. El derecho a la protección de los datos personales no es un derecho absoluto, sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad. El presente Reglamento respeta todos los derechos fundamentales y observa las libertades y los principios reconocidos en la Carta conforme se consagran en los Tratados, en particular el respeto de la vida privada y familiar, del domicilio y de las comunicaciones, la protección de los datos de carácter personal, la libertad de pensamiento, de conciencia y de religión, la libertad de expresión y de información, la libertad de empresa, el derecho a la tutela judicial efectiva y a un juicio justo, y la diversidad cultural, religiosa y lingüística.

Referencias

Austen, Jane. *Pride and Prejudice.* Harlow, England: Pearson Education Limited, 2019.

Bachelet, Michelle. "La inteligencia artificial plantea riesgos para la privacidad y exige una acción urgente, dice Bachelet", comunicado de prensa, Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, 15 de septiembre de 2021. https://www.ohchr.org/es/press-releases/2021/09/artificial-intelligence-risks-privacy-demand-urgent-action-bachelet.

Becerra, Juanjo.“Rafael Yuste, ideólogo del proyecto Brain: "La humanidad se subirá a la chepa de la inteligencia artificial." *El Mundo,* 26 del 2023.

Benjamin, Ari S., Hugo L. Fernandes, Tucker Tomlinson, Pavan Ramkumar, Chris VerSteeg, Lee Miller, Konrad Paul Kording. “Modern Machine Learning as a Benchmark for Fitting Neural Responses.” *Frontiers in Computational Neuroscience* (Julio del 2018). https://doi.org/10.3389/fncom.2018.00056

Bouton, Chad E., Ammar Shaikhouni, Nicholas V. Annetta, Marcia A. Bockbrader, *et al.* “Restoring cortical control of functional movement in a human with quadriplegia.” *Nature,* (Mayo del 2016). https://pubmed.ncbi.nlm.nih.gov/27074513/

Bracy, Jedidiah**.** “Westin’s Privacy Scholarship, Research Influenced a Generation**.**” *The Privacy Advisor,* 1 de marzo del 2013**.** https://web.archive.org/web/20130622195347/https:/www.privacyassociation.org/publications/2013_02_19_westins_privacy_scholarship_research_influenced_a_generation

Carajillo, Arturo y Matías Jackson. “Follow the Leader? A Comparative Law Study of the EU’s General Data Protection Regulation’s Impact in Latin America.” *ICL Journal, Volumen* 16, número 2.

Carta de Derechos Digitales del Reino de España. 14 de julio del 2021. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf

Chang, Kenneth. "*Quantum Computing Advance Begins New Era, IBM Says." New York Times,* 14 de junio del 2023. https://www.nytimes.com/2023/06/14/science/ibm-quantum-computing.html

Chen, Xiaogang, Yijun Wang, Masaki Nakanishi and Shangkai Gao." High-speed spelling with a noninvasive brain–computer interface." *Proceedings of the National Academy of Sciences of the United States of America (PNAS)* (19 de Octubre del 2015). https://doi.org/10.1073/pnas.1508080112

Comfort Insights. "Countries with GDPR-like Data Privacy Laws." Accedido Julio 25, 2022, https://insights.comforte.com/countries-with-gdpr-like-data-privacy-laws.

Constitución Política de los Estados Unidos Mexicanos, art. 16, Diario Oficial de la Federación, 5 de febrero de 1917. https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf

Corvalán, Francisco. "Neuroderechos: Corte Suprema acogió recurso contra empresa que almacena datos cerebrales." *LaTercera,* 11 de agosto del 2023. https://www.latercera.com/que-pasa/noticia/neuroderechos-corte-suprema-acogio-recurso-contra-empresa-que-almacena-datos-cerebrales/GX3KDMHC6NDUVCNHGIKBF4AOWI/

Dado, Thirza, Yağmur Güçlütürk, Luca Ambrogioni, Gabriëlle Ras, Sander Bosch, Marcel van Gerven y Umut Güçlü. "Hyperrealistic neural decoding for reconstructing faces from fMRI activations via the GAN latent space". *Scientific Reports* 12, Artículo número: 141 (2022). https://doi.org/10.1038/s41598-021-03938-w.

Diario Oficial de la República de Chile. Decreto núm 43,086-B del 2021 [con fuerza de ley]. Por medio del cual se modifica la Carta Fundamental, para establecer el desarrollo científico y tecnológico al servicio de las personas (Ley núm. 21,383). 25 de Octubre del 2021.

DOF. "DECRETO Promulgatorio del Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, hecho en Estrasburgo, Francia, el veintiocho de enero de mil novecientos ochenta y uno.", 28 de septiembre de 2018, Diario Oficial de la Federación, última modificación 28 de septiembre de 2018. https://www.dof.gob.mx/nota_detalle.php?codigo=5539473&fecha=28/09/2018#gsc.tab=0.

Flaherty, David. *Surveillance Societies*. Oxford: ABC-CLIO, 1989.

García-López, Eric, José M. Muñoz y Roberto Andorno. "Editorial: Neurorights and Mental Freedom: Emerging Challenges to Debates on Human Dignity and Neurotechnologies." *Frontiers in Human Neuroscience,* volumen 15 (Diciembre 2021). https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8727361/

Heikkilä, Melissa. "Machines Can Read Your Brain. There's Little That Can Stop Them," *POLITICO,* 1 de Septiembre, 2021. https://www.politico.eu/article/machines-brain-neurotechnology-neuroscience-privacy-neurorights-protection/#:~:text=Inception,brain%20activity%20and%20external%20circumstances.

Herrera-Ferrá, Karen, José M. Muñoz, Humberto Nicolini, Garbiñe Saruwatari Zavala y Víctor Manuel Martínez Bullé Goyri. "Contextual and Cultural Perspectives on Neurorights: Reflections Toward an International Consensus." *AJOB Neuroscience* (2022), 10.1080/21507740.2022.2048722

Hochberg, Leigh R., Daniel Bacher, Beata Jarosiewicz, Nicolas Y. Masse, *et al. "*Reach and grasp by people with tetraplegia using a neurally controlled robotic arm." *Nature*, 485 (2012): pp. 372-375. https://www.nature.com/articles/nature11076

Ienca, Marcello y Gianclaudio Malgieri. "Mental Data Protection and the GDPR." *Journal of Law and the Biosciences*, (5 de Mayo, 2021). http://dx.doi.org/10.2139/ssrn.3840403
Ienca, Marcello y Gianclaudio Malgieri. "Mental Data Protection and the GDPR," *Journal of Law and the Biosciences*, (5 de Mayo, 2021). http://dx.doi.org/10.2139/ssrn.3840403

Ienca, Marcello y Roberto Andorno. "Towards new human rights in the age of neuroscience and neurotechnology." *Life Sciences, Society and Policy,* Volumen 13, Artículo 5 (Abril 2017). https://lsspjournal.biomedcentral.com/articles/10.1186/s40504-017-0050-1

Janiesch, Ari S., Philipp Zschech, y Katharina Heinrich. 2021. "Machine learning and deep learning." *Electron Markets*31 (3): 685-695. https://doi.org/10.1007/s12525-021-00475-2.

Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), 5 de julio del 2010. México.https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Owen, Adrian M., Martin R. Coleman, Melanie Boly, Matthew H. Davis, Steven Laureys, John D. Pickar. "Detecting awareness in the vegetative state." *Science* (8 de Septiembre del 2006). https://www.science.org/doi/10.1126/science.1130197

Redacción. "Italia prepara un censo de gitanos para expulsar a los irregulares." *La vanguardia, 18 de junio del 2018.* https://www.lavanguardia.com/internacional/20180618/45226771012/italia-censo-gitanos-salvini.html

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

Roelfsema, Pieter R., Damiaan Deys, P. Christian Klink. "Mind Reading and Writing: The Future of Neurotechnology." *Trends in Cognitive Sciences*, Volumen 22, Número 7 (Julio 2018): 598-610. https://doi.org/10.1016/j.tics.2018.04.001

Ruby, Molly. "Quantum Computers in the Revolution of Artificial Intelligence and Machine Learning." *Medium*, 18 de marzo del 2023. https://towardsdatascience.com/quantum-computers-in-the-revolution-of-artificial-intelligence-and-machine-learning-c5b0356903f3

Safire, William. "Visions for a new field of neuroethics." *Neuroethics: Mapping the Field, Conference Proceedings, May 13-14, 2002*, (San Francisco: The Dana Press), 4–9. https://dana.org/wp-content/uploads/2022/05/neuroethics-mapping-the-field.pdf

Scott, S.H. "Neural Coding in Primary Motor Cortex," in *Encyclopedia of Neuroscience*, edited by Larry R. Squire (Academic Press, 2009). https://doi.org/10.1016/B978-008045046-9.01322-X.

Senado. "Histórica Aprobación: Información Cerebral Estará Protegida En La Constitución - Senado - República De Chile." Accedido el 6 de Junio, 2022. https://www.senado.cl/noticias/neuroderechos/historica-aprobacion-informacion-cerebral-estara-protegida-en-la.

The Neurorights Foundation. "Meet our people." Accedido el 3 de Diciembre, 2022. https://neurorightsfoundation.org/mission.

The Neurorights Foundation. “Mission.” Accedido el 3 de Diciembre de 2022. https://neurorightsfoundation.org/mission.

The White House. “The BRAIN Initiative.”, accedido el 1 de Junio del 2023. https://obamawhitehouse.archives.gov/BRAIN

Tirrell, Meg. “Defense Department Developing a 'Prosthetic Memory'.” *CNBC*, 25 de Mayo, 2016. https://www.cnbc.com/2016/05/24/defense-department-developing-a-prosthetic-memory.html.

Vance, Ashlee. "Brain-Computer Interface Company Implants New Type of Device." *Bloomberg*, Julio 18, 2022. https://www.bloomberg.com/news/articles/2022-07-18/brain-computer-interface-company-implants-new-type-of-device?leadSource=uverify wall.

Vidal Bustamante, Constanza M., Karolina Alama-Maruta, Carmen Ng y Daniel D.L. Coppersmith. “Should machines be allowed to ‘read our minds’? Uses and regulation of biometric techniques that attempt to infer mental states.” *MIT Science Policy Review* (2022). https://sciencepolicyreview.org/wp-content/uploads/securepdfs/2022/08/MITSPR-v3-191618003010.pdf

Westin, lan. Social and Political Dimensions of Privacy. *Journal of Social Issues, Vol. 59, No. 2, 2003.*

Yuste, Rafael, Jared Genser y Stephanie Herrmann. “It's Time for Neuro-Rights.” *Horizons,* Volumen 18 (Invierno 2021). https://www.cirsd.org/files/000/000/008/47/7dc9d3b6165ee497761b0abe69612108833b5cff.pdf

Zaeem, Razieh Nokhbeh y K. Suzanne Barber. 2020. "The Effect of the GDPR on Privacy Policies: Recent Progress and Future Promise." *ACM Trans. Manage. Inf. Syst.* 12, no. 1, Articulo 2 (Marzo 2021): 20, https://doi.org/10.1145/3389685.