revistapensamientopenal

INTERFACES HUMANO-MÁQUINA EN CLAVE DE DATOS

AGOSTINA MIQUELARENA*

"¿Cómo emprender la tentativa de poner bajo control las relaciones espontáneas entre progreso técnico y el mundo social de la vida?[1]

I. INTRODUCCIÓN: EL DATO EN EL ENTORNO DIGITAL DE LAS BCI[2]

Como todo escenario de análisis, es menester presentar las bases sobre las que se asientan las ideas que se construyen. Con tal finalidad, el "alma" o "espíritu" del entorno digital se condensa en una nueva ideología que tambalea valores y principios, deconstruyendo los significados de antiguas expresiones.

Así, podemos decir que, el dataísmo es un término que ha sido utilizado para describir la mentalidad, filosofía o religión creado por el significado emergente del *big data*, inteligencia artificial e internet de las cosas (IoT)[3].

En tal sentido, Harari entiende a dicha expresión como una religión emergente que no venera ni a dioses ni al hombre: adora los datos[4].

***Licenciada en Criminalística (IUPFA). Profesional de la Unidad Fiscal Especializada en Cibercrimen y Evidencia Digital (UFECyED) del Ministerio Público Fiscal de Chubut. Posgraduada en Ciberseguridad y Delitos Informáticos (UBA). Perito Informática Forense (CPCI). Disertante en jornadas y congresos nacionales e internacionales. Contacto: amiquelarena@juschubut.gov.ar**

[1] Habermas, *Ciencia y técnica como "ideología"*, 1997, p. 127.

[2] Entiéndase como Interfaces Cerebro-Computadora

[3] https://pijamasurf.com/2019/05/que_es_el_dataismo__llega_la_religion_que_adora_los_datos_1/. En la misma línea sostiene Byung Chul-Han que el mundo de las cosas de internet produce nuevos fantasmas, las cosas que en otros tiempos eran mudas, empiezan a hablar (Byung Chul-Han, *En el enjambre*, 2014, p. 82).

[4] Harari, *Homo Deus: Breve historia del mañana*, 2015, p. 353

Por ello, tal filosofía centrada en el dato, resguarda resumidamente la idea de que se cree que la información es lo único esencial y la libertad de la información es el mayor de todos los bienes[5].

En razón de tal ideología, nos encontramos en pleno dataísmo, dejando de ser el humano soberano de sí mismo, para pasar a ser el resultado de una operación algorítmica[6] en el contexto de la automatización del dato.

En la misma inteligencia, expresa el filósofo sur coreano que el *Homo Digitalis* ya no recepta y consume de manera pasiva la información, sino que la produce y comunica de manera activa. Siendo consumidores y productores al mismo tiempo[7].

En esta lógica disruptiva, opera una nueva tecnología llamada interfaz cerebro computadora o BCI (*Brain-Computer Interface*, por sus siglas en inglés), que tiene por finalidad lograr establecer un nuevo canal de comunicación entre una persona y su entorno, que no dependa de vías nerviosas o musculares, conllevando la misma una serie de loables aportes, los cuales no están exentos de ciertos peligros y amenazas, los cuales resultan objeto del presente trabajo.

II. BCI: BRAIN COMPUTER-INTERFACES

2.1. Concepto y aplicabilidad

La manera en que naturalmente se comunica el cerebro y nuestro cuerpo requiere de la presencia de nervios y músculos. Esta intención de comunicarse desencadena un proceso complejo en el que determinadas áreas del cerebro son activadas, enviando señales a través del sistema nervioso periférico[8] a los músculos correspondientes, encargados de realizar la tarea que comenzó en nuestro pensamiento.

En este marco, es que las BCI ofrecen una alternativa a esta forma natural de comunicación y control, ya que consiste en un sistema de ingeniería capaz de traducir nuestras intenciones en interacción real con un mundo físico o virtual. Esto se logra midiendo la actividad cerebral, procesándola para obtener las características de interés, y una vez obtenidas, interaccionando con el entorno de la forma deseada por la persona o usuario[9].

---

[5] https://pijamasurf.com/2019/05/que_es_el_dataismo__llega_la_religion_que_adora_los_datos_1/

[6] "Como fundamento de esta ideología está el dataísmo, que concibe el mundo como un flujo de datos". https://www.fundeu.es/recomendacion/dataismo-sustantivo-valido/

[7] Byung-Chul Han, *op. cit.,* p. 34.

[8] La función del Sistema nervioso periférico es conectar el sistema nervioso central con las extremidades y órganos, permitiendo la transmisión de información. http://www.docenciatraumatologia.uc.cl/biologia-del-sistema-nervioso-periferico/

[9] Minguez, *Tecnología de Interfaz Cerebro – Computador,* p. 2. https://webdiis.unizar.es/~jminguez/Sesion001_UJI.pdf

Dichas interfaces, inmersas dentro del área de la neurotecnología[10], entendiéndose a la misma como el conjunto de métodos e instrumentos que permiten una conexión directa de dispositivos técnicos con el sistema nervioso, fueron diseñadas con el objetivo de cubrir el mayor rango de necesidades posibles.

Entre ellas, se ha utilizado con el objeto de diagnosticar enfermedades neurológicas, monitorizar la epilepsia[11] y los trastornos del sueño[12], realizar tratamientos de fobias, rehabilitación cognitiva[13] en demencia, en trastorno por déficit de atención con hiperactividad (TDAH)[14] y en personas mayores, o neurorrehabilitación[15] para recuperar movilidad con neuro prótesis[16] en personas que tienen discapacidad de movimiento, facilitándoles el control de sillas de ruedas y prótesis robóticas.

Sin embargo, los usos de la misma no se extinguen en las aplicaciones antedichas. Automóviles conectados con la mente, implantes en el cerebro para curar el Alzheimer[17], control de videojuegos por medio del pensamiento, o cartas que se escriben solo con pensarlo, son algunos de los avances en los que se encuentra trabajando la neurotecnología. Las posibilidades de aplicación de las interfaces cerebro computador abarcan diversidad de usos: *gaming*, control domótico[18] (tecnología adaptada a nuestra vivienda), salud o automoción.

Dentro de las capacidades que ofrecen las BCI, se encuentran las de capturar las actividades cognitivas y emocionales de un usuario, permitiendo el desarrollo de actividades

---

[10] Roberts, *Neurotecnologías: los desafíos de conectar el cerebro humano y computadores*, 2019, p. 2. https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/27272/1/If01_Neurotecnologias_BCN_final.pdf

[11] Engel, J., Kuhl, D. E., Phelps, M. E., and Crandall, P. H., *Comparative localization of foci in partial epilepsy by PCT and EEG*, 1982, p. 529. https://onlinelibrary.wiley.com/doi/epdf/10.1002/ana.410120605

[12] Portas, et al, *Auditory Processing across the Sleep-Wake Cycle: Simultaneous EEG and fMRI Monitoring in Humans*, 2000, p. 991. https://www.cell.com/neuron/fulltext/S0896-6273(00)00169-0?_returnURL=https%3A%2F%2Flinkinghub.elsevier.com%2Fretrieve%2Fpii%2FS0896627300001690%3Fshowall%3Dtrue

[13] Rosenstein, et al, *Uso de VPRN en la implementación de una BCI para rehabilitación neurológica*, 2018, p. 777 http://sedici.unlp.edu.ar/bitstream/handle/10915/67974/Documento_completo.pdf-PDFA.pdf?sequence=1&isAllowed=y

[14] Arns, et al,*The Effects of QEEG-Informed Neurofeedback in ADHD: An Open-Label Pilot Study*, 2012, p. 172 https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3419351/

[15] Giménez, et al, I*nterfaz BCI-FES para Rehabilitación Neurológica: resultados preliminares,* 2011, p. 2 http://www.sabi2011.fi.mdp.edu.ar/proceedings/SABI/Pdf/SABI2011_22.pdf

[16] MoreGrasp es un proyecto que tiene el objetivo de desarrollar una BCI no invasiva para el control intuitivo de una neuroprótesis. http://www.moregrasp.eu/

[17] https://forbes.co/2020/08/28/tecnologia/elon-musk-revela-su-nuevo-chip-para-el-cerebro/

[18] Gutiérrez Martínez, et al, *Los sistemas de interfaz cerebro-computadora: una herramienta para apoyar la rehabilitación de pacientes con discapacidad motora*, 2013, p. 66. https://www.medigraphic.com/pdfs/invdis/ir-2013/ir132c.pdf

recreativas virtuales más adaptables, que responden a los estados afectivos de la persona, y ayudan a mejorar la experiencia del juego[19].

Razón por la cual, actualmente, un gran número de empresas dedicadas al entretenimiento como Emotiv[20], al bienestar como Muse[21], y al marketing, han detectado esta oportunidad y se han sumado al auge de esta tecnología, desarrollando prototipos comerciales de BCI.

Desde grandes empresas como Nissan con su Brain-To-Vehicle[22] (B2V), Facebook con su "teclado mental"[23], Microsoft con sus nuevas patentes[24], o nuevas *startups* financiadas millonariamente como Neuralink[25] del magnate Elon Musk, o Kernel[26] de Bryan Johnson. En 2008, The Nielsen Company[27] (una empresa líder en investigación de mercado) adquirió NeuroFocus[28], una empresa especializada en neurociencias, que ha desarrollado un dispositivo BCI llamado Mynd[29], a través del cual los investigadores podrán capturar los datos sobre las respuestas subconscientes de los consumidores en tiempo real, de forma inalámbrica.

Dicho lo anterior, es menester a continuación, adentrarnos en la clasificación de dicha tecnología.

2.2. Clasificación

Los métodos de adquisición de las señales eléctricas emitidas por el cerebro son diversos, concentrándonos en el presente trabajo en el electroencefalograma o EEG, por ser la más extendida en su uso.

Por lo tanto, según la manera en la que el EEG recoge la actividad cerebral, la BCI se puede clasificar en invasiva y no invasiva.

---

[19] Nijholt, *BCI for Games: A "State of the Art" Survey,* 2008, pp. 225 y 226. https://www.researchgate.net/publication/220851341_BCI_for_games_A_'state_of_the_art'_survey

[20] Empresa desarrolladora de sistemas BCI y accesorios para los mismos. https://www.emotiv.com/

[21] Muse es un dispositivo de EEG que mide la actividad cerebral y brinda retroalimentación en tiempo real sobre el estado cerebral para ayudar a guiar la práctica de meditación. Convierte las ondas cerebrales en sonidos orientadores del clima. https://choosemuse.com/es/

[22] Bitbrain es una empresa de neurotecnología dedicada a desarrollar equipos de EEG y otras tecnologías de monitorización humana. https://www.bitbrain.com/es/blog/interfaz-cerebro-computador-automovil

[23] Un equipo de especialistas desarrolló una tecnología encargada de transmitir mediante tecnología no invasiva mensajes de texto con la mente. https://www.theverge.com/2017/4/19/15360798/facebook-brain-computer-interface-ai-ar-f8-2017

[24] https://www.theregister.com/2018/01/15/microsoft_bci_patent_application/

[25] https://neuralink.com/

[26] https://www.kernel.com/about-us

[27] https://www.nielsen.com/us/en/solutions/capabilities/consumer-cience/

[28] https://www.nielsen.com/us/en/press-releases/2011/nielsen-acquires-neurofocus/

[29] http://neuromarca.com/blog/mynd/

A) Invasiva: en este tipo de técnica, la actividad de una neurona o pequeños grupos de estas pueden ser registrados usando microelectrodos intracraneales implantados directamente en el cerebro, es decir, debajo del cráneo, para poder estar en contacto con el córtex cerebral (o corteza motora)[30].

B) No invasiva: se utilizan electrodos no invasivos para medir la actividad cerebral y traducir las señales cerebrales registradas en comandos. En estos casos, los electrodos se colocan sobre el cuero cabelludo, a diferencia de los anteriores[31].

2.3. Diseño de arquitectura

Una BCI basada en EEG no invasiva tiene una arquitectura como la que se muestra a continuación:

Fuente: https://www.bitbrain.com/es/blog/ciberseguridad-cerebro-computadora

En general, un sistema BCI se compone de varios bloques de procesado de señal que trabajan de forma consecutiva.

Sobre la cabeza de la persona o usuario del sistema se coloca el dispositivo de EEG o diadema[32] (1). Este consta de unos electrodos cuyos sensores no invasivos miden la actividad eléctrica del cerebro en las diferentes áreas donde estos estén colocados[33].

---

[30] Opisso, *Interfaces cerebro-ordenador*, p. 14. https://siidon.guttmann.com/files/interfaces_cerebro-ordenador.pdf

[31] Sirvent, et eal, *Interfaz Cerebral no Invasiva basada en Potenciales Evocados para el Control de un Brazo Robot*, 2011, p. 103. https://www.elsevier.es/es-revista-revista-iberoamericana-automatica-e-informatica-331-pdf-S1697791211700310

[32] El montaje de un sistema EEG requiere de una diadema o gorro, el cual contiene sensores integrados para medir diferencias entre las señales eléctricas (Minguez, op. cit. p. 5).

[33] Rodríguez Bermúdez, et at, *Adquisición, procesamiento y clasificación de señales EEG para el diseño de sistemas BCI basados en imaginación de movimiento*, 2013, p. 10. https://repositorio.upct.es/bitstream/handle/10317/3295/apc.pdf?sequence=1&isAllowed=y

Debido a que dicho dispositivo tiene limitaciones de *hardware* y no puede procesar los datos del EEG (2), estos se envían a un dispositivo de control cercano (3) que usualmente tiene la forma de una aplicación en un *smartphone*, tablet u ordenador[34].

Este equipo recoge la actividad cerebral, la procesa y almacena; también puede interaccionar con el usuario a través de diferentes medios, enviando directamente estímulos visuales o somatosensoriales al usuario (4'), o enviando comandos a otros dispositivos (4) como una prótesis motora.

Algunas aplicaciones envían algunos de estos datos (5) a un dispositivo de control remoto (6) que usualmente toma la forma de servidor en la nube. Estos servidores o bien realizan tareas de almacenamiento o computación masiva de datos, o bien de un procesamiento de datos que requiere otros datos que se encuentran en el servidor.

Eventualmente, estos servidores pueden enviar información (7) al dispositivo de control cercano para cambiar su funcionamiento con ese usuario.

2.4. Origen de los neuroriesgos

Las personas ceden fácilmente sus derechos de privacidad a los proveedores comerciales de servicios, a través de la navegación por Internet, y el acceso a las redes sociales o al entretenimiento, sin comprender completamente a lo que están renunciando.

En este escenario, resulta clarificadora la dirección a la que se dirige el futuro de la neurotecnología, contexto en el cual una persona podría llegar a perder su vida mental privada, como consecuencia del acceso a sus datos neurales, permitiendo de esta manera nuevas formas de explotar y manipular a las mismas por parte de *hackers*[35], empresas o incluso gobiernos, logrando realizar un espionaje mental.

En este contexto, la utilización de algoritmos que se utilizan para orientar la publicidad, calcular las primas de seguros o emparejar socios potenciales, serán considerablemente más poderosos si se basan en información neuronal.

De esta manera, los dispositivos neuronales conectados a Internet insertan la posibilidad de que individuos u organizaciones (*hackers*, corporaciones o agencias gubernamentales) rastreen o incluso manipulen la experiencia mental de un individuo.

A) <u>Riesgos de privacidad</u>

[34] https://www.bitbrain.com/es/blog/ciberseguridad-cerebro-computadora
[35] Sain, *¿Qué es un hacker? (I),* 2015, p. 2. http://revista.pensamientopenal.com.ar/doctrina/40977-es-hacker-i

Como bien se mencionó con anterioridad, este tipo de tecnología se utiliza para conocer las reacciones emocionales o cognitivas de las personas en ámbitos de marketing o publicidad. De esta manera, determinados marcadores pueden permitir conocer las emociones, preferencias o gustos de una persona en relación a cuestiones políticas, de orientación sexual, consumo, entre otras; o incluso acceder a sus capacidades cognitivas como la memoria, aprendizaje, o resolución de problemas, entre las más diversas.

En otros casos, pueden detectar comportamientos anómalos del cerebro como epilepsia, hemorragias, desórdenes del sueño[36], encefalitis, tumores[37], migrañas, o el abuso de drogas o alcohol.

Este tipo de información privada de una persona, podría ser procesada para obtener, a través de algoritmos de predicción, la probabilidad de elaboración de ciertos sentimientos o desarrollo de ciertas enfermedades. De esta manera, los datos neurales pueden ser procesados para fines diversos a los debidos, erigiéndose como un producto comercial en el cual los usuarios o consumidores no resultan conscientes de tal utilización.

En relación a ello, los *Data Brokers*, o también conocidos como vendedores de datos, son empresas dedicadas a recopilar información de los usuarios y consumidores, para así someterlas a análisis, con el objeto de crear perfiles que serán luego susceptibles de transacciones comerciales, sin el conocimiento, y por ende, sin posibilidad de consentimiento de los mismos.

En efecto, los perfiles creados contienen información que permiten trazar la historia de los usuarios y consumidores (datos personales, gustos, necesidades, carencias), posibilitando la asignación de las ventas de acuerdo a cada perfil creado.

En este aspecto, supondría una ventaja competitiva fundamental para las empresas compradoras de datos, conocer de antemano estos perfiles de los usuarios y consumidores[38].

En esta lógica, conforme avancen las capacidades de la tecnología relacionadas con el método de adquisición EEG, el procesamiento de datos masivos, y el aditamento de información de acuerdo al advenimiento de nuevas tecnologías, hará que el conocimiento neurológico de los sujetos derivado de la monitorización de ondas cerebrales sea cada vez mayor, y la cartografía funcional del cerebro cada vez más precisa, por ende, el valor de los datos ascenderá considerablemente.

---

[36]Campbell, *EEG Recording and Analysis for Sleep Research*, 2009, p. 1. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2824445/

[37]Y Ko, *EEG in Brain Tumors*, 2018. https://emedicine.medscape.com/article/1137982-overview

[38] Algunos ejemplos de esta categoría son las aseguradoras que requieren optimizar al máximo el cálculo de las primas de sus clientes, empresas interesadas en minimizar los riesgos del proceso de selección de un empleado, empresas de recursos humanos, o incluso bancos que comercializan productos como hipotecas.

B) Riesgos de seguridad

Determinados delitos, como ser el acceso ilegítimo a los sistemas informáticos[39], comenzaron a manifestarse durante la década del 70. Con la liberalización de Internet[40] de la administración gubernamental norteamericana, y, por consiguiente, su expansión global en el nuevo milenio, las formas de delito tradicionales adoptaron nuevas modalidades mediante el uso de las tecnologías emergentes[41].

En este escenario, es que el crimen organizado[42] , como así otros delitos, han trasladado una parte fundamental de su actividad al mundo digital, debido a que este medio les ha permitido ampliar el espectro de destinatarios y, por ende, llegar a un mayor número de víctimas en menor tiempo, sin necesidad de inmediación física, con el solo requisito de poseer un dispositivo conectado a la red.

Este tipo de delitos, resultan hoy día un negocio de mayor relevancia lucrativa que el tráfico de drogas o de armas[43], aumentando los mismos debido al crecimiento exponencial de los dispositivos conectados[44], como así también a la escasa seguridad que ellos poseen, y a un desconocimiento de las medidas básicas de seguridad por parte de los usuarios y consumidores[45].

En este contexto, la irrupción de las interfaces cerebro-computadoras, supone un nuevo aliciente para este negocio que tendrá, en el ámbito de los datos neurales una nueva forma de extorsión, como, asimismo, en las nuevas interfaces conectadas al cuerpo del usuario y consumidor una nueva posibilidad de dañar física y mentalmente a los mismos de forma remota.

A continuación, se indican los posibles vectores de ataque relacionados a la seguridad de las BCI:

[39] Un sistema de acceso restringido es aquel que posee alguna medida de seguridad que impide el libre ingreso, por lo que debe sortearse alguna medida de protección para acceder (Palazzi, *Los delitos informáticos en el Código Penal. Análisis de la ley 26.388*, 2009, pp. 102 y 103).

[40] Como bien explica Castells, los orígenes de Internet se remontan a ARPANET, una red de ordenadores establecida por ARPA en septiembre de 1969, fundada por el Departamento de Defense de Estados Unidos con el objeto de alcanzar la superioridad tecnológica militar sobre la Unión Soviética (*La Galaxia Internet,* 2001, pp. 23 y 24).

[41] Sain, *Delito y nuevas tecnologías: fraude, narcotráfico y lavado de dinero por Internet*, 2012, p. 7.

[42] La Oficina de las Naciones Unidas contra la Droga y el Delito define grupo criminal organizado como un grupo de tres o más personas que no fue formado de manera aleatoria y que ha existido por un período de tiempo, el cual actuando de manera premeditada comete un delito punible con, al menos, 4 años de encarcelamiento, con el fin de obtener, directa o indirectamente, un beneficio financiero o material. https://www.unodc.org/ropan/es/organized-crime.html

[43] https://cincodias.elpais.com/cincodias/2018/07/30/mercados/1532962743_016593.html

[44] https://revistasumma.com/estas-son-las-predicciones-anuales-de-la-transformacion-digital-global-segun-cisco/

[45] https://skkynet.com/iiot-security-attacks-grow-likely-users-unaware/

Fuente: https://www.bitbrain.com/es/blog/ciberseguridad-cerebro-computadora

- Ataque al *firmware*[46] de la diadema: al acceder a la diadema EEG, resulta posible la introducción de un *malware*[47] en el *firmware*, accediendo de esta manera a los datos, ya sea con fines de extorsión o venta de los mismos a terceros. Asimismo, se pueden manipular los datos enviados al dispositivo de control cercano.
- Interceptación de la comunicación: en este caso se puede lograr establecer una comunicación con las dos partes, es decir, entre la diadema EEG y el dispositivo de control cercano, sin que éstas noten que el enlace ha sido vulnerado (*MiTM*[48]).

  De este modo, el atacante puede interceptar y alterar todos los mensajes transmitidos desde la diadema. De la misma manera, se pueden conseguir identificar las credenciales de un usuario (por ingeniería social[49], *phishing*[50]) y acceder con ellas a la aplicación del sistema BCI.
- Acceso no autorizado: en el dispositivo de control cercano, el atacante podría diseñar una aplicación BCI idéntica a la original del fabricante, pero con código adicional malicioso, logrando de esta manera que la aplicación original no funcione. De este modo se podrían enviar estímulos o acciones al usuario que le causen daño sobre su cuerpo o le sustraigan información.

[46] El firmware es el programa básico que controla los circuitos electrónicos de cualquier dispositivo. https://www.xataka.com/basics/que-firmware-que-se-diferencia-drivers
[47] https://es.m8alwarebytes.com/malware/
[48] El ataque MiTM o Man in the middle (hombre en el medio) consiste en interceptar la comunicación entre 2 o más interlocutores. https://www.incibe.es/protege-tu-empresa/blog/el-ataque-del-man-middle-empresa-riesgos-y-formas-evitarlo
[49] La ingeniería social es un conjunto de técnicas que usan los cibercriminales para engañar a los usuarios para que les envíen datos confidenciales, infecten sus computadoras con malware o abran enlaces a sitios infectados. https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering
[50] Grabosky, *Electronic Crime,* 2007, p. 4.

Siguiendo este lineamiento, se podrían enviar estímulos al usuario, estudiando la respuesta cerebral no consciente del mismo, a los fines de obtener información privada como ser gustos personales, el PIN de tarjetas de crédito o débito, fechas de cumpleaños y localizaciones de residencia, todo ello a través de una aplicación maliciosa conocida como *Brain spyware*[51].

- Escucha de la comunicación: en relación a la comunicación entre los dispositivos de control, un atacante podría lograr interceptar el canal de sincronización de datos, manipulando los datos enviados al dispositivo de control remoto.

2.5. Las BCI y la protección contra la integridad sexual de NNyA[52]

Partiendo del prisma del art. 75 inc. 23 se reconoce en la categoría de NNyA un plus de vulnerabilidad sobre el cual los Estados deben garantizar la igualdad de oportunidades y de trato, como así también el pleno goce y ejercicio de los derechos reconocidos por la misma constitución y los tratados internacionales vigentes sobre derechos humanos[53].

En este contexto constitucional es que debemos encuadrar la incidencia que una de las modalidades de las BCI posee en relación a los derechos de privacidad de los menores.

En tal sentido, en el marco del entretenimiento virtual, se generan nuevas formas de vinculación[54] y encuentros intersubjetivos entre los usuarios[55].

En este reciente entorno, no podemos dejar de contemplar que las nuevas tecnologías modelan las prácticas sociales y los intercambios cotidianos, a través de las distintas pantallas. Es allí, donde se encuentran los intersticios en los cuales se entrometen los ciberdelincuentes para aproximarse a las potenciales víctimas.

De esta manera, la utilización de las BCI propicia el acceso a datos neurales de los NNyA, los cuales poseen información sensible que la misma victima puede llegar a desconocer, lo

---

[51] Martinovic *et al*., 2012, p. 3. https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final56.pdf

[52] Entiéndase: niños, niñas y adolescentes.

[53] Art 75: Corresponde al Congreso, inc. 23: "Legislar y promover medidas de acción positiva que garanticen la igualdad real de oportunidades y de trato, y el pleno goce y ejercicio de los derechos reconocidos por esta Constitución y por los tratados internacionales vigentes sobre derechos humanos, en particular respecto de los niños, las mujeres, los ancianos y las personas con discapacidad".

[54] Blanco y Brea expresan que hablar de vínculos es hablar de ligazón, de unión con otros. Los cuales se han tornado frágiles, y superficiales (Blanco y Brea, *Vínculos adolescentes atravesados por la virtualidad*, 2019, p. 1 y ss.).

[55] La informática, Internet, las telecomunicaciones y sus soportes (televisores, computadoras, dispositivos móviles de telefonía, videoconsolas, etc.) han revolucionado el campo del conocimiento y el intercambio entre los individuos. Ha de considerarse que, sin dudas, estas innovaciones poseen influencias en el entramado de las relaciones intersubjetivas, tanto intra como intergeneracionales (Lastra, Saladino y Weintraub, La construcción de la subjetividad adolescente en la era digital, 2015, p. 2). https://www.controversiasonline.org.ar/PDF/anio2015-n17/1-LASTRA-ESP.pdf

cual les permitiría a los victimarios, utilizar los mismos a los fines de manipular y corromper a los menores en determinas prácticas[56].

III. LA PROTECCIÓN DEL DATO EN ARGENTINA. BREVE ESQUEMA REGULATORIO

Desandadas las cuestiones preliminares, es oportuno señalar al dato como objeto de tutela en el ordenamiento jurídico argentino. Como así también, desde la misma senda jurídica, referirnos a las fuentes sobre las cuales nuestro país ha echado mano para proteger a los mismos.

En relación a lo antedicho es dable resaltar que la protección de datos dentro del ordenamiento jurídico fue objeto de un cambio de perspectiva con el devenir del tiempo. En un primer momento, siguiendo las ideas de Zapico, se entendía como un derecho negativo, es decir, como una defensa al derecho de la intimidad. Luego, se fue transformando - conforme las necesidades de la realidad - a un derecho positivo consistente en un derecho de autodeterminación informativo, lo cual conlleva al ejercicio del titular de su derecho a decidir qué datos personales serán objeto de tratamiento y con qué alcance[57].

Por otro lado, resulta preciso considerar que, pese a los avatares legislativos que consigna el instituto, desde un reconocimiento constitucional de las vías procesales para su reconocimiento[58], como la labor que han enmarcado la protección de los mismos[59], aún con más vigor en la actualidad, el rol de los principios deviene determinante para resolver los gravosos efectos que despliega el paso del tiempo sobre las leyes estáticas[60].

---

[56] Ello se condice con lo expresado por Lastra, Saladino y Weintraub, al entender que el mundo globalizado de hoy se mueve por el constante accionar de individuos que propagan información continua, veloz y heterogénea que se plasma en realidades virtuales. Estos movimientos desdibujan barreras geográficas, pero también las fronteras entre lo privado e íntimo, y lo público. Especialmente en las nuevas generaciones, estas tecnologías median la creación de vínculos y modalidades inéditas de encuentro (o des-encuentro) con los otros, los lenguajes y códigos de comunicación, y repercuten además en la manera de vivir y comprender la realidad. Todo ello vinculado a una suerte de "hermandad virtual" (expresión utilizadas por las autoras) en los que se confunden los mismos límites de la confianza y el conocimiento de lo que el otro puede conocer de mi sin mi consentimiento (Lastra, *op. cit*. p. 2 y ss.).

[57] Zapico, María Victoria Cita Online: ar/doc/1169/2019. Relaciones jurídicas que surgen del contrato de cloud. Las obligaciones de las partes bajo la legislación protectora de los datos personales.

[58] Art 43 inc. 3 de la Constitucional Nacional. Incluido en la reforma constitucional de 1994. Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística.

59 Fallos de la CSJN en autos "Urteaga, Facundo R. v. Estado Mayor Conjunto de las Fuerzas Armadas" con fecha 15/10/1998. 321:2767. "Ganora, Mario F. y otra" con fecha 16/09/1999. 322:2139

[60] Tal interpretación sistémica surge de la correlación de los Fundamentos de los mentores del Código Civil y Comercial Argentino; … "Estos valores y principios están muy presentes en nuestra propuesta legislativa y ausentes de manera sistemática en una gran mayoría de los códigos de otros países, lo cual le confiere una singularidad cultural remarcable". Desde otra perspectiva, es necesario que los operadores jurídicos tengan

En tal sentido la reconocida Kemelmajer de Carlucci ha sostenido que no existe una regla fija acerca de cuándo es procedente un hábeas data para "reservar", y cuándo el contenido peligroso de esa información es tan grande que corresponde borrarla. El criterio es cambiante de pueblo a pueblo, y de momento a momento. Siendo, en definitiva, la judicatura la que en última instancia será la que precise el concepto indeterminado de "información sensible"[61].

3.1. Vía Sustancial

3.1.1. *La protección de la Ley 25.326 y el proyecto de reforma 2018*

Desde la consagración constitucional del habeas data resultó necesario un encuadre legislativo de la protección del dato. En tal sentido, en el año 2000 se sancionó[62] la ley 25.326 de Protección de Datos Personales[63].

De manera sintética, la ley 25.326 establece como objeto *la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean estos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional.*

A continuación, establece que, además de las personas humanas quedan sometidas a la presente ley las personas de existencia ideal[64].

Dentro de las incorporaciones, el art. 2 de la misma ley establece a una primera categoría de datos personales en forma genérica, entendida como la *información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables*. Por otro lado, refiere a los datos sensibles, entendido como *aquellos que revelan origen racial y étnico,*

---

guías para decidir en un sistema de fuentes complejo, en el que, frecuentemente, debe recurrirse a un diálogo de fuentes, y a la utilización no sólo de reglas, sino también de principios y valores. https://www.pensamientocivil.com.ar/nuevocodcivil/Fundamentos-del-Proyecto.pdf. Tal línea hermenéutica se complementa con la disposición de los Arts. 2 del CCCN. Art. 3, 1737, y ss.

[61] SC Mendoza, 15/4/1999, "Huertas, Juan C. c. Co.De.Me.", LA LEY, 1999-F, 296; LLGran Cuyo, 1999-600. En la misma línea véase: Julián Jalil, 2017. Cuantificación del daño. Región Patagonia. Ed. La Ley. Buenos Aires. P. 26.

[62] Con fecha 04/10/2000.

[63] En palabras de Velázquez Jorge, la misma tuvo como modelo la ley española: "Ley Orgánica de Regulación del Tratamiento Automatizado de Datos" (LORTAD) (1992), reemplazada luego por la "Ley Orgánica de Protección de Datos de Carácter Personal" (1999), y los precedentes jurisprudenciales de la Corte Suprema de Justicia de la Nación, "Urteaga" que se dispuso la obligación por parte del Estado de poner a disposición de los particulares la información contenida en sus bancos de datos o archivos y "Ganora" en el cual se estableció los caracteres y límites de la obtención de información de datos personales, en bases de datos de las Fuerzas Armadas y de organismos de seguridad, poniendo en consideración los límites del art. 43, CN.

[64] Esto es contrario a lo que sostiene el Proyecto de Ley Argentina 2018, en el cual solo se contempla como sujeto a la persona humana.

opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

Dentro de estos últimos, algunos autores, incluyen a los datos genéticos[65] y los datos biométricos[66].

Asimismo, existen los datos de acceso irrestricto los cuales se encuentran contemplados en el art. 5 de la ley 25.326. Disponiéndose por regla general que el tratamiento de los personales es lícito cuando es prestado el consentimiento libre, expreso e informado y escrito o por medio equiparable. Exceptuándose tal consentimiento, entre otras situaciones, cuando los datos se obtengan de fuentes de acceso público irrestricto[67].

A su vez, nos interesa destacar que los datos son susceptibles de diversos tratamientos. Siguiendo a Corvalán podemos dividir a los tratamientos en 3 grupos; 1) Estricto o clásico. 2) Electrónico. 3) Automatizado[68].

A continuación, habiendo enunciado la clasificación del tratamiento de datos, es menester analizar brevemente los principios que imperan en la materia. Para ello, debemos considerar en primer lugar que existen principios que resultan estructurales y transversales a todo tratamiento de datos, para luego referir a dos principios que resultan propios de la última categoría de tratamiento (automatizado).

3.1.1.1. Los principios generales del tratamiento de datos[69]

A) Principio de lealtad y transparencia: se entiende que el tratamiento es leal cuando el responsable se abstiene de tratar los datos personales a través de medios engañosos o fraudulentos[70].

[65] "Son aquellos relativos a las características genéticas heredadas o adquiridas de una persona humana que proporcionen información sobre su físico o salid, obtenido mediante un análisis de muestra biológica. Tal categoría no se encuentra en la ley vigente, pero sí en el Proyecto de Ley 2018" (Corvalán, *Perfiles digitales humanos*, 2020, p. 11).

[66] "Son aquellos obtenidos a partir de un tratamiento técnico especifico, relativos a las características físicas, fisiológicas o conductuales de una persona humana, que permitan o confirmen su identidad única". Tal categoría no se encuentra en la ley vigente, pero sí en el Proyecto de Ley 2018 (Corvalán, *op. cit.*, p. 10).

[67] En el Proyecto de Ley 2018 se contempla en el art. 14 que no será necesario el consentimiento previo para el tratamiento de datos cuando se trate de listados cuyos datos se limiten a nombre y apellido, DNI, identificación tributaria o previsional, ocupación, fecha de nacimiento, domicilio y correo electrónico, ni para el tratamiento de información crediticia en los términos del art. 6 (principio de finalidad de los datos personales), debiendo ser explícitos y legítimos. https://www.argentina.gob.ar/sites/default/files/proyecto_de_ley_de_proteccion_de_los_datos_personales.pdf

[68] Se relaciona con la utilización de IA, como puede ser el *Machine Learning* y el *Deep Learning,* los cuales se constituyen como subconjuntos de analítica avanzada, las cuales resulta más amplias aún que la misma inteligencia artificial en lo referente a las capacidades analíticas (Remolina, *Fintech, Regtech y Legaltech: Fundamentos y desafíos regulatorios*, 2020, p. 83).

[69] Hemos seguido la estructura que propone el Proyecto de Ley 2018.

[70] Art. 5 del Proyecto 2018.

B) Principio de finalidad: refiere a que los datos personales deben ser recogidos con fines determinados, explícitos y legítimos, y no deben ser tratados de manera incompatible con dichos fines[71].

C) Principio de exactitud: los datos deben ser tratados de modo que sean exactos y completos.

3.1.1.2. Los Principios específicos del tratamiento automatizado[72]

A) Principio de minimización de datos: esto significa que deben ser tratados de manera que sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para lo que fueron recolectados[73].

B) Principio de no maximización: el principio anterior tiene por complemento al principio de no maximización, con la excepción de que sean fruto de un consentimiento expreso y especifico y de total disponibilidad.

C) Principio de disponibilidad total: en este aspecto, cuando de tratamientos de datos automatizados referimos, se debe tener en cuenta que ante el perfilamiento que se haga de una persona en razón de una extracción masiva de datos y metadatos, que quien realice tal tratamiento debe brindar la información del procedimiento, fases de tratamiento. Es decir, se debe disponer por aquella persona sobre la cual se tratan los datos una serie de información sobre el tratamiento que de aquellos se realiza (vg. métodos, tipo de tratamiento, técnicas de IA, finalidades, etc.)[74].

D) Principio de confidencialidad y seguridad: la base de tal principio reside en que, si una persona brinda el consentimiento para que se realice un determinado tratamiento con sus datos, le sea garantizado que no serán sometidos a otro tratamiento. Lo que, a su vez, se complementa con el acceso a los datos reservados, los cuales deberán ser utilizados por personas autorizadas y extremando todas las medidas de seguridad pertinentes[75].

---

[71] Así se entiende del art. 4. 1 y 4.7 de la ley 25.326. Art 6 del Proyecto 2018.
[72] En este punto seguimos las ideas de Corvalán *op. cit*. p. 104 y 105.
[73] Art. 7 de Proyecto 2018.
[74] Corvalán, *op. cit.,* p. 104.
[75] En tal sentido, el art. 19 del Proyecto 2018 expresa que: "el encargado debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, perdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del

3.1.2. Protección del Código Penal

En el Código Penal Argentino[76], en estricta vinculación con los datos, poseemos un capítulo sobre violación de secretos y de la privacidad, estafas u otras defraudaciones y daños. A continuación, se enunciarán aquellos artículos incluidos en dichos capítulos que guarden relación con los intereses jurídicos que son objeto de tutela en el presente trabajo.

En el art. 153, el mismo vinculado a la protección constitucional del secreto y la confidencialidad de las comunicaciones, tutela como bien jurídico a la privacidad, y protege la apertura, acceso, apoderamiento, supresión, desvío, interceptación y captación de una comunicación electrónica o despacho de otra naturaleza que no le esté dirigida al autor[77].

Asimismo, se reprime al que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido.

Siguiendo esta línea, se ve agravada la pena, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica.

En el art. 153 bis, también vinculado a los mismos bienes jurídicos (confidencialidad y privacidad), se tipifica el acceso sin autorización o excediendo la que se posea y por cualquier medio a un sistema o dato informático de acceso restringido[78].

A continuación, el Código Penal en su art. 155, multa al quien, hallándose en posesión de una correspondencia, una comunicación electrónica, despacho telegráfico, telefónico o de otra naturaleza *no destinado a la publicidad,* lo difunda o lo haga publicar indebidamente, si el hecho causare perjuicios a terceros. Eximiéndose de responsabilidad penal al que hubiere obrado con el propósito inequívoco de proteger un interés público [79].

Asimismo, se contempla en el art. 156 la sanción de pena de multa e inhabilitación especial al sujeto que, teniendo noticia, por razón de su estado, oficio, empleo, profesión o arte, de un secreto cuya divulgación pueda causar daño, lo revelare sin justa causa[80].

A su vez, se sanciona en el art. 157 bis con pena de prisión a quien: 1) a sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de

---

medio técnico utilizado. Por su parte el Art. 21 del Proyecto 2018, dispone que el responsable del tratamiento, el encargado y las demás personas que intervengan en cualquier fase de tratamiento de datos están obligados a su confidencialidad respecto de los datos personales. Subsistiendo la misma incluso luego de finalizada la relación.

[76] Fue incorporado por el art. 3 de la ley 26.388 del año 2008.

[77] Gutiérrez, Radesca y Riquert, *Violación de Secretos y de la Privacidad,* 2013, p. 1. http://www.pensamientopenal.com.ar/cpcomentado/37762-art-153-violacion-secretos-y-privacidad

[78] Riquert (dir.), *Sistema Penal e Informática, T. I,* 2019, p. 140.

[79] Riquert, *op. cit.* p. 141.

[80] Art. 156 del CPA. El bien jurídico es la intimidad. Así, expresa Muñoz Conde que la intimidad de una persona es en tiempos posmodernos el bien jurídico más vulnerable. El derecho a la intimidad, se configura como uno de los derechos de la personalidad más sutiles y más difíciles de delimitar y proteger por el derecho penal (Muñoz Conde, *Derecho Penal, Parte Especial*, 1996, p. 216).

cualquier forma, a un banco de datos personales; 2. ilegítimamente proporcionare o revelare a otra información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley; 3. ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales[81].

De igual forma, el mismo cuerpo legal contempla en el art. 173 inciso 6 la sanción a la estafa o fraude informático, en lo especifico, en referencia a la posibilidad de defraudación mediante cualquier técnica de manipulación informática, ya sea que, altere el funcionamiento de un sistema informático o bien la transmisión de datos[82].

De la misma manera, el art. 183 del mismo cuerpo normativo establece en su segundo párrafo la penalización de aquel sujeto que altere, destruya o inutilice datos, documentos, programas o sistemas informáticos, o, asimismo, venda, distribuya o haga circular o introducir en un sistema informático, cualquier programa destinado a causar daños[83].

3.2. Vía Procesal

3.2.1. Habeas Data

En forma resumida, el "hábeas data" se ha constituido como la herramienta procesal permite hacer efectivo un conjunto de derechos referidos a datos personales contenidos en registros operados o en poder de terceros.

En virtud de ello, la doctrina y jurisprudencia ha sido conteste en que los objetivos del hábeas data son cinco: a) acceder a la información; b) actualizarla; c) rectificarla; d) asegurar su confidencialidad y e) suprimir la información sensible (intimidad, ideas políticas, religiosas, etc.)[84].

A los fines de circunscribir el tema, se da introducción por la vía civil al hábeas data como un medio constitucional útil para la protección de todos los derechos y garantías establecidos por la Constitución, tratados y leyes -no solo al derecho a la intimidad- cuando resultan violados por *vía informática*"[85].

De esta manera, se ha llegado a entender que lo dispuesto por el art. 43, párr. 3°, de la Constitución Nacional establece una subespecie de amparo, conocido en el derecho

[81] Art. 157 bis. Del CPA. Buompadre sostiene que estos delitos protegen la intimidad personal, entendida como espacio de reserva de los individuos necesario para el desarrollo de la personalidad y que el Estado debe preservar de toda intromisión ilícita por parte de personas no autorizadas (Buompadre, *Manual de Derecho Penal. Parte Especial*, 2013, p. 379).
[82] Riquert, *op. cit*., p. 146.
[83] Riquert, *op. cit*., p. 148.
[84] Altmark y Molina Quiroga, *Tratado de Derecho Informático,* T. II*, 2012,* p. 678.
[85] Altmark y Molina Quiroga refieren a ello con cita al fallo de la CNCiv., sala F, 6/7/1995, "B. de S., D. A. v. Sanatorio G. S.A. s/amparo", ED 165-257 por negarse la información contenida en la historia clínica requerida, en clara amenaza a la vida, la salud y la integridad personal.

comparado como hábeas data, que algunos califican como “amparo informativo” o “amparo informático”[86].

IV. CONCLUSIÓN

El desarrollo y uso de nuevas tecnologías está cambiando de manera vertiginosa el modo en que los individuos nos relacionamos, comunicamos, aprendemos o tomamos decisiones.

La vinculación existente entre la informática y las telecomunicaciones ha generado una nueva ola o revolución tecnológica: la denominada internet de las cosas. Personas, cosas, datos, lugares y procesos, se interrelacionan cada vez más intensamente. Una gran diversidad de artefactos y dispositivos conectados o conectables, con capacidad de interactuar entre sí, ya sea de forma manual o automática.

En este contexto de vertiginoso avance tecnológico, es que se han desarrollado nuevas formas alternativas de comunicación entre las personas y su entorno, como las BCI o interfaces cerebro-computadoras, las cuales, entre una de sus particularidades, es que se encuentran conectadas a internet para poder procesar la información.

Al ritmo de este tipo de avances en materia tecnológica, y de la difusión masiva de dichos progresos, emergen nuevos fenómenos delictivos y nuevas formas de comisión de delitos tradicionales adaptados a los entornos digitales, que tienen por objeto la obtención de datos e información de las potenciales víctimas.

Desde esta perspectiva, dichos cambios conllevan a tutelar nuevas necesidades sociales dignas de ser reconocidas, como, asimismo, dotar de nuevas respuestas y dinamismo a los procedimientos y métodos investigativos-probatorios, en clara observancia a la especial relevancia de la evidencia digital en dicho marco.[87]

Dichos escenarios, los cuales suponen riesgos de seguridad y privacidad, revisten una notable importancia que deberá ser considerada por la seguridad informática[88], y por regulaciones normativas adecuadas que propicien el tratamiento responsable de datos personales.

---

[86] CNCiv., sala A, 8/9/1997, “Pochini, Oscar y otro c. Organización Veraz S.A”., LA LEY, 1998 -B, 3. Cabe expresar que no compartimos la idea de que sea considerado al habeas data como un amparo stricto sensu, debido a que, como bien indican Altmark y Molina Quiroga, mientras el amparo requiere que exista “ilegalidad o arbitrariedad manifiesta”, el “hábeas data”, en cambio, tiene una finalidad muy específica, que es otorgar a toda persona un medio procesal eficaz para poder conocer y controlar la información de carácter personal que le concierna y para evitar que terceras personas hagan un uso indebido de esa información.

[87] Se entiende como evidencia digital a un tipo de evidencia física construida de campos magnéticos y pulsos eléctricos, que por sus características deben ser recolectados y analizados con herramientas y técnicas especiales (Di Lorio (dir.) *El rastro digital del delito. Aspectos técnicos, legales y estratégicos de la Informática Forense,* 2017, pp. 80 y 81).

[88] Disciplina que abarca diferentes medidas y actividades con el objetivo de proteger las infraestructuras tecnológicas y la información que se genera, procesa, transmite y se almacena en dichas infraestructuras, evitando que se comprometa su confidencialidad, autenticidad e integridad (Gómez Vieites, *Enciclopedia de la Seguridad Informática*, 2011, p. 38).

En todo este constructo de tecnologías disruptivas, y como consecuencia de lo anteriormente expuesto, asistimos a corroborar que en las neurotecnologías BCI, el dato se erige como el interés tutelar central a proteger, siempre que, la afectación del mismo se manifiesta en numerosas consecuencias dañosas.

V. BIBLIOGRAFÍA

Altmark, D. R., y Molina Quiroga, E. (2012). *Tratado de Derecho Informático* (T. II, 1era. ed.). Buenos Aires: La Ley.

Arns, M., Drinkenburg, W., and Kenemans, J. L. (2012). The Effects of QEEG-Informed Neurofeedback in ADHD: An Open-Label Pilot Study. *Applied Psychophysiology and Biofeedback, 37*(3), pp. 171-180. Recuperado de https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3419351/

Blanco, C., y Brea, N. (2019). Vínculos adolescentes atravesados por la virtualidad. *Revista Actualidad Psicológica*, pp. 1-5.

Buompadre, J. E. (2013). *Manual de Derecho Penal. Parte Especial*. Buenos Aires: Astrea.

Campbell, I. G. (2009). EEG Recording and Analysis for Sleep Research. *Current Protocols in Neuroscience,* pp. 1-21. Recuperado de https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2824445/pdf/nihms-176843.pdf

Castells, M. (2001). *La Galaxia Internet.* Madrid: Areté.

Cherñavsky, N. A., Gris Muniagurria, P. H., y Moreira, D. A. (2019). A diez años de la ley de delitos informáticos. Balance y propuestas. En Riquert, M. A. (dir.) *Sistema penal e informática (*vol. I, 1era. ed., pp. 129-156). Buenos Aires: Hammurabi.

Chul-Han, B. (2014). *En el enjambre.* Barcelona: Herder.

Corvalán, J. (2020). *Perfiles digitales humanos.* Buenos Aires: La Ley.

Di Lorio, A. H., Cistoldi, P. A., y Nuñez, L. (2017). Introducción a la Informática Forense, Criminalística e Investigación Penal. En A. H. Di Iorio (dir.). *El rastro digital del delito. Aspectos técnicos, legales y estratégicos de la Informática Forense* (1era. ed., pp. 46-82) Mar del Plata: Universidad Fasta.

Engel, J., Kuhl, D. E., Phelps, M. E., and Crandall, P. H. (1982). Comparative localization of foci in partial epilepsy by PCT and EEG. *Annals of Neurology, 12*(6), pp. 529-537. Recuperado de https://onlinelibrary.wiley.com/doi/epdf/10.1002/ana.410120605

Giménez, D. A., Arguissain, F. G., y Tabernig, C. B. (2011). Interfaz BCI-FES para Rehabilitación Neurológica: resultados preliminares. *XVIII Congreso Argentino de Bioingeniería SABI – VII Jornadas de Ingeniería Clínica*, pp. 1-10. Recuperado de http://www.sabi2011.fi.mdp.edu.ar/proceedings/SABI/Pdf/SABI2011_22.pdf

Gómez Vieites, A. (2011). Enciclopedia de la Seguridad Informática (2da. ed.). México D.F.: Alfaomega Grupo Editor.

Grabosky, P. (2007). *Electronic Crime. Prentice Hall's Masters Series in Criminology.* Pearson Prentice Hall

Gutiérrez Martínez, J., Castillo Negrete, J., Cariño Escobar, R. I., y Elías Viñas, D. (2013). Los sistemas de interfaz cerebro-computadora: una herramienta para apoyar la rehabilitación de pacientes con discapacidad motora, *Investigación en discapacidad, 2*(2), pp. 62-69. Recuperado de https://www.medigraphic.com/pdfs/invdis/ir-2013/ir132c.pdf

Gutiérrez R., Radesca, L. C., y Riquert, M. A. (2013). Violación de Secretos y de la Privacidad. *Revista Pensamiento Penal*. Recuperado de http://www.pensamientopenal.com.ar/cpcomentado/37762-art-153-violacion-secretos-y-privacidad

Habermas, J. (1997). *Ciencia y técnica como "ideología".* Madrid: Tecnos.

Harari, Y. N. (2015). *Homo Deus: Breve historia del mañana*. Madrid: Debate.

Lastra, S. A., Saladino, G., y Weintraub, E. (2015). La construcción de la subjetividad adolescente en la era digital. En *Controversias en Psicoanálisis de Niños y Adolescentes, 17*.

Martinovic, I., Davies, D., Frank, M., Perito, D., Ros, T., & Song, D. (2012). On the Feasibility of Side-Channel Attacks with Brain-Computer Interfaces. *Security'12: Proceedings of the 21st USENIX conference on Security symposium,* pp. 1-16. Recuperado de https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final56.pdf

Muñoz Conde, F. (1996). *Derecho Penal. Parte Especial*. Valencia: Tirant lo Blanch.

Nijholt, A. (2008). BCI for Games: A "State of the Art" Survey. International Conference Enternainment Computing, pp. 225-228. Recuperado de https://www.researchgate.net/publication/220851341_BCI_for_games_A_'state_of_the_art'_survey

Opisso, E. (s.f.) Interfaces cerebro-ordenador. *Institut Guttmann*, pp. 13-18. Recuperado de https://siidon.guttmann.com/files/interfaces_cerebro-ordenador.pdf

Palazzi, P. (2009). *Los delitos informáticos en el Código Penal. Análisis de la ley 26.388*. Buenos Aires: Abeledo Perrot.

Portas, C. M., Krakow, K., Allen, P., Josephs, O., Armony, J. L., and Frith, C. D. (2000). Auditory Processing across the Sleep-Wake Cycle: Simultaneous EEG and fMRI Monitoring in Humans. *Neuron, 28,* pp. 991-999. Recuperado de https://www.cell.com/neuron/fulltext/S0896-6273(00)00169-0?_returnURL=https%3A%2F%2Flinkinghub.elsevier.com%2Fretrieve%2Fpii%2FS0896627300001690%3Fshowall%3Dtrue

Roberts, R. (2019). Neurotecnologías: los desafíos de conectar el cerebro humano y computadores. *Biblioteca del Congreso Nacional de Chile. Asesoría Técnica Parlamentaria.* Recuperado de https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/27272/1/If01_Neurotecnologias_BCN_final.pdf

Rodríguez Bermúdez, G., García Laencina, P.J., Brizion, D., y Roca Dorda, J. (2013). Adquisición, procesamiento y clasificación de señales EEG para el diseño de sistemas BCI basados en imaginación de movimiento. *Centro Universitario de la Defensa (CUD), 6,* pp. 10-12. Recuperado de https://repositorio.upct.es/bitstream/handle/10317/3295/apc.pdf?sequence=1&isAllowed=y

Rosenstein, J. J., Marianetti, O. E. and Otoya Bet, R. E. (2018). Uso de VPRN en la implementación de una BCI para rehabilitación neurológica. *XX Workshop de Investigadores en Ciencias de*

la Computación (WICC 2018, Universidad Nacional del Nordeste), pp. 776-779. Recuperado de http://sedici.unlp.edu.ar/bitstream/handle/10915/67974/Documento_completo.pdf-PDFA.pdf?sequence=1&isAllowed=y

Sain, G. (2012). *Delito y nuevas tecnologías: fraude, narcotráfico y lavado de dinero por Internet*. Buenos Aires: Editores del Puerto.

Sain, G. (2015). ¿Qué es un hacker? (I). *Revista de Pensamiento Penal, 2015(4),* pp. 1-3. Recuperado de http://revista.pensamientopenal.com.ar/doctrina/40977-es-hacker-i

Sirvent, J.L., Azorín, J.M., Iáñez, E., Úbeda, A., y Fernández, E. (2011). Interfaz Cerebral no Invasiva basada en Potenciales Evocados para el Control de un Brazo Robot). *Revista Iberoamericana de Automática e Informática Industrial*, *8* (2), 103-111. Recuperado de https://www.elsevier.es/es-revista-revista-iberoamericana-automatica-e-informatica-331-pdf-S1697791211700310

Y Ko, D. (2018). EEG in Brain Tumors. *Medscape.* Recuperado de https://emedicine.medscape.com/article/1137982-overview