El cerebro conectado: ¿pueden hackear tu mente?

Tecnología

El cerebro conectado: ¿pueden hackear tu mente?

Las interfaces cerebro-computadora prometen devolver el tacto o controlar dispositivos con el pensamiento. Sin embargo, si alguien logra

interceptar sus señales, la privacidad de tu mente podría estar en riesgo

Por Fernando Bruzzoni

En 2007, Dick Cheney, entonces vicepresidente de Estados Unidos, reunió a su equipo médico con una solicitud fuera de lo común: **desactivar la capacidad de comunicación inalámbrica de su desfibrilador cardioversor implantable (DCI)**. Tras sufrir varios infartos a lo largo de su vida, Cheney dependía de este dispositivo para su supervivencia, que detecta arritmias peligrosas y las corrige mediante impulsos eléctricos para restablecer el ritmo normal. **Su temor era que terroristas pudieran hackear el desfibrilador** y utilizarlo para atentar contra su vida mediante la aplicación de descargas eléctricas mortales directamente en su corazón.

La orden de Cheney podía parecer un tanto excesiva, o hasta fruto de la paranoia. Aunque el riesgo de que un terrorista o un hacker interfiriera su DCI era teóricamente posible, en la práctica resultaba poco probable, ya que **hasta entonces no se conocían casos de hackeo de dispositivos médicos**.

En 2007, Dick Cheney mandó desactivar la función inalámbrica de su desfibrilador por temor a un hackeo

Sin embargo, Cheney no estaba del todo equivocado en desconfiar. Apenas un año después, una investigación realizada por un equipo de especialistas en seguridad informática de la Universidad de Massachusetts Amherst y la Universidad de Washington, demostró que **era posible interferir la comunicación por radiofrecuencia** que los médicos utilizaban para ajustar los parámetros de estos

dispositivos y alterar su funcionamiento a varios metros de distancia, **sin necesidad de estar en contacto físico con el paciente**.

Estudios posteriores evidenciaron aún más que tecnologías diseñadas para salvar vidas podían convertirse en blanco de ataques. En 2011, Barnaby Jack, un experto en ciberseguridad que trabajaba para McAfee, **demostró cómo hackear una bomba de insulina desde 90 metros de distancia con un equipo casero**, haciendo liberar una dosis letal sin que el paciente lo notara

.

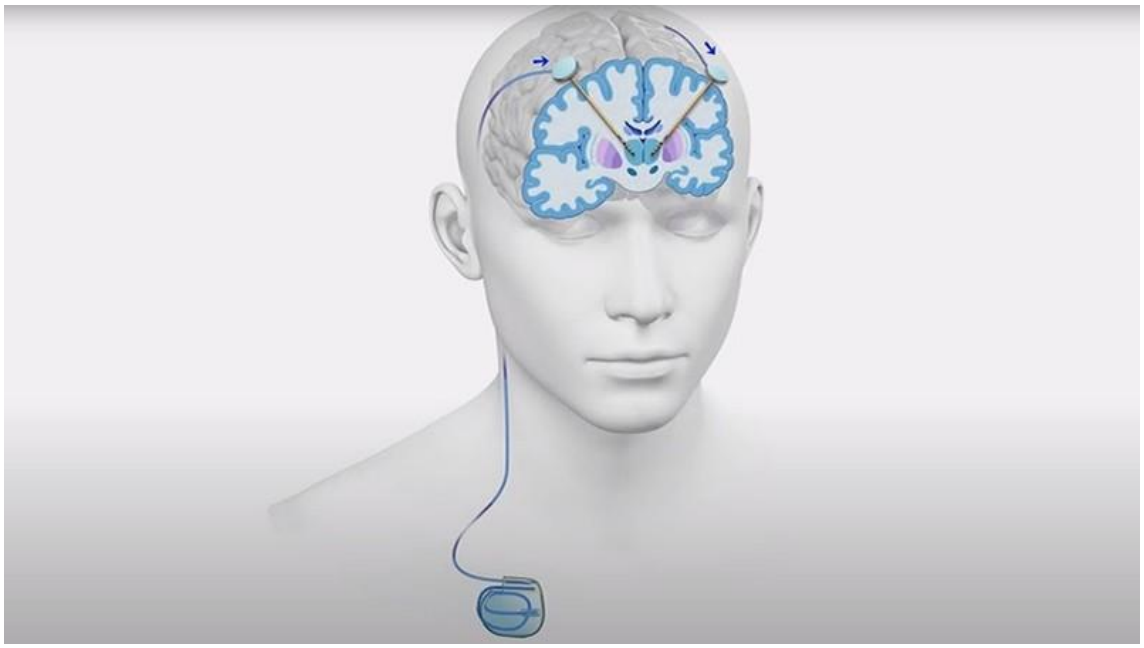
Barnaby Jack demostró que hackear dispositivos médicos es un peligro real

También desarrolló **métodos para interferir marcapasos y desfibriladores cardioversores implantables de forma remota**, interceptando las señales para apagar los dispositivos, leer su memoria o, en el caso de un DCI, provocar una descarga de hasta 830 voltios, **suficiente para matar a una persona**. Su demostración no pretendía ser un manual de instrucciones para atacantes, sino un llamado de atención para la industria médica. Estas pruebas influyeron en la Administración de Alimentos y Medicamentos de EE.UU., que **modificó las regulaciones sobre la seguridad de dispositivos médicos inalámbricos**, ya que muchos de estos aparatos salían de fábrica con poca o ninguna protección contra ataques.

Hoy, las interfaces cerebro-computadora (BCI) **llevan este riesgo a un terreno mucho más íntimo: la mente**. Recientemente, un equipo científico de la Universidad de Chicago y de la Universidad Chalmers en Suecia, logró **avances impresionantes con manos biónicas que no solo se mueven con el pensamiento**, sino que devuelven el sentido del tacto. En uno de los casos, consiguieron que un amputado perciba la presión de un huevo o la forma de una banana mediante una prótesis conectada a los nervios de su brazo. **Los sensores de la mano envían señales eléctricas que el cerebro interpreta** como si tocara algo con su propia mano.

Un participante controla una mano biónica a través de una BCI y siente los cambios de presión al mover el volante

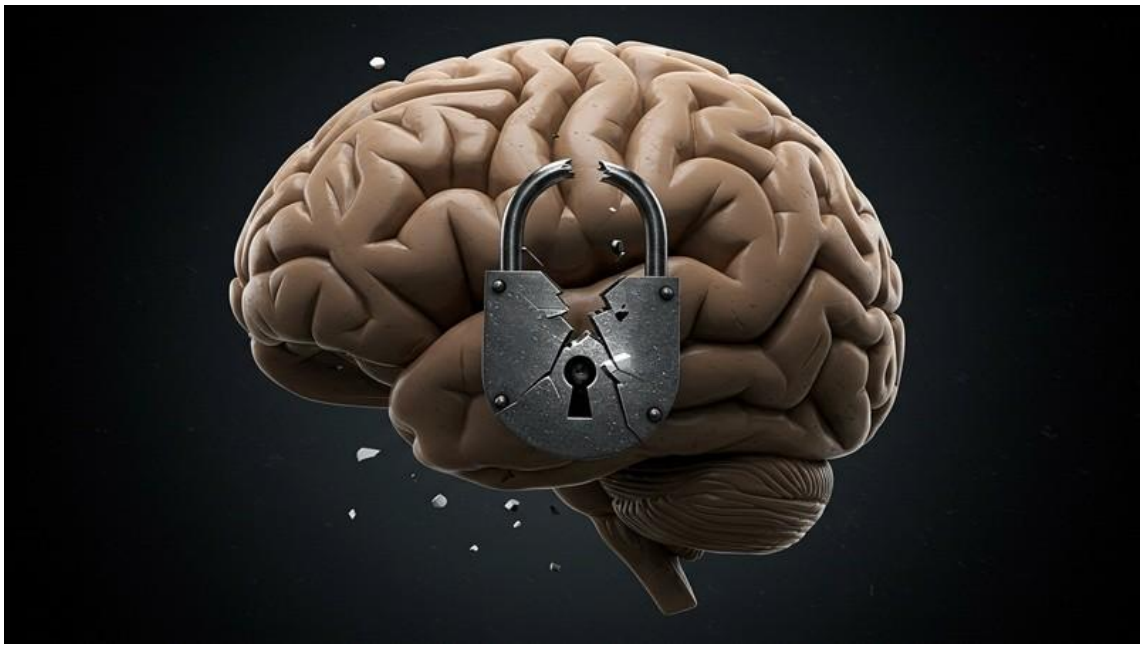
Se trata de dispositivos con capacidades bidireccionales que no solo captan la actividad neuronal, sino que también **envían señales al cerebro, "escribiendo" sensaciones directamente en la mente**. Esta proeza tecnológica y científica, que permite al cerebro sentir de nuevo, **es un triunfo para aquellos que han perdido extremidades o funciones**, pero también abre una grieta inquietante. ¿Qué impide que alguien intercepte o manipule estas señales? Un hacker podría alterarlas, haciendo que el usuario sienta dolor, reviva sus antiguos síntomas o incluso perciba un mundo que no existe, **engañando sus sentidos desde adentro**. A esto se lo llama brainjacking, el control no autorizado de implantes cerebrales, como los sistemas de estimulación cerebral profunda (DBS) utilizados para tratar el Parkinson, epilepsia y otras enfermedades neurológicas.



Un implante contra el Parkinson puede ser un blanco para el ‘brainjacking’

Lo que antes era una preocupación teórica, **hoy aparece como un riesgo real**, aunque por ahora limitado a pacientes en tratamiento. Sin embargo, en un futuro cercano, las interfaces cerebro-computadora podrían integrarse a nuestra vida diaria como hoy lo hacen los teléfonos inteligentes o las computadoras. Al menos, eso es lo que buscan los gigantes tecnológicos, que esperan que **en los próximos años dejemos atrás teclados y pantallas táctiles para adoptar algún tipo de BCI**.

No solo Meta está explorando alternativas no quirúrgicas para interpretar señales cerebrales y traducir pensamientos en acciones. **En 2022, Snap, la empresa detrás de Snapchat, compró NextMind, una pequeña pero innovadora startup francesa**. Esta compañía desarrolló una vincha que, mediante sensores en la cabeza, permite **controlar dispositivos solo con el pensamiento**: mirar un botón en una pantalla y concentrarse es suficiente para “presionarlo”. Snap integró ese equipo a su división de realidad aumentada, con la idea de que algún día podamos manejar lentes inteligentes sin mover un dedo.



La privacidad del cerebro, una barrera que el ‘brainjacking’ amenaza con romper

Ese mismo año, Apple dio un paso similar al patentar una tecnología en la que sus AirPods **utilizan electroencefalografía (EEG)** para medir la actividad eléctrica del cerebro desde el oído. En esa misma línea, en julio de 2024 OpenAI se asoció con Synchron, la startup de neurotecnología detrás del implante Stentrode, para integrar ChatGPT a su implante cerebral.

Los avances en inteligencia artificial están impulsando **descubrimientos médicos que hasta hace muy poco parecían imposibles**, como leer y escribir en nuestro cerebro como si fuera una pieza de hardware. Pero **esta fusión entre IA y BCI también nos expone al inevitable riesgo del brainjacking**, donde atacantes o empresas sin escrúpulos podrían espiar pensamientos, alterar percepciones o incluso imponer intenciones. **La mente, esa última frontera de privacidad que creíamos intocable, se acerca a un abismo peligroso**.