35JNA
JORNADA NOTARIAL ARGENTINA

Título: Protocolo Notarial — Uso de Biometría y Perfilamiento en IA – Y desafíos de los Neuroderechos

TEMA #2 Ejercicio notarial en la era digital

Coordinadores nacionales:
Santiago Francisco Oscar Scattolini
Federico Jorge Panero
Subcoordinadora:
Cecilia García Puente

Autor/a:
Andrea Fabiana Dazzi
Correo electrónico de contacto:
andrea.dazzi37@gmail.com

PONENCIA

En este contexto surge un interrogante clave para el notariado argentino ¿Cómo el notario puede liderar este debate en la Argentina? A través de la adopción de protocolos y estándares como los que se desarrollan más adelante, con capacitaciones interdisciplinarias, y estandarizaciones sociotécnicas, trabajando en la implementación de normativas. No solo debemos mitigar riesgos sino forjar una identidad digital ética y soberana. Debemos sumarnos con la fe pública a este cambio y eso nos distingue y es nuestro valor agregado

Protocolo Notarial para el Uso de Biometría y Perfilamiento mediante Inteligencia Artificial: Una Aproximación Normativa y Práctica

Se debe analizar la metamorfosis de la identidad humana en la era digital, propulsada por la huella digital, el perfilamiento algorítmico vía IA y paradigmas emergentes como el "DNI cognitivo" y los neuroderechos

En el contexto de la transformación digital de los actos jurídicos, el empleo de tecnologías biométricas y de perfilamiento algorítmico por inteligencia artificial (IA) emerge como un instrumento innovador para la identificación de personas en escrituras públicas, contratos y consentimientos.

Sin embargo, su implementación plantea desafíos significativos en materia de protección de datos personales, exigiendo un marco protocolar que equilibre la eficiencia tecnológica con el resguardo de derechos fundamentales.

El presente protocolo, diseñado para su incorporación en la actuación notarial, sintetiza una lista de riesgos y un modelo de cláusulas recomendadas

Fundamentadas en un mix entre Ley 25.326 de Protección de Datos Personales y estándares internacionales como el Reglamento General de Protección de Datos (RGPD)

Mediante este enfoque se trata no solo mitiga responsabilidades profesionales, sino que contribuye al debate ético-jurídico sobre la identidad digital, alineándose con regulaciones emergentes como el AI Act de la Unión Europea

Lista de Riesgos: Evaluación Sistemática La evaluación de riesgos constituye el eje central de este protocolo, orientada a prevenir vulnerabilidades inherentes al procesamiento de datos sensibles.

Esta checklist se encuentra estructurado y derivado de principios rectores como el consentimiento informado y la minimización de datos.

1) La base se sustenta en la ley 25.326 y estándares internacionales.

2) Coloca como uno de los ejes centrales al consentimiento informado que debe ser: a) previo, b) expreso, c) especifico y d) esencialmente revocable

3) El compareciente ha de comprender los datos recolectados, su **finalidad y duración de conservación**, conforme al art. 5 de la Ley 25.326.

4) Otro de los ejes **finalidad y proporcionalidad.** Aplicar el principio de minimización: recolectar solo lo necesario. Prohibir usos secundarios, tales como marketing, para preservar la integridad del proceso.

5) Riesgos de seguridad. Evaluar filtraciones de bases biométricas y riesgos de suplantación vía IA (ej. deepfakes), priorizando protocolos de ciberseguridad.

6) Derechos del titular, el requirente. Garantizar ejercicio de derechos ARCO (acceso, rectificación, actualización, supresión) y oposición a decisiones automatizadas (art. 10, Ley 25.326).

7) Transparencia y auditabilidad Documentar proveedores tecnológicos, mecanismos de almacenamiento y auditorías periódicas. Incluir exención de responsabilidad notarial por fallos técnicos

8) Internacionalización. Evaluar transferencias transfronterizas, asegurando niveles adecuados de protección (art. 12, Ley 25.326)

Esta checklist no solo opera como herramienta operativa, sino como instrumento pedagógico para sensibilizar a los actores involucrados en la preservación de la autonomía individual.

Cláusulas Modelo: Instrumentos para la Formalización Jurídica

Las cláusulas propuestas buscan tipificar la documentación notarial, asegurando trazabilidad y cumplimiento normativo.

Ejemplos de cláusulas:

- consentimiento Expreso Biométrico El compareciente otorga su consentimiento libre, expreso e informado para la captación y tratamiento de datos biométricos y/o conductuales (huella dactilar, reconocimiento facial, perfil de tecleo u otros), exclusivamente con la finalidad de verificar su identidad en el presente acto. Se consigna que ha sido informado sobre la finalidad, alcance, riesgos inherentes y derechos asistenciales conforme a la Ley 25.326 , en particular los de acceso, rectificación y supresión.
- Limitación de Finalidad Los datos biométricos obtenidos en este acto no podrán destinarse a finalidades distintas de la acreditación de identidad aquí prevista, ni transferirse a terceros ajenos al proceso, salvo obligación legal o mandato judicial.
- Plazo de Conservación La retención de datos biométricos se circunscribirá al plazo estrictamente necesario para la finalidad indicada, procediéndose subsiguientemente a su supresión o anonimización segura, en observancia del principio de limitación temporal (art. 4, Ley 25.326).
- Revocabilidad El otorgante podrá revocar en cualquier momento el consentimiento prestado, sin efectos retroactivos respecto de actos ya consumados.
- Exención de Responsabilidad Técnica Se declara que el notario interviniente no responde por aspectos técnicos de seguridad informática ni por vulneraciones

externas al sistema provisto por [nombre del proveedor], limitándose su intervención a la constatación jurídica del consentimiento.

- Transferencia Internacional En caso de alojamiento de datos en servidores fuera de la República Argentina, el proveedor certifica un nivel de protección equivalente al exigido por la Ley 25.326, conforme al art. 12

.

Estas cláusulas, inspiradas en el RGPD, tratan de fortalecer la robustez jurídica de los actos notariales en entornos digitales.

Identidad Digital, Perfilamiento por IA y el Desafío de los Neuroderechos

Se deben analizar elementos claves como es la evolución de la Huella Digital, que trasciende las relaciones clásicas para ahora integrar **datos biométricos** (rostro, huella dactilar, voz), y especialmente **conductuales** (patrones de tecleo, uso del mouse) y **ambientales** (señales Wi-Fi), constituyendo de este modo uno de los elementos claves para el perfilamiento predictivo.

Otro de los elementos claves es la distinción entre Identidad Funcional y Jurídica: La huella digital cumple roles identificatorios complementarios (ej., en servicios financieros), mas carece de equivalencia jurídica al DNI, dada su irreversibilidad y sensibilidad

Se debe analizar un factor clave y poco desarrollado en la doctrina notarial como es el nacimiento del "DNI Cognitivo" y Neuroderechos: Concepto teórico que abarca patrones cognitivos inferidos por IA, suscitando riesgos de manipulación y discriminación, lo que cataliza los neuroderechos para salvaguardar la privacidad mental

Existen grandes desafíos Regulatorios y Soluciones Prácticas como es la Ley 25.326 (no tan adecuada a estos tiempos pero que ayuda) y el RGPD proveen bases, complementadas por el AI Act y protocolos notariales que enfatizan consentimiento y transparencia.

En síntesis, la identidad digital conjuga avances en seguridad con amenazas a la autonomía, demandando un escrutinio regulatorio continuo.

Con la Evolución de la Huella Digital y el Perfilamiento por IA, la identidad contemporánea se erige sobre una amalgama de datos físicos y digitales, donde la huella digital amalgama con el rastro interactivo de la tecnología, procesado por IA para forjar perfiles persistentes.

La huella digital permite rescatar elementos multifacéticos para la identificación individual o de dispositivos.

La huella digital clásica, solo permite interacciones digitales como ser Cookies, direcciones IP, historial de búsqueda, metadatos, geolocalización

Pero si a esta huella digital clásica le agregamos datos biométricos, tendremos la huella digital biométrica basada en los Rasgos fisiológicos o conductuales únicos, entre ellos Huellas dactilares, reconocimiento facial, escaneo de iris, voz, ritmo cardíaco, patrones de tecleo, firma biométrica. La identificación entonces es diferente

Pero también podemos tener una huella digital de dispositivo que se basa en los datos técnicos identificatorios de hardware/software, con base en Headers, fuentes instaladas, plugins, canvas fingerprint

Y por último también existe la huella digital Ambiental (Emergente) que surge de la interacción con entornos físicos vía sensores y que detectan perturbaciones de en señales Wi-Fi para identificación sin cámaras (ej., investigación "WhoFi")

A esta huella digital en constante evolución se le debe sumar el rol del perfilamiento algorítmico, que se da en machine learning y deep learning

El perfilamiento infiere rasgos y predice conductas, habilitando aplicaciones como evaluación crediticia, vigilancia predictiva o inferencia emocional. No obstante, genera asimetrías de poder entre recolectores (corporaciones/Estados) e individuos

En la actualidad los usos de las tecnologías son claves y se encuentra Integradas en sectores como seguridad (biometría conductual en banca), marketing (publicidad dirigida), vigilancia (reconocimiento facial público) y ciberseguridad (device fingerprinting).

El notariado de ingresar al debate central que existe en la actualidad entre Huella Digital vs. Documento de Identidad

La tensión radica en si la huella biométrica equivale al DNI estatal.

En realidad existe una complementariedad funcional, no una equivalencia Jurídica

La huella opera como complemento funcional, mas requiere legislación específica para equivalencia jurídica.

El "DNI Cognitivo" genera una nueva frontera de la Identidad dado que extiende la identidad a la esfera cognitiva

Genera un perfil integral basado en patrones de pensamiento inferidos, procesos decisionales y rastros digitales persistentes

Realizando un comparativo entre el DNI Clásico y DNI Cognitivo, el clásico es de naturaliza documental y estatal pudiendo ser físico o digital en cambio el cognitivo nace de datos neurocognitivos inferidos por IA

También se diferencia en la fuente, el primero proviene del RENAPER que es un registro público y el cognitivo está integrado por biometría, huellas y neurodatos.

Otra de las diferencias a mi entender clave es que el primero, el clásico se función se agota en acreditar una civil o jurídica en cambio el cognitivo sirve para identificar, predecir y “manipular conductas” por esto último es clave la función notarial

También se diferencia en el control en el primero es estatal dado que es quien lo valida y lo expide. Y en el segundo puede en muy pocos casos ser estatal pero en principio y en la actualidad es pertenece a grandes corporaciones

El clásico es reemplazable y reversible y el cognitivo es irreversible

Si se podría decir que el DNI conductual tiene en principio una autenticación segura, permite una medicina personalizada, mitiga el fraude.-

Pero como expuse ante nos enfrentamos al riesgo de exposición mental y manipulación, como así también discriminación y control social

Desde el nacimiento de los Neuroderechos se ha tratado de conseguir un marco de protección en respuesta a amenazas neurotecnológicas

Los principales Neuroderechos Identificados son:

1. Privacidad mental.
2. Identidad psicológica.
3. Libre albedrío.
4. Acceso equitativo a neurotecnologías.

Uno de los países pioneros en el mundo que tiene normas al respecto es el país vecino de Chile que lo tiene contemplado en su constitución desde el 2021, en la misma se protege la integridad mental.

La Argentina solo cuenta con Ley 25.326, que exige como uno de sus principios el consentimiento y ARCO.

La Comunidad europea RGPD restringe perfilamiento; AI Act prohíbe categorización biométrica sensible.

Ya el TEDH en el caso “S. y Marper vs. Reino Unido (TEDH, 2008) limita almacenamiento indefinido de biométricos.

Debe existir por parte del notariado un Protocolo de Actuación Notarial para el Uso de Biometría para evitar responsabilidades.

Que nos permita obtener en las plataformas de IA una Identidad robusta, que

tengamos accesibilidad a servicios, y a los avances en neuroderechos

Pero teniendo especial cuidado y precauciones en los consentimientos invisibles, en la discriminación algorítmica, y en la exposición sensible.

Pero por fundamentalmente debemos evitar filtraciones irreversibles, suplantación (deepfakes), manipulación cognitiva y neurovigilancia.

Debemos gestionar un protocolo no solo operacionaliza la protección de datos en el ámbito notarial, sino que invite a un diálogo interdisciplinario sobre la identidad en la era IA.

Además se deberán contar con futuras actualizaciones ante evoluciones normativas

Neuroderechos en Chile: Un pionero en la Protección de la Integridad Mental y Cognitiva

Trata en el ámbito emergente del derecho humano que busca salvaguardar la esfera mental y cognitiva de los individuos frente a los avances en neurotecnologías, tales como interfaces cerebro-computadora (BCI), electroencefalogramas portátiles y algoritmos de decodificación neuronal.

Chile se erige como precursor global al incorporar explícitamente estos derechos en su ordenamiento jurídico mediante la reforma constitucional de 2021, estableciendo un estándar que trasciende la protección tradicional de datos personales para abarcar la privacidad mental, la libertad cognitiva y la integridad psíquica.

Esta iniciativa responde a la acelerada convergencia entre neurociencia, inteligencia artificial y biotecnología, que plantea riesgos como la manipulación conductual, la vigilancia neuronal y la desigualdad en el acceso a mejoras cognitivas.

La génesis de los neuroderechos en Chile se remonta al estallido social de 2019, que impulsó un proceso constituyente enfocado en derechos fundamentales. En este marco, el senador Guido Girardi presentó una moción para reconocer la protección neuronal, culminando en la promulgación de la Ley N° 21.383 el 25 de octubre de 2021. Esta norma modifica el artículo 19 N° 1 de la Constitución Política de la República, agregando un inciso final que establece:

"El desarrollo científico y tecnológico estará al servicio de las personas y se llevará a cabo con respeto a la vida y a la integridad física y psíquica. La ley regulará los requisitos, condiciones y restricciones para su utilización en las personas, debiendo resguardar especialmente la actividad cerebral, así como la información proveniente de ella."

Esta disposición constitucional impone un mandato al legislador para regular las neurotecnologías, priorizando el resguardo de la actividad cerebral y sus derivados informativos.

Se alinea con principios éticos internacionales, como la Declaración de la UNESCO sobre Bioética y Derechos Humanos (2005), pero innova al elevar la protección neuronal a rango constitucional, diferenciándose de marcos como el RGPD europeo, que no aborda explícitamente la dimensión cognitiva.

Los neuroderechos se materializan en dos pilares principales:

- Privacidad de los datos neuronales: Protege la información derivada de la actividad cerebral contra su recolección, almacenamiento o uso no consentido, considerándola sensible incluso en contextos no médicos. Esto subsume el derecho a la intimidad mental, evitando la "lectura" de pensamientos o emociones sin autorización.
- Libertad cognitiva: Salvaguarda los procesos mentales subyacentes a la conciencia, impidiendo manipulaciones que alteren la autonomía decisional o la identidad psicológica. Se distingue de la libertad de conciencia (artículo 19 N° 6) al enfocarse en el sustrato neuronal.

La implementación de la reforma ha sido gradual, complementada por normativas conexas como la Ley N° 20.584 sobre derechos en atención de salud y la Ley N° 20.120 sobre investigación científica en seres humanos.

Un hito clave fue el Proyecto de Ley sobre Protección de los Neuroderechos y la Integridad Mental. Este instrumento define neurotecnologías como "conjunto de dispositivos o instrumentos que permiten una conexión con el sistema nervioso central, para la lectura, el registro o la modificación de la actividad cerebral y de la información proveniente de ella".

Establece mecanismos como:

- Registro obligatorio ante el Instituto de Salud Pública (ISP) para usos en personas (artículo 7°).
- Consentimiento informado específico, revocable y documentado (artículos 4°-6°).

- Clasificación de datos neuronales como sensibles y reservados (artículo 11°), sujetos a la futura Ley General de Protección de Datos.
- Prohibiciones para usos que exploten vulnerabilidades (ej. en niños o grupos minoritarios) o afecten la neuroplasticidad (artículo 8°).
- Régimen de responsabilidad penal por "neurocrímenes", como manipulaciones electorales o laborales (artículo 15°).

En el ámbito judicial, el caso Emotiv (2023-2024) marca un precedente mundial. La Corte Suprema, a petición del senador Girardi, ordenó a la empresa Emotiv eliminar datos neuronales recolectados mediante su dispositivo EPOC (un electroencefalógrafo portátil) sin consentimiento adecuado, concluyendo que no califica como dispositivo médico pero vulnera la privacidad mental. El ISP evaluó el aparato en 2023, reforzando la aplicación práctica de la reforma.

En 2025, Chile consolida su liderazgo con iniciativas como la creación de un Observatorio de Neuroderechos en la Universidad de Chile y colaboraciones con la OEA para declaraciones regionales. Sin embargo, emergen retos: la proliferación de neurotecnologías accesibles con políticas de privacidad laxas, su empleo en monitoreo laboral (ej. detección de fatiga cognitiva) y el riesgo de "neuroarmas" en contextos de seguridad.

Expertos advierten sobre la necesidad de un enfoque holístico que integre ética, regulación adaptable y equidad, evitando brechas digitales que limiten el acceso a mejoras cognitivas a élites.

Podríamos decir que el estudio de la reforma de la constitución chilena de 2021 nos invita a un debate global sobre la extensión de los derechos humanos a la era neuronal. Al equilibrar innovación con protección, Chile ofrece un modelo exportable,

CONCLUSIÓN

En este contexto surge un interrogante clave para el notariado argentino ¿Cómo el notario puede liderar este debate en la Argentina? A través de la adopción de protocolos y estándares como lo propuesto, con capacitaciones interdisciplinaria, y estandarizaciones sociotécnicas, trabajando en implementación de normativas. No

solo debemos mitigar riesgos sino forjar una identidad digital ética y soberana. Debemos sumarnos con la fe pública a este cambio y eso nos distingue y es nuestro valor agregado

BIBLIOGRAFÍA

- Argentina. (2000). Ley N° 25.326 de Protección de Datos Personales. Boletín Oficial de la República Argentina. https://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm
- Unión Europea. (2016). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD). Diario Oficial de la Unión Europea, L 119/1. https://eur-lex.europa.eu/eli/reg/2016/679/oj
- Unión Europea. (2024). Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial. Diario Oficial de la Unión Europea, L/2024/1689. https://eur-lex.europa.eu/eli/reg/2024/1689/oj
- Argentina. (2001). Ley N° 25.506 de Firma Digital. Boletín Oficial de la República Argentina. http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70749/norma.htm
- Chile. (2021). Ley N° 21.383 que modifica la Constitución Política de la República en materia de desarrollo científico y tecnológico. Diario Oficial de la República de Chile. https://www.bcn.cl/leychile/navegar?idNorma=1166983
- Chile. Congreso Nacional. (2020-2025). Proyecto de Ley N° 13.828-19 sobre protección de los neuroderechos y la integridad mental. Cámara de Diputados. https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=14385&prmBOLETIN=13
- Tribunal Europeo de Derechos Humanos. (2008). S. and Marper v. United Kingdom (Solicitudes nos. 30562/04 y 30566/04). https://hudoc.echr.coe.int/eng?i=001-90051
- Cadwalladr, C., & Graham-Harrison, E. (2018, 17 de marzo). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The Guardian. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election