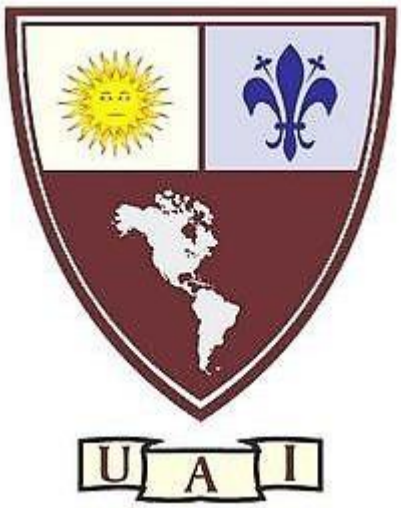



**UNIVERSIDAD ABIERTA INTERAMERICANA**

**FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS**

TRABAJO FINAL

# "UTILIZACIÓN DE LOS DATOS BIOMÉTRICOS EN LA ACTUALIDAD. REGULACIÓN, PROBLEMÁTICAS Y UNA MIRADA RESPONSABLE HACIA EL FUTURO"

**SEDE**: Castelar

**ALUMNO**: MAZZALUPO, Gustavo Fabián

**TUTOR**: MICELI, Carlos Alberto

**CARRERA**: Abogacía

**TÍTULO A OBTENER**: Abogado

**INDICE**

JUSTIFICACIÓN DE LA ELECCIÓN DEL PROBLEMA ..... 4

PROBLEMA GENERAL ..... 5

OBJETIVO GENERAL ..... 6

OBJETIVOS ESPECÍFICOS ..... 6

HIPÓTESIS ..... 7

INTRODUCCIÓN ..... 9

EN PALABRAS DE LOS MAESTROS DEL DERECHO ..... 10

CAPÍTULO I – EL PUNTO INICIAL ..... 11

SCUSA BIOMETRICA, MA TU CHI SEI? - UNA APROXIMACIÓN AL CONCEPTO DE DATOS BIOMÉTRICOS Y SU USO ..... 11

LA BIOMETRÍA SOMOS NOSOTROS MISMOS ..... 12

NUNCA TE VI EN MI VIDA – PROFUNDIZANDO SOBRE IDENTIFICACIÓN Y AUTENTICACIÓN ..... 14

CAPÍTULO II – HISTORIA Y EVOLUCIÓN ..... 15

HABÍA UNA VEZ -UN BREVE REPASO SOBRE LA HISTORIA DE LA BIOMETRÍA APLICADA ..... 15

TU DEDO ME SEÑALA – EL USO DE LA HUELLA DACTILAR ..... 15

HERSCHEL, EL LOCO DE LAS HUELLAS SUELTO EN INDIA ..... 16

DEJASTE TU HUELLA MARCADA EN MÍ ..... 17

AGÁRRAME SI PUEDES ..... 18

EL FALSO HOMBRE DE VITRUVIO – LA ANTROPOMETRÍA Y SUS INICIOS ..... 19

EL OSCURO ATAVISMO DE LOMBROSO – RIESGOS INTERPRETATIVOS DE LA ANTROPOMETRÍA ..... 20

EL RENACER DEL SUEÑO LOMBROSIANO - REFLEXIONES ..... 22

LA BIROME, VUCETICH Y EL DULCE DE LECHE – La dactiloscopía en Argentina ..... 23
SONRÍE, EL ESTADO TE AMA – Identidad y carga pública ..... 24
ESTA PLANTILLA ESTÁ HECHA A MEDIDA – El legajo de identificación 27
CAPÍTULO III – IMPORTANCIA DEL MANEJO REGULADO ..... 28
Biometría y derechos personalísimos ..... 28
SÍ, ACEPTO – La cuestión del consentimiento. Diversos supuestos y análisis del alcance ..... 31
CAPÍTULO IV – MANEJO NO REGULADO ..... 34
DAS UN POCO DE MIEDO – Riesgos potenciales en la manipulación de datos biométricos ..... 34
la ventaja que también es el problema ..... 34
CAPÍTULO V – BIOMETRÍA Y EL ÁMBITO DE LA SEGURIDAD ..... 37
NO SÉ SI USTED ES DE FIAR – Eficacia de las técnicas biométricas aplicadas ..... 37
Falsos positivos y falsos rechazos ..... 37
Reconocimiento facial ..... 38
USO APLICADO SOBRE SEGURIDAD PÚBLICA ..... 38
sistema de reconocimiento facial de prófugos ..... 39
Jurisprudencia directamente relacionada con el caso ..... 41
SOLO SE QUE NO SE NADA, PERO SÉ QUIEN ES USTED - El Sistema Federal de Identificación Biométrica para la seguridad (SIBIOS) ..... 43
CAPÍTULO VI – NORMATIVA VIGENTE ..... 46
Ley 25.326 de Protección de los Datos Personales ..... 46
Agencia de Acceso a la Información Pública ..... 50

Resoluciones complementarias de interés ..... 50
CAPÍTULO VII - PROYECTOS DE LEY ..... 52
ANÁLISIS del Mensaje 87/2023 - proyecto de "Ley de Protección de los Datos Personales" –INLEG-2023-74703583-APN-PTE (Nacional) ..... 52
Introducción ..... 52
La mitad de un vaso lleno es otra mitad vacía – Las modificaciones introducidas ..... 53
El Estado presente ..... 53
Marcando territorio ..... 54
Una cuestión de principios ..... 54
La biometría es de la partida ..... 55
Bases legales más sólidas ..... 55
Reperfilando el consentimiento ..... 57
Una pequeña luz en la oscuridad - Sector público, bases legales y limitaciones ..... 58
Estos son mis derechos, excepto que ..... 59
Creo que estoy casi seguro – El principio de seguridad ..... 60
Impacto profundo – Evaluación de impacto ..... 61
Un nuevo participante – El Delegado de Protección de Datos ..... 62
El sartén por el mango – Procedimientos y poder sancionatorio ..... 62
Expediente 1136/24-25 "marco normativo para la protección de datos biométricos utilizados por aplicaciones de telefonía celular que operan en la provincia de buenos aires" ..... 63
CAPÍTULO VIII - DERECHO COMPARADO ..... 66
Introducción ..... 66

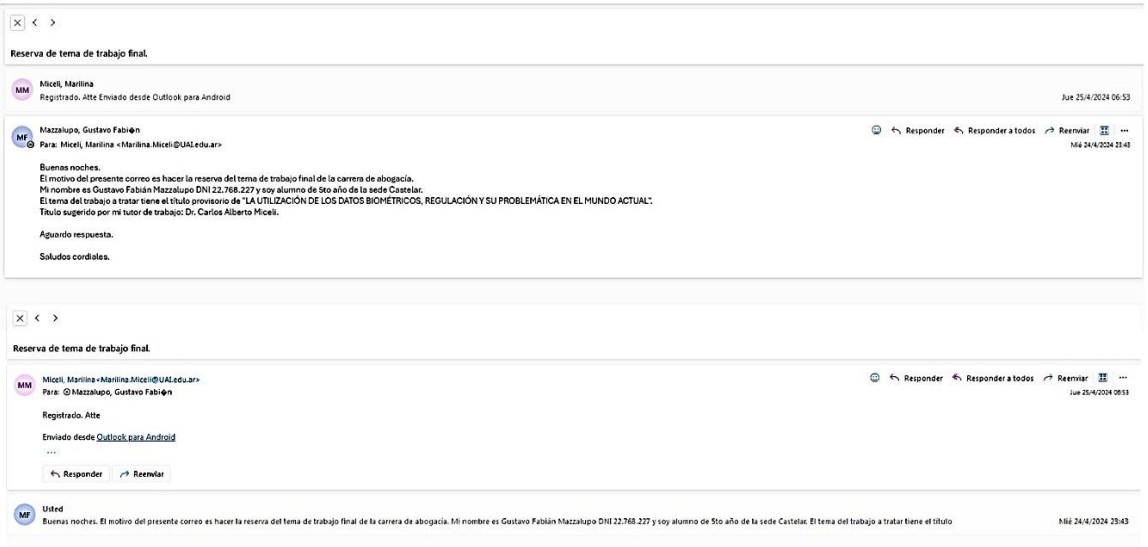
ACTA DE PRIVACIDAD DE INFORMACIÓN BIOMÉTRICA (BIPA) DE ILLINOIS ..... 66
DEFINICIONES, OBLIGACIONES Y DERECHOS QUE PLANTEA LA NORMA ..... 67
CASO DE APLICACIÓN DEL ACTA DE PRIVACIDAD DE INFORMACIÓN BIOMÉTRICA DE ILLINOIS ..... 68
UNA LEY DE DATOS PERSONALES PARA ILLINOIS ..... 69
UNIÓN EUROPEA: REGLAMENTO GENERAL DE DATOS (REGLAMENTO UE 2016/679)..... 69
ANÁLISIS DEL REGLAMENTO UE 2016/679..... 70
LA CARGA SOBRE LOS HOMBROS – INTERÉS PÚBLICO Y LA ACTUACIÓN DEL ESTADO 70
HABLEMOS DE DEFINICIONES..... 72
TIENE MI CONSENTIMIENTO, PERO ..... 74
ALGUNOS SON MÁS IGUALES QUE OTROS – CATEGORÍAS ESPECIALES DE DATOS ..... 75
DÉJEME SABER DE QUÉ SE TRATA – TRANSPARENCIA Y DATOS..... 76
¿ME LO ENVUELVE PARA LLEVAR? – PORTABILIDAD DE DATOS..... 77
A SEGURO SE LO LLEVARON PRESO – PROTECCIÓN DE LOS DATOS – SEGURIDAD DEL TRATAMIENTO ..... 78
USTED ES LA CULPABLE, DE TODAS MIS ANGUSTIAS…- RECURSOS, RESPONSABILIDAD Y SANCIONES ..... 79
CAPÍTULO IX – JURISPRUDENCIA..... 81
JURISPRUDENCIA COMPARADA ..... 81
CASO STATE OF NEW JERSEY V. FRANCISCO ARTEAGA ..... 81
CONCLUSIÓN DEL ANÁLISIS ..... 85
CAPÍTULO X - SOLUCIONES ALTERNATIVAS O ACCESORIAS – BIOMETRÍA Y OTROS CAMINOS ..... 86
NO SOY SOLO UN PEDAZO DE PLÁSTICO ..... 86

PORTUGAL PICA EN PUNTA ..... 87

REFLEXIONES ..... 88

CONCLUSIONES ..... 89

REFERENCIAS ..... 97



Reserva de tema de trabajo final.

MM Miceli, Marilina
Registrado. Atte Enviado desde Outlook para Android
Jue 25/4/2024 06:53

MF Mazzalupo, Gustavo Fabi◆n
Para: Miceli, Marilina <Marilina.Miceli@UAI.edu.ar>
Responder | Responder a todos | Reenviar
Mié 24/4/2024 21:43

Buenas noches.
El motivo del presente correo es hacer la reserva del tema de trabajo final de la carrera de abogacía.
Mi nombre es Gustavo Fabián Mazzalupo DNI 22.768.227 y soy alumno de 5to año de la sede Castelar.
El tema del trabajo a tratar tiene el título provisorio de "LA UTILIZACIÓN DE LOS DATOS BIOMÉTRICOS, REGULACIÓN Y SU PROBLEMÁTICA EN EL MUNDO ACTUAL".
Título sugerido por mi tutor de trabajo: Dr. Carlos Alberto Miceli.

Aguardo respuesta.

Saludos cordiales.



Reserva de tema de trabajo final.

MM Miceli, Marilina <Marilina.Miceli@UAI.edu.ar>
Para: Mazzalupo, Gustavo Fabi◆n
Responder | Responder a todos | Reenviar
Jue 25/4/2024 06:53

Registrado. Atte

Enviado desde Outlook para Android

...

Responder | Reenviar

MF Usted
Buenas noches. El motivo del presente correo es hacer la reserva del tema de trabajo final de la carrera de abogacía. Mi nombre es Gustavo Fabián Mazzalupo DNI 22.768.227 y soy alumno de 5to año de la sede Castelar. El tema del trabajo a tratar tiene el título
Mié 24/4/2024 21:43

**ACEPTACIÓN DE TUTORÍA**

**Autoridades de la Carrera de abogacía**

**Facultad de Derecho y Ciencias Políticas**

**Universidad Abierta Interamericana**

**S_____/_____D**

Por medio de la presente, como docente de la Facultad de Derecho y Ciencias Políticas, acepto ser el tutor del trabajo final con modalidad de discusión teórica titulado "**UTILIZACIÓN DE LOS DATOS BIOMÉTRICOS EN LA ACTUALIDAD. REGULACIÓN, PROBLEMÁTICAS Y UNA MIRADA RESPONSABLE HACIA EL FUTURO**" del alumno GUSTAVO FABIÁN MAZZALUPO para la obtención del título de ABOGADO. -

Sin otro particular, Saludo Atte.-

Profesor Miceli, Carlos

*El Ojo de Él está en todas partes, pero a algunos sitios llega más que a otros. Entendedlo, Él no puede verlo todo al mismo tiempo, todavía no. Ha conquistado todos los territorios al oeste de las Montañas de las Sombras, hasta el río, y domina los puentes. Cree que nadie podrá llegar a la Torre de la Luna sin librar una batalla en los puentes, o sin traer cantidades de embarcaciones imposibles de ocultar y que Él descubriría.*

*(Tolkien, J. R. R., 1954)*

*Las Dos Torres*

## AGRADECIMIENTOS

A mi familia y mis seres queridos, por su infinito amor, apoyo y respeto incondicional en esta travesía que, en un momento muy oscuro, empezó casi sin expectativas de base y pronto comenzó a germinar y a desarrollarse como una semilla en terreno muy fértil. Hoy día entro en razón de que comienzo a cosechar sus frutos.

A todas las genuinas muestras y gestos de afecto que recibí y recibo constantemente, de conocidos, de vecinos, de toda aquella persona que me brindó y me brinda sus más cálidas palabras de aliento, con emoción y alegría sincera.

Los planetas se alinearon de la manera más extraña, ese hecho, me puso al lado de personas increíbles, dedicadas, nobles y de gran corazón; comenzaron como mis compañeros y compañeras, hoy son mis colegas, pero, ante todo, amigos y amigas que siempre estuvieron y están; juntos remamos con fuerza y a ritmo parejo durante el camino completo, apoyándonos mutuamente, tanto en lo académico como en nuestras propias vidas, y sin quienes probablemente no hubiese alcanzado la meta.

Al plantel docente, muy especialmente a mi tutor Carlos Alberto Miceli, por su predisposición, al gran Sergio Muraca por su generosidad, al profesor Eugenio Rojas Molina, a la profesora Mirta Susana Collados por su rigurosidad bien intencionada, al profesor Pablo Dipietro, al profesor Santiago Civitico y al profesor Hernán Moyano. A la memoria del profesor Luis Forlani, de Patricia Cabral y a la de mi queridísimo y por siempre presente profe, Daniel Ernesto Novoa, por ser un ejemplo cabal de profesionalismo y calidez humana.

A mi madre, por ser un enigma tan inmenso como el amor que brinda a los otros.

A mi tía Ester, por ser una fuerza inconmensurable de la Naturaleza.

A Marcelo, por su ejemplo titánico, digno de la mitología. Por siempre.

Solo amor.

Gustavo Fabián Mazzalupo

## JUSTIFICACIÓN DE LA ELECCIÓN DEL PROBLEMA

El siguiente trabajo procura una mirada objetiva, sin demonizar ni glorificar las técnicas utilizadas en el tratamiento de los datos biométricos, manteniendo una mirada constructiva respecto de los avances y ventajas de la utilización tecnológica, y al mismo tiempo, compatibilizar la existencia de una normativa apropiada para que esta brinde todas sus ventajas y mantenga el respeto por los derechos individuales, previendo o reparando algún tipo de afectación que el uso de estas técnicas pudiera producir.

En la vida de cualquier ciudadano, una clave numérica o alfanumérica asignada por un sistema externo, como el del número de D.N.I., de la C.U.I.T. o del C.B.U. de una cuenta bancaria, etc., son todas asignadas a un sujeto desde "una fuente exterior hacia su persona"; pero el tratamiento de datos biométricos genera claves "a partir de la propia persona como fuente", con datos que le son únicos, inherentes e irrepetibles a cada individuo y por lo tanto, al no poder cambiarse, acarrea tanto potenciales beneficios como perjuicios, según sea el manejo de los mismos.

Cada ser es único en su propia individualidad, paradójicamente la misma está necesariamente constituida de múltiples características que, partiendo desde una forma primariamente fragmentada, se combinan para ensamblar esa unidad denominada persona. Comprendiendo esa totalidad e incluyendo las aristas de índole filosófica que componen nuestra humanidad, el presente trabajo toma como foco primario todo aquello que conforma la suma de particularidades orgánicas, biológicas y de comportamiento que nos pertenecen a cada uno de nosotros y que de manera irrepetible permite diferenciarnos de cualquier otro ser humano existente.

El valor del conocimiento de tales características personalísimas históricamente no ha pasado inadvertido, por lo tanto, ante la impresionante evolución de los sistemas compilatorios, de clasificación y posible uso no idóneo de las mismas por parte de interesados ajenos a la persona dueña originaria de su titularidad, resulta imprescindible la cuidadosa y efectiva tutela del individuo por parte de la ley con el fin de limitar la potencial afectación del pleno ejercicio de los derechos asociados a esas características únicas como, por ejemplo, el de la propia identidad.

El contexto es la incesante y veloz escalada de la técnica que progresivamente es aplicada al funcionamiento de muchos mecanismos de control e identificación humana, tanto en la esfera

estatal como en la privada, y cuya base es la tamización de los datos a través de motores de procesamiento y su reconversión en claves de acceso a los programas de control personal que son manejados por cada una de dichas esferas (pública y privada). Es entonces que, concentrando la atención en que su margen de acción no encuentra aún la suficiente contención para la totalidad de sus pautas de validez legal en Argentina, esto posibilita la apertura hacia el empleo poco nítido y a la manipulación dispersa de ese valioso cúmulo de información personalísima e inherente a nuestra existencia como individuos.

## PROBLEMA GENERAL

Tiene raíz en que las claves o códigos obtenidos se originan desde una fuente de titularidad que ya está asignada desde el inicio a cada ser humano, en la propia conceptualización filosófica de la persona y el ser, plasmada en principios que son base de los derechos del individuo, sus derechos personalísimos, los derechos fundamentales y en la norma; lo cual genera plantear el cuestionamiento sobre si en la actualidad, la articulación entre la ley existente y su posterior interpretación casuística, otorga un resultado que sea efectivamente capaz de dotar con la suficiente tutela a los titulares originales de esa información. ¿Qué alcance posee para custodiar adecuadamente, ante diversos supuestos, el ejercicio de control por parte de dichos titulares de derecho sobre la pertenencia de esa información que es exclusivamente inherente cada uno de ellos como individuo?

La ausencia de un enfoque integral de la problemática del uso de los datos biométricos, plasmada en la ley como un solo cuerpo normativo y que en Argentina, a través de la ley Nª25.326 de Protección de los Datos Personales[1], se encuentra desactualizada.

Se trata de la toma de efectivas acciones que permitan el ejercicio de defensa ante la potencial vulneración de estos particulares derechos, de la delimitación legal adecuada de los márgenes de uso y de la reparación o rehabilitación por el posible daño causado ante su utilización, sea esta, no consentida o de carácter ilícito.

Mientras que en el desarrollo longitudinal de este trabajo también se toman en cuenta y analizan paralelamente el destino de los proyectos de ley sobre la temática, se sostiene el

[1] LEY 25.326 de PROTECCIÓN DE LOS DATOS PERSONALES Recuperado marzo 20, 2025 de https://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm

planteo sobre la necesidad de que toda construcción, aporte o adecuación de la normativa existente sea con el criterio y amplitud suficiente para acompañar el rápido proceso evolutivo de la problemática tratada, lo cual debe inevitablemente compeler al creador de la norma a entender cabalmente que, la naturaleza de la información obtenida a través de los diversos motores de captación biométrica, tiene como fin reconvertir tecnológicamente la identidad de las personas en codificaciones para su aplicación específica a determinados fines, los cuales deben ser regulados claramente y sin ambigüedades. Esta exigencia de elaboración normativa debe además prever las futuras situaciones que necesariamente surgirán, ya que, la base de este tema está formada por la confluencia de dos características que también son de origen intrínseco a la naturaleza de los individuos: por una parte, el imperioso interés en alcanzar el conocimiento como acto de búsqueda y creación superadora, que en este caso impulsa al desarrollo científico y tecnológico, y por otra parte, la pulsión humana por la toma de control y su ejercicio en la aplicación de poder sobre los otros.

## OBJETIVO GENERAL

Establecer, dentro de las limitaciones del presente trabajo, las implicancias sociales y jurídicas derivadas de la recopilación y utilización de la información de origen biométrico, realizadas en Argentina, bajo la aplicación de los estándares tecnológicos y normativos vigentes en el país hasta el año 2024.

## OBJETIVOS ESPECÍFICOS

I. Describir las diversas metodologías de recolección, almacenamiento y utilización de la información de fuente biométrica, su evolución y estado actual.
II. Determinar la importancia del manejo regulado, controlado y seguro de la información obtenida por su relación con los derechos personalísimos de los individuos.
III. Investigar el manejo no regulado y no consentido de datos biométricos por parte de agentes públicos o privados y las consecuencias de tales acciones. Establecer los alcances sancionatorios ante tales supuestos.

IV. Analizar la aplicación de políticas de seguridad pública basadas en el uso de identificación por tecnología biométrica y la posible existencia de principios y derechos lesionados.

V. Evaluar la normativa existente en nuestro país y su extensión concreta en cuanto a la protección de datos de origen biométrico. Ver en paralelo el alcance de los proyectos de adecuación nacionales existentes.

VI. Interpretar el tipo de normativa ya aplicada en otros países y establecer puntos de coincidencia o no con las regulaciones contempladas por el marco legal vigente en Argentina.

## HIPÓTESIS

La irrupción vertiginosa de la tecnología aplicada al análisis de información de origen biométrico se contrapone con los tiempos de elaboración de las normas regulatorias en nuestro país, lo cual deja a esta última, necesariamente en una posición desventajosa para el momento en que esta entra en vigencia.

- ✓ Por lo tanto, la normativa vigente (la ley N°25.326 de Protección de los Datos Personales en Argentina), está desactualizada, abarca el contexto actual en líneas generales, pero carece de la suficiente amplitud de criterio para que el trabajo interpretativo resulte de aplicación sistemática, eficiente y directa, como un solo cuerpo normativo, ante la velocidad del proceso evolutivo de la problemática.

La desactualización conlleva una recepción insuficiente de la experiencia normativa internacional, la falta de una equiparación de estándares que alcancen la efectividad y agilidad necesaria para la resolución de posibles conflictos (la protección y trazabilidad de los datos recolectados, la tutela efectiva de los derechos y libertades individuales), que son parte de una problemática cuya naturaleza carece de las barreras geográficas tradicionales, ya que, aun cuando las regulaciones sean de aplicación en el contexto local, las implicancias las trascienden.

## RESUMEN

En el presente trabajo se intenta con las limitaciones del caso, analizar los efectos que provocan la recopilación y tratamiento de los datos biométricos de los individuos. Comienza con las definiciones conceptuales necesarias, una breve reseña de la evolución histórica de este tipo de métodos de identificación, además de su desarrollo tecnológico, alcances y fiabilidad; la importancia del manejo regulado de los mismos por su conexión con los derechos personalísimos, como contrapartida, se plantean los riesgos potenciales y concretos de los vacíos regulatorios y el mal manejo de la información. El fundamental rol del Estado en la recopilación y tratamiento de los datos, su uso en control poblacional y en su aplicación sobre seguridad pública. Se analiza el alcance de la normativa vigente en Argentina encabezada por la ley 25.326 de Protección de Datos Personales del año 2000 y se exponen sus carencias, que llevan la atención al prometedor Proyecto de Actualización de la misma, presentado en 2023. Se presenta una descripción de dos normativas pioneras como lo son el Acta de Privacidad de Información Biométrica de Illinois y el Reglamento General de Datos de la UE de 2016, ambos como marco normativo de comparación, junto con aplicaciones alternativas de éxito (caso Portugal) que se aleja de los clásicos métodos de tratamiento de los datos biométricos.

Es foco de este trabajo que la normativa debe ser lo suficientemente robusta como para articular con eficiencia la aplicación de la tecnología necesaria para el bien común con la tutela efectiva y prevalente de los derechos individuales.

# INTRODUCCIÓN

La identidad tiene una raíz de carácter filosófico que nace desde nuestro fuero interno, no solo por tomar conciencia respecto de quienes somos y darnos cuenta de nuestra propia existencia, sino también desde nuestra naturaleza como seres sociales, proyectando hacia quienes nos rodean una búsqueda de reconocimiento, validación y de pertenencia por parte de los otros, dejando en claro que somos efectivamente nosotros quienes nos presentamos ante ellos y que no se trata de cualquier otra persona.

Así entonces, desde el punto de vista de los demás, la identidad se conecta con el concepto de identificación, como proceso en el que desde sus respectivas esferas internas y a través de una pauta comparativa, nos separan del resto de las otras personas y pueden individuarnos. El siguiente desarrollo toma en principio estos últimos conceptos – la identificación a partir de la identidad y la individuación de un sujeto- y cómo estos generan el interés de terceros por la búsqueda de ese "patrón de referencia comparativa", por razones y finalidades de uso que comprenden un arco muy amplio y que son parte de la base de este trabajo.

## EN PALABRAS DE LOS MAESTROS DEL DERECHO

Este trabajo aborda desde su foco en una problemática en particular, como son los datos biométricos, la adecuación de los avances tecnológicos respecto de sus efectos sobre los individuos, lo que exige una especial atención y una articulación cuidada; en palabras del Dr. Eduardo Sirkin[2] en su disertación como parte del Ciclo "**Maestros del Derecho**"[3]: "…nos encontramos en la introducción y compatibilización de las nuevas tecnologías en todos los aspectos de la sociedad y con especial dedicación en el derecho". El Dr, Sirkin, en otro tramo de su exposición, toma conceptos del profesor e investigador de derecho informático y espacial Juan Cruz González Allonca[4], refiriéndose a uno de los muchos ejemplos que tiene la aplicación de la tecnología contrastada con los derechos individuales y plantea: "el desarrollo de las actividades de los buscadores de internet comprende dos derechos indispensables en la vida democrática moderna, el derecho a la información y el derecho a la protección de los datos personales. El éxito en su aplicación práctica depende de una equilibrada interpretación de los mismos, de forma tal, que no se imponga uno sobre el otro, sino que interactúen" y unido a esto agrega respecto de los individuos involucrados: "(…) el tratamiento de su información personal estará siempre protegido por los derechos que emanan de su dignidad, como es la protección de los datos personales, así, este derecho acompañará en forma equitativa el desarrollo tecnológico del tratamiento organizado de la información personal, otorgando mayor protección a las personas (…)" y agrega una reflexión importante dirigida al ámbito profesional: "(…) lo importante, a mi juicio, es la actualización constante del abogado, ante los desafíos de las nuevas normas que congenian con la preparación y adquisición del conocimiento".

---

[2] Dr. EDUARDO SIRKIN –
Profesor Adjunto Consulto de Derecho Procesal Civil de la Facultad de Derecho de la UBA.
Designado Profesor Honorario de la Universidad Abierta Interamericana desde noviembre 2014.
Designado Miembro Honorario de la Asociación Argentina de Derecho Procesal.
Recuperado marzo 5, 2025 de https://www.eldial.com/nuevo/pdf/suple-sirkin-c.pdf

[3] MAESTROS DEL DERECHO 17-11-2014 (Dr. Eduardo Sirkin)
Recuperado marzo 5, 2025 de https://www.youtube.com/watch?v=O6EpLIuZS78

[4] JUAN CRUZ GONZÁLEZ ALLONCA
Director Nacional de Protección de Datos Personales del Ministerio de Justicia y Derechos Humanos de la Nación. Abogado por la Facultad de Derecho de la UBA y especialista en Ingeniería de Sistemas de Información por la UTN - Recuperado marzo 5, 2025 de http://www.infojusnoticias.gov.ar/columnistas/juan-cruz-gonzalez-allonca-72.html

# CAPÍTULO I – EL PUNTO INICIAL

Con el propósito de cumplir el Objetivo I de este trabajo, en el presente y en el próximo capítulo (II), se abordarán de modo descriptivo, diversas metodologías de recolección, almacenamiento y utilización de la información de fuente biométrica, su evolución histórica y estado actual.

## SCUSA BIOMETRICA, MA TU CHI SEI?[5] - UNA APROXIMACIÓN AL CONCEPTO DE DATOS BIOMÉTRICOS Y SU USO

Como se mencionó, una parte de la justificación del presente trabajo, es el contexto de una constante y veloz evolución de la técnica que progresivamente es aplicada al funcionamiento de muchos mecanismos de control e identificación humana, tanto por parte del Estado como de actores privados, en los cuales, la base de tales sistemas es el filtrado de datos personalísimos de cada individuo a través de motores de procesamiento y su posterior reconversión en claves de acceso a programas de control personal que son manejados por cada una de dichas esferas (pública y privada). Para que quede claro desde ahora, se trata de las características únicas e inherentes a nuestra persona devenidas metafóricamente en una llave que abre distintos tipos de puertas. Demasiadas puertas.

¿Qué es lo que busca la biometría?

La aplicación de las técnicas que usan biometría busca como uno de sus objetivos, la identificación de una persona, y esto se logra contrastando los datos de ese individuo con una plantilla o conjunto de plantillas que forman una base de datos.

La otra aplicación que tiene esta técnica es determinar que la identidad de una persona es correcta, si la persona es quien dice ser, y esto se logra contrastando los datos de esa persona en particular, los cuales ya fueron registrados oportunamente en una etapa anterior. Esto es la autenticación.[6]

---

[5] Expresión en italiano: "DISCULPA BIOMETRÍA, ¿TÚ QUIÉN ERES?" – Cabe aclarar que la palabra italiana para BIOMETRÍA es BIOMETRICA (sin acento ortográfico).

[6] BIOMETRÍA PARA IDENTIFICACIÓN Y AUTENTICACIÓN. Recuperado mayo 1, 2024 de https://www.thalesgroup.com/es/countries/americas/latin-america/dis/gobierno/inspiracion/biometria

Las razones que llevan a tal aplicación encuentran su objeto en el resultado buscado, esto es, la individuación y autenticación de las personas, lo que, usando estas tecnologías, puede lograrse cada vez en menor tiempo y, en principio, con un margen de error que está por debajo de su nivel de confiabilidad.

Estas características estimularon rápidamente su adopción, y paulatinamente, fue migrando desde ámbitos que mayormente solo comprendían instalaciones de alta seguridad (como por ejemplo bóvedas de custodia de valores), hasta el actual uso cada vez más doméstico, como lo es la huella dactilar para desbloquear un celular o el escaneo facial para acceder a la cuenta de una aplicación perteneciente a una plataforma comercial de productos de venta online (por ejemplo: Mercado Libre en nuestro país o Amazon en Estados Unidos).

LA BIOMETRÍA SOMOS NOSOTROS MISMOS.

Para lograr extraer de una persona la suficiente cantidad de información, que luego sea objeto de proceso, registro clasificatorio y que, a su debido tiempo, sea utilizada como patrón de referencia comparativa y lograr la identificación de esa misma persona, se utiliza entonces la metodología denominada biometría, que consiste en captar un conjunto de patrones de medición.

¿Cuáles son estos patrones?[7] En una de sus variantes, se enfoca en diferentes aspectos únicos de índole física de un individuo, como lo es el mapeo de la estructura superficial del iris, el histórico método de toma de impresiones dactiloscópicas, la lectura de la retina ocular, la distribución de los puntos antropométricos faciales (dispersos entre los ojos, la boca, la nariz y las medidas angulares de la cara), la tecnología de registro de voz, registro de ADN, entre otros.

En otra de sus variantes, este análisis biométrico se centra en los patrones de comportamiento y de movimiento corporales. Estos últimos, que son aspectos de conducta, se miden de manera activa durante la interacción con los diversos dispositivos de captación, por ejemplo, los intervalos de velocidad al realizar una firma caligráfica, la forma particular de manipular una pantalla táctil o la postura, ritmo y marcha propios de una persona al ponerse en

[7] BIOMETRICS: DEFINITION, USE CASES, LATEST NEWS – Publicado mayo 5, 2023 – Recuperado mayo 3, 2024 de: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics

movimiento y caminar. Es importante, sin embargo, destacar que esta captación de datos que realizan los dispositivos se extiende casi de modo permanente, ya que se produce tanto en el momento en el cual se los utiliza activamente, como cuando están en reposo (captación pasiva). Así, celulares, Tablet, Smart-TV y diversos dispositivos de uso diario o frecuente registran de modo constante información biométrica conductual.

Entonces, para poner en orden y dar claridad a los dos principales grupos o tipos de identificadores utilizados por la biometría, por una parte, están los basados en medidas fisiológicas, que principalmente toman características morfológicas (la forma, la estructura) y, por otra parte, aquellos que se basan en la detección de determinados micro patrones de comportamiento o conducta dinámica de cada individuo.

Ambos tipos de mediciones conforman la totalidad de los datos biométricos que se utilizan actualmente, ya sea aplicando uno solo de ellos, en los sistemas de "modalidad única", o un conjunto de ellos, en los sistemas de "modalidad múltiple". Cabe aclarar que para algunas tendencias se prefieren los métodos morfológicos (los del primer grupo) porque tienen la ventaja de mantener determinados parámetros con una estabilidad que se extiende por un largo período de la existencia de un individuo, aun cuando deban tenerse en cuenta algunos ajustes, como los cambios físicos debidos a factores como el envejecimiento propio del rostro de la persona. La ventaja de estos parámetros físicos, a diferencia del grupo de patrones de comportamiento, es que no van a ser inmediatamente influenciados por determinadas circunstancias, como puede ser una situación de extrema tensión, angustia o enfermedad, que podría alterar el resultado de la medición del patrón conductual dinámico de un individuo debido a que un evento traumático puede modificar, aunque sea de forma temporaria, sus movimientos o acciones (por ejemplo un accidente con secuelas temporarias o permanentes en la faz motora o en el caso de manifestaciones presentes en enfermedades degenerativas en lo motriz, como la enfermedad de Parkinson), lo cual tornaría menos eficiente la posibilidad de comparación con el patrón identificatorio registrado inicialmente, y aumentaría la posibilidad de error en el reconocimiento de un individuo.

La Real Academia Española (RAE) tiene como una acepción de la palabra identificar: "Reconocer si una persona o cosa es la misma que se supone o se busca"[8]. Como ya se adelantó en este mismo capítulo, el mecanismo que maneja un sistema de identificación es en extremo básico, en principio, se obtiene el dato que corresponde al individuo en cuestión y en la segunda etapa se lo compara con un número de datos ya almacenado en un patrón de comparación. En definitiva, así se sabe quién es esa persona[9].

Para el caso del concepto de autenticación, la RAE nos lleva al verbo autentificar: "Autorizar o legalizar algo".

La autenticación[10] en ciberseguridad también es un proceso comparativo de datos de referencia, pero para confirmar que solamente un sujeto en particular (y solo ese sujeto) es quien está autorizado para acceder a recursos o ámbitos específicos. Es acreditar que efectivamente se trata de la persona autorizada a determinada acción la que solicita el permiso.

Debe quedar en claro que la identificación tiene como objetivo el reconocimiento de una persona mientras que la autenticación persigue verificar si la persona efectivamente es quien dice ser. Entendiendo que se tratan de conceptos diferentes, implican objetivos diferentes y, por lo tanto, determinadas técnicas se van a destinar para identificar, mientras que otras se usarán para autenticar al individuo.

Por lo tanto, si bien el proceso de identificación puede utilizarse por sí solo, por ejemplo, en ámbitos estatales para expedir documentación como un D.N.I. o un pasaporte, el proceso de autenticación toma ambos, primero con la identificación del individuo y, posteriormente, si este cuenta con el permiso correspondiente, al acceso que solicite, por ejemplo, el titular de una caja de seguridad en una bóveda bancaria con reserva de valores.

---

[8] IDENTIFICAR (Definición RAE) Recuperado julio 2, 2024 de: https://dle.rae.es/identificar?m=form

[9] BOULGOURIS, NIKOLAOS V., PLATANIOTIS, KONSTANTINOS N., MICHELI-TZANAKOU, EVANGELINA (2010) *Biometrics: Theory, Methods, and Applications - Chapter 3 A Comparative Survey on Biometric Identity Authentication Techniques* p 47

[10] AUTENTICACIÓN. Recuperado julio 2, 2024 de: https://www.microsoft.com/es-ar/security/business/security-101/what-is-authentication

## CAPÍTULO II – HISTORIA Y EVOLUCIÓN

### HABÍA UNA VEZ -UN BREVE REPASO SOBRE LA HISTORIA DE LA BIOMETRÍA APLICADA

En la introducción general se habló de la identidad unida al concepto de identificación y al hecho de poder ser individuados por otros. Este interés tanto propio como de terceros, que tiene su génesis en nuestra naturaleza social y la búsqueda de pertenencia, hizo que históricamente se hiciera evidente que algunas de nuestras características físicas, que nos son propias y únicas, nos diferenciaran claramente de otros. Ya sea desde la perspectiva del propio individuo como una manera de demostrar su presencia en determinado momento a través de su testimonio, pero que, tomada desde la vista de intereses ajenos, tal huella de presencia, en otro tipo de circunstancias particulares podría ser utilizada de manera desfavorable para la persona.

### TU DEDO ME SEÑALA – EL USO DE LA HUELLA DACTILAR

Como parte de la reseña histórica, es necesario ubicarse en China, bajo el dominio de la Dinastía Qin entre los años 221 a 206 a.C. en el que ya se utilizaban las impresiones palmares a modo de prueba y de la huella dactilar impresa en sellos de arcilla. Posteriormente y a lo largo de la historia, el interés que suscitó el estudio de la huella dactilar ya desde un punto de vista más científico-académico se multiplicó. En Europa hacia finales del siglo XVII, en 1687, el fisiólogo italiano Marcello Malpighi comenzó a estudiar y documentar los patrones dactilares. No fue hasta un siglo después, en 1788, en que se comenzó a reconocer la particularidad de los patrones de la huella digital a través de J. C. A. Mayer, un médico y anatomista alemán, que fue el precursor en determinar las características únicas de tales patrones. Ya en el siglo XIX, el científico inglés Sir Francis Galton (primo de Charles Darwin), centró su estudio primero en cuestiones hereditarias, y eventualmente, en las huellas dactilares.[11] Pero estos ejemplos, son de científicos que pusieron su atención en el punto de vista académico. Por el criterio del rumbo de este trabajo, es necesario poner en primer plano

[11] BARNES, J.G. (2017) HISTORIA - Capítulo 1 Página 5 *El Libro de Referencia de la Huelas Dactilares* Publicado agosto 2017 –
Recuperado julio 13, 2024 de https://nij.ojp.gov/library/publications/el-libro-de-referencia-de-las-huellas-dactilares

a una figura que se destacó primero por su curiosidad, pero sobre todo por su interés en la aplicación de una característica única y personal para la resolución de problemas prácticos: W. J. Herschel.

## HERSCHEL, EL LOCO DE LAS HUELLAS SUELTO EN INDIA

> *Le ofrezco esta antigua historia de los inicios de la toma de huellas dactilares, como modo de expresar mi cálida y continua admiración por esos magistrales desarrollos de sus aplicaciones originales, mediante los cuales, primero en Bengala y el Transvaal, y luego en Inglaterra, han creado un arma de penetrante certeza, para las necesidades más severas de Justicia.*
>
> *W. J. Herschel. Junio, 1916*

*(DEDICATORIA al Comisionado de la Policía Metropolitana Inglesa Sir Edward Henry)*[12]

Como ya se mencionó, a través de la historia moderna, varias personas se dedicaron a poner atención al particular diseño de patrones en la zona dígito-palmar humana, pero la mayoría fue por una curiosidad conectada con el interés teórico-científico. En esta parte del capítulo se desarrolla el trabajo de W.J. Herschel, quien, desde un comienzo impulsado por su propia curiosidad, llegó finalmente a encontrar una aplicación práctica para la resolución de un problema concreto, como método de identificación personal mediante huellas dactilares y palmares, el que luego continuó explorando en sus potencialidades, las cuales se adoptaron y sirvieron de base para otros sistemas identificatorios, profundizados en el área criminal. Además, como se verá a continuación, elaboró conceptos fundamentales en la materia, que son los mismos en los que actualmente se basa la técnica de biometría aplicada.

Este análisis surge por completo del libro "El origen de la huella dactilar", de su autoría, escrito en primera persona y publicado en 1916, del cual se rescatan los siguientes puntos de interés que él mismo detalla:

El libro se propone situar la génesis del método de identificación personal mediante huellas dactilares, desde su descubrimiento en Bengala en 1858, hasta su demostración pública allí en 1877-78.

[12] HERSCHEL, W. J. (1916) *The Origin of Finger-Printing*. Oxford University Press: London. Traducción realizada específicamente para este trabajo, de la obra original digitalizada en idioma inglés.

“Creo que estas páginas serán suficientes para mostrar la originalidad de mi estudio de sus dos rasgos esenciales, la estricta individualidad y la obstinada persistencia de los patrones de nuestros dedos” (Herschel, 1916).

DEJASTE TU HUELLA MARCADA EN MÍ

En julio 1858, mientras Herschel se desempeñaba como Asistente bajo la antigua Compañía de las Indias Orientales, estaba comenzando el primer tramo de carretera asfaltada y se licitó el suministro de un material que servía de aglutinante para carreteras ligeras. Un proveedor nativo llamado Rajyadhar Konai, llegó a un acuerdo con Herschel, y por indicación de este último, Konai redactó el acuerdo de su puño y letra (la forma estilada comercialmente), y en este momento Hercshel relata:

> *“Estaba a punto de firmalo de la forma habitual, en la parte de la esquina superior derecha, cuando lo detuve para leerlo yo mismo; y entonces se me ocurrió intentar un experimento tomando el sello de su mano, como forma de firmar en lugar de escribir”* (Herschel, 1916, p 8).

Su propósito era desalentar a Konai de toda idea de repudiar su firma posteriormente.

> *“La posibilidad misma de una "sanción" de ese tipo (...) para el uso de una huella dactilar no se me ocurrió hasta después de una larga experiencia, e incluso entonces, no pasó de ser una convicción personal durante muchos años más. Lo decisivo que una huella dactilar es ahora una de las ayudas más poderosas para la Justicia”* (Herschel, 1916)

Herschel aplicó un sistema de recolección y registro de huellas dactilares (que encontró más prácticas que la de toda la palma) y tuvo la constancia de aplicarlo a ciudadanos indios de todas las clases sociales, incluso hasta pedirle a amigos, conocidos y colegas que ofrecieran repetir sus huellas con períodos de separación entre 30 hasta 57 años, probando de manera empírica la persistencia de los patrones dactilares a través del tiempo.

En 1860 se lo comisionó como magistrado en una ciudad cercana a Calcuta, con altos grados de violencia, litigios y fraude, falsificación y perjurio (quebrantamiento de la fe jurada). Herschel cuenta que en la cárcel que estaba en su propia jurisdicción, se encontró un notorio convicto, que, en su propia celda, falsificaba sellos de firmas de terratenientes hechos de arcilla. Él mismo relata en su libro: “Me vi obligado a tomar huellas dactilares ahora con un objetivo definido ante mí, y durante tres años seguí tomando una gran cantidad de todo tipo

y condición de hombres". Ante la duda de si podían ser falsificadas por profesionales le presentó algunos ejemplares a los mejores artistas de Calcuta para que los imitaran. Todos fracasaron y eso bastó para disipar toda inquietud al respecto.

Posteriormente, al retornar a la India, ya como recaudador de impuestos cerca de Calcuta, le dio el control, no sólo de los tribunales penales, sino de la cárcel y del moderno Departamento de Registro de Escrituras de todo tipo y el pago de las jubilaciones y pensiones del Gobierno, implementando su sistema para identificar a quienes debían cobrarlas.

## AGÁRRAME SI PUEDES

Pero otra forma en la que utilizó el nuevo sistema para fines públicos fue en la cárcel. El recurso habitual en ese momento era contratar a un sustituto para que cumpliera una condena, pero implicaba un largo proceso de detección. La precaución que adoptó fue tomar las huellas dactilares de cada infractor al dictar sentencia de prisión, tanto en los registros del Tribunal como en la orden de arresto del carcelero.

Herschel fue un pionero, y muchos autores pasan por alto esta aplicación directamente ligada a la identificación de personas en el ámbito criminal. Como él mismo admite en su libro, todos estos procedimientos se utilizaban plenamente cuando dejó la India, en 1878.

En una carta al Inspector de Cárceles y al Registrador General de entonces, lo instó a que probaran el sistema:

> *Le adjunto un documento que parece inusual, pero que espero que tenga algún valor. Muestra un método de identificación de personas que (...) para todos los efectos prácticos, es mucho más infalible que la fotografía. Consiste en tomar una impresión similar a un sello, en tinta de sello común, de las marcas en la piel de los dedos índices de la mano derecha (...) Puedo decir que estas marcas no cambian (salvo accidentes) en el transcurso de diez o quince años tanto como para afectar la utilidad de la prueba.*
>
> *He aquí el medio de verificar la identidad de cada hombre en prisión con el hombre sentenciado por el tribunal, en cualquier momento, de día o de noche (...)* (Herschel, 1916)

Hacia fines del siglo XIX Alphonse Bertillon, siendo empleado de la Prefectura de Policía de París, comenzó a estudiar las medidas corporales de varios sujetos y reuniendo los datos obtenidos de manera sistemática, dando comienzo a la antropometría, que es el estudio de las medidas y proporciones del cuerpo humano con fines específicos de identificación.

El propio Alphonse Bertillon en 1890 expuso en su libro "*La photographie judiciaire, avec un appendice sur la classification et l'identification anthropométriques*"[13] una explicación sobre la utilización de sistematizaciones que aun hoy en día son utilizadas como argumento. Refiriéndose a las fotografías tomadas para la identificación de criminales y la enorme cantidad de registros que se lograron obtener en las principales capitales de Francia.

> *"¿Sabían que en siete años la Policía recogió más de 90.000 tarjetas de hombres adultos (sin contar el mujeres y niños), lo que representa todo el conjunto de la población criminal de París? ¿Creerían que es posible, de los cien acusados detenidos todos los días, examinar sucesivamente estas 90.000 fotografías?"* (Bertillon, 1890)

Y explicaba que tanto más imposible era analizar tal cantidad en cuanto que la mayoría de las personas con condenas penales buscaban esconderlas tomando nombres falsos. Por lo cual, presentó en el mencionado libro, el proceso de clasificación de fotografías que fue propuesto para remediarlo, y que fue adoptado por la Prefectura de Policía desde 1882.

El método antropométrico que desarrolló Bertillon tomaba la altura de la persona, la medida total de la apertura de los brazos extendidos, la circunferencia y largo de tronco, la circunferencia y largo craneal, las medidas de la oreja derecha, entre otras medidas físicas específicas y muy particulares. Además, utilizaba los datos obtenidos para ir agrupándolos y descartando por categorías.

> "*También es casi imposible encontrar dos informes antropométricos equivalentes relativos a diferentes individuos. No sólo este proceso es un instrumento clasificación, pero es suficiente para asegurar la identidad de cada persona*

[13] BERTILLON, A. (1890). *La photographie judiciaire, avec un appendice sur la classification et l'identification anthropométriques*. Paris: Gauthier-Villars et fils. Universidad de Michigan - Digitalizado: 23 Jun 2006
https://babel.hathitrust.org/cgi/pt?id=mdp.39015026761356&seq=11
Traducción realizada en este trabajo de la versión original digitalizada en francés.

*mesurada, a pesar de todos los cambios físicos que pueden ocurrir y producir en ella durante toda la vida e incluso después".* (Bertillon, 1890)

La antropometría como método de recopilación de datos corporales es un método biométrico de identificación, y se tomó como estándar aplicado sobre personas que hubieren cometido algún tipo de ilícito en casi todo el mundo desde su presentación hacia 1880 hasta pasada la primera década del siglo XX. Durante su aplicación convivió con la dactiloscopia, que seguía siendo un método efectivo y más sencillo de obtener, por lo que se agregaban las plantillas de huellas a la lista de datos de los registros antropométricos, que constaban entonces de las medidas corporales, fotografías del rostro y la plantilla con las 10 huellas dactilares.

## EL OSCURO ATAVISMO DE LOMBROSO – RIESGOS INTERPRETATIVOS DE LA ANTROPOMETRÍA

Conceptualmente en biología, el atavismo se constituye cuando ciertos rasgos de organismos antepasados reaparecen en un organismo del presente. Estos caracteres son típicos de una instancia evolutiva previa cuyo gen recesivo vuelve a expresarse en generaciones posteriores[14]. Esta concepción del origen genético de ciertas características que se repiten inexorablemente en un futuro, debido su condición atávica, fue tomado como base para el desarrollo de teorías conductuales delictivas focalizadas en la evolución humana. Entonces, el siglo XIX no solo trajo la aparición de la antropometría como método identificatorio, sino que sirvió de sustrato, junto con la teoría evolutiva de las especies de Darwin[15], para que algunas elaboraciones teóricas -que a la luz de los ojos actuales se ven al borde del absurdo

[14] PÉREZ PORTO J. - MERINO, M. Actualizado el 24 de octubre de 2017. *Atavismo - Qué es, definición y concepto*.
Recuperado septiembre 28, 2024 de https://definicion.de/atavismo/

[15] LA TEORÍA DE DARWIN SE BASA EN TRES CONCEPTOS BÁSICOS:

VARIACION GENÉTICA - Las especies evolucionan por la variación genética y de aquellos rasgos que dan ventajas adaptativas en un entorno específico.
SELECCIÓN NATURAL - Este proceso es la forma en que ciertos rasgos heredados tienen más posibilidades de ser transmitidos en las generaciones futuras debido a que favorecen la supervivencia de los individuos en un entorno particular.
ANCESTROS COMUNES - Todas las formas de vida comparten un ancestro común en algún punto de su historia evolutiva.
Recuperado marzo 04, 2025 de https://www.nationalgeographic.com.es/ciencia/tres-puntos-clave-para-entender-teoria-evolucion-darwin_21543

(aunque no para todos los ojos)- tomaran fuerza, y lograran posicionarse en ciertos círculos académicos, al menos, durante cierto período. El contexto económicamente empobrecido como efecto colateral del desarrollo industrializado, y el consecuente aumento de la criminalidad, fue el terreno fértil para la proliferación de los enfoques científicos que buscaban respuestas y soluciones ante una realidad social que golpeaba con hechos insoslayables, "*se trataba de hacer visible lo que era invisible, es decir, a través del examen riguroso del cuerpo humano se pretendía descubrir la peligrosidad del hombre*"[16].

Cesare Lombroso (1835-1909) fue un médico militar italiano que, ante esta situación brindada por la realidad, supo capitalizarla avocándose al estudio de la posible relación entre la fisiología desde lo evolutivo, la antropometría y el comportamiento criminal. Así, según la teoría elaborada por él, los caracteres atávicos que presentaban los criminales, eran la prueba fáctica de su diferenciación con el resto de la población. Estableció relaciones proporcionales utilizando el índice cefálico[17] (porcentaje de ancho a largo en un cráneo) que proponía una clasificación de acuerdo al formato craneal[18]y planteó de modo estadístico una correlación entre estos, las tasas de criminalidad y su distribución geográfica dentro del territorio italiano.[19]

> *"Sin embargo, debemos tener en cuenta que los doligocéfalos están todos agrupados en las provincias del sur, excepto Lucca, que es una excepción. Por el contrario, los braquicéfalos, excepto los Abruzos, se encuentran todos en el norte de Italia, y los ultrabraquicéfalos en sus regiones montañosas, que dan menos crímenes de sangre. En cuanto a los mesocefálicos, se distribuyen principalmente en Italia. del sur o en*

---

[16] VELÁZQUEZ DELGADO – CHRISTIANSEN (2015) - *Tras las huellas de la peligrosidad: la teoría criminológica de Cesare Lombroso en el siglo XIX* - La Razón Histórica, nº29, 2015 [231-253] ISSN 1989-2659

[17] CEPHALIC INDEX (ÍNDICE CEFÁLICO)
Recuperado marzo 2, 2025 de https://www.britannica.com/science/cephalic-index

[18] "La CLASIFICACIÓN BASADA EN LA MORFOLOGÍA CRANEAL se atribuye al profesor de anatomía Anders Retzius (1840):
Describió como **dolicocéfalos (o doligocéfalos)** a aquellos individuos con cráneo alargado y como **braquicéfalos** a aquellos con cráneos cortos". El término intermedio, **mesocéfalos**, fue introducido posteriormente.
*Brachycephalic, dolichocephalic and mesocephalic: is it appropriate to describe the face using skull patterns?* - Dental Press J. Orthod. 18 (3) - June 2013
Recuperado septiembre 18, 2024 de https://www.scielo.br/j/dpjo/a/Ysjy9xVxQJbNTQNb3wy3YkQ/?lang=en

[19] LOMBROSO, Cesare (1876) *L'uomo delinquente* - in rapporto all'antropologia, alla giurisprudenza ed alla psichiatria (cause e rimedi)- Capítulo III "Índice Cefálico" p. 48
T O R I N O FRATELLI BOCCA EDITORI - Edición de 1897

*las regiones más cálidas del norte de Italia, como Livorno, Génova".* (Lombroso, 1876, p. 48)

Defendió con vehemencia su teoría de las evidencias que ponían en duda el nivel de acierto en sus determinaciones; así lo expresó en su obra *L'uomo delinquente in rapporto all'antropologia, alla giurisprudenza ed alla psichiatria (cause e rimedi)*, que se toma como referencia para el desarrollo de este trabajo, en el apartado "atavismo y criminalidad" sostenía:

*"(...) la teoría de que el asesinato, el robo y otros delitos sean acciones normales en la vida silvestre, es demasiado simple y por tanto insuficiente para explicar todos los hechos que el estudio de los pueblos inferiores ofrece, un cierto número de los cuales están decididamente en contra de esta tesis"* y agregaba que, sin embargo, *"(...) estas objeciones no destruyen la teoría del atavismo, siempre que se transporte desde la materialidad de la acción que se denomina delito a las características psicológicas que, posiblemente ante determinados estímulos, ellos lo determinan".* (Lombroso, 1876, p. 633)

EL RENACER DEL SUEÑO LOMBROSIANO - REFLEXIONES

Esta teoría de la criminología, con sustentación científica basada en lo evolutivo, fue decayendo hacia las primeras décadas del siglo XX. Ahora bien, dado el tema de este trabajo, es interesante que resulte casi inevitable trazar un paralelismo con realidades actuales, como los sesgos con los cuales son alimentados los motores de búsqueda, captura y análisis de datos biométricos, los cuales pueden influir en las lecturas que estos hagan. El instrumento tecnológico en este caso, es adiestrado con información que le ingresan operadores humanos, y si estos se basan en indicadores que, por ejemplo, se asocian generalmente a determinadas etnias, el algoritmo va a estar entrenado para buscar esas particularidades, las que no siempre van a dar identificaciones fidedignas (en este mismo trabajo, en el capítulo XI sobre jurisprudencia comparada, se analiza el caso Francisco Arteaga contra el Estado de New Jersey[20]), lo que resulta en un verdadero "atavismo informatizado". Esto se combate con

[20] ESCUELA DE LA DEFENSA PÚBLICA – REPOSITORIO
Recuperado octubre 20, 2024 de
https://repositorio.mpd.gov.ar/jspui/bitstream/123456789/4713/1/SUPERIOR%20COURT%20OF%20NEW%20JERSEY.%20ARTEGA.pdf
TEXTO ORIGINAL DEL FALLO en idioma inglés.

reglamentaciones que obliguen a la preparación idónea y capacitación técnica, pero con conciencia social y ética de todos los intervinientes humanos en la cadena de tratamiento de los datos.

## LA BIROME, VUCETICH Y EL DULCE DE LECHE – LA DACTILOSCOPÍA EN ARGENTINA

Ivan Vucetic (1858) nació en Croacia y a los 26 años emigró hacia Argentina en búsqueda de una vida mejor. A sus 30 años, en 1888 y ya nacionalizado, ingresó al Departamento Central de Policía de La Plata, pero debido a su interés particular por las estadísticas criminales, su dedicación y su curiosidad científica, llegó a jefe de la nueva Oficina de Identificación Antropométrica, en 1891. Tomó particular interés en los desarrollos que había realizado Sir Francis Galton, pero entendió que, para poder ser aplicadas con eficiencia como una herramienta para la individualización, debían tener una metodología sistematizada, entonces, *"Trabajando con el sistema general de clasificación de tres patrones de Galton, rápidamente creó un sistema de clasificación que utilizaba subcategorías para clasificar, archivar y localizar tarjetas de huellas dactilares".*[21]Además, su método ordenaba los registros en fichas y legajos, por lo que eran fácilmente ubicables, si el sujeto ya había sido ingresado al sistema,[22]lo que convirtió a esta sistematización en el primero de uso identificatorio con fines policiales a nivel mundial. Pero, ante todo, el asumió convencido que la dactiloscopía, generaba una nueva manera de ordenar los datos sobre la identidad de la población en general, una forma de control. Como lo desarrolla Mercedes García Ferrari en *"El Bertillon Americano". Una aproximación a la trayectoria intelectual de Juan Vucetich*, la propuesta de ley de Registro General de Identificación establecía registros separados destinados para los ciudadanos, para la seguridad pública y para aquellos que ya hubiesen cometido delitos.

---

[21] HUTCHINS, L.A. (2017) *El Libro de Referencia de la Huelas Dactilares* – Sistema de Clasificación de crestas de fricción - Capítulo 5.4.1- Publicado agosto 2017.
Recuperado julio 13, 2024 de https://nij.ojp.gov/library/publications/el-libro-de-referencia-de-las-huellas-dactilares

[22] GARCÍA FERRARI, M. (2009) *"El Bertillon Americano". Una aproximación a la trayectoria intelectual de Juan Vucetich.*
Recuperado julio 15, 2024 de https://static.ides.org.ar/archivo/garcia-ferrari.pdf

La base de tal convencimiento por su sistema dactiloscópico era debida a su carácter inmutable y así lo expresaba:

> *"No es la ciencia quien ha querido que la identificación tenga un solo medio y logre una sola eficacia, sino la Naturaleza. Todo es mudable en la vida, menos el esquema digital; todo es reproducible en los congéneres, menos el dibujo papilar*"[23]

## SONRÍE, EL ESTADO TE AMA – IDENTIDAD Y CARGA PÚBLICA

A diferencia de otros países del mundo, en la República Argentina no se encuentra discutida la carga pública que significa para cada habitante del país la toma de su fotografía y de sus huellas dactilares como proceso de registro y parte de la tramitación del Documento Nacional de Identidad. Pero, ¿cómo inició todo?

En el año 1948, a instancias del primer mandato de Juan Domingo Perón como presidente de la Nación, fue creado el Registro Nacional de las Personas por ley del Congreso Nº13.482 (29 de septiembre de 1948 - Boletín Oficial, 20 de octubre de 1948)[24], con vigencia y alcance general, cuyas funciones y competencia es registrar y certificar la identidad de todas las personas de existencia visible, argentinas o no, que se hallen viviendo en el país (establecido en los artículos 1º y 2 de la ley). Cabe destacar que tal recolección de datos tenía, desde el inicio, una clara finalidad clasificatoria y de utilización ya sea por parte del Estado, con fines militares, electorales y los que fueran reglamentados y por parte de los particulares que realizaran los informes o certificados establecidos por la ley o tuvieran funciones de coordinación en los censos nacionales, tal como lo establecen los incisos b; c y d del ya citado artículo 2.

---

[23] MILANTA A. (1993) *Vucetich* – Copyright by DEI GENITRIX – 1993 ISBN (L.22399) 987-9014-00-6 (814)
Recuperado julio 21, 2024 de
https://www.google.com.ar/books/edition/Vucetich/PF55BgAAQBAJ?gbpv=1

[24] CREACION DEL REGISTRO NACIONAL DE LAS PERSONAS**.** LEY 13.482 BUENOS AIRES, 29 de septiembre de 1948 Boletín Oficial, 20 de octubre de 1948 Vigente, de alcance general Id SAIJ: LNS0001999 Recuperado julio 23, 2024 de http://www.saij.gob.ar/13482-nacional-creacion-registro-nacional-personas-lns0001999-1948-09-29/123456789-0abc-defg-g99-91000scanyel#

Esta ley, estableció desde su creación, el procedimiento que debía llevar a cabo el organismo, así en su artículo 6, indica que la identificación debe realizarse mediante fotografías, impresiones dactiloscópicas (el texto de la norma utiliza este término, por lo que estamos ante la primera mención local de recolección de datos biométricos por parte del Estado), descripción de señas físicas y datos individuales (señas personales y defectos físicos visibles – artículo 9 inciso p- lo cual es un resabio conectado a las técnicas utilizadas por el sistema antropométrico de Bertillon). Pero lo que ya deja verse es la aplicación de la carga sobre el ciudadano al expresar que este debe concurrir "para someterse a los procedimientos pertinentes". De la misma forma, la ley es muy eficiente al establecer, en su artículo 7, un calendario de actualización de los datos de identificación que ya se le exige al menor de edad hasta los ocho años incluyendo su fotografía y una impresión dactiloscópica en la libreta de identidad.

El Registro Nacional de las Personas fue creado además como único organismo de emisión de los Documentos Nacionales de Identidad (en todas sus variantes históricas desde 1948): Libreta nacional de identidad; Certificado nacional de identidad; Certificado condicional de identidad y Pasaporte.

Teniendo como primer punto el establecimiento del organismo encargado de gestionar los registros de identificación poblacional a nivel país, este desarrollo se traslada entonces, hasta la Ley de Identificación, Registro y Clasificación del Potencial Humano Nacional, que bajo el N°17.671[25], fue puesta en funciones por un decreto presidencial de 1968 "en uso de las atribuciones conferidas por el artículo 5 del Estatuto de la Revolución Argentina de 1966"[26] por parte de la dictadura cívico-militar que asumió el poder a través del golpe de Estado del 28 de junio de 1966 contra el régimen democrático del presidente Arturo Illia. El decreto surgió del ejecutivo fundamentado en que el artículo 5 del antedicho Estatuto le confería al Jefe del Estado el ejercicio de prácticamente la totalidad de las facultades que en materia de

[25] LEY DE IDENTIFICACIÓN, REGISTRO Y CLASIFICACIÓN DEL POTENCIAL HUMANO NACIONAL N°17.671 (1968)
Rescatado julio 23, 2024 de https://servicios.infoleg.gob.ar/infolegInternet/anexos/25000-29999/28130/texact.htm

[26] ESTATUTO DE LA REVOLUCIÓN ARGENTINA (1966)
Rescatado julio 23, 2024 de https://www.argentina.gob.ar/sites/default/files/acta_de_la_revolucion_argentina-1966.pdf

legislación la Constitución Nacional otorgaba (y otorga) al Congreso, incluidas las que eran privativas de cada una de las Cámaras.

Así, desde el artículo 1º, la ley 17.671, en consonancia con lo ya establecido por la ley 13.482 extendió su aplicación a todas las personas de existencia visible que se domiciliaran en territorio argentino, mientras que en su artículo 9, estableció al igual que la ley 13.482 el procedimiento que iniciaba con la apertura de un legajo de identificación que incluía fotografías del ciudadano, el registro de sus huellas dactilares, la descripción de particularidades físicas y demás datos individuales, incluido el grupo y factor de sangre. Por su parte, el artículo 10 estableció régimen de actualización de la información receptando el ya dispuesto para el Registro Nacional de las Personas, pero completándolo con una segunda y tercera etapa de la actualización de los datos de los ciudadanos a realizarse para los catorce y a los treinta años de edad respectivamente.

## ESTA PLANTILLA ESTÁ HECHA A MEDIDA – EL LEGAJO DE IDENTIFICACIÓN

Algo interesante de ley 17.671 es que definió una clasificación de los datos obtenidos, así en su artículo 22 les otorgó interés nacional y su divulgación o uso estaba limitado según el carácter que adquirieran los datos, siendo públicos si no afectaba intereses "legítimos" y si los afectaba, eran considerados de carácter reservado.

Pero un punto importante para el desarrollo de este trabajo es lo que puede definirse como una verdadera plantilla de información biométrica, es decir, la recolección de datos plasmada en un soporte que permite su proceso y lo constituye el legajo de identificación establecido por la ley 17.671 en el artículo 7, ya que una vez realizada la inscripción por el Registro Nacional de las Personas, este organismo otorga al individuo "un número fijo, exclusivo e inmutable" (es decir, la codificación numérica de la identidad de una persona) y es el encargado de que este legajo sea completado con toda información personal relevante de la vida del individuo, datos patronímicos, imagen fotográfica, registros dactilares e información mensurable recolectada ya sea por el sistema dactiloscópico o cualquier otro método aportado por la tecnología, estableciendo como lugar de almacenamiento de dichas plantillas la propia sede del Registro Nacional de las Personas.

Es notorio, visto desde una corta distancia histórica para lo que significa la existencia de un país bicentenario, que la combinación de una ley emanada desde el Congreso de la Nación al crear un registro de población y dos décadas después, un decreto redactado desde un poder ejecutivo perteneciente a una dictadura cívico-militar, constituyó una muestra acabada de la extensión para el uso del control poblacional por parte del Estado de una técnica biométrica que inicialmente fue desarrollada con la específica finalidad de la identificación y verificación de criminales reincidentes, como lo era el sistema de dactiloscopia de Juan Vucetich, para transformarla en una carga pública aplicada a todo ciudadano de la Nación; pero aún más notorio es el hecho de que una práctica de control introducida por esta combinación de leyes, haya sido sostenida posteriormente como una política de Estado que perdura hasta la actualidad, y más aún, que sirva de base y se siga alimentando de la aplicación de tecnologías cada vez más innovadoras, pero con el mismo fin de control que generó tales leyes en el siglo pasado.

# CAPÍTULO III – IMPORTANCIA DEL MANEJO REGULADO

## BIOMETRÍA Y DERECHOS PERSONALÍSIMOS

En este capítulo, se desarrollará el objetivo II del trabajo:
Determinar la importancia del manejo regulado, controlado y seguro de la información obtenida por su relación con los derechos personalísimos de los individuos.

En esta elaboración se propone a los datos biométricos como parte de los derechos personalísimos, es decir, aquellos derechos que están íntimamente unidos a la persona, que nacen con ella y no pueden separarse en toda su existencia, se encuentran estrechamente ligados a los atributos de la personalidad, son derechos subjetivos absolutos privados, de carácter extrapatrimonial, que posee toda persona por ser tal y que garantizan la tutela y protección de los bienes jurídicos inmersos en el ser humano como la vida, la integridad física, la salud, la libertad, el honor, la intimidad, etc.
Los derechos PERSONALÍSIMOS son derechos subjetivos *y* comprenden a las facultades que se ejercen sobre manifestaciones de la persona misma (vida, cuerpo, honor, intimidad, etc.), como vinculación directa que exige el respeto de los demás, también *erga omnes,* pero con objeto extrapatrimonial (Cifuentes, 1995, p. 37)
Son el medio más eficaz de la defensa de la persona en su aspecto individual, la tutela de su dignidad y su libertad. Si se presentara un conflicto entre la vida, la salud, imagen, honor o intimidad, estos prevalecen sobre algún otro bien, no se discute la necesidad primaria de preservación de los bienes personalísimos. En contraposición frente a cualquier otro derecho, los personalísimos son esenciales y constituyen el mínimo indispensable para la persona y su consideración humana, que es el sujeto de los demás derechos.
Al decir de Cifuentes:

> *"Nunca como ahora se ha hecho más imprescindible organizar un sistema de defensas, que rescaten al hombre y sus instancias personales de peligros individuales y masivos. Las avanzadas científicas y sociales ponen de relieve la imperiosa necesidad de reglamentar la tutela jurídica de los derechos personalísimos".* (Cifuentes, 1999, p. 48)

Los derechos personalísimos son derechos que no se pueden negar en nadie, corresponden a cualquier persona por el hecho mismo de serlo.

CARACTERES

Los derechos personalísimos tienen un conjunto de caracteres demostrativos de su autonomía, revela que son inconfundibles y que los apartan de los demás derechos subjetivos formando una institución que tiene perfiles propios e independientes. Es importante señalar que, si hubiera algún derecho subjetivo que tuviera estructura más o menos similar, pero que no coincidiera exactamente con los caracteres que corresponden a los personalísimos, podría admitirse que no son una variedad, sino que responden a otra institución. (Cifuentes, 1999, p 50).

En la explicación de cada uno de estos caracteres se pueden señalar las siguientes:

INNATOS. Para establecer este carácter hay que considerar el primer momento de la existencia de este derecho y es el de comenzar a ser persona. En el caso de su relación con los datos biométricos, estos son parte de nuestra fisiología desde nuestro inicio como seres.

VITALICIOS. Porque "siguen", se mantienen con la persona durante su vida y terminan con la muerte del portador de los mismos.

NECESARIOS. No pueden faltar durante la vida, aunque pueda limitarse su ejercicio, sea por autoridad pública, o por acto transitorio o limitado. Está unido al carácter de innato y vitalicio y estos tres caracteres tienen correlatividad, de modo que es dable sostener que la conjunción de los tres es privativa de los derechos personalísimos.

ESENCIALES. En el sentido de opuestos a eventuales. Los eventuales son los que en ciertos casos pueden faltar en el sujeto y vienen por circunstancias ajenas al principio de la existencia de la persona. Los personalísimos, dado que son el mínimo indispensable para el contenido de la existencia de la persona, son esenciales y no derivados ni eventuales.

DE OBJETO INTERIOR. Debido a que son manifestaciones o facetas del hombre como persona, están indisolublemente unidos a él. Como son manifestaciones idealmente captadas en la unidad compuesta del hombre, no están separados ni son exteriores sino interiores al propio sujeto, ni pueden tener por objeto una parte exterior del mundo circundante.

INHERENTES. Porque son intransmisibles en virtud de su inescindible unión con la persona. Y este carácter es la base del fundamento de su protección ante sus manejos incorrectos o desregulados.

EXTRAPATRIMONIALES. En el sentido de que no pueden ser medidos o mensurados en dinero. No asientan sobre bienes estimables o calculables pecuniariamente.

RELATIVAMENTE INDISPONIBLES. No es posible cambiar el destino del derecho en forma total y permanente. Pero sí es posible hacer algún tipo de alteración parcial y transitoria. Por oposición a relativa disponibilidad, surge que son inenajenables, inembargables, intransferibles, inejecutables por el acreedor, inexpropiables por el Estado, imprescriptibles por el correr del tiempo e irrenunciables por su titular. (Cifuentes, 1999, p 53)

ABSOLUTOS. Al igual que el derecho de propiedad y los reales en general, son oponibles erga omnes.

PRIVADOS. Ya que se ubican en el ámbito del actuar de los particulares. Aunque existen derechos subjetivos públicos, los personalísimos implican interacciones entre las personas.

AUTÓNOMOS. Surge este carácter de la combinación de todos los caracteres estudiados. El conjunto de las notas y características nos ponen frente a una figura particular, no identificable con otras.

Si se analizan estos caracteres, son perfectamente coincidentes con los aplicables al derecho de autodeterminación informativa, es decir al derecho del ejercicio de control sobre el conjunto de nuestros propios datos, y cuya información, proviene justamente de los caracteres de nuestra personalidad.

Por su parte, el Código Civil y Comercial de la Nación[27], aprobado por ley N°26.994, hace referencia expresa a los derechos personalísimos en su artículo 52, estableciendo que "*La persona humana lesionada en su intimidad personal o familiar, honra o reputación, imagen o identidad, o que de cualquier modo resulte menoscabada en su dignidad personal, puede reclamar la prevención y reparación de los daños sufridos*…". Y en lo que respecta al derecho a la imagen en el artículo 53 del mismo cuerpo normativo prescribe que "…*para captar o reproducir la imagen o la voz de una persona, de cualquier modo que se haga, es necesario su consentimiento*" excepto en los casos previstos por el propio artículo: si la persona participa en actos públicos, cuando exista un interés científico, cultural, educacional prioritario y se tomen todas las precauciones tendientes a evitar un daño innecesario y cuando se trate del ejercicio regular del derecho a informar sobre acontecimientos de interés general (siempre que no se incurra en abuso de derecho).

[27] CÓDIGO CIVIL Y COMERCIAL DE LA NACIÓN
Recuperado julio 20, 2024 de https://servicios.infoleg.gob.ar/infolegInternet/anexos/235000-239999/235975/texact.htm

Sin embargo, y en consonancia con las reglas interpretativas constitucionales, los derechos no son absolutos y existen excepciones que habilitan ciertas limitaciones o restricciones en el ejercicio.

## SÍ, ACEPTO – La cuestión del consentimiento. Diversos supuestos y análisis del alcance

Una de las cuestiones centrales que surgen en este trabajo es si los titulares de la información personal que de ellos se extrae, por medio de la técnica de captura biométrica, tienen el suficiente control sobre la misma. Este control pasa por el entendimiento fehaciente de la finalidad de dichos datos, la accesibilidad a los mismos, el conocimiento sobre el tipo de bancos en los que estos serán almacenados y los encargados de su gestión. Además, incluye la facultad de corregir posibles errores cometidos en la recolección de los mismos y la eventual eliminación de los registros si estos no se ajusten a la verdad y no puedan ser subsanados por algún motivo. El control de todos estos ítems mencionados es lo que define al derecho de autodeterminación informativa, garantizado por la Constitución Nacional como parte del tercer párrafo de su artículo 43[28]. Un concepto que va a ser relevante en el siguiente desarrollo de este capítulo y los posteriores, que, si bien está aplicado a la generalidad de los datos personales, serán siempre de particular tratamiento en este trabajo, los obtenidos por biometría. El derecho a la autodeterminación informativa permite entonces al individuo estar en cabeza de la opción sobre qué información de sí mismo va a ser compartida, recopilada y procesada por los motores biométricos, y al mismo tiempo, mantener determinada cantidad y calidad de información reservada solamente para sí y su fuero interno.

[28] CONSTITUCIÓN NACIONAL Artículo 43 (Tercer párrafo) 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.
Recuperado julio 24, 2024 de https://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/804/norma.htm

Pero si se habla de consentimiento, es necesario establecer su significado. Es interesante trasladarse a la fuente de la Real Academia Española para aproximarnos a las diferentes acepciones del verbo consentir[29]:

- ✓ Permitir algo o condescender en que se haga;
- ✓ Creer (tener algo por cierto);
- ✓ Otorgar, obligarse;
- ✓ Dicho de una cosa: Soportar, tolerar algo, resistirlo;
- ✓ Dicho de una cosa: Resentirse, desencajarse, principiar a romperse.

Y es curioso, tal vez no casual para este desarrollo, que nos remitan al concepto de creer y al de la tolerancia, a resistir una cosa que también se resiente, se desencaja y que puede comenzar a romperse, como la compleja y dispersa estructura sobre la cual está edificado el sistema en el cual se asientan los múltiples bancos de datos biométricos.

*"La protección de los datos personales se basa en los principios de calidad de los datos, licitud de la recolección, respeto de la finalidad declarada, consentimiento y conocimiento del afectado y existencia de órganos de control independientes".*[30]

Para el correcto ejercicio del derecho de control sobre la propia información debe existir la posibilidad de fácil acceso a la misma, en caso de ser necesario, siempre que se la solicite correctamente a través de los medios garantizados constitucionalmente. Ya que esta cuestión está ligada inicialmente al consentimiento prestado por el titular original de la información al comienzo mismo del proceso, a su utilización específica y destino, en particular si esta es de carácter sensible respecto de la persona, como lo es la obtenida de los datos biométricos; la regla debería ser simple: si no hay consentimiento, no hay recopilación, o en caso de haberla sin mediar dicho consentimiento, esta captura debería ser informada a su titular. Pero,

[29] CONSENTIR – Definición RAE
Recuperado julio 22, 2024 de https://dle.rae.es/consentir

[30] MOLINA QUIROGA, EDUARDO (2003) *Protección de datos personales como derecho autónomo. Principios rectores. Informes de solvencia crediticia. Uso arbitrario. Daño moral y material* - www.saij.jus.gov.ar Id SAIJ: DACC030027
Recuperado julio 22, 2024 de http://www.saij.gob.ar/eduardo-molina-quiroga-proteccion-datos-personales-como-derecho-autonomo-principios-rectores-informes-solvencia-crediticia-uso-arbitrario-dano-moral-material-dacc030027-2003/123456789-0abc-defg7200-30ccanirtcod#

si bien esto está contemplado por la ley vigente, también lo están los supuestos para las excepciones previstas principalmente en lo referido a las funciones del Estado.

> *"La fundamentación jurídica del derecho a la protección de datos personales, sin duda puede y debe relacionarse con el tradicional derecho a la intimidad, pero lo excede ya que también alcanza a datos públicos, incide en otros derechos personalísimos como el honor, la imagen o la identidad, y que no solo se vincula con personas físicas, sino también con personas jurídicas."* (Molina Quiroga, 2003)[31]

El principio de proporcionalidad debe formar parte ineludible en el debate de la actuación del Estado en la administración de los datos de la población, no puede postergarse, ya que sus funciones son tan necesarias como la claridad jurídica a la que sean sometidas las personas en su rol de ciudadanos.

[31] MOLINA QUIROGA, EDUARDO (2003) *"Protección de datos personales como derecho autónomo. Principios rectores. Informes de solvencia crediticia. Uso arbitrario. Daño moral y material"* (2003) p. 347; Recuperado julio 22, 2024 de http://www.saij.gob.ar/docs-f/dossier-f/habeas_data.pdf

# CAPÍTULO IV – MANEJO NO REGULADO

## DAS UN POCO DE MIEDO – RIESGOS POTENCIALES EN LA MANIPULACIÓN DE DATOS BIOMÉTRICOS

En este capítulo se tratará el objetivo III del trabajo: investigar el manejo no regulado y no consentido de datos biométricos por parte de agentes públicos o privados y las consecuencias de tales acciones. Establecer los alcances sancionatorios ante tales supuestos.
Quedarse solo en un abordaje que ponga el foco en los datos personales como regulación de los datos biométricos resulta poco eficiente, sobre todo al ritmo del avance tecnológico y en lo que respecta al ámbito de la autodeterminación informativa.

## LA VENTAJA QUE TAMBIÉN ES EL PROBLEMA

Como se estableció desde el inicio del trabajo, la tecnología basada en datos biométricos incorporada cada vez más a la vida cotidiana de los individuos, otorga ventajas, practicidad y confort, como por ejemplo, el ahorro de tiempo comparado con el uso de múltiples códigos de acceso, por ejemplo, para ingresar a servicios como una cuenta bancaria, chequear la propia condición fiscal en un sitio como el de ARCA, ingresar a una página de una plataforma de compraventa online como Mercadolibre o a una bóveda de custodia de valores, entre muchos otros. El hecho de que la clave de acceso sea generada desde los propios patrones personales, individuales, únicos e irrepetibles, remite a una primera sensación de seguridad plena, ya que los datos biométricos de una persona son irremplazables. Pero es en este último concepto utilizado, donde también radica el principal problema, ya que un código externo, una clave, una tarjeta de acceso, sí puede ser reemplazada ante el caso de olvido, extravío o robo, pero esto no es posible ante la vulneración de los datos de origen biométrico, ya sea porque hayan sido recolectados sin mediar consentimiento, aún más grave es el caso de la captación sin conocimiento de la persona titular de los datos. La falta de un control apropiado, de la posibilidad de constatar la trazabilidad de la captura y las herramientas para accionar ante una vulneración sufrida.

A comienzos de octubre de 2021 se hizo público el hackeo a la base del Registro Nacional de las Personas (RENAPER) y probablemente la obtención de un número indeterminado de datos identificatorios de ciudadanos; a modo de prueba, a través de una cuenta del entonces Twitter (hoy X) se publicaron como muestra los datos de una cantidad de personas públicas, sus números de D.N.I, las fotos correspondientes en alta resolución, el número de trámite del D.N.I (un código numérico de validación que se encuentra en todos los documentos) y hasta algunos números de celular[32]. Además de esto publicó parte de una base de datos con numeraciones correlativas de identificaciones. Finalmente, a través de un foro de piratería se puso a la venta el acceso a esos datos y todo lo necesario para la suplantación de una identidad, a través de un archivo que contenía casi todos los datos personales de las identidades vulneradas. La versión del RENAPER fue que se trató de un uso indebido de usuario con acceso o robo de la clave del mismo, no existiendo tal filtración ni vulneración de la base de datos, constituyéndose en querellante de una denuncia penal ante el Juzgado en lo Criminal y Correccional Federal N°11 Secretaría N°22[33]. Pero aún si no se trató de un hackeo masivo y fue el mal accionar de un individuo (empleado o no) con acceso a una limitada cantidad de datos, esto pone de manifiesto la necesidad de un ordenamiento en la organización y el sistema de control desde lo administrativo y de una sólida estructuración sistematizada de la ley que lo acompaña, ante lo que no importa el volumen de los datos vulnerados, no deja de suponer un perjuicio a futuro para cualquiera de las personas damnificadas por la filtración.

- Sanciones vigentes

La ley N°25.326, contempla dos categorías de sanciones, aquellas administrativas, en su artículo 31 y las penales, establecidas en el artículo 32. Así, para el primer supuesto ante responsabilidades administrativas, la inobservancia de la norma que cause daños y perjuicios

[32] FITZ PATRICK, M; RUIZ, I.; CRUCIANELLI, S (2021) *Cuáles son las principales hipótesis detrás del hackeo a la base del Renaper* - Recuperado agosto 13, 2024 de https://www.infobae.com/politica/2021/10/31/cuales-son-las-principales-hipotesis-detras-del-hackeo-a-la-base-del-renaper/

[33] EL RENAPER DETECTÓ EL USO INDEBIDO DE UNA CLAVE OTORGADA A UN ORGANISMO PÚBLICO Y FORMALIZÓ UNA DENUNCIA PENAL (2021)
Recuperado agosto 13, 2024 de https://www.argentina.gob.ar/noticias/el-renaper-detecto-el-uso-indebido-de-una-clave-otorgada-un-organismo-publico-y-formalizo

o responsabilidad penal, la Autoridad de Aplicación puede imponer, según la gravedad, un apercibimiento, suspensión, multa o clausura. Siendo una ley de hace veinticinco años (2000) es clara la necesidad de una actualización ya que los valores de las multas van de los irrisorios mil a cien mil pesos.

Para el caso de las sanciones penales, éstas se mantienen también en el proyecto de reforma de la ley presentado en 2023, siendo el artículo 117 bis del Código Penal: un mes a dos años para la inserción de datos falsos en archivo de datos personales, de seis meses a tres años para la proporción de información falsa, el aumento de la pena en la mitad del mínimo y del máximo ante el perjuicio a un individuo y, finalmente, al tratarse de funcionario público en ejercicio de funciones, una inhabilitación accesoria para el desempeño de cargos públicos por el doble del tiempo que el de la condena que reciba. Además del artículo 157 bis, que debería ser el aplicado en el caso de filtración en el RENAPER, el cual establece pena de prisión de un mes a dos años, por la violación consciente de sistemas de confidencialidad y seguridad de datos o acceso ilegítimo a un banco de datos personales, o revelar a otro, información que está obligada a preservarse en secreto por ley. En este caso, además, si el autor es funcionario público se lo inhabilitará de uno a cuatro años.

# CAPÍTULO V – BIOMETRÍA Y EL ÁMBITO DE LA SEGURIDAD

## NO SÉ SI USTED ES DE FIAR – EFICACIA DE LAS TÉCNICAS BIOMÉTRICAS APLICADAS

En esta etapa se procurará cumplir con el objetivo IV del trabajo: analizar la aplicación de políticas de seguridad pública basadas en el uso de identificación por tecnología biométrica y la posible existencia de principios y derechos lesionados.

Pero antes de desarrollar el capítulo es válida la siguiente cuestión: ¿Qué tan confiable es la biometría? La autenticación por este método se basa en algoritmos estadísticos. Por lo tanto, como fue aclarado en el comienzo del trabajo, tanto en la ciencia como en la tecnología, no existe ni el 100% como totalidad ni el cero como idea de ausencia absoluta, por lo tanto, la utilización de un solo método no puede ser 100 % fiable, incluso cuando se utilice la combinación de resultados de diferentes métodos en las técnicas de modalidad múltiple. Se puede reducir el margen del error, pero nunca, eliminar su posibilidad.

## FALSOS POSITIVOS Y FALSOS RECHAZOS

Si un algoritmo capta un dato y luego de pasarlo por el motor de procesamiento comparativo, el resultado es que este no reconoce un dato biométrico que efectivamente corresponde a la persona, esto constituye un falso rechazo.

En cambio, si el motor de procesamiento comparativo atribuye como compatiblemente válidos dos datos biométricos que no pertenecen a la misma persona, esto es una falsa aceptación o falso positivo[34].

Los desafíos técnicos del reconocimiento automatizado de individuos en función de sus características biológicas y de comportamiento son inherentes a la transformación de información analógica (imagen facial, huellas dactilares, patrón de voz) en digital (patrones) que luego puede procesarse, compararse y compararse con algoritmos eficaces.

[34] BIOMETRICS, DEFINITION, USE CASES, LATEST NEWS (2023)
Recuperado julio 18, 2024 de https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics

Los resultados por parte de los sistemas biométricos deben tomarse en tiempo real, por lo tanto, la eficiencia del algoritmo y los motores de procesamiento debería ser fundamental en tales aplicaciones.

RECONOCIMIENTO FACIAL

Cuando los métodos utilizados para lectura de rostro tienen una determinada sofisticación tecnológica, ofrecen la ventaja de realizar las lecturas a distancia, sin aproximación del sujeto al sistema de captación. Del mismo modo que el escaneo de fotografías previamente tomadas, como en el caso de identificaciones o pasaportes de un inmenso volumen de individuos.
Los algoritmos de identificación se nutren de la información que reciben, y si la mayor cantidad de datos pertenecen a una mayoría étnica, esto puede producir malas lecturas o márgenes de error interpretativo más altos en sectores de población proporcionalmente minoritarios, y esta tasa de error más elevada de lectura sobre estos segmentos, puede provocar, por lo tanto, sesgos discriminatorios. En nuestro país, el anexo I de la resolución N° 4/2019[35] emitida por la Agencia de Acceso a la Información Pública establece que los datos biométricos "se considerarán datos sensibles cuando puedan revelar datos adicionales cuyo uso pueda resultar potencialmente discriminatorio para su titular" entre los cuales se encuentra el origen étnico de una persona.

USO APLICADO SOBRE SEGURIDAD PÚBLICA

Esta categoría abarca todos los usos de la biometría aplicada específicamente a la identificación de delincuentes, como los sistemas automatizados de huellas dactilares y palmares (AFIS)[36]. Almacenan, buscan y recuperan imágenes de huellas dactilares y registros

[35] CRITERIOS ORIENTADORES E INDICADORES DE MEJORES PRÁCTICAS EN LA APLICACIÓN DE LA LEY Nº25.326 (2019) – Anexo I – Recuperado julio 22, 2024 de https://www.argentina.gob.ar/sites/default/files/infoleg/res4AAIP-318874.pdf

[36] El SISTEMA AUTOMATIZADO DE IDENTIFICACIÓN DE HUELLAS DACTILARES (AFIS) es un sistema biométrico digitalizado diseñado para capturar, almacenar, analizar y comparar datos de huellas dactilares. El AFIS no se limita a las investigaciones penales. Desde la verificación de pasaportes y la seguridad de las transacciones financieras hasta los problemas de seguridad pública y más. Recuperado julio 28, 2024 de https://www.aratek.co/es/news/automated-fingerprint-identification-system-afis-an-overview

de sujetos. Hoy en día, los sistemas automatizados de identificación biométrica (ABIS) pueden obtener y almacenar información que coincida con plantillas biométricas para el rostro, las huellas dactiloscópicas y el iris.

Los diversos tipos de software utilizados para el reconocimiento facial en vivo (la capacidad de realizar una identificación facial a través de un escaneo general en una multitud y en tiempo real, o posterior, resulta de interés para la seguridad pública (en ciudades, aeropuertos, fronteras u otros espacios sensibles como los lugares de culto). Estos sistemas de vigilancia se están probando o utilizando en muchos países. Son cuestionados y a veces sometidos a revisión.

SISTEMA DE RECONOCIMIENTO FACIAL DE PRÓFUGOS

> *"Es fácil imaginar los servicios que una clasificación de este tipo podría hacer en este cierto tipo de casos criminales o de seguridad pública. Creemos que es difícil, pero no imposible para poner en práctica. Quizás se intente un día"* (Bertillon, 1890)

En este punto se analiza la implementación del Sistema de Reconocimiento Facial de Prófugos (SRFP), que además contempla un sistema de predicción de situaciones en el espacio público, desarrollado con un software de Inteligencia Artificial y puesto en funcionamiento en la Ciudad Autónoma de Buenos Aires en el año 2019 que fue la primera en todo el país en utilizar un sistema basado en tecnología de estas características, fundado en la necesidad de detectar y detener prófugos de la justicia.

Este tipo de sistemas en otros países dieron casos de falsos positivos. Se trata de errores en el reconocimiento facial, que indica a los operadores del sistema que se detectó a una de las personas buscadas, cuando en realidad se trata de otra persona.

San Francisco fue la primera ciudad en los Estados Unidos en prohibir este tipo de sistemas[37]. Al tratarse de tecnologías que realizan mapeos continuos sobre grandes volúmenes de personas en espacios públicos, se decidió presentar la "Ordenanza para Detener la Vigilancia

[37] SAN FRANCISCO PROHÍBE A LA POLICÍA USAR TECNOLOGÍA DE RECONOCIMIENTO FACIAL; EN LONDRES, EL 96 POR CIENTO DE LAS VECES DA FALSOS POSITIVOS (2019) Recuperado septiembre 19, 2024 de https://www.lanacion.com.ar/tecnologia/san-francisco-prohibe-policia-usar-tecnologia-reconocimiento-nid2247555/

Secreta" (Stop Secret Surveillance Ordinance), aprobada en mayo de 2019). La misma establece en parte de su texto:

"*Deben existir salvaguardas legalmente exigibles, incluidas sólidas medidas de transparencia, supervisión y rendición de cuentas, para proteger los derechos civiles y las libertades civiles antes de que se implemente cualquier tecnología de vigilancia; y si se aprueba una tecnología de vigilancia, deben adoptarse medidas de presentación de datos que faculten a la Junta de Supervisores y al público para verificar que se han respetado estrictamente las salvaguardas obligatorias de los derechos civiles y las libertades civiles*".[38]

En 2019, Argentina recibió la visita de una relatoría especial de la Organización de Naciones Unidas (ONU)[39]. Luego de realizar el informe preliminar, el encargado de la misma sostuvo que deberían hacerse evaluaciones de impacto respecto de los derechos humanos de los ciudadanos antes de poner en funcionamiento este tipo de sistemas ya que no guardaba criterio de proporcionalidad con la finalidad buscada[40].

A principios de este capítulo, se desarrolló el concepto de falsos positivos y falsos negativos de este tipo de sistemas, esto fue lo que sucedió en 2019 con Guillermo Federico Ibarrola quien tras un resultado positivo arrojado por el Sistema de Reconocimiento Facial de Prófugos, fue detenido en Retiro de acuerdo a un pedido de captura del Juzgado de Garantías N°2 de Bahía Blanca, recién luego de 6 días se comprobó que en el sistema se cargó su D.N.I y no el de Guillermo Walter Ibarrola, la persona a la cual se buscaba[41].

Es por esto, ante la posibilidad de afectación de derechos fundamentales como el de la libertad, es que los motores de tratamiento deben ser correctamente entrenados en la

---

[38] Parte del texto de la STOP SECRET SURVEILLANCE ORDINANCE (06/05/2019) Recuperado septiembre 19, 2024 de https://www.eff.org/document/stop-secret-surveillance-ordinance-05062019

[39] LAS RELATORÍAS ESPECIALES Y LOS GRUPOS DE TRABAJO DEL CONSEJO DE DERECHOS HUMANOS: son expertos/as independientes con mandato para informar y asesorar sobre los derechos humanos desde una perspectiva temática o de país. Recuperado septiembre 20, 2024 de https://www.argentina.gob.ar/derechoshumanos/compromisos-internacionales-en-derechos-humanos/visitas-de-relatores-y-grupos-de

[40] DECLARACIÓN DEL RELATOR ESPECIAL SOBRE EL DERECHO A LA PRIVACIDAD TRAS VISITAR ARGENTINA
Recuperado septiembre 20, 2024 de https://argentina.un.org/es/168010-declaraci%C3%B3n-del-relator-especial-sobre-el-derecho-la-privacidad-tras-visitar-argentina

[41] UN HOMBRE ESTUVO SEIS DÍAS PRESO POR UN ERROR POLICIAL Recuperado julio 22, 2024 de https://www.infobae.com/sociedad/policiales/2019/08/02/un-hombre-estuvo-seis-dias-preso-por-un-error-del-sistema-de-reconocimiento-facial/

información que reciben sus bases de datos y siempre previo a una evaluación de impacto, en este caso específico debido al escaneo masivo y escrutinio permanente que debe realizarse sobre todos los ciudadanos y ciudadanas que transitan un espacio público.

Los datos biométricos son datos sensibles y la ley N°25.326 vigente establece en el inciso 2 de su artículo 7 que estos solo pueden recolectarse o tratarse cuando medien razones de interés general autorizadas por ley, uno de los puntos clave justamente es que el sistema carece de sustento normativo que lo legitime.

Ante estos sucesos, en 2019, el Observatorio de Derecho Informático Argentino (O.D.I.A.)[42] realizó una acción de amparo, que luego de varios procesos concluyó en 2022 con la suspensión del Sistema de Reconocimiento Facial de Prófugos por no tener los mecanismos de control adecuados, carecer del estudio de impacto necesario y no respetar el criterio de proporcionalidad respecto de la finalidad perseguida.

Hasta el momento de escribir este capítulo (2024)[43], aún se encuentra suspendido hasta tanto no se realice una auditoría que constate la ausencia de cualquier sesgo en sus motores de búsqueda y rastreo, sean de carácter étnico, de género o racial, previendo eventuales daños, perjuicios y vulneraciones de derechos que pudiera ocasionar su uso.

JURISPRUDENCIA DIRECTAMENTE RELACIONADA CON EL CASO

**Cámara de Apelaciones en lo Contencioso Administrativo, Tributario y de Relaciones de Consumo. Sala I. Secretaría única. "Observatorio de Derecho Informático Argentino (O.D.I.A.)"[44]. Expediente N°182908/2020. Actuación N°1055665/2023. 28/4/2023.**

---

[42] EL OBSERVATORIO DE DERECHO INFORMÁTICO ARGENTINO (O.D.I.A.) es una asociación civil sin fines de lucro. Fue creada con el objetivo de promover el ejercicio responsable de la ciudadanía digital y garantizar que los derechos de la comunidad sean respetados.
Recuperado octubre 10, 2024 de https://odia.legal/

[43] BRODERSEN, J (2024) *Por qué el reconocimiento facial sigue suspendido en la ciudad de buenos aires: claves para entender los usos y riesgos de esta inteligencia artificial* Recuperado julio 25, 2024 de https://www.clarin.com/tecnologia/reconocimiento-facial-sigue-suspendido-ciudad-buenos-aires-claves-entender-usos-riesgos-inteligencia-artificial_0_eT30Dwx2Gm.html?srsltid=AfmBOopvCOYGO9IQkTB5d-5Z8gF2TLaPKdqMHNasVbLdrCGZ6Wj8H-bo

[44] REPOSITORIO DEL MINISTERIO PÚBLICO DE LA DEFENSA
Recuperado diciembre 22, 2024 de https://repositorio.mpd.gov.ar/jspui/handle/123456789/4657

En 2019 el Gobierno de la Ciudad de Buenos Aires puso en funcionamiento el Sistema de Reconocimiento Facial de Prófugos (SRFP) dentro de su jurisdicción. El SRFP utilizaba cámaras de videovigilancia buscando coincidencias con los rostros almacenados en la base de datos del sistema de Consulta Nacional de Rebeldía y Capturas (CoNaRC). El Observatorio de Derecho Informático Argentino (O.D.I.A.) promovió una acción de amparo para que se declaren inconstitucionales la Resolución N°398/MJYSGC/19[45] y la Ley N°6339[46], que implementaron el SRFP, por considerar que afectaba, el derecho a la libre circulación de las personas, el derecho de reunión, a la intimidad, a la no discriminación, a la igualdad y la protección de datos. El juzgado de primera instancia en lo Contencioso Administrativo y Tributario N°4 dictó sentencia contra el GCBA y suspendió el uso del SRFP. En la sentencia sostuvo que "no significaba reducir el resto de sistemas de videovigilancia (monitoreo urbano); ni un menoscabo en el servicio de seguridad pública". No se hizo foco en las consecuencias sobre el respeto por los derechos y garantías de las personas. Se determinó que, para ser implementado nuevamente, debían funcionar los mecanismos de control, constituirse un registro de datos relativo al sistema de videovigilancia, realizarse una Evaluación del Impacto en la Privacidad y convocarse a la ciudadanía a debatir sobre dicho mecanismo.

Contra esa decisión, O.D.I.A. junto al CELS, interpusieron un recurso de apelación. La parte actora criticó el fallo de primera instancia por mantener la vigencia del SRFP supeditada al funcionamiento de los órganos de control (Comisión Especial de Seguimiento de los Sistemas de Video Vigilancia y Defensoría del Pueblo local) y que según el peritaje técnico el sistema era deficiente y destacó que eran las características del sistema lo que lo tornaba inseguro, más allá de los contralores competentes, por lo que no existía ningún mecanismo de vigilancia que hiciera compatible esta herramienta con los derechos personales afectados. Asimismo, cuestionó la falta de participación y debate ciudadano antes de la sanción de las normas que regulan el SRFP. Afirmó que **el sistema violaba los derechos personales a la intimidad, privacidad y de protección de datos personales porque las cámaras captaban**

[45] Resolución N°398/MJYSGC/19 - Puede consultarse el texto completo en https://documentosboletinoficial.buenosaires.gob.ar/publico/ck_PE-RES-MJYSGC-MJYSGC-398-19-5604.pdf

[46] Ley N°6339 - Texto completo puede consultarse en https://documentosboletinoficial.buenosaires.gob.ar/publico/ck_PL-LEY-LCABA-LCBA-6339-20-6002.pdf

**la totalidad de los rostros que pasaban por delante de ella y porque dotaba al Estado de información precisa respecto de los lugares públicos dentro de C.A.B.A**. Y que en la primera instancia no se analizó la afectación provocada sobre tales derechos y que el SRFP **realizaba un tratamiento de datos personales sensibles que requería el consentimiento del titular de la imagen**. Por su parte, el CELS, sostuvo que el algoritmo **era discriminatorio atentando contra el derecho a la igualdad toda vez que la precisión de los sistemas de reconocimiento facial variaba en función del color, la raza, el género de las personas, incrementando las posibilidades de errores y de falsos positivos, generando impactos desproporcionados sobre grupos en situación de vulnerabilidad.**

Decisión

La Sala I de la Cámara de Apelaciones en lo Contencioso Administrativo, Tributario y de Relaciones de Consumo, no hizo lugar al recurso de apelación interpuesto por O.D.I.A, ni por los demás actores. Sin embargo, **sí hizo lugar parcialmente a los agravios del CELS y, en consecuencia, ordenó que la rehabilitación del funcionamiento del SRFP, además de quedar supeditada a la constitución y debido funcionamiento de los órganos de control, quedará sujeta a la realización de las investigaciones y pruebas necesarias sobre el software que utiliza el SRFP**.

A la fecha de la redacción de este trabajo, el SRFP, continúa suspendido.

## SOLO SE QUE NO SE NADA, PERO SÉ QUIEN ES USTED - EL SISTEMA FEDERAL DE IDENTIFICACIÓN BIOMÉTRICA PARA LA SEGURIDAD (SIBIOS)

A diferencia de la ley del Congreso de 1948 Nº13.482[47] que creó el Registro nacional de la Personas, todo el resto del sistema securitario aplicado al control poblacional se basó históricamente en su mayor parte en un andamiaje de decretos presidenciales y reglamentaciones internas emitidas por los propios entes y organismos de aplicación. En la ley de seguridad interior Nº24.059 de 1992 (sí sancionada por el Congreso el 18 de diciembre de 1991), esta enumera las finalidades y su alcance, estableciendo una definición en su artículo 2 que "es la situación de hecho basada en el derecho en la cual se encuentran

[47] CREACION DEL REGISTRO NACIONAL DE LAS PERSONAS LEY 13.482 (1948) Recuperado agosto 5, 2024 de https://www.argentina.gob.ar/normativa/nacional/ley-13482-295928/actualizacion

resguardadas la libertad, la vida y el patrimonio de los habitantes, sus derechos y garantías y la plena vigencia de las instituciones del sistema representativo, republicano y federal que establece la Constitución Nacional"[48]. Pero dicho resguardo de los derechos y garantías de los ciudadanos es realizado a través de las funciones que despliega el poder de policía, lo que es la aplicación de la teoría de Max Weber a través de los organismos específicamente autorizados por el Estado para utilizar o legitimar la utilización de la violencia.

El gobierno de Cristina Fernández de Kirchner -sin debate parlamentario y con la firma del Decreto del Poder Ejecutivo Nacional 1766/2011- creó el Sistema Federal de Identificación Biométrica[49], concentrando millones de datos biométricos poblacionales en una base de información unificada a cargo del Ministerio de Seguridad. El sistema almacena las huellas dactilares, las huellas palmares y los rasgos faciales de todos los ciudadanos argentinos tanto como de los extranjeros que ingresen o egresen a Argentina. Las bases de datos existentes con anterioridad al Decreto 1766/11 se encontraban incompletas, y con el fin de poder tener los registros de la totalidad de habitantes del país, la principal fuente de estos datos era (y es) el Registro Nacional de las Personas, como la autoridad a cargo de emitir el Documento Nacional de Identidad y del Pasaporte Nacional.

Los artículos 1 y 2 de la ley N°13.482 de creación del RENAPER[50] establecen los fines y funciones del mismo, de igual modo lo hace la ley N°17.671 (1968)[51]: registrar y certificar la identidad de todos los ciudadanos argentinos, de sus antecedentes de mayor importancia desde el nacimiento, desarrollando, con carácter exclusivo, la expedición de los documentos nacionales de identidad con las características, nomenclatura y plazos fijados por la normativa aplicable. Por otra parte, el decreto N°1766/2011 de creación del SIBIOS "posee

[48] LEY DE SEGURIDAD INTERIOR Nº24.059 (1992)
Recuperado julio 24, 2024 de https://www.argentina.gob.ar/normativa/nacional/ley-24059-458/actualizacion

[49] SISTEMA FEDERAL DE IDENTIFICACIÓN BIOMÉTRICA (2011) Decreto 1766/2011
Recuperado julio 25, 2024 de https://www.argentina.gob.ar/normativa/nacional/decreto-1766-2011-189382/actualizacion

[50] CREACION DEL REGISTRO NACIONAL DE LAS PERSONAS LEY 13.482 (1948)
Recuperado agosto 5, 2024 de https://www.argentina.gob.ar/normativa/nacional/ley-13482-295928/actualizacion

[51] LEY DE IDENTIFICACION, REGISTRO Y CLASIFICACION DEL POTENCIAL HUMANO NACIONAL (1968) N°17.671
Recuperado agosto 5, 2024 de https://www.argentina.gob.ar/normativa/nacional/ley-17671-28130/actualizacion

como finalidad principal instrumentar un servicio informático para permitir la comprobación idónea y oportuna de identificación de personas y rastros para fines de seguridad pública y de investigación judicial" (considerando 15°). El problema radica en el artículo 2 del mismo decreto que establece: "el Registro Nacional de las Personas brindará la información biométrica necesaria para que el Sistema Automatizado de Identificación de Huellas Digitales (AFIS) y de rostros en uso en la Policía Federal Argentina pueda satisfacer los requerimientos de identificación del Sistema Federal de Identificación Biométrica para la Seguridad (SIBIOS)"

El planteo principal es que si bien la cesión de datos entre organismos del Estado de forma directa está permitida por la ley N°25.326 (artículo 11) sin necesidad de consentimiento del Titular de los datos, aún no cumple el deber de información a los mismos. Pero lo que es aún más polémico es que el uso de la información para aportar al SIBIOS viola el principio de finalidad dentro del artículo 4 de la misma ley N°25.326 ya que "Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención", el punto focal es que se trata de dos registros diferentes (RENAPER y SIBIOS) con dos finalidades completamente distintas, convirtiendo al primer registro (de datos de ciudadanos) en una herramienta destinada a la política criminal del Estado a través de la manipulación y violación de normativas vigentes.

## CAPÍTULO VI – NORMATIVA VIGENTE

En el presente capítulo y en el siguiente (capítulo VII) se llevará adelante el objetivo V: Evaluar la normativa existente en nuestro país y su extensión concreta en cuanto a la protección de datos de origen biométrico. Ver en paralelo el alcance de proyectos de adecuación nacionales existentes.

### LEY 25.326 DE PROTECCIÓN DE LOS DATOS PERSONALES

Es necesario aclarar que la ley en el cuerpo original de su texto actual no refiere en específico al tratamiento de los datos biométricos, pero se incluye su análisis para entender su estructura, hacia qué puntos enfoca, el posterior tratamiento de anexos y de resoluciones siguientes con el fin de actualizar su contenido y de ese modo comprender si existen falencias o mejoras posibles respecto del objeto de este trabajo.

La ley N°25.326[52] que fue sancionada en octubre de 2000, se desprende directamente de lo establecido en el artículo 43 de la Constitución Nacional cuyo párrafo tercero contempla el Habeas Data, redactado de la siguiente forma:

*"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 aquellos. No podrá afectarse el secreto de las fuentes de información periodística".*[53]

Desde su artículo 1, la ley establece como su objeto la protección de los datos personales recopilados en diferentes soportes (archivos, registros, bancos de datos; etc.) para garantizar el derecho al honor e intimidad de las personas, como así también el ejercicio de acceso a los mismos, consecuencia del avance tecnológico y la velocidad recopilatoria de datos cuyo uso pueda afectar de algún modo los derechos de los individuos.

---

[52] PROTECCION DE LOS DATOS PERSONALES – LEY N°25.326
Recuperado enero 20, 2024 de https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790/actualizacion

[53] CONSTITUCIÓN NACIONAL
Recuperado enero 22, 2025 de https://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/804/norma.htm

A partir del artículo 2 se dan las definiciones que son contempladas en la ley, así se considera de importancia para este trabajo, las siguientes:

- ✓ Datos sensibles, como aquellos datos personales que den a conocer entre otros, el origen étnico, racial, información sobre salud o vida sexual.
- ✓ Titular de los datos es la persona física (o de existencia ideal) cuya información sea el objeto del tratamiento de datos, que a su vez es definido como:
- ✓ Tratamiento de datos comprende todas las operaciones y procedimientos sistemáticos (sean o no electrónicos) de todo procesamiento de datos personales (recolección, almacenamiento, modificación, evaluación, destrucción, bloqueo; etc.) así como su cesión a terceros.
- ✓ Responsable de archivo, base o banco de datos es el titular del mismo y puede ser una persona física o de existencia ideal (pública o privada).
- ✓ Usuario de datos es quien lleva a cabo el tratamiento de los mismos.

El principio de licitud de los archivos y bases de datos (artículo 3) está unido a su debida inscripción[54] (artículo 21) y observancia de la ley, sin tener finalidades contrarias a la misma o a la moral pública.

En cuanto a la calidad de los datos recolectados, deben cumplir la condición de ser ciertos y adecuados, exactos y debidamente actualizados, agregando que deben ser pertinentes y no excesivos respecto de la finalidad del tratamiento. Esta recolección debe ser lícita (no desleal o fraudulenta) y los datos no pueden ser utilizados para una finalidad diferente a la que originalmente justificó el procedimiento; en cuanto al almacenamiento de la información, una vez cumplido el fin del tratamiento, los datos deben destruirse de no ser ya necesarios. Como contrapartida, ante la presencia de datos que no cumplan el requerimiento de exactitud o sean incompletos, deben ser sustituidos, completados o en último caso, suprimidos, sea por el responsable de la base de datos como en ejercicio de los derechos del propio Titular de los mismos.

- Consentimiento

[54] BUSCADOR DEL REGISTRO NACIONAL DE BASES DE DATOS PERSONALES: pone en conocimiento las bases inscriptas, sus finalidades y datos de contacto.
Se puede consultar en: https://www.argentina.gob.ar/aaip/datospersonales/reclama

El consentimiento del titular casi el único supuesto de base legal y es tratado en el artículo 5, siendo este análisis desde el texto original de la ley, es necesario aclarar que varias de estas condiciones se encuentran mejoradas en el proyecto de ley presentado en 2023. Así, en la ley N°25.326 vigente, el titular debe darlo de forma libre, expresa, informada y debe constar por escrito o medio que sea equiparable. No se incluye la condición de consentimiento unívoco, claramente específico para una finalidad determinada (que si incluye el proyecto de reforma). Esta necesidad de consentimiento cae, entre otros supuestos, si los datos provienen de fuentes de acceso público irrestricto y ante las funciones propias de los poderes del Estado u obligación legal.

- Derechos de los Titulares de los Datos

En cuanto al derecho de información que reciba el Titular de los datos (artículos 6 y 13), esta debe ser previa a su recolección, expresa y clara respecto de la finalidad del tratamiento, sobre los destinatarios y la existencia del tipo de soporte de almacenamiento (archivo, banco de datos, registro) como el domicilio del responsable del mismo. El titular de los datos tiene derecho a conocer las consecuencias tanto de dar los datos, como de negarlos o proporcionarlos de modo inexacto; así también, la posibilidad de ejercer su derecho de acceso (artículo 14), rectificación, actualización o supresión de los mismos, establecidos en el artículo 16, siendo tanto el Responsable o el Usuario del banco de datos los encargados de realizar la tarea si el Titular así lo requiriese.

El artículo 7 trata la categoría de datos, estableciendo que nadie puede ser obligado a dar datos sensibles (en el cuerpo original de la ley, no se menciona en principio, a los datos biométricos dentro de la categoría, que luego fue subsanado por las resoluciones complementarias posteriores), estos solo se pueden recolectar y tratar por razones de interés general autorizadas por ley o con finalidades estadísticas o científicas cuando el Titular de los datos no pueda ser identificado.

- Seguridad

La seguridad de los datos del artículo 9 (en el proyecto modificatorio de ley lo establece como principio de seguridad) ponen en cabeza del responsable o usuario garantizar la seguridad y confidencialidad para evitar cualquier adulteración o posibilidad de pérdida, consulta o tratamiento sin autorización, incluidas la detección de desviaciones de información, por error o intención (de origen humano o tecnológico).

- Cesión de datos

En referencia a la cesión de datos, media la información (finalidad e identidad del cesionario) y el previo consentimiento del Titular de los mismos (el cual es revocable) y sólo si la finalidad está directamente relacionada con el interés legítimo del cedente y del cesionario. No es necesario este consentimiento si los datos provienen de fuentes de acceso público irrestricto y ante las funciones propias de los poderes del Estado u obligación legal.

- Excepciones

La ley incluye excepciones dentro del artículo 17, aun cuando se aclare que se debe brindar acceso si el afectado tiene que ejercer su derecho de defensa (ante una acusación o perjuicio), los Responsables o Usuarios de bancos de datos públicos pueden denegar el ejercicio de los principios de acceso, rectificación o supresión amparados en la protección de la defensa nacional y la seguridad pública o protección de derechos de terceros.

- Sanciones

Como se explica en el Capítulo IV de este trabajo (Manejo no regulado) la ley N°25.326, contempla dos categorías de sanciones, aquellas administrativas, en su artículo 31, y las penales, establecidas en el artículo 32. Ante responsabilidades administrativas, la inobservancia de la norma que cause daños y perjuicios o responsabilidad penal, la Autoridad de Aplicación puede imponer, un apercibimiento, suspensión, multa o clausura. Como ya se analizó, siendo una ley del año 2000, es clara la necesidad de una actualización ya que los valores de las multas van de mil a cien mil pesos.

Para el caso de las sanciones penales (se mantienen también en el proyecto de reforma de la ley presentado en 2023), siendo el artículo 117 bis del Código Penal: un mes a dos años para la inserción de datos falsos en archivo de datos personales, de seis meses a tres años para la proporción de información falsa, el aumento de la pena en la mitad del mínimo y del máximo ante el perjuicio a un individuo y, finalmente, al tratarse de funcionario público en ejercicio de funciones, una inhabilitación accesoria para el desempeño de cargos públicos por el doble del tiempo que el de la condena que reciba. Además del artículo 157 bis, el cual establece pena de prisión de un mes a dos años, por la violación consciente de sistemas de confidencialidad y seguridad de datos o acceso ilegítimo a un banco de datos personales, o revelar a otro, información que está obligada a preservarse en secreto por ley. En este caso, además, si el autor es funcionario público se lo inhabilitará de uno a cuatro años.

- Hábeas Data

A partir del capítulo VII la ley establece desde el artículo 33 cómo y cuándo procede la acción de protección de los datos personales o de Hábeas Data que forma parte de nuestro andamiaje constitucional en el artículo 43 (artículo fundante de la ley). En el artículo 34 se explica además la legitimación activa, es decir la ejercida por el afectado, sus tutores o curadores y los sucesores; el artículo 35 hace lo mismo con la legitimación pasiva, respecto de los responsables y usuarios de bancos de datos.
En cuanto a la competencia para la acción es a elección del actor: el juez de su domicilio; el del domicilio del demandado; el del lugar donde se hayan producido efectos.

## AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA

En el año 2017, a través del Decreto N°746 /2017[55], el artículo 11 del mismo, crea la Agencia de Acceso a la Información Pública, como ente autárquico con autonomía funcional en el ámbito de la Jefatura de Gabinete de Ministros. El Decreto la transforma en la Autoridad de Aplicación de la Ley 25.326 por lo que, desde ese momento, incorpora dentro de sus dependencias a la Dirección Nacional de Protección de Datos Personales, la cual funciona en la práctica como la primera instancia legal y técnica para la aplicación de la ley, dejando para la instancia resolutoria a la propia Agencia de Acceso a la Información Pública.

## RESOLUCIONES COMPLEMENTARIAS DE INTERÉS

En la Resolución 4/2019[56] y posteriormente en el Anexo I sobre criterios orientadores[57] , la Agencia de Acceso a la Información Pública, establece algunas definiciones y aclaraciones en relación a la ley 25.326. Así, en el Criterio 2, integra a los datos biométricos, como "los datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona humana, que permitan o confirmen su identificación única", y que estos, se considerarán datos sensibles únicamente

[55] TEXTO DECRETO 746/2017 Recuperado marzo 1, 2025 de https://www.argentina.gob.ar/normativa/nacional/decreto-746-2017-279940/texto

[56] AGENCIA DE ACCESO A LA INFORMACION PUBLICA - RESOL-2019-4-APN-AAIP Recuperado marzo 1, 2025 de https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-4-2019-318874/texto

[57] ANEXO I Criterios orientadores e indicadores de mejores prácticas en la aplicación de la Ley Nº 25.326 Recuperado marzo 1, 2025 de https://www.argentina.gob.ar/sites/default/files/infoleg/res4AAIP-318874.pdf

cuando puedan revelar datos adicionales cuyo uso pueda resultar potencialmente discriminatorio para su titular (a instancias del artículo 2 de la ley 25.326, como lo es el origen racial, étnico o los datos de salud).

Por otra parte, considera los registros de imágenes captados por sistemas de video vigilancia como una base de datos, también en los términos del artículo 2 de la Ley 25.326, lo que se conecta con el derecho de acceso en relación a datos personales que han sido recolectados por sistemas de video vigilancia (un tema desarrollado en este trabajo en el punto sobre reconocimiento facial aplicado a la seguridad pública y sus riesgos), ante las dificultades prácticas que pueda tener el Responsable de la base de datos para suministrar la información pedida por el requirente (artículo 15 ley 25.326), la Agencia de Acceso a la Información Pública establece entonces, el alcance del ejercicio del derecho de acceso del titular de los datos cuando le hubiesen causado grave perjuicio y el Responsable de la base de datos haya tomado decisiones basadas únicamente en el tratamiento automatizado de datos (Criterio 1 del Anexo I).

# CAPÍTULO VII - PROYECTOS DE LEY

## ANÁLISIS DEL MENSAJE 87/2023 - PROYECTO DE "LEY DE PROTECCIÓN DE LOS DATOS PERSONALES" –INLEG-2023-74703583-APN-PTE (NACIONAL)[58]

El siguiente análisis se hace siguiendo el texto publicado del proyecto de ley.

### INTRODUCCIÓN

En junio de 2023, bajo el mandato del presidente Alberto Fernández, se presentó un proyecto de actualización de la Ley de Protección de los Datos Personales Nº25.326 y su modificatoria. En el mensaje 87/2023 se describen los lineamientos de la reforma, planteándose que se tienen en cuenta diferentes normativas y recomendaciones ya puestas en práctica en distintas regiones de América y Europa, como así también otros anteproyectos presentados anteriormente y que no fueron tratados oportunamente. Se resalta el Protocolo modificatorio del Convenio Nº108+ del Consejo de Europa para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal[59] (el primer convenio 108 fue firmado en enero de 1981 y en octubre de 2018 se realizó el acuerdo STCE Nº223[60] para su actualización, con más de 55 estados parte. Este convenio tiene como finalidad justamente darle un marco normativo a la privacidad de los datos personales ante las vulneraciones que estos puedan sufrir durante su recolección y procesamiento) y que fue aprobado por el Congreso de la Nación a través de la ley 27.699 (BO. 30/11/2022)[61].

Esta propuesta de reforma hace foco en la protección de los datos personales en su carácter de derechos humanos, el concepto de la autodeterminación informativa de los individuos, los

---

[58] PROYECTO DE LEY DE PROTECCIÓN DE DATOS PERSONALES, MENSJ-2023-87-APN-PTE. Expediente Diputados: 12-PE-2023. Publicado en: Trámite Parlamentario N°84, 30/06/2023 Recuperado julio 22, 2024 de https://www.argentina.gob.ar/sites/default/files/mensajeyproyecto_leypdp2023.pdf

[59] CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA
Recuperado julio 22, 2024 de https://rm.coe.int/1680078b37

[60] Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia, relativo a la cooperación reforzada y la divulgación de pruebas electrónicas - Estrasburgo, 12.V. 2022 – Recuperado agosto, 2024 de https://rm.coe.int/1680a83724

[61] Recuperado julio 22, 2024 de https://www.boletinoficial.gob.ar/detalleAviso/primera/276783/20221130

principios éticos en la tecnología y que la actualización de la ley establezca claridad normativa. Si bien la reforma planteada en el proyecto abarca a todos los datos personales, a continuación, se realizará un análisis de los principales puntos que estén conectados en particular con el tratamiento de los datos biométricos, los cuales son el eje de este trabajo.

## LA MITAD DE UN VASO LLENO ES OTRA MITAD VACÍA – LAS MODIFICACIONES INTRODUCIDAS

En las Disposiciones Generales del capítulo 1 se establece en su primer artículo, como el objeto de la ley, regular el tratamiento de los datos personales (esto incluye los derechos de los individuos y los deberes de quienes están a cargo de la recopilación y procesamiento de datos) y las reglas para ejercer la autodeterminación informativa a fin de garantizar el ejercicio del derecho fundamental de las personas humanas a la protección de sus datos personales y privacidad: "el derecho de la persona a decidir o autorizar de forma libre, previa, expresa e informada la recolección, uso o tratamiento de sus datos personales, así como de conocer, actualizar, rectificar o suprimirlos, o controlar lo que se hace con su información" (artículo 2), ya establecido por el artículo 43 de la Constitución Nacional y también distribuido en diversos Tratados y Convenciones del Bloque Convencional – Constitucional. Como dato positivo entonces, que se diferencia del texto original de la ley del año 2000, es que se introduce el concepto de derecho fundamental asociado al de datos personales, como así también el recién mencionado de autodeterminación informativa del individuo, constituido por el derecho de control sobre todo aspecto de su propia información personal.

### EL ESTADO PRESENTE

Es muy interesante que en cuanto al ámbito de aplicación material propuesto por el proyecto de ley que es tratado en el artículo 3, además de incluir dentro del universo de quienes efectúen el tratamiento de datos a personas físicas o jurídicas (sean estas públicas o privadas), incluye al propio Estado ejerciendo facultades sobre cuestiones de salud y seguridad pública, defensa nacional y la protección de las libertades de terceros. Con respecto a la inclusión del Estado como agente de tratamiento podría augurarse como un gran avance respecto a intromisiones excesivas de éste en las esferas individuales.

### MARCANDO TERRITORIO

Un concepto importante que forma parte de este proyecto (y que debería serlo además de cualquier otro proyecto futuro sobre este tema) es el tratado en el ámbito de aplicación territorial del artículo 4. En una problemática que tiene una de sus bases en la utilización de tecnologías, que como ya se adelantó en la presentación del trabajo, por su propia naturaleza trascienden cualquier frontera geográfica física, es imperativo que toda adecuación que pretenda ser mínimamente efectiva a los efectos de la norma, debe contemplar cómo regular los extremos ubicados en diferentes puntos tanto territoriales internos como extraterritoriales. Los supuestos que aborda este proyecto abarcan el caso del responsable o encargado del tratamiento dentro del territorio nacional independientemente de que los datos se traten fuera del mismo; al responsable o encargado del tratamiento establecido fuera del país, pero que realiza el tratamiento dentro del territorio; y el caso particular de ubicación extraterritorial, pero con aplicación de la ley argentina por derecho internacional o por disposiciones contractuales.

### UNA CUESTIÓN DE PRINCIPIOS

En cuanto al tratamiento de los datos personales que forman parte del Capítulo 2 del proyecto de ley, se establece una reformulación en forma de principios de los puntos que ya forman parte del artículo 4 de la ley 25.326 que enumera la "calidad de los datos". A criterio de este análisis, los eufemismos en una norma que debe plantear un cambio son innecesarios, ya que no aportan nada sustancialmente nuevo, aunque no dejan de ser importantes; así se lista desde el artículo 6 al artículo 9:

- ✓ el principio de licitud (conforme a la ley),
- ✓ de lealtad (no por medios engañosos o fraudulentos),
- ✓ de transparencia (información accesible y clara),
- ✓ de finalidad (solo pueden usarse para el fin explícito y legítimo de su recolección),
- ✓ de minimización de datos (limitarlos solo en relación con los fines de su recopilación),
- ✓ el principio de exactitud (datos veraces, completos, comprobables y actualizados).

Además, el principio de seguridad de los datos personales establecido en el artículo 20, y el importantísimo principio de responsabilidad proactiva y demostrada del artículo 12, que constituye el deber de los intervinientes en el tratamiento de los datos personales de poner

foco en medidas que garanticen diligencia y un trato adecuado de los datos, estas medidas son de cumplimiento obligatorio y posibles de comprobar ante la Autoridad de Aplicación, debe notarse que son una reformulación y escasa actualización de las pautas establecidas en el artículo 9 (seguridad de los datos) de la actual ley 25.326. Se agregan, sin embargo, en el artículo 39 del proyecto de ley, cuáles son las medidas para el cumplimiento de este principio de responsabilidad proactiva y procedimientos que posibiliten ejercitar los derechos de los Titulares de datos, controles a través de supervisiones o auditorías (internas o externas) y el deber de una evaluación de impacto. Todo esto debe estar documentado y a disposición de la Autoridad de Aplicación, para ser ponderado por la misma ante la implementación de una sanción en caso de violación de la ley.

Sí es destacable dentro de este proyecto, el principio de preeminencia del artículo 10, en el que ante la duda sobre la interpretación y la aplicación de la ley prevalece la más favorable a la persona Titular de los datos personales, como así también, el plazo de conservación, en el artículo 11, limitado al tiempo "estrictamente necesario para el cumplimiento de la finalidad del tratamiento". Ambas constituyen herramientas de protección muy importantes, la primera ante un derecho lesionado, la segunda como prevención de posibles usos no idóneos ante la permanencia innecesaria de los datos.

### La biometría es de la partida

Volviendo al artículo 2 del proyecto, se introducen las definiciones de datos biométricos y datos genéticos (relativos a características genéticas heredadas o adquiridas de una persona humana que proporcionen una información sobre su fisiología o salud) lo cual sí resulta interesante porque ambos conceptos son incluidos a su vez en las definiciones de datos personales (como información sobre personas humanas determinadas o determinables, incorporando en el listado las características de su identidad biométrica y genética) y en el concepto de datos personales sensibles (agregando a la esfera íntima de la persona Titular los datos genéticos o biométricos cuando puedan revelar datos adicionales, por ejemplo datos de salud, origen étnico -entre otros- cuyo uso pueda ser potencialmente discriminatorio para la misma y que tengan por fin identificarla de manera unívoca).

### Bases legales más sólidas

El artículo 13 establece las bases legales para el tratamiento de los datos, partiendo desde el consentimiento del Titular, pero sin ponerlo como supuesto principal como la vigente ley

25.326, así entonces, se encuentra también el que sea necesario para ejercer y cumplir las funciones y facultades propias de los poderes del Estado; para algunas interpretaciones este supuesto tiene un carácter casi imprescindible, "esta legitimación para el tratamiento apunta a permitir al Estado poder recolectar datos personales a los efectos de poder cumplir con sus funciones"[62].

El resto de los supuestos implican:

- ✓ el cumplimiento de una obligación legal específica para el Responsable[63] o para el Encargado[64] del tratamiento, esto es una evolución respecto de la obligación legal que se encuentra vigente en la ley 25.326 en su artículo 5 pero como una excepción al consentimiento y sin especificación alguna;
- ✓ la necesidad que surja para la ejecución de un contrato o aplicación de medidas precontractuales;
- ✓ la salvaguarda de la vida del Titular de los datos (siempre que esta no pudiera otorgar el consentimiento por sí misma o sus representantes) y para el caso de la vida de terceros, no deben prevalecer ni intereses ni derechos del Titular de los datos;
- ✓ la existencia de un interés legítimo (inciso f). Este punto es importante para el desarrollo de este trabajo ya que en él se apoya la justificación de la recolección de datos por parte del Responsable del tratamiento. Prevalece el interés de la persona Titular (sobre todo si se trata de niños, niñas o adolescentes) y la fundamentación de este interés legítimo de quienes deban tratar los datos, con la obligación de un análisis documentado sobre el contexto, circunstancias y riesgos, respetando el principio de minimización de datos y siguiendo criterios de proporcionalidad y razonabilidad, quedando en cabeza del mismo la carga de la prueba ante la solicitud de esta justificación por parte de la Autoridad de Aplicación.

---

[62] PERUZZOTTI, MARIANO (2024) *"Las nuevas bases legales en el proyecto de Ley de Protección de Datos Personales"* para "*Proyecto de Ley de Protección de Datos Personales de la AAIP: diversas miradas y un consenso: la necesidad de actualizar la legislación argentina"* / Beatriz de Anchorena; Compilación de Beatriz de Anchorena. - 1a ed - Ciudad Autónoma de Buenos Aires: Ediciones AAIP, 2024. p. 84

[63] RESPONSABLE DE TRATAMIENTO DE DATOS PERSONALES: *Persona humana o jurídica, pública o privada, que solo o conjuntamente con otros decide sobre la finalidad y el tratamiento de datos personales* (artículo 2 - Definiciones)

[64] ENCARGADO DE TRATAMIENTO: *Persona humana o jurídica, pública o privada, que trate datos personales por cuenta del Responsable de tratamiento* (artículo 2 – Definiciones)

En lo referido específicamente al consentimiento, el artículo 14 del proyecto establece que, cuando este sea la base legal para el supuesto, el Titular de los datos debe darlo mediante:

- ✓ una declaración o una clara acción afirmativa (es decir, de forma expresa);
- ✓ previa (el consentimiento debe darse antes de la recolección);
- ✓ libre (sin vicios, con la posibilidad de negarse sin que le traiga perjuicios);
- ✓ específica (para la finalidad de cada recolección);
- ✓ informada (sobre qué tipos de datos se recogen, su finalidad, si habrá transferencias, quién es el Responsable o Encargado del tratamiento; etc.) e
- ✓ inequívoca (el consentimiento no debe dejar dudas respecto de su alcance exacto, lo que no está contemplado en la ley 25.326 vigente).

Cuando sea el caso la revocación del consentimiento, el proyecto establece en su artículo 15 que, puede realizarse en cualquier momento y sin fundamentar el pedido, con la disposición de mecanismos de revocación tanto o más fáciles que los de otorgamiento del mismo.

Para dar un consentimiento informado (como es solicitado en el artículo 15 del proyecto), el Titular de los datos necesariamente debe disponer de todas las pautas de manejo que tendrán los mismos, y para esto, el artículo 16 del proyecto de ley prevé que, quienes traten los datos, den de modo conciso, fácilmente entendible y de simple acceso, todos los ítems siguientes:

- ✓ Los datos personales y legales ya sea del Responsable o Encargado de tratamiento, Delegado de Protección de datos o Representante en territorio nacional de los Responsables no establecidos en el país.
- ✓ Categorías de los datos a tratarse (biométricos y genéticos para este trabajo) y su finalidad.
- ✓ Que el Titular de los datos sea informado de sus derechos y sobre cómo ejercerlos (presentar una denuncia o tramitar la protección de sus datos ante la Autoridad de Aplicación), como así también de ejercer la acción de Hábeas Data.
- ✓ Conocer si su información va a ser cedida a otros Responsable o Encargados de tratamiento o si ésta va a ser transferida a otros países, facilitando todos los datos del destinatario de la misma, finalidad, posibles riesgos y cómo ejercer sus derechos ante vulneraciones. Debiendo informarse si los datos se obtuvieron directamente del

Titular de los mismos o demostrar si la base legal que legitimó al Responsable de tratamiento no era el consentimiento.

- ✓ Que pueda saber si es el caso, obligatorio o no dar sus datos personales y si otorgarlos, no hacerlo o darlos de modo incompleto o erróneo le traerá algún perjuicio. Establece que sepa su derecho a la posibilidad de revocación de tal consentimiento.
- ✓ Debe incluir, la gran importancia del plazo de conservación de los datos y de la existencia o no de decisiones automatizadas o semiautomatizadas incluyendo el extremadamente sensible caso de la elaboración de perfiles (con su latente potencial discriminatorio).

Toda la información que los intervinientes en el tratamiento, y que, el artículo 16 establece como obligación de brindar, va en exacta concordancia con el derecho de acceso a los datos que establece el artículo 27, dentro del Capítulo 4 titulado "Derechos de los Titulares de los datos", quien por lo tanto, estos puede recibirla acreditando su identidad, sumada al derecho de solicitar la rectificación, oposición y/o supresión (establecidos respectivamente en los artículos 28, 29 y 30 del mismo capítulo). En cuanto a la existencia de decisiones automatizadas (parciales o semiautomatizadas) donde "no hay participación humana significativa" se establece en el artículo 31 el derecho a no ser objeto de las mismas si produce vulneraciones en el aspecto jurídico o en el caso de que tengan efectos discriminatorios (elaboración de perfiles). Todos estos derechos se ejercitan a través de un trámite de protección de datos personales ante la Autoridad de Aplicación.

### UNA PEQUEÑA LUZ EN LA OSCURIDAD - SECTOR PÚBLICO, BASES LEGALES Y LIMITACIONES

El Estado, desplegando su actividad a través del sector público, representa uno de los mayores recopiladores y procesadores de datos personales de los individuos, ya que, en este caso, estos últimos deben asumir su rol de ciudadanos. Esta enorme cantidad de información que se procesa, debería en principio, tener como finalidad principal su aplicación en las políticas públicas, para hacerlas cada vez más eficientes. Esto hace que gran parte de las leyes de datos personales, ya sea la ley 25.326 argentina tanto como la europea, por citar dos ejemplos de referencia del presente trabajo, eximan al Estado del cumplimiento de muchos

artículos sobre consentimiento y cesiones de información[65], cubriéndolo siempre bajo el paraguas protectorio del "ejercicio de las funciones propias de los poderes" del mismo.

En el artículo 18 del proyecto se establecen las bases legales dirigidas al sector público, esto constituye tal vez una de las reformas más ambiciosas dentro del articulado y también la que probablemente ofrezca más resistencia al momento de tratarlo. En principio establece que el tratamiento de datos debe estar fundado en al menos alguno de los supuestos que conforman las bases legales del artículo 13 y que son descriptas ut supra en este mismo capítulo; al mismo tiempo "cumplir con todos los principios y condiciones que definen la licitud para el tratamiento" que establece el proyecto de ley. Para el caso de cesiones de datos, este debe realizarse mediante acuerdo entre Responsables de tratamiento (el cedente y aquel cesionario), este acuerdo debe aclarar finalidad, categoría de datos, bases legales que legitiman el tratamiento, medidas de seguridad y plazo de conservación, todo bajo la supervisión de la Autoridad de Aplicación; además ambos Responsables de tratamiento responden solidariamente ante cualquier inobservancia. El punto sobre cesiones pone sobre la mesa tanto las que proceden dentro del propio sector público, como entre éste y un privado, por lo que esta equiparación resulta más que novedosa en términos de los eternos eximentes respecto de la responsabilidad del Estado.

ESTOS SON MIS DERECHOS, EXCEPTO QUE…

Así como se describió en un párrafo anterior los derechos que asisten a los Titulares de los datos, dentro del mismo Capítulo 4 (en el artículo 34), se trata el ejercicio de estos derechos, calificándolos como "irrenunciables y nula de pleno derecho toda estipulación en contrario", aclarando, que el ejercicio de cualquiera de ellos no es requisito previo ni impide el ejercicio de otro derecho. Esto, en principio, coloca un fuerte resguardo respecto de los mismos, debiendo obtener una respuesta en un breve plazo desde haberse efectuado una intimación fehaciente, luego del cual, se habilita el trámite de protección de los datos personales ante la Autoridad de Aplicación o la interposición de la acción de Hábeas Data. Todo debe

[65] DOZO, ANASTASIA; OROVITZ, JORGE; ROSA, SOLANGE (2024) *"Protección de datos personales en la era digital: los desafíos de una actualización imprescindible"* para *"Proyecto de Ley de Protección de Datos Personales de la AAIP: diversas miradas y un consenso: la necesidad de actualizar la legislación argentina"* / Beatriz de Anchorena; Compilación de Beatriz de Anchorena. - 1a ed - Ciudad Autónoma de Buenos Aires: Ediciones AAIP, 2024. p. 37

establecerse a través de “medios y procedimiento simples, expeditos, accesibles y gratuitos”, obligación que recae en cabeza de quienes están a cargo del tratamiento.

Pero el ejercicio de los derechos descriptos encuentra limitaciones que vuelven a chocar con las funciones propias del Estado, estas son las excepciones al ejercicio de los derechos que se establecen en el artículo 35 del proyecto, mientras “sea necesario y proporcional para salvaguardar la seguridad pública, la defensa de la Nación, la protección de la salud pública y las libertades de terceros y en resguardo del interés público”. De esta forma vemos que si bien se dota de herramientas de protección en favor de los Titulares de los datos siempre se presenta el dilema de articularlo con funciones necesarias para el sector público, cuyo marco de legalidad queda plasmado en la propia ley, y si bien se destaca la obligación de brindar certeza sobre el destino, finalidad y salvaguarda de los datos, además de que estas limitaciones “deben ser las necesarias, adecuadas y proporcionales en una sociedad democrática, y deben respetar los derechos y las libertades fundamentales de las personas Titulares de los datos” siempre queda la duda razonable respecto de una implementación práctica y realista, ya que las prerrogativas del Estado, con una historia de gran peso a través de las cargas públicas tan arraigadas en Argentina, parecieran volver el ejercicio de estos derechos no tan fácilmente viables, por lo que tales cargas deberían ser objeto necesario de un análisis, discusión y posible replanteo particular de cara al futuro.

### CREO QUE ESTOY CASI SEGURO – EL PRINCIPIO DE SEGURIDAD

En el apartado de los principios incluidos en el proyecto de ley se comentó brevemente el principio de seguridad, establecido en el artículo 20 para el Responsable y el Encargado de tratamiento, que deben prever desde lo técnico y organizativo cualquier “adulteración, pérdida, uso, consulta o tratamiento no autorizado” de los datos que pudiera afectar la seguridad y confidencialidad de los mismos, detectando desviaciones de información (intencionales o no y de origen humano o tecnológico), es decir, asegura la posibilidad de establecer la trazabilidad ante una vulneración. El proyecto obliga en el desarrollo del artículo 20 a la adopción de un sistema de administración de riesgos asociados, teniendo en cuenta tanto la categoría de los datos (los biométricos en el caso de este trabajo), el volumen de recopilación y la posibilidad de riesgos inherente a los mismos, sin dejar de lado la ponderación de qué tipo de perjuicios ocasionaría en el Titular de los datos teniendo en cuenta

los incidentes de seguridad en los sistemas de tratamiento que ya se hayan registrado con anterioridad y que deben ser documentados (artículo 21).

Para poder cumplir con el principio de seguridad, entre otros, es interpretación de este análisis que necesariamente se encuentren las obligaciones de los Responsables y Encargados de tratamiento (Capítulo 5), así, debido al carácter particularmente tecnológico-dependiente que tienen los datos biométricos, se pone foco en este trabajo en el artículo 40 donde se establece la protección de datos desde el diseño y por defecto que recae en el Responsable de tratamiento, tomando en cuenta medidas tecnológicas y de organización que permitan cumplir los principios de la ley, garantizarle al Titular de los datos el ejercicio de sus derechos y la posibilidad de mitigar riesgos en el tratamiento de los datos. Según el artículo, esta aplicación preventiva debe garantizar por defecto que "solo sean objeto de tratamiento aquellos datos personales que sean necesarios para cada uno de los fines del tratamiento", del mismo modo que debe tener en cuenta el alcance del tratamiento, la garantía de que los datos no sean accesibles para un número indeterminado de personas, así como el plazo de conservación de los mismos.

IMPACTO PROFUNDO – EVALUACIÓN DE IMPACTO

La incorporación de una evaluación de impacto relativa a la protección de datos personales, pone al proyecto de ley en sintonía con la corriente tomada por leyes avanzadas como la europea, así, el artículo 41 del proyecto de ley la torna obligatoria para "evaluaciones de aspectos personales basados en tratamiento automatizado y semiautomatizado, sobre los que se tomen decisiones que afecten o provoquen efectos jurídicos sobre personas humanas" (inciso a), como el caso de la elaboración de perfiles y su alto potencial discriminatorio. De igual modo para el "tratamiento de datos sensibles a gran escala, antecedentes penales y contravencionales" (inciso b). Por último, toma la polémica "observación sistemática a gran escala de zonas de acceso público" (inciso c), utilizadas para cumplir deberes de seguridad. Esta evaluación debe contener la finalidad, el interés legítimo del Responsable de tratamiento, evaluar la necesidad y proporcionalidad respecto de sus fines, los riesgos que impliquen para los datos y las medidas de seguridad que garanticen su protección (artículo 42).

### UN NUEVO PARTICIPANTE – EL DELEGADO DE PROTECCIÓN DE DATOS

El proyecto de ley incorpora la figura del Delegado de Protección de Datos, establecido en los artículos 44 y 45; este nuevo actor con idoneidad y conocimiento para la tarea, debe informar y asesorar a todos los involucrados en el tratamiento de datos, participar del diseño y aplicación de las políticas adecuadas, tiene el rol de supervisor de la ley, forma al personal encargado de tratamiento, realiza las auditorías que sean necesarias y asesora en la realización de la evaluación de impacto, cooperando como referente de la Autoridad de Aplicación. Una potestad interesante es que ejerce sus funciones de manera autónoma, no recibe instrucciones y no puede ser destituido ni sancionado en cumplimiento de su labor. Pero seguramente, lo más innovador, es que los Responsables y Encargados de tratamiento tienen obligación de designarlo en dos supuestos: "cuando se trate de autoridad u organismo público" y "cuando el volumen, naturaleza de la actividad, alcance o finalidades del tratamiento requieran control permanente" (artículo 44).

Cabe preguntarse si la importante figura del Delegado de Protección de Datos, con un claro rol y amplias potestades de contralor de las actividades dentro de una organización, sea esta privada o pública, en la que el tratamiento de datos tenga preponderancia para sus actividades, pueda en la práctica tener allanado el camino para verdaderamente cumplir de forma acabada con sus funciones.

### EL SARTÉN POR EL MANGO – PROCEDIMIENTOS Y PODER SANCIONATORIO

Anteriormente, en este recorrido por el articulado del proyecto de ley de actualización de datos personales, se mencionó que dentro del Capítulo 4 titulado "Derechos de los Titulares de los datos", se establece el derecho de acceso a los datos (artículo 27), por lo que el Titular debe recibir información sobre sus datos, previa acreditación de su identidad, sumada al derecho de solicitar la rectificación, oposición y/o supresión. Ahora bien, ¿cómo es el procedimiento contemplado ante una vulneración? El artículo 56 establece que el Titular de los datos (o representante legal), una vez realizada una intimación fehaciente ante el Responsable de tratamiento y no haber obtenido respuesta satisfactoria (artículo 34), podrá realizar una denuncia. La Autoridad de Aplicación establecida por este proyecto que es la Agencia de Acceso a la Información Pública y Protección de los Datos Personales (artículo 53), intimará a los Responsables o Encargados de tratamiento para responder la misma. Posteriormente la propia Autoridad de Aplicación es quien emite una resolución fundada,

que en caso de considerar válido el requerimiento, insta a los mismos a "hacer efectivo el ejercicio de los derechos objeto de protección". Para el caso de violaciones a la ley, el régimen de sanciones previsto en el artículo 61, llevadas a cabo por la propia Autoridad de Aplicación, implica desde apercibimientos y multas, hasta la suspensión de actividades y cierre temporal o definitivo de las operaciones.

El poder sancionatorio que incluye el sector público, plasmado en el artículo 64 se establece que, ante un incumplimiento de la ley por parte de ese sector, la Autoridad de Aplicación puede imponer "medidas correctivas" que subsanen o mitiguen los efectos producidos. Estas ya están presentes en la vigente ley 25.326, ante infracciones a la ley las sanciones aplicables son apercibimiento, suspensión y cierre temporal o definitivo de las operaciones (resulta improbable que esto pudiese llevarse a cabo tratándose del Estado), sumada a las sanciones civiles, disciplinarias y penales de los artículos 117 bis[66] y 157 bis[67] del Código Penal de la Nación respecto de funcionarios públicos responsables.

EXPEDIENTE 1136/24-25 "MARCO NORMATIVO PARA LA PROTECCIÓN DE DATOS BIOMÉTRICOS UTILIZADOS POR APLICACIONES DE TELEFONÍA CELULAR QUE OPERAN EN LA PROVINCIA DE BUENOS AIRES"

El proyecto de ley provincial bajo el expediente D-1136/24-25-0[68] trata de dar un marco normativo para la protección de datos biométricos utilizados por aplicaciones de telefonía

[66] ARTÍCULO 117 Bis.
2. La pena será de seis meses a tres años, al que proporcionara a un tercero a sabiendas información falsa contenida en un archivo de datos personales.
3. La escala penal se aumentará en la mitad del mínimo y del máximo, cuando del hecho se derive perjuicio a alguna persona.
4. Cuando el autor o responsable del ilícito sea funcionario público en ejercicio de sus funciones, se le aplicará la accesoria de inhabilitación para el desempeño de cargos públicos por el doble del tiempo que el de la condena.
Recuperado febrero 7, 2025 de https://leyes-ar.com/codigo_penal/117%20Bis.htm

[67] ARTÍCULO 157 bis. Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que:
1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;
2. Ilegítimamente proporcionare o revelare a otro 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.
Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de un (1) a cuatro (4) años. Recuperado febrero 7, 2025 de https://leyes-ar.com/codigo_penal/157%20Bis.htm

[68] PROYECTO DE LEY PARA LA PROTECCIÓN DE DATOS BIOMÉTRICOS UTILIZADOS POR

celular que operan dentro de la Provincia de Buenos Aires, con el objeto de regular las relaciones (de consumo) entre los usuarios y los proveedores de las mismas. En principio, en su artículo 3, prohíbe a las empresas proveedoras o prestadoras de aplicaciones digitales que no cumplan los requisitos de la ley, que recolecten, manipulen, vendan y/o distribuyan datos biométricos. Entre estos requisitos (artículo 5) se estipula que los contratos de adhesión sean claros en cuanto a su redacción, términos y condiciones (artículo7) y no contengan cláusulas abusivas. La ley está claramente tratada desde la óptica de la relación consumidor – proveedor y va en concordancia con el Código Provincial de Implementación de los Derechos de los Consumidores y Usuarios, ley provincial N°13.133[69] del año 2004 que establece las bases legales para la defensa del consumidor y del usuario según los términos del artículo 38º de la Constitución de la Provincia de Buenos Aires[70].

Propone una autoridad de aplicación designada por el Poder Ejecutivo con las funciones de supervisión, control, registro y fiscalización; además de recibir y gestionar denuncias, asesorar y orientar a los usuarios sobre sus derechos (de información, de seguridad sobre sus datos, de denunciar incumplimientos) y como autoridad de aplicación de sanciones.

Como punto interesante presenta la creación específica de un Registro Provincial de Aplicaciones Digitales de Datos Biométricos (artículo 17), el cual será administrado por la autoridad de aplicación, el cual permitiría conocer la cantidad de empresas y ejercer control de la información contenida por sus bases de datos. El proyecto es noble ante la falta de una actualización de la ley N°25.326, que, al ser de alcance nacional, tendría un efecto sistematizador de mayor extensión; de cualquier modo, el proyecto de reforma de la ley

APLICACIONES DE TELEFONÍA CELULAR QUE OPERAN EN LA PROVINCIA DE BUENOS AIRES
Recuperado julio 24, 2024 de https://intranet.hcdiputados-ba.gov.ar/proyectos/24-25D1136012024-04-1116-10-44.pdf

[69] CÓDIGO PROVINCIAL DE IMPLEMENTACIÓN DE LOS DERECHOS DE LOS CONSUMIDORES Y USUARIOS Ley provincial N°13.133
Recuperado julio 24, 2024 de https://normas.gba.gob.ar/documentos/VJJalfJV.html

[70] ARTÍCULO 38.- Los consumidores y usuarios tienen derecho, en la relación de consumo, a la protección frente a los riesgos para la salud y su seguridad, a la promoción y defensa de sus intereses económicos y a una información adecuada y veraz.
Constitución Provincia de Buenos Aires (1994)
Recuperado julio 24, 2024 de https://www.infoleg.gob.ar/?page_id=173

nacional, debería incluir un registro específico como el propuesto por la Provincia de Buenos Aires, ante la proliferación de aplicaciones digitales que recolectan datos biométricos.

# CAPÍTULO VIII - DERECHO COMPARADO

Desarrollo del objetivo VI: Interpretar el tipo de normativa ya aplicada en otros países y establecer puntos de coincidencia o no con las regulaciones contempladas por el marco legal vigente en Argentina.

## INTRODUCCIÓN

A pesar del carácter muy particular de la información biométrica, el avance sobre disposiciones legales específicas a nivel mundial para su protección aún no está ampliamente difundida. Como en Argentina, los textos legales se basan en disposiciones relativas a la protección de datos personales y a la privacidad en sentido amplio, pero a veces resultan poco adaptadas a los datos biométricos. Salvo algunas excepciones.

A nivel internacional, en relación a los datos biométricos fueron pioneros los estados de Illinois y Texas en Estados Unidos al sancionar legislación que protege los datos biométricos, considerándolos sensibles y dándoles un tratamiento de especial protección, como son el Acta de Privacidad de Información Biométrica (BIPA) de Illinois, y la Ley de Privacidad Biométrica en Texas (TDPSA). En Europa, los países que conforman la Unión Europea han decidido crear una legislación comunitaria que proteja los datos y su tratamiento, en todo el territorio de la UE, sancionando el Reglamento General de Protección de Datos (Reglamento UE 2016/679) que entró en vigencia el 25 de mayo de 2018. Se procederá a analizar en concreto, el Acta de Privacidad de Información Biométrica (BIPA) de Illinois y el Reglamento General de Protección de Datos (RGPD) de la UE.

## ACTA DE PRIVACIDAD DE INFORMACIÓN BIOMÉTRICA (BIPA) DE ILLINOIS

El estado de Illinois en los Estados Unidos, fue pionero en la redacción de una ley específica sobre el tema, así, la Ley de Privacidad de la Información Biométrica de Illinois[71] o Biometric Information Privacy Act (BIPA), fue aprobada en 2008, y regula, entre varios puntos, la recopilación, almacenamiento, retención, salvaguarda, uso y destrucción de información e

[71] ACTA DE PRIVACIDAD DE INFORMACIÓN BIOMÉTRICA (BIPA) DE ILLINOIS. Recuperado julio 02, 2024 de https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57

identificadores biométricos. Cabe aclarar que está dirigida prácticamente en su totalidad a las acciones del sector privado.

DEFINICIONES, OBLIGACIONES Y DERECHOS QUE PLANTEA LA NORMA

Establecido que la biometría es biológicamente única para cada individuo, al verse afectada, no existen recursos aplicables ante el mayor riesgo de robo de identidad y otros usos ilícitos. Además, reconoce que, las ramificaciones completas de la tecnología biométrica no se conocen totalmente. Por lo tanto, el bienestar público, la seguridad y la protección de los datos se ven favorecidos mediante la regulación de la recopilación, el uso, la protección, el manejo, el almacenamiento, la retención y la destrucción de identificadores e información biométrica.

Entre las definiciones que incluye esta ley:

- ✓ "Identificador biométrico": incluye el escaneo de retina o iris, la huella dactilar, el patrón de voz o escaneo de la geometría de la mano o el rostro. Esta ley no incluye muestras de escritura o firmas, fotografías, datos demográficos o descripciones físicas. Tampoco materiales biológicos regulados por la Ley de Privacidad de la Información Genética.
- ✓ "Información biométrica" significa cualquier información, independientemente de cómo se capture, trate, almacene o comparta, según el identificador biométrico de una persona, sea utilizado para identificar a la misma.
- ✓ "Información confidencial y sensible" es toda información personal que pueda identificar de forma única a una persona o la cuenta o propiedad de una persona (es interesante que incluya ejemplos como un número de cuenta, un número PIN, un código de acceso, un número de licencia de conducir o un número de seguro social).

- Retención, recopilación, divulgación y destrucción

Debe desarrollarse una política escrita, de acceso público con un cronograma de conservación y destrucción de la información recopilada una vez cumplida la finalidad de la misma.

- Consentimiento e información

La recopilación debe ser informada previamente al individuo objeto de la misma, o su representante legal, sobre el propósito específico, el plazo de tratamiento y conservación de los datos. En caso de autorización, esta debe ser por escrito y firmada.

- Los datos biométricos quedan fuera del comercio.

- Confidencialidad

La información biométrica no puede divulgarse, excepto consentimiento expreso, en virtud de ley estatal, federal u ordenanza municipal y por orden judicial.

- Deberes para las entidades privadas que traten los datos

Utilizar un estándar razonable (de seguridad) en el almacenamiento, transmisión y protección en cuanto a la posibilidad de divulgación, esto implica una protección con un estándar equiparado o mejor que el usado para otra categoría de información confidencial y sensible.

- Derecho de acción

Queda reservado el derecho de acción ante un tribunal de jurisdicción del Estado (Illinois) para cualquier persona que resulte perjudicada por una violación a esta ley. Del mismo modo, se tendrá derecho a una demanda complementaria en un tribunal federal contra la parte infractora.

- Interpretación

Ante una acción, nada de lo dispuesto en la ley debe interpretarse en modo adverso a la admisión de información biométrica como prueba, sea en cualquier acción de cualquier tipo ante cualquier tribunal, junta, agencia o persona. Pero inmediatamente contradice lo antedicho con la excepción que presenta este punto:

"Nada de lo dispuesto en esta Ley se interpretará como aplicable a un contratista, subcontratista o agente de una agencia estatal o unidad local de gobierno cuando trabaje para esa agencia estatal o unidad local de gobierno" de esta manera deja a la ley casi en su totalidad de aplicación al sector privado.

## Caso de aplicación del Acta de Privacidad de Información Biométrica de Illinois

El *leading case* Rosenbach contra Six Flags Entertainment Corporation[72] (2019) presenta a Stacy como demandante en representación de su hijo Alexander de entonces 14 años, acusando a Six Flags Corporation de recolectar su huella digital como medio de acceso al parque de entretenimientos durante una visita al mismo en junio de 2014. Fundó su reclamo en la violación del Acta de Privacidad de Información Biométrica que prohíbe la recopilación de datos sin informar previamente y sin recibir una autorización firmada y por escrito. Six

[72] ROSENBACH v. SIX FLAGS ENTERTAINMENT Corp. 2019 IL 123186
Recuperado febrero 15, 2025 de https://www.illinoiscourts.gov/Resources/f71510f1-fb2a-43d8-ba14-292c8009dfd9/123186.pdf

Flags Corporation contestó la demanda con el argumento de que el derecho de acción (sección 20) de la ley debía ejercerse ante daño o amenaza real producida, lo que no se comprobó.

El Tribunal Supremo sostuvo que: cuando una entidad privada no cumple con los procedimientos legales "el derecho del individuo a mantener [su] privacidad biométrica se desvanece en el aire. Entonces se hace realidad el daño preciso que la legislatura de Illinois intentó prevenir" el daño es real y significativo. Una persona no necesita alegar algún daño real o efecto adverso, más allá de la violación de sus derechos bajo la Ley, para ser calificada como una persona "agraviada" y tener derecho a solicitar daños y perjuicios liquidados y medidas cautelares de conformidad con la Ley. Por lo tanto, se revocó la sentencia del Tribunal de apelaciones.

## UNA LEY DE DATOS PERSONALES PARA ILLINOIS

Al mismo tiempo en que nuestro país presentó un proyecto de ley de actualización de la ley N°25.326, un proyecto de ley (HB3385)[73] fue presentado en febrero de 2023 para crear la "Ley de Protección y Privacidad de Datos de Illinois" ya que, si bien fueron pioneros en la ley para biometría, aún carecen de una ley de datos de carácter general. Los lineamientos van en concordancia con el Proyecto de Adecuación argentino, incluyendo entre otros, el principio de minimización de datos. Al momento de redactar este trabajo, aún se encuentra sin tratamiento[74].

## UNIÓN EUROPEA: REGLAMENTO GENERAL DE DATOS (REGLAMENTO UE 2016/679)

El Reglamento General de Protección de Datos (RGPD) de los Estados miembros europeos sí aborda los datos biométricos. Esto es una diferencia, por ejemplo, del caso de Estados

[73] TEXTO COMPLETO DEL PROYECTO HB3385 (Versión en inglés)
Recuperado febrero 20 , 2025 de
https://ilga.gov/legislation/fulltext.asp?DocName=10300HB3385&GA=103&SessionId=112&DocTypeId=HB&LegID=148551&DocNum=3385&GAID=17&SpecSess=&Session=&print=true

[74] El estado de tratamiento del proyecto de ley HB3385 se puede consultar en:
https://ilga.gov/legislation/BillStatus.asp?GA=103&SessionID=112&DocTypeID=HB&DocNum=3385

Unidos donde no existe una ley federal única y completa que regule la recopilación y el uso de datos biométricos.

El RGPD de la UE establece un marco armonizado dentro de la Unión Europea, el derecho al olvido, el consentimiento inequívoco y afirmativo y, entre otras cosas, severas sanciones por el incumplimiento de estas normas. El Reglamento 2012/0011 fue adoptado oficialmente el 27 de abril de 2016.

## ANÁLISIS DEL REGLAMENTO UE 2016/679[75]

El reglamento tiene como objeto presentar los lineamientos generales en cuanto al tratamiento de los datos personales recolectados (para el caso de este trabajo, los biométricos) y proteger los derechos y libertades individuales que puedan verse involucradas durante el manejo de los datos una vez obtenidos. Sin perjuicio de lo antedicho, y aun cuando pueda parecer contradictorio en cierto punto, esta reglamentación, además, asegura la libertad de circulación de la información recolectada, la cual no puede ser "restringida o prohibida" anteponiendo "razones de protección del tratamiento de datos de los individuos". En lo referido a la aplicación material, tratado en el artículo 2, toma en cuenta los diferentes modos de tratamiento, lo cual tiene sentido de acuerdo al avance tecnológico, cubriendo tanto los automatizados, sean de manera total o parcial, como aquellos no automatizados.

### LA CARGA SOBRE LOS HOMBROS – INTERÉS PÚBLICO Y LA ACTUACIÓN DEL ESTADO

En casi todas las reglamentaciones o normativas (sea la presente, así como la de otras regiones geográficas), existe siempre una delgada línea sobre la cual se sostiene el delicado balance entre los derechos personales y la actuación del Estado en el cumplimiento de sus funciones, la carga pública que se encuentra presente para el individuo en su rol de ciudadano y, cuyo equilibrio en su aplicación, puede verse expresado con éxito dispar (el concepto de carga pública debería dejar una apertura a revisiones periódicas, debates y cuestionamientos en particular en cuanto a la función y necesidad o no de algunas de ellas, ponderando su

[75] REGLAMENTO (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (Texto pertinente a efectos del EEE)
Recuperado octubre 30,2024, de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32016R0679

verdadero fundamento y destino, así como su utilidad vigente respecto de los cambios paulatinos e inevitables del contexto social y el uso de las tecnologías por parte del Estado), para el caso de la presente normativa europea, aclara que no se aplican las regulaciones del documento cuando el tratamiento lo ejerza la autoridad competente "con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención", artículo 2[76] inciso 2 d). Los conceptos relativos a este punto se encuentran ampliados en modo particular en la "Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo"[77] y que a su vez son receptados por diferentes leyes dentro de la propia Unión Europea, como en el caso de España en su "Ley Orgánica 7/2021 de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales". (2024)[78]

El paraguas constituido por los conceptos "prevención, investigación, detección o enjuiciamiento de infracciones penales" siempre debe ser contextualizado con detenimiento para evitar vulnerar derechos de personas ajenas a los destinatarios de tal búsqueda u objetivo de aplicación. En este mismo trabajo se le da profundidad al análisis particular de los sistemas

[76] Artículo 2 UE RGDP "Ámbito de aplicación material". Recuperado octubre 30, 2024 de https://www.privacy-regulation.eu/es/2.htm

[77] Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.
Recuperado octubre 30,2024 de https://publications.europa.eu/resource/cellar/182703d1-11bd-11e6-ba9a-01aa75ed71a1.0022.03/DOC_1

[78] LEY ORGÁNICA 7/2021, de 26 de mayo, de Protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. (2024).
Recuperado octubre 31, 2024, de www.boe.es/buscar/act.php?id=BOE-A-2021-8806

de detección de prófugos basados en la lectura biométrica y la afectación de derechos que puede acarrear.

## HABLEMOS DE DEFINICIONES

Al repasar las definiciones tomadas por el reglamento de la Unión Europea (listadas en el artículo 4)[79], se constata que son las mismas en cuanto a su significado o contenido, que las que pueden encontrarse en otras leyes o reglamentaciones respecto de datos personales establecidas en diversos países como ya fue aclarado para la ley española, de hecho, las mismas han sido receptadas como fuente por algunas leyes sobre este tipo de datos, fuera de la esfera europea, que es lo que sucede en el caso de la ley vigente de datos personales argentina. Así, para el objeto del presente trabajo, podemos encontrar dentro de la definición de "datos personales" que se trata de "toda información sobre una persona identificada o identificable" y cuya identidad sea determinada a través de un "identificador", dentro de los cuales, se utilizan los elementos propios de la identidad "física, fisiológica y genética" que no es otra cosa que una primera aproximación sobre los datos biométricos que encontramos dentro del reglamento. El inciso 4) del mismo artículo 4, se centra en definir el sensible y polémico tema de la "elaboración de perfiles" que apunta al tratamiento automatizado de los datos con el fin de "evaluar determinados aspectos personales de una persona física" que incluyen, por ejemplo, la salud, el comportamiento y los movimientos de un individuo, entre algunos de los aspectos que se tienen en cuenta, los cuales deben ser analizados contextualmente, ya que involucran la posibilidad de vulnerar derechos como, por ejemplo, la libertad de movimiento (artículo 13 de la Declaración Universal de los Derechos Humanos)[80]

Dentro de este análisis de las definiciones, en el inciso 5) se encuentra un concepto interesante, a tener en cuenta como regla de tratamiento a utilizar en el manejo de los datos personales (con foco en los biométricos para el objeto de estudio del presente trabajo), se

---

[79] Artículo 4 UE RGDP "Definiciones". Recuperado octubre 30, 2024 de https://www.privacy-regulation.eu/es/4.htm

[80] ARTÍCULO 13 de la DECLARACIÓN UNIVERSAL DE LOS DERECHOS HUMANOS
1. Toda persona tiene derecho a circular libremente y a elegir su residencia en el territorio de un Estado.
2. Toda persona tiene derecho a salir de cualquier país, incluso del propio, y a regresar a su país.
Recuperado octubre 30,2024, de https://www.un.org/es/about-us/universal-declaration-of-human-rights

trata de la denominada “seudonimización”[81], que implica tratar la información obtenida de manera que ya no se la pueda atribuir a una persona física en particular. Esta técnica es fundamental, por ejemplo, en el tratamiento de datos estadísticos, ya que puede obtenerse el conjunto de datos necesario, pero sin atribuirlo a un individuo identificado o identificable.

Otro punto importante es que se encuentre incluida la definición del “consentimiento del interesado” en el inciso 11), como una herramienta de expresión de una voluntad informada por parte de la persona, de la aceptación del tratamiento de los propios datos, dejando en claro que tal manifestación debe ser para un tratamiento puntual y tiene que plasmarse de modo escrito o verbal; aunque como se analiza en este mismo trabajo, siempre debe ir acompañada de la posibilidad igualmente inequívoca de retractación absoluta como posibilidad de control sobre el manejo de los mismos. A su vez, algo que se prioriza cada vez más en muchos ámbitos es el uso de lenguaje simple y claro, por lo que los modelos de planillas para consentimiento que provengan de parte de quienes realicen el tratamiento de datos deben estar redactados siguiendo estos lineamientos y puedan ser interpretados fácilmente, sin esconder motivos ulteriores.

Para el presente trabajo, resulta de suma importancia la inclusión de la definición de “datos genéticos”- inciso 15)- ya que contempla que, a partir del análisis de material biológico, único y perteneciente a una persona en particular, se obtienen las características genéticas heredadas o adquiridas de la misma, así como gran cantidad de información sobre su fisiología o su salud, que además entra en la categoría de dato sensible. De igual manera, es central la incorporación del significado de “datos biométricos” en el reglamento, esta inclusión se ajusta a una definición clásica (ya tratada en este trabajo) en cuanto a la evaluación de “las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos”. El hecho de que no aporte nada novedoso en cuanto a la definición, no le resta mérito a que haya sido necesariamente incorporada para que se ajuste a la aplicación del reglamento.

[81] SEUDONIMIZACIÓN es una técnica de enmascaramiento de datos por la que los datos denominativos (o sensibles) son reemplazados por seudónimos. Así, un atributo sensible queda sustituido por otro de tal modo que queda protegido. Solo mediante el uso de una clave u otra información, es posible vincular de nuevo el dato denominativo con la información relacionada.
Recuperado octubre 25,2024, de https://icariatechnology.com/que-es-la-seudonimizacion-de-los-datos/

A partir del "Capítulo II" comienza el desarrollo de determinados principios para el tratamiento de los datos, así, en el artículo 5[82] se mencionan la licitud, lealtad y transparencia. En cuanto a los fines de su obtención, que sean determinados, explícitos y que tales datos sean exactos y limitados solo a los fines de su tratamiento, lo que implica el concepto de "minimización de datos" que sirve como argumento para la práctica contrapuesta que es el dragado masivo de datos con técnicas utilizadas, por ejemplo, en los sistemas utilizados en seguridad aeroportuaria y en los usados para el reconocimiento facial de prófugos.

Un acierto del reglamento es establecer un tiempo determinado de almacenamiento de los datos obtenidos -inciso e)- que solo está indicado en la extensión necesaria para el fin de su recolección, esta "limitación del plazo de conservación" como lo expresa el texto, es una medida de protección de los derechos y libertades, siguiendo el espíritu original del reglamento. Esta limitación además incluye una medida de protección de los datos, denominada "integridad y confidencialidad" ya sea ante el tratamiento ilícito (por ejemplo, que su uso no haya sido permitido por el titular de los mismos), de igual modo ante la pérdida, daño accidental o destrucción.

### TIENE MI CONSENTIMIENTO, PERO…

En el párrafo sobre definiciones del artículo 4, se estableció la correspondiente al "consentimiento del interesado", mientras que en el artículo 7[83] se determinan las condiciones para el mismo. Es interesante, que cuando el tratamiento se basa en este permiso, queda en cabeza del responsable del tratamiento la carga de la prueba del consentimiento. Por otra parte, cuando la declaración sea escrita, debe estar redactada de tal forma que quede claramente identificada que la aceptación es específicamente sobre el tratamiento, y no sobre otros asuntos, para lo cual se exige una redacción en lenguaje accesible, de otro modo será considerada ineficaz. Esto se enlaza con la facultad de retractación que posee el titular, la cual, si bien no tiene efectos retroactivos sobre los datos ya tratados, sí puede ejercerse en cualquier momento y el reglamento insta a que el procedimiento sea tan fácil para retirarlo,

[82] Artículo 5 UE RGDP "Principios relativos al tratamiento". Recuperado octubre 30, 2024 de https://www.privacy-regulation.eu/es/5.htm

[83] Artículo 7 UE RGDP "Condiciones para el consentimiento". Recuperado octubre 30, 2024 de https://www.privacy-regulation.eu/es/7.htm

así como fue para darlo. La simple mención de esta potestad tiene un inmenso poder de control, siempre y cuando concretamente el hecho de retirar el consentimiento también lleve a que sus efectos sean tan inmediatos como sea posible. Este tema se relacionará oportunamente con el modo en el que el consentimiento es manejado dentro de la ley de datos personales argentina.

Para el caso de niños, niñas y adolescentes se establece en el artículo 8 el límite de 16 años para el ejercicio lícito del consentimiento, mientras que, por debajo de esa edad, para cualquier tratamiento lícito de datos de un niño o niña, debe constar la autorización o consentimiento del encargado de la responsabilidad parental y ese permiso solo se extiende a los datos y fines específicamente autorizados para el tratamiento. Aclara, sin embargo, que cualquier Estado miembro de la Unión Europea puede llegar establecer por ley propia una edad menor, pero el límite de base inferior es de 13 años de edad.

### ALGUNOS SON MÁS IGUALES QUE OTROS – CATEGORÍAS ESPECIALES DE DATOS

En lo referente a categorías especiales de datos personales, siguiendo la línea de análisis, se tomarán los que se relacionan con el objeto de estudio del presente trabajo, por lo que en el reglamento (artículo 9)[84], se encuentra prohibido todo tipo de tratamiento de datos sobre origen étnico o racial así como los datos genéticos y los biométricos, ya que permiten la individualización de personas, lo cual puede llevar al uso de esa información para la "elaboración de perfiles" cuya definición se introdujo al hablar del artículo 4 del reglamento y cuyo fin es "evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física". La elaboración de perfiles utilizando datos personales prohibidos, constituyen una profunda violación a los derechos y libertades de las personas afectadas, no solo a la luz del reglamento que se analiza, sino que va en clara violación de Tratados y Pactos internacionales de Derechos Humanos, para el caso se cita el artículo 26 del Pacto Internacional de Derechos Civiles y Políticos que establece que:

[84] Artículo 9 UE RGDP "Tratamiento de categorías especiales de datos personales". Recuperado octubre 30, 2024 de https://www.privacy-regulation.eu/es/9.htm

*"Todas las personas son iguales ante la ley y tienen derecho sin discriminación a igual protección de la ley. A este respecto, la ley prohibirá toda discriminación y garantizará a todas las personas protección igual y efectiva contra cualquier discriminación por motivos de raza, color, sexo, idioma, religión, opiniones políticas o de cualquier índole, origen nacional o social, posición económica, nacimiento o cualquier otra condición social".*[85]

Aun así, como en casi todo cuerpo normativo, se establecen también todas las excepciones posibles basadas en el interés público, fines de medicina preventiva o laboral, salud pública y las inciertas razones de "un interés público esencial" (sobre la base de Derecho de la Unión o de los Estados parte) respetando, cuanto sea posible "un tratamiento proporcional al fin perseguido", (cuya definición de proporcionalidad no establece) y con medidas que resguarden los datos y las que protejan los intereses y derechos fundamentales del interesado en una clara contradicción con la ya establecida violación de tales derechos.

Dentro del tratamiento de las categorías de datos especiales, para el reglamento de la Unión Europea, no se incluyen a las imágenes fotográficas de forma genérica, ya que se las encuadra específicamente como técnica de captación de datos biométricos cuando sean utilizadas técnicas de identificación o de autenticación de los individuos. A criterio del razonamiento aplicado en este trabajo para el análisis de este cuerpo normativo, se incurre en un desacierto al no tomarse el tratamiento de imágenes fotográficas como de categorías especiales de datos personales, ya que, sí se concuerda en que se trata de una herramienta de recolección de datos biométricos, como lo son los rostros de las personas, pero indiscutiblemente, este instrumento es uno de los utilizados necesariamente para captar los datos faciales y sin el cual no se podría analizar las características respecto del origen étnico, color de piel y otras características visibles que permitan ejercer diferenciaciones, es decir que es uno de los instrumentos de captación visual inherente al análisis de categorías de datos especiales.

### DÉJEME SABER DE QUÉ SE TRATA – TRANSPARENCIA Y DATOS

El "Capítulo III" comienza tratando la transparencia respecto de la información obtenida, que, según el criterio utilizado en el análisis de este reglamento, constituye uno de los uno de

[85] PACTO INTERNACIONAL DE DERECHOS CIVILES Y POLÍTICOS. Recuperado octubre 28,2024, de https://www.ohchr.org/es/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

los puntos nodales para determinar si se está en presencia de una regulación que pueda ser lo suficientemente eficaz en el control que pueda ejercer el titular original de los datos biométricos. En principio, esta debe ser de acceso fácil y posible a toda la información requerida por el titular de la misma en ejercicio de su derecho a ser informado. En el artículo 13[86] se explica el tipo de información que se pone a disposición de la persona titular de los datos; esta comprende desde la identidad de todos los intervinientes en la cadena de tratamiento, la finalidad del mismo y el marco jurídico en la que se apoya la recolección de la información y el procesamiento. Del mismo modo, se le debe informar acerca de los destinatarios de los datos ya procesados, como así también si estos van a ser transferidos, y si es así, el destino de los mismos. Tal como lo establece el inciso e) del capítulo 5, debe informarse por cuánto tiempo van a ser conservados los datos o en su defecto, una estimación de cálculo del mismo. El deber de información se extiende a la posibilidad de elaboración de perfiles y en el caso de que esto ocurra o haya ocurrido, qué implicancias resultan para la persona titular de los datos.

Entonces se encuentra como idea fundamental del artículo 13 que insta a los responsables intervinientes a que deban proporcionar el acceso lo suficientemente ágil y eficiente como para poder ejercitar el derecho a rectificar, suprimir, limitar u oponerse al tratamiento de los datos, en un claro ejemplo de la posibilidad que, cualquier apropiada regulación sobre la materia, debería poner a disposición del titular original de la información recopilada y procesada sobre su propia persona.

### ¿ME LO ENVUELVE PARA LLEVAR? – PORTABILIDAD DE DATOS

Desde el inicio del presente trabajo y durante el desarrollo de los diferentes capítulos se sostiene la postura respecto de que solo existe un titular de los datos y, por lo tanto, lo asiste la totalidad de los derechos que aseguren su control en todos los aspectos en los cuales sea posible ejercerlo. En este capítulo en particular, en el que se analiza una de las bases de la normativa europea respecto de los datos personales (y como ya se estableció, con foco en los biométricos) en el capítulo 20[87] se encuentra desarrollado otro tema fundamental para el

[86] Artículo 13 UE RGDP "Información que deberá facilitarse cuando los datos personales se obtengan del interesado" Recuperado octubre 30, 2024, de https://www.privacy-regulation.eu/es/13.htm

[87] Artículo 20 UE RGDP "Derecho a la portabilidad de los datos"
Recuperado octubre 30, 2024, de https://www.privacy-regulation.eu/es/20.htm

control de los propios datos y es la portabilidad de los mismos. El responsable del tratamiento debe entregar, a solicitud del titular que inicialmente prestó su consentimiento, la totalidad de los datos recolectados y tratados de modo que sea fácilmente transmisible, si esto fuera requerido, a otro responsable de tratamiento "en un formato estructurado, de uso común y lectura mecánica" o, en su defecto, transmitírselo directamente a este último cuando sea posible técnicamente. Un punto que cabe preguntarse es por qué la reglamentación no aclara qué sucede con aquellos titulares que no han consentido previamente la recolección de sus datos y desean recuperarlos de parte de los responsables del tratamiento.

Y como en otros artículos del reglamento, se establecen las excepciones, ya sean amparadas en el cumplimiento del interés público o en el ejercicio de poderes públicos otorgados al responsable del tratamiento. Pero, aun así, persiste el ejercicio del derecho a oposición al tratamiento de sus datos por parte del titular, y se pone en cabeza del responsable del tratamiento la demostración o prueba que tales motivos prevalecen sobre los derechos y libertades fundamentales del individuo; claro está, que se presenta nuevamente la contraposición de ambas legitimaciones, entre estos derechos individuales, y la carga pública o el ejercicio de los poderes públicos.

### A SEGURO SE LO LLEVARON PRESO – PROTECCIÓN DE LOS DATOS – SEGURIDAD DEL TRATAMIENTO

En el artículo 25[88] del Reglamento se trata la Protección de datos desde el diseño y por defecto. Las variables a considerar sobre el tratamiento de datos engloban entre otras, a la técnica, el contexto, la finalidad y los riesgos potenciales que afecten los derechos y libertades de los individuos (ya en el artículo 22[89] se establece que ante el tratamiento automatizado, el responsable debe tomar medidas de protección de los derechos, libertades e intereses legítimos del titular de los datos), para lo cual deben adoptarse medidas preventivas garantizadas, como la seudonimización y la minimización de los datos y que solo sean tratados aquellos necesarios para las finalidades especificadas, a la cantidad de información recolectada, al tiempo requerido tanto para su tratamiento como para la conservación de la

[88] Artículo 25 UE RGDP "Protección de datos desde el diseño y por defecto"
Recuperado octubre 30, 2024, de https://www.privacy-regulation.eu/es/25.htm

[89] Artículo 22 UE RGDP " Decisiones individuales automatizadas, incluida la elaboración de perfiles"
Recuperado octubre 30, 2024, de https://www.privacy-regulation.eu/es/22.htm

misma, garantizando siempre la accesibilidad por parte del titular, pero no por parte de terceros indeterminados.

Dentro del artículo 32, continúan las obligaciones por parte del responsable del tratamiento de datos, como el hecho de ser capaz de garantizar la confidencialidad e integridad de los mismos, poder "restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico", evaluar regularmente tanto la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento como los riesgos potenciales, ya sea desde la destrucción o pérdida, la alteración de los mismos, tanto de modo accidental como de naturaleza ilícita y finalmente la protección ante el filtrado o acceso desautorizado al almacenamiento o banco de datos.[90]

¿Pero qué sucede ante una violación de seguridad?

El responsable del tratamiento debe notificar a la autoridad de control competente, pero, ¿cuál es? Si el tratamiento es realizado por autoridades públicas o por organismos privados que cumplan una obligación legal, en interés público o en el ejercicio de poderes públicos que le fueron otorgados, será competente la autoridad de control del Estado miembro de que se trate. Es importante destacar también que las autoridades de control no son competentes para controlar las operaciones de tratamiento efectuadas por los tribunales en el ejercicio de su función judicial.

Esta notificación debe ser dentro de las 72 horas, describiendo la naturaleza de la violación, si es posible, las categorías y el número aproximado de interesados y de registros afectados y las posibles consecuencias de la violación de la seguridad de los datos personales; documentando los efectos y las medidas de corrección tomadas.[91]

### USTED ES LA CULPABLE, DE TODAS MIS ANGUSTIAS…- RECURSOS, RESPONSABILIDAD Y SANCIONES

De acuerdo a lo establecido en el artículo 79[92] del Reglamento, sin perjuicio de los recursos (administrativos o extrajudiciales) que tiene derecho a presentar el interesado, también tendrá derecho a la tutela judicial efectiva cuando considere que sus derechos hayan sido vulnerados

[90] Artículo 32 UE RGDP " Seguridad del tratamiento"
Recuperado noviembre 03, 2024 de https://www.privacy-regulation.eu/es/32.htm

[91] Artículo 77 UE RGDP "Derecho a presentar una reclamación ante una autoridad de control"
Recuperado noviembre 03, 2024 de https://www.privacy-regulation.eu/es/77.htm

[92] Artículo 79 UE RGDP " Derecho a la tutela judicial efectiva contra un responsable o encargado del tratamiento". Recuperado noviembre 03, 2024 de https://www.privacy-regulation.eu/es/79.htm

como consecuencia del tratamiento de sus datos personales, esto es, a través de acciones ante los tribunales del Estado miembro en el que el responsable o encargado tenga un establecimiento. Pero, una vez más, se presenta la limitación al presentar cualquier acción, si el responsable o el encargado es una autoridad pública de un Estado miembro que actúe en ejercicio de sus poderes públicos.

Y en cuanto al derecho a indemnización y responsabilidad tratado en el artículo 82 ante daños y perjuicios (materiales o inmateriales) sufridos como consecuencia de una infracción del Reglamento toda persona tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización. Responde cualquier responsable que participe en la operación de tratamiento siempre en caso de que dicha operación no cumpla lo dispuesto por el Reglamento (queda en cabeza del mismo demostrar si el daño sufrido no fue por un hecho de su responsabilidad). Si hay más de un responsable o encargado para un mismo tratamiento, cada uno de ellos será considerado responsable de todos los daños y perjuicios, más allá de las acciones de repetición que surjan entre ellos. La competencia del tribunal corresponde al Derecho del Estado miembro donde se produjo el daño.

## CAPÍTULO IX – JURISPRUDENCIA

JURISPRUDENCIA COMPARADA

CASO STATE OF NEW JERSEY v. FRANCISCO ARTEAGA

A continuación, se presenta un caso de jurisprudencia comparada en el que el rol de la tecnología de reconocimiento es protagónico, no por el concepto de la técnica en sí, sino porque la escasa fiabilidad de los métodos de captura hace que el respectivo análisis resulte altamente deficiente y forzado en la búsqueda de un objetivo que lleva a la posible aplicación de un sesgo y definitivamente en la vulneración de un derecho individual.

**"State of New Jersey v. Francisco Arteaga"** Defendant- Appellant (Causa N°A-3078)[93]

Tribunal Superior de New Jersey (Law Division, Hudson County, Indictment No.21-01-0035).

Jueces: Whipple, Mawla, and Walcott-Henderson. Fecha de Decisión: 7-junio-2023

El 29 de noviembre de 2019 ocurrió un robo a una tienda en West New York. Una de las empleadas describió al presunto autor como un "hombre hispano usando un gorro tejido negro y con un arma". La gerente de la tienda Judy Cardozo, quien no estuvo presente al momento del hecho, creyó reconocer a la persona luego de ver las cámaras de seguridad. Esta información fue utilizada por los detectives que recuperaron las grabaciones de las cámaras de vigilancia del local y las de una propiedad cercana y usaron esas filmaciones para generar una imagen fija (fotografía) de baja calidad que fue enviada al Centro de Inteligencia de Operaciones Regionales de Nueva Jersey (NJROIC "New Jersey Regional Operations Intelligence Center") **para su análisis a través del uso de tecnología de reconocimiento facial**. Personal de **la NJROIC informó que no existían coincidencias entre la imagen generada por los detectives y su base de datos, ya que necesitaban una imagen de mejor calidad**.

Aun así, los detectives enviaron todas las imágenes de vigilancia obtenidas al Sector de Identificación Facial del Centro de Delincuencia en Tiempo Real del Departamento de

[93] ESCUELA DE LA DEFENSA PÚBLICA – REPOSITORIO
Recuperado octubre 20, 2024 de
https://repositorio.mpd.gov.ar/jspui/bitstream/123456789/4713/1/SUPERIOR%20COURT%20OF%20NEW%20JERSEY.%20ARTEGA.pdf
TEXTO ORIGINAL DEL FALLO en idioma inglés.

Policía de Nueva York (NYPD RTCC "Facial Identification Section of the New York Police Department Real Time Crime Center"). Una "imagen fija" seleccionada por los investigadores fue comparada con la base de datos del centro y **sugirió a Francisco Arteaga como "posible coincidencia"**. Con ese dato se generaron las matrices fotográficas para que sean vistas por los testigos, quienes identificaron a Arteaga como el autor del delito.

Su defensa, fundándose en la declaración de un experto en tecnología de reconocimiento facial en la que se explicaba los principales problemas de fiabilidad de ese tipo de tecnología, solicitó de manera inteligente, un número de pruebas que, cabe resaltar que, **para el objeto de este trabajo, también representan un excelente resumen de la mayor parte de las DUDAS Y CUESTIONAMIENTOS que en general se plantean frente al uso de tecnologías de reconocimiento,** así, entre otras cuestiones:

1. El nombre y el fabricante del software de reconocimiento facial utilizado, **el número de versión y el año de desarrollo de los algoritmos**.

2. El **código fuente de los algoritmos** de reconocimiento facial;

3. Una **lista de las mediciones, puntos nodales u otras marcas de identificación únicas que utiliza el sistema para crear vectores de características faciales.**

4. Las **tasas de error para el sistema de reconocimiento facial utilizado, incluidas las tasas de falso positivo y falso rechazo.**

5. El **rendimiento de los algoritmos utilizados en las pruebas de proveedores de reconocimiento facial aplicables**, si están disponibles;

6. **La copia original de la foto de consulta o "investigación"** enviada a la Sección de Identificación Facial del Centro de Delitos en Tiempo Real;

7. Todas las copias **editadas** de la foto de consulta o "investigación" enviadas al sistema de reconocimiento facial.

8. Una copia de la foto de la base de datos que coincida con la foto de consulta o "investigación" y el porcentaje de coincidencia en la lista de candidatos;

9. Una lista **los puntajes de confianza producidos por el sistema, incluida la escala en la que se basa el sistema (por ejemplo, porcentaje, logarítmico, otro**);

10. Una **copia de la lista completa de candidatos devuelta por el reconocimiento facial** o los primeros [veinte] candidatos en la lista, en orden de clasificación e incluyendo el porcentaje de coincidencia asignada a cada foto por el sistema de reconocimiento facial;

11. Una **lista de los parámetros de la base de datos utilizada**, incluyendo: a. **Cuántas fotos hay en la base de datos**; b. **Cómo se obtienen** las fotos; c. **Cuánto tiempo se almacenan** las fotos; d. **Con qué frecuencia se purga la base de datos**; e. **Cuál es el proceso para ser eliminado** de la base de datos; f. **Quién tiene acceso** a la base de datos; g. **Cómo se mantiene** la base de datos; h. **La Política de privacidad** de la base de datos;

12. **El informe elaborado por el analista** o técnico; y

13. La **formación, certificaciones o calificaciones del analista** que ejecutó la consulta.

El tribunal rechazó el pedido explicando que la fiscalía no tenía la obligación de producir la información solicitada por la defensa, porque el sistema de reconocimiento facial no estaba bajo su cuidado, custodia o control. Por lo cual, la defensa interpuso un recurso de apelación. El Tribunal Superior de Nueva Jersey hizo lugar al recurso, revocó lo resuelto por el tribunal y ordenó a la fiscalía que provea la información solicitada. Argumentó que:

"**La prueba que se busca está directamente vinculada a la capacidad de la defensa para probar la fiabilidad de la Tecnología de Reconocimiento Facial (Facial Recognition Technology, FRT)**".

"El Tribunal no está convencido de que el Centro de Delincuencia en Tiempo Real del Departamento de Policía de Nueva York no formara parte del equipo de la acusación. Esto porque el fiscal envió una solicitud a la NYPD RTCC cuya respuesta fue utilizada como elemento de acusación de Arteaga." **Con este argumento conecta a la fiscalía con el uso del sistema de reconocimiento facial, ya que de otro modo no habría conseguido la prueba utilizada**".

"El Estado sostiene que no es que no pudo obtener la información adicional (datos utilizados para entrenar el RFT y la evaluación de la fiabilidad de los métodos) solicitada por la defensa, ya sea por razones de propiedad intelectual o de otro tipo, sino que la presentación de esa información le corresponde al acusado y no a él. **Rechazamos esta afirmación porque la carga de la prueba recae en el Estado toda vez que la FRT resulta novedosa y no ha sido probada o encontrada confiable por ninguna corte de Nueva Jersey**".

En cuanto al Sistema de Reconocimiento Facial y la Protección de datos personales, La FRT puede detectar un rostro humano dentro de una imagen. Utiliza un algoritmo para realizar el análisis, que reconoce ´puntos nodales´[94] (**En el presente trabajo se realiza mención de los mismos al desarrollar el método antropométrico facial, desarrollado principalmente por Alphonse Bertillon en el siglo XIX)** y su comparación con los rasgos correspondientes en imágenes seleccionadas.

**A los fines de este trabajo, este fallo pone en evidencia que, la tecnología de análisis no está a la par con la menor evolución de algunos dispositivos utilizados en la captura de los datos, en este caso, la calidad de resolución de las cámaras de seguridad ampliamente diseminadas en el uso de seguridad "doméstica-comercial",** como lo expresa el Tribunal de Apelaciones: Las imágenes de menor calidad pueden editarse para corregir la iluminación o el color, para mejorar los detalles o incluso para cambiar la expresión facial. Luego, la tecnología descompone la imagen en rasgos componentes y los destila en una ´huella facial´, **lo que a menudo se traduce en un bajo rendimiento en el análisis de rostros no blancos**. […]. Además, la calidad de una imagen de sondeo, incluida su resolución, iluminación ambiental y expresión facial […], así como el alcance de cualquier edición realizada en ella […] **pueden afectar a la precisión de la ´huella facial´ resultante.**

Y esto conlleva a un efecto cascada, así el Tribunal expone: "Consideramos que la solicitud de revelación de la FRT es relevante para la capacidad del acusado de impugnar la identificación y la investigación, y su capacidad general de establecer una duda razonable en el juicio. **La fiabilidad de la FRT tiene implicaciones obvias para la exactitud del proceso de identificación, porque una rueda construida en torno a una coincidencia potencial errónea dejaría al testigo sin un autor real para elegir**.

A continuación, el Tribunal expresa con gran sentido común: "A medida que prolifera la tecnología, también lo hace su uso en los procesos penales. Los tribunales deben esforzarse

[94] PUNTOS NODALES "Los 22 puntos de interés son: iris izquierdo, iris derecho, punta de la nariz, fosa izquierda, fosa derecha, puente nasal, comisura izquierda del labio, comisura derecha del labio, labio superior, labio inferior, entrecejo, ceja izquierda-lado derecho, ceja izquierda-centro, ceja izquierda-lado izquierdo, ceja derecha-lado izquierdo, ceja derecha-centro, ceja derecha-lado derecho, oreja izquierda, oreja derecha, mandíbula lado izquierdo, mandíbula lado derecho y mentón".
GONZÁLEZ, A., & PRIETO, F. (2011). Extracción de puntos característicos del rostro para medidas antropométricas. Revista Ingenierías Universidad De Medellín, 9(17), 139–150.
Recuperado octubre 20, 2024 de https://revistas.udem.edu.co/index.php/ingenierias/article/view/172

por comprender la nueva tecnología… y permitir a la defensa una oportunidad significativa para examinarla. **Sin examinar el código fuente de su software –un conjunto de instrucciones hechas por el hombre que pueden contener errores, fallos y defectos– en el contexto de un sistema acusatorio, no se podría llegar a la conclusión realista de que implementa adecuadamente la ciencia subyacente. En consecuencia, es imperativo permitir un examen significativo del código fuente, que obliga al análisis crítico independiente necesario para que un juez haga una determinación de umbral en cuanto a la fiabilidad** en una audiencia […]"[95]. Por lo que "El acusado debe tener las herramientas para impugnar el caso del Estado y sembrar la duda razonable. Por estas razones, revocamos y devolvemos el caso para que se dicte una orden que ordene al Estado proporcionar los once elementos de prueba restantes solicitados por la defensa".

CONCLUSIÓN DEL ANÁLISIS

Históricamente, la aplicación de las tecnologías de reconocimiento siempre ha mostrado debilidades y márgenes de errores a la hora de su aplicación. Un sistema de identificación consta de un conjunto de factores técnicos que deben funcionar a la par, pero cuando estas condiciones no se dan, la obtención de la posible prueba inicial desvirtúa cualquier análisis posterior. Sumado a ello, la existencia de sesgos provenientes del componente humano hace que una herramienta potencialmente útil termine siendo un forzado instrumento de daño a los derechos de los individuos erróneamente afectados.

[95] ESCUELA DE LA DEFENSA PÚBLICA – REPOSITORIO
Recuperado octubre 20, 2024 de https://repositorio.mpd.gov.ar/jspui/handle/123456789/4713

## CAPÍTULO X - SOLUCIONES ALTERNATIVAS O ACCESORIAS – Biometría y otros caminos

Una de los grandes temas respecto del uso de la tecnología biométrica es que, para llevar a cabo la comparación del dato de la persona, esta debe realizarse con un dato previamente obtenido y almacenado, de ahí que se genere toda la problemática, tecnológica y legislativa, apuntando hacia la regulación y el control de las bases de datos centralizadas, para aumentar los grados de seguridad y confidencialidad. Pero en los últimos años, a la par de todo este desarrollo, se continuó mejorando la tecnología aplicada a soportes ya existentes. En este trabajo se presenta el ejemplo de uno de ellos.

### NO SOY SOLO UN PEDAZO DE PLÁSTICO

Existen muchos tipos de tarjetas inteligentes, las que funcionan con un pin o chip de capacidad mínima y limitada a su función, pero la tecnología evolucionó hacia otro tipo de tarjetas más complejas y completas, las cuales también pueden incluir información biométrica, pero en la cuales, esta se maneja de un modo diferente. La seguridad de este tipo de soportes se basa en un algoritmo llamado Match-on-card, que hace que este sistema se diferencie de los procedimientos habituales de comparación biométrica, porque esta evaluación se realiza dentro del propio espacio físico de la tarjeta, a través de un microprocesador integrado en la misma, y, que sirve de banco de datos situado localmente, además, incluye un lector de huella dactilar, por lo que la tarjeta es personal y se activa a través de la huella del titular de los datos previamente almacenada en la propia tarjeta (similar al desbloqueo por huella de muchos celulares). De este modo, la información queda protegida y por fuera de lo que podría provocar un hackeo o filtración de una base de datos centralizada, ya que los datos no abandonan la tarjeta, y, en caso de extravío o robo, no podría desbloquearse sin la huella del titular de la misma[96]. Otra ventaja que provee es que los datos no pueden ser interceptados, como en los casos actuales al momento de realizar la transferencia a un lector externo. Claramente, los estándares de calidad respecto del

[96] BIOMETRICS: DEFINITION, USE CASES, LATEST NEWS
Recuperado febrero 12, 2025 de https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics

microprocesador, su capacidad de almacenamiento, el sistema operativo utilizado y el lector incorporado, deben ser sumamente altos y seguros.

PORTUGAL PICA EN PUNTA

Uno de los casos de aplicación emblemático es Portugal y su tarjeta nacional de identidad, aplicada desde 2007[97]. Entre varias medidas de seguridad incluye el sistema Match-on-card, pero con un paso más, las huellas leídas desde las tarjetas, por cualquier sistema, una vez que fuera identificada la persona, se destruyen (cumple el principio de finalidad de manera inmediata). El sistema utilizado por la tarjeta se diferencia, como se expuso en el párrafo anterior, y durante todo el trabajo, de los procedimientos que utilizan tecnología biométrica tradicional, con recolección previa y almacenamiento central en un banco de datos, por lo que, al realizar una verificación de identidad, la huella escaneada se compara con la previamente obtenida y guardada en esta base.

Específicamente en el caso portugués, ya pasa a ser una tarjeta ciudadana completa, simplificando tiempo en la interacción con los diferentes requerimientos del Estado, ya que, al tener alta capacidad de almacenamiento, permite guardar los datos de otro tipo de documentación; de este modo, cumple funciones de D.N.I, de credencial fiscal, de tarjeta de votación, de tarjeta de salud y de carnet de la seguridad social[98]. Además, desde junio de 2024, cumple con las normas de seguridad de la Organización de aviación Civil Internacional y la Unión Europea, por lo que puede usarse como documento da viaje válido tanto para los Estados parte de la UE como dentro del espacio Schengen[99]. Otro de los usos que permite la tarjeta es el de token para la firma electrónica y para la autenticación en línea para el caso de

[97] BIOMETRICS WITH STRICT CONFIDENTIALITY. THE PORTUGUESE EXPERIENCE
Recuperado febrero 17, 2025 de https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics/portugal

[98] CARTÃO DE CIDADÃO
Recuperado febrero 22, 2025 de https://buenosaires.embaixadaportugal.mne.gov.pt/es/seccion-consular/documentos/cartao-de-cidadao

[99] ESPACIO SCHENGEN
Es un acuerdo dentro de la UE que forma **un espacio sin controles en las fronteras interiores** supone que los países:

- no efectúen controles en sus fronteras interiores, excepto en caso de amenazas específicas;
- lleven a cabo controles armonizados en sus fronteras exteriores conforme a unos criterios claramente definidos.

Recuperado febrero 22, 2025 de https://www.consilium.europa.eu/es/policies/schengen-area/

transacciones electrónicas, esto sí va acompañado del uso de un código personal que la valide[100].

REFLEXIONES

El ejemplo presentado lleva al menos a pensar en la utilización de manera paralela o accesoria, de mecanismos que no impliquen una centralización de datos masiva, con los costos de seguridad, control y riesgos que esto conlleva. Los sistemas descentralizados como las tarjetas inteligentes u otros dispositivos, no significa que eliminen cualquier tipo de riesgo, pero si lo llevan a una escala menor. Además, este tipo de sistemas, presentan una característica que los pone en ventaja respecto de otros: el hecho de que la información está en posesión del Titular y su uso personal asegurado por las medidas biométricas que contiene, el control le pertenece, por lo que su información deja de requerir una base de datos externa y con responsables ajenos, que es el obvio factor de la construcción de todo un andamiaje tecnológico y normativo en pos de prever y morigerar los riesgos y potenciales perjuicios que ello conlleva.

[100] eID since 2007: PORTUGAL'S CITIZEN CARD
Recuperado febrero 18, 2025 de https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/portugal-id

# CONCLUSIONES

Sobre los objetivos específicos planteados para este trabajo:

**I. Describir las diversas metodologías de recolección, almacenamiento y utilización de la información de fuente biométrica, su evolución y estado actual.**

Como se planteó al inicio del trabajo, la identidad propia de una persona unida al concepto de identificación y al hecho de poder ser individuados por otros es un interés tanto propio como de terceros, que tiene su génesis en nuestra naturaleza social y la búsqueda de pertenencia. Esto hizo que históricamente se hiciera evidente que algunas de nuestras características, propias y únicas, nos diferenciaran claramente de otros.

El uso de la tecnología biométrica sistematizada nos acompaña aproximadamente desde hace dos siglos, y este camino fue acompañado de las antiguas técnicas modernizadas junto con las nuevas, potenciadas en los últimos años por un nivel tecnológico a escalas poco imaginadas en el pasado. Desde la curiosidad inherente al hombre y que siempre lo impulsó a tratar de descubrir el porqué de las cosas, hasta la aplicación de esos descubrimientos a la resolución de situaciones prácticas unidas a la oportunidad de satisfacer la pulsión del ejercicio de control sobre los otros, la evolución histórica de los diferentes métodos de recopilación biométrica deja en evidencia una línea de seguimiento en la que a medida que avanza la eficacia de los procesos tecnológicos de recolección con la finalidad de identificar a un individuo, mayor es la cantidad de información obtenida del sujeto y, por lo tanto, más completo es el mapa general que resulta del mismo, ya no solo incluyendo sus particularidades físicas intrínsecas, sino las que le son propias a una persona en el modo de interactuar con el mundo que lo rodea. Este formato de registro de modalidad que derivó, con el tiempo, en múltiples sistemas, permite en la actualidad tener finalmente un perfil cada vez más acabado y preciso que, luego de su procesamiento, derivará en la obtención de un código que permitirá, por lo menos en la teoría, una futura comparación identificatoria con un margen de error cada vez menor. Pero como ya se dijo en el desarrollo de este trabajo, en tecnología, así como en ciencia aplicada, no existe el concepto ni de cien (100) por ciento como totalidad, ni de cero (0) absoluto como ausencia, por lo que la reducción del error, nunca implicará una total e inequívoca certeza, aun cuando la tecnología sea cada vez más sofisticada y veloz.

**II. Determinar la importancia del manejo regulado, controlado y seguro de la información obtenida por su relación con los derechos personalísimos de los individuos.**

Como este trabajo intenta ser objetivo, es innegable que la tecnología es una gran aliada para nuestras vidas, nos facilita muchas acciones que deben estimarse en el ahorro de un valor tan esencial como es el tiempo. Del mismo modo, los avances bien aplicados deberían estar enfocados en brindar a los individuos y a la sociedad un mayor nivel de confort y seguridad, pero este logro no debería comprometer derechos imperativos, como los personalísimos o los fundamentales. Un enfoque regulatorio correcto sobre esta temática, debe tener como foco principal la tutela de la persona, más allá de que por la propia naturaleza tecnológica de la problemática, la metodología de una normativa se enfoque en una estructura más técnica, no es el resultado digitalizado ni el dato en sí lo que se protege, sino los derechos y principios que son insoslayables, y que dada la condición invasiva de los datos biométricos (en el sentido que analizan cada uno de los caracteres únicos de un individuo), deben considerarse como estrechamente ligados a los atributos de la personalidad, por tal motivo, entran sin duda alguna en la categoría de derechos personalísimos y su manejo es el que definirá qué tipo de consecuencias traiga al individuo del que se lo extrajo, tanto en su esfera privada como en su esfera pública, por ejemplo, su intimidad, su honor, su dignidad, el propio cuerpo, el derecho al trato no discriminatorio y a la autodeterminación informativa, es decir, conocer qué puede afectar el conjunto de las libertades individuales de su persona. Una normativa correcta, no solo actúa como barrera preventiva, garantizando los controles y evaluaciones necesarias, sino que provee de las herramientas para la reparación ante la afectación de los derechos; aun cuando el tratamiento y procesamiento de los datos se acerque peligrosamente a la codificación de un objeto, de un producto, de una cosa, el legislador nunca debe olvidar que tras ese código se encuentra concentrado un ser que debe protegerse ante cualquier vulneración y por lo tanto, ser objeto de la suficiente tutela por parte de la norma para que la misma tienda a garantizar los posibles beneficios y a prevenir o morigerar los potenciales riesgos.

**III. Investigar el manejo no regulado y no consentido de datos biométricos por parte de agentes públicos o privados y las consecuencias de tales acciones. Establecer los alcances sancionatorios ante tales supuestos.**

Es así, que los sistemas normativos deban estar actualizados y abiertos a receptar modificaciones, las grandes ventajas que tiene el uso de tecnología biométrica, es también la

puerta de entrada a sus desventajas. La fuente del sistema son nuestros datos únicos e irremplazables por lo que el manejo no regulado lleva a ocasionar perjuicios más profundos que los de la pérdida de una tarjeta de acceso o el hackeo de una clave alfanumérica. La ausencia de los controles adecuados sobre el propio sistema tecnológico, como de los intervinientes humanos en el mismo, puede favorecer prácticas ilícitas, como la recopilación sin consentimiento previo (cuando sí sea necesario) o sin conocimiento por parte del futuro individuo afectado; la filtración de datos, pero con una vulneración potenciada al estar conectados a nuestros derechos personalísimos (como ya fue establecido durante el trabajo) provocando potenciales casos de usurpación de identidad, fraude o cualquier otro perjuicio económico o social relevante y la propia acción no regulada del Estado como en el desarrollo de los ejemplos SIBIOS y SRFP; ante estos casos, la norma debe contemplar la posibilidad concreta de obtener una trazabilidad por parte del Titular de los datos, para poder obtener las pruebas que le permitan ejercer de manera efectiva su derecho de defensa llegado el momento necesario. Para el caso los responsables de tratamiento, la ley necesita una actualización seria en término de sanciones pecuniarias y para el ejemplo presentado de filtraciones en el RENAPER, debe hacerse extensivo a toda dependencia pública, para un funcionario con acceso al sistema, caben las efectivas sanciones penales ya dispuestas por los artículos 117 bis y 157 bis del Código Penal; sin embargo, debe ser reforzada la aplicación sancionatoria respecto de los organismos y su negligencia en la falta de control, la cual debe ser primordial como responsables de tratamiento de datos en el sector público.

**IV. Analizar la aplicación de políticas de seguridad pública basadas en el uso de identificación por tecnología biométrica y la posible existencia de principios y derechos lesionados.**

En la utilización de políticas de seguridad, a nivel nacional como internacional, el mencionado perfilado de individuos por condenas e infracciones penales y cualquier otra búsqueda que implica el escaneo masivo de personas y su posterior tratamiento para ser filtrados, involucra un gran volumen de datos personales que pueden afectar a un enorme volumen de individuos ajenos al objeto de la búsqueda. Estos daños son potenciales consecuencias de prácticas que se han analizado, como la focalización en determinados orígenes étnicos y cualquier otra característica visualmente notoria que se encuentre por fuera de un patrón de referencia limitadamente estandarizado que responde a entrenamientos de los motores de búsqueda con sesgos incorporados en la propia matriz por los encargados de

entrenarlos. Esto constituye una clara violación del derecho de igualdad, como en el caso de la elaboración de perfiles, o por el tratamiento de categorías especiales de datos biométricos o datos sobre condenas e infracciones penales y que resulte en actitudes de discriminación por la puesta en práctica de ciertas políticas públicas. Todo esto sin dejar de lado los niveles de fiabilidad que puedan ser cuestionados, y que fueron ejemplo en la fundamentación de la suspensión del Sistema de Reconocimiento Facial de Prófugos presentada en este trabajo.

**V. Evaluar la normativa existente en nuestro país y su extensión concreta en cuanto a la protección de datos de origen biométrico. Ver en paralelo el alcance de los proyectos de adecuación nacionales existentes.**

El cuerpo original de la ley 25.326 no hace referencia a los datos biométricos, los cuales son incorporados como definición recién en 2019 a través de los criterios orientadores de aplicación de la ley, en la Resolución 4/2019 y el Anexo I, pero no se plantean cuestiones de fondo sobre los mismos, esto es subsanado en el Proyecto de Actualización, incorporándolo desde un comienzo al cuerpo principal. Respecto de las bases de datos, la ley actual aclara que deben adoptarse medidas técnicas y organizativas que garanticen la seguridad y el resguardo, pero no establece ninguna especificación sobre qué medidas tomar, en el Proyecto de Actualización de la Ley esto se refuerza incorporando en el artículo 39 las medidas para el cumplimiento del principio de responsabilidad proactiva, con la adopción de procesos internos efectivos, procedimientos que atiendan el ejercicio de los derechos de los Titulares de datos, control interno del cumplimiento a través de supervisiones o auditorías (internas o externas) y el uso de procedimientos que permitan una evaluación de impacto (EDI), este último, adoptado internacionalmente como instrumento fundamental de casi todas las leyes de avanzada en la temática, la ley N°25.326 no contempla el concepto de Evaluación de Impacto, mientras que el Proyecto de Actualización lo incorpora explícitamente, estableciendo su obligatoriedad en determinados casos. Cabe aclarar que la la Agencia de Acceso a la Información Pública (AAIP) y la autoridad de control uruguaya (URCDP) redactaron una guía muy completa, pero como tal, no tiene el peso de una norma y sí una destacada utilidad en el seguimiento de criterios orientadores, los cuales van a ser un instrumento imprescindible para trabajarlo en conjunto con una nueva y actualizada ley sobre la temática.

En cuanto las bases legales de la ley actual, tiene al consentimiento como supuesto principal, algo que el Proyecto de reforma de 2023 amplía agregando las bases legales necesarias para

ejercer y cumplir las funciones y facultades propias de los poderes del Estado, la existencia de un interés legítimo por parte del Responsable del tratamiento (con un análisis documentado) respetando el principio de minimización de datos y siguiendo criterios de proporcionalidad y razonabilidad. El cumplimiento de obligaciones legales específicas para el Responsable del tratamiento en el proyecto de ley se presenta como una evolución respecto de la obligación legal que se encuentra vigente en la ley 25.326 en su artículo 5 pero como una excepción al consentimiento y sin especificación alguna.

Una gran diferencia entre la ley vigente y el Proyecto de Actualización se constata en lo referido al sector público; así las excepciones siempre presentes respecto del Estado en "ejercicio de las funciones propias de sus poderes" encuentran limitaciones, ya que, el tratamiento de datos debe estar fundado en al menos alguno de los supuestos que conforman las bases legales del proyecto, cumplir con todos los principios y condiciones que definen la licitud para el tratamiento y para el caso de cesiones de datos hace más evidente la equiparación, ya que ambos Responsables de tratamiento responden solidariamente ante cualquier inobservancia (las cesiones que proceden dentro del propio sector público, como entre éste y un privado) resultando más que novedosa en términos de los límites a los eximentes respecto de la responsabilidad del Estado.

Pero el punto necesario de interpretación es el rol del principio de necesidad y proporcionalidad presente en el Proyecto de Actualización, por ejemplo, excepciones al ejercicio de ciertos derechos, mientras "sea necesario y proporcional para salvaguardar la seguridad pública, la defensa de la Nación, la protección de la salud pública y las libertades de terceros y en resguardo del interés público". De esta forma vemos que si bien se dota de herramientas de protección en favor de los Titulares de los datos siempre se presenta el dilema de articularlo con funciones necesarias para el sector público, cuyo marco de legalidad queda plasmado en la propia ley, y que estas limitaciones "deben ser las necesarias, adecuadas y proporcionales en una sociedad democrática, y deben respetar los derechos y las libertades fundamentales de las personas Titulares de los datos" siempre queda la duda razonable respecto de una implementación práctica y realista de ciertos derechos de frente a las prerrogativas del Estado.

**VI. Interpretar el tipo de normativa ya aplicada en otros países y establecer puntos de coincidencia o no con las regulaciones contempladas por el marco legal vigente en Argentina.**

Al momento de establecer una comparación entre dos leyes vigentes, por un lado la ley argentina N°25.362 del año 2000 y una norma más actualizada, como el RGPD de la Unión Europea que fue sancionado en 2016, si bien hay puntos coincidentes, las diferencias son relevantes en muchos aspectos, aun cuando la ley argentina ha sido objeto de parches normativos a través de diversas resoluciones, en un intento por actualizarla parcialmente, el cuerpo original denota la necesidad de integrar y sistematizar todas las actualizaciones en una sola norma funcional.

La norma europea establece como objeto la protección de los datos personales, algo que comparte con la ley 25.326, pero agrega que es para garantizar el derecho al honor y a la intimidad de las personas, así como el acceso a la información a los datos. Y mientras la ley 25.326 establece como sujetos de la misma al Titular de los datos, al Responsable (de archivo, registro o banco de datos) y al Usuario (el encargado del tratamiento), este último es denominado Encargado en el Reglamento europeo y es el término elegido también para el proyecto de reforma nacional.

El Reglamento europeo es mucho más extenso en el tema de definiciones que la ley argentina vigente, así, incorpora la "elaboración de perfiles" (y su peligroso potencial discriminatorio), "datos biométricos" y "datos genéticos", todos estos sí son incorporados en el Proyecto de Actualización de la ley de 2023. En cuanto a la aplicación territorial, el RGPD establece un supuesto con un Responsable domiciliado en la UE (más allá de dónde se realice el tratamiento) y el otro supuesto para Responsables fuera de la Unión pero que realizan el tratamiento dentro de ella[101]. Esto no es tratado por la ley 25.326 vigente pero sí es incorporado por el Proyecto de Actualización, agregando además el caso particular de ubicación extraterritorial, pero con aplicación de la ley argentina por derecho internacional o por disposiciones contractuales.

Otro punto importante del Reglamento RGPD es que se encuentre incluida la definición del "consentimiento del interesado", como una herramienta de expresión de una voluntad informada por parte de la persona, de la aceptación del tratamiento, dejando en claro que tal

[101] FERREYRA, EDUARDO (2019) EL RGPD Y LA LEY ARGENTINA DE PROTECCIÓN DE DATOS PERSONALES *Análisis comparativo*
Recuperado marzo 7, 2025 de https://adc.org.ar/wp-content/uploads/2019/06/041-el-RGPD-y-la-ley-argentina-de-proteccion-de-datos-personales-XX-2018.pdf

manifestación debe ser para un tratamiento puntual y tiene que plasmarse de modo escrito o verbal; pero no es la única base legítima. Para la ley 25.326, el consentimiento es el supuesto de base legal para el tratamiento, y se presenta como excepciones a los casos en los que no se necesita dicho consentimiento. Esto cambia en el Proyecto de Actualización, que va en plena sintonía con la norma europea.

Se debe destacar que tanto el Reglamento de la UE como la ley 25.326 son coincidentes al tratar los principios de licitud, finalidad, exactitud, necesidad, confidencialidad y limitación del plazo de conservación. Pero como fue mencionado en el desarrollo del trabajo, tanto el principio de minimización de datos (que sirve como limitación al dragado masivo de datos con técnicas utilizadas, por ejemplo, en los sistemas utilizados en seguridad aeroportuaria y en los usados para el reconocimiento facial de prófugos) y el principio de responsabilidad proactiva y demostrada (el Responsable y el Encargado de tratamiento deben adoptar todas las medidas con el fin de garantizar un tratamiento adecuado de los datos) son fundamentales, y este último en particular, es parte importante del Proyecto de Adecuación de la ley.

Si se continúa con un análisis pormenorizado, son varias las coincidencias, pero múltiples las carencias normativas que se encuentran entre ambas leyes, especialmente la posición desventajosa de la ley 25.326. La carta fuerte a jugar en el futuro próximo está representa por el Proyecto de Adecuación de la ley de 2023, que recepta una enorme cantidad de conceptos, e incluso mejoras, respecto del Reglamento RGDP de la UE, es la gran oportunidad de quedar en pie de igualdad con los estándares internacionales actuales, pero de una manera ordenada, sistematizada y unificada en un solo cuerpo normativo.

## CONCLUSIÓN SOBRE LA HIPÓTESIS

Como fue desarrollado durante el trabajo, se pone en evidencia que la norma vigente, encabezada por la ley N°25.326 de Datos Personales debido a que su texto original se remonta al año 2000, presenta carencias en múltiples aspectos respecto a la temática referente a datos biométricos, partiendo de la base de que el propio término, no forma parte siquiera del cuerpo original de la misma. Debe reconocerse que posteriores resoluciones, como ejemplo la 4/2019 y el Anexo I sobre criterios orientadores, emitidos por la Agencia de Acceso a la Información Pública, aportaron ampliaciones y cubrieron estos faltantes, pero al confrontarla con un marco regulatorio más sólido y sistematizado, como por ejemplo, el

Reglamento General de Protección de Datos (RGPD) de la Unión Europea, tal como se desarrolló en el capítulo VIII sobre derecho comparado y en las conclusiones del objetivo específico VI de este trabajo, pone en evidencia la necesidad de un cambio, en principio de criterio, no haciendo foco en el dato en sí mismo sino en la tutela del individuo Titular del mismo, garantizando su derecho a la autodeterminación informativa respecto de sus datos biométricos. La posibilidad del ejercicio de una trazabilidad cierta con los supuestos de territorialidad (y el innovador supuesto del proyecto de ley nacional de ubicación extraterritorial, pero con aplicación de la ley argentina por derecho internacional o por disposiciones contractuales).

La seguridad jurídica representada en el principio de responsabilidad proactiva y demostrada para el caso de los Responsables y Encargados del tratamiento y en la regulación del sector público, como gran protagonista en la recopilación de información biométrica a través de sus recursos tecnológicos, para lograr una transparencia necesaria respecto de las finalidades de los tratamientos que este realiza.

Como se desarrolló también en el trabajo, la respuesta a esta actualización viene de la mano del proyecto de ley que fue enviado al Congreso a través del mensaje 87/2023 y que, de aprobarse en su totalidad, sanearía una imprescindible adecuación de la normativa nacional.

En el planteo de la hipótesis se expuso que la irrupción vertiginosa de la tecnología aplicada al análisis de información de origen biométrico se contrapone con los tiempos de elaboración de las normas regulatorias en nuestro país, lo cual deja a esta última, necesariamente en una posición desventajosa para el momento en que esta entra en vigencia, esto es así, pero no por ello se deben bajar los brazos.

> *-Tienes razón -replicó Pedro-. Pero no quise decir que fueras siervo, sino servidor.*
> *-No veo más diferencia -respondió Rafael-, que la adición de una sílaba.*
> *-Llámalo como quieras -insistió Pedro-, lo que quiero decir es que ése sería el camino por el que llegarías a ser feliz y en el que podrías ser útil tanto a la sociedad como a los individuos.* (Tomás Moro, 1516, p. 24) Utopía

## REFERENCIAS


Barnes, J.G. (2017) Historia - Capítulo 1 Página 5 *El Libro de Referencia de la Huelas Dactilares* - Publicado agosto 2017.
https://nij.ojp.gov/library/publications/el-libro-de-referencia-de-las-huellas-dactilares

Bertillon, A. (1890). *La photographie judiciaire, avec un appendice sur la classification et l'identification anthropométriques.* Paris: Gauthier-Villars et fils. Procedencia del original: Universidad de Michigan - Digitalizado: 23 Jun 2006
https://babel.hathitrust.org/cgi/pt?id=mdp.39015026761356&seq=11

Boulgouris, N. V.; Plataniotis, K. N.; Micheli-Tzanakou, E. (2010) *Biometrics: Theory, Methods, and Applications* IEEE and WILEY, Estados Unidos, 2010 ISBN 978-0470-24782-2

Cifuentes, S. (1995) *Elementos de derecho civil* – Parte general – 4ta ed. actualizada y ampliada. Astrea, 1999.

Dozo, A.; Orovitz, J.; Rosa, S. (2024) Protección de datos personales en la era digital: los desafíos de una actualización imprescindible. *Proyecto de Ley de Protección de Datos Personales de la AAIP: diversas miradas y un consenso: la necesidad de actualizar la legislación argentina*. Ediciones AAIP, 2024.

Ferreyra, E. (2019) *EL RGPD Y LA LEY ARGENTINA DE PROTECCIÓN DE DATOS PERSONALES Análisis comparativo.* Asociación por los Derechos Civiles.
https://adc.org.ar/wp-content/uploads/2019/06/041-el-RGPD-y-la-ley-argentina-de-proteccion-de-datos-personales-XX-2018.pdf

García Ferrari, M. (2009) *"El Bertillon Americano". Una aproximación a la trayectoria intelectual de Juan Vucetich.*
https://static.ides.org.ar/archivo/garcia-ferrari.pdf

González, A.; Prieto, F. (2011). Extracción de puntos característicos del rostro para medidas antropométricas. *Revista Ingenierías Universidad De Medellín*, 9(17), 139–150. https://revistas.udem.edu.co/index.php/ingenierias/article/view/172

Hutchins, L.A. (2017) Sistema de Clasificación de crestas de fricción Capítulo 5.4.1-*El Libro de Referencia de la Huelas Dactilares* –Publicado agosto 2017. https://nij.ojp.gov/library/publications/el-libro-de-referencia-de-las-huellas-dactilares

Herschel, W. J. (1916) *The Origin of Finger-Printing.* Oxford University Press: London. (Traducción realizada específicamente para este trabajo, de la obra original digitalizada en idioma inglés).

Maestros del Derecho. Disertación del Dr. Eduardo Sirkin realizada el 17 de noviembre de 2024.

Recuperado marzo 5, 2025 de https://www.youtube.com/watch?v=O6EpLIuZS78 https://uai.edu.ar/facultades/derecho-y-ciencias-pol%C3%ADticas/comprender-el-derecho/maestros-del-derecho/

Milanta A. (1993) *Vucetich* – Copyright by DEI GENITRIX – 1993 ISBN (L.22399) 987-9014-00-6 (814) https://www.google.com.ar/books/edition/Vucetich/PF55BgAAQBAJ?gbpv=1

Molina Quiroga, E. (2003) *"Protección de datos personales como derecho autónomo. Principios rectores. Informes de solvencia crediticia. Uso arbitrario. Daño moral y material"* (2003). http://www.saij.gob.ar/docs-f/dossier-f/habeas_data.pdf

Moro, T. (1516) *Utopía* – Buenos Aires: Libertador, 2009 ISBN 978-987-1512-12-6

Peruzzotti, M. (2024) Las nuevas bases legales en el proyecto de Ley de Protección de Datos Personales. *Proyecto de Ley de Protección de Datos Personales de la AAIP: diversas miradas y un consenso: la necesidad de actualizar la legislación argentina*. Ediciones AAIP, 2024.

Tolkien, J. R. R. (1954) *Las Dos Torres* - Minotauro ISBN: 9788445077924 – (p. 291)

Velázquez Delgado – Christiansen (2015) Tras las huellas de la peligrosidad: la teoría criminológica de Cesare Lombroso en el siglo XIX - *La Razón Histórica*, nº29, 2015 [231-253] ISSN 1989-2659

## PÁGINAS WEB CONSULTADAS

Brodersen, J (2024) *Por qué el reconocimiento facial sigue suspendido en la ciudad de buenos aires: claves para entender los usos y riesgos de esta inteligencia artificial.* Clarín.

Recuperado julio 25, 2024 de https://www.clarin.com/tecnologia/reconocimiento-facial-sigue-suspendido-ciudad-buenos-aires-claves-entender-usos-riesgos-inteligencia-artificial_0_eT30Dwx2Gm.html?srsltid=AfmBOopvCOYGO9IQkTB5d-5Z8gF2TLaPKdqMHNasVbLdrCGZ6Wj8H-bo

Fitz Patrick, M; Ruiz, I.; Crucianelli, S (2021) *Cuáles son las principales hipótesis detrás del hackeo a la base del Renaper* – Infobae. Recuperado agosto 13, 2024 de https://www.infobae.com/politica/2021/10/31/cuales-son-las-principales-hipotesis-detras-del-hackeo-a-la-base-del-renaper/

Pérez Porto J.- Merino M. Actualizado el 24 de octubre de 2017. *Atavismo* - Qué es, definición y concepto. https://definicion.de/atavismo/

THALES (2023, 03 de mayo) *Biometría definición casos de uso últimas noticias - Ultima actualización 20 de mayo 2023.* Thales Group.

https://www.thalesgroup.com/en/markets/digital-identity-and security/government/inspired/biometrics

THALES (2023) *BIOMETRICS WITH STRICT CONFIDENTIALITY. THE PORTUGUESE EXPERIENCE.* Thales Group.

Recuperado febrero 17, 2025 de https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics/portugal

THALES (2023) *eID since 2007: Portugal's citizen card.* Thales Group.

Recuperado febrero 17, 2025 de https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/portugal-id

## LEYES, REGLAMENTOS, RESOLUCIONES, PROYECTOS DE LEY


PROTECCION DE LOS DATOS PERSONALES – LEY N°25.326 (2000)

Recuperado enero 20, 2024 de https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790/actualizacion

CRITERIOS ORIENTADORES E INDICADORES DE MEJORES PRÁCTICAS EN LA APLICACIÓN DE LA LEY Nº25.326 (2019) – Anexo I – Recuperado julio 22, 2024 de https://www.argentina.gob.ar/sites/default/files/infoleg/res4AAIP-318874.pdf

AGENCIA DE ACCESO A LA INFORMACION PUBLICA - RESOL-2019-4-APN-AAIP Recuperado marzo 1, 2025 de https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-4-2019-318874/texto

PROYECTO DE LEY DE PROTECCIÓN DE DATOS PERSONALES, MENSJ-2023-87-APN-PTE. Expediente Diputados: 12-PE-2023. Publicado en: Trámite Parlamentario N°84, 30/06/2023. Recuperado julio 22, 2024 de https://www.argentina.gob.ar/sites/default/files/mensajeyproyecto_leypdp2023.pdf

Proyecto de Ley para la Protección de Datos Biométricos Utilizados por Aplicaciones de Telefonía Celular que operan en la Provincia De Buenos Aires

Recuperado julio 24, 2024 de https://intranet.hcdiputados-ba.gov.ar/proyectos/24-25D1136012024-04-1116-10-44.pdf

CÓDIGO PROVINCIAL DE IMPLEMENTACIÓN DE LOS DERECHOS DE LOS CONSUMIDORES Y USUARIOS - Ley provincial N°13.133

Recuperado julio 24, 2024 de https://normas.gba.gob.ar/documentos/VJJalfJV.html

PACTO INTERNACIONAL DE DERECHOS CIVILES Y POLÍTICOS

Recuperado octubre 28,2024, de https://www.ohchr.org/es/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

CONSTITUCIÓN NACIONAL

Recuperado enero 22, 2025 de https://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/804/norma.htm

CÓDIGO CIVIL Y COMERCIAL DE LA NACIÓN

Recuperado julio 20, 2024 de https://servicios.infoleg.gob.ar/infolegInternet/anexos/235000-239999/235975/texact.htm

CREACION DEL REGISTRO NACIONAL DE LAS PERSONAS**.** LEY 13.482 BUENOS AIRES, 29 de septiembre de 1948 Boletín Oficial, 20 de octubre de 1948 Vigente, de alcance general Id SAIJ: LNS0001999. Recuperado julio 23, 2024 de http://www.saij.gob.ar/13482-nacional-creacion-registro-nacional-personas-lns0001999-1948-09-29/123456789-0abc-defg-g99-91000scanyel#

LEY DE IDENTIFICACIÓN, REGISTRO Y CLASIFICACIÓN DEL POTENCIAL HUMANO NACIONAL N°17.671 (1968). Recuperado julio 23, 2024 de https://servicios.infoleg.gob.ar/infolegInternet/anexos/25000-29999/28130/texact.htm

ESTATUTO DE LA REVOLUCIÓN ARGENTINA (1966). Recuperado julio 23, 2024 de https://www.argentina.gob.ar/sites/default/files/acta_de_la_revolucion_argentina-1966.pdf

LEY DE SEGURIDAD INTERIOR Nº24.059 (1992). Recuperado julio 24, 2024 de https://www.argentina.gob.ar/normativa/nacional/ley-24059-458/actualizacion

SISTEMA FEDERAL DE IDENTIFICACIÓN BIOMÉTRICA (2011) Decreto 1766/2011 Recuperado julio 25, 2024 de https://www.argentina.gob.ar/normativa/nacional/decreto-1766-2011-189382/actualizacion

Acta de Privacidad de Información Biométrica (BIPA) de Illinois. Recuperado julio 27, 2024 de https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57

REGLAMENTO (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (Texto pertinente a efectos del EEE). Recuperado octubre 30, 2024, de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32016R0679

CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA
Recuperado julio 22, 2024 de https://rm.coe.int/1680078b37

Segundo Protocolo Adicional al Convenio sobre la Ciberdelincuencia, relativo a la cooperación reforzada y la divulgación de pruebas electrónicas - Estrasburgo, 12.V. 2022 – Recuperado agosto, 2024 de https://rm.coe.int/1680a83724

LEY ORGÁNICA 7/2021, de 26 de mayo, de Protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. (2024). ESPAÑA
Recuperado octubre 31, 2024, de https://www.boe.es/buscar/doc.php?id=BOE-A-2021-8806

**JURISPRUDENCIA**

Fallo: Cámara de Apelaciones en lo Contencioso Administrativo, Tributario y de Relaciones de Consumo. Sala I. Secretaría única. "Observatorio de Derecho Informático Argentino (O.D.I.A.)". Expediente N°182908/2020. Actuación N°1055665/2023. 28/4/2023.
Repositorio del Ministerio Público de La Defensa. Recuperado diciembre 22, 2024 de https://repositorio.mpd.gov.ar/jspui/handle/123456789/4657

Fallo: ROSENBACH v. SIX FLAGS ENTERTAINMENT Corp. 2019 IL 123186
Recuperado febrero 15, 2025 de https://www.illinoiscourts.gov/Resources/f71510f1-fb2a-43d8-ba14-292c8009dfd9/123186.pdf
(Texto original en idioma inglés)

Fallo: "State of New Jersey v. Francisco Arteaga" Defendant- Appellant (Causa N°A-3078). ESCUELA DE LA DEFENSA PÚBLICA – REPOSITORIO
Recuperado octubre 20, 2024 de https://repositorio.mpd.gov.ar/jspui/bitstream/123456789/4713/1/SUPERIOR%20COURT%20OF%20NEW%20JERSEY.%20ARTEGA.pdf
(Texto original del fallo en idioma inglés).

**APROBACIÓN DEL TUTOR**

En la Ciudad de Buenos Aires, al día 20 del mes de marzo de 2025

En mi carácter de Tutor de Trabajo Final presentado por el alumno GUSTAVO FABIÁN MAZZALUPO, titulado "**UTILIZACIÓN DE LOS DATOS BIOMÉTRICOS EN LA ACTUALIDAD. REGULACIÓN, PROBLEMÁTICAS Y UNA MIRADA RESPONSABLE HACIA EL FUTURO**" manifiesto que el trabajo ha sido confeccionado bajo mi supervisión considerando que dicho trabajo reúne los requisitos y méritos suficientes para su presentación y evaluación.

Sin otro particular, Saludo Atte.-

Profesor Miceli, Carlos