EL DATO BIOMÉTRICO Y LA VIDEOVIGILANCIA COMO HERRAMIENTAS DE CONTROL SOCIAL [1]

BIOMETRIC DATA AND VIDEO SURVEILLANCE AS TOOLS FOR SOCIAL CONTROL

Por *María Raquel Burgueño* (*)

RESUMEN: El presente trabajo tiene como fin comprender los alcances de la videovigilancia desde una reflexión socio-jurídica en un ámbito donde las legislaciones internacionales tienen diferentes miradas. En tal sentido entendemos que la protección de datos personales, en este caso, el de la biometría facial, se encuentra en constante tensión con otros bienes jurídicos como la seguridad y la integridad de las personas y sus bienes. Algunos Gobiernos, como el caso de China, consideran que los datos personales pertenecen al Estado Nacional. Por el contrario, para los Estados Unidos de América, los datos personales se encuentran estrechamente relacionados con el concepto de "Mercado", y le pertenecen a éste. Finalmente, en un tercer bloque la Unión Europea reconoce la exclusividad del titular del dato, como único propietario de éste, entendiendo así, que los datos biométricos deben ser protegidos a través de regulaciones que aseguren una efectiva protección de los datos personales y consecuentemente de los derechos humanos digitales.

PALABRAS CLAVES: BIOMETRÍA FACIAL; VIDEOVIGILANCIA; PROTECCIÓN DE DATOS PERSONALES; SEGURIDAD; INTEGRIDAD; DERECHOS HUMANOS DIGITALES; LEGISLACIÓN INTERNACIONAL; PANÓPTICO; MICHEL FOUCAULT; GEORGE ORWELL; BIG BROTHER; EXTIMIDAD; INTELIGENCIA ARTIFICIAL; VIGILANCIA; CONTROL SOCIAL; ÉMILE DURKHEIM INSTITUCIONES DISCIPLINARIAS; JEREMY BENTHAM; UTILITARISMO MODERNO; EPIDEMIAS; DISTOPÍA; REBELIÓN EN LA GRANJA; DICTADURAS; FAKE NEWS; REDES SOCIALES; AUTOVIGILANCIA; MARKETING GLOBALIZADO; GEOLOCALIZACIÓN; SMART PHONES; WEARABLES; NANOCHIPS; SILLICON VALLEY; CAPITALISMO DE LAS PLATAFORMAS; INTERNET DE LAS COSAS (IOT); CCTV; DERECHOS HUMANOS; NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST); UNIÓN INTERNACIONAL DE TELECOMUNICACIONES (ITU); REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS DE LA UE; LEY 25.326.

ABSTRACT: This paper aims to understand the scope of video surveillance from a socio-legal reflection in an area where international legislation has different perspectives. In this sense, we understand that the protection of personal data, in this case, facial biometrics, is in constant tension with other legal assets such as the security and

[1] Artículo aprobado para su publicación el 15 de diciembre de 2024. El presente es una adaptación del Trabajo presentado para Programa de Actualización en Data Governance, Data Compliance, Infosec & Ciberseguridad, realizado en el segundo semestre del año 2022.

(*) Abogada, Escribana Titular del Registro 803 CABA. Especialización en Derecho Informático (UBA). Diplomada en Blockchain y Smart Contracts (UCC); Fintech y Blockchain (ITBA); Gestión de la Ciberseguridad (UCEMA); Dataprivacy e Infosec (DATALAB UBA). IA y Derecho y Web 3, Gaming y Metaverso (UBA IALAB). Maestranda Escuela de Economía y Negocios (UNSAM) en la Maestría Gestión y Diseño de la Tecnología y la Innovación. Consultora de Empresa Familiar Certificada (IADEF). Profesora Adjunta Seminario de Nuevas Tecnologías y Notariado en Postítulo Notariado (USAL). Prof. Adjunta Catedra Teoría y Práctica del Derecho Registral. (USAL). Docente Auxiliar CPO (UBA DERECHO).

integrity of people and property. Some governments, such as China, consider that personal data belongs to the National State. On the contrary, for the United States of America, personal data is closely related to the concept of the Market and belongs to it. Finally, in a third block, the European Union recognizes the exclusivity of the data owner as the sole proprietor, thus understanding that biometric data must be protected through regulations that ensure effective protection of personal data and consequently digital human rights.

KEY WORDS: FACIAL BIOMETRICS; VIDEO SURVEILLANCE; DATA PROTECTION; SECURITY; INTEGRITY; DIGITAL HUMAN RIGHTS; INTERNATIONAL LEGISLATION; PANOPTICON; MICHEL FOUCAULT; GEORGE ORWELL; BIG BROTHER; EXTIMACY; ARTIFICIAL INTELLIGENCE; SURVEILLANCE; SOCIAL CONTROL; ÉMILE DURKHEIM; DISCIPLINARY INSTITUTIONS; JEREMY BENTHAM; MODERN UTILITARIANISM; EPIDEMICS; DYSTOPIA; ANIMAL FARM; DICTATORSHIPS; FAKE NEWS; SOCIAL NETWORKS - SELF-SURVEILLANCE; GLOBALIZED MARKETING; GEOLOCATION; SMART PHONES; WEARABLES; NANOCHIPS; SILICON VALLEY; PLATFORM CAPITALISM; INTERNET OF THINGS (IOT); CCTV; HUMAN RIGHTS; NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST); INTERNATIONAL TELECOMMUNICATION UNION (ITU); EU GENERAL DATA PROTECTION REGULATION (GDPR); LAW 25.326.

DOI: https://doi.org/10.22529/rbia.2025(6)03

INTRODUCCIÓN

a) Un recorrido por los conceptos de vigilancia y videovigilancia.

A través de la historia de la humanidad podemos identificar hechos sociales que son extrínsecos al individuo, es decir exteriores a las conciencias individuales y que son capaces de ejercer sobre estas conciencias particulares una influencia coercitiva. Así lo postulaba Émile Durkheim uno de los grandes autores considerado como "padre" de la Sociología, en su obra. [3] Es por ello por lo que podemos afirmar que el concepto de "vigilancia" cumple con las características de un hecho social, nos viene impuesto a los seres humanos desde que somos pequeños, en nuestros hogares de origen y de la mano del concepto de "cuidado" y "preservación". Más tarde la Institución "Escuela" sigue imponiendo estas normas de vigilancia en los alumnos, acompañada de otras instituciones a las que años más tarde Michael Foucault dio en llamar "Instituciones Disciplinarias o de Encierro" como los Hospitales, Psiquiátricos, Prisiones, Asilos, Orfanatos y Cuarteles. Esta vigilancia busca homogeneizar los rasgos y conductas particulares alternativos o divergentes que en los casos estudiados por Foucault se destacaron las conductas que salen del proceso de "normalización" siendo considerados los individuos allí encerrados como "disfuncionales" o "antisociales". En este esquema se busca recompensar a quien mantiene el orden que imponen aquellos que ostentar el uso del poder y castigar a los individuos considerados por este grupo como fuera del orden. A tal efecto la vigilancia se ha convertido en la herramienta más importante para detectar estos comportamientos. De esta manera se corre el riesgo de anular el pensamiento creativo, crítico, innovador bajo el pretexto de que pueda comprometer los postulados del pensamiento hegemónico instalado.

Es así como en la historia aparece una nueva herramienta tecnológica disciplinaria: El Panóptico.

b) El Panóptico de Jeremy Bentham.

[3] Durkheim, Émile. "Las reglas del método sociológico". Ed. Gorla. 2012. Segunda reimpresión.

Si bien quien describió a la perfección la noción de panóptico como dispositivo disciplinario fue el filósofo y sociólogo Michel Foucault, a quien relacionaremos en el siguiente punto, los antecedentes arquitectónicos en cuanto al diseño de esta tecnología fueron ideados por Jeremy Bentham y su hermano Samuel.

Jeremy Bentham fue un reconocido filósofo de origen inglés. Se lo considera el padre del "utilitarismo moderno" y se lo reconoce como un gran defensor de las libertades individuales y el derecho a la expresión, entre otros. Su afán era lograr construir un modelo de construcción destinada a la reclusión de presidiarios que generara costos mínimos de personal, higiene y seguridad para el Estado. Durante su vida se desveló insatisfactoriamente para poder concretar la construcción de ese edificio. Sin embargo, sentó las bases para que más tarde otros autores pudieran explicar este fenómeno.

c) Michael Foucault "Vigilar y castigar".

Si bien como vimos la noción de panóptico responde al pensamiento creativo de Jeremy Bentham, el desarrollo del término "Panoptismo" se encuentra descripto por Michel Foucault en su obra "Vigilar y Castigar" [4]. Foucault describe la vigilancia de manera impecable al tratar las cuarentenas por epidemias que dicho sea de paso cualquier semejanza con la realidad y actualidad es pura coincidencia, cuando recordamos los recientes episodios vividos por la humanidad durante la pandemia de COVID – 19 en el año 2020 y subsiguientes.

Dice el autor: *" … Este este espacio cerrado, recortado, vigilado, en todos sus puntos, en el que los individuos están insertos en un lugar fijo, en el que los menores movimientos se hallan controlados, en el que todos los acontecimientos están registrados, en el que un trabajo ininterrumpido de escritura une el centro y la periferia, en el que el poder se ejerce por entero, de acuerdo con una figura jerárquica continua, en el que cada individuo está constantemente localizado, examinado y distribuido entre los vivos, los enfermos y los muertos, todo esto constituye un modelo compacto del dispositivo disciplinario…"*

De esta manera Foucault describía la actividad de vigilancia que los reglamentos implementaban para el caso de instalarse una "peste" en alguna ciudad. La vigilancia era ejercida por los Intendentes, los síndicos y los soldados de la guardia. Las personas debían

[4] Foucault, Michel. "Vigilar y castigar. Nacimiento de la prisión". Colección Nueva Criminología. Editorial Siglo XXI Editores.

acercarse a una única ventana para mostrar que estaban vivas en las inspecciones que se realizaban casa por casa mientras durara la cuarentena.

Para este autor el Panóptico de Bentham *"… es la figura arquitectónica de esta composición. Conocido es su principio: en la periferia, una construcción en forma de anillo; en el centro, una torre, ésta con anchas ventanas que se abren en la cara interior del anillo. La construcción periférica está dividida en celdas, cada una de las cuales atraviesa toda la anchura de la construcción. Tienen dos ventanas, una que da al interior, correspondiente a las ventanas de la torre, y la otra que da al exterior, permite que la luz atraviese la celda de una parte a otra. Basta entonces situar un vigilante en la torre central y encerrar en cada celda a un loco, un enfermo, un condenado, un obrero, o un escolar. Por el efecto de la contraluz, se pueden percibir desde la torre, recortándose perfectamente sobre la luz las pequeñas siluetas cautivas en las celdas de la periferia. Tantos pequeños teatros como celdas, en los que cada actor está solo, perfectamente individualizado y constantemente visible. El dispositivo panóptico dispone de unidades espaciales que permiten ver sin cesar y reconocer el punto. En suma, se invierte el principio del calabozo, o más bien de sus tres funciones – encerrar, privar de luz y ocultar – no se conserva más que la primera y se suprimen las otras dos. La plena luz y la mirada de un vigilante captan mejor que la sombra, que en último término protegía. La visibilidad es una trampa. … ésta es la garantía del orden…"*

d) George Orwell y 1984 – "Big Brother is watching you".

George Orwell era el seudónimo utilizado por el escritor Eric Blair quien supo llevar el concepto de vigilancia al extremo e introduce en su distópica novela "1984" el concepto de "videovigilancia" como control social. De allí la célebre frase Big Brother is watching you" (El gran hermano te vigila). La introducción de un personaje como El Gran Hermano y el efecto de su omnipresencia en los ciudadanos a través de diferentes objetos simbólicos como la moneda, propaganda y una pantalla que cumple la función de monitor para poder controlar incluso hasta el pensamiento de los seres humanos representa la manera que tienen las artes literarias de sublimar los acontecimientos y experiencias de sus autores. En su caso Orwell había sido testigo de varios eventos mundiales que lo llevan a representar este mundo al que cada vez podemos catalogar de menos distópico, pues muchas de las descripciones efectuadas en su obra se han vuelto lamentablemente realidad.

Orwell fue también un defensor del sistema democrático y militó en el Frente Popular español contra el régimen franquista. Los sistemas dictatoriales y sus prácticas restrictivas de las libertades individuales son denunciados en sus obras, la ya mencionada 1984 y "Rebelión en la granja". Como contexto histórico a su novela que fue publicada en 1949 podemos encontrar los siguientes eventos:

- La Alemania Nazi bajo la dictadura de Hitler de 1933 a 1945.
- La dictadura fascista de Francisco Franco en España de 1936 a 1975.
- La dictadura comunista de Stalin en Rusia de 1922 a 1952.
- La dictadura fascista de Benito Mussolini en Italia de 1922 a 1943.
- La dictadura de Salazar en Portugal de 1932 a 1968.

Anticipamos en este punto algunas de las conclusiones de este trabajo y advertimos la peligrosidad del uso de herramientas tecnológicas como recursos para desestabilizar los sistemas democráticos. Los discursos de odio, la cultura de la cancelación, las fake news que existieron en el mundo analógico se han hecho masivos en el mundo digital a través de su propagación inmediata en las redes sociales, las cuales, además, gozan del distanciamiento que genera una pantalla para impedir el contacto humano y permitir ampararse impunemente detrás de un dispositivo electrónico donde muchas veces ni siquiera existe el accionar humano y son cuentas de redes sociales accionadas por bots.

El trabajo de los asesores jurídicos es advertir y denunciar estas prácticas como así también ejercer la función docente en esta materia para prevenir a los usuarios y a la ciudadanía en general respecto de la conservación de sus datos personales y de los derechos de privacidad que a éstos le asisten como la autodeterminación informativa dinámica.

e) La era digital: Paula Sibilia: Intimidad – Extimidad y Éric Sadin Antihumanismo radical:

Con el avance de la tecnología y la revolución digital que implicó la llegada de internet el concepto "vigilancia" adquiere nuevas dimensiones. Según la antropóloga Paula Sibilia[5] la vida digital se escurrió en las subjetividades, y en este nuevo escenario encontramos que además de

[5] Sibilia, Paula. Mutaciones de la subjetividad. La exhibición de la intimidad como un eclipse de la interioridad. Un problema del Psicoanálisis Psicolibro Ediciones, Paidós, Bs As. Argentina, 2010.

los conceptos de normalización de los sujetos que mencionaba Foucault, en el mundo digital la normalización se presenta a través del concepto de "auto vigilancia". Los conceptos expresados por el citado autor relativos a "El buen encauzamiento"; "La vigilancia jerárquica" y la "sanción normalizadora"[6], demuestran la búsqueda constante de quienes detentan el poder, antes el Estado, hoy se le suman también los grandes grupos económicos, con el fin de generar seres humanos dóciles, domesticados, adiestrados y disciplinados, con el fin de sostener el modelo de producción capitalista (cuerpos dóciles y cuerpos útiles).

Las tecnologías contribuyeron a configurar nuevos productos en el mercado: Nuevas subjetividades, modos de ser estandarizados y propuestos por el marketing globalizado a través de subliminales recomendaciones que aparecen en nuestros dispositivos digitales, sugiriendo la adquisición de tal o cual producto, generando la creación de nuevas necesidades a los consumidores que contribuyen a las ganancias de industrias y servicios.

La particularidad de estas nuevas técnicas de mercadeo es que utilizan la información libremente dada por los usuarios a través de las redes sociales y diferentes bases de datos combinadas con el uso de las tecnologías, como la inteligencia artificial, con el fin de analizar velozmente el perfil del consumidor e inducir sigilosamente al consumo de productos y servicios exhibiendo al mismo tiempo "cánones de normalización" y "grupos de pertenencia" que inducen al consumidor a la adquisición de dichos productos y/o servicios para encontrarse dentro del estándar propuesto.

Ahora bien, en este traspaso del mundo analógico al mundo digital, que expresa Sibilia en su obra, se dan nuevas maneras de construir la subjetividad, metamorfosis de la realidad en donde las paredes se transforman en redes, la intimidad en "extimidad", la introspección en conexión, la concentración en dispersión, y aparecen conceptos de visibilidad y multitasking. Donde el ciudadano se transforma en consumidor, y se distancia del "deber" que le impone el Estado: "tengo que" - "usted debe" y se entusiasma con su propio empoderamiento y libertad: "yo quiero" - "vos podés". Donde la subjetividad se construye en el afuera "extimidad"[7] desistiendo de la privacidad.

[6] Foucault, Michel. Óp. Cit.
[7] Sibilia, Paula. Óp. Cit.

Las redes sociales, sustentadas por el desarrollo de las tecnologías, pasaron a ser las nuevas vitrinas desde donde monitoreamos y controlamos a los demás y a su vez somos también, al mismo tiempo, objeto de monitoreo y de control. El mercado capitalista hoy nos exige nuevas aptitudes para permanecer en los cánones de normalización: permanecer "visibles" y "conectados". La geolocalización y los dispositivos electrónicos como celulares inteligentes (Smart phones) y sus extensiones como relojes / wearables (Smart watch, dispositivos amigables que permiten la conectividad) proveen nuevas herramientas sociotécnicas de control en un mundo donde todo y todos pueden ser rastreado a través de los sensores y señales que emanan de dichos dispositivos. "***En Dios confiamos, a todos los demás, los monitoreamos***".

Paula Sibilia cita en su trabajo, "El hombre postorgánico"[8], al sociólogo y epistemólogo portugués Herminio Martins, quien sostiene que estamos en presencia de una "tecnociencia de vocación fáustica" que rechaza el carácter orgánico y material del cuerpo humano y pretende superarlo buscando un ideal aséptico, artificial, virtual e inmortal, en contraposición al sentido de la técnica de "Prometeo", que respeta el principio de la racionalidad científica y de que ciertos asuntos pertenecen exclusivamente al dominio divino, donde hay un espacio que queda reservado a los misterios del origen de la vida y de la evolución biológica.

La planificación "Fáustica" en la composición del ser humano libre de "fallas" como proyecto de modificación de la composición no sólo genética natural del ser humano, sino también cultural, emocional e ideológica tiende a convertir las subjetividades al modelo de "cuerpos dóciles", al decir de Foucault[9], de manera de someterlas a parámetros de normalidad arquitectónicamente orquestados por los grupos de intereses económicos y de gobiernos centralizados en desmedro de aquellos que se encuentran en la periferia. Este uso de las tecnologías configura nuevas maneras de alienación y generan sutilmente sesgos de discriminación a quienes no se ajusten a dichos cánones de normalización. Cuando se hace referencia a que estos sesgos son sutiles, se intenta destacar que los mismos nacen producto de una carga sesgada que realizan los propios seres humanos en las bases de datos que utilizarán luego los algoritmos (Dataset). Estos algoritmos actúan tras las bambalinas de las pantallas

[8] Sibilia, Paula. Óp. cit.
[9] Foucault, Michel. Óp. cit

electrónicas y plasmas de los dispositivos electrónicos que constantemente conviven con nuestras subjetividades y que como bien dice Eric Sadin[10] se transforman en una extensión de nuestro propio ser al punto de desear incorporarlo dentro de nuestros cuerpos, como por ejemplo el caso de los nanochips o chips de información alojados dentro del cuerpo de un individuo a nivel subcutáneo. De esta manera el ser humano genera un "apego digital" y se ubica bajo una especie de sumisión consentida y deslumbrada a la que el filósofo francés denomina un "Complemento de uno mismo o un alter ego superior". Para el pensamiento de Sadin, el cual se encuentra enrolado en lo que algunos autores denominan "tecno pesimismo", esos hilos sutiles detrás de la pantalla responden a intereses de una filosofía de pensamiento al que denomina "TECNOLIBERTARISMO", en donde existe un pasaje del gobierno de las cosas al gobierno de las personas, donde aparecen nuevas formas de tecno vigilancia y donde se avecina una "***neutralización algorítmica de la voluntad humana***", pues la inteligencia artificial se hace presente al momento de tener que tomar decisiones, como por ejemplo las atinentes a procesos de creatividad como la innovación, que pertenece al ámbito de la creación de los seres humanos. Sadin Postula a la Inteligencia Artificial como un "**Antihumanismo radical**" que atenta contra los tres principios humanizadores: La autonomía del juicio; la libre decisión y el Principio de responsabilidad. De esta manera desde Sillicon Valley nace este nuevo "Capitalismo de las Plataformas".[11]

Todos los autores expuestos han investigado de una u otra forma el concepto de vigilancia. Este concepto a través de herramientas técnicas como una cámara permitieron expandir el concepto de vigilancia hacia una dimensión que ya no requiere de la presencia física para continuar ejerciendo esta función. Además, con el desarrollo tecnológico en materia de cámaras CCTV, éstas se conectan entre sí a través de la tecnología denominada Internet de las cosas (IoT) y no solo pueden estar dirigidas en un determinado sentido con un objetivo fijo, sino que han adoptado la función de domos que pueden monitorear espacios físicos en un radio de trescientos sesenta grados, lo que permite efectuar un cameo total del lugar.

[10] Sadin, Eric. "La Humanidad aumentada. La administración digital del mundo". Editorial Caja Negra. 2018.
[11] Sadin, Éric. "La silicolonización del mundo. La irresistible expansión del liberalismo digital". Editorial Caja Negra. 2018.

Nos preguntamos cuál es el objetivo principal que justifica que existan tantas cantidades de cámaras en el mundo. La **ONG** de origen británica "**BIG BROTHER WATCH**", abierta defensora de la privacidad y activa denunciante de la violación de los derechos humanos en materia de control social por parte de los Estados a través de la videovigilancia y recolección de datos biométricos de las personas ha denunciado que el número de cámaras ha aumentado de 1.85 a 4.2 millones. La denuncia constante a las empresas de tecnologías CCTV de origen chino como Hikvision [12] y otras ha despertado nuevamente la alerta a la invasión de la privacidad de los ciudadanos, arremetiendo contra datos sensibles como lo son los de índole biométricos. Estos datos revelan no sólo las características individuales de las personas, sino que permiten hacer una primera clasificación de su pertenencia étnica y en algunos casos hasta religiosa como por ejemplo el uso de velo en las mujeres de religión musulmana.

Esta ONG busca informar a sus representantes en el parlamento británico sobre los riesgos significativos del reconocimiento facial en vivo que plantea la vigilancia de los derechos humanos.

Por su parte en cuanto a la justificación de la utilización de estos sistemas de videovigilancia abierta se basa por parte de los Estados con la finalidad de garantizar la seguridad de las personas, sus bienes e instalaciones. Asimismo, la videovigilancia también es utilizada no sólo por el Estado sino también por empresas privadas bajo la fundamentación, además de razones de seguridad, de otros fines como la asistencia sanitaria, la investigación, o el control de la prestación laboral por parte de los trabajadores.

La ONG "BIG BROTHER WATCH" alertó en un informe del mes de junio de 2020 sobre los peligros de la videovigilancia respecto del avasallamiento de los DDHH. Éstos son los principales puntos de advertencia:

- Una amenaza a la libertad: El uso de la vigilancia de reconocimiento facial en vivo por parte de la policía de Inglaterra y Gales representa una enorme expansión de la vigilancia estatal y una de las más graves amenazas a las libertades civiles de los últimos años. Esta herramienta de vigilancia masiva al estilo chino corre el riesgo de

[12] The Guardian - Chinese state-owned surveillance company launches sinister ethnicity recognition tech while facing UK ban — Big Brother Watch

convertir las cámaras de CCTV en puestos biométricos de control y a los ciudadanos en "tarjetas de identificación personal" que caminan.

- Incompatible con los DDHH: Exploramos el impacto del reconocimiento facial de la videovigilancia de los Derechos Humanos en el Reino Unido y explicamos por qué estos puntos de control no pueden ser compatibles en el marco de los DDHH.
- Personas inocentes monitoreadas: La policía ha utilizado esta vigilancia intrusiva para monitorear y rastrear a personas inocentes con problemas de salud mental, manifestantes pacíficos y sus propios procedimientos operativos establecen que las personas sin antecedentes penales pueden ser rastreadas y seguidas por reconocimiento facial en vivo.
- Efectos discriminatorios: La investigación ha encontrado que muchos algoritmos de reconocimiento facial en vivo tienen un efecto claramente discriminatorio y desproporcionado, identificando erróneamente a personas de color y a mujeres.
- Inexistencia de políticas de garantía. Uso de videovigilancia sin sustento legal que la avale: El parlamento inglés nunca ha aprobado una ley que permita a la policía el uso de la vigilancia por reconocimiento facial. No existen leyes que prevean la garantía de los ciudadanos en esta alarmante expansión de la vigilancia en el Reino Unido.
- Ineficacia de la herramienta: En los últimos años, el reconocimiento facial en vivo ha demostrado ser peligrosamente inexacta, produciendo miles de identificaciones erróneas, lo que resulta en la detención de personas inocentes a quienes se les exige en muchos casos que demuestren que no son criminales buscados.
- Excesos en la vigilancia: Big Brother Watch ha sido testigo de miembros inocentes del público que han sido identificados erróneamente, detenidos y registrados, incluido en ellos un niño de catorce años de color usando su uniforme escolar. También ha sido testigo de personas detenidas que han sido forzadas a mostrar una identificación y en algunos casos hasta multados por usar chaquetas con capuchas o bufandas que les cubrieran la barbilla en invierno.

III) DATOS BIOMÉTRICOS

¿Qué es la Biometría? [13]

Denominamos biometría al estudio mensurativo o estadístico de los fenómenos o procesos biológicos. El "National Institute of Standards and Technology" (NIST) lo define como el análisis estadístico de observaciones biológicas y sus fenómenos.

El término, proveniente del griego bios (vida) y metron (medida), es comúnmente acuñado a efectos de identificar al estudio del reconocimiento inequívoco de personas basado en sus características físicas, fisiológicas o de comportamiento denominado autentificación biométrica. La autenticación biométrica es un método automatizado que incluye tres factores fundamentales: un mecanismo capaz de escanear y capturar imágenes, tanto de forma digital o analógica, de una característica personal viva; el procesamiento de dicha imagen con su comparación con una base de datos previa; y la interfaz con sistemas de aplicaciones.

Un sistema biométrico, "… es un sistema informático de reconocimiento en base a diversos patrones obtenidos mediante la captación de datos biométricos y comparándolos con plantillas previamente registradas. Según la Unión Internacional de Telecomunicaciones o por sus siglas en inglés ITU (International Telecommunication Union), se han establecido factores de calidad relevantes que pueden influir en la toma de decisión sobre qué sistema biométrico utilizar". A saber:

- Performance: Determina si la medición es robusta, adecuada, rápida y eficiente.
- Aceptación: Nivel de aceptación de individuos.
- Confiabilidad: Nivel de seguridad ante fraudes.
- Legalidad: Grado de adecuación a la legislación local.
- Costo: Capacidad económica para su implementación y utilización por parte de los usuarios.

Los sistemas biométricos están compuestos por una entidad de almacenamiento que contiene los datos biométricos recolectados; un dispositivo o sensor utilizado para la recopilación de datos; un proceso de comparación entre los datos recopilados y la base de datos; y una función de decisión (matching decision) que establece la similitud entre los datos

[13] Cita: TR LALEY AR/DOC/1997/2021

comparados y su grado de éxito.[14]

El Reglamento General de Protección de Datos de la UE define a los datos biométricos como: "Datos personales obtenidos a partir de un tratamiento técnico específico, relativos a 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".

Además, establece con respecto a los datos biométricos lo siguiente:

Limitación al tratamiento de datos biométricos: "Los Estados miembros deben estar facultados para mantener o introducir otras condiciones, incluidas limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud".

Datos biométricos y evaluación de impacto: "La evaluación de impacto relativa a la protección de datos debe realizarse también en los casos en los que se tratan datos personales para adoptar decisiones relativas a personas físicas concretas a raíz de una evaluación sistemática y exhaustiva de aspectos personales propios de personas físicas, basada en la elaboración de perfiles de dichos datos o a raíz del tratamiento de categorías especiales de datos personales, datos biométricos o datos sobre condenas e infracciones penales o medidas de seguridad conexas. También es necesaria una evaluación de impacto relativa a la protección de datos para el control de zonas de acceso público a gran escala, en particular cuando se utilicen dispositivos optoelectrónicos o para cualquier otro tipo de operación cuando la autoridad de control competente considere que el tratamiento entrañe probablemente un alto riesgo para los derechos y libertades de los interesados, en particular porque impida a los interesados ejercer un derecho o utilizar un servicio o ejecutar un contrato, o porque se efectúe sistemáticamente a gran escala".

Prohibición de Tratamiento: Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a

[14] Cita: TR LALEY AR/DOC/1997/2021

identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física.

La Ley 25.326 respecto a la Protección de Datos Personales en la República Argentina prevé el concepto de dato sensible, más no hace una referencia expresa al dato biométrico en sí, entendemos que esto ha sido así por ser una ley que data del año 2000 donde los avances tecnológicos sobre reconocimiento facial y su impacto sobre los datos personales aún no podían ser previstos por el legislador.

En el artículo 2° destinado a definiciones terminológicas caracterizó a los datos sensibles como aquellos datos personales que revelan el origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

En su artículo 7° nuestra ley previó la categoría de datos, dándole expresa protección a aquellos que revelen el carácter de datos sensibles, en tal sentido dispone que:

> 1. Ninguna persona puede ser obligada a proporcionar datos sensibles.
>
> 2. Los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley. También podrán ser tratados con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares.
>
> 3. Queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles. Sin perjuicio de ello, la Iglesia Católica, las asociaciones religiosas y las organizaciones políticas y sindicales podrán llevar un registro de sus miembros.
>
> 4. Los datos relativos a antecedentes penales o contravencionales sólo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de las leyes y reglamentaciones respectivas.

ANTEPROYECTO Y PROYECTO DE MODIFICACIÓN DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES

La Ley 25.326 cuenta con dos intentos infructuosos que previeron su modificación. El primero, es el anteproyecto que data del año 2018 y el segundo el proyecto del año 2020, en ambos casos perdieron estado parlamentario.

El anteproyecto del año 2018 además de ser ampliamente criticado, con justa razón, por el intento de introducir el consentimiento tácito tampoco tuvo la previsión de incorporar en su articulado los **datos biométricos como datos sensibles** siguiendo la línea del RGPD de la UE, limitándose a enunciarlos como datos personales en el ámbito de las definiciones.

Idéntica suerte tuvo el proyecto del año 2020, aún frente a las críticas efectuadas por el ámbito de organizaciones de DDHH que fueron prodigadas al anteproyecto del año 2018, no se logró madurar el texto anterior o directamente no interesó hacerlo quedando en una exacta copia de su antecesor de 2018 en materia de datos biométricos.

El Proyecto del año 2022:

Este proyecto presentado al Congreso Nacional en el mes de octubre de 2002 incorpora en su artículo 2° de Definiciones el concepto de Datos Biométricos entendiéndolos como aquellos datos 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, tales como imágenes faciales o datos dactiloscópicos, entre otros.

Asimismo, vuelve a enunciar los Datos Biométricos cuando define a los datos sensibles[15]. En tal sentido establece que son Datos Personales Sensibles aquellos que se refieren a la esfera íntima de su Titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical u opiniones políticas; datos relativos a la salud, discapacidad, a la preferencia u orientación sexual, datos genéticos o **biométricos** cuando puedan revelar datos

[15] Finalmente, luego de dos intentos fallidos se mantiene la congruencia con el espíritu del RGPD de la UE.

adicionales cuyo uso pueda resultar potencialmente discriminatorio para su Titular y que estén dirigidos a identificar de manera unívoca a una persona humana.

Críticas al Proyecto del año 2022 respecto a las temáticas de Datos Biométricos y Videovigilancia:

Hacemos nuestras las críticas formuladas al anteproyecto del año 2022 por nuestra titular de posgrado, Doctora Johanna C. Faliero (PhD) en su artículo de Doctrina publicado en el Diario la Ley con fecha 3 de octubre de 2022.

> *" … Cuando el nuevo Anteproyecto define a los datos personales sensibles comete el error de que, si bien incluye a los datos biométricos en su listado enunciativo, lo hace aclarando que* ***protege a los "datos biométricos dirigidos a identificar de manera unívoca a una persona humana"****, lo que no es detalle menor, ya que permite entonces considerar como "no sensible" un dato biométrico no dirigido a identificar de manera unívoca a una persona humana, lo que con las técnicas actuales de procesamiento de datos que disponemos puede ser igualmente lesivo…"*
>
> *"… Con relación a las definiciones establecidas en el art. 2º del nuevo Anteproyecto, resta decir que, si bien el listado es extenso, no explota todo su potencial ni aprovecha la oportunidad de renovación, donde no es ya revolucionario incluir conceptos publicados en el RGPD de 2016, sino que hubiera sido verdaderamente revelador hacerlo con conceptos nuevos relevantes para este escenario actual, donde ya se podría haber avanzado y hablado sobre la sensibilidad de los datos de geolocalización, entre otras categorías a las nuevas que se han sumado en 2016 en Europa, y la clarificación de definiciones acompañadas de principios específicos que resultan muy relevantes y controversiales en el actual escenario de la protección de datos (Servicios de la sociedad de la información,* ***Videovigilancia****, Cloud computing, Big data, Data mining, Inteligencia artificial, Machine learning, Deep learning, IoT / internet de las cosas, Geolocalización,* ***Vigilancia electrónica*** */* ***ciber vigilancia****, OSINT y SOCMINT, etc.)…"*

Realmente coincidimos con nuestra docente respecto de la pérdida de chance de haber podido producir una legislación ejemplar y pionera en materia de protección de datos frente a

los peligros que se nos imponen con el uso de tecnologías como las ya mencionadas en los comentarios aludidos. Máxime que estas tecnologías ya llevan tiempo de implementación siendo posible la investigación de sus efectos desde la mirada de los Derechos Humanos y no se requería hacer una previsión a futuro de nuevas tecnologías aún no descubiertas o algún otro tipo de previsión específica sobre tecnologías cuya existencia se conoce, como Blockchain y su problemática en la irreversibilidad en los datos registrados en la cadena de bloques y todo aquello atinente al ámbito de la web 3 como la construcción de espacios inmersivos como los metaversos, o aquellas tecnologías que aún se encuentran en fases no exploradas suficientemente desde el uso comercial y por ende no pueden establecerse con precisión sus efectos, como es el caso de la computación cuántica[16]. No obstante, ello nos permitimos también sumarnos a las críticas antes transcriptas con esta baja previsión legal del proyecto de 2022 respectos de los efectos frente a estos últimos supuestos mencionados.

> *"… Debió haberse establecido la limitación de la admisibilidad de valoraciones personales automatizadas, sus mecanismos de supervisión y garantido un derecho a oposición real, con expresa prohibición de prácticas abusivas de perfilamiento a través de procesamiento automatizado de datos del titular y de prácticas abusivas e invasivas de tratamiento de datos personales a escala masiva por parte del Estado, como lo son para la población general el uso de biometría, datos de geolocalización y videovigilancia sin controles adecuados…"*

Asimismo, tampoco se especificaron en materia de videovigilancia y biometría la implementaron de procedimientos para la defensa de los derechos de los titulares de datos en materia del tratamiento automatizado de sus datos personales. Hubiera sido una excelente oportunidad para crear organismos independientes que garanticen la debida defensa de los titulares de los datos, como por ejemplo la creación de la figura del "**Ombudsman y por qué no de la Ombudswoman**" de los datos personales de los ciudadanos.

LA IMPORTANCIA DE LOS TRATADOS INTERNACIONALES FRENTE A LOS VACÍOS LEGALES:

[16] ¿Qué es la computación cuántica? | IBM

Sabemos que por aplicación del artículo 75.22 de nuestra Constitución Nacional, los Tratados Internacionales que sean adheridos por nuestro país a través del voto de las dos terceras partes de ambas Cámaras del Congreso Nacional, gozan de jerarquía constitucional. Esta norma viene a salvar los vacíos legales que encontremos en materia de Protección de Datos en nuestra legislación nacional y promete ser la última ratio en materia de protección de datos personales que nuestra propia ley no haya podido concebir, ya sea por falta de previsión legal, ya sea por el avance vertiginosos de la tecnología, ya sea por la tensión generada entre los DDHH con los intereses comerciales creados por la Industria IT so pretexto de la libre innovación.

La República Argentina en el año 2019 mediante la Ley 27.483 aprobó el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal suscripto en la ciudad de Estrasburgo, Francia, el 28 de enero de 1981, así como también el protocolo adicional al Convenio.

El Convenio 108 posteriormente fue modificado en el mes de mayo de 2018 resultando en su continuador, el Convenio 108 +, aguardando a que nuestro país hiciera nuevamente adhesión a esta modificación.

Finalmente, la República Argentina adhirió al Convenio 108 + a través de la Ley 27.699 sancionada recientemente, con fecha 10 de noviembre de 2022. Si bien como ya dijimos nuestro país ya era un Estado - Parte de este convenio aún quedaba pendiente ratificar su modificación que respondía, según así surge del mismo convenio, a razones de "diversificación, intensificación, globalización del tratamiento de datos y el flujo de los datos personales".

En su articulado el Convenio 108 + establece que "El tratamiento de datos genéticos, datos personales relativos a delitos, procesos y condenas penales y medidas de seguridad relacionadas, **datos biométricos** que identifiquen de manera exclusiva a una persona, datos personales para la información que se divulgue relativa a origen racial o étnico, opinión política, afiliación a gremios, creencias religiosas o de otra índole, salud o vida sexual, sólo se permitirá cuando la ley establezca salvaguardas adecuadas que complementen las previstas en el presente Convenio. Dichas salvaguardas brindarán protección contra los riesgos que el

tratamiento de datos sensibles pueda generar para los intereses, derechos y libertades fundamentales del titular de los datos, especialmente el riesgo de discriminación.

NORMATIVA Y PAUTAS PARA SU RECOLECCIÓN Y TRATAMIENTO A TRAVÉS DE CÁMARAS DE VIDEOVIGILANCIA.

A continuación, haremos un breve recorrido por algunas de las normativas vigentes que pueden estar vinculadas a la protección de datos biométricos, especialmente aquellos que puedan ser capturados por sistemas de videovigilancia.

NORMATIVA UNESCO

Recomendación sobre la ética de la Inteligencia Artificial:

Esta recomendación fue aprobada por la Conferencia General de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) con fecha 23 de noviembre de 2021 y con respecto a la temática que nos ocupa establece respecto a los datos biométricos lo siguiente:

> *"Ámbito de Actuación 3: Política de Datos. Acápite 74: Los Estados Miembros deberían establecer sus políticas de datos o marcos equivalentes, o reforzar las políticas y marcos existentes, para garantizar la seguridad total de los datos personales y los datos sensibles que, de ser divulgados, puedan causar daños, lesiones o dificultades excepcionales a las personas. Cabe citar como ejemplos los datos relativos a infracciones, procesos penales y condenas, así como a las medidas de seguridad conexas; los* ***datos biométricos****, genéticos y de salud; y los datos personales como los relativos a la raza, el color, la ascendencia, el género, la edad, el idioma, la religión, las opiniones políticas, el origen nacional, étnico o social, la condición económica o social de nacimiento, la discapacidad o cualquier otra característica".*

Se hace especial mención de la consideración de cuestiones éticas y lo concerniente al impacto de la Inteligencia Artificial en el ámbito de los DDHH, en tal sentido establece que se presta especial atención a:

"…La identidad y la diversidad culturales, ya que las tecnologías de la IA pueden enriquecer las industrias culturales y creativas, pero también pueden dar lugar a una mayor concentración de la oferta de contenidos, los datos, los mercados y los ingresos de la cultura en manos de unos pocos actores, lo que puede tener **consecuencias negativas para la diversidad y el pluralismo de las lenguas, los medios de comunicación, las expresiones culturales, la participación y la igualdad**…"

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS.

La Agencia Española de Protección de Datos publicó una Guía sobre el uso de videocámaras para seguridad y otras finalidades donde realizó una compilación de la normativa vigente en la materia.

La legitimación en el uso de videovigilancia descansa en el cumplimiento de la misión del "interés público". Ello estaría cumplimentado en la finalidad de garantizar la seguridad de personas, bienes e instalaciones.

Los principales lineamientos sobre el uso de videovigilancia que pueden destacarse son los siguientes.

- La recolección de imágenes deberá responder por tanto al principio de finalidad, debiendo circunscribirse su captura únicamente a los fines para los cuales se requirió la videovigilancia que por supuesto estará amparada en el interés legítimo arriba explicado.
- Aplica al principio de minimización de datos en materia de "videovigilancia" para ello se pueden utilizar técnicas como la denominada "enmascaramiento" de imágenes.
- La responsabilidad proactiva en el tratamiento de los datos.

El RGPD establece un catálogo de medidas que el responsable y, en ocasiones los encargados, deben aplicar para garantizar que los tratamientos son conformes a la norma europea. No obstante, es preciso matizar que no en todos los casos, estas medidas deben aplicarse obligatoriamente.

- BRECHAS DE SEGURIDAD: Se notifica a la AEPD. Plazo máximo de 72 horas. El contenido mínimo de la comunicación de la brecha de seguridad a la AEPD deberá contener:

  · naturaleza de la brecha de seguridad:

  · categorías de afectados (ej. menores, discapacitados, empleados, ciudadanos)

  · número aproximado de afectados

  · categorías de datos comprometidos (ej. identificativos, salud, laborales)

  · número de registros de datos personales afectados

  · nombre y datos de contacto del Delegado de Protección de Datos

  · posibles consecuencias de la brecha de seguridad sufrida

  · medidas adoptadas o propuestas para remediar esta brecha.

- EVALUACION DE IMPACTO: Se trata de una herramienta de carácter preventivo que debe realizar el responsable del tratamiento para poder identificar, evaluar y gestionar los riesgos a los que están expuestas sus actividades de tratamiento con el objetivo de garantizar los derechos y libertades de las personas físicas.

- PROTECCIÓ DE DATOS POR DISEÑO: El principio de protección de datos desde el diseño supone que la protección de datos ha de estar presente en las primeras fases de concepción de un proyecto y formar parte de la lista de elementos a considerar antes de iniciar las sucesivas etapas de desarrollo.
- PROTECCIÓN DE DATOS POR DEFECTO: Supone que se adopten las medidas técnicas y organizativas apropiadas para garantizar que, como su nombre indica, por defecto, sólo sean objeto de tratamiento los datos personales necesarios para cada uno de los fines específicos del tratamiento.
- DERECHO DE INFORMACIÓN: Otra de las obligaciones que conlleva el uso de la videovigilancia con fines de seguridad, en relación con la protección de datos, es cumplir con el derecho de información, mediante un distintivo informativo.

A tal efecto propone una infografía a título de ejemplo para colocar en los sectores videovigilados y permitir el derecho de información:

- CONTRATACIÓN DE SERVCIOS DE VIDEOVIGILIANCIA DE TERCEROS: Cuando una entidad que ha instalado cámaras de videovigilancia encarga a un tercero la gestión de estas, facilitando el acceso a las imágenes, deberá existir un contrato u otro acto jurídico con arreglo al Derecho de la Unión Europea, en el que se establezca el objeto, la duración, la naturaleza y finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable.
- CONTENIDO MÍNIMO DEL CONTRATO: Las instrucciones del responsable del tratamiento. El deber de confidencialidad. Las medidas de seguridad. El régimen de la subcontratación. La forma en que el encargado asistirá al responsable en el cumplimiento de responder el ejercicio de los derechos de los afectados. La colaboración en el cumplimiento de las obligaciones del responsable. El destino de los datos al finalizar la prestación.
- EMPRESAS DE SEGURIDAD: En este sentido, y respecto a la prestación de este tipo de servicios por las empresas de seguridad, éstas tendrán la condición de encargado de tratamiento. Sin embargo, si la empresa de seguridad gestiona el sistema de videovigilancia en el domicilio de las personas físicas, adquiere la condición de responsable del tratamiento.
- PLAZO DE CONSERVACIÓN DE VIDEOGRABACIONES: Plazo de conservación de **máximo de un mes.** No será de cancelación sino de supresión, salvo en aquellos supuestos en que se deban conservar para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones.
- DERECHOS DE LAS PERSONAS (ARCO): Acceso, rectificación, supresión, limitación del tratamiento, portabilidad, oposición, y oposición a decisiones individuales automatizadas. No obstante, **el ejercicio de estos derechos debe ser matizado en el ámbito de la videovigilancia**. En primer lugar, no resulta posible el ejercicio del derecho de rectificación ya que por la naturaleza de los datos -imágenes tomadas de la realidad que reflejan un hecho objetivo-, se trataría del ejercicio de un derecho de contenido imposible. En segundo lugar, tampoco sería aplicable el derecho de portabilidad ya que, aunque se trata de un tratamiento automatizado, la legitimación no se basa ni en el consentimiento ni en la ejecución de un contrato. En tercer lugar,

no se aplicaría parte del contenido del derecho a la limitación del tratamiento, en su aspecto de "cancelación cautelar" que está vinculada al ejercicio de los derechos de rectificación y oposición.

- COMUNICACIONES DE IMAGENES A TERCEROS: actividades realizadas por la Policía u otras fuerzas y cuerpos de seguridad, que también pueden incluir el ejercicio de autoridad mediante medidas coercitivas, como es el caso de las actuaciones policiales en manifestaciones, grandes acontecimientos deportivos y disturbios, así como el mantenimiento del orden público. Las grabaciones se entregan por pedido fundado: En todo caso, la petición de las grabaciones en los supuestos descritos debe realizarse de forma motivada, y la entrega de las mismas debe ser proporcional a la finalidad del requerimiento realizado, sin que se produzca una comunicación indiscriminada.
- ESPACIOS PÚBLICOS: tiene normativa propia: Respecto a las videocámaras instaladas en espacios públicos, habrá que acudir a la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos.
- ESPACIOS PRIVADOS: La ley 5/2014, de 4 de abril, de Seguridad Privada hace referencia a la utilización de cámaras de videovigilancia en espacios privados. También existe otra normativa de ámbito más específico que habilita al uso de la videovigilancia, como puede ser la referente al sector de los espectáculos deportivos.
- ESPECTACULOS DEPORTIVOS: Deberán instalar circuitos cerrados de televisión para grabar el acceso y el aforo completo del recinto deportivo, inclusive los aledaños en que puedan producirse aglomeraciones de público. Además, adoptarán las medidas necesarias para garantizar su buen estado de conservación y correcto funcionamiento.
- ENTIDADES FINANCIERAS: La instalación de este tipo de cámaras y videocámaras es de titularidad privada, siendo las propias entidades las responsables de las mismas. Las imágenes estarán exclusivamente a disposición de las autoridades judiciales y de las Fuerzas y Cuerpos de Seguridad, a las que se deberán facilitar inmediatamente aquellas que se refieran a la comisión de hechos delictivos. En principio, las imágenes sólo

podrán ser visualizadas por las Fuerzas y Cuerpos de Seguridad, los Jueces y Tribunales, por la Inspección de la Agencia Española de Protección de Datos.

- JOYERIAS, GALERIA DE ARTE Y TIENDA DE ANTIGUEDADES: Estos establecimientos deberán informar al público sobre la implantación de estos sistemas de cámaras o videocámaras conforme a la regla general, es decir, mediante la colocación de carteles informativos y disposición de formularios informativos. En este caso, la obligación de adoptar medidas de seguridad por estas entidades no sustituye las previsiones del RGPD. La instalación de este tipo de cámaras y videocámaras es de titularidad privada, siendo las propias entidades las responsables de las mismas.
- GRABACIONES POR DETECTIVES PRIVADOS: La AEPD considera lícito el tratamiento de datos de carácter personal que puedan derivarse de la realización de actividades de investigación privada, siempre que resulte ajustado a los principios de limitación de la finalidad y minimización y que quede circunscrito al ámbito del encargo en cuyo seno se desarrolla la actividad investigadora, respetando los citados principios y siendo regulada esta actividad mediante la existencia de una relación contractual.
- COMUNIDAD DE PROPIETARIOS: Tratándose de la captación de imágenes en zonas o elementos comunes de comunidades de propietarios, la adopción de esta medida requiere el acuerdo de la junta de propietarios en los términos previstos en la Ley de Propiedad Horizontal. Las cámaras sólo podrán captar las zonas comunes de la comunidad, no siendo factible la grabación de imágenes de la vía pública, a excepción de una franja mínima de los accesos al inmueble. Tampoco se podrá realizar la captación de imágenes de terrenos y viviendas colindantes o de cualquier otro espacio ajeno. En este último caso, si se usan cámaras orientables y/o con zoom, será necesaria la instalación de máscaras de privacidad para evitar esta grabación. El acceso a las imágenes estará restringido a las personas designadas por la comunidad de propietarios. En ningún caso estarán accesibles a los vecinos mediante canal de televisión comunitaria. Si el acceso se realiza con conexión a internet, se restringirá con un código de usuario y una contraseña (o cualquier otro medio que garantice la identificación y autenticación unívoca), que sólo serán conocidos por las personas autorizadas a

acceder a dichas imágenes. Una vez instalado el sistema, se recomienda el cambio regular de la contraseña, evitando las fácilmente deducibles.

- ENTORNOS ESCOLARES: La instalación de cámaras de videovigilancia en estos entornos con el fin de controlar conductas que puedan afectar a la seguridad, sólo será legítima cuando la medida sea proporcional en relación con la infracción que se pretenda evitar y, en ningún caso, debe suponer el medio inicial para llevar a cabo funciones de vigilancia. La zona objeto de videovigilancia será la mínima imprescindible abarcando espacios públicos como accesos o pasillos. No podrán instalarse en espacios protegidos por el derecho a la intimidad como baños, vestuarios o aquellos en los que se desarrollen actividades cuya captación pueda afectar a la imagen o a la vida privada como los gimnasios. Salvo en circunstancias excepcionales, no podrán utilizarse con fines de control de asistencia escolar. Se pueden instalar cámaras en los patios de recreo y comedores cuando la instalación responda a la protección del interés superior del menor, toda vez que, sin perjuicio de otras actuaciones como el control presencial por adultos, se trata de espacios en los que se pueden producir acciones que pongan en riesgo su integridad física, psicológica y emocional. La grabación en las aulas mientras los alumnos realizan pruebas de nivel de conocimientos sería desproporcionado.

Respecto a la temática escolar el Gabinete Jurídico de la Agencia Española de Protección de Datos Personales se expidió sobre la proporcionalidad en el uso de la huella dactilar de alumnos de un establecimiento escolar [17]. El motivo de la consulta pretendía establecer un sistema de control para gestionar las ausencias y retrasos de los alumnos, basado en la obtención de la huella dactilar de éstos. Mediante dicha huella dactilar pretendía gestionarse el control de acceso – entradas y salidas – de los alumnos de un centro escolar. En dicho informe concluyó el Gabinete Jurídico que resultaba desproporcionado y por ello contrario a lo dispuesto en el artículo 4.1 de la Ley Orgánica 15/1999, la utilización de la huella dactilar como medio para controlar el acceso de los alumnos al centro escolar y tal finalidad puede

[17] Informe 368/2006 AEPD

conseguirse, sin duda, de una manera menos intrusiva en relación con los derechos de los alumnos.

Otro caso en medio del contexto de exámenes durante la pandemia de COVID – 19 remonta a la Universidad Estatal de Cleveland –Cleveland State University-, Aaron Ogletree, en la que un alumno alegó que el escaneo de su habitación al momento de rendir un examen remoto conculcaba sus derechos.

El Tribunal de Distrito de los Estados Unidos para el Distrito Norte de Ohio, división Este, hizo lugar a su planteo sosteniendo que se había violado la expectativa razonable de privacidad [18].

- SANIDAD Y CENTROS DE ASISTENCIA: Aunque la finalidad sea la videovigilancia, se considera desproporcionado el uso de cámaras en las habitaciones de los pacientes para que sus familiares puedan visionar en "streaming" su estado de salud.

- CAMARAS ON BOARD: Este tipo de tecnología consiste en instalar una cámara dentro de un vehículo o también en ocasiones en el casco del conductor, e ir grabando todo el recorrido que se realiza con el mismo. Incluso, existen vehículos que ya llevan incluidos este tipo de cámaras. Las grabaciones para una finalidad "doméstica" estarían exceptuadas de la aplicación de la normativa de protección de datos, excepto que las mismas luego sea publicadas en internet. Las grabaciones con la finalidad de obtener pruebas para determinar responsabilidades asociadas a la producción de un suceso a los fines probatorios, como el caso de un accidente de tránsito pueden ser permitidas por la aplicación de la regla del interés legítimo (art.6.1. f del RGPD), en base al derecho a la tutela judicial efectiva, derecho fundamental recogido por la Constitución Española de 1978.

[18] https://palabrasdelderecho.com.ar/articulo/3997/Estados-Unidos-es-inconstitucional-grabar-las-habitaciones-de-los-alumnos-al-rendir-examenes-virtuales

- DRONES: Otra de las tecnologías que junto a las cámaras "on-board" se han popularizado en los últimos años son las aeronaves pilotadas de forma remota, más conocidas con el nombre de drones. Los drones pueden llevar o no, sistemas de procesamiento de información (de datos en general) de muy diversos tipos: sistemas de grabación de imagen, sistemas de detección (sensores ópticos o electrónicos, infrarrojos, de humos), o equipos de radiofrecuencia (antenas para capturar emisiones de radio o de wi-fi).

- La operativa de drones implicará:

· Valorar la posibilidad de realizar una Evaluación de Impacto de la Protección de Datos, atendiendo al tipo de dron y la tecnología de captación de datos para el tratamiento.

· Evitar captar o tratar datos innecesarios a la finalidad pretendida.

· Informar de la forma más apropiada y con carácter previo a los afectados, incluyendo una indicación clara de quién es el responsable y las finalidades del tratamiento, así como las indicaciones claras y específicas para el ejercicio de derechos.

· Establecer medidas de seguridad apropiadas para los riesgos que representan el tratamiento pretendido.

· Borrar y/o anonimizar cualquier dato innecesario.

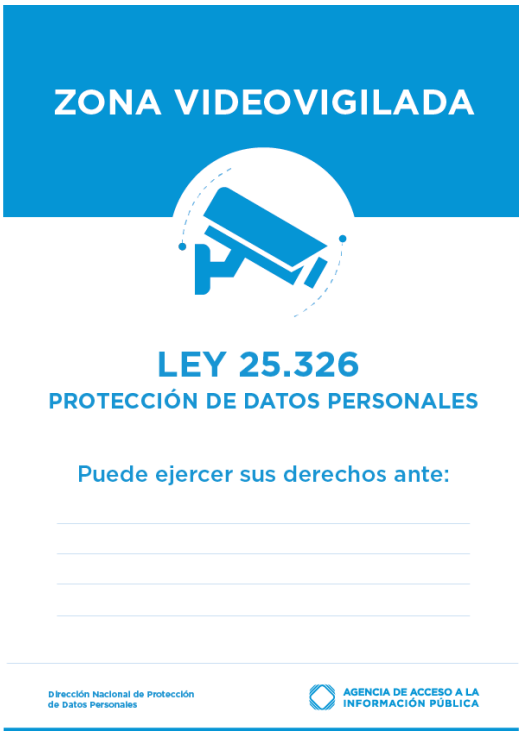
Los siguientes supuestos excluyen el tratamiento de protección de datos personales:

- Fines domésticos o privados.
- Imágenes publicadas en Medios de comunicación masiva (Libertad de Expresión).
- Uso de cámaras simuladas.
- Imágenes turísticas de panorámica general (No permite que se identifiquen personas).

ESTADO NACIONAL ARGENTINO Y CIUDAD DE BUENOS AIRES.

En el ámbito de la Nación Argentina la Dirección de Protección de Datos Personales dictó la Disposición 10/2015 de fecha 24 de febrero de 2015 mediante la cual se aprobaron las condiciones de licitud para las actividades de recolección y posterior tratamiento de imágenes digitales de personas con fines de seguridad. Estas condiciones están redactadas en el Anexo I de la disposición. Esta actividad será lícita en la medida que cuente con el consentimiento previo e informado del titular del dato en los términos previstos por los artículos 5° y 6° de la Ley N° 25.326.

- Al igual que el modelo español se requiere también en la disposición argentina el cumplimiento del requisito de información previa al titular del dato podrá lograrse a través de carteles que en forma clara indiquen al público la existencia de dichos dispositivos de seguridad los fines de la captación de las imágenes y el responsable del tratamiento con su domicilio y datos de contacto para el correcto ejercicio de los derechos por parte del titular del dato. Los espacios que cuenten con videovigilancia disponen de una publicación modelo editable para colocar en estos sectores y cumplimentar debidamente el deber de información.



Modelo editable de advertencia de uso de cámaras en el lugar aprobado también como Anexo 2 de la Disposición 10/2015 y que luego fuera reemplazada por su última versión el 31 de enero del año 2024 mediante Resolución 38/2024 de la Agencia de Acceso a la Información Pública como se ilustra a continuación:

Última versión instaurada por Resolución 38/2024 AAIP

- Las **excepciones a la solicitud del consentimiento** se encuentran determinadas en tres supuestos siempre y cuando la recolección de imágenes personales no implique una intromisión desproporcionada en su privacidad:

a) Realización de un evento privado (se realice o no en espacio público) en el que la recolección de los datos sea efectuada por parte del organizador o responsable del evento.

b) Sea realizada por el Estado en el ejercicio de sus funciones, siendo en principio suficiente notificación de los requisitos del artículo 6° de la Ley N° 25.326 su publicación en el Boletín Oficial (conforme artículo 22 de la Ley N° 25.326); sin perjuicio de ello, en las oficinas y/o establecimientos públicos deberá hacerse saber dicha recolección conforme lo dispuesto en el segundo párrafo del presente artículo.

c) los datos se recolecten dentro de un predio de uso propio (por ejemplo: ser propiedad privada, alquilado, concesión pública, etc.) y/o su perímetro sin invadir el espacio de uso público o de terceros, salvo en aquello que resulte una consecuencia inevitable, debiendo restringirlo al mínimo necesario y previendo mecanismos razonables para que el público y/o los terceros se informen de una eventual recolección de su información personal en tales circunstancias.

- Los datos recolectados deben respetar el requisito de finalidad y de calidad de los datos. (adecuados, pertinentes y no excesivos).
- La eliminación inmediata de imágenes que puedan ser conculcadoras de los derechos de privacidad de las personas.
- A diferencia de la normativa española no determina un plazo cierto para la conservación de dichas imágenes (recordemos que en España es de un mes) sino que sólo limita a la obligación de destruirlas cuando hayan cumplido su finalidad. El plazo de conservación quedará librado al que estipule el responsable de la recolección y tratamiento y que deberá informar en un manual de uso.
- Deberá asegurar las medidas de seguridad y confidencialidad de los datos personales.

- El responsable del tratamiento debe cumplir con el deber de información hacia los titulares de los datos brindando toda aquella información que le fuera requerida.
- Deberán inscribirse en el REGISTRO NACIONAL DE BASES DE DATOS dependiente de la Dirección Nacional de Protección de Datos Personales.
- Deberán contar con un manual o política de tratamiento de datos personales y privacidad, que ponga en práctica las condiciones de licitud previstas en la Ley N° 25.326 para el caso concreto.

Éste deberá contener al menos la siguiente información:

- Forma de la recolección; referencia de los lugares, fechas y horarios en los que se prevé que operarán.
- Plazo de conservación de los datos.
- Mecanismos técnicos de seguridad y confidencialidad previstos.
- Medidas dispuestas para el cumplimiento de los derechos del titular del dato contemplados en los artículos 14, 15 y 16 de la Ley N° 25.326
- Los argumentos que justifiquen la toma de fotografías para el ingreso al predio, en caso de disponerse dicha medida de seguridad.

Con respecto al ámbito de la ciudad de Buenos Aires la Ley 5688 regula la Seguridad en el ámbito de la Ciudad de Buenos Aires y en función de ello los aspectos de dicha ley que tienen correlación con la temática de videovigilancia y biometría son las enunciadas a continuación:

En el Libro VI. Título I Artículos 436 y consecutivos regula la actuación de las empresas de seguridad privadas dentro del ámbito de la Ciudad de Buenos Aires.

- El artículo 439 inciso d) hace mención a los servicios de vigilancia a través de recursos tecnológicos: Los de vigilancia por medios electrónicos, ópticos y electroópticos. Tiene

por objeto brindar servicios con dispositivos centrales de observación, registro de imagen, audio y alarmas. [19]

- Dentro de sus cláusulas transitorias el Libro VII expresamente hace mención al "**SISTEMA INTEGRAL DE VIDEOVIGILANCIA**" en su cláusula trigésima: "En el plazo de dos (2) meses a partir de la promulgación de la presente ley, la autoridad de aplicación procederá a confeccionar los informes acerca de las instalaciones de videocámaras actualmente existentes, así como a destruir aquellas grabaciones que no reúnan las condiciones legales para su conservación".
- **Responsable Técnico – Obligatoriedad de Inscripción**: El artículo 444 prevé que los prestadores que incluyan en sus servicios los descriptos en el Artículo 439, inciso 2, apartado d, deben cumplir con los siguientes requisitos específicos:

1. Designar un responsable técnico, graduado universitario en ingeniería electrónica, sistemas, informática, programación, comunicaciones o telecomunicaciones, licenciatura en tecnología aplicada a la seguridad o carrera afín; en este último supuesto será la autoridad de aplicación mediante resolución fundada, quien apruebe la presentación de títulos de nuevas carreras de grado que sea menester. El director técnico podrá acreditarse como responsable técnico, si cumple con los requisitos suficientes para desempeñarse en ambos cargos simultáneamente.

2. Contar con certificados de aprobación de las instalaciones, emitidos por autoridad competente, de acuerdo a lo que la reglamentación determine.

3. Las empresas que brinden servicios de sistemas de vigilancia, monitoreo y alarma electrónica deben inscribir a los responsables técnicos, técnicos instaladores y operadores de monitoreo en el registro creado a tales efectos. Solo sus inscriptos se encuentran autorizados para la supervisión, instalación y operatividad de dichos servicios.

- **Responsable técnico – Solidaridad:** El artículo 446 establece los alcances de las funciones del responsable técnico: El responsable técnico es la persona que asegura el

[19] Inscripción al Registro de Cámaras de Videovigilancia Privadas – RECAVIP (Ley 5688 Libro VII Título IV - Resol 2019-826-GCABA-MJYSGC) | Buenos Aires Ciudad - Gobierno de la Ciudad Autónoma de Buenos Aires

funcionamiento técnico de las instalaciones y del equipamiento que posee la prestadora de servicios de vigilancia electrónica, como así también del que fuera entregado a los prestatarios. Responde solidariamente con la prestadora en caso de incumplimiento cuando éste se deba a fallas de orden técnico.

- Prohibiciones: Artículo 450.- Los prestadores tienen expresamente prohibido ….:

  7. Dar a conocer a terceros la información de la que tomen conocimiento por el ejercicio de la actividad, sobre sus clientes, personas relacionadas con éstos, así como de los bienes o efectos que custodien.

  8. Interceptar o captar el contenido de comunicaciones postales, telefónicas, telegráficas, radiofónicas, por télex, facsímil o cualquier otro medio de transmisión de voces, imágenes o datos a distancia.

- Artículo 461.- El Ministerio de Justicia y Seguridad es la autoridad de aplicación, fiscalización y control del cumplimiento del presente Libro por parte de las empresas de seguridad privada y sus prestatarios, teniendo al respecto las siguientes funciones:

  9. Llevar el registro único de técnicos instaladores de sistemas de vigilancia, monitoreo y alarma electrónica.

- La ley cuyo articulado se viene relacionando en su LIBRO VII regula de manera expresa el **SISTEMA PÚBLICO INTEGRAL DE VIDEO VIGILANCIA DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES** en su artículo 474. El objeto y alcance de las facultades de videovigilancia se encuentran estipuladas en el artículo 475 y permite al Poder Ejecutivo:
  - grabar imágenes en lugares públicos y a los que se refieren los artículos 485 y 486, estableciendo específicamente el posterior tratamiento de tales imágenes y el régimen de garantías de los derechos fundamentales y libertades públicas de los ciudadanos que habrá de respetarse ineludiblemente en las sucesivas fases de grabación y uso de las imágenes.
- Deber de cumplimiento de los principios de proporcionalidad y razonabilidad, en su doble versión de procedencia y de intervención mínima. La procedencia determina que sólo podrá emplearse cuando resulte adecuado, en una situación concreta, para

asegurar la convivencia ciudadana, la utilización pacífica de las vías y espacios públicos, la elaboración de políticas públicas de planificación urbana, así como para la prevención de faltas, contravenciones y delitos y otras infracciones relacionadas con la seguridad pública. La intervención mínima exige la ponderación en cada caso de la finalidad pretendida y **la posible afectación al derecho a la propia imagen, a la intimidad y a la privacidad de las personas**, de conformidad con los principios consagrados en la Constitución Nacional y la Constitución de la Ciudad Autónoma de Buenos Aires.

PRINCIPIOS RECTORES: Artículo 477.- La gestión del sistema público integral de video vigilancia, se sujeta a los siguientes principios rectores:

1. Planificación estratégica: se rige por medio de planes de acción basados en criterios estratégico-institucionales que son comprobados mediante los ejercicios de la gestión.
2. Tecnología e innovación: promueve el uso intensivo de nuevas tecnologías para el abordaje de sus funciones y la mejora de la gestión institucional.
3. Información estadística confiable: reúne registros de datos sobre la estadística y de los mapas de ocurrencia de hechos delictivos, a los efectos de desarrollar informes eficaces y oportunos sobre la materia en la Ciudad de Buenos Aires.
4. Coordinación: articula su esfuerzo operacional con el resto de los componentes que intervienen en el sistema integral de seguridad pública.

INSTALACIÓN Y USO DE LOS SISTEMAS DE VIDEO VIGILANCIA POR PARTE DEL PODER EJECUTIVO:

- Procederá en la medida en que resulte de utilidad concreta a fin de proporcionar información necesaria para adoptar eventuales medidas de gobierno relacionadas con la utilización del espacio público.

- El Poder Ejecutivo no puede utilizar los sistemas de video vigilancia para tomar imágenes del interior de propiedades privadas, salvo por autorización judicial expresa.

- Pueden instalarse sistemas de video vigilancia en espacios públicos salvo cuando se afecte de forma directa y grave la intimidad de las personas.

- En ningún caso los sistemas de video vigilancia pueden captar sonidos, excepto en el caso de que sea accionado el dispositivo de emergencia, y al solo efecto de establecer la comunicación con el solicitante.
- La captación de sonidos se debe desactivar automáticamente a los tres (3) minutos de pulsado el dispositivo y únicamente puede reactivarse mediante una nueva pulsación del dispositivo de emergencia. El sistema debe impedir su activación por parte del operador del centro de monitoreo.

Si en forma accidental se obtuviesen imágenes cuya captación resulte violatoria de la normativa, deben ser destruidas inmediatamente por quien tenga la responsabilidad de su custodia.

- Lector Inteligente de Patentes de GCBA. Las referencias a sistemas de videovigilancia se entienden hechas a cualquier medio técnico análogo y, en general, a cualquier sistema que permita las grabaciones previstas en esta normativa.
- IMÁGENES: La captación y almacenamiento de imágenes en los términos previstos en la normativa, así como las actividades preparatorias, **no se consideran intromisiones ilegítimas en el derecho a la intimidad personal y familiar y a la propia imagen**, siempre y cuando no contradigan lo establecido en la Constitución Nacional, la Constitución de la Ciudad Autónoma de Buenos Aires, la Ley Nacional N° 25.326 y la Ley 1845 (texto consolidado por Ley 5454).
- **Intervención de las Fuerzas de Seguridad**: La obtención de imágenes no tiene por objetivo la formulación de denuncias judiciales por parte de la autoridad de aplicación. En caso de detectarse la ocurrencia flagrante de un hecho delictivo o contravencional la autoridad de aplicación arbitra los medios necesarios para dar inmediato aviso a la fuerza de seguridad correspondiente y pone la cinta o soporte original de las imágenes en su integridad a disposición judicial con la mayor celeridad posible.
- **Intervención al Órgano Administrativo: Foto multas y Detección de Patentes Automotores**: Si la grabación captara hechos que pudieran ser constitutivos de infracciones administrativas se remiten al órgano competente, de inmediato, para el inicio del procedimiento sancionatorio.
- **Intervención de funcionario competente**: El acceso a toda información obtenida como consecuencia de las grabaciones se restringe a aquellos funcionarios que el Poder Ejecutivo individualmente determine, por razón de su función específica.
- **Prohibición de Cesión de imágenes**: Se prohíbe la cesión o copia de las imágenes salvo en los supuestos previstos en esta normativa o en aquellos que se dispongan por vía reglamentaria o en el propio interés del titular.
- **Deber de reserva, confidencialidad y sigilo**: Cualquier persona que por razón del ejercicio de sus funciones tenga acceso a las grabaciones debe observar la debida reserva, confidencialidad y sigilo resultando de aplicación, en caso contrario, lo dispuesto en la legislación penal. Cuando no correspondan responsabilidades penales, las infracciones a lo dispuesto en esta normativa son sancionadas con arreglo al

régimen disciplinario correspondiente a los infractores y, en su defecto, con sujeción al régimen de sanciones en materia de protección de datos de carácter personal.

- **Plazo de custodia de grabaciones - Excepciones**: Las grabaciones son destruidas una vez transcurridos sesenta (60) días corridos desde su captación. No serán destruidas las que estén relacionadas con infracciones penales o administrativas en materia de seguridad pública, con una investigación policial en curso o con un procedimiento judicial o administrativo abierto.

ANÁLISIS JURISPRUDENCIAL.

(SRFP) El Sistema de Reconocimiento Facial de Prófugos. Inconstitucionalidad del artículo 1° de la Resolución N° 398/MJYSGC/2019 de fecha 24 de abril de 2019.-
Acciones de Amparo contra el Estado:

Uno de los casos judiciales más mediáticos que debió afrontar el Estado local en materia de videovigilancia y recolección y tratamiento de datos biométricos ha sido la acción de amparo que fuera circunstanciada ante el Juzgado de Primera Instancia en lo Contencioso Administrativo y Tributario N° 4, Secretaría N° 7 de la Ciudad de Buenos Aires en los autos caratulados. "**OBSERVATORIO DE DERECHO INFORMÁTICO ARGENTINO O.D.I.A. Y OTROS CONTRA GCBA SOBRE AMPARO – OTROS"**

Número: EXP 182908/2020-0. CUIJ: EXP J-01-00409611-4/2020-0. Actuación Nro.: 2453371/2022.-

Este fallo resulta trascendente en materia de protección de datos personales biométricos y configura un claro límite a las pretendidas funciones de hipervigilancia que el Estado de la Ciudad de Buenos Aires buscaba implementar.

Dentro de este pronunciamiento podemos determinar las siguientes cuestiones atinentes a la videovigilancia y la recolección y tratamiento de los datos biométricos:

Uso de nuevas tecnologías – Evaluación de Impacto: "Con el fin de **mitigar los riesgos que entraña el uso de las nuevas tecnologías, el tratamiento automatizado de datos y la inteligencia artificial**, la Agencia de Acceso a la Información Pública de la Nación y su par de la República Oriental del Uruguay, han diseñado un mecanismo de carácter

preventivo que busca minimizar los potenciales daños a la privacidad llamado **"Guía para la Evaluación de Impacto en la Protección de Datos (EIPD)".** Para ello, las Autoridades de Control han seguido las más modernas legislaciones y guías en la materia, con particular atención a los principios y las directrices establecidas en el Convenio previamente referido. Allí, **considerando que el tratamiento de datos personales puede provocar impactos en los derechos de las personas que deben ser identificados, gestionados, minimizados o eliminados** para cumplir con la normativa vigente se expone que una Evaluación de Impacto en la Protección de Datos (EIPD) es un proceso que las organizaciones deben efectuar para identificar y tratar los riesgos que puedan producir sus actividades habituales, sus nuevos proyectos o sus políticas corporativas cuando involucran el tratamiento de datos personales. También se pone de relieve que la EIPD resulta desde hace tiempo una buena práctica reconocida por normas técnicas internacionales y que "su objetivo es reforzar los principios en materia de protección de datos personales y orientar al responsable a los efectos de su cumplimiento, en especial cuando la complejidad del proyecto o actividad bajo análisis exige un examen más detallado."

Evaluación de Impacto de Protección de Datos: en todos los casos, la EIPD es un **proceso que genera valor para la organización que la lleva adelante**. Por un lado, les permite a los organismos públicos establecer lazos de confianza con la ciudadanía, y, por otro, en el caso de las empresas privadas, evita potenciales costos reputacionales y fideliza a los clientes o consumidores. Ello, con el beneficio de que no es necesariamente un proceso complejo e injustificadamente oneroso. Sin importar cuál sea la metodología aplicada a la EIPD, ésta **debe asegurar la homogeneidad y comparabilidad de los resultados, mediante un proceso sistemático y repetible, garantizando así la objetividad del proceso**.

La Evaluación de Impacto en la Protección de Datos (EIPD) **luce por excelencia como la herramienta más atinada y fundamental a fin de abordar los efectos que la implementación del SRFP** –o cualquier otro sistema que opere con datos personales– puede tener sobre los derechos humanos de quienes, en este caso, transitan la CABA.

Sistema de Reconocimiento Facial de Prófugos: Se puso en marcha el SRFP [20] **sin garantizar que éste cuente con los organismos de control que el cuerpo legal tanto nacional como internacional requieren**, lo que se da de bruces con el principio de legalidad que debe regir todo accionar de la Administración.

El sistema debe ser comprendido de modo integral, en su totalidad y no en forma compartimentada. Más allá de que la CoNaRC [21] no se encuentre dentro de la órbita del GCBA, lo cierto es que **en virtud de los efectos que trae aparejado el uso de esta base en el marco del SRFP, deben desarrollarse mecanismos de articulación concretos para eliminar situaciones que vayan en detrimento de los derechos de las personas** y ese es el sentido de los controles establecidos en el ámbito de la Ciudad pero que no se cumplen.

Base de datos – Borrados físicos y Borrados manuales – Diferencias y Discrepancias en las tablas de datos: Los errores en la base de datos per se no generarían, en el marco de lo debatido en autos, una afectación de los derechos de las personas. Empero, en la utilización de aquélla por medio del SRFP se advierte lo contrario, y más aún **ante la orfandad de controles legales, tales como la Defensoría del Pueblo de la Ciudad, la Comisión en la Legislatura, auditorías internas**, etc. Sobre este punto resulta necesario aclarar lo siguiente. El GCBA, refiriéndose a esta base de datos, aduce que "desde los últimos ajustes en la configuración del sistema en septiembre de 2019, **no hubo falsos positivos**" (ver actuación nº 982777/22 del 29/04/2022) y el Ministerio de Justicia y Seguridad, sostiene que "a partir de septiembre del 2019, a raíz de la implementación de una pluralidad de optimizaciones tecnológicas (referenciadas en el punto h), no se han registrado falsos positivos" (actuación n° 111120/22). **Sin embargo, los informes efectuados por el Defensor del Pueblo y por el Director del Registro Nacional de Reincidencia fueron emitidos el 06/08/2020 y 1/11/2021 respectivamente. Es decir, tiempo después de haberse realizado la depuración referida por el demandado.** Es más, el propio Director

[20](SRFP) Sistema de Reconocimiento Facial de Prófugos. Instrumento comprendido dentro del Sistema Público de Video Vigilancia de la Ciudad Autónoma de Buenos Aires, el cual mediante una cámara de video vigilancia reconoce los rostros de las personas requeridas por orden judicial, registradas en las Bases de Datos del Sistema de Consulta Nacional de Rebeldías y Capturas (CONARC) del Registro de Reincidencia del Ministerio de Justicia y DDHH de la Nación.
[21] Base de Datos de Consulta Nacional de Rebeldías y Capturas.

asumió que "a pesar de realizarse los pertinentes contralores y relevamientos permanentes de la información contenida en dicha base de datos" el sistema puede, no obstante, arrojar falsos positivos. **La mera eventualidad de estas falencias con las consecuencias que se derivan en los derechos personalísimos de las personas afectadas y la ausencia de controles -no por no estar contemplados en las leyes sino por la ausencia de debida implementación conforme a ellas-, demuestra un grave grado de riesgo de vulneración de derechos personales**."

Ausencia de la Comisión Especial de Seguimiento de los Sistemas de Video Vigilancia – Incumplimiento de su creación- Incumplimiento de registración de base de datos de videovigilancia – Vicios de Nulidad Insanable en la implementación del SRFP: El artículo 495 bis de la Ley 5688 crea la Comisión Especial de Seguimiento de los Sistemas de Video Vigilancia. Ella, debe estar **integrada por los/as Presidentes/as de las Comisiones de Justicia y de Seguridad, y tres diputados/as designados por la Vicepresidencia Primera del cuerpo.** Y, prevé la posibilidad de "**convocar a especialistas y organizaciones de la sociedad civil para analizar y proponer sobre los aspectos que son de su incumbencia**". Es decir, debe ser conformada por representantes escogidos por el pueblo y con la posibilidad de ser convocados, garantizando así la participación indirecta y directa de les ciudadanes. **La omisión respecto de la creación de la Comisión Especial de Seguimiento de los Sistemas de Video Vigilancia sumado a la nula convocatoria de la ciudadanía a debatir las cuestiones relativas a la implementación y funcionamiento Sistema de Reconocimiento Facial de Prófugos, que como surge de las probanzas de autos, tiene disfuncionalidades varias, hace que el resultado sea que no hay garantías adecuadas efectivas con relación la intimidad, la privacidad, el honor, por el contrario están, en un continuo, en condiciones de absoluto riesgo de ser violadas**. Ello en cuanto se ha privado tanto a habitantes, como legisladores y organizaciones especializadas, de intervenir conforme lo ordena la Constitución Local y la ley de Seguridad Pública a colaborar en la mejor decisión a adoptar respecto a la creación, funcionamiento e implementación del SRFP.

En lo que respecta a los mecanismos de control previstos en el régimen del SRFP **cabe concluir, en primer lugar, que la Comisión Especial de Seguimiento de los Sistemas de Video Vigilancia no ha sido constituida al día de fecha**. Dicha situación impide que el Poder Legislativo de la Ciudad ejerza las atribuciones informativas y de contralor que le fueron asignadas legalmente, de tal modo **configuraría un incumplimiento de lo dispuesto por el artículo 495 bis de la ley 5.688**. En segundo lugar, la Defensoría del Pueblo a su vez se encuentra imposibilitada de ejercer eficazmente sus funciones de control, en tanto no tendría a su disposición la información sobre los resultados de gestión del sistema que el Ministerio de Justicia y Seguridad de la CABA, en su carácter de órgano de aplicación, debe recabar, analizar y remitirle de conformidad a lo previsto por el artículo 495 de la ley 5.688. En tercer lugar, el Ministerio de Justicia y Seguridad tampoco realizó una auditoría interna. **Por otro lado, en torno a las fuentes de información del SRFP se observa que se está incumpliendo con lo dispuesto por los artículos 495 de la ley 5.688 y 23 de la ley 1.845 en tanto no se creó e inscribió el registro de datos relativo al sistema de videovigilancia**. Ello, a su vez, traería aparejado que el SRFP haga uso del registro de la CoNaRC –el que posee serias falencias– y **originaría detenciones irregulares**. De tal modo, el cúmulo de los defectos que el SRFP ostenta, según constancias probatorias en este expediente, **permite concluir que hay vicios de nulidad insanable a la hora de la implementación del SRFP**.

Afectación de Derechos Constitucionales: Se encuentra configurada una ilegítima restricción a los derechos constitucionales mencionados … Ahora bien, dicha restricción es consecuencia de:

a) La no constitución de la Comisión Especial en la Legislatura de la CABA.

b) La falta de informes por parte de la Defensoría del Pueblo CABA.

c) La inexistencia de un estudio de impacto sobre los derechos de los ciudadanos previa implementación del SRFP.

d) Las fallas en las bases de datos de las que se nutre el SRFP.

e) La exclusión de la participación ciudadana.

Es decir, **no se centra en el SRFP en sí, sino en las consecuencias que acarreó su prematura implementación y su utilización en condiciones precarias de respeto por los derechos y garantías de las personas.** De este modo, **toda vez que el artículo 1 de la resolución 398/MJYSGC/19 implementó el Sistema de Reconocimiento Facial de Prófugos sin encontrarse cumplidos los mecanismos normativos necesarios para garantizar el adecuado uso del sistema** –circunstancia que dio lugar a la afectación negativa de los derechos constitucionales referidos cuya protección no puede ser desconocida por la legislación ni por las autoridades locales– **corresponderá declarar su inconstitucionalidad**.

Resulta necesario que al momento en que vuelva a ser implementado el SRFP: a) se cuente con los mecanismos de control de este sistema, es decir se constituya la Comisión Especial de Seguimiento de los Sistemas de Video Vigilancia y que la Defensoría del Pueblo como órgano de contralor pueda ejercer eficazmente sus funciones; b) se constituya el registro de datos relativo al sistema de videovigilancia; c) se realice un estudio previo relativo al impacto sobre los datos personales y d) se convoque a la ciudadanía a debatir las cuestiones relativas al Sistema de Reconocimiento Facial de Prófugos. Pues, lo contrario se traduce en graves consecuencias sobre los derechos de las personas que transitan la Ciudad, tal como sucedió en los casos repasados.

Irregularidades en las bases de datos: Existen personas que NO deberían encontrarse dentro en la base de datos del SRFP, para que de forma posterior no sean localizados por el motor del SFRP. Estos registros deberían haberse eliminado (lógico, no físico) para que no sean detectados por el sistema **dando lugar a detenciones arbitrarias por falsos positivos**, tal es el caso de COLOMBO VIÑA, LEANDRO que al día de la presente su rostro (DATOS BIOMETRICOS) continúa siendo buscado y detectado por el SRFP, a pesar de que esta persona no fue requerida por la justicia**. Existen 84 registros de personas con imágenes (algunas no de RENAPER) ingresados bajo el nombre "INTERPOL" de los cuales hay 46 personas que solamente indican esta solicitud (INTERPOL) y 38 personas indican una posible causa judicial en curso**, no pudiendo dar certeza que sea una causa judicial en Argentina, además las fotografías contienen una marca de agua que indican ser propias del RENIEC del Perú. Ninguno de los registros (DNI) integra la base de CONARC,

por el contrario, poseen números de DNI que podrían no resultar ARGENTINOS (cantidad de dígitos). No encontrando ningún otro registro similar con el nombre de otra fuerza y organismo internacional. Como corolario del presente informe, los consultores técnicos (veedores) y perito interviniente, concluyen que **resulta de prístina claridad que el SRPF posee inconsistencias y errores en los procesos administrativos de alta/baja/modificación, observando también vestigios del entorno de desarrollo que deberían encontrarse solucionados al momento de implementarse en modelo de producción"**

En función de los hechos acreditados el Juzgado resolvió:

1) **Hacer lugar a la acción de amparo** declarando la **inconstitucionalidad del artículo 1 de la Resolución 398/19 en cuanto el SRFP se implementó sin cumplir con los recaudos legales de protección de los derechos personalísimos** de los habitantes de la Ciudad de Bs.As.

2) **Declarar la nulidad de todo lo actuado por el Ministerio de Justicia y Seguridad de la Ciudad de Bs.As. en el marco del SRFP**, en violación del artículo 3 del Anexo de la Resolución 398/19, es decir, sin orden judicial constatable.

3) **Supeditar la puesta en funcionamiento del SRFP a la constitución y debido funcionamiento de los órganos de control** (comisión especial de seguimiento de los sistemas de video vigilancia en el ámbito de la Legislatura de la Ciudad de Bs.As. –art. 495 bis ley 5.688–, y Defensoría del Pueblo de la Ciudad de Bs.As. –art. 22 ley 1845).

En el ámbito laboral:

El Tribunal Supremo de España le dio la razón a la cafetería Starbucks y consideró lícita la prueba de videovigilancia en la que se basó para despedir a una empleada que regalaba consumiciones a sus amigos.

CONCLUSIONES

Resulta fundamental comprender el alcance de la peligrosidad en la utilización de sistemas de videovigilancia que afectan la captura y tratamiento de los datos biométricos de las

personas, ya claramente reconocidos en la Legislación Argentina como DATO SENSIBLE, gracias a la incorporación a nuestra legislación de Tratados Internacionales como el aquí relacionado Convenio 108 +.

La actividad asesora y docente en materia de protección de datos personales ante la embestida tecnológica en la que nos encontramos inmersos los seres humanos no resultará suficiente en la medida que no exista compromiso de las Organizaciones Civiles y las Políticas Públicas de Estado que instalen estas temáticas en la educación primaria y secundaria fundamentalmente.

Tal como anticipáramos previamente el sistema democrático depende del ejercicio efectivo de la ciudadanía de los derechos amparados en la Constitución Nacional y demás normativa vigente. La concentración en los Estados y en las Organizaciones Privadas de recursos tecnológicos que invadan la privacidad y la libertad de los individuos, así como sus derechos fundamentales son el puntapié inicial para permitir el camino a regímenes totalitarios que torna en ilusoria la autodeterminación informativa dinámica.

La Industria IT deberá contar con normativa ética y sujetarse al cumplimiento estricto de la normativa existente en materia de Protección de Datos Personales, entendiendo que la privacidad se impone a un errado concepto de innovación.

Los sistemas de vigilancia implementados por el Estado deben ser objeto de la más estricta normativa y del contralor de los otros poderes públicos y de la Ciudadanía antes de su implementación, debiendo someterse a estrictos controles de índole técnico.

La creación de una figura autónoma protectoria de los datos personales de los individuos (Defensor / Defensora de Datos Personales) podría llegar a ser un incentivo para las personas a recurrir de manera activa en la solicitud de protección de sus derechos.

BIBLIOGRAFÍA.

Durkheim, É. (2012). *Las reglas del método sociológico* (2ª reimp.). Ed. Gorla.

Foucault, M. (2003). *Vigilar y castigar. Nacimiento de la prisión*. Siglo Veintiuno Editores Argentina SA

Gómez Jolis, G. (2021). *Biometria y derecho. Usos, aplicación y protección de los datos biométricos*. LA LEY.

Sadin, E. (2018). *La humanidad aumentada. La administración digital del mundo*. Caja Negra.

Sibilia, P. (2010). *Mutaciones de la subjetividad. La exhibición de la intimidad como un eclipse de la interioridad. Un problema del psicoanálisis*. Psicolibro Ediciones, Paidós.