REVISTA DE
INVESTIGACIÓN ACADÉMICA SIN FRONTERA

Año 16 / Núm. 39 / -Junio-julio 2023
Revista de Investigación Académica sin Frontera
ISSN 2007-8870

REVISTAS UNISON
"El saber de mis hijos hará mi grandeza"

Gestión de la identidad en la prevención de medios de vigilancia social

Identity management in social surveillance media prevention

Daniel García Gallegos[1]

[1]httpp://orcid.org/0000-0001-9042-8614, Maestro en Estudios Jurídicos, Universidad Juárez Autónoma de Tabasco, daniboygarcia79@gmail.com.

DOI: https://doi.org/10.46589/rdiasf.vi39.550
Recibido: 28 de Febrero de 2023
Aceptado: 26 de Abril de 2023
Publicado: 30 de Mayo de 2023

Resumen

En una realidad cada vez más informática, los datos personales juegan un papel relevante en el manejo de las masas e ideologías. Si bien, la implementación de mecanismos de reconocimiento por datos biométricos otorgan grandes beneficios en seguridad, velocidad, legalidad de la información o diversas actividades. La concentración e inadecuada manipulación de los datos pudieran forjar espacios de vigilancia y represión social.

México no es la excepción pues se han presentado algunas iniciativas que podrían estar aportando los principios hacia una construcción de infraestructura de vigilancia ciudadana que mal utilizadas, podrían vulnerar muchos de los derechos fundamentales de las personas.

Palabras Clave: Derechos Humanos, Datos biométricos, Cibervigilancia

Abstract

In an increasingly computerized reality, personal data plays an important role in managing the masses and ideologies. Although, the implementation of biometric data recognition mechanisms provide great benefits in security, speed, legality of information or various activities. The

ISSN: 2007-8870
Universidad de Sonora

Año 16 / Núm. 39 / -Junio-julio 2023
Revista de Investigación Académica sin Frontera
ISSN 2007-8870

concentration and inadequate manipulation of data could forge spaces of surveillance and social repression.

Mexico is not the exception, as some initiatives have been presented that could be contributing the principles towards a construction of citizen surveillance infrastructure that if misused, could violate many of the fundamental rights of people.

Keywords: Human Rights, Biometric data, Cyber surveillance

Introducción

Los avances tecnológicos permiten optimizar operaciones tradicionales, otorgándoles peculiaridades que hacen más eficientes sus resultados. A consecuencia de dicha migración digital, el Estado se ve mayormente inclinando por el uso más frecuente de mecanismos para el procesamiento y recopilación de datos personales de los ciudadanos, con el fin de dar solución a diversas problemáticas que surgen en la aplicación u administración de sus servicios.

Pese su enorme utilidad, la actual dependencia social por la tecnología y herramientas digitales hace que numerosas personas brinden información privada sin evaluar las consecuencias, pues para el ojo incauto o poco entendido acerca de la sensibilidad de sus datos, ellos pueden parecer a simple vista información intrascendente. Pero, si se comprenden las consecuencias de su inadecuada manipulación, la perspectiva cambia de manera radical.

La creación, recopilación y manejo de información para bases de datos por parte del Estado genera amplias incertidumbres acerca de la veracidad y responsabilidad que recae sobre las partes intervinientes en el uso y el objeto de dicha información. Cabe entonces preguntarse, ¿Esta dispuesto a proporcionar al gobierno su información privada?, ¿Confía absolutamente que se le proporcionara el manejo apropiado a los datos? ¿Sacrificar la privacidad significa mayor seguridad?

Los medios masivos de almacenamiento en México y su implementación merecen un debate juicioso. Teniendo en cuenta ello, la investigación se centra en analizar los parámetros por

ISSN: 2007-8870
Universidad de Sonora

Año 16 / Núm. 39 / -Junio-julio 2023
Revista de Investigación Académica sin Frontera
ISSN 2007-8870

los cuales toda institución pública como privada debe de ajustarse al momento de generar bases de datos y las implicaciones que el mal uso de dicha información contraerá en la privacidad de los ciudadanos, limitando el derecho a la intimidad y expresión.

Admito que la adopción de sistemas de reconocimiento facial o el aumento de recolección de datos personales no debe de llegar a un punto donde se satanice el concepto, pues estos sistemas aportan grandes beneficios en seguridad, velocidad, eficacia de las actividades cotidianas y la expansión de las redes sociales, los servicios en línea, la *big data*, los teléfonos inteligentes y demás dispositivos de comunicación, han favorecido la integración de mecanismos de recopilación, almacenamiento y procesamiento de datos personales de todas los ciudadanos cotidianamente.

El punto clave es que dichos procesos deben ser implementados de manera lícita, honesta, segura y transparente, para no genera nerviosismo social. Las bases datos llaman la atención puesto que podrían convertir a cualquier país en un mina de oro de datos que cualquier gobierno o agrupación pudiera utilizar para los fines que requieran, facilitar la represión de opositores políticos, control de masas y espionaje; igualmente para la venta de información con fines comerciales, la falsificación de documentos, el robo de identidad, el terrorismo y las múltiples formas de delincuencia informática, que pudieran propiciarse a raíz de un mal uso de dichas bases.

Método

Para fines de la investigación se utilizó el método de la doctrina analítica para estudiar las múltiples publicaciones y establecer una figura clara sobre la trascendencia que las bases de datos e identidad digital pudieran adquirir en México.

Los métodos como la sociología jurídica y el derecho comparado se utilizaron para lograr así diseñar alternativas apropiadas para la aplicación y desarrollo de la nueva identidad digital, evaluando tanto las incompatibilidades, defectos y los aciertos del sistema de diversos países que poseen una comprensión distinta y perfeccionada en los procesos de creación, recopilación y manejo de información a través de bases de datos o identidades digitales.

ISSN: 2007-8870
Universidad de Sonora

Año 16 / Núm. 39 / -Junio-julio 2023
Revista de Investigación Académica sin Frontera
ISSN 2007-8870

La implementación de medios de gobernanza digital y construcción de medios de vigilancia.

Haciendo una recapitulación histórica, se ha llegado a la conclusión que la información brinda poder y dicha conceptualización no había alcanzado parámetros tan reales hasta la creación de los medios digitales, los cuales, hoy en día han permitido la captura y manejo masivo de información de cualquier índole. En efecto, su uso intensificado ha propiciado que el flujo de datos personales de los ciudadanos se vea comprometido cada vez con mayor facilidad.

Todo esto, ha ocasiona el aumento de potenciales actos de manipulación de datos con fines ajenos a los que se habría advertido, puesto que, todos los días a través de las medios digitales los usuarios generamos información y datos que pudieran ser utilizado para diversos sectores, incluyendo ahí datos personales o sensibles.

Hay que mencionar además que muchas veces las autoridades de control exceden los límites de privacidad permitidos, mismos actos que culminan en escenarios de intromisión en el derecho a la privacidad u otras esferas jurídicas.

Con esto en mente, se origina una preocupación alrededor de la constante compilación y sistematización de datos personales que realizan diversas instituciones privadas como públicas, pues cada año se incorporan millones de personas a las redes de interconexión digital. A raíz de ello, desde 1948 el matemático estadounidense Norbert Wiener[1] manifestó la relevancia de designar nuevos métodos interdisciplinarios entre a la comunicación, control del hombre y la máquina. (Wiener, 1985)

Basado en ello, florecieron diversas ideologías tecnológicas, una de las más relevantes es la del "poder informático"[2], estas no fueron indiferentes a la mirada analítica del derecho, pues a partir de ellas se adaptaron diversas perspectivas para introducir las conductas al sistema normativo y establecer controles de comportamiento.

[1] Matemático estadounidense, conocido como el fundador de la cibernética, el estudio interdisciplinario de la estructura de los sistemas reguladores. Es decir, la ciencia que estudia los flujos de energía estrechamente vinculados a la teoría de control y a la teoría de sistemas.
[2] Vittorio Frosini lo define como la acumulación, centralización y control de información en cantidades ilimitadas de los individuos y colectividades, con el objeto de transmitirlas como mercancía permitiendo un nuevo poder de dominio social sobe el individuo. Fuente: Vittorio Frosini, El Horizonte Jurídico de Internet, Revista de Derecho Constitucional Europeo, Editorial Aranzadi, Año 14, número 28, 2017, p. 193.

ISSN: 2007-8870
Universidad de Sonora

Año 16 / Núm. 39 / -Junio-julio 2023
Revista de Investigación Académica sin Frontera
ISSN 2007-8870

Es así, que diversas obras de Wiener se centraron en estudiar temas específicos acerca de la interdisciplinariedad que existía entre el derecho y las comunicaciones, las cuales aportaron grandes beneficios metodológicos en la resolución de problemas sistemáticos. Dichos aportes hoy en día han adquirido matices más elevados en las relaciones humanas, puesto que el derecho se encuentra estrechamente vinculado con la informática y las actividades digitales.

Hay que señalar, que a cualquier gestión e implementación de nuevas tecnologías para el ejercicio de sus funciones deben de garantizarse el pleno respeto, seguridad, legalidad a los derechos humanos y además la honra de las personas, aún más, cuando se habla de medios en los que se manipulen datos personales.

El Estado debe de materializar normas, lineamientos de evaluación, protocolos, índices de responsabilidad o demás instrumentos que se encuentren en su facultad y dentro de los principios establecidos por la constitución y los tratados internacionales, para resguardar en su totalidad la plenitud de los derechos humanos. Dichos medios deben obligatoriamente no solo encontrarse publicados sino además ir acordes dichas actividades o adelantos tecnológicos con la finalidad de no afectar otros esferas jurídicas y ser lo suficientemente precisas para prevenir vacíos legales que puedan ser usadas en contra de las personas. (Conde González, 2016)

Lo curioso es, que de acuerdo a la "teoría del garantismo"[3], el Estado es el ente comisionado a la defensa y garantía de los derechos de los ciudadanos. No obstante, muchas veces, esté, es el mismo encargado a su transgresión y responsable del incumplimiento ante terceros, haciendo caso indolente a las disposiciones constitucionales que por decreto fueron publicadas en el Diario Oficial de la Federación el 10 de junio de 2011[4]. No es difícil imaginar, pero de acuerdo con la ONU la revolución digital ha forjado un constante, libre flujo de información, datos y conocimientos

[3] El garantismo se presenta como un modelo de derecho y de Estado de derecho que propone el aseguramiento de los derechos con base en una estructura de los ordenamientos jurídicos que tiene en la cúspide a la Constitución y a los derechos fundamentales; cualquier acto que busque legalidad y legitimidad debe sujetarse a estos presupuestos. Fuente: Torres Ávila, Jheison, La teoría del Garantismo: poder y constitución en el Estado contemporáneo, Revista de Derecho, N.47, Barranquilla, 2017, p. 162.

[4] El 10 de junio de 2011 se publicó en el Diario Oficial de la Federación una reforma constitucional de Derechos Humanos, la cual tuvo como eje principal establecer una nueva perspectiva de los derechos humanos, poniendo al centro la dignidad de las personas. Fuente: Arturo Zaldívar, Reforma Constitucional en materia de Derechos Humanos. 10 de junio, CNDH, México, 2021, https://www.cndh.org.mx/index.php/noticia/reforma-constitucional-en-materia-de-derechos-humanos-10-de-junio.

ISSN: 2007-8870
Universidad de Sonora

Año 16 / Núm. 39 / -Junio-julio 2023
Revista de Investigación Académica sin Frontera
ISSN 2007-8870

alrededor de mundo. Esto ha conducido que los datos adquieran una mayor relevancia como herramienta social u comercial. Si bien, es cierto que las innovaciones tecnológicas ofrecen múltiples beneficios y contribuyen al progreso económico de los sectores que las implementan, estas a su vez, generan escenarios qué, de no detectarse, analizarse y subsanarse se vuelven perjudiciales para las actividades jurídicas y de desarrollo.

La realidad, es que México posee una calificación de 60/100 en cuanto a la libertad, acceso y violación de los derechos humanos de los usuarios en medios digitales. (Shahbaz & Funk, 2021) Si bien, se promueve el desarrollo de un entorno en línea, aumentan los índices de autocensura y la eliminación de contenido politizado, además de un déficits en el estado de derecho que limita el pleno disfrute de los derechos políticos y libertades civiles, sumado los actos que se realizan por agrupaciones criminales, la corrupción y abusos de poder. (Shahbaz & Funk, 2021)

Actualmente los avances tecnológicos han permitido que diversas actividades se puedan trasladar a medios digitales, cambiando el mecanismo en el que las actividades del estado se ejecutan. El nacimiento de nuevos panoramas de gobernanza en medios digitales ha llegado para replantear las políticas públicas y pensar más en las necesidades de los ciudadanos teniendo un alto contenido normativo para asegurar la protección a los derechos humanos.

Como efecto a sociedades con una mayor atención en el desarrollo, el uso de las tecnologías e iniciativas poblacionales para mayores espacios de participación democrática, se desplegaron nuevas perspectivas ideológicas de gobernanza y de aplicación de los derechos humanos en materia digital.

En última década en especial, las tecnologías han demostrado su enorme potencial para crear los espacios de desarrollo para la sociedad en temas de participación, transparencia, accesibilidad, velocidad y seguridad, lo que genera un empoderamiento de las herramientas tecnológicas en la aplicación del Estado de Derecho y la defensa de los derechos humanos.

Basándose en dicha interacción entre el derecho y la tecnología se constituyeron nuevas perspectivas ideológicas en medios de gobernanza, como desafíos hacia los operadores jurídicos y todos los sectores vinculados (Sanz Larruga, EL derecho ante las nuevas tecnologías de la información, 1997). Ello resulto en el establecimiento de *gobiernos digitales o electrónicos,* los

ISSN: 2007-8870
Universidad de Sonora

Año 16 / Núm. 39 / -Junio-julio 2023
Revista de Investigación Académica sin Frontera
ISSN 2007-8870

cuales buscan soluciones dirigidas a implementar, proveer y promover servicios orientados hacia los ciudadanos por medio de la innovación para la eficiencia de la gestión pública, mejorar los servicios ofrecidos y transparencia (Secretaría de la Función Pública, 2013).

Son innegable los grandes aportes y utilidades que el uso de las tecnologías puede generar en el desarrollo de un Estado. No obstante, de dicha inclinación surge la duda acerca del potencial y el riesgo que el uso inadecuado de las plataformas tecnológicas pueda generar.

Al tomar en cuenta como punto de partida la creación de servicios orientados más al ciudadano, diversos países han optado por desarrollar *arquitecturas de interoperabilidad*, la cual se define como el conjunto de políticas y componentes técnicos precisos para el intercambio y verificación de datos entre los sistemas de información que poseen las instituciones estatales (Harbitz & Arcos Axt, 2010). Ello con el fin de integrar servicios públicos más accesibles. Sin embargo, los sistemas que permiten interoperabilidad entre bases de datos o sistemas de información, no siempre consideran adecuadamente los alcances legales u operativos necesarios de protección para los usuarios.

Por todo esto, surgen los "derechos a las nuevas tecnologías", los cuales requieren de una legislación especializada, con el fin de desarrollar estándares normativos de carácter preventivo y correctivo. Es importante comprender que el nacimiento de dichos derechos radica de las industrias, empresas o cualquier intermediario que posibilite sus actividades mediante herramientas tecnológicas o digitales, no necesariamente se apoya en mecanismos digitales para el ejercicio adecuado de los derechos, sino para la generación de beneficios económicos.

Esto nos lleva a entender, porque cuando se utilizan nuevas alternativas digitales, el garantizar los derechos de los usuarios es el último punto en el que las instituciones o empresas se preocupan. He aquí, donde la actividad vigilante del Estado ostenta mayor importancia, pues este debe de certificar que los derechos ciudadanos estén plenamente presentes en el entorno digital como el real. (Comisión de Derechos Humanos del Distrito Federal, 2016)

Ahora bien, frente al desarrollo de un gobierno digital, el peligro de la falsificación de documentos, robo de identidad, ciber-terrorismo y las múltiples formas de delincuencia informática, la necesidad de generar medidas cada vez más seguras para la identificación de las

ISSN: 2007-8870
Universidad de Sonora

Año 16 / Núm. 39 / -Junio-julio 2023
Revista de Investigación Académica sin Frontera
ISSN 2007-8870

personas en la actual Sociedad de la Información, se exige una mayor y más robusta regulación de los mecanismos o procedimientos; despuntando así, la utilización de captura de información biométrica en los usuarios de todos los órdenes, trabajadores, clientes o ciudadanos.

De esta manera, proyectos como el proyecto de la "Cedula Única de Identidad"[5], el actual "Protocolo de actuación digital notarial"[6] y el famoso "Padrón Nacional de Líneas Telefónicas"[7] han generado una relevancia mayor por la información biométrica al estar ligadas a la identificación oficial, a los documentos personales y sensibles de los ciudadanos mexicanos, los cuales elevan de manera considerable el rango de los datos biométricos al colocarlos en la línea principal de la actividad administrativa del estado y pueden generar mayores problemáticas sino previenen las medidas necesarias para su utilización y protección.

Se debe distinguir, que la Cédula Única de Identidad es uno de los proyectos más ambiciosos en materia tecnológica que se pudieran desarrollar en el país, pues la implementación de esta herramienta de identificación tendrá beneficios en un sin número de sectores y aportara mayores alcances a los derechos de los ciudadanos. No obstante, el problema radica, en el desarrollo e implementación de una nueva configuración de atribuciones en las autoridades de control ante un nuevo paradigma en los derechos ARCO, la evolución del derecho a la identidad y la nueva perspectiva de los datos personales en país.

[5] Documento oficial que contiene datos filiatorios de la persona, como el nombre, la profesión, el domicilio y los datos biométricos como huella digital, dactilar, foto, firma, y en el que se pueden consignar otras circunstancias propias del individuo. Fuente: Mia Harbitz, Iván Arcos Axt, Diccionario para registros civiles e identificación 2013, Banco Interamericano de Desarrollo, 2013, p. 11.

[6] Un sistema que permitirá a los notarios estar vinculados al INE lo que les proporcionará acceso a su base de datos, como además la incorporación de dispositivos biométricos oficiales para verificar a través de un sistema binario los datos del INE o cualquier documentos oficial que se les presente para al realizar algún trámite e identificar fehacientemente a la persona garantizando la certeza jurídica en las operaciones celebradas. Fuente: Carlos Cataño Muro Sandoval, Verificación biométrica INE, Notaria 51 de la Ciudad de México, México, https://notaria51.mx/verificacion_biometrica.html.

[7] Fue un proyecto para la creación de una base de datos que contuviera la información biométrica de las personas que contratan una línea telefónica móvil en México. Fuente: Tribunal Pleno de la Suprema Corte de Justicia de la Nación, Acción de inconstitucionalidad 82/2021 y su acumulada 86/2021, LXIV Legislatura, México, 2021.

ISSN: 2007-8870
Universidad de Sonora

Año 16 / Núm. 39 / -Junio-julio 2023
Revista de Investigación Académica sin Frontera
ISSN 2007-8870

Vigilancia gubernamental en la era digital.

Como se ha establecido anteriormente, las nuevas perspectivas en gobernanza sumadas a los avances tecnológicos han concebido una nueva línea en la forma de aplicar y desplegar las actividades del Estado. Si bien, esta configuración de gobernanza digital es utilizada en diversos países, poseyendo grandes beneficios económicos y sociales, como en el caso de la republica de Estonia en Rusia, el cual hoy día es considerado como el país líder en gobierno digital. (Tapscott & Tapscott, 2018) En otros puntos geográficos se ha aplicado este medio de gobierno para el desarrollo de medios de vigilancia, control y análisis de las masas, como también en la limitación de los derechos fundamentales de los ciudadanos.

Uno de los casos más notables en este tema, fueron las revelaciones aportadas por Edward Snowdena acerca de las prácticas que llevaban a cabo las agencias de EEUU, Reino Unido, Canadá, Australia y Nueva Zelanda en las cuales espiaban a los ciudadanos de todo el mundo, como substraían datos a una escala sin precedentes, los almacenaban y utilizaban para fines propios. (Altvater, 2014)

Dichas revelaciones iniciaron un debate mundial acerca de la fuerte amenaza que diversos servicios digitales o de recopilación de datos pudieran ocasionar, así como la relevancia de lineamientos de seguridad y evaluación que se debían de implementar sobre el internet, como a las instituciones privadas y del Estado en general. Este acontecimiento no solo se demostró que violaban la privacidad de las personas, sino además la gran amenaza para la libertad de opinión, ideologías políticas y los derechos a la protección de datos.

A raíz de esto, diversos organismos internacionales han expresado múltiples opiniones acerca de los medios de vigilancia masiva y como deben de replantearse las estructuras políticas hacia los medios digitales de recopilación de datos.

El tema no debe centrarse solamente en entre elegir libertad o seguridad, sino en buscar un equilibrio que responda a las necesidades y mantenga una buena relación entre los ciudadanos con el Estado.

Comencemos por aclarar que los datos personales constituyen bloques enormes de información, bienes que las empresas u instituciones estatales utilizan para el desarrollo de diversas

ISSN: 2007-8870
Universidad de Sonora

Año 16 / Núm. 39 / -Junio-julio 2023
Revista de Investigación Académica sin Frontera
ISSN 2007-8870

actividades. Dicha información actualmente posee alto valor, equiparable a ciertos activos intangibles, tales como el software o el valor comercial de los nombres de dominio, considerándolos como el petróleo de la sociedad de la información y del conocimiento.

He aquí el problema insoslayable de la revolución tecnológica, otorgamos nuestros datos a empresas e instituciones, consintiendo la intromisión a nuestra vida privacidad y confiriendo facultades para su utilización como medio de obtención de estadísticas, investigación, entre otras. Los datos se convierten entonces en una de las monedas de cambio más significativas en el sector empresarial o político actualmente. (B. Ocariz, 2018)

Dado que hoy en día, gran variedad de empresas privadas ofrecen servicios gratuitos a cambio del acceso a los datos, ello les posibilita poder realizar innumerables actividades, lo que ocasiona el aumento de actos de manipulación con fines ajenos a los que se habría advertido. Todos los días a través de las medias digitales los usuarios generamos información y datos que pudieran ser utilizados para diversos sectores, incluyendo ahí datos personales o sensibles.

El valor económico otorgado a la información de las personas no radica en el dato por sí mismo, sino en el tratamiento, asociación con otros datos y utilidad que se le dé. Esto permite obtener un lucro, a través de la explotación comercial de aspectos privados, orientados al consumo, que incluso se interesan en predecir conductas y patrones de comportamiento. (Mendoza Enríquez, 2018)

Basta como muestra, el robo de los datos personales de 1.6 millones de servidores públicos federales de México sucedido en el 2020, cuando un analista de seguridad, Bob Diachenko, se topó con la base de datos de los empleados federales en el motor de búsqueda “Shodan” (Montes, 2021). La controversia se suscitó al momento en el que la Secretaría de la Función Pública (SFP) al no poseer las medidas de seguridad apropiadas, indebidamente, quiso trasladar la información del DeclaraNet y del sistema del Registro Único de Servidores Públicos (RUSP) a una nueva base de datos.

La información era la concentración de los datos personales de empleados públicos que no habían cumplido con sus obligaciones en la declaración patrimonial de ese momento, los cuales días posteriores ya habían sido extorsionados a cambio de no divulgar su información.

ISSN: 2007-8870
Universidad de Sonora

Año 16 / Núm. 39 / -Junio-julio 2023
Revista de Investigación Académica sin Frontera
ISSN 2007-8870

Algo semejante ocurre con los datos biométricos, si bien su comercialización es más complicada, no los exenta de ser materia de interés para diversas organizaciones políticas como de delincuencia, pues su versatilidad da pie a diversos tipos de actividades ilegales. Como se ha mencionado se trata de un nuevo mecanismo tecnológico, no obstante, muchas veces la base de su actividad se halla construida a partir de alguna actividad ya existente, es decir; las bases de datos biométricas son la versión actualizada de los padrones, libros de empleados o usuarios. Con esto en mente, la regulación tecnológica debe de sustentarse en el hecho de que no es simplemente una herramienta sino un medio por el cual se crean posibles ilícitos o violación de derechos y muchas otras actividades ya reguladas por las leyes de cada materia.

Las técnicas de control biométrico son muy variadas, pueden utilizar distintas características de la persona. Aunque suelen identificarse como medios de reconocimiento a través de los rasgos físicos, la realidad es más amplia, y existen un amplio abanico de sistemas de vigilancia, clasificados en dos grandes grupos.

Por un lado, se encuentran los datos "fisiológicos", los cuales se refieren solo a las características físicas y fisiológicas de la persona, como lo son las huellas dactilares, el iris, la geometría de la mano, la retina, los vasos sanguíneos en determinadas partes del cuerpo, la voz, el sudor, las orejas y el ADN. (Puyol, 2019)

Por el otro lado, están los datos relacionados con el comportamiento de la persona, la forma en que realizan ciertas conductas. Entre éstos destacan la escritura, el ritmo cardiaco, el ritmo respiratorio, la firma, la utilización de un teclado, la forma de conducir, la forma de andar o de moverse, y la marcha. (INAI, 2018)

Se debe agregar que, múltiples acontecimientos han surgido a raíz de la implementación de medios de manipulación y recopilación de datos biométricos en diversas partes del mundo. Lo que demuestra que muchas veces es el mismo Estado quien hace del ente vulnerador de los derechos humanos.

Para ilustrarnos mejor, tenemos el caso de la cadena de supermercados Mercadona, en España; la cual en el 2020 anuncio la instalación de un sistema de reconocimiento facial en al menos unos 40 supermercados, con el fin de robustecer su seguridad. Este mecanismo fue creado

ISSN: 2007-8870
Universidad de Sonora

Año 16 / Núm. 39 / -Junio-julio 2023
Revista de Investigación Académica sin Frontera
ISSN 2007-8870

para detectar a personas que tuvieran una sentencia de orden de alejamiento del local, el cual al detectar el ingreso o acercamiento al mismo, alertaría a los cuerpos policiales en menos de 0,3 segundos. (Pérez, 2020)

Las implicaciones que sistemas de reconocimiento facial a nivel legal pudiera ocasionar son múltiples, pues en el caso concreto viola el derecho a la privacidad de las personas, pues sin su consentimiento accede a una base de datos para investigar su historial penal e impedir el acceso o tránsito por diversos lugares.

México no carece de legislación aplicable, sino de normas especializadas en medias digitales precisas para integrar adecuadamente las nuevas herramientas tecnológicas que se vayan desarrollando. Lamentablemente el marco normativo en el territorio mexicano no se ha centrado en materializar leyes, reformas, protocolos de acción o demás instrumentos que se encuentren en su facultad, ni mucho menos en las repercusiones que se pudieran ocasionar, lo que ha ocasionado que múltiples veces se invada la privacidad de los ciudadanos. (Escobar Pérez , El papel del derecho en relación con el uso de tecnologías de información)

De manera que al buscar establecerse como un gobierno digital, se debe de estudiar no solo los nuevos elementos que se buscan incorporar, sino además es necesario analizar la situación política, social, económica y cultural del país o región en donde se busque aplicarlas.

Aquí he de referirme a un suceso destacado en desarrollo de dichas herramientas, pues el progreso tecnológico supera cada vez más rápido a las mismas disposiciones normativas que regularizan las actividades. Esto ocasiona que se hallen en limbos jurídicos o paraísos sin restricción alguna en las cuales solo se afectan a los usuarios de dichas herramientas.

Como resultado de dicha problemática, se generó una de las principales trayectorias esenciales a dicha transformación paradigmática. La cual radica en la protección de los mismos derechos de los ciudadanos, buscando una perspectiva con enfoques más amplios en el reforzamiento de la posición de control que poseen los propietarios sobre sus propios datos y la utilidad que se genera a través de su análisis. (Rodríguez Ayuso, 2021)

Esta renovación paradigmática se refleja mayormente en una ampliación de los derechos tradicionales, más en específico para los derechos al acceso, rectificación, cancelación u oposición

ISSN: 2007-8870
Universidad de Sonora

Año 16 / Núm. 39 / -Junio-julio 2023
Revista de Investigación Académica sin Frontera
ISSN 2007-8870

de los datos personales o derechos ARCO; los cuales son la base jurídica que poseen los usuarios en medios digitales y los principales parámetros a resguardar para quienes trabajan con datos personales en México.

Lo que acontece es que en el Estado recae el compromiso de profundizar en los posibles efectos que determinado ejercicio o política producirá; a pesar de ello, cuando se analizan los gobiernos digitales muchas veces se cometen los mismos errores, solo se buscan recursos tecnológicos que satisfagan las necesidades o resuelvan el problema en turno sin tomar en cuenta los cambios drásticos que este pudiera ocasionar dentro de la misma institución o ante la ciudadanía.

Al respecto conviene especificar, el derecho a la protección de datos personales no siempre fue de gran trascendencia, este en un principio instruyó como una garantía a la vida privada, que posteriormente se volvió un derecho a la autodeterminación informativa, llegando a convertirse en un derecho humano fundamental. (Razza, 2020)

Es el título de *derecho humano* el que le brinda la capacidad de ejecutar un amplio compromiso de amparo frente a las autoridades de control o cualquier poseedor de bases de datos públicos o privados (Guzmán, 2013); lo que también posibilita la nueva reestructuración del paradigma hacia los derechos ARCO ampliando su panorama no solo a los derechos antes mencionados que conforman su siglas sino agregando además el *derecho al olvido o supresión*, *limitación de tratamiento*, *portabilidad de los datos* y *a no ser objeto de una decisión únicamente en el tratamiento automatizado de elaboración de perfiles* (Rodríguez Ayuso, 2021) actualmente definidas como los derechos ARSULIPO.

Aquí vale la pena especificar, dicha reestructuración ideológica en la ampliación a los derechos de los usuarios despunta a raíz de la nueva figura normativa europea, más en concreto del Reglamento General de Protección de Datos (RGPD). De manera que, España inicio la reforma de diversos apartados normativos para encontrarse amoldada a su nueva configuración, con el fin de proveer una estructura normativa sólida y actualizada en la regulación del tratamiento de datos personales de las personas físicas y garantizar la protección de los nuevos derechos digitales. (Ayudaley, 2021)

ISSN: 2007-8870
Universidad de Sonora

Año 16 / Núm. 39 / -Junio-julio 2023
Revista de Investigación Académica sin Frontera
ISSN 2007-8870

Para ilustrar mejor, la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal quedó derogada por la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD) del 2018 la cual modifico las exigencias en el tratamiento de información personal de usuarios y empresas.

A demás de ampliar la gama de derechos que poseen los usuarios con respecto a sus datos personales, se incorporó por primera vez en su Título X (Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales, 2018) los *derechos digitales*, los cuales son tomados como derechos muy independientes a los derechos de datos personales, otorgándoles su propia identidad jurídica. No solo ello, sino que además establecieron esquemas antes no presentes en materia jurídica digital como el *derecho a la educación digital*, el *derecho a la actualización de noticias en medios digitales*, el *derecho a la portabilidad en servicios de redes sociales*, el *derecho al testamento digital*.

Sorprende, la introducción de una novedosa regulación, la cual pudiera ser calificada como un modelo transcendental en materia digital para España. En vista de que no solo se enfoca en los derechos esenciales de los usuarios, y la protección de sus datos personales, sino que además trasciende a los derechos laborales como *la intimidad de los trabajadores en el uso de dispositivos digitales*, *el derecho a la desconexión digital* fuera del tiempo de trabajo y el *derecho a la intimidad de los empleados ante la utilización de dispositivos de geolocalización* por los empresarios, entre muchos otros de trascendencia jurídica.

Hemos visto que gran parte de la nueva perspectiva paradigmática digital va dirigida fuertemente a los principios de derechos a la protección de datos personales; en el caso de la norma española haciendo gran exigencia en la *exactitud*, la trascendencia del concepto de la *autodeterminación informativa* y del *control que posee el titular sobre sus propios datos*.

La injerencia en la *exactitud*, va referida a que los datos de los usuarios cuando se encuentren en posesión de un tercero estos deben de ser exactos y si fuere necesario actualizados de acuerdo con el artículo 5.1.d del Reglamento (UE) 2016/679 y el Artículo 4 de la LOPDGDD. Por su parte los demás puntos de análisis se desarrollaran con mayor detalle más adelante.

ISSN: 2007-8870
Universidad de Sonora

Año 16 / Núm. 39 / -Junio-julio 2023
Revista de Investigación Académica sin Frontera
ISSN 2007-8870

Es, la implementación de los nuevos parámetros normativos en materia digital instituidos por la norma española lo que forja nuevas fronteras en la aplicación de estos derechos; son diversos los países que han reconocido la relevancia por la protección de los datos personales y los medios digitales, pero no todos cuentan con la misma profundidad en el tema.

Por su parte en México es un tema en actual discusión, si bien se establece la protección a los datos personales en la Constitución Política, ciertos derechos como el *derecho al olvido*, *desconexión digital* entre otros no se encuentran instituidos dejando en incertidumbre a los ciudadanos.

De manera general los datos personales se encuentran sujetos por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; ninguno hace alusión a los datos biométricos ni alguna aproximación técnica dentro de su texto. Acorde a dicha inquietud, el INAI ha mencionado que si bien el término de datos biométricos no se encuentra tácitamente señalado en las leyes actuales, ello no debería de ser una limitante para que se consideren como datos personales bajo ciertas circunstancias.

Si bien, esto solamente es una mera interpretación, pues no hay norma vinculante que expresamente disponga que los datos biométricos se constituyen datos sensibles. El único acervo en dicha materia son los tratados internacionales y del derecho comparado, los cuales aciertan reiteradamente asignarles tal carácter de sensibles.

Ahora bien, tomando en cuenta lo mencionado por el INAI y de acuerdo con ambas leyes de datos personales, las condiciones para que un dato biométrico pudiera ser considerado comodato sensible, radica en:

a) Que el dato represente la esfera más íntima de su titular
b) Que el manejo indebido pudiera ocasionar discriminación alguna
c) Que el uso ilegítimo conlleve un alto riesgo para el titular (Rubio Fernández & Pérez-Jaén , 2022)

Hay que advertir, que si bien se tiene la creencia que los datos biométricos solo poseen la función de identificar a la persona. La realidad es que su versatilidad hacer que en muchos países

ISSN: 2007-8870
Universidad de Sonora

Año 16 / Núm. 39 / -Junio-julio 2023
Revista de Investigación Académica sin Frontera
ISSN 2007-8870

sean considerados como datos sensibles y con algunos rangos más elevados de seguridad, pues la posesión o manejo de estos pudieran conllevar a una multiplicidad de delitos.

Estados Unidos es un país donde se usa este tipo de tecnologías para la lucha contra el crimen, sin embargo, se han presentado debates sociales acerca de los alcances y límites que dichas bases de datos deberían de poseer. En consecuencia, se han presentado situaciones en las que la misma inteligencia artificial que proporciona la información arroja sesgos raciales y de género, los cuales en algunas ocasiones tan basados a partir de ideologías políticas, (Sheng, Chang, Natarajan, & Peng, 2019) además de la creación de infraestructuras de vigilancia donde no hay suficiente transparencia sobre el uso que se le puede dar a este tipo de tecnologías.

Un ejemplo famoso es el caso de Cambridge Analytica y su rol en las elecciones presidencias en las que resultó ganador Donald Trump, todo esto mediante los análisis de datos de una encuesta de personalidad que se realizó a través de la plataforma de Facebook sin el consentimiento de los usuarios. La información obtenida permitió obtener los perfiles de alrededor de 50 millones de usuarios, los cuales fueron manipulados en favor de la campaña de Donald Trump mediante la creación de publicidad seccionada según cada perfil y creando noticias falsas. (García Fernández, 2018)

Este es un claro ejemplo de cómo los medios de recolección de datos pueden ser utilizados con fines fuera de los establecidos, permitiendo que instituciones, agrupaciones o personajes utilicen dicha información para fines propios, lo que puede generar falsas ideologías políticas acerca de una persona y en el caso en concreto hacer que tenga una mayor aceptación política que le beneficiara para la obtención de un cargo público.

Los algoritmos de inteligencia artificial que poseen los buscadores, aplicaciones o diversas herramientas digitales cada vez afectan más nuestras decisiones, pues estas aprenden nuestros gustos y a partir de ellos nos muestran el contenido que pretendemos buscar o interesar, no obstante esto limita la libertada de conocimiento, pues se le encapsula al usuario en un solo sector de información que difícilmente pueda alterar en pocos días.

Si, dichos algoritmos son utilizados por empresas privadas o por el Estado, estos pudieran generar un análisis de las necesidades de la población, identificar posibles localizaciones de

ISSN: 2007-8870
Universidad de Sonora

Año 16 / Núm. 39 / -Junio-julio 2023
Revista de Investigación Académica sin Frontera
ISSN 2007-8870

individuos, rastreo de perfiles potenciales de criminalidad, entre muchos otros pero al mismo tiempo pueden introducir falsas ideas a través de publicidad engañosa o secura de la información.

México no es la excepción pues se han presentado algunas iniciativas que podrían estar aportando los principios hacia una construcción de infraestructura de vigilancia ciudadana que mal utilizadas, podrían vulnerar muchos de los derechos fundamentales de las personas.

En el 2021 se presentó la creación de un Padrón Nacional de Usuarios de Telefonía Móvil, que obligaría a la entrega de datos biométricos para poder tener acceso a una línea de teléfono móvil al Gobierno y a las empresas de telefonía. (Pleno, 2021) Iniciativa que ya es aplicada en otros 17 países como China, Perú, Singapur, Tailandia, Venezuela. No obstante, fue suspendido luego de que fuera considerado inconstitucional.

La historia ha demostrado que el poseedor de información tiene la capacidad de controlar a los demás a su alrededor y el estado actual de los datos biométricos no invitan al optimismo, por ello la protección de los datos personales como biométricos de los ciudadanos es sumamente relevante en la materia jurídica.

Observemos ahora una de las potencias mundiales en tecnología, China; país en el cual sus avances en medios de recolección, manejo y análisis de datos personales de sus ciudadanos es tan avanzado que actualmente ha generado diversos temas en materia de un claro ejemplo de medios de vigilancia gubernamental.

En dicho país, quien contrate algún servicio de telefonía deberá proporcionar sus datos biométricos, es especifico, un escaneo facial. Medida que llama la atención pues el país ya cuenta con más de 170 millones de cámaras con inteligencia artificial y tecnología de reconocimiento facial.

El gobierno chino ha establecido que el requisito telefónico, es solo con la finalidad de verificar la identidad de los millones de usuarios que poseen internet en su país y que estos lo hagan bajo su perfil autentico y "proteger los derechos e intereses legítimos de los ciudadanos en el ciberespacio" (spanish.news.cn, 2022).

Jeffrey Ding, un investigador de inteligencia artificial chino de la Universidad de Oxford, ha mencionado que la finalidad para dicha base de datos es la de eliminar los números telefónicos

ISSN: 2007-8870
Universidad de Sonora

Año 16 / Núm. 39 / -Junio-julio 2023
Revista de Investigación Académica sin Frontera
ISSN 2007-8870

anónimos y reducir los fraudes, no obstante no se cierra a la posibilidad de que sea para el uso de mejorar el rastreo de la población. (BBC News Mundo, 2019)

Todo esto ha despertado un gran debate social pues el uso intensivo de estos mecanismos ha llegado a la implementarse en otras áreas. Como en el Instituto de Secundaria Número 11 de Hangzhou de China, donde se instalaron en las aulas cámaras de reconocimiento facial sobre la pizarra los cuales escanean cada 30 segundos los rostros de los estudiantes y los datos se acumulan un ordenador el cual analiza los registros clasificándolos según sus expresiones feliz, triste, decepcionado, molesto, asustado, sorprendido y neutro. (Arana, 2019)

Si bien, estos mecanismos funcionan para medir los grados de concentración, adaptar las clases para mejorar los métodos de enseñanza de los profesores y rendimiento de los alumnos. También están siendo aplicados por fuerzas de seguridad, siendo aptos de identificar si alguien en la calle posee antecedentes legales o de hallar a una persona entre una multitud.

Las ventajas que suponen son evidentes: seguridad, fiabilidad, control, comodidad, transportabilidad pero es necesario que los legisladores comiencen a reflexionar de manera completa sobre la integración y adecuación de mecanismos jurídicos que verdaderamente permitan seguridad y responsabilidad en relación a los datos biométricos, protección y gestión de la identidad de los ciudadanos.

Cualquier Gobierno, en especial el mexicano debe de debatir seriamente sobre los esquemas de identificación y la implementación de bases de datos de los ciudadanos. Quienes serán los encargados de custodiar dicha información, como debe de custodiarse, hoy en día existen alternativas como el denominado “Blockchain”, este considerado el siguiente paso del internet, ya que desde ser utilizada principalmente para compartir información, ahora pasa a ser una red para compartir valor. En términos simplificados, la blockchain es un registro distribuido e indeleble. (Biblioteca del Congreso Nacional de Chile, 2018)

Mecanismos como estos que se encuentran en la vanguardia de medios de seguridad e inalterables podrían ser algunas de las alternativas que el Estado pudiera optar para generar mayor transparencia en la consolidación de bases de datos.

ISSN: 2007-8870
Universidad de Sonora

Año 16 / Núm. 39 / -Junio-julio 2023
Revista de Investigación Académica sin Frontera
ISSN 2007-8870

Conclusiones y recomendaciones

En la búsqueda por generar mejor calidad en los servicios brindados hacia los consumidores o los ciudadanos, las empresas e instituciones gubernamentales han buscado incluir mecanismos digitales que ofrezcan eficacia, velocidad, certeza y seguridad en sus actividades. Ello ha llevado a la instalación de bases de datos, sistemas de análisis de datos, medios de control biométrico, entre muchos otros.

Queda definido, que las herramientas tecnológicas de esta índole brindan grandiosas ventajas en los servicios y la interacción con los usuarios, no obstante al mismo tiempo se convierten en una mina de oro que diversas agrupaciones pudieran manipular para múltiples fines.

Hay que reconocer que el auge también se ha visto presente en el país, pues el derecho a la información y el acceso a tenido diversas variaciones en su alcances y figura; a partir de la publicación realizada en el Diario Oficial de la Federación el 11 de junio de 2012, con la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, fundó las bases para la creación del Instituto Federal de Acceso a la Información (IFAI) un órgano descentralizado de la APF, constituido como un órgano autónomo constitucional, garante en materia de transparencia y protección de datos, actualmente renombrado como el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). (Pedroza de la Llave, 2019)

No obstante, el caso de la nueva perspectiva a los derechos ARSULIPO no se encuentra representada en el territorio; De la misma manera que la tecnología está en constante evolución las ideologías y normas debería de ir en constante actualización. Por ello, es necesario apostar por políticas públicas que posean un profundo análisis en el impacto de las nuevas tecnologías y mitigar así los riesgos hacia los derechos de los usuarios sin renunciar a las funcionalidades que otorgan, (Gil, 2016) pero sobre todo que permitan establecer nuevos parámetros o perspectivas acerca de los derechos como lo ha logrado España.

Hoy en día las nuevas tecnologías han trazado retos para los legisladores, ocasionando muchas veces que las propuestas o adopciones vayan alienadas a intereses comerciales o políticos,

ISSN: 2007-8870
Universidad de Sonora

Año 16 / Núm. 39 / -Junio-julio 2023
Revista de Investigación Académica sin Frontera
ISSN 2007-8870

es decir ha intervenido para eliminar obstáculos jurídicos, en vez de aportar cimientos para un ecosistema normativo en armonía de seguridad y desarrollo. (Peguera Poch, Agustino Gui, & Casas Vallèsm, 2005)

El trabajo legislativo debe centrarse en los campos que el derechos mexicano no ha buscado profundizar como lo hizo España con su nueva regulación en materia digital; el Internet, las bases de datos, los derechos digitales pues son hoy en día los sectores que se están desarrollando con mayor aplicación en la sociedad y requieren de una reestructuración o replanteamiento de las normas para poder coexistir en equilibrio. Todo ello con el fin de asegurar incluir normas específicas en la materia, que protejan los datos personales, contemplen las posibles amenazas que puedan cometerse a través de los medios digitales, definir claramente los organismos o entidades que tendrán legitimación para los particulares como para el sector público, pues ellas deben de ser herramientas que faciliten las actividades y no amenazas contra el orden público.

Es de afirmarse que no solo se debe de enfocar en la creación de normas para los derechos de las nuevas tecnologías sino además en fomentar y promover las ventajas que el uso de estas proporcionan a la sociedad, ello con el objeto de fomentar la actividad ciudadana y no el rechazo. (Escobar Pérez, El papel del derecho en relación con el uso de tecnologías de información)

El normalizar el uso de instrumentos de vigilancia masiva, como cámaras con reconocimiento facial y de temperatura en lugares públicos, acceso del gobierno a la geolocalización y a la señal de bluetooth de los celulares de los ciudadanos se vuelve un paso en la generación de medios con los cuales cualquier agrupación o el mismo estado pudieran iniciar con la intromisión en la vida privada de las personas, caso similar el que ocurrió en la Ciudad de México a raíz de la aplicación *Periscope* la cual tuvo polémicas por el tratamiento ilegal y arbitrario a los datos personales de diversos ciudadanos. (Humanos, 2019).

Como es sabido, él Estado mexicano ha intentado múltiples veces establecer un sistema federal de identidad a través de la identificación oficial de RENAPO, todas culminando como aspiraciones insostenibles, no obstante diversos presidentes continúan aspirando a desarrollar su potencial. Es oportuno, que México reflexione sobre los tropiezos y las fallas que ha cometido en

ISSN: 2007-8870
Universidad de Sonora

Año 16 / Núm. 39 / -Junio-julio 2023
Revista de Investigación Académica sin Frontera
ISSN 2007-8870

materia de medios tecnológicos para establecer verdaderos panoramas de aplicación de nuevas herramientas y generar un ambiente amistoso entre la tecnología y los derechos humanos.

Actualmente los avances tecnológicos han permitido que diversas actividades se puedan trasladar a medios digitales, cambiando el mecanismo en el que las actividades del Estado se ejecutan. El nacimiento de nuevos panoramas de gobernanza en medios digitales ha llegado para replantear las políticas públicas y pensar más en las necesidades de los ciudadanos teniendo un alto contenido normativo para asegurar la protección a los derechos humanos.

Él Estado al generar bases de datos debe tener la capacidad de llevar a cabo sus objetivos de manera legal y responsable, no obstante es necesario la existencia de lineamientos normativos para determinar las medidas de comportamiento de los actores involucrados, que permitan la seguridad de la información y sea usada para los fines establecidos. La próxima implementación de la Cédula Única de Identidad Digital en México, eleva de manera considerable el rango de los datos biométricos al colocarlos en la línea principal de la actividad administrativa del estado, con ello al derecho a la identidad y libertad de expresión.

Terminare diciendo que, existe una gran brecha por superar, pues la poca credibilidad que hoy poseen algunos gobiernos, como el mexicano, son muros que de cierta manera que perjudican el proceso para perfeccionar la interacción social y trascender a medios más proactivos de gobierno. Es entonces, responsabilidad de los representantes políticos generar una convivencia sana, los cuales deben de dar el primer paso recuperar su credibilidad.

La actividad no debe circunscribirse únicamente a establecer referentes normativos en el uso de las bases de datos y manipulación de los datos personales, sino que además debe de asegurar un adecuado equilibrio entre el libre acceso a las nuevas tecnologías en conjunto con la protección de los derechos humanos, promover las ventajas que dichas herramientas tecnologías aportan a la administración de sus actividades, con el fin de mantener o aumentar la credibilidad del estado de derecho.

Es limitante solo formar soluciones técnicas, si no existe o se desarrollan estrategias políticas y regulatorias en materia de los sistemas digitales de almacenamiento de datos para ambos sectores público y privado (Harbitz & Arcos Axt, Políticas de identificación y gobernanza, Los

ISSN: 2007-8870
Universidad de Sonora

fundamentos jurídicos, técnicos e institucionales que rigen las relaciones e interacciones del ciudadano con el gobierno y la sociedad, 2010), así como estrategias de gobernanza en sistemas de identidad digital solidos que permitan una verdadera protección de los datos personales.

Bibliografía

Altvater, E. (2014). El control del futuro. Edward Snowden y la nueva era. *Nueva Sociedad 252*.

Arana, I. (18 de 05 de 2019). *La Vanguardia*. Obtenido de La inquietante apuesta china por el reconocimiento facial: https://www.lavanguardia.com/tecnologia/20190518/462270404745/reconocimiento-facial-china-derechos-humanos.html

Ayudaley. (2021). Obtenido de Guía adaptación de la LOPD a LOPDGDD en 2021: https://ayudaleyprotecciondatos.es/lopdgdd/.

B. Ocariz, E. (2018). *Blockchain y Samart Contracts, La revolución de la confianza.* México: Alfaomega Grupo Editor.

BBC News Mundo. (1 de 12 de 2019). *BBC News Mundo*. Obtenido de La polémica en China por la imposición del reconocimiento facial a todos los compradores de teléfonos: https://www.bbc.com/mundo/noticias-50622301#:~:text=A%20menudo%20se%20describe%20a,otros%20400%20millones%20para%202020

Biblioteca del Congreso Nacional de Chile. (2018). *Tecnología Blockchain: elementos básicos, aplicaciones y marcos regulatorios.* Chile.

Comisión de Derechos Humanos del Distrito Federal. (2016). El uso de las nuevas tecnologías y los derechos humanos. *Revista Dfensor*.

Conde González, F. (2016). El uso de redes sociales por parte de autoridades: consideraciones desde los derechos humanos. *Revista Dfensor, Número 6, año XIV*, 16-21.

Escobar Pérez , R. (s.f.). *El papel del derecho en relación con el uso de tecnologías de información.* Obtenido de http://www.ordenjuridico.gob.mx/Congreso/pdf/91.pdf.

Escobar Pérez, R. (s.f.). *El papel del derecho en relación con el uso de tecnologías de información.* Obtenido de ordenjuridico: http://www.ordenjuridico.gob.mx/Congreso/pdf/91.pdf

ISSN: 2007-8870
Universidad de Sonora

García Fernández, A. (27 de 03 de 2018). *celag.org*. Obtenido de Cambridge Analytica, el big data y su influencia en las elecciones: https://www.celag.org/cambridge-analytica-el-big-data-y-su-influencia-en-las-elecciones/

Gil, E. (2016). *Big data, privacidad y protección de datos.* Madrid: Agencia Española de Protección de Datos.

González, F. (2019). *Big data, algoritmos y política: las ciencias sociales en la era de las redes digitales.* Santiago, Chile: Observatorio de Política y Redes Sociales, Universidad Central de Chile.

Guzmán, M. (2013). *El derecho fundamental a la protección de datos personales en México: análisis desde la influencia del ordenamiento jurídico español.* Obtenido de Universidad Complutense de Madrid: https://eprints.ucm.es/22817/1/T34727.pdf.

Harbitz, M., & Arcos Axt, I. (2010). *Políticas de identificación y gobernanza, Los fundamentos jurídicos, técnicos e institucionales que rigen las relaciones e interacciones del ciudadano con el gobierno y la sociedad.* Washington D.C.: Banco Interamericano de Desarrollo.

Harbitz, M., & Arcos Axt, I. (2010). *Políticas de identificación y gobernanza, Los fundamentos jurídicos, técnicos e institucionales que rigen las relaciones e interacciones del ciudadano con el gobierno y la sociedad.* Banco Interamericano de Desarrollo.

Humanos, C. d. (2019). *Alcaldía Miguel Hidalgo ofrece disculpa pública por transmisiones en Periscope.* México: Dirección de Promoción e Información, Boletín 129/2019.

INAI. (2018). *GUÍA para el Tratamiento de Datos Biométricos* . Mexico: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales. (2018). España: Boletín Oficial del Estado, núm. 294.

Mendoza Enríquez, O. (2018). Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento, , . *Revista del Instituto de Ciencias Jurídicas de Puebla*, 267-291.

Montes, R. (31 de 5 de 2021). *Así hackearon los datos de más de un millón de empleados federales en DeclaraNet*. Obtenido de Milenio: https://www.milenio.com/politica/declaranet-hackearon-datos-de-mas-de-un-millon-de-empleados

P. T. (2021). *Acción de inconstitucionalidad 82/2021 y su acumulada 86/2021*. México: LXIV Legislatura.

ISSN: 2007-8870
Universidad de Sonora

Pedroza de la Llave, S. T. (2019). *Derecho y Tecnologías de la Información y la Comunicación.* Obtenido de forojuridico: https://forojuridico.mx/derecho-y-tecnologias-de-la-informacion-y-la-comunicacion/

Peguera Poch, M., Agustino Gui, A., & Casas Vallèsm, R. (2005). *Derecho y nuevas tecnologías.* Editorial UOC.

Pérez, E. (6 de 6 de 2020). *xataka*. Obtenido de Mercadona instala un sistema de reconocimiento facial en sus supermercados: cómo funciona y por qué genera importantes dudas sobre la privacidad: https://www.xataka.com/privacidad/mercadona-instala-sistema-reconocimiento-facial-sus-supermercados-como-funciona-que-genera-importantes-dudas-privacidad

Puyol, J. (03 de 11 de 2019). *¿Cuáles son los sistemas de reconocimiento e identificación biométrica de las personas?* Obtenido de Confilegal: https://confilegal.com/20190311-cuales-son-los-sistemas-de-reconocimiento-e-identificacion-de-las-personas/

Razza, C. (2020). *Transferencia internacional de datos personales en Latinoamérica.* Ecuador: CÁLAMO, Revista de Estudios Jurídicos.

Rodríguez Ayuso, J. F. (2021). *Garantía administrativa de los derechos del interesado en materia de protección de datos personales.* Barcelona: Bosch Edito.

Rubio Fernández, P., & Pérez-Jaén , M. (2022). *Iniciativa con proyecto de decreto, por el que se reforma la Ley general de protección de datos personales en posesión de sujetos obligados y la Ley federal de protección de datos personales en posesión de los particulares, en materia de datos biométricos.* México: LXV Legislatura del Honorable Congreso de la Unión. Obtenido de Iniciativa con proyecto de decreto, por el que se reforma la Ley general de protección de datos personales en posesión de sujetos obligados y la Ley federal de protección de datos personales en po.

Sanz Larruga, F. (1997). *EL derecho ante las nuevas tecnologías de la información.* España: Anuario da Facultade de Dereito da Universidade da Coruña.

Sanz Larruga, F. (1997). *EL derecho ante las nuevas tecnologías de la información.* España: Anuario da Facultade de Dereito da Universidade da Coruña.

Secretaría de la Función Pública. (2013). *Gobierno Digital o Electrónico*. Obtenido de www.gob.mx/sfp/documentos/gobierno-digital-o-electronico

Shahbaz, A., & Funk, A. (2021). *Freedom on the net 2021, The Global Drive to Control Big Tech* . Washington, DC: Freedomhouse.

ISSN: 2007-8870
Universidad de Sonora

Sheng, E., Chang, K.-W., Natarajan, P., & Peng, N. (2019). The Woman Worked as a Babysitter: On Biases in Language Generation. *Conference on Empirical Methods in Natural Language Processing and the 9th International Joint Conference on Natural Language Processing* (págs. 3407–3412). Hong Kong, China: Association for Computational Linguistics.

spanish.news.cn. (8 de 9 de 2022). *Xinhua Español*. Obtenido de China evalúa sistema de supervisión de aplicación de ley en ciberespacio: https://spanish.news.cn/20220908/561059a9b32244a6bcd60ae64503e834/c.html

Tapscott, D., & Tapscott, A. (2018). *La rebolución blockchain.* Mexico: Paidós.

Wiener, N. (1985). *Cibernética o el control y comunicación en animales y máquinas.* Barcelona: Tusquets Editores.

CÓMO CITAR

GALLEGOS, D. (2023). Gestión de la identidad en la prevención de medios de vigilancia social. *Revista De Investigación Académica Sin Frontera: División De Ciencias Económicas y Sociales*, (39). https://doi.org/10.46589/rdiasf.vi39.550

ISSN: 2007-8870
Universidad de Sonora