



DERECHO ADMINISTRATIVO, BIG DATA Y PROTECCIÓN DE DATOS PERSONALES

ADMINISTRATIVE LAW, BIG DATA AND PERSONAL DATA PROTECTION

FELIPE ROTONDO TORNARÍA ¹

RESUMEN

La Administración estatal debe servir al público, lo que legitima el ejercicio de poderes que el ordenamiento jurídico establece. Para ello utiliza herramientas, entre ellas las que hoy día provienen de las nuevas tecnologías de la información y la comunicación.

En todo caso y como en toda materia procede el respeto de los derechos humanos, entre ellos el de protección de los datos personales.

PALABRAS CLAVE

Administración | Su carácter servicial | Instrumentos tecnológicos y derechos humanos.

CONTENIDO

1. Derecho Administrativo, **1.1** Su objeto. Carácter servicial de la Administración, **1.2** Sujeción al derecho. Enfoque ético; **2.** Big data, **2.1** Noción Básica, **2.2** Tipos y fuentes de datos, **2.3** Valor de los datos, **2.4** Inteligencia artificial: referencia; **3.** La Administración y las TIC, **3.1** Utilización de las nuevas tecnologías, **3.2** Incidencia en la organización, **3.3** Incidencia en el procedimiento, **3.4** Continuación, **3.5** Relación con el Open Data, **3.6** Utilidad del Big Data; **4.** Derecho a la Protección de Datos Personales, **4.1** Naturaleza. Sujetos, **4.2** Configuración, **4.3** Principios; **5.** Anotaciones Finales; **6.** Bibliografía.

SOBRE EL ARTÍCULO

El presente artículo fue recibido por la Comisión de Publicaciones el 29 de abril de 2021 y aprobado para su publicación el 19 de agosto de 2021.

1. DERECHO ADMINISTRATIVO

1.1. Su objeto. Carácter servicial de la Administración

El Derecho Administrativo trata básicamente de la organización y actividad de la

¹ Profesor de Derecho Administrativo, Universidad de Montevideo. Integrante de la Unidad Reguladora y de Control de Datos Personales cuyo Consejo Ejecutivo preside por períodos anuales en alternancia con otro miembro, y de la Comisión Nacional de Servicio Civil de la República Oriental del Uruguay.

Administración, la cual es el conjunto de órganos estatales que ejercen función administrativa.

La Administración forma parte, pues, del Estado y como tal, en un Estado constitucional de Derecho, su centro radica en la persona humana, titular de una dignidad que es atributo de su esencia y vale con independencia de la dignidad moral individual².

La Administración debe servir al interés general, el cual justifica el ejercicio del poder público y, a la vez, lo configura como instrumento para cumplir las competencias que establece el ordenamiento jurídico y ello de manera transparente, razonable y motivada. Así podrá hacer efectiva una “buena administración”, la cual se concibe hoy como un principio de derecho y, por tanto, un deber de la organización administrativa³.

El referido interés general “es la dimensión pública de los intereses individuales, o sea de los intereses de cada individuo en cuanto participe de la sociedad (jurídicamente organizada en el Estado) (Bandeira de Mello, 2010, p. 18)⁴; en términos de la legislación uruguaya, este interés:

...se expresa, entre otras manifestaciones, en la satisfacción de necesidades colectivas, de manera regular y continua, en la buena fe en el ejercicio del poder, en la imparcialidad de las decisiones adoptadas, en el desempeño de las atribuciones y obligaciones funcionales, en la rectitud de su ejercicio y en la idónea administración de los recursos públicos. La satisfacción de necesidades colectivas debe ser compatible con la protección de los derechos individuales, los inherentes a la personalidad humana o los que se deriven de la forma republicana de gobierno⁵.

1.2. Sujeción al Derecho. Enfoque ético

Las reglas que constituyen este Derecho se dirigen, pues, a atender el bienestar colectivo, el cual se configura con el goce de los derechos de las personas.

Tienden a su protección y la de los diversos grupos sociales en relación al ejercicio del poder público; mejor, a asegurar que este cumpla con su misión servicial. Si la esfera pública es la “de los intereses de todos”, su forma más acabada se genera:

-
- 2 Conf. Ardao, Arturo. El hombre en cuanto objeto axiológico, en “El hombre y su conducta. Ensayos filosóficos en honor de Risieri Frondizi”. Puerto Rico 1980, Ed. Universitaria, pp. 73-74, cit. por Héctor Gros Espiell, La dignidad humana en los instrumentos internacionales sobre Derechos Humanos. Anuario de Derechos Humanos. Nueva época Vol. 4. Instituto de Derechos Humanos. Facultad de Derecho. Universidad Complutense. Madrid 2003, p. 193.
 - 3 Sobre la buena administración, la Carta Iberoamericana de los Derechos y Deberes del Ciudadano en relación con la Administración (CLAD, Caracas 2013) expresa que es la que actúa según los principios de eficacia, con procedimientos que remuevan de oficio obstáculos formales y dilaciones “buscando la compatibilidad con la equidad y el servicio objetivo al interés general”; eficiencia, que exige “optimizar los resultados alcanzados en relación con los recursos (...)” y economía en cuanto al “uso racional de los recursos públicos disponibles. El gasto público se realizará atendiendo a criterios de equidad, economía, eficiencia y transparencia”.
 - 4 Bandeira de Mello, Celso Antonio. Grandes temas de Direito Administrativo. 1ª ed. 2º tirajem. Malheiro Ed. S. Paulo 2010, A noção jurídica de interesse público, p. 181.
 - 5 Leyes N° 17.060 de 23-XII-1998, art. 20 y N° 19.823 de 19-IX-2019 sobre Normas de Conducta en la Función Pública.

...por la constitucionalización de esos intereses de todos que son los derechos universales y, por ello, fundamentales. Dígase lo mismo 'del pueblo', aquí definido como el sujeto jurídico colectivo cuyos componentes son unificados por la igual titularidad de expectativas constituidas, como son precisamente los derechos fundamentales. (Ferrajoli, 2011, p. 52-53)⁶.

Por otra parte, el Estado y su Administración se sujeta a las reglas de Derecho, tanto a los principios como a la normativa constitucional, legal, reglamentaria y, por cierto, a la internacional, en especial la concerniente a los Derechos Humanos.

El Derecho Administrativo no se enfoca, entonces, en la potestad pública, sino en el administrado, mejor dicho, la persona. Sus normas:

...se dirigen a atender el bienestar colectivo, el cual se configura con el goce de los derechos de las personas. Tienden a su protección y la de los diversos grupos sociales en relación al ejercicio debido del poder público; a asegurar que este cumpla con su misión servicial" (Rotondo, 2015, p. 87) ⁷.

Es un Derecho Administrativo personalizado y garantista que supera: "concepciones meramente técnicas para asumir la prevalencia del enfoque ético, en que se reconoce la supremacía de los derechos fundamentales y la consagración de los procedimientos democráticos de formación y manifestación de la voluntad estatal" (Justen Filho, 2006, p. 47-48)⁸.

2. BIG DATA

2.1. Notión básica

El big data dice relación con las tecnologías de la información y la comunicación (TIC), e implica el tratamiento de grandes cantidades de datos procedentes de diversas fuentes con el fin de hallar interrelaciones, encontrar patrones repetitivos e inferir información; al efecto la dinámica de las nuevas tecnologías usa algoritmos. Sus características van más allá de la capacidad de las herramientas habituales del software.

El concepto de 'datos masivos' implica la búsqueda, recolección y almacenamiento de enormes cantidades de datos, así como los procedimientos seguidos para su análisis y obtención de tendencias; el análisis puede configurarse, entre otras modalidades, mediante asociaciones que habilitan hallar relaciones entre variables y minería de datos para ubicar comportamientos predictivos, combinando métodos estadísticos y de machine learning con almacenamiento en bases.

6 Ferrajoli, Luigi. Principia iuris. Teoría del derecho y de la democracia. 2. Teoría de la democracia. Ed. Trotta. Madrid 2011, pp. 52-53: "*Las instituciones públicas son las que están dirigidas al ejercicio de funciones públicas y/o la garantía de situaciones universales, las primeras de todos los derechos fundamentales*".

7 Rotondo, Felipe. Derechos fundamentales y Derecho administrativo. Revista de Derecho Público, Año 24. N° 47. Mdeo. 2015, p. 87.

8 Justen Filho, Marçal. Curso de Direito Administrativo. 2ª ed. Ed. Saraiva 2006, pp. 47-48. Carlos F. Balbín. Curso de Derecho Administrativo. La Ley T. I 1ª ed. 1ª reimpresión Bs.As. 2008, pp. 95-98 refiere al "*(...) equilibrio del poder, entendido como el conjunto de prerrogativas que persiguen el reconocimiento de derechos vs. otros derechos. Ese equilibrio entre derechos con intermediación del poder estatal y sus prerrogativas es el paradigma (...) del Derecho Administrativo actual*".

El valor del Big data no radica (solo) en la cantidad (*volumen*) de datos procesados sino en la capacidad de inferencia que deriva de su *variedad* y *velocidad* (de crecimiento), y se vincula a las notas de veracidad, calidad, confiabilidad y a las cuestiones de su tratamiento en virtud, precisamente, del enorme volumen y complejidad.

2.2. Tipos y fuentes de datos

Los datos pueden ser *estructurados*, con formato y longitud definidos, (ejemplo, datos fiscales de los contribuyentes); *no estructurados*, dispersos (ejemplos, los e-mails o datos que surgen de expedientes administrativos) o *semiestructurados*, que con sus propios metadatos refieren a los objetos y sus relaciones (caso del HTML).

Por otra parte, pueden ser estáticos, concretos en el tiempo (renta de una persona en cierto período) o dinámicos, obtenidos de modo continuo, los cuales permiten mayor análisis hacia el futuro (ejemplo, sobre el tráfico de la ciudad o los lapsos de acceso a servicios públicos).

En cuanto a sus fuentes, los datos pueden generarse por las personas, así al enviar mensajes de whatsapp, correos electrónicos, tuitear contenidos, utilizar motores de búsqueda, etc.; emerger de cruzamientos de datos, automáticamente o no; producirse entre máquinas con diversos dispositivos, caso de los sensores, geo-localizadores, etc. y generarse por lectores biométricos de huella, retina, etc.

En este sentido el Big Data se vincula con el Internet de las Cosas (IoT), estructura de red por la cual los dispositivos físicos se interconectan de modo de recabar, transmitir, almacenar y analizar datos como tablets con pantallas más grandes, electrodomésticos inteligentes, wearables.

El volumen y velocidad con que los datos se generan exigen un adecuado almacenamiento, procesamiento y análisis, incluso para que no queden obsoletos, sean veraces y contribuyan a la finalidad del titular de la base y, si corresponde, se supriman, actualicen o archiven.

A los efectos indicados existe hoy la disciplina llamada Ciencia de Datos.

2.3. Valor de los datos

Los datos como información tienen un valor inconmensurable en todo sentido y ámbito (social, económico, científico, administrativo, etc.) dados los resultados que pueden alcanzarse con el trío que forman con la tecnología y el análisis.

Pero si bien esto da lugar o habilita beneficios implica, a la vez, riesgos, entre otros a la vulneración de la privacidad y de los datos personales.

En ese sentido, cabe citar el documento "*Seizing opportunities, preserving values*" derivado del mandato del entonces Presidente de Estados Unidos de Norteamérica Barack Obama, quien se comprometió entonces (enero 2014) a ajustar el programa de vigilancia sobre datos telefónicos. Expresa que las tecnologías de Big Data, como toda tecnología, no son, *per se*, buenas o malas, que pueden utilizarse para el bien de la sociedad o para dañar y que en su perspectiva positiva contribuyen a fortalecer la democracia, generar crecimiento económico y mejorar la calidad de vida de los ciudadanos en diversas áreas.

Afirma, también, que en cuanto a los derechos de los ciudadanos el tratamiento de datos habilita a las autoridades públicas a realizar prácticas discriminatorias y que los valores en peligro se relacionan directamente con la privacidad, por lo que es necesaria la protección

de toda información personal con adecuadas leyes de protección a consumidores y a los ciudadanos en general, garantizando que la información recolectada sea utilizada para fines permitidos y previamente establecidos.

2.4. Inteligencia Artificial: referencia

El Big data y la capacidad de aprendizaje autónomo “hacen posible que las computadoras perciban, aprendan, razonen y colaboren en el proceso de toma de decisiones para la resolución de problemas en formas que resultan similares a lo que hace la gente” (Smith y Shum, 2018)⁹.

He ahí la Inteligencia Artificial, sobre la cual no existe una única definición:

...podría afirmarse que, en su concepción amplia, se trata de un término ‘sombrija’ que incluye una variedad de técnicas computacionales y de procesos enfocados a mejorar la capacidad de las máquinas para realizar muchas actividades, los que comprenden desde modelos algorítmicos, pasando por los sistemas de machine learning, hasta llegar a las técnicas de deep learning” (Red Iberoamericana de Protección de Datos, 2019)¹⁰.

Hoy día la Inteligencia Artificial se aplica cada vez más: “asistentes virtuales en nuestros celulares, algoritmos en las redes sociales que nos muestran de una u otra forma la información, autos sin conductor, programas que aprenden de nuestras acciones para recomendarnos música, películas o artículos de consumo en tienda online, traductores en tiempo real, sistemas que detectan de forma temprana enfermedades o riesgos sanitarios, entre otros” (AGESIC, 2019)¹¹.

Pero, también, sirven para alterar o falsificar videos y hacer aparecer personas ausentes en una reunión o hacerles decir lo que no han dicho, con incidencia en múltiples ámbitos, incluso en la actividad política y el voto del ciudadano y otras múltiples situaciones, lo cual puede darse, incluso, sin mala fe por defecto de los diseños de sistemas.

Todo ello plantea cuestiones éticas y jurídicas, propias de la esencia de la persona humana, ser social y responsable, que debe asumir lo que debe hacer o no hacer y cómo hacerlo y las consecuencias de su conducta¹².

9 El futuro computarizado. La Inteligencia Artificial y su rol en la sociedad, por Microsoft. Prólogo de Brad Smith y Harry Shum. Washington. EE.UU. 2018. En el Capítulo 1 señala que las tecnologías abarcan capacidad de diversa índole de las computadoras: visión (‘ver’ mediante el reconocimiento de lo que figura en una imagen o video); voz (‘escuchar’ mediante la comprensión de las palabras que las personas dicen y transcribirlas a texto); lenguaje (‘comprender’ el significado de las palabras según los diversos matices y complejidades del lenguaje) y conocimiento (‘razonar’ mediante la comprensión de la relación entre personas, cosas, lugares, eventos y conceptos similares).

10 Cf. Recomendaciones generales para el Tratamiento de Datos en la Inteligencia Artificial aprobadas por la Red Iberoamericana de Protección de Datos. XVII Encuentro, Naucalpan de Juárez-México 2019.

11 Estrategia de Inteligencia Artificial para el Gobierno Digital. Agencia para el Desarrollo del Gobierno de Gestión Electrónico y la Sociedad de la Información. (AGESIC) Uruguay. <http://www.fic.edu.uy/sites/default/files/2019-10/estrategia%20de%20inteligencia%20artificial.pdf>

12 Las diversas cuestiones involucradas han determinado la Propuesta de Reglamento del Parlamento Europeo y del Consejo, de 21-IV-2021, por el que se establece normas armonizadas en materia de Inteligencia Artificial (Ley de Inteligencia Artificial) y modifican determinados actos legislativos de la Unión. Contiene una clasificación en base a riesgos según la función del sistema de Inteligencia Artificial; plantea como no admisibles, entre

Procede tener en cuenta, por otra parte, que: “El cúmulo abrumador de información que nos inunda no significa más sabiduría. La sabiduría no se fabrica con búsquedas ansiosas por Internet, ni es una sumatoria de información cuya veracidad no está asegurada (...)” (Francisco, 2020, p. 37)¹³.

3. LA ADMINISTRACIÓN Y LAS TIC

3.1. Utilización de las nuevas tecnologías

La Administración, en su organización y en su actividad, debe mirar hacia el futuro y replantearse, efectuar el tránsito de la Galaxia Gutenberg a la Galaxia Internet¹⁴.

Las TIC, “por sí solas no transforman los roles, la estructura y las funciones, pero en un sistema democrático, abren importantes posibilidades para que los agentes transformadores impulsen genuinas reformas” (Prats y Catalá Joan, 2015, p. 21)¹⁵.

Elas contribuyen a la interrelación de la Administración con el entorno, a que sea abierta a la participación ciudadana, transparente y a que preste los servicios de la mejor manera, con procedimientos más simples y de menor duración, que sean idóneos en cuanto a resultado, tiempo y costos, a que se reduzcan las molestias del administrado, por ejemplo, al no exigirse su desplazamiento a la oficina para recabar informaciones.

3.2. Incidencia en la organización

Desde esta perspectiva, las nuevas tecnologías habilitan a la Administración a reducir el número de cargos de supervisión; a ampliar el ámbito físico de las tareas y hasta independizarlo mediante el correo electrónico, la videoconferencia, el teletrabajo, etc., de modo que contribuyen a la flexibilidad de la estructura, a redefinir sus fronteras e implicar un nuevo gerenciamiento, a la transversalidad interna de cada entidad y entre las entidades que integran la Administración de modo que operen como unidad, con mayor servicialidad hacia el administrado.

No se eliminan las modalidades organizativas clásicas (desconcentración, delegación, descentralización, etc.) pero se requiere una mayor coordinación y una estructuración

otros, los que presentan gran potencial para manipular personas con técnicas subliminales que van más allá de sus conciencias o explotan vulnerabilidades de grupos como menores de edad o personas con discapacidad, y pueden distorsionar su conducta hasta generar, en ellos o terceros, un daño físico o psíquico. También los sistemas gubernamentales de puntuación social o los de identificación biométrica remota en tiempo real en lugares públicos como el reconocimiento facial, salvo caso de extrema gravedad; entre los sistemas de alto riesgo están los de filtrado de perfiles profesionales en procesos de selección- susceptibles de replicar sesgos-, o los de calificación crediticia, entre otros. En cuanto al uso de algoritmos, complementa la normativa con requerimientos específicos para minimizar el riesgo de discriminación, en especial la referida al diseño y calidad de los sets de datos utilizados, lo que se complementaría con obligaciones de gestión de riesgos, testeos y supervisión humana a lo largo de todo el ciclo vital de los sistemas.

13 SS Francisco. Carta Encíclica Fratelli Tutti. Sobre la fraternidad y la amistad social. Paulinas. Bs.As. 2020, p. 37.

14 El primero, título del libro de Marshall Mc Luhan de 1962, el segundo de Manuel Castells. Barcelona. Areté 2001.

15 Prats y Catalá Joan. De la Burocracia al Management, del Management a la Gobernanza. Las transformaciones de las Administraciones Públicas de nuestro tiempo. Estudios Goberna. INAP. Madrid, 2005, p. 21.

que promueva y asegure el uso adecuado de las tecnologías y permita una articulación más fuerte, nexos basados en la disposición de información estratégica confiable en una actividad mancomunada, incluso en el ámbito de la llamada “descentralización por colaboración”, que comprende la actuación del sector privado.

Hoy la gobernanza se inserta en la Sociedad de Redes porque además de implicar una conexión entre la Administración, prestadores privados de servicios, usuarios, unidades de investigación, etc., ellos son interdependientes y dan lugar a un grupo determinante en el proceso de elaboración de políticas.

“En la Sociedad de Redes moderna, (...) estamos dependiendo cada más del acceso a las redes y a la información que contienen y los servicios que ofrecen. Podemos hablar de un entorno digital (...)” (Saarenpää, 2019, p. 105)^{16/17}.

3.3. Incidencia en el procedimiento

La despapelización de los expedientes, ahora digitales, determina por su parte la necesaria adecuación de los procesos y, en su caso de las normas jurídicas, “para continuar otorgando a las personas los mismos derechos y garantías que en el ámbito material” (Viega, 2013)¹⁸, garantías que corresponden al principio de seguridad, expresión específica del de juridicidad.

Dada la innegable importancia del soporte, se ha llegado a identificar procedimiento y expediente, si bien este es el resultado documental del procedimiento.

Así se ha dicho que el soporte papel se convirtió “en una de las herramientas básicas de la Administración” y recordado que uno de los principios de dominación legal de Max Weber es el “atenerse al expediente”, lo que debería mantenerse en la era de la Administración Electrónica, “convenientemente puesto al día”, porque es “una herramienta básica del principio de legalidad, en tanto forma esencial de expresión de la voluntad administrativa. La escritura es garantía de una Administración más cerebral que pasional, menos caprichosa y mejor informada, con más criterio sobre las decisiones a tomar, más objetiva en suma” (Ortega, 2008, p. 52-55)¹⁹.

La despapelización habilita enlaces de diversa documentación a modo de hiperexpediente

16 Saarenpää, Atthi. “Protección de datos: lo excepcional llega a ser lo natural”. Revista de Derecho y Nuevas Tecnologías N° 1-2019. La Ley Uruguay, pp. 105 y ss. Expresa: “en el gobierno de la información actual dependemos de un entorno operativo digital y los enlaces electrónicos del ciudadano promedio con el gobierno son más interactivos y se realizan en tiempo más real que antes”; “en la Sociedad de Redes, dependemos críticamente de las redes de información y su uso en el gobierno y en otros lugares. Su utilización toma diversas formas, desde la creación de documentos, hasta la comunicación y desde iniciar asuntos de manera electrónica hasta la utilización de una gran variedad de cuentas electrónicas (canales seguros de hecho) que establecen los individuos y las organizaciones”.

17 “(...) en un mundo donde las funciones públicas esenciales, la comunicación social y la información personal migran a plataformas digitales, los gobiernos en colaboración con la sociedad civil y las empresas, necesitan crear las reglas, los controles y los equilibrios necesarios para mantener la justicia, la competitividad, la equidad e incluso la propiedad intelectual, la seguridad y la fiabilidad”, Klaus Schwab. La Cuarta Revolución Industrial. World Economic Forum. Ed. Debate, España 2016.

18 Conf. Viega, María José. Procedimiento administrativo electrónico. Presentación realizada en las VIII Jornadas del Tribunal de lo Contencioso Administrativo. Mdeo, 2013.

19 Rivero Ortega, Ricardo. El Expediente Administrativo. De los Legajos a los Soportes Electrónicos. Thomson Aranzadi. Pamplona 2008, pp.52-55.

y un mejor manejo simultáneo de expedientes, lo que es especialmente útil en la actividad de control o en el funcionamiento de órganos colegiados²⁰.

3.4. Continuación

En el aspecto del procedimiento administrativo, como secuencia de etapas conformadas por actos jurídicos y operaciones materiales dirigidas a cierto objetivo, de los cuales el más usual es el dictado de un acto jurídico principal (resolución de un asunto), la cuestión se proyecta en el *procedimiento electrónico*, el cual implica actuaciones de esta índole, incluso actos administrativos que se forman por medio del computador o este los “crea”.

En el segundo caso se trata de actos automatizados, especie del electrónico, en los que no intervienen personas físicas, sino que el sistema produce la decisión (Delpiazzo, 2010, p. 79)²¹.

Por ello, para que no se “traslade” la autoridad de las personas a los algoritmos y acorde con principios como los de objetividad y transparencia, procede establecer “previamente el órgano u órganos competentes, según los casos, para la definición de las especificaciones, programación, mantenimiento, supervisión y control de calidad y, en su caso, auditoría del sistema de información y de su código fuente. Asimismo, indicarse ‘el órgano que debe ser considerado responsable a efectos de impugnación (Ley española N° 40/2015)”^{22/23}.

En cuanto al objeto de los referidos actos, las innovaciones tecnológicas como la Inteligencia Artificial habilitan a la Administración a tomar decisiones derivadas de algoritmos con base en análisis predictivos y sistemas con capacidad de aprendizaje. Pero esos algoritmos pueden contener un parámetro con un supuesto erróneo o que sea irrelevante para adoptar una medida jurídicamente válida; también pueden tener una falla de programación, así; por ejemplo, parámetros vinculados en términos ilógicos entre sí o con relación a la regla a aplicar.

De ahí que “la confianza ciega en la tecnología puede traducirse en situaciones de profunda injusticia de nula o tardía solución si no se cuenta con mecanismos de contingencia y

20 En ese sentido el decreto uruguayo N° 276/013 de 9-IX-2013 sobre procedimiento electrónico en la Administración Central, art. 11, establece que “Cuando un expediente electrónico esté a consideración de un órgano colegiado será puesto en conocimiento simultáneo a todos sus integrantes a efectos de ser estudiado y resuelto dentro del mismo plazo” y el art. 12, que si se requiere la actuación de otro órgano u organismo, “esta se producirá a través de medios electrónicos de comunicación, salvo que causas justificadas lo impidan, dejándose constancia explicativa de ello”.

21 Delpiazzo, Carlos E. Noción y regulación del procedimiento y del acto administrativo electrónico, en Estudios de Derecho Administrativo. La Ley, Mdeo. 2010 N° 1, p. 79 y ss. Expresa que es viable en la actividad reglada y en la discrecional, en esta última “mediante la implementación de sistemas expertos capaces de emular la conducta de un experto humano dentro de un dominio limitado a partir del llamado ‘razonamiento cibernético’ (...)”.

22 Ley española N° 40/2015, 1° de octubre, de Régimen Jurídico del Sector Público, art. 41.2. Condice con el Reglamento (UE) 2016 del Parlamento Europeo y del Consejo, de 27-IV-2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la circulación de estos datos, art. 22.

23 En ese sentido, Valero Torrijos, Julián. Las garantías jurídicas de la inteligencia artificial en la actividad administrativa desde la perspectiva de la buena administración. Revista Catalana de Dret Public N° 58-2019, pp. 82 y ss.

acción con recursos humanos calificados para responder” (Pezzutti, 2020).²⁴

Otro aspecto de incidencia de las nuevas tecnologías es el de posibilitar una mayor participación ciudadana, habilitando que los habitantes sean informados y consultados en los asuntos que les atañen.

Al efecto se les reconoce el derecho a relacionarse electrónicamente con la Administración, sin excluir los medios tradicionales, por lo cual el uso y desarrollo de las TIC no es una facultad discrecional de los organismos públicos sino su obligación²⁵, “lo que supone que las Administraciones estén interrelacionadas entre sí a fin de simplificar los procedimientos” (2007)²⁶.

La interoperabilidad es un supuesto imprescindible para la actuación administrativa electrónica; se la entiende como la capacidad de los sistemas de información, y por ende de los procedimientos a los que estos dan soporte, de compartir datos y posibilitar el intercambio de información entre ellos. Se trata de una cuestión instrumental que tiene como sustrato la viabilidad de la circulación de la información pública entre las Administraciones como cuestión sustancial (Delpiazzo, 2020, p. 17-36)^{27/28}.

3.5. Relación con el Open Data

Las TIC interesan, también, en relación al open data que refiere a los datos abiertos por parte de la Administración, accesibles a cualquier persona de manera gratuita o a un costo mínimo, y por medios de publicidad que deben resultar amigables, con contenido veraz y lenguaje entendible, en tiempo real.

24 Conf. Pezzutti, Miguel. Los actos administrativos electrónicos. Mdeo. 2020 inédito. Ejemplifica con la actual pandemia del coronavirus y los esfuerzos por suministrar vacunas: “La implementación de sistemas que distribuyan agendas solo mediante acceso remoto, resulta idónea para garantizar la inexistencia de privilegios indebidos en el acceso, por lo que parece contar con sólidos fundamentos en los principios de igualdad y eficacia. Pero si existe una base de datos con errores (ejemplo de supuesto inválido en el algoritmo por errores en las fechas de nacimiento) que impidan a cierto sector de la población vulnerable (mayores de 80 años, por ejemplo) acceder a la vacuna, podrían verificarse contagios con efectos graves que podían prevenirse o bien el agotamiento de partidas con la definitiva imposibilidad de acceso en una campaña, puesto que la eficiencia en el reparto conspira contra los indebidamente excluidos”.

25 Así en el Uruguay este derecho se prevé por la ley N° 19.355 de 18-XII-2015, art. 74.

26 Carta Iberoamericana de Gobierno Electrónico aprobada por la IX Conferencia Iberoamericana de Ministros de Administración Pública y Reforma del Estado, Pucón, Chile, 31-V y 1-VI- 2007; se adoptó por la XVII Cumbre Iberoamericana de Jefes de Estado y de Gobierno, Sgo. de Chile, 10-XI- 2007.

27 Delpiazzo, Carlos E. Impacto de las TIC en el Derecho Administrativo en Impacto de las Nuevas Tecnologías en el Derecho Administrativo. Instituto de Derecho Administrativo, Facultad de Derecho. Universidad de la República. FCU. Mdeo. 2020, pp. 17-36.

28 La ley uruguaya N° 18.719 de 27-XII-2010, arts. 157 a 161, establece que las entidades públicas, estatales o no, deberán adoptar las medidas necesarias e incorporar en sus respectivos ámbitos tecnologías para promover el intercambio de información pública o privada autorizada por su titular, disponible en medios electrónicos; que deben cumplir con las obligaciones de secreto, reserva o confidencialidad y las medidas necesarias para garantizar niveles de seguridad y confidencialidad adecuados; que recabarán el consentimiento cuando corresponda según la ley de Protección de Datos Personales y que responderán por la veracidad de la información al momento de producirse el intercambio. El art. 159 nomina como principios rectores los de cooperación e integralidad; finalidad; confianza y seguridad; previo consentimiento informado de los titulares de los datos personales; eficiencia y eficacia.

En la sociedad de la información y el conocimiento cobra vigor el derecho al acceso a la información como modo de llegar a la verdad, propio de la naturaleza racional de la persona y del principio de transparencia, esencial en un sistema democrático; en este sentido la regla es la transparencia activa y pasiva de lo que es, precisamente, de naturaleza “pública”.

Así se tiene el derecho al acceso a la información pública el cual, por otro lado, permite un mejor proceso de toma de decisiones al implicar mayor visibilidad, contribuir a la participación ciudadana y a que la Administración sirva realmente al interés general, evitando la corrupción²⁹.

Al efecto procede una ponderación de derechos en base a criterios generales cuya aplicación, obviamente, exige atender la especificidad de cada caso.

El open data debe darse, además, de manera global en el ámbito de la Administración, lo que exige cooperación entre las entidades que la conforman y la sujeción a buenas prácticas.

De todos modos, hay información en poder de la Administración Pública que al referir a personas identificadas o identificables no es pública y está tutelada por la normativa de protección de datos personales.

3.6. Utilidad del Big Data

En cuanto al uso de las tecnologías de Big Data por la Administración, los tratamientos contribuyen al cumplimiento de sus cometidos y el ejercicio de los respectivos poderes instrumentales.

Por ejemplo, en áreas como las de la salud, para prevenir riesgos sanitarios, establecer los caracteres de enfermedades y su atención médica, ordenar los tiempos hospitalarios o controlar beneficios por licencia por enfermedad; en la materia energética, a fin de gestionar la eficiencia en el uso del alumbrado público o controlar el consumo particular; en la recaudación tributaria, para mejorar la actividad inspectiva y verificar las declaraciones de los contribuyentes; en la educativa, para prevenir la deserción escolar o encarar programas de estudio adecuados; en la seguridad pública, para prevención de delitos, determinar tendencias por zonas, en lo cual es especialmente relevante la protección de la identidad de las personas y evitar “*sesgos incrustados*” de cualquier índole (de género, etnia, posición económica, etc.).

La utilización en las ciudades inteligentes (smart cities) es un ejemplo del aporte *coordinado* de información de diverso tipo (tratamiento de información sobre energía, tránsito vehicular, ambiental, etc.) con un objetivo de desarrollo sostenible basado en inversiones variadas, más allá de la tecnológica.

29 En el Uruguay rige la ley 18.381 de 17-X-2008, que define como información pública “*la que emane o esté en posesión de cualquier organismo público, estatal o no estatal*” y reconoce el derecho al acceso a esa información sin necesidad de justificarse las razones por las que se la solicita. Los lineamientos esenciales son los de divulgación máxima de la información; presunción *juris tantum* a favor de la publicidad; proporcionalidad y legalidad (formal, no por reglamento) de las restricciones a la información, para las cuales deben existir razones objetivas y explícitas que revelen el daño para un bien jurídico protegido, sea un interés público o una información privada cuya tutela sea de interés público. Ninguna razón es admisible si la información refiere a violaciones de derechos humanos o es relevante para investigar, prevenir o evitar estas violaciones.

De manera general, el Big data contribuye al diseño, implementación, evaluación y monitoreo de políticas públicas y a la prestación de servicios públicos, lo cual debe insertarse en una gobernanza digital que respete y haga respetar los derechos de las personas, entre ellos a la protección de los datos personales, dado el enorme cúmulo de datos recabados y almacenados por la organización administrativa, con creación de perfiles de quien se relaciona con la Administración como usuario, consumidor, etc.

Por lo mismo, el uso del Big data ha de configurarse sobre un principio de transparencia *reforzado* porque muchos datos pueden proceder de terceros, de cruzamiento de información entre las entidades, etc. sin el conocimiento del afectado y, además, en interconexión con dispositivos digitales, lo que hace que el uso de los datos sea más complejo y opaco.

También sobre el principio de igualdad que por esencia es relacional y no admite ninguna discriminación o sesgo arbitrarios; este principio puede encararse incluso como de inocuidad en el sentido de que de ningún modo se lesionen valores humanos, individuales o sociales.

Estos principios se interrelacionan con los aplicables en materia de protección de datos personales que se indican en el apartado siguiente.

De otra manera la innovación tecnológica llevará a ilegitimidad de los tratamientos y a que no se logre la confianza social que la respalde.

4. DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

4.1. Naturaleza. Sujetos

Existe el derecho a la *intimidad*, a lo reservado de cada persona, el derecho a “*ser dejado solo*” (a la soledad, de Warren y Brandeis, ‘*The Right to Privacy*’, 1890), “prerrequisito para la construcción de la autonomía individual que a su vez constituye el rasgo esencial del sujeto democráticamente activo” (Tribunal Constitucional de Colombia, 2010)³⁰.

También, en visión usualmente seguida, el más amplio de privacidad respecto a un ámbito que se comparte con los más cercanos; corresponde al respeto de una *esfera privada* de cada persona y su entorno, exento de la invasión de terceros y de la autoridad de los magistrados.

En ese enfoque se hace referencia a generaciones de derechos, si bien en todos ellos, de un modo u otro, se configuran nuevas facetas por la incidencia de la sociedad tecnológica.

Dada la fuerza expansiva de los derechos y con base en el de la intimidad y el más amplio de la privacidad, se desarrolló el relativo a la protección de los datos personales en un entorno en que el obligado es tanto público como privado, constituyendo un derecho de tercera generación, fundamental y propio de un sistema democrático.

Muchas normativas, entre ellas la ley uruguaya N° 18.331 de 11-VIII-2008, art. 1°, lo

30 Términos de la sentencia del Tribunal Constitucional de Colombia, sentencia C-640/10 de 18-VIII-2010.

reconocen como derecho “inherente a la personalidad humana”^{31/32}.

El reconocimiento o declaración, con finalidad tuitiva, procede por esa inherencia; el art. 6º inciso 2º de la citada ley establece, por otra parte, que: “Las bases de datos no pueden tener finalidades violatorias de derechos humanos” o “contrarias a las leyes o a la moral pública”.

4.2. Configuración

El derecho a la protección de los datos personales tiene una configuración compleja ya que comprende varios poderes de disposición y control de esos datos: “la facultad de saber en todo momento quién dispone de ellos y a qué uso los está sometiendo”; “el poder oponerse a esa posesión y usos.(...)”, el “consentir sobre la recogida y uso de los datos personales y a saber de los mismos”; el de requerir a quien corresponda que ponga fin a su posesión y empleo, o “en su caso, requerirle para que los rectifique o los cancele” (Tribunal Constitucional español 292/000)³³.

Asimismo, comprende el derecho a impugnar valoraciones personales efectuadas en base a un tratamiento automatizado de datos, lo que es relevante ante la utilización del Big data.

Por cierto, el derecho de la protección de datos personales no es absoluto; la Suprema Corte de Justicia de Uruguay suele expresar en sus fallos que los derechos no son ilimitados, salvo la vida, “un derecho ilimitado sería antisocial por ello su necesidad de hacerlo compatible con el derecho de los demás dentro de la comunidad y con los intereses superiores de esta última” (2016)³⁴.

El titular es una persona física determinada o determinable aunque alguna legislación, como la uruguaya, lo extiende a la persona jurídica “en cuanto corresponda”, lo que se fundamenta en que ella cuenta con una imagen propia en el sector de su actividad, con un valor que se proyecta sobre sus actividades y sus propios bienes o, que en su caso, se le reconoce la titularidad de derechos que sirven instrumentalmente a la intimidad de sus

31 Esa disposición legal agrega que “está comprendido en el art. 72 de la Constitución”, el cual recibe la esencia humanista del jusnaturalismo liberal a través de los principios generales de derecho, los cuales configuran un bloque de juridicidad con la normativa constitucional y el Derecho internacional de los Derechos Humanos.

32 El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo cit., en su Primer “Considerando” expresa que “La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental”; tiene en cuenta textos jurídicos como la Carta de los Derechos fundamentales, art. 8 ap. 1 y el Tratado de Funcionamiento de la UE, art. 16 ap. 1

33 Sentencia del Tribunal Constitucional español 292/000, de 30-XI. Expresa que el derecho alcanza “a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros puede afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual (...), sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos, que, por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos (...)”.

34 Entre otras, sentencias N° 312/995, 220/002, 54/004, 564/012, 697/014, 79/016, esta última de 5-IV-2016. En igual sentido, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo cit., en su Cuarto “Considerando” afirma que este derecho “debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos, con arreglo al principio de proporcionalidad (...)”.

integrantes o que están directamente conectados con esta³⁵.

El sujeto obligado, "responsable de la base de datos o del tratamiento" puede ser una persona física o jurídica, pública o privada "propietaria de la base o quien decida sobre finalidad, contenido y uso del tratamiento" (ley citada, art. 4 "K"), por lo que está comprendida la Administración a través de las diversas personas jurídicas estatales que ejercen función administrativa.

El ámbito subjetivo no tiene, pues, exclusiones en lo que atañe al titular de la información, al responsable ni al encargado del tratamiento.

Por su parte, el tratamiento de los datos personales se define como "operaciones y procedimientos sistemáticos, de carácter automatizado o no, que permiten el procesamiento de datos personales, así como también su cesión a terceros mediante comunicaciones, consultas, interconexiones o transferencias" (ley citada, art. 4 "M").

4.3. Principios

A continuación, se mencionan algunos de los que rigen en la materia, reglas que explicitan valores superiores y contribuyen a dar coherencia y permanencia al ordenamiento, sobre todo ante los incesantes cambios tecnológicos. Los principios están interrelacionados, se sustentan en el de juridicidad y contribuyen para la interpretación e integración de la normativa:

- A. Veracidad, según el cual los datos deben ser veraces, adecuados, ecuanímenes y no excesivos en relación con la finalidad ("*minimización*"); además no podrán obtenerse por medios desleales, fraudulentos, abusivos o, extorsivos.

Este principio pone en juego criterios de proporcionalidad y, por tanto, juicios de idoneidad, necesidad y ponderación.

- B. Finalidad, que impone fines precisos y la coherencia en el tratamiento de datos con relación a los que dan mérito a su obtención; asimismo su eliminación cuando no sean necesarios o pertinentes a los fines para los cuales hubieren sido recolectados, por lo que abarca la regla de la limitación temporal sin perjuicio de casos de excepción por razones históricas, estadísticas o científicas y, en la medida de lo posible, disociados.

Impone, pues la especificación relativa a los fines de los tratamientos, lo que se relaciona con el principio especialidad que delimita las competencias de los órganos públicos ya que ellos no se rigen por el principio de libertad, solo pueden desarrollar los cometidos que el ordenamiento les asigna.

En cuanto a la disociación, es clave que impida vincular a persona determinada o determinable, sin posible reidentificación; puede efectuarse mediante anonimización. Y en todo caso exige controles periódicos determinados por el responsable de la respectiva base, ante la aparición de nuevas tecnologías y de métodos para prevenir y evitar los posibles riesgos de reidentificación.

- C. Consentimiento informado: previo a todo tratamiento de datos o a su comunicación,

35 La ley uruguaya N° 18.331 vigente (arts. 3 'A', 9 'A' y 22) contiene normas que no se aplican a la persona jurídica, así respecto al límite del registro por un plazo determinado de datos relativos a obligaciones de carácter comercial; se las excluye de la titularidad de bases destinadas a exclusivo uso personal o doméstico y de la exigencia del previo consentimiento informado respecto del tratamiento del dato de su teléfono.

que exige una declaración o acción afirmativa clara del titular del dato (Reglamento (UE) 2016/679 del Parlamento)³⁶.

Debe ser informado para que este titular conozca inequívocamente la finalidad a la que se destinarán los datos y el tipo de actividad del responsable, mediante un medio sencillo y claro; esto es especialmente relevante en el caso de datos sensibles como los de salud, de origen racial o étnico, opiniones políticas, biométricos, etc.

El vínculo entre los principios es evidente, así entre el de finalidad y el del consentimiento; y ellos cobran vigor en el Big Data.

En efecto:

“Una de las características de algunos tratamientos masivos de datos consiste, en la reutilización de datos que inicialmente habían sido recogidos para otra finalidad, o bien con una legitimación diferente. Pensemos en los casos en que se tratan datos personales que son necesarios para la ejecución de un contrato, en sentido estricto, y luego son reutilizados por el responsable de tratamiento para otros fines como, por ejemplo, en el caso de los pagos efectuados mediante tarjeta de crédito. En el caso de que el emisor de la tarjeta considerase efectuar un tratamiento adicional para, digamos, ofrecer a sus clientes sus propios productos financieros, puede entenderse que se trata de una finalidad conexa y compatible con la original. Sin embargo, una reutilización consistente en cruzar la información detallada de las compras efectuadas, con el fin de elaborar perfiles de consumo para luego ser ofertados a terceros resulta ajena a la relación contractual inicial. Esto constituye una desviación de la finalidad, para la cual se necesitaría una nueva legitimación en base al consentimiento” (González, 2017)³⁷.

Es posible un fundamento diverso al consentimiento para el tratamiento de datos, así si este tiene como base el interés legítimo o razones de interés general autorizadas por ley, o si el organismo solicitante tiene mandato legal para hacerlo^{38/39}.

36 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo cit., art. 4 numeral 11 y Estándares de la Red Iberoamericana de Protección de Datos Personales de 20-VI-2017, art. 12.1.

37 González, Pedro Alberto. Responsabilidad proactiva en los tratamientos masivos de datos. Revista Internacional de Éticas aplicadas. N° 24-2017, pp. 115 y ss. <https://www.dilemata.net/revista/index.php/dilemata/article/view/412000103>

38 La ley uruguaya prevé excepciones al consentimiento, así para el ejercicio de funciones propias de los Poderes públicos, cumplir una obligación legal y comunicar datos personales relativos a la salud, si esto es necesario “por razones sanitarias, de emergencia o para la realización de estudios epidemiológicos, preservando la identidad de los titulares mediante mecanismos de disociación adecuados, cuando ello sea pertinente”, ley N° 18.331, art. 17 inc. 3° ‘C’, texto dado por ley N° 18.719 de 27-XII-2010, art. 153. El art. 19 prevé que “Los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquéllos, respetando los principios del secreto profesional, la normativa específica y lo establecido en la presente ley”.

39 También hay situaciones, “particularmente en el contexto de la acción humanitaria”, en las que “obtener el consentimiento puede ser muy difícil, y, por ende, puede ser necesario y legítimo recurrir a otro fundamento jurídico, como el interés público o los intereses vitales del titular de datos. La posibilidad de basarse en motivos de interés público es particularmente

- D. Seguridad que comprende aspectos físicos, lógicos y jurídicos lo que se relaciona con la gestión de la información, determinación de los activos de que se dispone y de los niveles de riesgos, así como la formación del personal de la organización. En caso de violación a la seguridad de la base, su responsable debe comunicarlo a quienes pueden verse afectados y al órgano garante en cierto plazo⁴⁰.
- E. Reserva, de acuerdo con el cual *“las personas físicas o jurídicas que obtuvieren legítimamente información proveniente de una base de datos que les brinde tratamiento”,* deben utilizarla *“en forma reservada y exclusivamente para las operaciones habituales de su giro o actividad”*.

Prohíbe toda difusión de la información a terceros, y quienes trabajen para el responsable en cualquier relación jurídica, están sujetos a secreto profesional.

- F. Responsabilidad, por toda violación de la normativa lo que es propio de un Estado de Derecho y se proyecta en diversas áreas, básicamente administrativa, civil y penal.

En interrelación con otros principios, se enfatiza una responsabilidad proactiva que configura la accountability. Ella se dirige a asegurar el debido cumplimiento de la normativa y a implementar medidas para acreditarlo: registro de actividades, auditorías, evaluaciones de impacto, adopción de la privacidad por diseño desde el inicio del sistema de información, sin que disminuya su funcionalidad.

La referida privacidad impone que sea por defecto en el sentido de configurar a los sistemas de modo que, por defecto, brinden mayor protección a la privacidad a fin de no compartir información del usuario, salvo acción de este que altere la configuración; la funcionalidad que integra y garantiza seguridad y privacidad; la protección durante todo el ciclo de vida de los datos, incluyendo su supresión o eliminación, sin perjuicio de los lapsos de retención lícitos.

Se añade la transparencia en tanto el responsable de la base debe informar los términos de uso desde un principio y no modificarlos sin el previo consentimiento del titular de los datos, así como someterse a una verificación adecuada⁴¹.

relevante para organizaciones humanitarias que, debido a la naturaleza de sus actividades y las situaciones de emergencia en la que generalmente operan, tienen mayores dificultades para obtener consentimiento (...) Esto puede ser el caso, por ejemplo, cuando el tratamiento de datos personales es un prerrequisito para recibir asistencia, o cuando se requieran recopilar los datos de una persona desaparecida”, Informe del Comité Jurídico Interamericano Principios Actualizados sobre la Privacidad y la Protección de Datos Personales con Anotaciones. 98° Periodo Ordinario de Sesiones 5-9 abril de 2021 (OEA/Ser.Q CJI/doc. 638/21- 8abril2021). Principio Dos: Transparencia y Consentimiento.

- 40 En el Uruguay, por ley N° 19.670 de 15-X-2018 art. 38 y decreto N° 64/020, arts. 3 y 4, la comunicación referida debe hacerse en plazo máximo de 72 horas de conocida la vulneración. Se dispone también que *“Constatada la existencia de incidentes de seguridad que ocasionen, entre otras, la divulgación, destrucción, pérdida o alteración accidental o ilícita de datos personales, o la comunicación o acceso no autorizados a dichos datos, los responsables o encargados de tratamiento deberán iniciar los procedimientos previstos necesarios para minimizar el impacto de dichos incidentes dentro de las primeras 24 horas de constatados”*.

- 41 V. Brian Nougères, Ana. La protección inteligente de los datos personales: privacy by design (PbD). Revista Internacional de Protección de Datos Personales. N° 1 - Universidad de los Andes. Bogotá 2012. Concluye que *“El concepto de Privacy by Design constituye una teoría para implementar los principios de la protección de datos personales de una forma integral, con una visión holística, que los incorpora con la concepción del negocio y de los sistemas de información”*.

Se ha agregado la actualización o rediseño, basado en “repensar, rediseñar y revivir”, o sea rever las estrategias de mitigación de riesgos y sistemas para una mayor protección a la privacidad, minimizando los datos recabados, reexaminando y limitando sus periodos de retención y siempre que sean estrictamente necesarios para la respectiva finalidad, reforzando la seguridad, etc.

En cuanto a la evaluación de impacto, se impone si el tratamiento refiere a un importante número de datos personales, lo que ha sido establecido por diversa normativa, entre ella el Reglamento Europeo ya citado⁴² y reciente legislación uruguaya^{43/44}.

5. ANOTACIONES FINALES

- i) La Administración debe ser instrumento del interés general y, para ello, cumplir las reglas de Derecho, siendo idónea en cuanto al resultado debido (eficaz) y propiamente eficiente respecto a la actividad y medios utilizados, que estos sean adecuados cualitativa y cuantitativamente. Ello en la sustancia de las medidas y en su motivación o justificación.
- ii) Las TIC contribuyen a la “eficacia eficiente”⁴⁵ e inciden en la configuración de un Derecho administrativo de la información, aggiornado, centrado en la persona y sus derechos fundamentales.

42 Art. 35 apartado 1: “Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares de los datos vinculados a la comisión de infracciones penales, civiles o administrativas”.

43 La evaluación de impacto se incluye como una medida de la responsabilidad proactiva según ley N° 19.670 ya citada, art. 39 y decreto 64/020; el art. 6 de este dispone que “En forma previa al inicio del tratamiento, el responsable y el encargado del tratamiento en su caso, deberán realizar una evaluación de impacto en la protección de datos personales, cuando en las operaciones de tratamiento pueda: a) Utilizarse datos sensibles como negocio principal. b) Proyectarse un tratamiento permanente o estable de los datos especialmente protegidos (...) o de los datos vinculados a la comisión de infracciones penales, civiles o administrativas; c) Implicar una evaluación de aspectos personales de los titulares con el fin de crear o utilizar perfiles personales, en particular mediante el análisis o la predicción de aspectos referidos a su rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad de comportamiento y solvencia financiera y localización. d) Llevarse a cabo el tratamiento de datos de grupos de personas en situación de especial vulnerabilidad y, en particular, de menores de edad o personas con discapacidad. e) Producirse un tratamiento de grandes volúmenes de datos personales. f) Transferirse datos personales a otros Estados u organizaciones internacionales respecto de los que no exista nivel adecuado de protección) Otros que determine la Unidad Reguladora y de Control de Datos Personales”.

44 La Unidad Reguladora y de Control de Datos de Uruguay conjuntamente con la Agencia de Acceso a la Información Pública de la Argentina emitieron un Guía de Evaluación de Impacto en Protección de datos. V. <https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/publicaciones/guia-evaluacion-impacto-proteccion-datos>.

45 Parejo Alfonso, Luciano. Perspectivas del Derecho Administrativo para el próximo milenio. Parte IV La eficacia administrativa y la calidad total de los servicios públicos. Ed. Jurídicas Gustavo Ibáñez. Bogotá 1998, p. 89 y ss. Expresa que “(...) la eficacia engloba necesariamente la eficiencia y economía en la ejecución del gasto encomendado a la administración”, “la eficacia reclamada por la Constitución” (española), es una eficacia eficiente”.

Los datos que posee la Administración son un activo en la medida que sean exactos, oportunos, auditables y trazables.

Tanto en su creación como en su aplicación, los procedimientos deben brindar confianza a los habitantes, enfatizando en la seguridad del procesamiento y análisis de los datos masivos y, en general, en el respeto de los derechos, entre ellos el de protección de los datos personales.

Solo así las herramientas tecnológicas contribuyen realmente a crear valor público.

- iii) El referido uso responsable involucra dimensiones de índole ética, jurídica, técnica y social que permitan una transformación digital que habilite, legítimamente, anticiparse a las necesidades de las personas y prevenir situaciones problemáticas.

Para ello son aplicables los principios de responsabilidad proactiva, con “responsable” claramente identificable; transparencia, que lleve a poner a disposición los datos utilizados y los algoritmos, siendo estos neutrales y auditables; seguridad, para la cual se enfatiza en controles permanentes y en la privacidad por diseño.

- iv) Las personas no son un (mero) conjunto de enorme cantidad de datos y, por otro lado, importa que sean ellas quienes ejerzan efectivamente la autoridad pública necesaria en la comunidad y no que las decisiones provengan de algoritmos, en una especie de *gobierno* desarrollado por los datos.

“El marco regulatorio debe adaptarse igualmente a los nuevos apremios. Además de confianza, los ciudadanos reclaman seguridad en la utilización de las nuevas tecnologías. Las soluciones jurídicas deben ser integrales, contemplando todos los elementos afectados, y garantizando la regularidad y la eficacia de los procesos”. (Sánchez Bravo, 2007, p.83).

6. BIBLIOGRAFÍA

Agencia para el Desarrollo del Gobierno de Gestión Electrónico y la Sociedad de la Información (AGESIC). (2019). *Estrategia de Inteligencia Artificial para el Gobierno Digital*. <http://www.fic.edu.uy/sites/default/files/2019-10/estrategia%20de%20inteligencia%20artificial.pdf>

Balbín, C. (2008). *Curso de Derecho Administrativo*.

Bandeira de Mello, C. (2010). *Grandes temas de Direito Administrativo*. Malheiro.

Brian, A. (2012). La protección inteligente de los datos personales: privacy by design (PbD). *Revista Internacional de Protección de Datos Personales y Acceso a la información*, (1), 4-15.

Centro Latinoamericano de Administración para el Desarrollo. (2007). *Carta Iberoamericana de Gobierno Electrónico*.

Delpiazzo, C. (2010). Noción y regulación del procedimiento y del acto administrativo electrónico. *Estudios de Derecho Administrativo*, (1).

Delpiazzo, C. (2020). Impacto de las TIC en el Derecho Administrativo. En C. Vázquez, *Impacto de las Nuevas Tecnologías en el Derecho Administrativo* (pp. 17-36).

Montevideo: Fundación de Cultura Universitaria.

- Ferrajoli, L. (2011). *Principia iuris. Teoría del derecho y de la democracia*. Trotta.
- González, P. (2017). Responsabilidad proactiva en los tratamientos masivos de datos. *Revista Internacional de Éticas aplicadas*, (24), 115- 129. <https://www.dilemata.net/revista/index.php/dilemata/article/view/412000103>
- Justen Filho, M. (2006). *Curso de Direito Administrativo*. 2ª edición. Saraiva.
- Parejo, L. (1998). *Perspectivas del Derecho Administrativo para el próximo milenio*. Ed. Jurídicas Gustavo Ibáñez.
- Parlamento y Consejo Europeo. (27 de abril de 2016). Reglamento UE 2016/679.
- Pezzutti, M. (2020). Los actos administrativos electrónicos. MDEO.
- Prats, J. (2005). *De la Burocracia al "management", del "management" a la gobernanza. Las transformaciones de las Administraciones Públicas de nuestro tiempo*. INAP.
- Red Iberoamericana de Protección de Datos. (2019). *Recomendaciones generales para el Tratamiento de Datos en la Inteligencia Artificial aprobadas por la Red Iberoamericana de Protección de Datos. XVII Encuentro*.
- Rivero, R. (2008). *El Expediente Administrativo. De los Legajos a los Soportes Electrónicos*. Thomson Aranzadi.
- Rotondo, F. (2015). Derechos fundamentales y Derecho administrativo. *Revista de Derecho Público*, Año 24, (47), 87-102.
- Saarenpää, A. (2019). Protección de datos: lo excepcional llega a ser lo natural. *Revista de Derecho y Nuevas Tecnologías*, (1), 105-140.
- Sánchez, A. (2007). *La Administración Electrónica en España*. *Revista do direito*, (28), 83-111.
- Smith, B. y Shum, H. (2018). Prólogo. En Microsoft, *El futuro computarizado. La Inteligencia Artificial y su rol en la sociedad*.
- Tribunal Constitucional de Colombia. (18 de agosto de 2010). Sentencia C-640/10.
- Viega, M. (2013). Procedimiento administrativo electrónico. Presentación realizada en las VIII Jornadas del Tribunal de lo Contencioso Administrativo. MDEO.