UNIVERSIDAD Panamericana

RATIO DECIDENDI

2024 | ISSN 3061-760X

Acerca de las etapas del constitucionalismo y de las generaciones de derechos humanos y de las leyes de protección de datos

About the stages of constitutionalism and the generations of human rights and data protection laws

Óscar R. Puccinelli

Óscar R. Puccinelli

Cámara de Apelaciones en lo Civil y Comercial de Rosario, Argentina
Pontificia Universidad Católica Argentina
oscarpuccinelli@gmail.com
https://orcid.org/0000-0002-7978-7111

Recibido: 14 - 05 - 2024
Aceptado: 31 - 05 - 2024
Publicado en línea: 13 - 07 - 2024

Cómo citar este texto

Puccinelli, Ó. R. (2024). Acerca de las etapas del constitucionalismo y de las generaciones de derechos humanos y de las leyes de protección de datos. *Ratio Decidendi*, año 1, n. 1, 1-29. https://doi.org/10.21555/rd.2024.3155

Resumen

Las revoluciones independentistas e industriales, las guerras mundiales, la carrera espacial y las dos guerras frías, entre otros fenómenos, han tenido un alto impacto en distintos ámbitos y de hecho constituyeron hitos que sirvieron de bisagras para definir etapas en el constitucionalismo y en los derechos humanos. En la evolución de la protección de éstos, nos centramos en la gestación y desarrollo de uno que está estrechamente vinculado a las tecnologías de la información y de la comunicación (TICs) y que surgió como respuesta ante los avances sobre los derechos de las personas –en especial pero no exclusivamente sobre la intimidad- por parte de quienes tratan información personal: el "derecho a la protección de datos" (inicialmente rotulado "derecho a la autodeterminación informativa, que actualmente aporta una cantidad ingente de contenidos a los "derechos digitales"), refiriendo a las principales normativas gestadas en sus cinco generaciones, desplegadas entre 1970 y la actualidad.

Palabras clave: Constitucionalismo, Derechos humanos, TICs, Derechos digitales, Protección de datos, Autodeterminación informativa, Privacidad, Internet, Redes sociales, *Habeas data*, Inteligencia Artificial, Neuroderechos.

Abstract

The independence and industrial revolutions, the two World Wars, the space race, and the two Cold Wars, among other phenomena, have had a significant impact across various domains. In fact, they constituted pivotal milestones that defined stages in constitutionalism and human rights. In the evolution of protecting these rights, our focus centers on the genesis and development of one closely linked to Information and Communication Technologies (ICTs), that emerged in response to advances concerning personal rights—especially but not exclusively privacy—by those handling personal information: the "right to data protection" (initially labeled the "right to informational self-determination," which currently contributes a wealth of content to "digital rights"), referring to key regulations developed across its five generations, spanning from 1970 to the present.

Keywords: Constitutionalism, Human rights, ICTs, Digital rights, Data protection, Informational self-determination, Privacy, Internet, Social networks, *Habeas data*, Artificial Intelligence, Neurorights.

Contenido

1. Introducción: Las revoluciones políticas e industriales, el constitucionalismo y las generaciones de los derechos humanos

1.1. El desarrollo de las TICs y la generación de nuevos derechos

El paso entre las cinco revoluciones industriales estuvo principalmente marcado por el ritmo en que fueron incorporándose los recursos naturales y tecnológicos a los procesos productivos, en un tránsito que fue más lento entre las tres primeras (que se medían de siglo en siglo), y que se aceleró en las dos últimas (entre las cuales apenas transcurrieron unas décadas) debido especialmente a la migración de los medios de generación de capital del sector industrial al de los servicios, fenómeno especialmente provocado por el vertiginoso desarrollo habido en el ámbito de las tecnologías de la información y de la comunicación (TICs), en cierta medida acelerado por exigencias propias de la carrera espacial y de la primer guerra fría[1].

En efecto, durante el último tercio del siglo XX y lo que va de este siglo, las TICs —entre otras tecnologías habidas en otros ámbitos, como el sanitario— han provocado cambios altamente disruptivos que a la par de favorecer el desarrollo económico y social, trajeron efectos no deseados sobre los derechos de las personas, situación que puso sobre el tapete cada vez con más intensidad la insuficiencia de las reglas constitucionales y, más particularmente, las de los icónicos instrumentos internacionales de derechos humanos adoptados a mediados de siglo pasado en los ámbitos globales y regionales (Declaraciones universal y americana de Derechos Humanos, Convenio europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales) e incluso de los convenios "insignia" creados ya avanzada la década de los años 1960 (los Pactos internacionales de Derechos Civiles y Políticos y de Derechos Económicos, Sociales y Culturales, en el ámbito de la ONU y la Convención Americana sobre Derechos Humanos, en el ámbito de la OEA).

El vertiginoso avance ocurrido en las TICs tendrá un destacadísimo emergente precisamente en diciembre de 1969, cuando –escasos meses después de aprobada la citada Convención Americana-, se interconectaron los nodos de la Universidad de California en Los Ángeles y Santa Bárbara, el Stanford Research Institute y la University of Utah, dando origen a Arpanet, el antecedente inmediato de Internet-, hecho que, entre otros típicos del ingreso a la era informática, dio el puntapié inicial a una gradual pero incesante reconfiguración de los derechos y principios preexistentes, así como un creciente reconocimiento de otros nuevos.

Este efecto de los avances en las TICs en el derecho no fue estrictamente una novedad. Su antecedente más relevante puede encontrarse sobre finales del siglo XIX cuando muchos

1 En rigor no hay consenso generalizado en que ya esté plenamente configurada la quinta, pero sí en cuanto a la existencia, hasta el presente, de cuatro revoluciones industriales: a) la primera, iniciada alrededor de 1765, a partir del uso del carbón reemplazando la fuerza humana, momento en que se pasó de una economía rural basada fundamentalmente en la agricultura y el comercio a una urbana, industrializada y mecanizada; b) la segunda, configurada alrededor de 1870, con la incorporación del gas y la electricidad, del petróleo y del acero a los procesos productivos, y con la aparición de nuevos medios de comunicación y de transporte: c) la tercera, ubicada simbólicamente a partir de 1969 –coincidentemente con la llegada del hombre a la luna y la aparición de Arpanet-, se dará con la incorporación de la electrónica, la energía nuclear, una mayor utilización de las energías renovables y formas de almacenamiento de energía, el desarrollo de redes eléctricas inteligentes, vehículos eléctricos e híbridos; d) la cuarta, iniciada alrededor de 2000, con la incorporación de Internet y las tecnologías inteligentes de automatización a los procesos productivos, la robótica, la inteligencia artificial, la cadena de bloques, la nanotecnología, la computación cuántica, la biotecnología, la internet de las cosas y los vehículos autónomos, y e) la quinta –como se dijo, comenzando- estaría caracterizada por la presencia de industrias de valor centradas en la persona y en la colaboración ser humano-máquina, la digitalización total de las empresas, la interconexión eficaz entre procesos, sistemas y máquinas, y en una mayor focalización en un ambiente sostenible.

periódicos empezaron a radicalizar sus noticias en pos de ganar suscriptores frente a sus competidores y en ese contexto vieron en la incorporación de nuevas tecnologías a los procesos editoriales (la prensa rotativa, el teléfono y la fotografía) la posibilidad de dar un importante giro en sus modelos de negocios, ampliando el rol tradicional de la prensa que le valió considerarla como el "cuarto poder" (esto es, como medio de control social de los actos de gobierno) al de entretener, casi sin tapujos, con informaciones sobre asuntos privados carentes de interés público, dando origen así a la denominada "prensa amarillista"[2].

En tal nuevo contexto, y en ausencia de normas específicas para enfrentar las afecciones del ejercicio abusivo y despiadado de una libertad privilegiada como la de prensa, la respuesta se edificó a partir del principio del derecho inglés -expuesto por William Pitt en 1763 en un célebre discurso ante el parlamento británico- que concebía a la morada como un espacio inexpugnable[3], el que fue en definitiva redefinido un siglo más tarde y ya en tierras americanas por Cooley como el derecho a "ser dejado solo"[4] y muy poco después reconfigurado como "*the right to privacy*" (el derecho a la privacidad) en el famoso opúsculo de Warren y Brandeis publicado en 1890 por la Harvard Review, donde ese derecho a ser dejado solo, frente a los avances despiadados de la prensa sobre la privacidad, se entendió primordialmente como la facultad de exclusión de terceros respecto de determinadas facetas de la vida personal (Warren y Brandeis, 1890).

1.2. Las etapas del constitucionalismo y las generaciones de derechos humanos

La evolución de los derechos humanos (en gran medida impulsada por las revoluciones políticas e industriales y por las consecuencias de las dos grandes conflagraciones bélicas mundiales) suele ser dividida en cuatro —y hasta cinco— generaciones, a las que usualmente se las hace coincidir con las distintas etapas del constitucionalismo[5].

La primera generación, desplegada en tiempos del "preconstitucionalismo" inglés del siglo XVII, trajo consigo la aprobación de diversos y relevantes documentos como el Bill of Rights de 1689 y el reconocimiento de dos principios básicos que abrían paso a la monarquía

2 "Periodismo amarillo" (*yellow journalism*), es un término generado por el periódico New York Press que alude a la batalla periodística entre los periódicos neoyorkinos The New York World de Józef Pulitzer (pionero del Infotainment) y el New York Journal de Willliam Hearst, y que diera vida en ambos periódicos a historietas con el personaje The yellow kid, representado vestido de color amarillo, aunque el término no refiere en realidad a ese color puesto que *yellow* en inglés, significa también cruel y cobarde, que es precisamente el sentido de la alocución.

3 William Pitt sostuvo en tal ocasión la máxima del common law que proclama a la casa del hombre como su castillo (a man's house as his castle), reivindicando la protección personal del individuo frente al poder del Monarca incluso en la más humilde morada. Afirmó allí que "El hombre más pobre, en su cabaña, desafía todas las fuerzas de la Corona. [Su cabaña] puede ser frágil, su techo tal vez es inestable, el viento se cuela por él, la tempestad lo penetra, no impide el paso de la lluvia, pero el Rey de Inglaterra no puede entrar en ella; ni con todo su poder se atreve a cruzar el umbral de esa ruinosa morada" (Pitt, 1806-1820, vol. 15 (1753-1765), pág. 1307).

4 En 1873 Thomas MacIntyre Cooley - profesor de derecho constitucional y miembro de la Corte Suprema de Michigan- en su obra "The Elements of Torts" formuló su conocido "*right to be let alone*", aludiendo al derecho a ser dejado solo o de no ser perturbado o molestado por injerencias externas no deseadas, concepto que desarrolló en el fallo "Brents vs. Morgan", concibiéndolo como el derecho que tiene cada persona de no ser objeto de una publicidad ilegal; el derecho de vivir sin interferencias ilegales del público en lo concerniente a asuntos en los cuales ese público no tiene un interés legítimo".

5 Se denomina "constitucionalismo" al movimiento iniciado con ciertos antecedentes inmediatos en el siglo XVII pero desplegado a partir del siglo XVIII, que se caracteriza por su objetivo primordial de racionalizar el poder político a través de la adopción de un documento legal (la constitución) escrito, único y orgánico, con supremacía jurídica sobre el resto de las normas y basado en la división de poderes y el reconocimiento de derechos personales.

constitucional: el del *rule of law* (imperio de la ley o Estado de derecho) y el de la soberanía del Parlamento (que quedaba así a la par del poder Real).

La segunda, denominada del "constitucionalismo individualista y liberal" (forjada a partir de las revoluciones inglesa, estadounidense y francesa) comienza la "era de las constituciones escritas" y se caracteriza por el reconocimiento expreso de los derechos civiles y políticos en el marco de un orden económico individualista y liberal (la Constitución de Virginia de 1776, la Constitución norteamericana de 1987 y sus primeras enmiendas, la Declaración de Derechos del Hombre y del Ciudadano de 1789, etc.).

La tercera, del "constitucionalismo social" o del "estado social de derecho" se manifiesta a partir de la segunda década del siglo XX como consecuencia tanto de la Primera Guerra Mundial como de la Revolución Industrial, hechos que minaron las bases del sistema económico liberal, llevando a poner en crisis sus idearios de libertad, igualdad y justicia y a tornar ilusoria la bandera de "fraternidad", eje central de la revolución francesa. En ese contexto se instaló sobre el tapete la "cuestión social" en pos de lograr, entre otros objetivos, una igualdad sustancial, un trato digno de los trabajadores, la solidaridad como deber y el reconocimiento de la función social de la propiedad, provocando la aparición del "constitucionalismo neoliberal—social" (constituciones de Querétaro de 1917 y de Weimar de 1919), del "constitucionalismo marxista" (constitución de la República Socialista Federativa de los Soviets de Rusia de 1918) y del "constitucionalismo corporativo" (regímenes de Mussolini, Oliveira Salazar y Franco).

La cuarta generación, rotulada del "constitucionalismo internacional", se iniciará a partir de la finalización de la Segunda Guerra mundial, y se caracterizará por la aparición de organismos internacionales y regionales con la consecuente atenuación del principio de soberanía a partir del reconocimiento de la jurisdicción supranacional; la incorporación del Derecho Internacional de los Derechos Humanos a las constituciones nacionales –con diferentes recetas—; la consagración tanto de nuevos derechos individuales (a la imagen, a la voz, etc.), como de los sectoriales y colectivos (los del consumidor y del usuario, al ambiente, etc.) e incluso de otros mixtos (el derecho de acceso a la información), y el reconocimiento de órganos de control locales que dieron una nueva fisonomía al *check and balances* puro pergeñado en el siglo XVIII (como el defensor del pueblo y los consejos de la magistratura).

Así, a partir de las emblemáticas declaraciones de derechos humanos que fueron aprobadas por las Asambleas Generales de la ONU y de la OEA en 1948, se fueron dictando diversos instrumentos convencionales que esencialmente reconocieron un listado más o menos extenso y detallado de derechos –lo cual de por sí constituye un primer medio de protección–, y además, especialmente en el caso de las convenciones regionales, por un lado, cargaron a los Estados parte con una serie de deberes que tienden tanto a promover esos derechos como a establecer mecanismos internos efectivos para su tutela[6], y por el otro, crearon medios supranacionales de protección que, a partir de la intervención de órganos especializados, se constituyeron en verdaderas garantías específicas que funcionan cuando, ante la ausencia o insuficiencia de los mecanismos internos, se falla en la mentada misión protectora, y se lesionan derechos contenidos en tales instrumentos[7].

6 V.gr., arts. 2, 7 y 25 de la Convención Americana sobre Derechos Humanos (CADH).

7 Un claro ejemplo de estos órganos, al que luego referiremos en detalle, se puede encontrar en la Convención Americana sobre Derechos Humanos (CADH), a través de cuyo articulado se creó, por un lado, a la Comisión Interamericana de Derechos Humanos (CIDH), que cumple un rol particular, preventivo y conciliador, y sólo excepcionalmente –en principio, luego de agotados los medios de que dispone– disparador de roles contenciosos, y por el otro, a la Corte Interamericana de Derechos Humanos (Corte IDH), cuyas principales funciones son las de evacuar opiniones consultivas solicitadas por cualquier Estado parte, y dictar sentencias sobre casos contenciosos de violaciones de derechos humanos sometidos a su juzgamiento por la Comisión.

Finalmente, y si bien resultaría discutible aludir a una nueva etapa del constitucionalismo pues no se advierten cambios políticos estructurales, puede reconocerse desde las postrimerías del siglo pasado y principios de este siglo una quinta generación de los derechos que parten de una suerte de "revolución digital" generadora de los consecuentes "derechos humanos digitales" tendientes a afrontar las consecuencias –positivas y negativas— de tal revolución. Se trataría así, del "constitucionalismo de la 5ª Revolución Industrial", donde los avances tecnológicos arrolladora y exponencialmente habidos hasta el presente han ido generando diferentes respuestas en pos de resguardar los derechos individuales, sectoriales y colectivos afectados especialmente por el impacto de las nuevas tecnologías de la información y de la comunicación, pero intentando promover la libre circulación de la información debidamente tratada.

Es en este último contexto donde se desarrollará el presente trabajo, por el cual se pretende mostrar esa evolución y los principales principios y derechos "técnicos" surgidos en el ámbito del derecho de la protección de datos (personales) al calor de la innovación tecnológica.

2. Los derechos "de" y "a" la protección de datos.

Luego de una prolongada evolución conceptual que lo considerara como parte del derecho a la privacidad, el recientemente rotulado "derecho a la protección de datos" (al que también se llamó "libertad informática", "intimidad informática", "derecho a la autodeterminación informativa", "derecho a la autodeterminación informática", y *hábeas data*), se ha escindido y consolidado conceptualmente, generando una importante cantidad de principios y derechos específicos que son incesantemente formulados y reformulados al calor de dichos avances tecnológicos.

Si bien se insinuó desde antes, la denominación "derecho a la protección de datos" se comenzó a adoptar homogéneamente a partir de 2000, con la Carta de los Derechos Fundamentales de la Unión Europea —un documento adoptado en Niza en el que se recogen todos los derechos civiles, políticos, jurídicos, sociales y económicos de los ciudadanos europeos—, cuyo art. 8 fue el primero en reconocer expresamente este derecho, con carácter autónomo y con tal rótulo, escindiéndolo del derecho a la privacidad, regulado en el artículo anterior.

Por decirlo de una manera simple, este novel derecho refleja, por un lado, la facultad con que cuenta toda persona para actuar *per se* y para exigir la actuación del Estado a fin de tutelar los diversos derechos que pudieran verse afectados en virtud del tratamiento indebido de los datos de carácter personal que le conciernen, y por el otro, el derecho a que el Estado –y hoy más que nunca, la comunidad internacional- establezcan marcos regulatorios integrales en los cuales se fijen las pautas esenciales para el debido tratamiento de tales datos y a la par se diseñen mecanismos específicos para su tutela tanto judicial como administrativa.

Ahora bien: pese a que el objeto de este derecho aparece desde una perspectiva lexical limitado a la protección de los datos en sí, en realidad su fin último es la tutela de otros y muy variados bienes jurídicos (la intimidad, el honor, la autodeterminación, la dignidad, la propiedad, etc.), razón por la cual se trata de un derecho de carácter "medial" que no se sustenta por sí mismo ya que desaparecería si no existiesen los derechos que procura resguardar —como ocurre con las garantías (por ejemplo, el amparo y el hábeas corpus), aunque no debe confundirse con éstas pues no alcanza a reunir sus notas típicas[8]—.

8 Muchos de los denominados "derechos" que poseen tal carácter instrumental son en realidad garantías, en virtud de constituir en sí el medio técnico de tutela de ciertos derechos para cuya protección han sido creados (v.gr., el "derecho de réplica" y el "derecho de huelga"). En este caso, el derecho a la protección de datos contiene reglas de fondo propias y es tutelable a través de ciertas garantías específicamente creadas para ello (v.gr., institucionales, como la Comisión Nacional de Informática y Libertades francesa, o procesales, como el habeas data brasileño).

En este sentido, resulta clarificador lo señalado por Bidart Campos:

> Dentro del ámbito tutelar de los derechos personales, y en afinidad con las garantías clásicas frente al Estado, hay "derechos" denominados tales que, en rigor, sirven y se usan para la defensa de otros derechos; a aquellos denominados derechos que se dirigen a proteger otros derechos se les asigna la categoría y naturaleza de garantías.
>
> [...] Por otro lado, también interesa captar que hay en el rubro clásico de los derechos, algunos llamados tales y definidos como tales que, por servir para defensa y tutela de otros derechos, exhiben un rostro garantizador y una semejanza con las garantías personales.
>
> En este último caso –ejemplo de los derechos de huelga y de réplica–, sugerimos una alternativa: a) o decir que son realmente derechos cuyo ejercicio ampara a derechos distintos, con lo que entre los derechos habría que computar una categoría enderezada a no agotar un derecho en su propio ejercicio sino a verlo como instrumento "garantizador" de otro u otros derechos; b) o decir que no son realmente derechos aunque así se los apode y se los incluya en el rubro de los derechos, sino que son verdaderas garantías en cuanto mecanismos protectores de derechos" (Bidart Campos, 1991).

Puede así hoy aludirse a los derechos *a* y *de* la protección de datos –el primero, como facultad de tutela concedida a las personas afectadas por los tratamientos ilegales o ilegítimos de sus datos y el segundo, como nueva rama del derecho con contenidos específicos– que tienen por objeto inmediato la protección de los datos, pero como fin último y primordial, la tutela del amplio plexo de bienes jurídicos que pueden ser afectados por el tratamiento ilegal o ilegítimo de los datos relativos a personas identificadas o identificables. Y esa protección debe brindarse a través de diversos medios, entre los cuales se encuentran, en especial: a) la protección administrativa a través de autoridades de control en los ámbitos locales (v.gr., la Agencia Española de Protección de Datos), regionales (v.gr., el Supervisor Europeo de Protección de Datos, para los datos de las instituciones y organismos de la Unión Europea y el Comité Europeo de Protección de Datos, organismo público europeo independiente cuyos objetivos son garantizar la aplicación coherente del Reglamento General de Protección de Datos en la Unión Europea, así como Noruega, Liechtenstein e Islandia) y eventualmente internacionales -donde el estado de cosas ya reclama, en un mundo hiperconectado que no conoce de fronteras físicas, una autoridad global-; y b) la tutela judicial, a partir de los procesos en general y del *hábeas data* típico del constitucionalismo latinoamericano como acción y como proceso judicial específico en particular.

3. De la protección de la privacidad al derecho "a" la protección de datos

Señala Estadella Yuste que si bien los rudimentarios sistemas de registro, propios de la etapa anterior a las computadoras, ya auguraban los riesgos que implicaba un fichero con datos incompletos, falsos o utilizados para otros propósitos,

> El derecho a la 'protección de datos' pertenece al contexto de la era informática, y ciertamente resulta atrevido afirmar que esta compleja disciplina legal estuviera ya implícita en las referencias generales al derecho a la intimidad inserta en cuerpos normativos de ámbito nacional o internacional de la era preinformática (Estadella Yuste, 1995, p. 25).

En aquel primitivo contexto, la defensa contra las afecciones provocadas por los avances de las TICs se realizaba a partir de la primitiva noción del derecho a la privacidad, pero siguiendo la impronta marcada por Warren y Brandeis en 1890, esto fue mutando. Como lo indica Carranza Torres:

> De esta formulación principal se desgajaron, a partir de entonces y hasta el presente, una serie de derechos más específicos. Por ello se dice que el concepto moderno de la privacidad engloba una 'colección' de intereses jurídicamente protegidos, tales como la privacidad de las ideas, la protección de la imagen personal, la privacidad en el domicilio, y la protección del honor, entre otros... la forma de regulación jurídica de lo relacionado con el derecho a la intimidad en el derecho internacional parte de entender al mismo como un derecho multidimensional, que en definitiva agrupa a otros que, partiendo de su contenido de base, desarrollan de modo más específico las distintas facetas que el mismo adquiere en contacto con la realidad...
>
> El concepto de 'derecho a la autodeterminación informativa' se construye a partir de la noción de intimidad, privacy, riservatezza o vie privée.
>
> En los años sesenta surge en la doctrina el reconocimiento de un derecho de las personas encaminado a reivindicar la protección jurídica frente a la captación y utilización no autorizada de información personal, en diversos autores como Alan F. Westin, 1967 (*Privacy and Freedom*), Arthur R. Miller, 1971 (*Personal privacy in the computer age: the challenge of new technology in an information oriented society*), Guido Alpa (*"Privacy" e estatuto dell'informazione*) y Richard F. Hixson (*Privacy in a public society*).
>
> Refiere Palazzi que ya en el año 1968 Charles Freid definió la *privacy*, concepto jurídico semejante al nuestro de intimidad, como el control que se tiene sobre los propios datos. Tal definición fue de aceptación general de la doctrina. Posteriormente, Lawrence Tribe, en su obra *American Constitutional Law*, se refirió a un derecho a controlar la masa de información por la que se define la identidad de una persona, como parte del derecho que cada persona desea (o no) mostrar a la sociedad" (Carranza Torres, 2001, Con cita de Pablo A. Palazzi, *El hábeas data en el derecho argentino*, pág. 5).

De acuerdo con lo expuesto, en la doctrina especializada hay consenso –en algunos casos, cuanto menos, tácito– en cuanto a que, por una suerte de mutación evolutiva del derecho a la intimidad (que en un momento resultó insuficiente para abrigar los intereses dignos de tutela frente al tratamiento de datos), se fue forjando un derecho nuevo, con matices propios que lo dotan de autonomía, al que se le adjudican distintos nombres, según el sistema jurídico de que se trate, y que nosotros preferimos rotular "derecho a la protección de los datos de carácter personal" (o "derecho a la protección de datos", a secas), por reflejar con mayor precisión su contenido.

En esa evolución, y salvo por el aislado precedente de la Constitución alemana de 1919 que reconoció a todo funcionario el derecho a controlar la información contenida en su legajo personal y a justificarse de cualquier imputación antes de que se asiente su sanción (art. 129), fue recién a partir de 1970 —cuando los ordenadores mostraron un notable incremento en los potenciales riesgos del tratamiento de datos de carácter personal—, que comenzó el desarrollo normativo del derecho a la protección de datos.

Así, los países por entonces tecnológicamente más avanzados –en especial, los Estados Unidos y los países de Europa central– fueron elaborando paulatinamente legislación específica sobre el tema, apuntando a establecer reglas concretas para enfrentar la nueva problemática, aunque con diferentes enfoques. Sin embargo, tales regulaciones partieron de diferentes enfoques, pues mientras en los Estados Unidos preponderantemente se ha recurrido a regular esta temática sólo cuando se lo consideró imprescindible y de manera limitada a través de leyes sectoriales específicas –salvo en la última década donde empezaron a florecer algunas leyes generales estaduales, iniciando por la de California—, en Europa se ha realizado una pormenorizada regulación tanto en el ámbito comunitario, a partir de convenios, directivas y reglamentos –entre los cuales se destaca actualmente el Reglamento General de Protección de Datos—, como en el de los países integrantes de la unión, ya por medio de leyes generales aplicables a todos los tratamientos —que prevén además determinados órganos específicos de tutela—, y regulaciones constitucionales de al menos algunos de sus contenidos (v.gr., Constituciones de Portugal, de 1976 y de España, de 1978), en tendencia que se extendió rápidamente a otros países extracomunitarios.

Por su parte, en Latinoamérica, sustancialmente más retrasada en el acceso a los recursos tecnológicos, inicialmente sólo se constitucionalizaron algunos aspectos del instituto (en especial incorporando la figura del hábeas data como garantía procesal constitucional a partir de la Constitución brasileña de 1988), y se dictaron regulaciones aisladas a través de leyes de carácter general al estilo europeo, las cuales afortunadamente se han extendido en la última década al punto de cubrir actualmente casi toda la región.

Pese a ello, y a diferencia de la realidad europea, no existe al momento regulación regional alguna del derecho a la protección de datos, sino sólo normas de *soft law*, en particular los "Principios sobre la Privacidad y la Protección de Datos Personales", adoptados por la OEA en 2015 y actualizados en 2021 (OEA, 2021) y los más completos "Estándares de protección de datos personales para los estados iberoamericanos"(RIPD, 2017) aprobados en 2017 por la Red Iberoamericana de Protección de Datos (RIPD), que siguen el molde del Reglamento General de Protección de Datos de la Unión Europea.

La insuficiente protección, via *soft law*, existente en la región se vio mejorada desde fines de 2023 a partir de una sentencia de la Corte IDH, que reconoció como derecho autónomo emergente de la Convención Americana sobre Derechos Humanos al "derecho a la autodeterminación informativa", al cual también denomina, casi siempre indistintamente, "derecho a la protección de datos"[9].

4. Las cinco generaciones de las normas de protección de datos

Teniendo en cuenta los cambios tecnológicos y la progresividad de los derechos humanos, cabe distinguir en cinco generaciones de normas, las cuales están marcadas por diversas improntas.

Conforme ya lo anticipara Fappiano hace algunos años, las sucesivas formulaciones reguladoras han ido acompañando a las generaciones de derechos humanos, y así, mientras las primigenias leyes apuntaron a tutelar la libertad individual, en tanto derecho al honor, a la intimidad personal y familiar, las posteriores hicieron lo propio con los derechos económicos, sociales y culturales al asegurar la igualdad, en tanto igualdad de oportunidades, mediante la prohibición de la recolección de los denominados "datos sensibles", debido a su potencialidad

9 Corte IDH. Caso Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" Vs. Colombia. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 18 de octubre de 2023. Serie C No. 506, disponible en https://www.corteidh.or.cr/docs/casos/articulos/seriec_506_esp.pdf.

discriminatoria. Y finalmente, en la actualidad tienden a asegurar el derecho al desarrollo, en tanto desarrollo de la propia personalidad, amenazado por determinados usos del producto de los progresos científicos y tecnológicos, usos que han dado lugar a ese fenómeno llamado "la contaminación de las libertades" (*liberties pollution*), concediendo a los titulares de los datos los derechos a conocer, de acceder e intervenir los datos almacenados y a los recursos para su efectiva tutela jurisdiccional (Fappiano, 1998, pp. 647, 648).

4.1. Primera generación

Esta primera etapa se inicia paralelamente en en Europa y en los Estados Unidos en el período de "antagonismo oscilatorio" de los años 1960 que sucedió a la primer "Guerra Fría". Son tiempos signados por la llegada del hombre a la luna y la aparición de Arpanet, cuando se potenciaron notoriamente las amenazas a la vida privada a partir de importantes avances tecnológicos habidos en el ámbito de las TICs.

Frente a este intimidante panorama tecnológico, el Consejo de Europa creó en 1967 una Comisión Consultiva encargada de estudiar el impacto de las nuevas tecnologías sobre los Derechos Humanos; en 1968 la Asamblea Parlamentaria de dicho Consejo le solicitó al Comité de Ministros determinar si las legislaciones de los Estados miembros daban o no una protección adecuada a la vida privada de las personas (Resolución sobre "los Derechos Humanos y los nuevos logros científicos y técnicos"); frente a la respuesta negativa a la consulta evacuada en 1970 en el informe "Derecho al respeto de la privacidad afectada por los dispositivos científicos y tecnológicos modernos"("*Right to respect for privacy as affected by modern scientific and technological devices*"), en 1971 el Comité instó a la comisión de expertos a que elaborara las medidas apropiadas; como consecuencia de las cuales dictó en 1973 y 1974 dos resoluciones "sobre la protección de la vida privada en los bancos electrónicos de datos" –Resoluciones (73) 22, referida al sector privado[10] y (74) 29, relativa al sector público[11]–, por las que se definieron los principios de la protección de datos personales a fin de promover la elaboración de legislaciones nacionales basadas en éstos, y finalmente, en 1976 se designó una comisión de expertos encargada de desarrollar los trabajos preparatorios de lo que fructificaría luego en la aprobación, en enero de 1981 y por parte de los Estados miembros del Consejo de Europa, del Convenio 108 "para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal"[12], norma que, junto con las "Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales" emanadas de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) [13], servirán de cierre de esta etapa y de apertura de la siguiente.

En este contexto, apenas iniciada la década de 1970 diversos países europeos fueron dictando sus leyes de protección de datos, en concreto Alemania (1970 a nivel estadual y 1977 a nivel federal) e inmediatamente después Suecia (1973), Francia (1977), Austria (1978), Dinamarca (1978), Noruega (1978) y Luxemburgo (1979).

10 Resolution (73)22 on the protection of the privacy of individuals vis-a-vis electronic data banks in the private sector. 26 September 1973. Council of Europe. Committee of Ministers. https://rm.coe.int/1680502830

11 Resolution of the privacy of individuals vis-a-vis electronic data banks in the public sector. 20 September 1974. Council of Europe. Committee of Ministers. https://rm.coe.int/16804d1c51

12 Convenio n. 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y protocolo adicional al convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, a las autoridades de control y a los flujos trasfronterizos de datos. Noviembre 2012. https://www.oas.org/es/sla/ddi/docs/u12%20convenio%20n%20108.pdf

13 Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales. 1980. https://archivos.juridicas.unam.mx/www/bjv/libros/7/3249/28.pdf

En ellas se reguló el tratamiento de datos personales de las personas físicas en sistemas "informáticos" o "mecanizados" del sector público -y en algunos casos también del sector privado-, reconociéndose los derechos más elementales y, aunque eran inferibles de sus disposiciones, con un casi nulo y desestructurado desarrollo de los principios.

Por ejemplo, la ley federal de Alemania de 1977, que trajo regulaciones diferenciales para los sectores público y privado, reconoció los derechos de los titulares de datos a la información, rectificación, supresión, bloqueo (cuando no se pudiere acreditar la exactitud de los datos y en el caso de los registros privados cuando ya no fueren necesarios para cumplir con el objetivo del almacenamiento), seguridad (a través de medidas técnicas y organizativas) y al secreto profesional de los tratantes. Estableció el principio del consentimiento para el tratamiento de los datos personales y el deber de informar a los titulares cuando aquellos fueron recopilados por el sector público en virtud de una ley. Creó las figuras del Comisionado de Protección de datos (con facultades amplias, incluidas las sancionatorias, elegido por el presidente por recomendación del gobierno federal y dependiente del Ministerio del Interior) y la del Delegado de Protección de Datos para los tratamientos en el ámbito privado de acuerdo a la cantidad de empleados y a los tipos de tratamientos.

Ya en el ámbito constitucional, destacan las previsiones contenidas en las constituciones de Portugal (1976, reformada en 1991) y de España (1978), que apuntaban primordialmente a la protección de la vida privada y familiar frente a los avances de la informática.

Paralelamente, en los Estados Unidos se adoptaron la *Fair Credit Reporting Act* (FCRA, Ley de reportes de créditos justos, de 1970), la *Family Educational Rights and Privacy Act* (FERPA, Ley de protección de los derechos educativos de la familia, de 1974) y la *Privacy Act* (Ley de privacidad, de 1974, reformada en 2014), por la que se normó el uso de la información personal por los órganos y entes federales, norma que complementa la *Freedom of information act* (FOIA, Ley de libertad de información, de 1966, con las reformas de 1974, 1976, 1986, 1996). También se produjeron en este período reformas a la *Federal Trade Commision Act*, (FTCA, Ley de la Comisión Federal de Comercio, de 1914).

Ya en el ámbito latinoamericano, en gran medida sumido en regímenes autoritarios y con escaso acceso a las tecnologías informáticas por entonces disponibles, no se registraron reglas constitucionales ni legales similares.

4.2. Segunda generación

Como se anticipó, esta nueva etapa se abre con la aprobación de las "Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales" de la OCDE, de 1980 (las que fueron actualizadas en 2013 (OECD, 2013)) y por la adopción del Convenio n° 108, de 1981 "para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal" (STE n° 108) por parte de los países miembros del Consejo de Europa, -norma a la cual se le adicionarán luego un Protocolo adicional, aprobado en 2001, por el que se requirió a los Estados parte establecieran autoridades de supervisión que ejercieran sus funciones con total independencia (STE n° 181) (Council of Europe, 2001), y una enmienda tendiente a modernizar el convenio, adoptada en 2018 (Convenio 108+[14])-. Este período se extenderá hasta 1995, cuando fuera aprobada por el Parlamento Europeo y el Consejo la Directiva 95/46/CE, "relativa a la protección de las personas físicas, en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos"[15].

14 Convention 108 and protocols. https://www.coe.int/es/web/data-protection/convention108-and-protocol

15 Directiva 95/46/CE del Parlamento Europeo y del consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. https://www.oas.org/es/sla/ddi/docs/Directiva-95-46-CE.pdf

Estas normas, en un entorno apenas previo a la aparición de Internet, tomarán la experiencia de las primeras leyes de protección de datos y sistematizarán más adecuadamente los principios y derechos por ellas reconocidos, a la par de preocuparse por el libre flujo de los datos debidamente tratados, en un entorno marcado por notorios avances tecnológicos de variada índole.

Así, como indica la doctrina:

> Además del refinamiento en hardware y software en todas las plataformas, la aparición de nuevas aplicaciones; el abaratamiento de los soportes físicos y la extensión cuasi universal del microordenador, hay tres fenómenos que han sido identificados por la doctrina en lo relativo a las leyes de protección de datos.
>
> En primer lugar, la trivialización del procesamiento de datos, causada por la evolución de los grandes sistemas informáticos de los años sesenta, escasos y poco accesibles, a los numerosos microordenadores personales interconectados en redes de área local muy potentes y accesibles.
>
> En segundo lugar, la diversificación de los datos: las clásicas bases de datos de grandes organizaciones no son hoy en día los únicos sistemas de información existentes; existen también sistemas expertos, sistemas de microficha, discos ópticos con y sin imágenes y bases de datos en CD-ROM.
>
> Por último, el creciente sistema de distribución e información interactivos tales como sistemas bidireccionales de televisión por cable, servicios educativos, juegos interactivos, sistemas expertos y correo y conferencias electrónicas...” (Lázpita Gurtubay, 1994).

En el ámbito normativo, las Directrices de la OCDE reconocieron los principios de:

a) limitación de la recolección de los datos (recogida mediante medios lícitos y justos y, en su caso, con el conocimiento o consentimiento del titular de los datos);

b) calidad de los datos (pertinentes, exactos, completos y actualizados) c) especificación de la finalidad;

d) limitación del uso;

e) salvaguardia de la seguridad;

f) apertura (con respecto a avances, prácticas y políticas con respecto a los datos personales, dotándose de medios fácilmente disponibles para establecer la existencia e índole de los datos personales, y de las principales finalidades para su uso, así como la identidad y domicilio del controlador de los datos);

g) participación individual (derechos de los titulares a recabar información sobre la existencia y contenido de sus datos; impugnarlos y, en su caso obtener la supresión, la rectificación o que se completen o modifiquen) y responsabilidad por el cumplimiento de las medidas que den efecto a los principios.

Por su parte, el Convenio n° 108 se diseñó para regir los tratamientos de los “ficheros” y de los “tratamientos automatizados” que se lleven a cabo tanto en el sector público como en el privado, pudiendo ser ampliado a los “no automatizados” y a “agrupaciones, asociaciones, fundaciones, sociedades, compañías y cualquier otro organismo compuesto directa o indirectamente de personas físicas, tengan o no personalidad jurídica”.

Los principios establecidos en el Convenio son los siguientes:

a) calidad de los datos (deben ser obtenidos y tratados leal y legalmente; almacenados para fines específicos y legítimos y no utilizado de manera incompatible con esos fines; adecuados,

pertinentes y no excesivos en relación con los fines para los que se almacenan; exactos; actualizados cuando sea necesario; conservados en una forma que permita la identificación de los interesados por no más tiempo del necesario para el propósito para el cual se almacenan esos datos);

b) protección especial de los datos sensibles;

c) seguridad de los datos y

d) protección frente al flujo transfronterizo de datos.

Ya en cuanto a los derechos, los reconocidos a los titulares de los datos son los de: a) información; b) acceso, c) rectificación y d) borrado (cancelación).

Dado que al momento de la aprobación del Convenio 108 no había surgido todavía Internet (esto ocurriría en 1983 con la adopción, como estándar, del protocolo TCP/IP), y tampoco se había logrado una masiva utilización de computadoras personales que ofrecieran conectividad a la red (lo que aconteció a partir de la puesta en el mercado de la Apple McIntosh), este convenio en realidad

> No fue innovador, reflejando los puntos de vista ya recogidos en las leyes existentes, la gran aportación fue que los principios de protección de datos fueron investidos con la autoridad de un organismo internacional, lo que propició la expansión de las leyes de protección de datos, conocidas como de segunda generación y la revisión de las leyes anteriores, para adecuarse a la nueva realidad tecnológica y al Convenio del Consejo de Europa… Aunque todas las leyes internas siguen el modelo del Convenio, la protección ofrecida en la práctica varía sensiblemente de unos países a otros. El Convenio es enunciado en términos muy generales. Los principios básicos de protección hacen referencia a la calidad y seguridad de los datos, a las garantías de las personas cuyos datos han sido registrados, al régimen especial a que someter los datos que merecen una protección cualificada y a las excepciones y restricciones legítimas (Lázpita Gurtubay, 1994).

En este período, y como consecuencia de las reglas emanadas del Convenio, se aprobaron numerosas leyes europeas, en algunos casos por primera vez (como los del Reino Unido, en 1984 y de España, en 1992) y en otros, produciendo reformas a las leyes dictadas en el período anterior (como en el caso de Alemania, en 1990, cuyo Tribunal Constitucional Federal ya había dado partida de nacimiento, en 1983, al "derecho a la autodeterminación informativa" en su célebre sentencia sobre la inconstitucionalidad de la Ley de Censo de Población de 1982[16]).

Así, fueron aprobadas, entre otras, las leyes del Reino Unido (*Data Protection Act*, de 1984), Finlandia (1987), la Dinamarca (1987 y 1991), Irlanda (1988), Países Bajos (1989), República Federal Alemana (1990), Portugal (1991), Suecia (1992), Hungría (1992), Bélgica (1992) y España (1992), aunque no todas tuvieron idénticos alcances puesto que el Convenio dejó un amplio margen de maniobra nacional (así, por ejemplo, sólo algunas como las de Francia, Dinamarca, y Luxemburgo extendieron su aplicación a las personas jurídicas).

De otro lado, en el plano constitucional, en este período se incorporaron disposiciones específicas en las constituciones de Holanda (1983); Croacia (1990), Eslovaquia (1991), Eslovenia (1991), Albania (1991), Bulgaria (1991), Bosnia—Herzegovina (1992), Estonia (1992), República Checa (1992), Rusia (1993) Bielorrusia (1994), Azerbaiján (1995); Gabón (1991), Cabo Verde (1992), Sudáfrica (1996) y Fiji (1990).

16 Sentencia de 15 de diciembre de 1983, BJC Boletín de Jurisprudencia Constitucional, núm. 33, enero 1984, Publicaciones de las Cortes Generales, Madrid, págs. 126-170.

Ya en el ámbito internacional global, la Asamblea General de la ONU adoptó una serie de principios rectores para la reglamentación de los ficheros computadorizados de datos personales (Resolución 45/95, del 14/12/90), en los cuales marcó ciertas orientaciones que deben seguir los Estados al regular lo concerniente a los ficheros computadorizados (públicos o privados, y con extensión facultativa a los ficheros manuales) que contengan datos de personas físicas (con extensión también facultativa a los de las personas jurídicas, en particular cuando contengan información sobre personas físicas)[17].

Pasando a América, Canadá adoptó la *Privacy act (Ley de privacidad, de 1983, aplicable al sector público*) y en los Estados Unidos se aprobaron en este período diversas normas sectoriales, en concreto la *Cable TV Privacy Act* (Ley de privacidad para los operadores de cable, de 1984); la *Video Privacy Protection Act* (VPPA, Ley de privacidad en el alquiler de videos, de 1988); la *Telephone Consumer Protection Act* (TCPA, Ley de protección del consumidor telefónico, de 1991), y la *Driver's Privacy Protection Act* (DPPA, Ley de privacidad de los conductores, de 1994).

Finalmente, en Latinoamérica, si bien en este período no se aprobaron leyes de protección de datos, sí se incorporaron reglas constitucionales específicas tanto en estados nacionales como subnacionales, en los primeros años siguiendo primordialmente el molde de la Constitución española de 1978 y luego de la aprobación de la Constitución brasileña de 1988 predominantemente incorporando la figura del hábeas data o aludiendo a la protección contra el tratamiento indebido de los datos personales.

Son de este período las constituciones de Guatemala (1985, art. 31); Nicaragua (1987, reformada en 1995, art. 26, inc. 4); Brasil (1988, arts. 5; numerales X, LXXII y LXXVII); Colombia (1991, art. 15, actualizado en 2003); Paraguay (1992, art. 135); Perú (1993 con su reforma de 1995, arts. 2, incs. 5 y 6, y art. 200); Argentina (1994, art. 43, párr. 3º).

4.3. Tercera generación

La tercera generación de normas de protección de datos se abrirá con la aprobación de la Directiva 95/46/CE "relativa a la protección de las personas físicas, en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos" y se extenderá hasta 2009, cuando la 31ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad adoptara la "Propuesta Conjunta para la Redacción de Estándares Internacionales para la protección de la Privacidad, en relación con el Tratamiento de Datos de carácter personal" ("Resolución de Madrid") (AEPD, 2009).

Dentro de esta etapa se gestarán cambios tecnológicos muy relevantes que darán lugar a la configuración de la "web 2.0", los que tendrán, en el futuro inmediato, un impacto normativo significativo. Así, promediando esta etapa y a partir de la aparición de la primera gran red social de edición colaborativa (Wikipedia, 2001), se produjo una verdadera explosión de éstas (entre 2003 y 2006 se lanzarían LinkedIn, Myspace, Skype, Facebook, Youtube y Twitter, entre las más populares), fenómeno altamente potenciado luego de la salida al mercado, a mediados de 2007, del primer teléfono inteligente (*smartphone*) con wifi (el *Iphone* de Apple), adelanto técnico que, al convertirse rápidamente en un centro de convergencia tecnológica que además era portable, intensificó enormemente el uso de Internet y de todos los servicios de la sociedad de la información, dando el entorno perfecto a la web "social" o "participativa", donde los usuarios interactúan y colaboran entre sí, como creadores de contenido, especialmente a través de redes sociales.

17 Directrices de protección de datos de la ONU de 14 de diciembre de 1990. https://www.informatica-juridica.com/anexos/directrices-de-proteccion-de-datos-de-la-onu-de-14-de-diciembre-de-1990

Esta confluencia de tecnologías disruptivas llevará a una profunda movilización y cambios en el enfoque de la protección de datos a partir del creciente reclamo por el reconocimiento de nuevos derechos y principios frente a la clara insuficiencia del esquema normativo preexistente para afrontar a los nuevos y variados efectos que estaban produciendo los avances tecnológicos. Y si bien estos cambios normativos no se dieron en plenitud en este período, la mayoría de los planteos se gestaron aquí y se verán concretados en las dos etapas posteriores.

La Directiva que inicia esta etapa refiere a su ámbito de aplicación (los tratamientos de datos de los sectores público y privado), a sus principios informadores, a los derechos de los titulares de datos, a la responsabilidad por los tratamientos y a los mecanismos de control.

Los principios rectores de la normativa –y de las leyes de transposición dictadas en su consecuencia— son los de: a) licitud y lealtad; b) calidad de los datos; c) consentimiento informado del titular para el tratamiento (excepto intereses individuales o sociales estimados prevalecientes); d) seguridad de los datos; e) confidencialidad; f) uso acorde a la finalidad y g) protección especial de los datos sensibles.

Los derechos reconocidos a los titulares de los datos son los de: a) información; b) acceso; c) rectificación; d) cancelación; e) bloqueo; f) notificación a terceros cedidos respecto de rectificaciones, supresiones o bloqueos; g) oposición a tratamientos;h) no ser sometido a decisiones fundadas únicamente en el tratamiento automatizado de datos.

Dado que por su carácter de Directiva no resultaba de aplicación inmediata en los países de la Unión, fue necesaria la transposición de sus normativas, con algún margen de apreciación nacional, a través de la adopción de las respectivas leyes internas. Esto provocó, como ocurrió en el período anterior con la aprobación del Convenio 108/81, que los países comunitarios que todavía no habían aprobado leyes de protección de datos las adoptaran y que aquellos que ya las tenían, las reformaran para adaptarlas a las nuevas exigencias comunitarias.

Así, se dictaron en este período, entre otras, las leyes de Italia "Sobre la tutela de las personas y otros sujetos respecto al tratamiento de datos personales" (1996); de Suecia, "Sobre protección de datos de carácter personal" (1998); de Reino Unido (la *Data Protection Act* de 1998) y de España "de protección de datos de carácter personal" (1999), llegándose durante la primera década de este siglo a que todos los estados miembros adecuaran su derecho interno a las exigencias de la Directiva.

Ya en 2000, se aprobó la Carta de Derechos Fundamentales de la Unión Europea (Declaración de Niza), que luego de reconocer el derecho a la vida privada (art. 7) consagra como derecho autónomo al derecho a la protección de datos (art. 8[18]), cuya configuración teórica ya había sido reconocida por el Tribunal Constitucional alemán en el período anterior, en posición luego seguida por distintos pronunciamientos en la región, como es el caso del Tribunal Constitucional español[19].

Y con posterioridad, siempre en el ámbito europeo, diversas normativas comunitarias comenzaron a dar más forma a ciertos tratamientos sectoriales específicos de datos, entre ellas

18 Artículo 8. Protección de los bienes de carácter personal

1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.

2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.

3. El respeto de estas normas quedará sujeto al control de una autoridad independiente.

19 Sentencias 254/1993, 11/1998, 105/1998 y 124/1998.

el Reglamento (CE) nº 45/2001 de protección de datos de las instituciones de la UE[20], la Directiva 2000/31/CE, sobre el comercio electrónico[21], la Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas[22] y la Directiva 2003/98/CE relativa a la reutilización de la información del sector público[23].

También dentro de este período, se aprobó en 2004 el Marco de Privacidad del Foro de Cooperación Económica Asia – Pacífico (APEC)[24], el que será luego actualizado en 2015, que promueve un enfoque flexible para la protección de la privacidad de la información en las economías de sus Estados miembros -varios de los cuales son americanos[25]- a fin de evitar la creación de barreras innecesarias para los flujos de información y asegurar un intercambio continuo y el crecimiento económico en la región.

Sus principios clave son:

a) prevención de daño a las personas por el manejo inadecuado de su información personal;

b) deber de información (aviso) a las personas sobre la recolección y el uso de sus datos personales;

c) limitaciones a la recolección a la estrictamente relevante para el propósito específico;

d) tratamiento de los datos personales conforme a los fines;

e) libertad de elección respecto de los usos de la información personal;

f) integridad de la información, garantizándose su exactitud y actualización;

g) seguridad, a partir de medidas protectorias adecuadas;

h) acceso y rectificación de los datos, e

i) responsabilidad por el cumplimiento de estos principios.

Pasando a las Américas, en el ámbito de la OEA se gestó un Anteproyecto de Convención Americana sobre Autodeterminación Informativa (1997) que finalmente no fructificó, pero se destaca la creación de la "Red Iberoamericana de Protección de Datos" (La Antigua, junio de 2003) y la "Declaración de Santa Cruz de la Sierra" (Bolivia, noviembre de 2003) (Cumbre Iberoamericana, 2003), adoptada por los jefes de Estado y de Gobiernos Iberoamericanos, a tenor de cuyo texto (núm. 45) se reconoció el rango de derecho fundamental del derecho a la protección de los datos de carácter personal y se destacó la importancia tanto de las iniciativas regulatorias iberoamericanas, como de la creación de la Red Iberoamericana de Protección de Datos, integrada actualmente por todas las autoridades de control iberoamericanas.

---

20 Reglamento (CE) n° 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos, DO 2001 L 8. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32001R0045.

21 Directiva 2000/31/CE, del 08/06/00, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior. https://www.boe.es/buscar/doc.php?id=DOUE-L-2000-81295.

22 Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, DO 2002 L 201. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002L0058

23 Directiva 2003/98/CE relativa a la reutilización de la información del sector público. https://www.boe.es/doue/2003/345/L00090-00096.pdf.

24 Anexo XVIII. Marco de privacidad del foro de cooperación económica Asia Pacífico (APEC). https://archivos.juridicas.unam.mx/www/bjv/libros/7/3249/27.pdf

25 Integran la APEC Australia, Brunéi, Canadá, Chile, China, Corea del Sur, Estados Unidos, Filipinas, Hong Kong, Indonesia, Japón, Malasia, México, Nueva Zelandia, Papúa Nueva Guinea, Perú, Rusia, Singapur, Tailandia, Taiwán y Vietnam.

Ya en el plano nacional, Canadá adoptó la *Personal Information Protection and Electronic Documents Act* (PIPEDA) (Ley de protección de información personal y documentos electrónicos", de 2000, aplicable al sector privado), y en los Estados Unidos fueron aprobadas diversas leyes federales, en concreto,

- *Health Insurance Portability and Accountability Act* (Ley de portabilidad y responsabilidad demostrada en los seguros médicos, de 1996);
- *Children's Online Privacy Protection Act* (COPPA, Ley de protección de la privacidad en línea de los niños, de 1998);
- *Gramm Leach Bliley Act* (GLBA, Ley de protección de la "Información personal no pública" recopilada por bancos, aseguradoras y compañías de servicios financieros, de 1999);
- *Fair and Accurate Credit Transactions Act* (FACTA) (Ley de informaciones justas y precisas sobre transacciones de crédito, de 2003);
- *Controlling the Assault of Non-Solicited Pornography And Marketing Act* (CAN-SPAM, Ley para controlar el envío de pornografía y marketing no deseado, de 2003).

Por su parte, en Latinoamérica se aprobaron normas constitucionales en Ecuador (1998, art. 94 y 2008 y reforma de 2008, arts. 66 incs. 11 y 19, 40, inc. 5, 92, 215 y 436), Venezuela (1999, arts. 28, 60 y 281) Panamá (2004, arts. 42 y 44); Bolivia (2004, art. 23 y 2009, arts. 130 y 131); Honduras (2006, arts. 76 y 182) y México (2007, art. 6). Se aprobaron asimismo leyes en Chile (1999, ley 19.628), Argentina (2000, ley 25.326), Paraguay (2001, ley 1682), Uruguay (2004, ley 17.838 y 2008, ley 18.331) y Colombia (2008, ley 1.266 y 2012, ley 1.581). Finalmente, en el Caribe adoptaron leyes Bahamas (2003) y San Vicente y Granadinas (2003).

4.4. Cuarta generación

La cuarta generación se inicia, como se indicó, a partir de la adopción, en 2009, de los Estándares Internacionales para la protección de datos ("Resolución de Madrid") y se extenderá hasta 2016, cuando fuera aprobado el Reglamento (UE) 2016/679 "Relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos" ("Reglamento general de protección de datos", que deroga la Directiva 95/46/CE e impone revisión Directiva 2002/58/CE), instrumento que significará otro punto de inflexión –en este caso, normativo— que provocará la incorporación de nuevos y sustanciales cambios regulatorios, al calor de los cambios tecnológicos que se aceleraron promediando la etapa anterior.

En efecto, mientras la velocidad y capacidad de almacenamiento de los ordenadores iba en aumento y los servicios de la sociedad de la información ampliaban sus capacidades operativas y se expandían, aparecieron nuevos fenómenos que confluyeron a conformar un estado de coas altamente complejo que requirió la atención del derecho.

Entre muchas otras manifestaciones tecnológicas, se destaca en este período el uso masivo de los servicios de computación en la nube (con mucha mayor capacidad de almacenamiento), el perfeccionamiento de los buscadores, la conformación del *big data*, los *smartphones* con conectividad a Internet, una creciente variedad y cantidad de aplicaciones (*apps*), la geolocalización, la tecnología para llevar puesta (*wearables*), la domótica, la aparición de las ciudades inteligentes (*smart cities*), el *deep* (*machine*) *learning*, la realidad aumentada, el perfilado a través de algoritmos (en buena medida sesgados), las decisiones automatizadas, el uso diversificado de las cadenas de bloques (*blockchains*), una tecnología popularizada por la aparición del bitcoin y otras criptomonedas, y los metaversos, entre otros fenómenos convergentes.

Son productos de esta etapa, en el ámbito comunitario europeo, la "Resolución de Madrid"; el "Convenio del Consejo de Europa sobre el Acceso a los Documentos Públicos", adoptado también en 2009 (Council of Europe, 2009), las nuevas Directrices de la OCDE "sobre protección de la privacidad y flujos transfronterizos de datos personales", aprobadas en 2013 (OECD, 2013) y la Directiva 2013/37 CE que reforma a la 2003/98/CE relativa a la reutilización de la información del sector público, también de 2013[26].

La "Resolución de Madrid" desarrolla sus diferentes contenidos en los siguientes capítulos:

I) Disposiciones generales:
a) objeto, b) definiciones, c) ámbito de aplicación, d) medidas excepcionales y e) excepciones.

II) Principios básicos:
a) lealtad y legalidad; b) finalidad; c) proporcionalidad, d) calidad de los datos; e) transparencia; f) responsabilidad.

III) Legitimación para el tratamiento:
a) principio general de legitimación; b) especial protección de los datos sensibles; c) prestación de servicios de tratamiento; d) transferencias internacionales.

IV) Derechos del interesado:
a) acceso; b) rectificación y cancelación; c) oposición; d) ejercicio de los derechos.

V) Seguridad:
a) medidas de seguridad y notificación de brechas; b) deber de confidencialidad;

VI) Deber de supervisión:
a) medidas proactivas; b) supervisión; c) cooperación y coordinación; d) responsabilidad.

Ya en las Américas, la OEA aprobó en 2015 los "Principios sobre la protección de la privacidad y los datos personales (CJI, 2015)" –que fueron luego actualizados en 2021—, un documento muy básico que recoge los componentes más elementales de la protección de datos, reconociendo los siguientes principios: a) propósitos legítimos y justos; b) claridad y consentimiento; c) pertinencia y necesidad; d) uso limitado y retención; e) deber de confidencialidad; f) protección y seguridad; g) fidelidad de los datos; h) acceso y corrección; i) protección de los datos personales sensibles; j) responsabilidad; k) flujo transfronterizo de datos y responsabilidad y l) publicidad de las excepciones.

En los Estados Unidos se aprobó la *Health Information Privacy Protection Act* (HIPPA) (Ley de protección de la privacidad de la información de salud, de 2013).

Ya en Latinoamérica, en el ámbito constitucional fueron dictadas normas en México (2009, reforma al art. 6, y art. 16 y art. 73 numeral XXIX—O); Ecuador (reforma de 2008, arts. 66 incs. 11 y 19, 40, inc. 5, 92, 215 y 436) y República Dominicana (2010, reformada en 2015, arts. 44 y 70).

Y en el ámbito legal, se aprobaron leyes en, México (2010), Perú (2011, ley 29.733), Costa Rica (2011, ley 8968), Nicaragua (2012, ley 787) y República Dominicana (2013, ley 172). También se aprobaron leyes en Curaçao (2010), San Martín (2010), Santa Lucia (2011), y Trinidad y Tobago (2011).

Más allá de los avances normativos mencionados y como se indicó más arriba, durante esta etapa se gestaron algunos de esos nuevos principios y derechos que reclamaba esta nueva realidad, especialmente por vía doctrinaria, jurisprudencial y administrativa (a partir de la

26 Directiva 2013/37/UE del Parlamento Europeo y del Consejo, de 26 de junio de 2013, por la que se modifica la Directiva 2003/98/CE relativa a la reutilización de la información del sector público. https://www.boe.es/buscar/doc.php?id=DOUE-L-2013-81251

influencia incesante de las autoridades de control), generándose incluso diversas normas de *soft law*.

Por poner algunos ejemplos, con respecto al principio de protección de datos desde el diseño (*privacy by design*), motorizado por Ann Kavoukian desde 1995, éste fue adoptado luego de la publicación del "*The privacy by design framework*" en 2009, por la Asamblea Internacional de Comisionados de Privacidad y Autoridades de Protección de Datos en 2010.

Algo similar ocurrió con los derechos al olvido y a la portabilidad de los datos en el ámbito europeo. El primero, afincado en la doctrina (donde se destaca el libro de Victor Mayer-Schönberger "Borrar: la virtud de olvidar en la era digital" ("*Delete: the virtue of fogetting in the digital age*") y reconocido previamente por la Agencia Española de Protección de Datos, tuvo recepción jurisprudencial por parte de la Gran Sala del Superior Tribunal de Justicia de la Unión Europea en el célebre caso "Costeja" o "Google Spain"[27] y el segundo, fogoneado, entre muchos otros, por Viviane Reding siendo Comisaria de Protección de Datos de la UE, que tuvo como primer antecedente en el "*Data Portability Project*", iniciado en los Estados Unidos por un grupo de expertos y decisores del sector de nuevas tecnologías 5rá a la carga sobre estos mismos temas (derechos al olvido y a la portabilidad), ya siendo Vicepresidenta primera de la Comisión Europea, en la Conferencia Europea sobre protección de datos y Privacidad, al justificar que la Unión Europea necesitaba nuevas reglas de protección de datos personales, haciendo especial hincapié en la necesidad de reconocer el derecho al olvido.

Esta línea de pensamiento fue luego corroborada en una Comunicación de la Comisión Europea por la cual se realizaba un diagnóstico sobre la protección de los datos personales en la Unión, donde se enfatizó acerca de la necesidad de aportar herramientas para resolver los problemas de privacidad relacionados con los niños en la red —especialmente debido a que pueden ser menos conscientes de los riesgos, consecuencias y derechos vinculados al tratamiento de datos personales—; reforzar el principio de minimización de datos, mejorar las modalidades de ejercicio de los derechos de acceso, rectificación, borrado o bloqueo de datos, y reconocer explícitamente tanto el derecho al olvido como el derecho a la portabilidad de los datos, por el cual se confiera a la persona concernida «el derecho explícito a retirar sus datos (por ejemplo, fotografías o listas de amigos) de una aplicación o de un servicio, de modo que los datos retirados puedan transferirse a otra aplicación u otro servicio, siempre que ello sea técnicamente posible, sin que los responsables del tratamiento lo obstaculicen[28].

Pocos meses más tarde, en la Comunicación de la Comisión Europea COM (2012) 9 ("La protección de la privacidad en un mundo interconectado. Un marco europeo de protección de datos para el siglo XXI"), se presentaron dos iniciativas legislativas por medio de las cuales se pretendía adecuar el marco normativo existente —a través de un Reglamento General de Protección de Datos y una Directiva respecto del tratamiento de los datos penales— puesto que, en opinión de la Comisión, aquél ya no era suficientemente eficaz para preservar el derecho a la protección de datos personales en el "nuevo y complejo entorno digital actual".

El camino hacia la adopción urgente de una nueva normativa comunitaria que acompasara los tiempos que corrían estaba allanado y luego de algunos cambios en el proyecto original –entre los cuales, por ejemplo, se desguazó la regulación original del derecho al olvido— se aprobó en 2016 el Reglamento General de Protección de Datos (RGPD), que cierra esta etapa con la feliz consagración de nuevos derechos y principios y que deroga, a partir de su plena entrada en vigencia, en 2018, a la Directiva 95/46/CE, como se verá de inmediato.

27 "Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (es), Mario Costeja González", Case n° C–131/12, ECLI:EU:C:2014:317.

28 Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, "Un enfoque global de la protección de los datos personales en la Unión Europea", COM (2010) 609. Bruselas, 04/11/2010.

4.5. Quinta generación

Esta última generación de derechos, como se indicó, arranca a partir de 2016 con la aprobación del Reglamento (UE) 2016/679 "Relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos" ("Reglamento general de protección de datos")[29] y se extiende hasta el presente, donde la aceleración de los tiempos, en un entorno de una "web 3.0" que va camino a la "web 4.0", al calor de la intensificación del uso de la tecnología *blockchain*, de los metaversos y multiversos, de la Inteligencia Artificial Generativa (*GenAI*[30]) y de las neurotecnologías, entre otros fenómenos disruptivos, ya hace presagiar la pronta iniciación de una sexta generación de normas de protección de datos.

Es la etapa de mayor impacto de las tecnologías sobre el mundo jurídico, donde no sólo se ampliaron los alcances de anteriores derechos y principios e incluso se subdividieron los preexistentes en más específicos, sino que fueron creados o incorporados otros, forzados por los nuevos fenómenos (por ejemplo, el limitado principio de responsabilidad típico de la primera generación, actualmente fue ampliado y complementado a través de conceptos tan próximos como los de *compliance*; *accountability*, rendición de cuentas o responsabilidad proactiva o demostrada; transparencia y explicabilidad –este último típico principio aplicable a los procesos de la IA).

En esta etapa, en el plano global la ONU aprobó sus "Principios que informan la privacidad y la protección de datos personales" (A/77/196)[31], norma en la que se reconocieron los siguientes principios: a) legalidad, b) licitud y legitimidad; c) consentimiento; d) transparencia; e) finalidad; f) lealtad; g) proporcionalidad; h) minimización; i) calidad; j) responsabilidad y k) seguridad.

En el ámbito regional europeo, como se dijo, esta etapa se abre con el Reglamento General de Protección de Datos (RGPD), que es el principal pilar del esquema protectorio europeo en la materia y posee una gran potencia por ser de aplicación extraterritorial, ya que se extiende a responsables o encargados de tratamiento no establecidos en la Unión Europea que realicen tratamientos derivados de una oferta de bienes o servicios destinados a ciudadanos de la Unión o como consecuencia de una monitorización y seguimiento de su comportamiento (quienes deben designar representante en la Unión Europea, que actuará como punto de contacto de las autoridades de supervisión y de los ciudadanos).

Esta norma se estructura en 11 capítulos y 99 artículos, precedidos de 173 considerandos que explican con minuciosidad el sentido de sus reglas, al referir a los principios que rigen los tratamientos, consagra los de: a) licitud, b) lealtad, c) transparencia; d) limitación de finalidad; e) minimización de datos; f) exactitud; g) limitación del plazo de conservación; h) integridad y confidencialidad (seguridad); i) responsabilidad proactiva o demostrada (*accountability*), y j) control independiente.

---

29 Reglamento (UE) 2016/679 "relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos" ("Reglamento general de protección de datos", que deroga la Directiva 95/46/CE e impone revisión Directiva 2002/58/CE). https://www.boe.es/doue/2016/119/L00001-00088.pdf

30 La Inteligencia Artificial Generativa es una rama de la IA que se enfoca en la creación de contenido original a partir de datos prexistentes, siendo sus primeras aplicaciones más populares del mercado Midjourney y ChatGPT

31 A/77/196: Principios que informan la privacidad y la protección de datos personales. 20 julio 2022. https://www.ohchr.org/es/documents/thematic-reports/a77196-principles-underpinning-privacy-and-protection-personal-data#:~:text=Analizaremos%20en%20particular%20los%20siguientes,y%20protecci%C3%B3n%20de%20datos%20personales

Introduce además dos nuevos derechos -al olvido y a la portabilidad de los datos y en cuanto a las medidas específicas que prevé se encuentran las de: a) protección de datos desde el diseño; b) protección de datos por defecto; c) medidas de seguridad; d) mantenimiento de un registro de tratamientos; e) realización de evaluaciones de impacto sobre la protección de datos; f) nombramiento de un delegado de protección de datos; g) notificación de violaciones de la seguridad de los datos; h) promoción de códigos de conducta y esquemas de certificación, e i) análisis de riesgo de los tratamientos.

Sobre el consentimiento en general, exige que sea libre, informado, específico e inequívoco (mediante una declaración de los interesados o una acción positiva que indique el acuerdo, pero no puede deducirse del silencio o de la inacción), aunque para ciertos tratamientos debe además ser explícito y verificable (v.gr., datos sensibles), con reglas específicas para el caso de los menores (donde el consentimiento tiene que ser verificable y el aviso de privacidad debe restar redactado en un lenguaje que éstos puedan entender), quienes podrán consentir a partir de una edad que puede variar entre los 13 y 16 años según lo establezca cada Estado miembro.

Finalmente, en cuanto al control del cumplimiento de sus reglas, establece un procedimiento de cooperación entre las autoridades de los países involucrados en el caso, para que los afectados puedan reclamar ante sus autoridades (sistema de "ventanilla única"), eleva significativamente las sanciones y reemplaza al Grupo de Trabajo del art. 29 (GT 29) de la Directiva 95/46 por el Comité Europeo de Protección de Datos, un organismo público europeo independiente cuyo objetivo es garantizar la aplicación coherente del RGPD y está integrado por el Supervisor Europeo de Protección de Datos y todas las autoridades de protección de datos de la región.

Complementaron inmediatamente a esta pontentísima norma la Directiva (UE) 2016/680 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos[32]; la Directiva (UE) 2016/681 relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave[33] y la Directiva (UE) 2016/1148 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión[34].

En 2018, ya entrando plenamente en vigencia el RGPD, se aprobó el Protocolo adicional al Convenio 108 de 1981 (Convenio 108+), por el cual se modernizó el ya antiguo convenio, estableciéndose nuevos lineamientos, entre los que se destacan los siguientes:

a) aplicación de los principios a todas las actividades de tratamiento, incluso por seguridad nacional (con las excepciones y restricciones del caso, pero bajo supervisión independiente y efectiva);

32 Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del consejo. https://www.boe.es/doue/2016/119/L00089-00131.pdf

33 Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la utilización de datos del registro de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave. https://www.boe.es/doue/2016/119/L00132-00149.pdf

34 Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. https://www.boe.es/doue/2016/194/L00001-00030.pdf

b) aplicación del principio de "privacidad por diseño";

c) requisitos más estrictos respecto a los principios generales sobre tratamiento de datos, como el principio de proporcionalidad y de minimización de datos;

d) ampliación de la definición de datos sensibles, incluyendo los datos genéticos, biométricos, de afiliación sindical y sobre origen étnico;

e) obligación de informar sobre incidentes de seguridad;

f) reconocimiento de nuevos derechos en un contexto de decisiones algorítmicas, con impacto directo en la inteligencia artificial;

g) mayor injerencia del principio de *accountability* para los responsables de tratamiento;

h) actualización del régimen relativo a transferencia internacional de datos, e

i) nuevas atribuciones y facultades de las autoridades de control y ampliación de las bases legales para la cooperación internacional.

Además de estas dos reglas sumamente trascendentales para el derecho europeo (y para los países extracomunitarios, tanto para aquellos que ratificaron el Convenio 108+ como para los que han logrado y logren la decisión de adecuación al RGPD) y ya en tren de ajustar las recientes normativas comunitarias, se sancionaron otros reglamentos y directivas comunitarias complementarias sumamente relevantes.

Respecto de los primeros, se dictaron el Reglamento (UE) 2018/1724 relativo a la creación de una pasarela digital única de acceso a información, procedimientos y servicios de asistencia y resolución de problemas y por el que se modifica el Reglamento (UE) 1024/2012[35]; el Reglamento (UE) 2018/1725 (Gobernanza de datos) relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) nº 45/2001 y la Decisión nº 1247/2002/CE[36], en el cual se establece un Supervisor Europeo de Protección de Datos como organismo independiente de la UE que se encarga de supervisar la aplicación de las normas sobre protección de datos en las instituciones europeas y de investigar las denuncias y el Reglamento (UE) 2022/868 relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos)[37].

En cuanto a las segundas, se aprobaron la Directiva (UE) 2019/790 sobre los derechos de autor y derechos afines en el mercado único digital y por la que se modifican las Directivas 96/9/CE y 2001/29/CE[38]; la Directiva (UE) 2019/1024 relativa a los datos abiertos y

35 Reglamento (UE) 2018/1724 del Parlamento Europeo y del Consejo de 2 de octubre de 2018 relativo a la creación de una pasarela digital única de acceso a información, procedimientos y servicios de asistencia y resolución de problemas y por el que se modifica el Reglamento (UE) n. 1024/2012. https://www.boe.es/doue/2018/295/L00001-00038.pdf

36 Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) nº 45/2001 y la Decisión nº 1247/2002/CE. https://www.boe.es/buscar/doc.php?id=DOUE-L-2018-81849

37 Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo de 30 de mayo de 2022 relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos). https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-80835

38 Directiva (UE) 2019/790 del Parlamento Europeo y del Consejo de 17 de abril de 2019 sobre los derechos de autor y derechos afines en el mercado único digital y por la que se modifican las Directivas 96/9/CE y 2001/29/CE. https://www.boe.es/doue/2019/130/L00092-00125.pdf

la reutilización de la información del sector público[39]; la Directiva (UE) 2019/1937 relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión[40], la Directiva (UE) 2022/2555 (Directiva SRI2), relativa a las medidas para un elevado nivel común de ciberseguridad en toda la Unión[41], el Reglamento (UE) 2022/1925, sobre mercados disputables y equitativos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828 (Reglamento de Mercados Digitales)[42] y el Reglamento (UE) 2022/2065 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE sobre comercio electrónico (Reglamento de Servicios Digitales)[43].

Independientemente de estas normas, en 2022 la OCDE aprobó su "Declaración sobre un futuro digital fiable, sostenible e inclusivo" (OECD, 2022) y en 2023 el Parlamento Europeo, el Consejo y la Comisión aprobaron la "Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital" (2023/C 23/01)[44], donde en sus seis capítulos se propugna: a) una transformación digital centrada en las personas; b) solidaridad e inclusión; c) libertad de elección; d) participación en el espacio público digital; e) seguridad, protección y empoderamiento, y f) sostenibilidad.

La marcada preocupación que provocaron especialmente los disruptivos desarrollos que se venían gestando en el campo de la *GenAI* y en las neurotecnologías provocó que en todo el orbe se dictaran recomendaciones y regulaciones de todo tipo y fuente entre las cuales la Comisión Europea lanzó en 2018 sus "Directrices éticas para una IA fiable"[45], y más recientemente, ante la aparición en el mercado de múltiples aplicaciones que utilizan GenAI en los tratamientos, la Comisión Europea propuso un Reglamento "por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de inteligencia artificial) y se modifican determinados actos legislativos de la Unión"[46] y más recientemente, ante la aparición en el mercado de múltiples aplicaciones que utilizan GenAI en los tratamientos, la Unión

39 Directiva (UE) 2019/1024 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, relativa a los datos abiertos y la reutilización de la información del sector público (versión refundida). https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A32019L1024

40 Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo de 23 de octubre de 2019 relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión. https://www.boe.es/doue/2019/305/L00017-00056.pdf

41 Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2). https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81963

42 Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo de 14 de septiembre de 2022 sobre mercados disputables y equitativos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828 (Reglamento de Mercados Digitales) (Texto pertinente a efectos del EEE). https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32022R1925

43 Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales) (Texto pertinente a efectos del EEE). https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32022R2065

44 Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32023C0123(01)

45 Comisión Europea, Dirección General de Redes de Comunicación, Contenido y Tecnologías, Directrices éticas para una IA fiable, Oficina de Publicaciones, 2019, https://data.europa.eu/doi/10.2759/14078

46 Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión. https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX-:52021PC0206

Europea adoptó un "Reglamento de Inteligencia Artificial"[47] cuyo objetivo es introducir un marco normativo y jurídico único para los sistemas de inteligencia artificial.

La norma en cuestión se propone abordar los riesgos creados específicamente por las aplicaciones de IA; prohibir las prácticas de IA que plantean riesgos inaceptables; determinar una lista de aplicaciones de alto riesgo; establecer requisitos claros para los sistemas de IA para aplicaciones de alto riesgo; definir obligaciones específicas para implementadores y proveedores de aplicaciones de IA de alto riesgo; exigir una evaluación de conformidad antes de la puesta en servicio o la introducción en el mercado de un sistema de IA determinado; poner en marcha la supervisión después de la introducción en el mercado de un sistema de IA determinado y establecer una estructura de gobernanza a nivel europeo y nacional[48].

En concreto, los aspectos centrales de la norma se refieren a los siguientes tópicos:

1. Objetivos y ámbito de aplicación: se aplica a los sistemas de IA en el mercado de la UE o utilizados en ella, afectando tanto a proveedores como a usuarios.

2. Definición de sistemas de IA: sistemas basados en máquinas con distintos niveles de autonomía y adaptabilidad.

3. Sistemas de alto riesgo: deben cumplir criterios rigurosos de calidad y seguridad, incluyendo gestión de riesgos y transparencia para garantizar que no presenten riesgos inaceptables.

4. Prohibiciones de ciertos usos: se prohíbe, entre otros, la manipulación subliminal que pueda causar daño.

5. Supervisión y control: las autoridades nacionales y la Oficina de IA supervisarán el cumplimiento del reglamento, con facultades para investigar y sancionar.

6. Consejo de IA: compuesto por representantes de los Estados miembros, un grupo de expertos científicos para integrar a la comunidad científica y un foro consultivo para facilitar las aportaciones de las partes interesadas a la aplicación del presente Reglamento, asesorará y asistirá a la Comisión y a los Estados miembros en la aplicación coherente y eficaz de la ley.

7. Participación de expertos científicos: un grupo de expertos apoyará a la Oficina de IA en evaluación de riesgos y clasificación de modelos.

8. Espacios controlados de pruebas: se fomentará la innovación y se permitirán pruebas de sistemas de IA en un entorno regulado.

9. Transparencia y comunicación: los sistemas de alto riesgo deben proporcionar instrucciones claras a los usuarios.

10. Conservación de registros: se deben registrar automáticamente los eventos relevantes a lo largo de su ciclo de vida.

11. Evaluación de impacto de protección de datos: los responsables deben realizar tales evaluaciones de impacto.

12. Responsabilidad y sanciones: se establecen sanciones por infracciones, incluyendo multas efectivas, proporcionadas y disuasorias.

13. Apoyo a la innovación: se fomenta la innovación con espacios de pruebas y apoyo a las pymes.

---

47 Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.° 300/2008, (UE) n.° 167/2013, (UE) n.° 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial). https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ%3AL_202401689

48 Comisión Europea, Configurar el destino digital de Europa. https://digital-strategy.ec.europa.eu/es/policies/regulatory-framework-ai

14. Compatibilidad con otras normas: este Reglamento no afecta a prácticas prohibidas por otras normativas de la UE.

15. Orientación y apoyo a microempresas: a través del cumplimiento simplificado de ciertas exigencias del sistema de gestión de calidad.

16. Acceso a datos de calidad: se promueve el acceso a datos de alta calidad y la creación de repositorios de datos abiertos.

17. Confidencialidad y protección de datos: se garantiza la confidencialidad de la información y de los datos obtenidos en funciones relacionadas con la IA.

18. Interoperabilidad y estándares: se fomenta el uso de normas armonizadas y especificaciones comunes.

19. Alfabetización en IA: se promueve la alfabetización y el diseño inclusivo y diverso de los sistemas de IA.

20. Ciberseguridad: se deben cumplir con estándares de ciberseguridad para protegerse contra ataques y garantizar la integridad de los datos.

21. Capacitación: se debe incentivar la formación continua en IA para profesionales de la industria.

22. Protección contra los sesgos algorítmicos: se deben implementar mecanismos para identificar y corregir sesgos en los algoritmos, asegurando la adopción de decisiones justas.

23. Iniciativas de igualdad de género y diversidad: se promueve la aplicación de las perspectivas de género y diversidad, minimizando los sesgos y las discriminaciones.

24. Efectos sobre el empleo: se debe evaluar el impacto del empleo de la IA en el empleo y se deben desarrollar políticas para mitigar los efectos adversos, promoviendo la creación de nuevos puestos de trabajo.

25. Impacto ambiental: se fomenta el desarrollo de sistemas que contribuyan a la sostenibilidad y protección del medio ambiente.

26. Consultas públicas y participación ciudadana: se incentiva la participación de ciudadanos y organizaciones en la elaboración de políticas y normativas.

26. Responsabilidad y reparación de daños: se establecen mecanismos claros para la responsabilidad y reparación de daños causados por sistemas de IA, proporcionando vías legales para las víctimas.

27. Colaboración internacional: se impone a la UE propender a la armonización de las regulaciones con estándares internacionales, facilitando la colaboración global.

28. Entrada en vigor: la mayoría de las disposiciones entrarán en vigor a partir del 02/08/26, mientras que algunas prohibiciones lo harán desde el 02/02/25.

En las Américas, en este período se dictaron cuatro normas de *soft law* sumamente relevantes que impactan en la región.

En primer lugar, en el ámbito de la OEA los "Principios sobre la Privacidad y la Protección de Datos Personales", de 2015 fueron actualizados en 2021, reconociéndose los de: a) finalidades legítimas y lealtad; b) transparencia y consentimiento; c) pertinencia y necesidad; d) tratamiento y conservación limitados; e) confidencialidad; f) seguridad de los datos; g) exactitud de los datos; h) acceso, rectificación, cancelación, oposición y portabilidad; i) datos personales sensibles; j) responsabilidad; k) flujo transfronterizo de datos y responsabilidad; l) excepciones al régimen y m) autoridades de protección de datos independientes.

En segundo término, y ya en el plano de las autoridades nacionales de control reunidas en la Red Iberoamericana de Protección de Datos (RIPD), en 2017 se aprobaron los "Están-

dares de protección de datos personales para los estados iberoamericanos"[49], los que siguen esencialmente el molde del Reglamento General de Protección de Datos de la Unión Europea, aunque no se reconocen exactamente los mismos derechos (v.gr., no incluye el "derecho al olvido", cuya compatibilidad con el sistema interamericano ha sido puesta en duda por la Relatoría de Libertad de Expresión de la Comisión IDH).

En tercer lugar y cuarto lugar, también en 2019, la RIPD aprobó conjuntamente dos documentos muy significativos. El primero, sus "Recomendaciones generales para el tratamiento de datos en la inteligencia artificial" (RIPD, 2019a), que alude en concreto a las siguientes: a) cumplir con las normas locales sobre tratamiento de datos personales; b) efectuar estudios de impacto de privacidad; c) incorporar la privacidad, ética y seguridad desde el diseño y por defecto; d) materializar el principio de responsabilidad demostrada (*accountability*); e) diseñar esquemas apropiados de gobernanza de tratamiento de datos personales en las organizaciones que desarrollan productos de IA; f) adoptar medidas para garantizar los principios del tratamiento de datos personales en los proyectos de IA; g) respetar los derechos de los titulares de datos e implementar mecanismos efectivos para el tratamiento de los mismos; h) asegurar la calidad de los datos personales; i) utilizar herramientas de anonimización, y j) incrementar la confianza y la transparencia con los titulares de datos personales. El segundo, complementando estas recomendaciones, aprobó sus "Orientaciones específicas para el cumplimiento de los principios y derechos que rigen la protección de los datos personales en los proyectos de inteligencia artificial" (RIPD, 2019b).

A la preocupación generada por los tratamientos de datos por los crecientes y cada vez más complejos sistemas de inteligencia artificial se agregó recientemente la necesidad de reconocer nuevos derechos frente al desarrollo de las neurotecnologías, que actualmente permiten intervenir en el cerebro con la implantación de neurodispositivos intracraneales con múltiples posibilidades de brindar beneficios terapéuticos, pero que a la vez conllevan riesgos concretos para las personas tanto por la manipulación de las habilidades cognitivas como por el indebido tratamiento de sus datos neuronales y de toda la información que puede ser inferida a través de la actividad cerebral captada.

Así, como lo refiere doctrina autorizada:

> Son varios países, organizaciones internacionales y organismos regionales, como se verá más adelante, los que han adelantado varias iniciativas de neuroderechos. Al respecto, Chile, Brasil, Argentina, España, Francia y México son algunos ejemplos de Estados que han adoptado, o están adelantando, proyectos al respecto. A nivel internacional, la Organización de Naciones Unidas, en sede de la UNESCO y la Asamblea General, ha adelantado y encomendado estudios en materia de neurociencias y derechos humanos. En organismos regionales, por su parte, la Organización de Estados Americanos, y particularmente el Comité Jurídico Interamericano, ha realizado declaraciones y emitido unos principios interamericanos en la materia. Por último, el Parlamento Latinoamericano y Caribeño (en adelante Parlatino), promulgó una Ley Modelo para que los países miembros cuenten con las bases para legislar en dicha materia (Borbón et al., 2023, 230).

A esto cabe agregar que en 2021 Chile reformó en su constitución, incorporando a su art. 19, inc. 1 una regla -la primera de ese rango en el mundo- por la cual se dispone: "El de-

49 Estándares de protección de datos personales para los Estados Iberoamericanos. https://www.redipd.org/es/documentos/estandares-iberoamericanos

sarrollo científico y tecnológico estará al servicio de las personas y se llevará a cabo con respeto a la vida y a la integridad física y psíquica. La ley regulará los requisitos, condiciones y restricciones para su utilización en las personas, debiendo resguardar especialmente la actividad cerebral, así como la información proveniente de ella" y que en la "Ley Modelo de Neuroderechos para Latinoamérica y el Caribe" emitida por el Parlatino en 2023[50], se reconocen los derechos a: a) la privacidad mental; b) la identidad y autonomía personal; c) el libre albedrío y la autodeterminación; d) el acceso equitativo a la aumentación cognitiva o al desarrollo cognitivo; e) la protección de sesgos de algoritmos o procesos automatizados de toma de decisiones; f) no ser objeto de cualquier forma de intervención de las conexiones neuronales o cualquier forma de intrusión a nivel cerebral mediante el uso de neurotecnología, interfaz cerebro computadora o cualquier otro sistema o dispositivo, sin contar con el consentimiento libre, expreso e informado, de la persona o usuario del dispositivo, inclusive en circunstancias médicas, y g) no ser sujeto involuntario o no informado, de cualquier proceso o actividad que pueda de alguna manera interferir en los procesos cognitivos del individuo.

Ya pasando a los ámbitos nacionales, en los Estados Unidos si bien a nivel federal hasta el momento sólo existen proyectos para la adopción de una norma general de protección de datos al estilo europeo, en 2018 se aprobó la "Ley de Clarificación del Uso de Datos en el Extranjero" (*CLOUD Act*) que modifica las leyes de vigilancia informática, facilitando el acceso de las agencias de seguridad a los contenidos de las comunicaciones electrónicas y otros datos relacionados, incluso almacenados en el extranjero, permitiendo a los proveedores de servicios de internet norteamericanos colaborar con los procesos y órdenes judiciales del exterior que requieran datos de comunicaciones almacenados en el país, en la medida en que el de origen haya celebrado un acuerdo con los Estados Unidos.

En el plano de los estados federados, han dictado normas generales sobre protección de datos y privacidad o respecto del consumidor: Nevada (2017, con reformas en 2019 y 2021), California ("California Consumer Privacy Act" vigente desde 2020 y reformada por la "California Privacy Rights Act", vigente desde 2023), Colorado ("Colorado Privacy Act" vigente desde 2023), Delaware ("Delaware Personal Data Privacy Act", vigente desde 2025), Indiana ("Indiana Consumer Data Protection Act", vigente desde 2026), Iowa ("Iowa Consumer Data Protection Act", vigente desde 2025), Kentucky ("Kentucky Consumer Data Protection Act", vigente desde 2026), Montana ("Montana Consumer Data Privacy Act", vigente desde 2024), Nebraska ("Nebraska Privacy Act", vigente desde 2025), New Hampshire (SB 255, vigente desde 2025), New Jersey (SB 332, vigente desde 2025), Oregon ("Oregon Consumer Privacy Act", vigente desde 2024), Tennessee ("Tennessee Information Protection Act", vigente desde 2025), Texas ("Texas Data Privacy and Security Act", vigente desde 2025), Utah ("Utah Consumer Privacy Act", vigente desde 2023), y Virginia ("Virginia Consumer Data Protection Act" vigente desde 2023).

En el Caribe se han aprobado leyes en Bermuda (2016), Islas Cayman (2017) y Saint Kitts & Nevis (2018), y ya en el ámbito latinoamericano se destaca en este período la adopción de normas constitucionales en Chile (2018, art. 19, inc. 4 y reforma de 2021, art. 19, inc. 1) y Cuba (2019, art. 97), y en el plano legal las leyes emitidas en México (2017), Brasil (2018), Panamá (2019), Paraguay (2020) y Ecuador (2021).

50 Ley modelo de neuroderechos para América Latina y el Caribe. https://parlatino.org/wp-content/uploads/2017/09/leym-neuroderechos-7-3-2023.pdf

5. Conclusiones

La sucesión de las etapas habidas en el constitucionalismo tuvo, sin duda alguna, un importante impacto en la evolución de las generaciones de derechos humanos, donde si bien su mayor desarrollo se verificó particularmente a partir del ingreso al constitucionalismo internacional, a mediados del siglo pasado, se hizo mucho más patente a partir del "constitucionalismo de la 5ª Revolución industrial", donde los avances tecnológicos provocaron, entre muchos otros efectos, la aparición de los "derechos digitales" y dentro de ellos, del derecho a la protección de datos, áreas en las que, especialmente en lo que va del siglo, han fructificado en numerosos derechos y principios –en buena parte "técnicos"- tendientes tanto a preservar a las personas de los efectos perniciosos de las nuevas tecnologías como a gozar efectivamente y sin discriminación alguna de los beneficios de éstas, lo que actualmente tiene un campo de acción fecundo por ejemplo, en lo que atañe a la GenIA y a los neuroderechos. Este trabajo pretendió mostrar esas evoluciones y sus principales productos, objetivo que esperamos haber alcanzado satisfactoriamente.

6. Referencias

Agencia Española de Protección de Datos (2009). *Estándares internacionales sobre protección de datos personales y privacidad. Resolución de Madrid*. https://www.edps.europa.eu/sites/default/files/publication/09-11-05_madrid_int_standards_es.pdf

Bidart Campos, G. J. (1991). Repensando las garantías constitucionales. *La Ley*, B–977/978.

Borbón, D., Borbón, L., Mora-Gómez, X., & Villamil-Mayoral, S. (2023). El preocupante clausulado de la Ley Modelo de Neuroderechos del Parlatino. *Ius et scientia*, *9*(2). https://doi.org/10.12795/IESTSCIENTIA.2023.i02.11

Carranza Torres, L. (2001). *Hábeas data: la protección jurídica de los datos personales*. Alveroni Ediciones.

Comité Jurídico Interamericano (2015). Guía legislativa sobre la privacidad y la protección de datos personales en las Américas (Adoptada por el Comité Jurídico Interamericano). https://www.oas.org/es/sla/ddi/docs/proteccion_datos_personales_Guia_Legilsativa_CJI.pdf

Council of Europe (2001). *Protocolo adicional al convenio para la protección de las personas con respecto al tratamiento automatiado de datos de carácter personal, a las autoridades de control y a los flujos transfronterizos de datos*. STE 181. https://rm.coe.int/16806c1abe

Council of Europe (2001). *Convenio del Consejo de Europa sobre el acceso a los documentos públicos*. Council of Europe. https://www.oas.org/es/sla/ddi/docs/acceso_informacion_desarrollos_convenio_consejo_europeo.pdf

Cumbre Iberoamericana (2003). *Declaración de Santa Cruz de la Sierra*. XIII Cumbre Iberoamericana de jefes de estado y de gobierno. 14 y 15 de noviembre de 2003. https://www.segib.org/wp-content/uploads/DeclaraciondeSantaCruz.pdf

Estadella Yuste, O. (1995). *La protección de la intimidad frente a la transmisión internacional de datos personales*. Tecnos.

Fappiano, Ó. L. (1998). *Hábeas data: una aproximación a su problemática*. En: *Liber Amicorum: Héctor Fix Zamudio* (pp. 643 y 666). Corte Interamericana de Derechos Humanos.

Lázpita Gurtubay M. (1994). Análisis comparado de las Legislaciones sobre Protección de Datos de los Estados Miembros de la Comunidad Europea. *Informática y derecho: Revista iberoamericana de derecho informático*, 6-7, 394-420. https://dialnet.unirioja.es/descarga/articulo/248383.pdf

Organización de los Estados Americanos (2021). *Principios actualizados sobre la privacidad y la protección de datos personales*. Departamento de Derecho Internacional, Secretaría de Asuntos Jurídicos de la OEA. https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf

OECD (2013). *Recommendation of the Council concerning guidelines governing the protection of privacy and transborder flows of personal data*. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188

OECD (2022). *Declaración sobre un futuro digital fiable, sostenible e inclusivo*. https://legalinstruments.oecd.org/api/download/?uri=/public/f347ae7c-4e38-4e7a-8d29-af489cffb84e.pdf

Pitt, W. (1806-1820). Speech on the Excise Bill. In: T. C. Hansard (ed.). *The Parliamentary History of England from the Earliest Period to the Year 1803*, 23 vols., London, vol. 15 (1753-1765), pág. 1307.

Red Iberoamericana de Protección de Datos (2017). *Estándares de protección de datos personales*. RIPD. https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf

Red Iberoamericana de Protección de Datos (2019a). *Recomendaciones generales para el tratamiento de datos en la Inteligencia Artificial.* RIPD. https://www.redipd.org/sites/default/files/2020-02/guia-recomendaciones-generales-tratamiento-datos-ia.pdf

Red Iberoamericana de Protección de Datos (2019b). Orientaciones específicas para el cumplimiento de los principios y derechos que rigen la protección de los datos personales en los proyectos de Inteligencia Artificial. RIPD. https://www.redipd.org/sites/default/files/2020-02/guia-orientaciones-espec%C3%ADficas-proteccion-datos-ia.pdf

Sagüés, N. P. (2007). *Manual de Derecho Constitucional*. Astrea, Buenos Aires.

Warren, S., & Brandeis, L. (1890). *The right to privacy*. Harvard Law Review, *4*(5), 193–220. https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf