INTERNATIONAL JOURNAL OF DIGITAL LAW – IJDL
ano 04 · n. 03 · setembro/dezembro 2023 – Publicação quadrimestral
DOI: 10.47975/digital.law.vol.4.n.3

04

ISSN 2675-7087

IJDL

International Journal of DIGITAL LAW

NUPED
Núcleo de Pesquisas em Políticas Públicas e Desenvolvimento Humano da PUCPR

FORUM

IJDL – INTERNATIONAL JOURNAL OF DIGITAL LAW

NUPED
Núcleo de Pesquisas em Políticas Públicas e Desenvolvimento Humano da PUCPR

FORUM
Luís Cláudio Rodrigues Ferreira
Presidente e Editor

Rua Paulo Ribeiro Bastos, 211 – Jardim Atlântico – CEP 31710-430
Belo Horizonte/MG – Brasil – Tel.: (31) 99412.0131
www.editoraforum.com.br / E-mail: editoraforum@editoraforum.com.br

Impressa no Brasil / Printed in Brazil / Distribuída em todo o Território Nacional

IN61 International Journal of Digital Law – IJDL. – ano 1, n. 1 (abr. 2020) –.– Belo Horizonte: Fórum, 2020-.

Quadrimestral; Publicação eletrônica
ISSN: 2675-7087

1. Direito. 2. Direito Digital. 3. Teoria do Direito. I. Fórum.

CDD: 340.0285
CDU: 34.004

Coordenação editorial: Leonardo Eustáquio Siqueira Araújo
Aline Sobreira
Capa: Igor Jamur
Projeto gráfico e diagramação: Walter Santos
Revisão: Nathalia Campos

DOI: 10.47975/digital.law.vol.4.n.3.rosarodriguez

Gobernanza de datos, herramientas digitales en el mundo del trabajo y la economía: análisis del régimen legal y sus perspectivas

Data governance, digital tools in the world of labor and economy: Analysis of the legal framework and its perspectives

Ana Rosa Rodriguez*
[I]Universidade Positivo (Curitiba, Paraná, Brasil)
anarosaunse1@gmail.com
https://orcid.org/0000-0002-4156-625X

Recebido/Received: 28.01.2024/January 28th, 2024
Aprovado/Approved: 19.02.2024/February 19th, 2024

Resumen: El presente artículo se propone describir el escenario global actual en materia de regulaciones sobre datos personales analizando la relación entre ellos y las herramientas tecnológicas, modelos de negocios basados en procesamientos de macrodatos y el mundo del trabajo. La creciente importancia de los datos en el ámbito laboral y económico ha generado la necesidad de un enfoque riguroso en términos de regulación y protección explorando las vías para optimizar el uso de las herramientas digitales en el entorno laboral con el objetivo de promover la innovación y el crecimiento económico mientras se garantiza la protección de los derechos individuales y la privacidad de los datos. Se analizan los marcos regulatorios vigentes a nivel global con implicancia importantes para las políticas públicas y las estrategias empresariales en la era digital.

Como citar esse artigo/How to cite this article: RODRIGUEZ, Ana Rosa. Gobernanza de datos, herramientas digitales en el mundo del trabajo y la economía: análisis del régimen legal y sus perspectivas. *International Journal of Digital Law – IJDL*, Belo Horizonte, ano 4, n. 3, p. 11-41, set./dez. 2023. DOI: 10.47975/digital.law.vol.4.n.3.rosarodriguez.

* Profesora Asociada Regular de la Facultad de Humanidades, Ciencias Sociales y de la Salud de la Universidad Nacional de Santiago del Estero y Profesora Adjunta de la Universidad Católica de Santiago del Estero. Doctora en Derecho del Trabajo por la Universidad Nacional de Tres de Febrero. *E-mail*: anarosaunse1@gmail.com.

Palabras-clave: Datos personales. Trabajo. Economía digital. Gobernanza. Regulación. Protección.

Abstract: This article aims to describe the current global scenario regarding regulations on personal data by analyzing the relationship between them and technological tools, business models based on big data processing, and the world of work. The growing importance of data in the labor and economic spheres has generated the necessity of a rigorous approach in terms of regulation and protection, exploring pathways to optimize the use of digital tools in the workplace with the aim of promoting innovation and economic growth while ensuring the protection of individual rights and data privacy. Current regulatory frameworks at the global level are analyzed with significant implications for public policies and business strategies in the digital era.

Keywords: Personal data. Work. Digital economy. Governance. Regulation. Protection.

1 Introducción: datos personales, IA y empresas

El siglo XXI se distingue por la importancia creciente de las decisiones automatizadas, basadas en aplicaciones de Inteligencia Artificial (IA), que, con o sin intervención humana decisoria, producen efectos relevantes sobre las personas en el ámbito económico, social y jurídico. Vivimos inmersos en una economía donde los datos incluyendo los de carácter personal constituyen uno de los principales insumos para las empresas.

El análisis de macrodatos, a través de sistemas de aprendizaje automático, ha facilitado la creación de perfiles, ha automatizado las decisiones en amplios sectores de la actividad recopilando grandes volúmenes de información que son la base de varias tecnologías que están profundizando cada vez más, la información que se puede extraer de carácter personal.

Luego hay una convergencia en toda la tecnología la que, cada vez es más próxima y conectada. Una revolución que ya está ocurriendo a través del 5g unido al internet de las cosas y, al número de dispositivos conectados que, al día de hoy, se ha calculado tres veces la población mundial – o era la proyección para el 2020. Si combinamos esa conectividad con la capacidad de procesamiento de datos se advierte, un aumento exponencial de información que a modo de detalle ahora está siendo medida en *zetabytes*.[1]

[1] Unidad de almacenamiento de información cuyo símbolo es ZB, equivale a 1021 *bytes*.

La economía del conocimiento[2] de la que hoy se habla corrientemente se basa en el procesamiento automatizado de grandes volúmenes de datos, permitiendo a quienes la operan conocer nuestras preferencias, intereses y deseos incluso antes que nosotros mismos. Ello nos lleva a pensar que es muy probable que empresas como Google ya tengan información sobre nuestras futuras decisiones, como el destino de nuestros viajes, antes de que lo hayamos decidido o pensado conscientemente.

Estos modelos de negocio, impulsados por un procesamiento masivo de datos, se multiplican de manera exponencial gracias a nuevas tecnologías ya disponibles o próximas a lanzarse, como la Inteligencia Artificial (IA), la computación cuántica, el Internet de las Cosas (IoT) y la biotecnología.

El panorama, al menos en apariencia, resulta auspicioso por las ventajas que promete en áreas como la medicina, la ingeniería, la biología y el entretenimiento, pero también genera preocupación debido a los diversos riesgos, a menudo desconocidos, a los que estos cambios nos exponen.

Ante esta dualidad, surge un desafío global crítico: desarrollar y actualizar periódicamente normas y procedimientos que aseguren un uso adecuado de nuestros datos personales. Además, es fundamental establecer mecanismos efectivos para supervisar su implementación, con el objetivo urgente de controlar los avances tecnológicos y prevenir escenarios distópicos donde los humanos nos encontremos a merced de máquinas sin control.

No hay una solución única, para establecer un contexto real en el ejercicio del derecho a la privacidad, y la protección efectiva de los datos personales en un escenario complejo y dinámico.

A su vez, el tratamiento de datos personales en el ámbito del trabajo constituye una realidad incontestable marcada por la necesidad de gestionar, desde múltiples puntos de vista, las relaciones laborales existentes en el seno de las empresas, así como en el Estado garante principal de los derechos a la intimidad y a la privacidad.

Los avances tecnológicos en la gestión del personal y la protección de datos personales de los trabajadores dan cuenta que resulta un hecho evidente la progresiva incorporación de las nuevas tecnologías informáticas y de la información en la empresa de todo tamaño y condición, cambiando de forma sustancial los modos y modelos de trabajo.

---

[2] Muchos países de Latinoamérica, entre ellos Argentina, tienen un régimen de promoción de la economía del conocimiento, cuyo objetivo es "promocionar actividades económicas que apliquen el uso del conocimiento y la digitalización de la información apoyado en los avances de la ciencia y de las tecnologías, a la obtención de bienes, prestación de servicios y/o mejoras de procesos" (REPÚBLICA ARGENTINA. Ley nº 27.506, de 10 de junio de 2019. Régimen de promoción de La economía del conocimiento. *Gobierno de Argentina*: Buenos Aires, 2019. Disponible en: https://www.argentina.gob.ar/normativa/nacional/ley-27506-324101/actualizacion. Acceso el: 15 dic. 2023).

No tan evidente resulta, en cambio, que la aplicación de aquellas tecnologías esté siendo llevada a cabo con el debido respeto a bienes y valores jurídicamente relevantes y consagrados en preceptos constitucionales y legales.

2 Desarrollo

2.1 Marco regulatorio complejo y dinámico

En la medida en que se fueron consolidando los ordenamientos jurídicos y se aumentó la preocupación por los temas de privacidad surgieron distintas alternativas a la hora de elegir cuáles son los mecanismos más adecuados para facilitar la circulación de la información y de los datos con el menor coste para los derechos individuales resultando importante proteger a las personas del abuso de vigilancia que constituye un riesgo, que cada vez se acentúa más, en la sociedad informatizada, donde toda información relativa a los ciudadanos/as es archivada electrónicamente de manera entrecruzada por medio de los diversos bancos de datos del fisco, de las empresas y de las asociaciones a las que está relacionado.

Así a nivel mundial podemos distinguir tres bloques de países en materia normativa: el bloque europeo, con países con fuerte inspiración en el derecho europeo continental – entre los que se enrolan los de la región Latinoamericana encontrando en ese grupo a la Argentina – donde el dato personal se considera un derecho fundamental con importantes implicancias; el bloque Canadá-EEUU, una potencia mundial a nivel tecnológico, con una visión más transaccional, donde el derecho a la privacidad no es considerado como un derecho irrenunciable e inalienable, sino que se puede negociar con él; y finalmente el tercer bloque "otros" ordenamientos jurídicos no occidentales, en el cual existen dudas respecto al uso que hace el Estado de los datos personales.

El ataque a las Torres Gemelas ocurrido en septiembre de 2001 determinó a los Estados Unidos dictar la USA Patriot Act,[3] o Ley Patriota, producto de un proceso acelerado de 30 días, ley que permite a su gobierno, entre otras cosas, tener acceso a información de personas y empresas con propósitos de seguridad nacional y exige a las empresas estadounidenses, sin ningún trámite burocrático o juicio, que entreguen información de las bases de datos que tienen bajo custodia. Se trata de una legislación a la cual las empresas no se pueden oponer, por lo que si la Central Intelligence Agency (CIA), el Federal Bureau of Investigation (FBI) o la National Security Agency (NSA) hacen algún requerimiento, el titular de los datos

[3] EEUU. *Act No. 56, Oct. 26, 2001*. Uniting And Strengthening America By Providing Appropriate Tools Required To Intercept And Obstruct Terrorism (Usa Patriot Act) Act Of 2001. Washington D.C., 6 Oct. 2001. Disponible en: https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.htm. Acceso el: 12 nov. 2023.

ni siquiera se va a enterar, lo cual constituye en los hechos un "toque de queda informático" que institucionaliza la unilateralidad y el monopolio digital del gobierno estadounidense.

Es el mismo criterio que sigue en el mismo país la Cloud Act[4] también conocida como "ley de la nube" que a pesar de estar en su nombre no regula la estructura de la nube sino más bien acerca de la protección de los datos en ella almacenados. Esta norma. de gran impacto sobre la privacidad de los ciudadanos y las empresas de la U.E., data del año 2018 y exige a los proveedores de servicios estadounidenses que revelen todos los datos que se encuentren bajo su posesión, custodia o control si son solicitados por las autoridades. Esta disposición también es aplicable respecto de los datos alojados en terceros países.

En este punto resulta importante señalar que existe una verdadera puja entre China y E.E.U.U. por ocupar una posición hegemónica en tecnología a nivel mundial, y uno de los temas de base es quién accede o quién tiene el control, no de los datos personales – que están en el paquete – sino que en estos países lo más importante tiene que ver con temas de soberanía nacional o seguridad. China es un ejemplo emblemático. En agosto de 2021 en forma sorpresiva China ha dictado su normativa de protección de datos personales que entró en vigencia en noviembre de ese mismo año con la impronta del GDPR de la UE.

El Reglamento Europeo de Protección de Datos (G.D.P.R.)[5] dictado en 2016 y entró en vigencia en 2018, es un reglamento general que básicamente ha establecido los requisitos comunes que luego han inspirado fuertemente las legislaciones en Argentina y la Lei Geral de Proteção de Dados[6] (Ley General de Protección de Datos) en Brasil con una visión de servicios de tecnología y la información en relaciones y B2B[7] de vital importancia a la hora de elegir cuáles son los mecanismos más adecuados para poder transferir información de un país a otro, así como los retos que enfrentan las empresas que operan en varios países en términos de: ¿qué metodología se utiliza para intentar capturar los datos que se están procesando? ¿desde dónde? ¿cuáles son las herramientas que utilizamos léase por herramientas

4 EEUU. *S.2383*. Ley de la Nube Cloud Act. Enmendar el título 18 del Código de los Estados Unidos para mejorar el acceso de las fuerzas del orden a los datos almacenados a través de fronteras y para otros fines, [2023]. Disponible en: https://www.congress.gov/bill/115th-congress/senate-bill/2383/text. Acceso el: 12 nov. 2023.

5 UNIÓN EUROPEA. *Reglamento nº 679/2016*. Relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. DOUE L 119. Bruselas: Unión Europea, 4 mayo 2016.

6 BRASIL. Lei Federal nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. *Diário Oficial da União*: Brasília, DF, 2018. Disponible en: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2349685. Acceso el: 2 oct. 2023.

7 BTB son las siglas correspondientes a una expresión de origen anglosajón que es *business to business*. Este término se emplea en los sectores del comercio y del marketing. Hace referencia a las operaciones de compra y de venta que se realizan entre empresas.

bases legales de acuerdo con la normativa aplicable para poder implementar una transferencia de datos personales sin violar derechos ni principios fundamentales que los protegen?

2.2 Trabajo y datos

Hace mucho tiempo se afirma que nuestra identidad está profundamente vinculada al trabajo y, al abordar la problemática de la protección de los datos personales en general y la de los trabajadores en particular, se ha sostenido reiteradamente la íntima e imprescindible relación entre los datos personales y la identidad misma de la persona. El tema acredita su vital relevancia, al igual que todo lo relacionado a su obtención, conservación, almacenamiento, adaptación o modificación, extracción, consulta, cotejo o interconexión, limitación, evaluación, bloqueo, supresión, destrucción, difusión, y cesión a terceros.

Estas operaciones y procedimientos – denominado tratamiento de datos personales – no constituye de ninguna manera un fenómeno reciente pues, desde tiempos remotos la tenencia de información permitió la generación de un poder que durante siglos fue canalizado con fines políticos, militares o económicos.

Como lo afirma Crawford[8] a menudo se habla de la automatización del trabajo como una historia futurista cuando bien se trata de una realidad largamente establecida en el trabajo contemporáneo. Entre los ejemplos que cita la autora refiere al trabajo que denomina *"secretarial"* advirtiendo que dicho trabajo se ha automatizado desde la década de 1980 y ahora es emulado por asistentes de IA – femeneizados – como Siri y Alexa.

Refiere la autora que los empleados que aún hoy se sienten menos amenazados por la automatización están cada vez más sujetos a ser vigilados en su lugar de trabajo, a la automatización de proceso y a la falta de distinción entre lo que es trabajo y el goce del tiempo libre.

Este escenario de profundización de automatización de procesos y de vigilancia en los lugares de trabajo se viene profundizando por la irrupción de una lógica en la que actualmente se encuentra invadido el sector tecnológico: la creencia inquebrantable de que cualquier cosa puede ser un dato, y de que los datos están ahí para los tome quien quiera.

En el contexto del mundo laboral resulta determinante la salvaguarda de los derechos fundamentales de las personas físicas trabajadoras en relación con el tratamiento de sus datos personales, de sus datos sensibles, así como el respeto al derecho a la intimidad y a la igualdad enlazándose con la prohibición de

[8] CRAWFORD, Kate. *Atlas de Inteligencia Artificial*. Poder, política y costos planetarios. Buenos Aires: Fondo de Cultura Económica, 2022.

discriminación, por lo que debe seguir siendo una prioridad frente a las decisiones automatizadas que puedan virtualmente menoscabarlos.

Las decisiones automatizadas tienen el potencial de incidir de manera significativa en los derechos y libertades individuales, así como en su utilidad para las organizaciones al proporcionar respuestas eficientes con ahorro de costos. No obstante, la conveniencia económica no debe eclipsar los riesgos inherentes a estos procesos para los derechos de las personas afectadas.

Una célebre anécdota que algunos tildan de apócrifa involucra a Henry Ford II, presidente de Ford Motor Company, y al líder sindical Walter Reuther. La anécdota se sitúa en la década de 1940, cuando el histórico líder sindical, quien lideraba el sindicato United Auto Workers (UAW), realizaba una visita y recorrido alrededor de una moderna planta de producción de automóviles.

Se dice que Ford II, queriendo impresionar a Reuther con la eficiencia de la fábrica, le preguntó: "¿Cómo vas a conseguir que los robots te paguen la cuota del sindicato?". La respuesta ingeniosa de Reuther fue: "¿cómo vas a conseguir que los robots te compren los autos?"

La historia destaca una cuestión de fondo – que, como decía Crawford, no es un relato futurista sino la realidad nuestra de todos los días – la automatización puede aumentar la eficiencia y la productividad, pero también amenaza las bases mismas del sistema que dependerá de la capacidad de consumo de las personas. Esta anécdota se ha utilizado a lo largo del tiempo además para ilustrar la importancia de la participación de los empleados en la toma de decisiones y la resolución de problemas en el entorno laboral.

El impacto de la automatización de procesos, la robótica y la Inteligencia Artificial tienen el potencial de resultar una amenaza para millones de puestos de trabajo de afectar algunos sectores productivos, con la preocupación de lo que ocurrirá con los y las trabajadoras de tareas rutinarias en sectores que se verán más afectados por estos cambios, generando desempleo y/o precarización laboral.

Este complejo escenario reduce aún más la facultad negocial en manos de los trabajadores y trabajadoras lo que interpela aún más en la necesidad de regular minuciosamente la potestad de la privacidad en cabeza de la persona trabajadora y el control tecnológico de la actividad laboral y vigilancia en manos del empresario a partir de la utilización de las TICs en el seno de las empresas proporcionando a ambos reglas claras y proporcionadas, lo que unido a los inconvenientes derivados de la indeterminación de la normativa heterónoma generan mayor vulnerabilidad y desprotección de los derechos fundamentales.

La protección de datos personales se ha convertido en un derecho humano fundamental en aquellos países que – siguiendo el modelo del derecho europeo-continental – priorizan la privacidad y los intereses individuales de los ciudadanos

y ciudadanas por encima de las ganancias y desarrollo de las empresas o por sobre funcione confiadas a los Estados en campos como la seguridad, la justicia, la salud pública y el sistema financiero, entre otros en los que el interés público puede erosionar el derecho a la privacidad de los datos.

Las organizaciones aplican las normas generales de protección de datos aggiornándolas a las relaciones laborales. Es, por ello, particularmente relevante tener en cuenta, como han venido recomendado los órganos consultivos internacionales en materia de protección de datos, que la legislación sobre protección de datos no debe aplicarse de forma independiente del Derecho del Trabajo y las prácticas laborales y que éstos, a su vez, no pueden aplicarse aisladamente, sin tener en cuenta la legislación sobre protección de datos. Esta interacción es necesaria y valiosa y debe contribuir al desarrollo de soluciones que protejan adecuadamente los intereses de los trabajadores.

Ahora bien, a esta altura surgen algunos interrogantes conceptuales que es necesario puntualizar.

¿Qué son los datos? ¿Cuándo un dato se convierte en Información? ¿Cuáles datos deben ser protegidos con más celo que otros? Para responder estos interrogantes se propone aclarar los conceptos que siguen. Se definen como Datos Simples a toda entidad de carácter objetivo, que resultan de la representación de hechos en la forma de palabras, números o letras. Son ejemplos de datos simples, el nombre el domicilio etc. que sirve para identificar a la persona. Asimismo, se entiende por Información al resultado del procesamiento organizado de datos del cual se obtiene un significado, el procesamiento convierte a los datos en información útil e involucra actividades, equipamiento y sujetos. Por su parte, se consideran Datos Personales cualquier información concerniente a una persona física (humana) identificada o identificable. En ese sentido el G.D.P.R. define a los “datos personales”:

> (…) toda información sobre una persona física identificada o identificable (“el interesado”); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

Dentro de los datos personales pueden a su vez distinguirse los datos sensibles, definidos por las legislaciones como aquellos datos que afectan la esfera más íntima de su titular, cuya utilización indebida puede dar origen a discriminación o

conlleve un grave riesgo para ello. A modo de ejemplo puede señalarse aquellos que revelan aspectos como el origen étnico racial estado de salud presente y futuro información genética creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas preferencia sexual, entre otros. Los anteriores difieren de los denominados datos biométricos que son aquellas propiedades biológicas, características fisiológicas, rasgos de la personalidad o tics atribuibles a una persona que son mensurables. A su vez los datos biométricos suelen clasificarse en estáticos y dinámicos. Los estáticos, entre los que se puede enumerar las huellas digitales, geometría de la mano, análisis del iris o la retina, el reconocimiento facial o del diafragma, análisis de ADN. En tanto los datos biométricos dinámicos: son tales como la firma manuscrita, la pulsación sobre las teclas, el análisis de la forma de caminar y el gestual.[9]

Los datos sensibles que requieren una preferente tutela son los datos de los niños y niñas y los biométricos los que deben ser resguardados por todas las legislaciones y cuya gobernanza no puede quedar librado al arbitrario de las empresas y el fomento de su desarrollo, sino que por el contrario deben quedar en la órbita de las funciones típicas confiadas a los Estados.

El contemporáneo Yuval Noa Harari,[10] renombrado escritor e historiador israelí, ilustra hábilmente la realidad que hoy nos rodea:

> En marzo de 2018, yo preferiría dar mis datos a Mark Zuckerberg que a Vladimir Putin (aunque el escándalo de Cambrige Analytica revelo que quizá no tengamos mucha elección, pues cualquier dato que confiemos a Zuckerberg bien podría acabar llegando a Putin)… Pero no tenemos mucha experiencia en regular la propiedad de los datos que es en sí misma una tarea mucho más difícil porque a diferencia de la tierra y de las máquinas, los datos están por todos lados y en ninguna parte al mismo tiempo, pueden desplazarse a la velocidad de la luz y podemos crear tantas copias de ellos como queramos.

Para el autor citado el misterio y el interrogante más importante de nuestra era resulta ser: ¿cómo regulamos la propiedad de los datos? Sugiere que lo mejor que se puede hacer en este momento es recurrir a abogados, políticos filósofos e incluso a poetas para que desentrañen el misterio.

---

9 El análisis gestual analiza e interpreta los gestos micro movimientos y actitudes corporales que se realizan de manera involuntaria. La *sinergología* es la disciplina que estudia la comunicación no verbal no consciente mediante la decodificación interpreta los gestos, y tiene como objetivo comprender mejor al interlocutor mediante el análisis y observación del lenguaje corporal (PALERMO, J. D. *¿Qué es la sinergología y cómo aplicarla a mi empresa?* [*S. l.*]: [*s. n.*], [2023]. Disponible en: https://www.elobservatoriodeltrabajo.org/que-es-la-sinergologia-y-como-aplicarla-a-mi-empresa/. Acceso el: 1 oct. 2023).

10 HARARI, Y. N. *21 lecciones para el siglo XXI*. Buenos Aires: Debate, 2023. p. 103.

Teniendo en cuenta las reflexiones precedentes, es posible considerar que una solución efectiva para restablecer un contexto real en el ejercicio del derecho a la privacidad debería contener una combinación de medidas que contribuya a mejorar significativamente la protección de la privacidad en un entorno digital en constante cambio, es decir hacer converger el impulso a la innovación y al desarrollo económico con la garantía de derechos teniendo en cuenta que, las transferencias internacionales de datos personales reviste vital importancia para el comercio internacional, para promover la economía digital.

De esta manera adoptar estándares internacionales significa que partir de una mirada situada y soberana al momento de suscribirlos lo que no significa necesariamente que uniformidad es decir estar de acuerdo en todo, pero sí contar con herramientas interoperables en un mundo donde la economía digital ha avanzado exponencialmente.

Existe un debate en la comunidad científica acerca de la conveniencia o no de la excesiva regulación de la tecnología por sus posibles efectos en su investigación, desarrollo e innovación. La aprobación del Reglamento de la Unión Europea ha profundizado este debate que según algunos tiene un sustrato ideológico y es el de que para que se garantice la innovación cuanta menos regulación, mejor.

Es difícil concebir Internet, ni las tecnologías de software incluyendo la Inteligencia Artificial que le sirven de soporte, sin promover la adopción de normas internacionales y estándares que aborden los desafíos actuales en la protección de la privacidad, proporcionando un marco más consistente a nivel global.

Será importante lograr consensos entre las distintas comunidades de grupos de interés (*stakeholders*) fabricantes, operadores, industria, gobiernos, clientes potenciales a la par que, las distintas organizaciones, lancen independientemente sus productos al mercado y que el mercado motorice el consenso en línea con la preferencia de los consumidores.

En las páginas que siguen se analizan algunos sistemas normativos relevantes con especial tratamiento a la legislación vigente en Argentina y aplicables a las personas vinculadas por un vínculo de trabajo.

2.3 Origen evolución y consolidación de la protección de los datos personales como un derecho fundamental

Recién a partir de finales del siglo XIX la vida privada fue objeto de protección jurídica en el ámbito del derecho anglosajón. Desde el prisma preeminentemente liberal, las amenazas a la vida privada eran entendidas como incursiones de terceros en el ámbito del derecho de propiedad; tanto la defensa como la tutela de la vida

íntima aparecían como una forma de tutela de un ámbito físico o territorial sobre el cual se ejerce propiedad. En este orden de ideas se entiende que los derechos constitucionales reconocidos en relación con la intimidad fueran la inviolabilidad del domicilio y de la correspondencia, los cuales obedecían al deseo de proteger al individuo frente a la amenaza dirigida desde el Estado.

Europa occidental desarrolló normas en materia de datos personales recién a partir de la segunda mitad del siglo XX, con la aparición de la Ley del Länder alemán de Hesse de 1970 – estado alemán de Hessia – iniciando así un extenso recorrido en vías de su reconocimiento como un derecho fundamental a la autodeterminación informativa como se la conoce en nuestros días.

Si bien la Declaración Universal de los Derechos del Hombre aprobada por la Asamblea General de Naciones Unidas de 1948 no se refiere a la protección de datos como un derecho fundamental, si declaró en su artículo 12 el derecho de las personas a preservar su privacidad.

A la ley del estado de Hessia le siguieron la Ley sueca del año 1973 ("Datalagen") y durante esa década otros países europeos consagraron leyes sobre la materia como Alemania (1977) Francia (1978) Dinamarca y Noruega (1978).

Algunos países otorgaron rango constitucional a la normativa como Portugal Austria y España que en su Constitución de 1978 en su artículo 19.4 establece la necesidad de limitar el uso de la informática y garantizar el honor y la intimidad personal y familiar de los ciudadanos.

Hasta aquí el panorama normativo europeo estaba caracterizado por la falta de armonización legislativa en materia de protección de datos resultando un factor distorsionante en la construcción del Mercado Único Europeo.

En efecto, si el derecho a la intimidad, no se garantiza a nivel comunitario, podía verse entorpecido el intercambio transfronterizo de datos, que se había hecho indispensable tanto para las actividades de las empresas, los organismos de investigación y para la colaboración entre las Administraciones de los Estados miembros en el marco del espacio sin fronteras. Un escenario caracterizado por el riesgo del traslado del tratamiento informático de los datos de carácter personal hacia el territorio de aquellos Estados miembros con ausencia total de reglamentación o con una regulación menos exigente en la materia, o por el contrario, la marginación de empresas de estos mismos Estados por parte de agentes económicos ubicados en otros estados más escrupulosos, ante el temor de enfrentar conflictos derivados de la falta de garantía adecuada.

Esta situación impulsó la adopción en el año 1981 del Convenio 108 del Consejo de Europa organización internacional nacida tras la Segunda Guerra Mundial como un ámbito de cooperación entre los gobiernos europeos.

El instrumento denominado Convenio para la Protección de las Persona con respecto al Tratamiento Automatizado de Datos de Carácter Personal[11] entró en vigor en el año 1985 y hasta hoy sigue siendo junto con su Protocolo Adicional del año 2001 el único instrumento internacional obligatorio en materia de protección de datos; asimismo de conformidad con su artículo 23 está abierto para la adhesión de Estados no miembros de la Unión Europea y en virtud de ello Argentina, en línea con la actitud que habían tomado Uruguay y México fue el tercer país de Latinoamérica en adherir al Convenio y al Protocolo.

En septiembre de 2017 el Comité de ministros del Consejo de Europa aceptó el pedido que hizo Argentina para adherir al Convenio que tiene como finalidad esencial garantizar a todas las personas el respeto de sus derechos y libertades fundamentales, protección ésta que alcanza a todas las personas que se encuentran en el territorio de alguno de los Estados partes del convenio, sin que para ello importe la nacionalidad o país de residencia.

El Convenio 108 es un instrumento de carácter regional europeo, pero con vocación de universalidad, ya que como se señaló supra su artículo 23 permite la adhesión de Estados no miembros. Este Convenio ha sido el documento base para la discusión de una norma internacional para la protección de datos personales. De hecho, la Conferencia Internacional de Autoridades de Protección de Datos de 2009, donde se adoptó la Resolución sobre estándares internacionales en materia de protección de datos y privacidad,[12] expresó su apoyo a los esfuerzos del Consejo de Europa para impulsar este derecho e invitó a los Estados, sean o no miembros de la organización, a ratificar el convenio.

Su objeto fue garantizar en el territorio de cada Estado Parte a cualquier persona física sea cual fuera su nacionalidad o residencia el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a las personas. Señala principios generales básicos para cualquier tratamiento de datos personales: compromiso de las partes (art. 4); calidad de los datos (art. 5); categoría para los datos (art. 6); seguridad de los datos (art. 7).

Posteriormente en el año 1995, tras la consolidación de la UE con el Tratado de Maastricht (1992), se sancionó la directiva 95/46[13] relativa a la protección

[11] CONSEJO EUROPEO. *Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal*. Estrasburgo: [*s. n.*], 28 ene. 1981. Disponible en: https://www.coe.int/es/web/data-protection/convention108-and-protocol. Acceso el: 23 de octubre de 2023.

[12] EUROPEAN DATA PROTECTION SUPERVISOR. *Resolución sobre estándares internacionales en materia de protección de datos y privacidad*. Madrid: European Data Protection Supervisor, 9 nov. 2005. Disponible en: https://www.edps.europa.eu/sites/default/files/publication/09-11-05_madrid_int_standards_es.pdf. Acceso el: 23 oct. 2023.

[13] UNIÓN EUROPEA. *Directiva 95/46 C.E.E. del Parlamento Europeo y del Consejo*. 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. Luxemburgo: Unión Europea, 24 oct. 1995. Disponible en: https://eur-lex.europa.eu/legal-content/es/ALL/?uri=CELEX%3A31995L0046. Acceso en: 1 oct. 2023.

de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Lo que se pretendía con la directiva era homogeneizar la legislación de los estados miembros, es decir, hasta aquí cada uno de los estados miembros de la comunidad económica europea tenía una legislación propia. La directiva trataba justamente de que todos tengan como principio general homogeneizada la legislación garantizando al mismo tiempo un nivel uniforme y elevado de protección de estos datos en el seno de la Unión, hasta que en el 2016 se dicta el reglamento general de protección de datos de la Unión Europea (GDPR).

Si bien fue un instrumento de naturaleza vinculante para las partes firmantes al revestir el carácter de una directiva – la característica de las directivas en el sentido de que no eran normas aplicables directamente, sino que era necesario que cada estado miembro las consagre en su derecho interno – dio lugar a una aplicación fragmentada de la protección de datos en el territorio de la Unión Europea y generado divergencias en la ejecución de las normativas entre los estados miembro.

El Reglamento General de Protección de Datos (GDPR) (Reglamento nº 2016/679), del 27 de abril de 2016, es un reglamento por el que el Parlamento Europeo, el Consejo de la Unión Europea y la Comisión Europea tienen la intención de reforzar y unificar la protección de datos para todos los individuos dentro de la Unión Europea (UE).

No se limita a reconocer el derecho a la protección de datos personales, sino que exige que cada Estado Miembro se dote de una infraestructura administrativa que permita proteger adecuadamente ese derecho. A tal fin, cada Estado Miembro debe contar con una autoridad de control que ejercerá las competencias y funciones relativas a la protección de datos personales, entre ellas la potestad sancionadora frente a incumplimientos en esta materia.

En concreto, el art. 57 del RGPD confiere a la autoridad de control funciones como: "Promover la sensibilización del público y su comprensión de los riesgos, normas, garantías y derechos en relación con el tratamiento" como asimismo "Promover la sensibilización de los responsables y encargados del tratamiento acerca de las obligaciones" en materia de protección de datos.

La citada norma entró en vigor el 24 de mayo de 2016, y se aplica desde el 25 de mayo de 2018, rige tanto a las organizaciones europeas que tratan datos personales de ciudadanos en la UE (En este caso, los 28 Estados miembros de la UE + Islandia, Noruega y Suiza) como a las organizaciones que tienen su sede fuera de la UE y cuya actividad se dirige a personas que viven en la UE.

Conforme surge de los considerandos así como del debate y documentos previos el reglamento tiene una doble finalidad: I) establecer reglas uniformes en materia de datos que se apliquen en forma homogénea a lo largo de la Unión, teniendo en cuenta que los reglamentos a diferencia de las directivas son normas de aplicación

directa no necesitando consagración particular dentro del derecho interno de los Estados miembros, y la segunda finalidad tiene que ver con los desafíos derivados de la evolución tecnológica y la globalización que genera una utilización masiva de datos personales en una escala sin precedentes por lo que se hace necesaria la actualización de normas y principios que regulen dicha utilización.

El Reglamento, sabiamente, previó un período de transición (*vacatio legis*) de dos años tiempo durante el cual las empresas debían adecuarse a las nuevas exigencias contenidas en el nuevo cuerpo normativo.

Con relación a la protección de los datos personales en el ámbito laboral el Reglamento se expide acerca de ellos en dos lugares: por un lado en el Considerando 155 que expresa: "El Derecho de los Estados miembros o los convenios colectivos, incluidos los "convenios de empresa", pueden establecer normas específicas relativas al tratamiento de datos personales de los trabajadores en el ámbito laboral, en particular en relación con las condiciones en las que los datos personales en el contexto laboral pueden ser objeto de tratamiento sobre la base del consentimiento del trabajador, los fines de la contratación, la ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por convenio colectivo, la gestión, planificación y organización del trabajo, la igualdad y seguridad en el lugar de trabajo, la salud y seguridad en el trabajo, así como a los fines del ejercicio y disfrute, sea individual o colectivo, de derechos y prestaciones relacionados con el empleo y a efectos de la rescisión de la relación laboral". Por el otro en el artículo 88 titulado "Tratamiento en el ámbito laboral", del cual resultan normas expresas y precisas que establecen un mandato acerca de cuáles deben ser las bases legales, así como el tratamiento de datos personales en dicho ámbito. De allí que el GDPR es novedoso y responde a la insistentemente demanda de la doctrina laboral.

2.4 Convenio 108 +

Transcurridos 30 años desde la adopción del Convenio 108 fue evidente la necesidad de su reforma, de manera de adaptarlo a los tiempos actuales dado que a la época de su sanción no existían las computadoras personales, *internet* con el desarrollo y acceso actual ni los teléfonos móviles como los conocemos hoy.

El Convenio 108 +[14] es la versión modernizada del Convenio 108 y ha perseguido dos objetivos principales: hacer frente a los retos derivados de la utilización de las

[14] Modernizar el Convenio 108 de 1981 persigue facilitar el flujo de datos entre fronteras y reforzar, al mismo tiempo, la efectiva aplicación del convenio en el contexto actual (CONSEJO DE EUROPA. *Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal* (...). [*S. l.*]: Consejo de Europa, [2023]. Disponible en: https://www.coe.int/es/web/data-protection/convention108-and-protocol. Acceso el: 23 oct. 20230).

nuevas tecnologías de la información y la comunicación; y reforzar la aplicación efectiva (enforcement) del Convenio.

La nueva normativa abandona conceptos claves como el de "fichero" por su obsolescencia y reemplaza la denominación de "autoridad controladora del fichero" por la de responsable del tratamiento. Asimismo, incorpora nuevos principios: el de transparencia y de responsabilidad proactiva – el principio *accountability* – por el cual, el responsable del tratamiento no solo deberá cumplir con la normativa, sino que deberá ser capaz de demostrarlo. También incorpora los nuevos derechos recogidos del GDPR: el de oposición y el rechazo a las decisiones fundadas únicamente en el tratamiento automatizado de datos. Como asimismo amplía las categorías especiales de datos incluyendo los genéticos y biométricos, así como los relativos a la afiliación sindical o el origen étnico introduciendo la obligación de notificar sin demora los incidentes de seguridad.

Argentina, a través de la Ley nº 27.699[15] aprobó el protocolo modificatorio del convenio para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal (Convenio 108 +) suscripto en la ciudad de Estrasburgo el 10 de octubre de 2018.

2.5 Panorama latinoamericano en materia de normas de protección de datos personales

Como se ha afirmado precedentemente los países de Latinoamérica han seguido en líneas generales la tradición del modelo europeo continental en materia de protección de datos consagrando – algunos en sus constituciones y otros en su legislación especial – el derecho a la autodeterminación informativa como un derecho fundamental basado en los principios, entre otros, del consentimiento informado, categorías de datos y de la existencia de una autoridad de control específica. Casi la totalidad de los países latinoamericanos han sancionado normativas inspiradas en legislación europea y la aprobación del nuevo GDPR ha generado un impacto profundo en la región habiéndose iniciado a partir de la sanción de la normativa europea procesos de modificación de sus normas a fin de adecuarlas a los nuevos estándares europeos como son los casos de Brasil, Ecuador y Panamá, y otros países que aún no han modificado pero están en proceso de hacerlo como Argentina Chile y Paraguay.

[15] REPÚBLICA ARGENTINA. Ley 27.699 – Convenio 108+ aprobación del protocolo modificatorio del convenio 108 para la con respecto al tratamiento automatizado de datos de carácter personal, suscripto en la ciudad de Estrasburgo – República Francesa – el 10 de octubre de 2018. *Gobierno de Argentina*: Buenos Aires, 2018. Disponible en: https://www.argentina.gob.ar/normativa/nacional/ley-27699-375738. Acceso el: 1 oct. 2023.

Brasil fue en el contexto latinoamericano el primer país en modificar la ley a partir de la entrada en vigor el 18 de setiembre de 2020 la Lei Geral de Proteção de Dados (ley general de protección de datos) con una visión de servicios de tecnologías de la información en relaciones B2B, dejando a salvo que las sanciones que prevé la nueva normativa, siguiendo las tendencias comentadas, recién serían exigibles a partir de agosto 2021 para que los operadores económicos ajusten sus estructuras a la nueva normativa. En el año 2022 Brasil a partir de una enmienda constitucional incluyó el derecho a la protección de datos entre los derechos y garantías fundamentales de su Constitución.

En el contexto regional del Mercosur se aprobó en 2021 el Acuerdo sobre Comercio Electrónico del Mercosur,[16] que estableció precisas estipulaciones aplicables al ámbito de protección de datos personales y los mecanismos, herramientas y bases legales para la transferencia transfronteriza de información a través de medios electrónicos (arts. 6 y 7) estableciendo el principio de protección equivalente entre los países miembros de la zona comercial que garantice que antes de que un dato pueda viajar a un tercer país tiene que cumplir con todos los requisitos de la ley de origen del dato, que tiene sus particularidades por ejemplo en cuanto a los principios entre los que se encuentran el de licitud, de minimización de los datos, proporcionalidad, todo el paquete inicial se tiene que cumplir por el controlador de los datos antes de que estos datos se exporten.

2.6 La legislación argentina en materia de protección de datos. Descripción general del estado de situación y en las relaciones de trabajo

La configuración del derecho a la privacidad de los datos en Argentina, ante el exponencial crecimiento del flujo informativo a raíz del progreso tecnológico, se concibió a partir de un enfoque centrado en el aspecto humano por encima de la visión economicista partiendo de la visión constitucional del derecho a la intimidad y la privacidad que fueran recogidas en los arts. 18 y 19 de la carta magna argentina.[17]

Con la reforma constitucional de 1994 se incorporó un instrumento específico de protección, cual es la acción de amparo por "habeas data" incluida en el art.43. Allí se amplió la protección al conocimiento de los datos personales ya sea que consten en bancos privados o públicos de modo de poder exigir su supresión,

[16] MERCOSUR. *Acuerdo sobre Comercio Electrónico del Mercosur*. CMC/DEC. nº 15/20. Montevideo, 28 ene. 2021. Disponível en: https://normas.mercosur.int/simfiles/normativas/82753_DEC_015-2020_ES_Acuerdo%20Comercio%20Electronico.pdf. Acceso el: 1 oct. 2023.

[17] REPÚBLICA ARGENTINA. [Constitución (1853)]. *Constitución de la Nación Argentina*. Buenos Aires: Presidencia de la República, 1995. Disponible en: https://www.argentina.gob.ar/normativa/constituciones/nacional. Acceso el: 23 ago. 2023.

rectificación o confidencialidad. Estos elementos poseen especial trascendencia a la luz del desarrollo informático y tecnológico al que se hizo mención en el inicio.

Al respecto Cifuentes (1999)[18] sostuvo que, si la Constitución Nacional receptó la defensa procesal del *habeas data*, es porque en la sustancia de lo amparado se avizoraba un derecho del individuo que movió a considerarlo en especial: los datos personales como entidad específica que se requirió resguardar.

La reforma indicada también dio lugar a la incorporación de los tratados internacionales en materia de derechos humanos a los que se le otorgó jerarquía constitucional y donde también se observan disposiciones relativas al derecho a la intimidad.

Recordemos que la Declaración Universal de los Derechos Humanos en su art. 12 proscribe la injerencia arbitraria en la vida privada, familiar, en el domicilio y la correspondencia; la Declaración Americana de los Derechos y Deberes del Hombre, en su art. 5, consagra la protección frente a ataques a la vida privada y familiar; resguardo que también se encuentra presente en la Convención Americana sobre Derechos Humanos, en el Pacto Internacional de Derechos Civiles y Políticos y en el Pacto Internacional de Derechos Económicos, Sociales y Culturales instrumentos estos que integran el bloque de constitucionalidad.

El aspecto subjetivo refiere a todo el espectro que alude a la persona, desde cuestiones relacionadas con la intimidad física o la psíquica, la vida sexual, creencias religiosas o filosóficas, simpatías políticas o de otra índole, y el desenvolvimiento territorial, es decir, aquel espacio vital vinculado a la dignidad como el domicilio.

Cabe destacar que en el año 2015 a través de la Ley 26.994[19] se reformó el Código Civil argentino – ahora denominado Código Civil y Comercial de la Nación, el cual introdujo importantes novedades en la temática. En primer lugar, le otorgó el espacio de un capítulo propio con once artículos a los que denominó “derechos y actos personalísimos”. La incorporación representó un avance en la materia y un acercamiento a lo dispuesto en los tratados internacionales con jerarquía constitucional a partir de 1994. En el art. 51 determinó la inviolabilidad de la persona humana y el derecho a exigir en cualquier circunstancia el reconocimiento y respeto de su dignidad. Por su parte el art. 52 determinó que la afectación a la dignidad da a quien viese lesionada su intimidad personal o familiar, honra o reputación, imagen o identidad, lugar a reclamar no solo reparación del daño sufrido sino la prevención de su padecimiento.

---

[18] Cifuentes, S. *Acciones procesales del artículo 43 de la Constitución Nacional*: naturaleza personalísima de los datos informáticos de la persona. Buenos Aires: La Ley, 1999.

[19] REPÚBLICA ARGENTINA. Ley 26.994/2015. Código Civil y Comercial de la Nación Argentina. *Infoleg*: Buenos Aires, 2015. Disponible en: https://servicios.infoleg.gob.ar/infolegInternet/anexos/235000-239999/235975/texact.htm. Acceso el: 1 oct. 2023.

Por otro lado en lo que respecta a las relaciones de trabajo se presenta el derecho a la privacidad e intimidad del trabajador, en contraposición con la facultad de dirección que posee el empleador como una característica principal del contrato laboral, cual es la dependencia o subordinación, situación observada por el legislador quien en la Ley nº 20.744,[20] de 1974 – de Contrato de Trabajo (L.C.T.) reconoció al contrato de trabajo como objeto principal la actividad productiva y creadora del hombre en sí, y solo después la relación de intercambio bajo un fin económico.

Esta concepción humana del trabajo replica así el derecho al respeto de la dignidad del trabajador, aunque eso no implicó la negativa al reconocimiento de las facultades de organización y dirección del empleador que fueron expresamente receptadas. De hecho, es lógico que quien tiene a cargo la gestión de la empresa posea el poder de dirigirla como así también de ejercer disciplina en caso de insurrección. Empero, resulta destacable que al sancionar la norma laboral se haya previsto la imposición de límites y se haya exigido razonabilidad en su ejercicio; pautas que no todas las legislaciones laborales habían receptado para la época. Asimismo, la norma previó el carácter funcional de las facultades de dirección, tomando en consideración entre otras variables, los derechos personales del trabajador.

Estos "derechos personales" a los que aludía el entonces art. 70 (actual art. 65 LCT) no son otros que los que el Código Civil y Comercial alude como "personalísimos" por lo que su entendimiento debe darse en ese contexto y como garantía de su respeto, cuya garantía ya hemos visto proviene además del texto constitucional y del bloque federal de constitucionalidad del que forman parte los tratados internacionales relevados. En definitiva, los derechos personalísimos del trabajador enumerados ahora en el C. C. y C.N. forman parte del límite infranqueable del ejercicio de mando por parte del empleador.

El control empresarial de los medios informáticos no puede ni debe vulnerar el derecho a la intimidad y a la privacidad. Para ello es necesaria una serie de pautas mínimas: Que dicha conducta por parte del empleador se encuentre expresamente limitada en la norma y que sea pasible de sanción su infracción, además que el trabajador sea debida y previamente informado de los controles establecidos y que se lo capacite en relación con el significado y el alcance de estos.

Los derechos fundamentales reconocidos a los ciudadanos poseen una especial implicancia al invocarlos un trabajador por la situación de desventaja de poder en que se halla en la relación social. Allí la intimidad y la privacidad precisan de un resguardo especial en aras a la protección de la dignidad humana.

[20] REPÚBLICA ARGENTINA. Ley 20.744/1974. Ley de Contrato de Trabajo. *Infoleg*: Buenos Aires, 1974. Disponible en: https://servicios.infoleg.gob.ar/infolegInternet/anexos/25000-29999/25552/texact.htm. Acceso el: 1 oct. 2023.

Como ya se explicó *supra* en el ámbito laboral la persona trabajadora ve reducida la facultad negocial razón ésta por lo que es necesario regular minuciosamente la potestad de privacidad en cabeza de la persona trabajadora y el control tecnológico de la actividad laboral y vigilancia en manos del empresario a partir de la utilización de las tecnologías de la información y comunicación (TICs).

En el seno de las empresas es necesario contar con reglas claras y proporcionadas, para evitar los inconvenientes derivados de la indeterminación de la normativa heterónoma generan mayor vulnerabilidad y desprotección de los derechos fundamentales. La mayoría de las legislaciones aplican a las relaciones jurídicas de estos colectivos las normas sobre privacidad generales *aggiornándolas* al ámbito del trabajo y sus peculiaridades con la excepción del Reglamento Europeo de Protección de Datos que tiene normas específicas abonado además por la prolífera interpretación del denominado Grupo de Trabajo del art. 29 –creado por la Directiva nº 95/46/CEE – y su sucesor en el marco del nuevo reglamento el Comité Europeo de Protección de Datos así como la labor de los tribunales europeos que ha tenido oportunidad de expedirse en estas cuestiones en numerosas oportunidades.[21]

En Argentina, la ley vigente en materia de protección de datos personales – Ley nº 25.326 –[22] de principios de siglo, es de las primeras normas que se activan en relación con el fenómeno de *internet*. Sancionada en octubre del año 2000 – junto a su decreto reglamentario 1558/01 – amplió el espectro de protección de los datos personales, denominado autodeterminación informativa y reguló en forma detallada su instrumentación. Sin embargo esa normativa resulta insuficiente para las exigencias derivadas del desarrollo tecnológico actual. En primer lugar, prácticamente el 100% de las transacciones comerciales se realizan en formato electrónico. Sumado a ello, el Estado argentino, en el ámbito de la administración pública nacional, tiene un sistema de gestión documental electrónico que hace que el 100% de las actuaciones administrativas sean en formato electrónico. Además del sistema, posee un marco jurídico muy sólido integrado por más de 20 decretos y 200 resoluciones, todas fundamentadas en la ley de firma digital, y hasta un reglamento de procedimientos administrativos que regula el expediente electrónico. Pero todo lo que tiene que ver con la protección de datos personales en el ámbito privado se quedó en el tiempo, con una realidad de mediados de los 90, del siglo pasado.

---

21 Tribunal Europeo de Derechos Humanos ha rectificado el fallo de la Sala de esa misma Corte (BOE.ES, 2019) en el caso de las cinco empleadas de la cadena Mercadona que fueron despedidas tras ser filmadas con cámara oculta cuando robaban, uno de los casos más resonantes. Para más detalles consultar: MERCADONA paga una sanción de 2,5 millones de euros a Protección de Datos: la cadena testó un proyecto piloto que permitía detectar personas con orden de alejamiento de sus tiendas. *El País*, Madrid. 22 jul. 2021. Disponible en: https://elpais.com/economia/2021-07-22/mercadona-paga-una-sancion-de-25-millones-de-euros-a-proteccion-de-datos.html . Acceso el: 15 feb. 2024.

22 REPÚBLICA ARGENTINA. Ley 25.326/2000. Ley de Protección de Datos Personales. *Infoleg*: Buenos Aires, 2000. Disponible en: https://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm. Acceso el: 1 oct. 2023.

Como un hito importante se señala la Decisión de Adecuación nº 2003/490/CE,[23] dictada el 30 de junio de 2003 de la Comisión del Parlamento Europeo y del Consejo por el que se declara a Argentina como un país que garantiza un nivel adecuado de protección por lo que respecta a los datos transferidos desde la Comunidad.

Al evaluar la adecuación[24] del nivel de protección, la comisión tiene en cuenta entre otros lo siguiente: la vigencia del el Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, tanto general como sectorial, incluida la relativa a la seguridad pública, la defensa, la seguridad nacional y la legislación penal, y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, las normas de protección de datos, las normas profesionales y las medidas de seguridad, incluidas las normas sobre transferencias ulteriores de datos personales a otro tercer país u organización internacional observadas en ese país u organización internacional, la jurisprudencia etc.

Esa resolución de adecuación del año 2003 fue hecha bajo la Directiva nº 95/46/CE –a los efectos del apartado 2 del artículo 25 – que al considerar que Argentina garantiza un nivel adecuado de protección por lo que respecto a los datos personales transferidos desde la Comunidad ello conlleva el beneficio de que al ser un país considerado adecuado facilitará el libre flujo de datos lo que se traduce en la práctica en oportunidades económicas para el país con nuevas oportunidades de negocios. La adecuación se encontraba en proceso de revisión desde el 2018 al haberse aprobado el G.D.P.R. por lo que es importante destacar que en enero de 2024 nuevamente Argentina fue declarada entre los países que garantizan un nivel adecuado de protección.

En términos expreso de la resolución de este año la Comisión acoge con satisfacción los avances en el marco legal argentino desde la adopción de la decisión de adecuación, incluyendo modificaciones legislativas, jurisprudencia y actividades de organismos de supervisión, que han contribuido a un mayor nivel de protección de datos. En particular, la independencia de la autoridad de supervisión de protección de

[23] COMISIÓN AL PARLAMENTO EUROPEO. *Decisión de la Comisión con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo de Adecuación de Argentina 2003/490/CE*. Bruselas: Parlamento Europeo, 20 jun. 2003. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32003D0490. Acceso el: 1 oct. 2023.

[24] El Tribunal de Justicia en su sentencia de 6 de octubre de 2015, Asunto C 362/14 Maximilliam Schrems c/ Comisionado de Protección de Datos, esto no requiere encontrar un nivel de protección idéntico. En particular los medios a los que recurra el tercer país en cuestión para proteger los datos personales pueden diferir de los empleados en la Unión, siempre que resulten, en la práctica, eficaces para garantizar un nivel adecuado de protección. El estándar de adecuación no requiere una réplica punto por punto de las normas de la Unión, sino que el sistema extranjero en su conjunto brinde el nivel requerido de protección (UNIÓN EUROPEA. Tribunal de Justicia. *Sentencia nº C-362/14*. Maximillian Schrems *vs.* Data Protection Commissioner. Luxemburgo, 6 oct. 2015).

datos de Argentina se fortaleció significativamente mediante el Decreto nº 746/17, que confió a la Agencia de Acceso a la Información Pública (AAIP) la responsabilidad de supervisar el cumplimiento de la ley de protección de datos. Además, la Agencia Argentina de Información Pública emitió varias regulaciones y opiniones vinculantes que aclaran cómo se debe interpretar y aplicar en la práctica el marco de protección de datos, contribuyendo así a mantener actualizada la ley de protección de datos. Argentina también fortaleció sus compromisos internacionales en el ámbito de la protección de datos al unirse al Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos personales y su Protocolo adicional en 2019, y al ratificar el protocolo enmendado que crea el convenio modernizado 108+ en 2023.

Se entiende que el fortalecimiento del marco normativo – cuya necesidad de actualización se señalaba como urgente – no solo viene de la mano de un proyecto de reforma de ley. Hay un conjunto de acciones y decisiones llevadas a cabo que nos llevan a decir que Argentina está de nuevo "a tope de gama" y que por eso hoy nuevamente el Consejo de la Unión Europea mediante resolución de fecha 15 de enero 2024 ha considerado a la Argentina – entre otros países – un país adecuado para las transferencias internacionales de datos.

Está claro que es necesario actualizar la ley pues ya pasaron más de 23 años desde su sanción. En el 2000 no existían los teléfonos inteligentes, era otra la realidad y el tratamiento de los datos personales cambió. Empresas como WhatsApp que hoy hacen un tratamiento intensivo de datos personales no existían en el año 2000.

La Ley nº 25.326 fue en su momento una ley de avanzada que vino a regular cuestiones que en ese momento eran impensadas. Aún hoy sigue siendo una ley robusta que permite seguir adelante pero que es una realidad que necesita urgente una actualización por el desarrollo de la innovación tecnológica.

Actualmente existe un proyecto de reforma – hubo otro en 2018 que perdió estado parlamentario – inspirada en lecciones aprendidas a partir del estudio del derecho comparado lo que disponen otros cuerpos normativos entre ellos, el GDPR, que no es la única fuente de inspiración sino, también lo son, las recomendaciones de ética de Inteligencia artificial de la Unesco, los estándares de la Red Iberoamericana de Protección de Datos[25] y los proyectos y las legislaciones de la región como la de Brasil, Uruguay, y los proyectos de Chile, Paraguay y Costa Rica.

[25] La Red está elaborando una guía (orientativa, no vinculante) para el uso de cláusulas contractuales como alternativa para realizar transferencias internacionales de datos personales (RED IBEROAMERICANA DE PROTECCION DE DATOS. Guía de implementación de cláusulas contractuales modelo para la transferencia internacional de datos personales (TIDP). [*S. l.*]: [*s. n.*], 2022. Disponible en: https://www.redipd.org/sites/default/files/ 2022-09/guia-clausulas-contractuales-modelo-para-tidp.pdf. Acceso el: 1 oct. 2023).

Alguna de las ideas claves que propone el proyecto de modificación se vincula con el ámbito de aplicación, incorporando el principio de extraterritorialidad que permite fiscalizar aquellas empresas o responsables del procesamiento de datos, del tratamiento, del almacenamiento y también por qué no de aquellos que infieren datos para el perfilamiento, lo que implica que aquellos responsables que no están radicados en Argentina (ej.: empresas no tienen cuit en Argentina), puedan ser alcanzados dentro de ámbito espacial de aplicación de la ley. Esto se encuentra estrechamente vinculado con el capítulo de transferencias internacionales de datos personales, un tema de vital importancia para el comercio internacional, para promover la economía digital. Y en este sentido la propuesta de proyecto de ley pretende hacer converger el impulso a la innovación y al desarrollo económico, pero con garantizando los derechos fundamentales.

Partiendo de una mirada situada y soberana al momento de suscribir estándares internacionales se propone la utilización de herramientas que garanticen la interoperabilidad con otros países o bloque de países. El principio de neutralidad tecnológica que significa que la ley aplica a todo tipo de tratamiento de datos al margen de las tecnologías o procedimientos que se utilicen para dicho efecto. De esta manera, la ley no quedará obsoleta frente a las futuras innovaciones tecnológicas. El respeto por el principio de no discriminación – un tema que es fundamental cuando hablamos de tecnologías como la Inteligencia artificial – teniendo en cuenta que existen algunas tecnologías que podrían no ser neutrales porque están modeladas según las elecciones y valores de quienes las diseñan – lo que entrañan riesgo por la producción de sesgos.[26] Ejemplo de ello fue el de la empresa Amazon que invento un algoritmo para agilizar su proceso de contratación y se descubrió que los datos que se utilizaron como base tenían un sesgo que implicara que se contratara siempre a personas del mismo sexo masculino excluyendo a las del sexo femenino.

Es importante entender que no puede pretenderse que todos los países tengan legislaciones iguales pues, cada uno tiene su idiosincrasia, sus particularidades resultando lo más aconsejable intentar el camino hacia la consagración de estándares comunes en materia de privacidad y tener en cuenta las legislaciones de países con los cuales se pueda garantizar un alto nivel de adecuación.

Para concluir este apartado entre los principales puntos del proyecto de reforma de la ley argentina pueden citarse en primer lugar la limitación de la protección de los datos solo a las personas humanas excluyendo las personas jurídicas diferenciándose así de la ley vigente, receptando la tendencia de las principales regulaciones a nivel global. Asimismo, elimina el requisito de registro de bases de datos ante la

[26] Cómo Amazon inventó accidentalmente un algoritmo de contratación sexista (GONZALEZ, G. How Amazon Accidentally Invented a Sexist Hiring Algorithm: A company experiment to use Artificial Intelligence in hiring inadvertently favored male candidates. *Inc.*, New York, Oct. 2018. Disponible en: https://www.inc.com/guadalupe-gonzalez/amazon-artificial-intelligence-ai-hiring-tool-hr.html. Acceso el: 1 oct. 2023).

autoridad de aplicación correspondiente actualmente previsto. También, califica como datos sensibles a los datos genéticos y biométricos. En igual sentido recepta el concepto de extraterritorialidad el cual implica que la norma será de aplicación siempre que el Responsable o Encargado del tratamiento se encuentre establecido en el territorio de la República Argentina, aun si el tratamiento de datos tuviese lugar fuera de dicho territorio; Cuando, no se encuentra establecido en el territorio de la república, pero se da alguno de los siguientes supuestos: realice el tratamiento de datos en el territorio del país mediante cualquier medio o procedimiento, físico o electrónico, conocido o por conocer, que le permite recolectar, usar, almacenar, indexar o tratar información de personas que se encuentren en el territorio; O bien cuando efectúe actividades de tratamiento relacionadas con la oferta de bienes o servicios a personas que se encuentren en el territorio de la Argentina; o el perfilamiento, seguimiento o control de los actos, comportamientos o intereses de dichas personas.

Otro de los principales aportes del proyecto referenciado lo es la incorporación de nuevos principios tales como: de transparencia, minimización de datos, preeminencia a favor del titular de los datos, responsabilidad proactiva *(acuontability*) protección desde el diseño y por defecto, así como la inclusión de nuevos conceptos tales como el de autodeterminación informativa, anonimización y seudonimización, elaboración de perfiles y encargado o responsable del tratamiento. Estas actualizaciones terminológicas ya están vigentes por la adhesión de Argentina al Convenio 108 + en 2019 mediante Ley nº 27.699.

No obstante, en la legislación proyectada el consentimiento continúa siendo la base jurídica que legitima el tratamiento de los datos personales. Sin embargo, se precisan los criterios para obtener ese consentimiento y su revocación, estableciendo principios para el tratamiento de los datos pertenecientes a niños niñas y adolescentes.

Otra de las novedades introducidas es la obligación de notificar los incidentes de seguridad a la autoridad de aplicación y al titular de los datos en lenguaje claro y sencillo. En la misma línea propone la creación de la figura del delegado de protección de datos obligatorio y se establecen criterios para la realización de las evaluaciones de impacto y su contenido mínimo. Finalmente, detalla el procedimiento a observar para aplicar sanciones y eleva el tope de las multas las que pueden alcanzar del 2 al 4 % de la facturación global.

De esta manera es de resaltar que Argentina siguiendo las tendencias internacionales (GDPR Convenio 108+ Recomendaciones Red Iberoamericana) haya impulsado esta reforma continuando con un modelo más avanzado hacia la protección de los derechos fundamentales. Ese impulso se ve acompañado por el dictado de una nueva resolución de adecuación por parte de la Unión Europea

para el flujo internacional de datos personales.[27] Entiendo saludable la práctica de un parlamento que, superando la efervescencia política contemporánea, pudiera consensuar la aprobación de normas de alto perfil técnico con ventajas más que evidentes para la ciudadanía en su conjunto.

2.7 Incidentes de privacidad a nivel global, antecedentes, multas aplicadas

Para comenzar a desarrollar este apartado resulta insoslayable recordar un hito en materia de reclamos por violaciones a la privacidad y que algunos califican como el hecho que desencandenó la sanción del GDPR: Asunto C-311/18 – Comisaria de Protección de Datos *vs.* Facebook Irlanda Maximilliam Schrems.

Según relata la prensa[28] un ciudadano austriaco de 23 años inició una batalla legal contra Facebook en 2013. La historia comenzó cuando aún era estudiante de Derecho mientras pasaba un semestre en la Universidad de Santa Clara en California muy cerca de los gigantes tecnológicos de Silicon Valley – Apple, Google, Facebook, Amazon, Tesla. Cuando asistía a una de sus clases en la Universidad recibió la visita de expertos legales de Facebook y Amazon quienes comentaron acerca del incumplimiento por parte de sus empresas de las reglas de privacidad calificando a las normas europeas como muy estrictas lo que no implicaba para ellos un problema por cuanto las multas eran irrisorias con relación a los cuantiosos beneficios que la utilización de datos "a piacere" les significaba por lo que no dudaban en evadir su cumplimiento. Al regresar de su estancia solicitó a Facebook los datos que esta red social poseía, ejercitando su derecho de acceso recibiendo una importante cantidad de información (1.200 páginas) acerca de su vida *online* desde 2008 detectando varias violaciones a su privacidad y procedió a realizar 22 denuncias ante la Comisión de Protección de Datos de Irlanda país este donde Facebook tiene su sede europea. Con el fundamento de que bajo leyes europeas se permitía a las compañías tecnológicas transferir datos de ciudadanos europeos a un puerto seguro en el extranjero, estas transferencias eran ejecutadas por unas 4000 compañías entre las que se encontraba Facebook: enviaban datos privados a servidores localizados en América. El reclamó llegó al Tribunal de Justicia de la Unión Europea y Shcrems ganó su batalla legal cuando en 2015 el Tribunal dictaminó que: "EEUU no garantiza una protección suficiente de los datos trasferidos".

---

[27] REPÚBLICA ARGENTINA. Argentina logró la nueva adecuación por parte de la Unión Europea para el flujo internacional de datos personales: es un hito para el país ya que beneficia las condiciones para el comercio internacional y el desarrollo económico al contar con las mismas garantías de protección de datos personales que la UE (...). *Gobierno de Argentina*: Buenos Aires, 2024. Disponível em: https://www.argentina.gob.ar/noticias/argentina-logro-la-nueva-adecuacion-por-parte-de-la-union-europea-para-el-flujo. Acceso em: 16 ene. 2024.

[28] GUILLERMO, A. Max Schrems, el hombre que retó a Mark Zuckerberg. *El País*, Madrid, 18 mayo 2018. Disponible en: https://elpais.com/elpais/2018/05/10/eps/1525952227_419658.html#?prm=copy_link. Acceso el: 15 feb. 2024.

En 2011 efectuó otra denuncia: la transferencia de datos privados desde Facebook a desarrolladores de aplicaciones sin un nivel adecuado de protección. Esa fue la causa por la que el propietario de Facebook Mark Zuckerberg debió comparecer ante el Congreso de EE. UU. a pedir perdón: su compañía permitió que una app colectara datos de 50 millones de usuarios que terminaron en manos de la consultora Cambridge Analytica que los utilizó en favor de uno de los candidatos a la Casa Blanca con los resultados que todos ya sabemos.[29]

El caso que se analiza resulta ser una muestra más acerca de que, las transferencias internacionales de datos entre UE y los EE. UU. han resultado continuamente conflictivas y en muchos casos los acuerdos han resultado infructuosos. Así, la Comisión Europea encargada de declarar tras analizar su legislación interna y los compromisos internacionales en el año 2000 adoptó una decisión de adecuación que autorizaba la transferencia de datos a los EEUU en el marco de un sistema de autocertificación de las empresas adherentes denominado "puerto seguro" (*safe harbour*) La decisión lograda tras complejas negociaciones era trascendente teniendo en cuenta el volumen de datos involucrados a través de los gigantes tecnológicos como Google, Facebook, Microsoft, Apple, todas ellas certificadas bajo el marco de puerto seguro. Sin embargo, tras las denuncias comentadas supra de parte de Scherems pidiendo que se prohibiera la transferencia de sus datos a los EEUU a la cuenta de que en el territorio no se garantizaba un nivel adecuado de protección de datos contra las actividades de vigilancia practicadas por las autoridades estadounidenses el Tribunal Europeo declaró inválido el sistema de puerto seguro y decidió que no garantiza una protección suficiente de los datos trasferidos. En 2016 hubo otro marco legal denominado escudo de privacidad (*privacy shield*) el que fue anulado nuevamente (por sentencia del 23 de julio del 2020) ante el reclamo del activista denominado Caso Schrems II considerando que, los distintos programas de vigilancia con fines de inteligencia exterior norteamericanos, no ofrecían un nivel de protección equivalente al ofrecido dentro de la UE declarando asimismo la resolución del Tribunal Europeo que el mecanismo del Defensor del Pueblo establecidos por EEUU no constituía tutela judicial efectiva que garantizara el ejercicio de los derechos de los titulares de los datos.

La situación se mantuvo entre idas y vueltas tras la anulación de la anterior decisión de adecuación (*privacy shield*, o escudo de privacidad) en 2020 y un período de tres años de vacío el 10 de julio 2023 se dictó una nueva decisión de adecuación denominada Marco Transatlántico de Privacidad.[30]

[29] HARARI, Y. N. *21 lecciones para el siglo XXI*. Buenos Aires: Debate, 2023. p. 103.

[30] ESTÉVEZ, D. Por fin tenemos aprobado el nuevo Marco de Privacidad de Datos entre la UE y Estados Unidos. [*S. l.*]: [*s. n.*], 2023. Disponible en: https://adenda.net/por-fin-tenemos-aprobado-el-nuevo-marco-de-privacidad-de-datos-entre-la-ue-y-estados-unidos/. Acceso em: 1 oct. 2024.

La gran novedad de este marco, indica la Comisión Europea es que la decisión de adecuación es seguida por la firma de EEUU de una Orden Ejecutiva sobre Mejora de las salvaguardias para las actividades de inteligencia. Esto quiere decir que las nuevas obligaciones están orientadas a garantizar que las agencias de inteligencia estadounidenses puedan acceder a los datos solo en la medida que sea necesario y proporcionado ofreciendo vías de reparación independientes e imparciales para resolver los posibles incidentes respecto de acceso y recopilación de datos de europeos incluso con mecanismos independientes para resolver conflictos y un panel de arbitraje gratuito y que existan garantías suficientes para la protección de la privacidad de los datos como un derecho fundamental.

Pueden destacarse otros incidentes de privacidad que significaron importantes multas para los gigantes tecnológicos en los últimos tres años. En julio 2021 Amazon recibe la mayor multa de privacidad hasta ese momento – 746 millones de euros – por no cumplir con el GDPR impuesta por la autoridad de protección de datos de Luxemburgo donde tiene su sede en Europa.[31] Al año siguiente Instagram recibió una multa de la Comisión Irlandesa de Protección de datos de 405 millones mientras que WhatsApp recibió una multa de 225 millones en 2021.[32] En mayo de 2023, Meta recibe la mayor multa de la historia de la Unión Europea por 1200 millones de euros[33] y en junio de ese mismo año, Microsoft fue sancionada con una multa de casi 350 millones por recopilar ilegalmente información personal de niños.[34]

3 Conclusión

Los datos son el combustible que alimenta la economía digital, un recurso valioso que permite llegar a más consumidores de manera más precisa. La convergencia en toda la tecnología, cada vez más próxima y conectada a través del análisis de macrodatos, de sistemas de aprendizaje automático, facilitando la creación de perfiles, la automatización de las decisiones en amplios sectores de la

[31] PERÉS, E. Amazon recibe la mayor multa de la historia de la Unión Europea en materia de privacidad: 746 millones de euros por no cumplir el RGPD. 746 millones de euros por no cumplir el RGPD. *Xataka*, [*S. l.*], 2021. Disponible en: https://www.xataka.com/privacidad/amazon-recibe-mayor-multa-historia-union-europea-materia-privacidad-746-millones-euros-no-cumplir-rgpd. Acceso en: 1 oct. 2023.

[32] AGUILAR, R. Sanción histórica para Instagram: se enfrenta a 405 millones de euros de multa por incumplir el RGPD. *Xataka*, [*S. l.*], 2022. Disponible en: https://www.xataka.com/privacidad/sancion-historica-para-instagram-instagram-se-enfrenta-a-405-millones-euros-multa-incumplir-rgpd. Acceso en: 1 oct. 2023.

[33] PERÉS, E. Meta recibe la mayor multa de la historia de la Unión Europea por protección de datos: 1.200 millones de euros. 746 millones de euros por no cumplir el RGPD. *Xataka*, [*S. l.*], 2023. Disponible en: https://www.xataka.com/legislacion-y-derechos/meta-recibe-mayor-multa-historia-union-europea-proteccion-datos-1-200-millones-euros. Acceso en: 1 oct. 2023.

[34] KENTH. Microsoft pagará una multa de casi 350 millones de pesos por recopilar ilegalmente información personal de niños en Xbox. *Xataka*, [*S. l.*], 2023. Disponible en: https://www.xataka.com.mx/videojuegos/microsoft-pagara-multa-casi-350-millones-pesos-recopilar-ilegalmente-informacion-personal-ninos-xboxAcceso en: 1 oct. 2023.

actividad recopilando grandes volúmenes de información requieren de normas claras y dinámicas que protejan el derecho a la protección de los datos para garantizar la zona de privacidad y de control sobre la información personal, las que deben evolucionar en la medida en que lo hace la transformación tecnológica.

A los fines de adaptarse a estas nuevas tecnologías, las organizaciones deben mantener seguros sus datos de posibles ataques cibernéticos para así ganar la confianza del público respecto a que sus datos serán tratados adecuadamente. Tanto los incidentes relacionados a la seguridad cibernética, como el incumplimiento de los requisitos de la protección de datos, podrían dañar la reputación, la marca o los negocios de una compañía. Es por ello que ellas, son directamente responsables por la protección de los datos personales que administran.

En este sentido, las empresas deberán desarrollar una estrategia integral para la seguridad y la protección de datos personales, en particular mediante la identificación de los obstáculos legales y reglamentarios que deben superarse y actualizarse constantemente para mantenerse a la altura y velocidad de adaptación de las nuevas tecnologías.

Por su parte, los países tendrían que adoptar una legislación actualizada e interoperable con el resto del mundo en materia de protección de datos personales como garantía para el desarrollo económico para lo cual es necesario la revisión permanente, que refleje adecuadamente las nuevas tecnologías y prácticas empresariales. Para ello se deberá promover la adopción de normas internacionales y estándares que aborden los desafíos actuales en la protección de la privacidad, proporcionando un marco más consistente a nivel global. En este sentido sería conveniente avanzar hacia un convenio jurídico universal y vinculante, tecnológicamente neutral y certificable en materia de PDP y privacidad. Asimismo, reforzar la transparencia en la recopilación y uso de datos, garantizando que las personas comprendan cómo se utilizan sus datos y tengan un control claro sobre su consentimiento.

Como consecuencia, tendrán que establecer mecanismos efectivos de cumplimiento y sanciones para asegurar que las entidades que manejan datos personales cumplan con las regulaciones de privacidad.

En otro orden de cosas desde las políticas públicas deberán promover programas de educación y concienciación para empoderar a las personas sobre sus derechos de privacidad y fomentar prácticas responsables por parte de las empresas, incentivando la investigación y el desarrollo de tecnologías protectorias, como encriptación robusta y herramientas de anonimización.

En términos de colaboración público-privada habrá que fomentar la cooperación entre gobiernos, empresas, y sociedad civil para abordar de manera conjunta los desafíos emergentes en la protección de la privacidad, realizando evaluaciones

periódicas y ajustes en las regulaciones y prácticas de privacidad para adaptarse a la evolución constante de la tecnología y estrategias comerciales.

En el ámbito del trabajo – en consonancia con lo propuesto en términos de privacidad global – sería de importancia crear una norma global para la gobernanza transparente por parte del empleador de los datos de sus dependientes que garanticen el control en las decisiones administrativas unilaterales tomadas por éste cuando se sustentan en tales datos. Ello se justifica por cuanto resulta más evidente en la relación laboral la asimetría de poder, dada la relativa facilidad de combinar datos de fuentes diversas, sin que la persona trabajadora cuente con voz ni influencia sobre qué datos se usan y cómo se usan.

Finalmente, para el logro de los fines propuestos resulta imperioso incluir la privacidad desde el diseño impregnando todo el proceso de la organización desde el inicio para resguardar la privacidad en el desarrollo de un sistema de una aplicación.

Estas sugerencias resultan del análisis profundo de todas aquellas aristas involucradas en la gobernanza de datos sin desconocer ni negar las particularidades propias de cada una de ellas, y sus implicancias en los contextos específicos de cada país.

Referencias

AGUILAR, R. Sanción histórica para Instagram: se enfrenta a 405 millones de euros de multa por incumplir el RGPD. *Xataka*, [*S. l.*], 2022. Disponible en: https://www.xataka.com/privacidad/sancion-historica-para-instagram-instagram-se-enfrenta-a-405-millones-euros-multa-incumplir-rgpd. Acceso el: 1 oct. 2023.

BRASIL. Lei Federal nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. *Diário Oficial da União*: Brasília, DF, 2018. Disponible en: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2349685. Acceso el: 2 oct. 2023.

CIFUENTES, S. *Acciones procesales del artículo 43 de la Constitución Nacional.* Naturaleza personalísima de los datos informáticos de la persona. Buenos Aires: La Ley, 1999.

COMISIÓN AL PARLAMENTO EUROPEO. *Decisión de la Comisión con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo de Adecuación de Argentina 2003/490/CE*. Bruselas: Parlamento Europeo, 20 jun. 2003. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32003D0490. Acceso el: 1 oct. 2023.

CONSEJO DE EUROPA. *Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal* (...). [*S. l.*]: Consejo de Europa, [2023]. Disponible en: https://www.coe.int/es/web/data-protection/convention108-and-protocol. Acceso el: 23 oct. 2023.

CONSEJO EUROPEO. *Convenio 108 +*. Estrasburgo, 10 oct. 2018. [*S. l.*]: Consejo de Europa, 2018. Disponible en: https://www.coe.int/es/web/data-protection/convention108/modernised. Acceso el: 01 oct. 2023.

CONSEJO EUROPEO. *Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal*. Estrasburgo: [*s. n.*], 28 ene; 1981. Disponible en: https://www.coe.int/es/web/data-protection/convention108-and-protocol. Acceso el: 23 de octubre de 2023.

CONSEJO EUROPEO. *Convenio 108.* Tratado nº 181 Protocolo Adicional Tratamiento Automático de Datos Personales, en relación con las autoridades de control y los flujos transfronterizos de datos (ETS nº 181). Estrasburgo: Consejo Europeo, 11 ago. 2001.

CRAWFORD, Kate. *Atlas de Inteligencia Artificial.* Poder, política y costos planetarios. Buenos Aires: Fondo de Cultura Económica, 2022.

EUROPEAN DATA PROTECTION SUPERVISOR. *Resolución sobre estándares internacionales en materia de protección de datos y privacidad*. [*S. l.*]: European Data Protection Supervisor, 9 nov. 2005. Disponible en: https://www.edps.europa.eu/sites/default/files/publication/09-11-05_madrid_int_standards_es.pdf. Acceso el: 23 oct. 2023.

EEUU. *Act No. 56, Oct. 26, 2001*. Uniting And Strengthening America By Providing Appropriate Tools Required To Intercept And Obstruct Terrorism (Usa Patriot Act) Act Of 2001. Washington D.C., 6 Oct. 2001. Disponible en: https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.htm. Acceso el: 12 nov. 2023.

EEUU. *S.2383.* Ley de la Nube Cloud Act. Enmendar el título 18 del Código de los Estados Unidos para mejorar el acceso de las fuerzas del orden a los datos almacenados a través de fronteras y para otros fines, [2023]. Disponible en: https://www.congress.gov/bill/115th-congress/senate-bill/2383/text. Acceso el: 12 nov. 2023.

ESTÉVEZ, D. *Por fin tenemos aprobado el nuevo Marco de Privacidad de Datos entre la UE y Estados Unidos*. [*S. l.*]: [*s. n.*], 2023. Disponible en: https://adenda.net/por-fin-tenemos-aprobado-el-nuevo-marco-de-privacidad-de-datos-entre-la-ue-y-estados-unidos/. Acceso em: 1 oct. 2024.

EUROPEAN DATA PROTECTION SUPERVISOR. *Resolución sobre estándares internacionales en materia de protección de datos y privacidad*. Madrid, [*s. n.*], [2023]. Disponible en: https://www.edps.europa.eu/sites/default/files/publication/09-11-05_madrid_int_standards_es.pdf. Acceso el: 23 de octubre de 2023.

GONZALEZ, G. How Amazon Accidentally Invented a Sexist Hiring Algorithm: A company experiment to use artificial intelligence in hiring inadvertently favored male candidates. *Inc.*, New York, Oct. 2018. Disponible en: https://www.inc.com/guadalupe-gonzalez/amazon-artificial-intelligence-ai-hiring-tool-hr.html. Acceso el: 1 oct. 2023.

GUILLERMO, A. Max Schrems, el hombre que retó a Mark Zuckerberg. *El País*, Madrid, 18 mayo 2018. Disponible en: https://elpais.com/elpais/2018/05/10/eps/1525952227_419658.html#?prm=copy_link. Acceso el: 15 feb. 2024.

HARARI, Y. N. *21 lecciones para el siglo XXI.* Buenos Aires: Debate, 2023.

KENTH. Microsoft pagará una multa de casi 350 millones de pesos por recopilar ilegalmente información personal de niños en Xbox. *Xataka*, [*S. l.*], 2023. Disponible en: https://www.xataka.com.mx/videojuegos/microsoft-pagara-multa-casi-350-millones-pesos-recopilar-ilegalmente-informacion-personal-ninos-xboxAcceso en: 1 oct. 2023.

MERCADONA paga una sanción de 2,5 millones de euros a Protección de Datos: la cadena testó un proyecto piloto que permitía detectar personas con orden de alejamiento de sus tiendas. *El País*, Madrid. 22 jul. 2021. Disponible en: https://elpais.com/economia/2021-07-22/mercadona-paga-una-sancion-de-25-millones-de-euros-a-proteccion-de-datos.html. Acceso el: 15 feb.2024.

MERCOSUR. *Acuerdo sobre Comercio Electrónico del Mercosur*. CMC/DEC. nº 15/20. Montevideo, 28 ene. 2021. Disponível en: https://normas.mercosur.int/simfiles/normativas/82753_DEC_015-2020_ES_Acuerdo%20Comercio%20Electronico.pdf. Acceso el: 1 oct. 2023.

PALERMO, J. D. *¿Qué es la sinergología y cómo aplicarla a mi empresa?* [*S. l.*]: [*s. n.*], [2023]. Disponible en: https://www.elobservatoriodeltrabajo.org/que-es-la-sinergologia-y-como-aplicarla-a-mi-empresa/. Acceso el: 1 oct. 2023.

PERÉS, E. Amazon recibe la mayor multa de la historia de la Unión Europea en materia de privacidad: 746 millones de euros por no cumplir el RGPD. 746 millones de euros por no cumplir el RGPD. *Xataka*, [*S. l.*], 2021. Disponible en: https://www.xataka.com/privacidad/amazon-recibe-mayor-multa-historia-union-europea-materia-privacidad-746-millones-euros-no-cumplir-rgpd. Acceso el: 1 oct. 2023.

PERÉS, E. Meta recibe la mayor multa de la historia de la Unión Europea por protección de datos: 1.200 millones de euros. 746 millones de euros por no cumplir el RGPD. *Xataka*, [*S. l.*], 2023. Disponible en: https://www.xataka.com/legislacion-y-derechos/meta-recibe-mayor-multa-historia-union-europea-proteccion-datos-1-200-millones-euros. Acceso en: 1 oct. 2023.

RED IBEROAMERICANA DE PROTECCION DE DATOS. *Guía de implementación de cláusulas contractuales modelo para la transferencia internacional de datos personales (TIDP)*. [*S. l.*]: [*s. n.*], 2022. Disponible en: https://www.redipd.org/sites/default/files/ 2022-09/guia-clausulas-contractuales-modelo-para-tidp.pdf. Acceso el: 1 oct. 2023.

REPÚBLICA ARGENTINA. *Argentina logró la nueva adecuación por parte de la Unión Europea para el flujo internacional de datos personales*: es un hito para el país ya que beneficia las condiciones para el comercio internacional y el desarrollo económico al contar con las mismas garantías de protección de datos personales que la UE (...). *Gobierno de Argentina*: Buenos Aires, 2024. Disponível em: https://www.argentina.gob.ar/noticias/argentina-logro-la-nueva-adecuacion-por-parte-de-la-union-europea-para-el-flujo. Acceso el: 16 ene. 2024.

REPÚBLICA ARGENTINA. [Constitución (1853)]. *Constitución de la Nación Argentina*. Buenos Aires: Presidencia de la República, 1995. Disponible en: https://www.argentina.gob.ar/normativa/constituciones/nacional. Acceso el: 23 ago. 2023.

REPÚBLICA ARGENTINA. Ley 20.744/1974. Ley de Contrato de Trabajo. *Infoleg*: Buenos Aires, 1974. Disponible en: https://servicios.infoleg.gob.ar/infolegInternet/anexos/25000-29999/25552/texact.htm. Acceso el: 1 oct. 2023.

REPÚBLICA ARGENTINA. Ley 25.326/2000. Ley de Protección de Datos Personales. *Infoleg*: Buenos Aires, 2000. Disponible en: https://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm. Acceso el: 1 oct. 2023.

REPÚBLICA ARGENTINA. Ley 26.994/2015. Código Civil y Comercial de la Nación Argentina. *Infoleg*: Buenos Aires, 2015. Disponible en: https://servicios.infoleg.gob.ar/infolegInternet/anexos/235000-239999/235975/texact.htm. Acceso el: 1 oct. 2023.

REPÚBLICA ARGENTINA. Ley 27.699 – Convenio 108+ aprobación del protocolo modificatorio del convenio 108 para la con respecto al tratamiento automatizado de datos de carácter personal,

suscripto en la ciudad de Estrasburgo – República Francesa – el 10 de octubre de 2018. *Gobierno de Argentina*: Buenos Aires, 2018. Disponible en: https://www.argentina.gob.ar/normativa/nacional/ley-27699-375738. Acceso el: 1 oct. 2023.

REPÚBLICA ARGENTINA. Ley nº 27.506, de 10 de junio de 2019. Régimen de promoción de La economía del conocimiento. *Gobierno de Argentina*: Buenos Aires, 2019. Disponible en: https://www.argentina.gob.ar/normativa/nacional/ley-27506-324101/actualizacion. Acceso el: 15 dic. 2023.

RESOLUCIÓN sobre estándares internacionales en materia de protección de datos y privacidad. *In:* CONFERENCIA INTERNACIONAL DE AUTORIDADES DE PROTECCIÓN DE DATOS Y PRIVACIDAD, 31., Madrid, 2009. *Annales* [...]. Madrid: [*s. n.*], 2009.

UNIÓN EUROPEA. Tribunal de Justicia. *Sentencia nº C-362/14.* Maximillian Schrems *vs.* Data Protection Commissioner. Luxemburgo, 6 oct. 2015.

UNIÓN EUROPEA. *Directiva 95/46 C.E.E. del Parlamento Europeo y del Consejo.* 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. Luxemburgo: Unión Europea, 24 oct. 1995. Disponible en: https://eur-lex.europa.eu/legal-content/es/ALL/?uri=CELEX%3A31995L0046. Acceso en: 1 oct. 2023.

UNIÓN EUROPEA. *Reglamento nº 679/2016.* Relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. DOUE L 119. Bruselas: Unión Europea, 4 mayo 2016.

Informação bibliográfica deste texto, conforme a NBR 6023:2018 da Associação Brasileira de Normas Técnicas (ABNT):

RODRIGUEZ, Ana Rosa. Gobernanza de datos, herramientas digitales en el mundo del trabajo y la economía: análisis del régimen legal y sus perspectivas. *International Journal of Digital Law – IJDL*, Belo Horizonte, ano 4, n. 3, p. 11-41, set./dez. 2023. DOI: 10.47975/digital.law.vol.4.n.3.rosarodriguez.

Sobre a Revista

IJDL – INTERNATIONAL JOURNAL OF DIGITAL LAW

Objetivo

O International Journal of Digital Law é um periódico científico eletrônico de acesso aberto e periodicidade quadrimestral promovido pelo **Núcleo de Pesquisas em Políticas Públicas e Desenvolvimento Humano (NUPED), do Programa de Pós-Graduação em Direito da Pontifícia Universidade Católica do Paraná**.

O Conselho Editorial é composto por renomados professores vinculados a instituições de ensino superior do Brasil, Argentina, Austrália, Colômbia, Espanha, Egito, França, Holanda e Índia. A linha editorial segue o eixo das atividades de pesquisa do NUPED, um grupo inscrito no diretório do CNPq e filiado à **Rede de Pesquisa em Direito Administrativo Social (REDAS)**. Seu enfoque é o estudo crítico das instituições jurídico-políticas típicas do Estado de Direito, notadamente as voltadas à inovação e ao desenvolvimento humano por intermédio da revolução digital.

Linha Editorial

A linha editorial segue o eixo de concentração do **NUPED – PPGD/PUCPR** intitulada "**Direito Econômico e Desenvolvimento**". Por sua vez, a área congrega duas importantes linhas de pesquisa: 1. **Estado, Economia e Desenvolvimento** e 2. **Direitos Sociais, Globalização e Desenvolvimento**. A revista dará destaque a este marco teórico. Entretanto, transversalmente ao tema da economia, do desenvolvimento, da globalização e dos direitos sociais, as palavras-chave que melhor definem o escopo da revista implicam a tratativa de temas como: acesso à informação, *big data*, *blockchain*, cidades inteligentes, contratos inteligentes, *crowdsourcing*, cibercrimes, democracia digital, direito à privacidade, direitos fundamentais, *e-business*, economia digital, educação digital, eficiência administrativa, e-*government*, *fake news*, *gig economy*, globalização, inclusão digital, infraestrutura, inovação, inteligência artificial, interesse público, internet, internet das coisas, jurimetria, *lawfare*, novas tecnologias, perfilamento digital, pesquisa em multimeios, processo administrativo eletrônico, proteção de dados, regulação administrativa, regulação econômica, risco, serviços públicos, sistemas de informação, sociedade da informação, transparência governamental e telecomunicações.

Double blind peer review

A publicação dos artigos submete-se ao procedimento *double blind peer review*. Os trabalhos são remetidos sem identificação de autoria a dois pareceristas *ad hoc* portadores de título de doutor, todos eles exógenos à instituição promotora da revista (PUCPR). Os pareceristas são, portanto, sempre pesquisadores vinculados a renomadas instituições de ensino superior nacionais e estrangeiras.

Cobertura temática (classificação do CNPq)

GRANDE: Ciências Sociais Aplicadas (6.00.00.00-7)/Área: Direito (6.01.00.00-1)/ Subárea: Direitos Especiais (6.01.04.00-7)

GRANDE: Ciências Sociais Aplicadas (6.00.00.00-7)/Área: Ciência da Informação (6.07.00.00-9)/Subárea: Teoria da Informação (6.07.01.00-5)

GRANDE: Ciências Exatas e da Terra (1.00.00.00-3)/Área: Ciência da Computação 1.03.00.00-7/Subárea: Sistemas de Computação (1.03.04.00-2)

Diretrizes para Autores

1. Submissão de artigos
As propostas de artigos para publicação na *International Journal of Digital Law* deverão ser enviadas através do sistema eletrônico de submissões (gratuitamente), por meio de cadastro no Sistema Eletrônico e acesso mediante login e senha a ser realizado no site. Não serão aceitas propostas enviadas por e-mail. A revista reserva-se o direito de aceitar ou rejeitar qualquer original recebido, de acordo com as recomendações do seu corpo editorial, inclusive por inadequação da temática do artigo ao perfil editorial da revista, como também o direito de propor eventuais alterações.

2. Qualificação dos autores
Ao menos um dos autores do artigo deverá possuir o título de Doutor (Dr.), Doctor of Juridical Science (J.S.D. ou S.J.D.), Doctor juris (Dr. iur. ou Dr. jur.), Doctor of Philosophy (Ph.D.) ou Legum Doctor (LL.D.). A exigência poderá ser relativizada, nunca extrapolando o percentual de 30% por edição, em casos excepcionais de: (i) artigos de autores afiliados a instituições estrangeiras; (ii) artigos escritos em inglês.

3. Ineditismo e exclusividade
Os textos para publicação na *International Journal of Digital Law* deverão ser inéditos e para publicação exclusiva, salvo no caso de artigos em língua estrangeira que tenham sido publicados fora do país. Uma vez publicados nesta revista, também poderão sê-lo em livros e coletâneas, desde que citada a publicação original. Roga-se aos autores o compromisso de não publicação em outras revistas e periódicos, bem como de que as propostas de artigo não se encontrem postulados de forma simultânea em outras revistas ou órgãos editoriais.

4. Idiomas
Podem ser submetidos artigos redigidos em Português, Espanhol ou Inglês.

5. Cadastro dos metadados no sistema eletrônico de submissões
5.1. No momento da submissão do artigo no sistema eletrônico, os campos dos metadados deverão ser preenchidos obrigatoriamente de acordo com estas diretrizes, sob pena de rejeição liminar da submissão.
5.2. Autores
5.2.1. *Nome/Nome do Meio/Sobrenome:* indicação do nome completo do(s) autor(es) apenas com as iniciais de cada nome em caixa alta. Em caso de artigos em coautoria, os nomes de todos os coautores devem ser inseridos no sistema na ordem que deverá constar no momento da publicação.
5.2.2. *E-mail:* indicação do e-mail do(s) autor(es) para contato, que será obrigatoriamente divulgado na versão publicada do artigo.
5.2.3. *ORCID iD:* indicação do número de identificação ORCID (para maiores informações clique aqui). O identificador ORCID pode ser obtido no registro ORCID. Você deve aceitar os padrões para apresentação de iD ORCID e incluir a URL completa; por exemplo: https://orcid.org/0000-0003-1781-1726.

5.2.4. *URL:* link para o currículo completo do autor. No caso de autores brasileiros, deve ser indicado o link para o Currículo Lattes.
5.2.5. *Instituição/Afiliação:* indicação da sua principal afiliação institucional ou das duas principais, caso o vínculo com ambas possua a mesma importância (instituição à qual encontra-se vinculado como docente ou discente, ou, caso não seja docente ou discente, a instituição onde foi obtido o seu maior título acadêmico, como doutorado, mestrado, especialização etc.). O nome da instituição deverá constar por extenso e na língua original da instituição (ou em inglês quando a escrita não for latina), seguida da indicação do país de origem da instituição entre parênteses. Caso o autor seja docente e esteja cursando mestrado ou doutorado em outra instituição, a afiliação principal será a da instituição na qual o autor figura como mestrando ou doutorando.
5.2.6. *País:* indicação do país da principal afiliação institucional do autor.
5.2.7. *Resumo da biografia:* indicação do mini currículo, iniciando com a indicação da instituição onde figura como docente, seguida de cidade, sigla do Estado e país entre parênteses, indicação das titulações acadêmicas (começando pela mais elevada), outros vínculos com associações científicas, profissão etc.
5.3. Título e Resumo
5.3.1. *Título:* título no idioma do artigo, com apenas a primeira letra da sentença em maiúscula.
5.3.2. *Resumo:* resumo no idioma do artigo, sem parágrafo ou citações e referências, com até 200 palavras.
5.4. Indexação
5.4.1. *Palavras-chave*: indicação de 5 palavras-chave no idioma do artigo (em letras minúsculas e separadas por ponto vírgula).
5.4.2. *Idioma*: indicar a sigla correspondente ao idioma do artigo (Português=pt; English=en; Español=es).
5.5. Contribuidores e Agências de fomento: os artigos resultantes de projetos de pesquisa financiados deverão indicar neste campo a fonte de financiamento.
5.6. Referências: inserir a lista completa de referências citadas no artigo, dando um espaço entre cada uma delas.

6. Apresentação do texto e elementos pré-textuais
6.1. Recomenda-se que o trabalho tenha entre 15 e 30 páginas (tamanho A4 – 21 cm x 29,7 cm), compreendendo a introdução, desenvolvimento, conclusão (não necessariamente com esses títulos) e uma lista de referências bibliográficas.
6.2. As margens utilizadas deverão ser: esquerda e superior de 3 cm e direita e inferior de 2 cm.
6.3. No corpo do texto deverá ser utilizada Fonte Times New Roman, tamanho 12, espaçamento entre linhas de 1,5 cm e espaçamento de 0 pt (pontos) antes e depois dos parágrafos.
6.4. Nas notas de rodapé deverá ser utilizada Fonte Times New Roman, tamanho 10, espaçamento simples entre linhas.
6.5. No desenvolvimento do texto, os parágrafos deverão conter recuo de 1,5 cm em relação à margem esquerda. Títulos e subtítulos deverão estar alinhados à margem esquerda, sem recuo.
6.6. A estruturação deverá observar a exposta neste item 6.6.

6.6.1. Título no idioma do artigo, com apenas a primeira letra da sentença em maiúscula e em itálico, centralizado.
6.6.2. Nos casos de necessidade de indicar informações a respeito do artigo (financiamento por agências de fomento, agradecimentos, tradutores do texto etc.), deverá ser inserida uma nota de rodapé com um asterisco (e não com número) situada à direita do título no idioma do artigo.
6.6.3. Título em inglês, com apenas a primeira letra da sentença em maiúscula, em itálico e centralizado. No caso de artigos redigidos em inglês, este elemento deverá ser substituído pelo título em português.
6.6.4. O artigo não deve incluir os nomes do(s) autor(es). As informações, para fins de publicação, serão retiradas dos metadados inseridos pelo(s) autor(es) no sistema eletrônico da revista no momento da submissão.
6.6.5. Resumo no idioma do artigo (fonte Times New Roman 12, espaçamento entre linhas simples, sem parágrafo ou citações e referências, com até 200 palavras), antecedido da palavra "Resumo" escrita no idioma do artigo.
6.6.6. Indicação de 6 palavras-chave no idioma do artigo (em letras minúsculas e separadas por ponto vírgula), antecedidas da expressão "Palavras-chave" redigida no idioma do artigo.
6.6.7. Resumo em inglês (Fonte Times New Roman 12, espaçamento entre linhas simples, sem parágrafo ou citações e referências, com até 200 palavras), antecedido da palavra "Abstract". No caso de artigos redigidos em inglês, este elemento deverá ser substituído pelo resumo em português.
6.6.8. Indicação de seis palavras-chave em inglês (em letras minúsculas e separadas por ponto e vírgula), antecedidas da expressão "Keywords". No caso de artigos redigidos em inglês, este elemento deverá ser substituído pelas palavras-chave em português.
6.6.9. Sumário com a identificação dos títulos das seções e das subseções, com numeração progressiva, separados por ponto vírgula, sequencialmente e em parágrafo único.
6.6.10. Desenvolvimento do trabalho científico: a numeração progressiva, em números arábicos, deve ser utilizada para evidenciar a sistematização do conteúdo do trabalho.
6.6.11. Lista das referências bibliográficas efetivamente utilizadas no artigo, ao final do trabalho, separadas por um espaço simples, alinhadas à margem esquerda (sem recuo).
6.6.12. Aplicam-se, para os demais aspectos de formatação, as normas técnicas brasileiras (ABNT NBR 10520:2002 e 14724:2011).
6.6.13. No caso de artigos com 4 ou mais autores, é necessário incluir uma nota de rodapé indicando qual foi a contribuição de cada um.
6.7. Todo destaque que se queira dar ao texto deve ser feito com o uso de itálico, ficando vedada a utilização de negrito, sublinhado ou caixa alta para fins de dar destaque ao texto.
6.8. Figuras e tabelas devem estar inseridas no texto, e não no final do documento na forma de anexos.

7. Metodologia científica
7.1. As referências dos livros, capítulos de obras coletivas, artigos, teses, dissertações e monografias de conclusão de curso de autores citados ou utilizados como base

para a redação do texto devem constar em nota de rodapé, com todas as informações do texto, em observância às normas técnicas brasileiras (ABNT NBR 6023:2018), e, especialmente, com a indicação da página da qual se tirou a informação apresentada no texto logo após a referência.

7.1.1. O destaque dado ao título dos livros (ou revistas) citados deverá constar em itálico, ficando vedada a utilização de negrito.

7.1.2. Os artigos redigidos com citação no formato AUTOR-DATA não serão aceitos para publicação, somente o sistema de chamadas numérico exposto nas notas de rodapé.

7.1.3. As referências deverão constar da seguinte forma:

7.1.3.1. Livros:

SOBRENOME, Nome. *Título da obra em itálico*: subtítulo sem itálico. número da edição. Cidade: Editora, ano.

Exemplo:

KEEN, Andrew. *Vertigem digital*: por que as redes sociais estão nos dividindo, diminuindo e desorientando. Trad. Alexandre Martins, Rio de Janeiro: Zahar, 2012. 254p.

7.1.3.2. Capítulos de livros coletivos:

SOBRENOME, Nome. Título do capítulo sem itálico. In: SOBRENOME DO 1º ORGANIZADOR, Nome do organizador; SOBRENOME DO 2º ORGANIZADOR, Nome do 2º organizador e assim sucessivamente, separados por ponto vírgula (Org. ou Coord.). *Título da obra ou coletânea em itálico*: subtítulo sem itálico. número da edição. Cidade: Editora, ano. página inicial-página final [antecedidas de "p."].

Exemplo**:**

DOTTA, Alexandre Godoy. Derechos de la Población LGBT+ en Brasil: Vulnerabilidad Social entre Avances y Retrocesos. In: BRAVO, Álvaro Sánches; CASIMIRO, Ligia Melo de; GABARDO, Emerson. (Org.). *Estado Social Y Derechos Fundamentales en Tiempos de Retroceso*. Sevilha: Ponto Rojo, 2019. p. 203-228.

7.1.3.3. Artigos em revistas:

SOBRENOME, Nome. Título do artigo sem itálico. *Título da Revista em itálico*, cidade, volume, número, página inicial-página final [antecedidas de "p."], meses da publicação [abreviados com as três primeiras letras do mês seguidas de ponto e separados por barra]. ano.

Exemplo:

GABARDO, Emerson; SAIKALI, Lucas Bossoni. A prescritibilidade da ação de ressarcimento ao erário em razão de atos de improbidade administrativa. *Revista Jurídica – Unicuritiba*, Curitiba, v. 1, p. 514-543, 2018.

7.1.3.4. Teses de Titularidade, Livre-Docência, Doutorado, Dissertações de Mestrado, Monografias de Conclusão de Curso de Graduação e Pós-Graduação:

SOBRENOME, Nome. *Título do trabalho em itálico*: subtítulo sem itálico. Cidade, ano. número de folhas seguido de "f". Modalidade do trabalho (Grau obtido com a defesa) – Órgão perante o qual o trabalho foi defendido, Nome da instituição.

Exemplo:

SANTOS, Fábio de Sousa. *Análise Comparada da Competição na Contratação Pública Brasileira e Estadunidense*. Curitiba, 2018. 134f. Dissertação (Mestrado em Mestrado em Direito) – Pontifícia Universidade Católica do Paraná. Curitiba: 2018.

7.1.3.5 DOI – Digital object identifier: Caso o documento consultado na pesquisa tenha o número de DOI recomenda-se a inclusão, de modo complementar, do número após o término de cada referência.
Exemplo:
DOTTA, Alexandre Godoy. Public policies for the assessment of quality of the Brazilian higher education system. *Revista de Investigações Constitucionais*, Curitiba, v. 3, p. 53-69, 2016. DOI. 10.5380/rinc.v3i3.49033.
7.1.3.6. Documentos em meio eletrônico: Documentos extraídos do meio eletrônico deverão apresentar após o término de cada referência o local da rede onde foi encontrado e apresentado da seguinte maneira.
Exemplo:
IJDL. International Journal of Digital Law. *Regras para a submissão de artigos*. Disponível em: https://journal.nuped.com.br/index.php/revista/about/submissions. Acesso em: 12 fev. 2020.
7.1.4. Os elementos das referências devem observar o seguinte padrão:
7.1.4.1. Autor: SOBRENOME em maiúsculas, vírgula, Nome com as iniciais em maiúsculas, seguido de ponto final.
7.1.4.2. Edição: deve ser incluída a informação somente a partir da segunda edição, sem ordinal, seguido de ponto e "ed.". Exemplo: 2. ed.
7.1.4.3. Ano: grafado com algarismos arábicos, sem ponto no milhar, antecedido de vírgula e seguido de ponto.
7.1.5. Nos casos em que for absolutamente impossível obter alguma das informações acima, a ausência deverá ser suprida da seguinte forma:
7.1.5.1. Ausência de cidade: substituir por [S.l.].
7.1.5.2. Ausência de editora: substituir por [s.n.].
7.1.5.3. Ausência de ano: indicar entre colchetes o ano aproximado, seguido de ponto de interrogação. Exemplo: [1998?].
7.2. As citações (palavras, expressões, períodos) deverão ser cuidadosamente conferidas aos textos originais.
7.2.1. Citações diretas devem seguir o seguinte padrão de registro: transcrição com até quatro linhas devem constar do corpo do texto, com letra e espaçamento normais, e estar entre aspas.
7.2.2. Recomenda-se fortemente que citações textuais longas (mais de quatro linhas) não sejam utilizadas. Entretanto, se imprescindíveis, deverão constituir um parágrafo independente, com recuo de 1,5 cm em relação à margem esquerda (alinhamento justificado), utilizando-se espaçamento entre linhas simples e tamanho da fonte 10. Neste caso, aspas não devem ser utilizadas.
7.2.3. Fica vedado o uso do op. cit., loc. cit., ibidem e idem nas notas bibliográficas, que deverão ser substituídas pela referência completa, por extenso.
7.2.4. Para menção de autores no corpo do texto, fica vedada sua utilização em caixa alta (ex.: para Nome SOBRENOME...). Nestes casos todas as menções devem ser feitas apenas com a primeira letra maiúscula (ex.: para Nome Sobrenome...).

8. Redação
8.1. Os textos devem ser revisados, além de terem sua linguagem adequada a uma publicação editorial científica.

8.2. No caso de artigos redigidos na língua portuguesa, a escrita deve obedecer às regras ortográficas em vigor desde a promulgação do ACORDO ORTOGRÁFICO DA LÍNGUA PORTUGUESA, a partir de 1º de janeiro de 2009.
8.3. As citações de textos anteriores ao ACORDO devem respeitar a ortografia original.

9. Artigos resultantes de pesquisas financiadas
Os artigos resultantes de projetos de pesquisa financiados deverão indicar em nota de rodapé, situada ao final do título do artigo no idioma do texto, a informação relativa ao financiamento da pesquisa.

10. Declaração de direitos autorais
Autores que publicam nesta revista concordam com os seguintes termos:
10.1. Não serão devidos direitos autorais ou qualquer outra remuneração pela publicação dos trabalhos.
10.2. Autores mantêm os direitos autorais e concedem à *IJDL* o direito de primeira publicação, com o trabalho simultaneamente licenciado sob a Licença Creative Commons Attribution que permite o compartilhamento do trabalho com reconhecimento da autoria e publicação inicial nesta revista. Ainda, em virtude de aparecerem nesta revista de acesso público, os artigos são de uso gratuito, com atribuições próprias, com aplicações educacionais e não comerciais.
10.3. Autores têm permissão e são estimulados a publicar e distribuir seu trabalho online (ex.: em repositórios institucionais ou na sua página pessoal) a qualquer ponto antes ou durante o processo editorial, já que isso pode gerar alterações produtivas, bem como aumentar o impacto e a citação do trabalho publicado (ver O Efeito do Acesso Livre).

11. Responsabilidade dos autores
11.1. Autores são responsáveis pelo conteúdo publicado, comprometendo-se, assim, a participar ativamente da discussão dos resultados de sua pesquisa científica, bem como do processo de revisão e aprovação da versão final do trabalho.
11.2. Autores são responsáveis pela condução, resultados e validade de toda investigação científica.
11.3. Autores devem noticiar a revista sobre qualquer conflito de interesse.
11.4. As opiniões emitidas pelos autores dos artigos são de sua exclusiva responsabilidade.
11.5. Ao submeter o artigo, o autor atesta que todas as afirmações contidas no manuscrito são verdadeiras ou baseadas em pesquisa com razoável exatidão.

12. Conflito de interesses
A confiabilidade pública no processo de revisão por pares e a credibilidade de artigos publicados dependem em parte de como os conflitos de interesses são administrados durante a redação, revisão por pares e tomada de decisões pelos editores.
12.1. É obrigatório que o autor do manuscrito declare a existência ou não de conflitos de interesse. Mesmo julgando não haver conflitos de interesse, o autor deve declarar essa informação no ato de submissão do artigo, marcando esse campo específico.
12.2. Conflitos de interesses podem surgir quando autores, pareceristas ou editores possuem interesses que, aparentes ou não, podem influenciar a elaboração ou avaliação

de manuscritos. O conflito de interesses pode ser de natureza pessoal, comercial, política, acadêmica ou financeira.

12.3. Quando os autores submetem um manuscrito, eles são responsáveis por reconhecer e revelar conflitos financeiros ou de outra natureza que possam ter influenciado seu trabalho.

12.4. Os autores devem reconhecer no manuscrito todo o apoio financeiro para o trabalho e outras conexões financeiras ou pessoais com relação à pesquisa. As contribuições de pessoas que são mencionadas nos agradecimentos por sua assistência na pesquisa devem ser descritas, e seu consentimento para publicação deve ser documentado.

12.5. Manuscritos não serão rejeitados simplesmente por haver um conflito de interesses, mas deverá ser feita uma declaração de que há ou não conflito de interesses.

12.6. Os pareceristas devem, igualmente, revelar aos editores quaisquer conflitos de interesse que poderiam influir em suas opiniões sobre o manuscrito, e devem declarar-se não qualificados para revisar originais específicos se acreditarem que esse procedimento é apropriado. Assim como no caso dos autores, se houver silêncio por parte dos pareceristas sobre conflitos potenciais, isso significará que os conflitos não existem.

12.7. No caso da identificação de conflito de interesse da parte dos pareceristas, o Conselho Editorial encaminhará o manuscrito a outro parecerista *ad hoc*.

12.8. Se os autores não tiverem certeza do que pode constituir um potencial conflito de interesses, devem contatar o Coordenador Editorial da Revista.

12.9. Para os casos em que editores ou algum outro membro publiquem com frequência na Revista, não serão atribuídos tratamentos especiais ou diferenciados. Todos os artigos submetidos serão avaliados através do procedimento *double blind peer review*.

13. Outras informações

13.1. Os trabalhos serão selecionados pelo Coordenador Editorial e pelo Conselho Editorial da Revista, que entrarão em contato com os respectivos autores para confirmar o recebimento dos textos, e em seguida os remeterão para análise de dois pareceristas do Conselho de Pareceristas.

13.2. Os originais recebidos e não publicados não serão devolvidos.

13.3. Asseguram-se aos autores o direito de recurso das decisões editorais.

13.3.1. Serão concedidos 5 (cinco) dias, contados da data da decisão final do Conselho Editorial.

13.3.2. O arrazoado escrito deverá ser enviado para o e-mail: journal@nuped.com.br.

13.3.3. O recurso será analisado pelo Conselho Editorial no prazo de 30 (trinta) dias.

CONDIÇÕES PARA SUBMISSÕES

Como parte do processo de submissão, os autores são obrigados a verificar a conformidade da submissão em relação a todos os itens listados a seguir. As submissões que não estiverem de acordo com as normas serão devolvidas aos autores.

1. A contribuição é original e inédita (salvo em caso de artigos em língua estrangeira publicados no exterior), e não está sendo avaliada para publicação por outra revista; caso contrário, deve-se justificar em “Comentários ao editor”.
2. O arquivo da submissão está em formato Microsoft Word.
3. URLs para as referências foram informadas quando possível.

4. O texto possui entre 15 e 30 páginas (tamanho A4 – 21 cm x 29,7 cm), compreendendo a introdução, desenvolvimento, conclusão (não necessariamente com esses títulos) e uma lista de referências bibliográficas; as margens utilizadas são: esquerda e superior de 3 cm e direita e inferior de 2 cm; no corpo do texto utilizou-se Fonte Times New Roman, tamanho 12, espaçamento entre linhas de 1,5, e espaçamento de 0 pt antes e depois dos parágrafos; nas notas de rodapé utilizou-se Fonte Times New Roman, tamanho 10, espaçamento simples entre linhas; no desenvolvimento do texto, os parágrafos contêm recuo de 1,5 cm em relação à margem esquerda; títulos e subtítulos estão alinhados à margem esquerda, sem recuo; as figuras e tabelas estão inseridas no texto, não no final do documento na forma de anexos.
5. O texto segue os padrões de estilo e requisitos bibliográficos descritos em Diretrizes para Autores, na página para submissão.
6. Em caso de submissão a uma seção com avaliação pelos pares (ex.: artigos), as instruções disponíveis em Assegurando a avaliação pelos pares cega foram seguidas.
7. O autor declara que, com exceção das citações diretas e indiretas claramente indicadas e referenciadas, este artigo é de sua autoria e, portanto, não contém plágio. Declara, ainda, que está ciente das implicações legais que a utilização de material de terceiros acarreta.
8. O autor declara que participou suficientemente do trabalho para tornar pública sua responsabilidade pelo conteúdo e que todas as afirmações contidas no manuscrito são verdadeiras ou baseadas em pesquisa com razoável exatidão.
9. O autor concorda com a política de responsabilidade estabelecida no item 10. Responsabilidade dos autores das Diretrizes para Autores.

POLÍTICA DE PRIVACIDADE

Os nomes e endereços informados nesta revista serão usados exclusivamente para os serviços prestados por esta publicação, não sendo disponibilizados para outras finalidades ou a terceiros.

Este periódico tem um compromisso com a ética e a qualidade das publicações, seguindo padrões internacionais de publicação científica. Defendemos um comportamento ético de todas as partes envolvidas na publicação em nosso periódico: autores, editor, pareceristas, Equipe Editorial e a Editora. Não aceitamos plágio ou qualquer outro comportamento antiético. Para isso, são seguidas as diretrizes do 2nd World Conference on Research Integrity, Singapore, July 22-24, 2010.

Deveres do Editor

- **Decisão de publicação:** o editor é responsável por decidir quais artigos submetidos à revista devem ser publicados. O editor é guiado pelas políticas decididas pelo Conselho Editorial. Essas políticas devem obedecer às exigências legais em vigor sobre difamação, violação de direitos autorais e plágio. Para tomada de decisões o editor pode consultar o Conselho Editorial e os pareceristas.
- **Transparência e respeito:** o editor deve avaliar os manuscritos submetidos sem levar em conta a raça, sexo, a orientação sexual, a crença religiosa, a origem étnica, a nacionalidade ou a filosofia política dos autores.

- **Confidencialidade:** o editor e demais membros da equipe editorial não devem divulgar qualquer informação sobre um manuscrito submetido, a não ser aos pareceristas e os conselheiros editoriais.
- **Divulgação e conflitos de interesse:** O editor não deve utilizar materiais inéditos divulgados em um manuscrito submetido em pesquisas próprias sem o consentimento expresso e por escrito do autor. O editor deve recusar avaliar os manuscritos em que tenha conflitos de interesse por questões competitivas, colaborativas ou outros relacionamentos ou ligações com qualquer um dos autores, empresas ou (possivelmente) instituições ligadas aos manuscritos.
- **Envolvimento e cooperação em investigações:** o editor deve tomar medidas necessárias cabíveis quando foram apresentadas reclamações éticas a respeito de um manuscrito submetido ou artigo publicado.

Deveres dos Pareceristas

- **Contribuição para as decisões editoriais:** a revisão dos pareceristas auxilia o editor na tomada de decisões editoriais e por meio das comunicações com o autor também pode auxiliar o mesmo na melhora do artigo.
- **Pontualidade:** qualquer avaliador de artigo que não se sinta qualificado para analisar o artigo ou sabe que a sua imediata leitura será impossível deve notificar imediatamente o editor.
- **Confidencialidade:** os trabalhos recebidos para análise devem ser tratados como documentos confidenciais. Eles não devem ser mostrados ou discutidos com os outros.
- **Padrões de objetividade:** os pareceres devem ser conduzidos de forma objetiva. Os pareceristas devem expressar seus pontos de vista de maneira clara e apoiados em argumentos.
- **Sobre as fontes:** os pareceristas devem identificar trabalhos publicados relevantes que não foram citados pelos autores. O parecerista deve chamar a atenção do editor sobre qualquer semelhança substancial ou sobreposição entre o manuscrito em questão e qualquer outro *artigo* publicado de que tenha conhecimento pessoal.
- **Divulgação e conflito de interesses:** informações privilegiadas ou ideias obtidas pelo parecerista por meio da leitura dos manuscritos devem ser mantidas em sigilo e não devem utilizadas para proveito pessoal. O parecerista não deve avaliar manuscritos em que tenha conflitos de interesse por questões competitivas, colaborativas ou outros relacionamentos ou ligações com qualquer um dos autores, empresas ou instituições ligadas aos manuscritos.

Deveres dos Autores

- **Normas gerais:** os autores de trabalhos que se referem a pesquisas originais devem apresentar um relato preciso do trabalho realizado, bem como uma discussão objetiva sobre o seu significado. Dados complementares devem ser representados com precisão no artigo. O documento deve conter detalhes suficientes e referências que permitam que outros possam replicar o trabalho. Declarações fraudulentas ou intencionalmente imprecisas constituem um comportamento antiético e são inaceitáveis.

- **Originalidade e plágio:** os autores devem garantir que as obras são inteiramente originais e se eles utilizam o trabalho e/ou textos dos outros que isso seja devidamente citado. Plágio em todas as suas formas constitui um comportamento editorial antiético e é inaceitável.
- **Publicação múltipla ou redundante:** um autor não deve publicar manuscritos que descrevam essencialmente a mesma pesquisa em mais de um periódico. Publicar o mesmo artigo em mais de um periódico sem informar os editores e obter seu consentimento constitui um comportamento editorial antiético e é inaceitável.
- **Sobre as fontes:** o trabalho de outros autores deve sempre ser reconhecido. Os autores devem citar as publicações que foram importantes na determinação da natureza do trabalho relatado. As informações obtidas em particular, como em uma conversa, correspondência, ou discussão com terceiros, não devem ser utilizadas ou relatadas sem a permissão explícita por escrito da fonte. As informações obtidas por meio de serviços confidenciais, tais como arbitragem manuscritos ou pedidos de bolsas, não devem ser utilizadas sem a permissão explícita por escrito do autor do trabalho envolvido nestes serviços.
- **Autoria:** a autoria do trabalho deve ser restrita àqueles que fizeram uma contribuição significativa para a concepção, projeto, execução ou interpretação do estudo relatado. Todos aqueles que fizeram contribuições significativas devem ser listados como coautores. Pessoas que participaram em certos aspectos do projeto de pesquisa devem ser listadas como colaboradores. O autor principal deve garantir que todos os coautores apropriados estejam incluídos no artigo. O autor principal também deve certificar-se que todos os coautores viram e aprovaram a versão final do manuscrito e que concordaram com sua submissão para publicação.
- **Divulgação e conflitos de interesses:** todos os autores devem divulgar no manuscrito qualquer conflito financeiro ou de outra natureza que possa influenciar os resultados ou a interpretação de seu manuscrito. Todas as fontes de apoio financeiro para o projeto devem ser divulgadas.
- **Erros fundamentais em trabalhos publicados:** quando um autor descobre um erro significativo ou imprecisão em seu trabalho publicado é obrigação do autor informar imediatamente o editor da revista ou a Editoria de Periódicos e cooperar com o editor para corrigir o artigo.

Deveres da Editora

Estamos empenhados em garantir que publicidade, reimpressão ou qualquer outra fonte de receita comercial não tenha qualquer impacto ou influência sobre as decisões editoriais.

Nossos artigos são avaliados por pares para garantir a qualidade da publicação científica. Este periódico utiliza o CrossCheck (software antiplágio da CrossRef).

* Esta declaração se baseia nas recomendações da Elsevier e no *Best Practice Guidelines for Journal Editors* do Committee on *Publication Ethics – COPE*.

Author Guidelines

1. Article Submission

Article propositions for publishing on the International Journal of Digital Law must be sent through the electronic submission system (free of cost) and access through login and password. Propositions sent by e-mail will not be accepted. The Journal has the right to accept or reject any originals received, according to its Editorial Board's recommendations, including the inadequacy of the article's theme to the journal's editorial profile, as well as the right to propose modifications.

2. Author Qualification

At least one of the authors must own either a PhD degree or a Doctor of Juridical Science (J.S.D. or S.J.D), Doctor juris (Dr. iur. or Dr. jur.), Doctor of Philosophy (Ph.D.) ou Legum Doctor (LL.D.) degree. This requirement can be relativized, never exceeding 30% of the articles per edition, in exceptional cases of: (i) authors affiliated to foreign institutions; (ii) articles written in English.

3. Originality and exclusivity

Articles for publication in the International Journal of Digital Law must be original and exclusive, except in case of articles written in a foreign language and published outside Brazil. After the publication of the article in this journal, it can also be published in books and compilations, as long as the original publication is mentioned. We ask the authors to commit to not publish the article in other journals or reviews, as well as not to submit it to other journals at the same time.

4. Languages

Articles can be submitted in English, Portuguese, and Spanish.

5. Registration of the metadata in the electronic submission system

5.1. At the time of submission of the article to the electronic system, the metadata fields must be filled in according to these guidelines, under penalty of preliminary rejection of the submission.

5.2. Authors

5.2.1. *First name/Middle name/Last name:* indication of the full name of the author(s) with only the initials of each name in capital letter. In case of articles in co-authorship, the names of all coauthors must be inserted in the system in the order that should appear at the time of publication.

5.2.2. *E-mail:* indication of the e-mail address of the author(s) for contact, which will mandatorily appear in the published version of the article.

5.2.3. *ORCID iD:* indication of the number of the author's ORCID identifier (for further information click here). The ORCID identifier can be obtained in ORCID register. Authors must have to accept the patterns for presentation of ORCID iD and include the full URL (e.g.: https://orcid.org/0000-0003-1781-1726).

5.2.4. *URL:* link to the author's full curriculum. In the case of Brazilian authors, the link to the Lattes Curriculum should be indicated.

5.2.5. *Affiliation:* indication of the author's main institutional affiliation (or two main affiliations if both of the links with them have the same importance). The main institution is where the author is professor or student, or, in case of not being professor or student anymore, the institution where the authors obtained their major academic title (PhD, J.S.D., LL.M, B.A., etc.). The institution's name must be written in full (not abbreviated) and in the original language of the institution (or in English for non-Latin languages), followed by an indication of the country of origin of the institution between parentheses. If the author is a professor and also a PhD, J.S.D or LL.M candidate in another institution, the main affiliation will be the institution where the author is candidate.
5.2.6. *Country:* indication of the country of the author's main institutional affiliation.
5.2.7. *Bio Statement:* indication of the author's abbreviated CV, with the information organized in the following sequence: first, the indication of the institution to which the author is affiliated as a professor; second, between parentheses, the city, state/province (if applicable) and country of the institution; third, indication of academic titles (starting with the highest); fourth, other bonds with scientific associations; fifth, profession; etc.

5.3. Title and Abstract

5.3.1. *Title:* title in the language of the article, with only the first letter of the sentence in capital letter.
5.3.2. *Abstract:* abstract in the language of the article, without paragraph or citations and references, with up to 200 words.

5.4. Indexing

5.4.1. *Keywords:* indication of 5 keywords in the language of the article (in lower case and separated by semicolons).
5.4.2. *Language:* indicate the acronym corresponding to the language of the article (Português=pt; English=en; Español=es).
5.5. *Supporting Agencies:* articles resulting from funded research projects should indicate in this field the source of funding.
5.6. *References:* insert the complete list of references cited in the article, with a space of one line between them.

6. Text Presentation and pre-textual elements

6.1. The article must have between 15 and 30 pages (size A4 – 21 cm × 29,7 cm), including introduction, development and conclusion (not necessarily with these titles) and a bibliographic reference list. The maximum number of pages can be relativized in exceptional cases, decided by the Editorial team.
6.2. Edges (margins) must be: top and left with 3 cm, bottom and right with 2 cm.
6.3. The text must use Font Times New Roman, size 12, line spacing 1.5, and spacing 0 pt before and after paragraphs.
6.4. References must use Font Times New Roman, size 10, simple space between lines.
6.5. In the development of the text, the paragraphs must contain decrease of 1.5 cm from the left margin. Titles and subtitles must be aligned with the left margin without decrease.
6.6. The structure should observe the following order:

6.6.1. Title in the article's language, in bold, centralized, with the first letter of the sentence in capital letter.
6.6.2. In case of indicating information related to the article (financing from sponsoring agencies, acknowledgments, translators, etc.), it is necessary to insert a footnote with an asterisk (not number) on the right side of the title in the article's language.
6.6.3. Title in English, with only the first letter in capital letter, in bold and in italic, centralized. In the case of articles written in English, this element must be substituted by the title in Portuguese.
6.6.4. The article must not include the names of the author(s). The information for publication purposes will be taken from the metadata entered by the author(s) in the journal's electronic system at the time of submission.
6.6.5. Abstract in the article's language (font Times New Roman, 12, simples lines, without paragraph or quotations and references, until 200 words), preceded by the word "Abstract" written in the article's language.
6.6.6. Indication of five keywords in the article's language (in lower case and separated by semicolon), preceded by the expression "Keywords" written in the article's language.
6.6.7. Abstract in English (font Times New Roman, 12, simples lines, without paragraph or quotations and references, up to 200 words), preceded by the word "Abstract". In case of articles written in English, this element must be replaced by the abstract ("*resumo*") in Portuguese.
6.6.8. Indication of five keywords in English (in lower case and separated by semicolon), preceded by the expression "Keywords". In case of articles written in English, this element must be replaced by keywords ("*palavras-chave*") in Portuguese.
6.6.9. Table of contents, indicating the titles of the sections and subsections, with progressive numbering in Arabic numbers.
6.6.10. Development of the scientific article: progressive numbering, in Arabic numbers, must be used to make clear the content's systematization.
6.6.11. Bibliographic references list must bring only sources that were really used, located in the end of the article, separated by a simple space, lined to the left margin (no indent).
6.6.12. For other aspects, apply Brazilian technical norms (ABNT NBR 10520:2002 e 14724:2011).
6.6.13. In the case of articles with 4 or more authors, it is necessary to include a footnote indicating the contribution of each one to the article.
6.7. Highlights must be made only in italics, meaning that bold, underlined or caps lock, cannot be used to highlight.
6.8. Images and boards must be inserted in the text, not in the end in form of attachments.

7. Scientific Methodology

7.1. The references of books, chapters in collective books, articles, theses, dissertations/essays, monographs of quoted authors used as base to write the text must be mentioned as a reference on the footnotes, with all the information about the text, according to the Brazilian technical norms (ABNT NBR 6023:2018 – summarized in the item 7.1.3 below), and especially, indicating the page of which the information written on the text was taken, right after the reference.

7.1.1. Book's title (or journal's title) must be highlighted in italics (bold shall not be used for that purpose).
7.1.2. Articles written in the format AUTHOR-YEAR will not be accepted for publishing.
7.1.3. References shall appear as follows:
7.1.3.1. Books:
LAST NAME, Name Middle Name. *Title of the book in italics:* subtitle not in italics. Number of the edition. City: Publisher, Year.
Example:
KEEN, Andrew. *Vertigem digital*: por que as redes sociais estão nos dividindo, diminuindo e desorientando. Trad. Alexandre Martins, Rio de Janeiro: Zahar, 2012. 254p.
7.1.3.2. Chapter in a collective book:
LAST NAME, Name Middle Name. Title of the Chapter not in bold. In: ORGANIZER'S LAST NAME, Name Middle Name; 2ND ORGANIZER'S LAST NAME, Name Middle Name, and so on, separated by semicolon (Org. or Coord.). *Title of the book in italics***:** subtitle not in Italics. Number of the edition. City: Publisher, Year. first page-last page [preceded by "p."].
Example:
DOTTA, Alexandre Godoy. Derechos de la Población LGBT+ en Brasil: Vulnerabilidad Social entre Avances y Retrocesos. In: BRAVO, Álvaro Sánches; CASIMIRO, Ligia Melo de; GABARDO, Emerson. (Org.). *Estado Social Y Derechos Fundamentales en Tiempos de Retroceso*. Sevilha: Ponto Rojo, 2019. p. 203-228.
7.1.3.3. Articles in journals:
LAST NAME, Name Middle Name. Title of the article not in bold. *Title of the journal in italics*, city, volume, number, first page-last page [preceded by "p."], months of publishing [abbreviated with the first three letters of the month followed by dot and separated by a slash]. Year.
Example:
GABARDO, Emerson; SAIKALI, Lucas Bossoni. A prescritibilidade da ação de ressarcimento ao erário em razão de atos de improbidade administrativa. *Revista Jurídica – Unicuritiba*, Curitiba, v. 1, p. 514-543, 2018.
7.1.3.4. Theses of Full Professor contests, Doctoral theses, Master's dissertations/ essays, Undergraduate and Graduate courses monographs:
LAST NAME, Name Middle Name. *Title in italics:* subtitle. City, year. number of pages followed by "f". Kind of the work (Degree obtained with the defense) – Department or Sector, Name of the institution.
Example:
SANTOS, Fábio de Sousa. *Análise Comparada da Competição na Contratação Pública Brasileira e Estadunidense*. Curitiba, 2018. 134f. Dissertação (Mestrado em Mestrado em Direito) – Pontifícia Universidade Católica do Paraná. Curitiba: 2018.
7.1.3.5. DOI – Digital object identifier: If the document consulted in the research has the DOI number, it is recommended to include, in a complementary way, the number after the end of each reference. Example:
DOTTA, Alexandre Godoy. Public policies for the assessment of quality of the Brazilian higher education system. *Revista de Investigações Constitucionais*, Curitiba, v. 3, p. 53-69, 2016. DOI. 10.5380/rinc.v3i3.49033.

7.1.3.6. Documents in electronic media: Documents extracted from electronic media must present after the end of each reference the location of the network where it was found and presented as follows. Example:
DIJDL. International Journal of Digital Law*. Regras para a submissão de artigos*. Disponível em: https://journal.nuped.com.br/index.php/revista/about/submissions. Acesso em: 12 fev. 2020.
7.1.4. The elements of references must observe the following model:
7.1.4.1. **Author:** LAST NAME in capital letters, comma, Name with the initials in capital letters, Middle Name with the initials in capital letters, followed by a dot.
7.1.4.2. Edition: the information must only be included after the second edition of the book, without ordinal, followed by a dot and "ed.". Example: 2. ed.
7.1.4.3. Year: it must be written with Arabic numerals, without dot in thousand, preceded by comma, and followed by a dot**.** Example: 1997.
7.1.5. In case of being impossible to find one of those elements, the absence must be resolved in the following manner:
7.1.5.1. Absence of city: replace for [S.l.].
7.1.5.2. Absence of publisher: replace for [s.n.].
7.1.5.3. Absence of year: the approximated year must be indicated between brackets, followed by a question mark. Example: [1998?].
7.2. The quotations (words, expressions, sentences) must be carefully reviewed by the authors and/or translators.
7.2.1. The direct quotations must follow this pattern: transcription until four lines should fit in the text body, with normal letter, normal spacing and quotation marks.
7.2.2. It is strongly recommended that long textual quotations (more than four lines) are not used. However, if indispensable, they shall constitute an independent paragraph, with 1,5 cm of decrease related to the left margin (justified alignment), with simple lines and font 10. In that situation, quotation marks must not be used.
7.2.3. It is forbidden the use of "op. cit.", "loc. cit.", "ibidem" and "idem" in the footnotes. The references in footnote must be complete and written out.
7.2.4. For the mention of authors in the text body, it is forbidden the use of capital letters (e.g. for Name LAST NAME...). In this case all mentions shall be written only with the first letter in capital letter (ex.: for Name Last Name...).

8. Composition
8.1. Apart from having an adequate scientific language for an editorial publication, the text must be reviewed.
8.2. In the case of articles written in Portuguese, the writing must obey the new orthographic rules in force since the promulgation of the Portuguese Language Orthographic Agreement, from January 1st, 2009.
8.3. Citations of texts that precede the Agreement must respect the original spelling.

9. Articles resulted from funded researches
Articles resulted from funded research projects shall indicate in a footnote, located at the end of the article title in the original language, the information related to the research financing.

10. Copyright statement

Authors who publish in this Journal have to agree to the following terms:

10.1. No copyright or any other remuneration for the publication of papers will be due.

10.2. Authors retain copyright and grant the International Journal of Digital Law the right of first publication with the article simultaneously licensed under the Creative Commons Attribution License, which allows sharing the work with recognition of its initial publication in this Journal. Moreover, because of their appearance in this open access Journal, articles are free to use, with proper attribution, in educational and non-commercial applications.

10.3. Authors are allowed and encouraged to post their work online (e.g. in institutional repositories or on their personal webpage) at any point before or during the submission process, as it can lead to productive exchanges, as well as increase the impact and citation of published work (see The Effect of Open Access).

11. Authors responsibilities

11.1. Authors are responsible for the published content, committing therefore to participate actively in the discussion of the results of their scientific research, as well as the review process and approval of the final version of the work.

11.2. Authors are responsible for the conducting all the scientific research, as well as its results and validity.

11.3. Authors should report the Journal about any conflict of interest.

11.4. Authors are fully and exclusively responsible for the opinions expressed in their articles.

11.5. When submitting the articles, authors recognize that all statements contained in the manuscript are true or based on research with reasonable accuracy.

12. Conflict of interest

The public confidence in the double-blind peer review process and the credibility of published articles depend in part on how conflicts of interest are managed during manuscript writing, peer review and decision making by the editors.

12.1. It is mandatory that the author of the manuscript declares the existence or not of conflicts of interest. Even thinking that there are no conflicts of interest, the author must declare this information in the article submission act, marking that field.

12.2. Conflicts of interest may appear when authors, reviewers or editors have interests that, apparently or not, may influence the development or evaluation of manuscripts.

12.3. When authors submit a manuscript, they are responsible for recognizing and revealing financial or other nature conflicts that may have influenced their work.

12.4. Authors must recognize all the financial support for the work and other financial or personal connections related to the research. The contributions of people who are mentioned in the acknowledgments for their assistance in the research must be described, and its consent to publication should be documented.

12.5. Manuscripts will not be simply dismissed because of a conflict of interest. A statement that there is or not a conflict of interest must be made.

12.6. The ad hoc reviewers must also reveal to editors any conflicts of interest that could influence their opinions about the manuscript and must declare themselves unqualified to review specific documents if they believe that this procedure is appropriate. In the

case of the authors, if there is silence from the peer reviewers about potential conflicts, it will mean that conflicts do not exist.

12.7. If a conflict of interest on the part of the peer reviewers is identified, the Editorial Board will send the manuscript to another ad hoc reviewer.

12.8. If the authors are not sure about what might constitute a potential conflict of interest, they should contact the Journal's Editor-in-Chief.

12.9. In cases in which members of the Editorial Team or some other member publish frequently in the Journal, it will not be given any special or different treatment. All submitted papers will be evaluated by double blind peer review procedure.

13. Other information

13.1. The articles will be selected by the Editor-in-Chief and the Editorial Board of the Journal, which will contact the respective authors to confirm the text reception, and then forward them to the two ad hoc reviewers' analysis.

13.2. The received and not published originals will not be given back.

13.3. Authors have the right to appeal of the editorial decisions.

13.3.1. They will be granted five (5) days from the date of the final decision of the Editorial Board to appeal.

13.3.2. The written appeal must be sent to the e-mail: <journal@nuped.com.br>.

13.3.3. The appeal will be examined by the Editorial Board within thirty (30) days

CONDITIONS FOR SUBMISSIONS

As part of the submission process, authors are required to check off their submission's compliance with all the following items, and submissions may be returned to authors that do not adhere to these guidelines.

1. The contribution is original and unpublished (except in the case of articles in a foreign language published abroad) and it is not being evaluated for publication by another Journal; otherwise, it must be justified in "Comments to the Editor."
2. The submission file is in Microsoft Word, OpenOffice or RTF.
3. URLs for the references have been informed when possible.
4. The text has between 15 and 30 pages (A4 size – 21 cm by 29.7 cm), including the introduction, development, conclusion (not necessarily with these titles) and a list of references; margins used are: left and top of 3 cm and right and bottom of 2 cm; the text is written in Times New Roman format, size 12, line spacing 1.5, and spacing 0 pt. before and after paragraphs; in the footnotes it was used Times New Roman, size 10, 1 pt. spacing; in the text development, paragraphs have an indent of 1.5 cm from the left margin; headings and subheadings are aligned on the left margin; figures and tables are inserted in the text, not in the end of the document as attachments.
5. The text respects the stylistic and bibliographic requirements outlined in the Author Guidelines, on the page About.
6. In case of submission to a section with peer review (e.g.: articles), the instructions available in Ensuring blind evaluation by peer reviewers have been followed.
7. The author states that, except for the direct and indirect quotations clearly indicated and referenced, the article is of his/her authorship and therefore does not contain plagiarism. And states that he/she is aware of the legal implications of the use of other authors material.

8. The author states that participated in the work enough to make public their responsibility for the content and that all statements contained in the manuscript are true or based on research with reasonable accuracy.
9. The author agrees with the liability policy defined in item 10. Authors responsibilities of the Author Guidelines.

PRIVACY STATEMENT

This journal is committed to ethics and quality in publication, following international patterns of scientific publication. We support standards of expected ethical behavior for all parties involved in publishing in our journal: the author, the journal editor, the peer reviewer and the publisher. We do not accept plagiarism or other unethical behavior. Thus, it follows the guidelines of the 2nd World Conference on Research Integrity, Singapore, July 22-24, 2010.

Duties of Editors

- **Publication decision:** The journal's editor is responsible for deciding which of the articles submitted to the journal should be published. The editor is guided by the policies of the journal's editorial board and constrained by such legal requirements as shall then be in force regarding libel, copyright infringement and plagiarism. The editor may consult with editorial board or reviewers in decision making.
- **Fair play:** The editor should evaluate manuscripts for their intellectual content without regard to race, gender, sexual orientation, religious belief, ethnic origin, citizenship, or political philosophy of the authors.
- **Confidentiality:** The editor and any editorial staff must not disclose any information about a submitted manuscript to anyone other than the corresponding author, reviewers, potential reviewers, other editorial advisers, and the publisher, as appropriate.
- **Disclosure and Conflicts of interest:** The editor must not use unpublished information in his/her own research without the express written consent of the author. The editor should recuse him/herself from considering manuscripts in which he/she has conflicts of interest resulting from competitive, collaborative, or other relationships or connections with any of the authors, companies, or (possibly) institutions connected to the papers.
- **Involvement and cooperation in investigations:** The editor should take reasonable responsive measures when ethical complaints have been presented concerning a submitted manuscript or published paper.

Duties of Reviewers

- **Contribution to Editorial Decision:** Peer review assists the editor in making editorial decisions and through the editorial communications with the author may also assist the author in improving the paper.
- **Promptness:** Any selected referee who feels unqualified to review the research reported in a manuscript or knows that its prompt review will be impossible should notify the editor and excuse himself from the review process.
- **Confidentiality:** Any manuscripts received for review must be treated as confidential documents. They must not be shown to or discussed with others.

- **Standards of Objectivity:** Reviews should be conducted objectively and referees should express their views clearly with supporting arguments.
- **Acknowledgement of Source:** Peer reviewers should identify relevant published work that has not been cited by the authors. The peer reviewer should also call to the editor's attention any substantial similarity or overlap between the manuscript under consideration and any other published paper of which they have personal knowledge.
- **Disclosure and Conflicts of Interest:** Privileged information or ideas obtained through peer review must be kept confidential and not used for personal advantage. Reviewers should not consider manuscripts in which they have conflicts of interest resulting from competitive, collaborative, or other relationships or connections with any of the authors, companies, or institutions connected to the papers.

Duties of Authors

- **Reporting standards:** Authors of reports of original research should present an accurate account of the work performed as well as an objective discussion of its significance. Underlying data should be represented accurately in the paper. A paper should contain sufficient detail and references to permit others to replicate the work. Fraudulent or knowingly inaccurate statements constitute unethical behavior and are unacceptable.
- **Originality and Plagiarism:** The authors should ensure that they have written entirely original works, and if the authors have used the work and/or words of others that this has been appropriately cited or quoted. Plagiarism in all its forms constitutes unethical publishing behavior and is unacceptable.
- **Multiple or Redundant Publication:** An author should not in general publish manuscripts describing essentially the same research in more than one journal or primary publication. To publish the same article in different journals without informing the editors and having their agreement constitute unethical publishing behavior and is unacceptable.
- **Acknowledgement of Sources:** Proper acknowledgment of the work of others must always be given. Authors should cite publications that have been influential in determining the nature of the reported work. Information obtained privately, as in conversation, correspondence, or discussion with third parties, must not be used or reported without explicit, written permission from the source. Information obtained in the course of confidential services, such as refereeing manuscripts or grant applications, must not be used without the explicit written permission of the author of the work involved in these services.
- **Authorship of the Paper:** Authorship should be limited to those who have made a significant contribution to the conception, design, execution, or interpretation of the reported study. All those who have made significant contributions should be listed as co-authors. Where there are others who have participated in certain substantive aspects of the research project, they should be acknowledged or listed as contributors. The corresponding author should ensure that all appropriate co-authors and no inappropriate co-authors are included on the paper, and that all co-authors have seen and approved the final version of the paper and have agreed to its submission for publication.

- **Disclosure and Conflicts of Interest:** All authors should disclose in their manuscript any financial or other substantive conflict of interest that might be construed to influence the results or interpretation of their manuscript. All sources of financial support for the project should be disclosed.
- **Fundamental errors in published works:** When an author discovers a significant error or inaccuracy in his/her own published work, it is the author's obligation to promptly notify the journal editor or publisher and cooperate with the editor to retract or correct the paper.

Duties of the Publisher

We are committed to ensuring that advertising, reprint or other commercial revenue has no impact or influence on editorial decisions.

Our articles are peer reviewed to ensure the quality of scientific publishing and we are also users of CrossCheck (CrossRef's plagiarism software).

* This statement is based on Elsevier recommendations and COPE's Best Practice Guidelines for Journal Editors.