DATA SHARING REPORTS

Javier Barreriro

Data sharing en Uruguay

Caso de estudio

IL-DA

IDRC · CRDI
International Development Research Centre
Centre de recherches pour le développement international

Canada

Expresamos nuestro especial agradecimiento a **Javier Barreiro**, quien llevó a cabo la investigación que sustenta este informe.

Con más de 15 años de experiencia en el sector de la tecnología, la trayectoria profesional de Javier le ha permitido participar en proyectos de alto impacto tanto como parte del sector público así como desde diversas organizaciones. Por más de 10 años fue parte de la Agesic, Agencia de Gobierno Digital de Uruguay, donde como Director de Tecnología de Agesic, fue responsable, por ejemplo, del diseño e implementación de primera Estrategia de Inteligencia Artificial para Gobierno Digital y la Política de Datos Públicos para la Transformación Digital, así como de diversos proyectos de arquitectura empresarial e interoperabilidad. Es docente universitario en Ingeniería de Software, miembro del Comité de Evaluación de Proyectos del Programa de Innovación en Servicios Públicos de ANII, así como fue parte del Grupo Asesor Científico Honorario (GACH) durante la pandemia. Es fundador y miembro de la Comisión Directiva de DaMa Uruguay, asociación sin fines de lucro, de profesionales dedicados a promover prácticas de gestión y gobernanza de datos. Se desempeña también como Consultor BID y RedGealc (Red de Gobierno Electrónico de LATAM y Caribe) en temáticas de datos, arquitectura empresarial y tecnologías emergentes. Actualmente, es parte de Domus Global, una organización aceleradora de la transformación digital, con visión 360 y de alta especialización. En Domus dirige IUGO, unidad de negocio especializada GovTech.

Este informe se elaboró en el marco del *Programa Interamericano de Datos y Algoritmos*, financiado por el *International Development Research Centre* (IDRC).

Autor:
Javier Barreiro

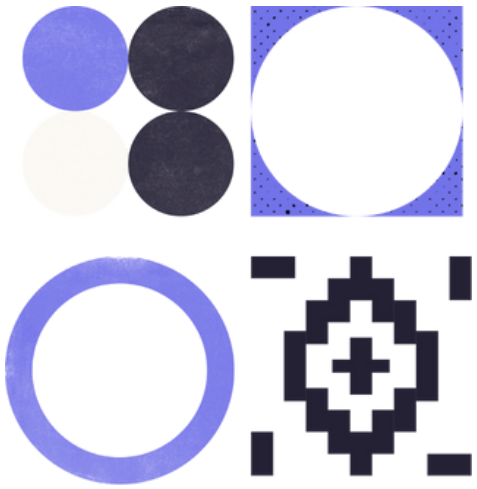
Panorama legal:
Cecilia Amieva, Socia Directora; Diego Fernando Saralegui y Carolina Vega de Equipo TMT de ECIJA Uruguay, conexión facilitada por TrustLaw, la red global legal de la Thomson Reuters Foundation, mediante una alianza con The Patrick J. McGovern Foundation.

Coordinación:
Gloria Guerrero

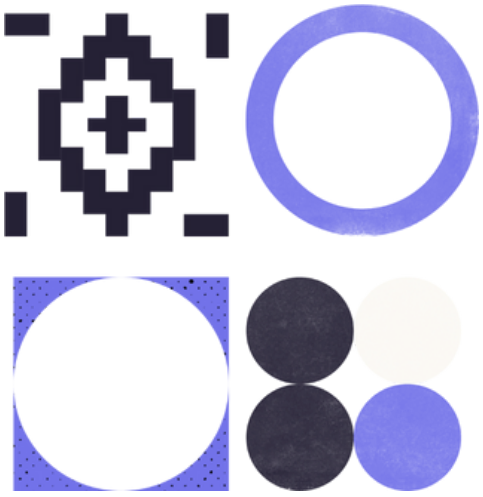
Diseño:
Violeta Belver

Estilo:
Aremí González

Agradecimientos:
International Development Research Center (IDRC)



Índice



Prólogo

Por: Gloria Guerrero,
Directora Ejecutiva de ILDA

En un mundo profundamente interconectado y cada vez más digital, el intercambio y la gobernanza de datos son fundamentales para enfrentar los desafíos del siglo XXI. En América Latina, estas dinámicas se ven influenciadas por contextos únicos que combinan avances prometedores y desafíos persistentes.

De acuerdo con la primera edición del *Barómetro Global de Datos,* América Latina enfrenta una fragmentación en sus políticas de datos: mientras algunos países han logrado avances significativos en apertura y protección de datos, el intercambio de datos o *Data Sharing* sigue siendo un terreno en construcción.

Para este proyecto, el intercambio de datos *(Data Sharing)* es entendido en un sentido amplio, que abarca los marcos normativos que establecen los lineamientos técnicos y organizativos para compartir datos, las capacidades institucionales y la voluntad política para destinar recursos y procesos que permitan el éxito de estas políticas. De esta forma, los procesos de intercambio de datos y de interoperabilidad tienen un componente técnico vinculado a la creación de habilidades internas y a su implementación, pero también político relacionado a la decisión de aplicar la política y al cambio cultural al interno de las organizaciones necesario para hacerlo. Por esto, se consideran los procesos, las personas y los sistemas que logran la permanencia de estas políticas en el tiempo.

Es en este contexto, la Iniciativa Latinoamericana por los Datos Abiertos realizó la investigación titulada, Estrategias de Intercambio de Datos en América Latina que consta de 3 estudios de casos nacionales. Este proyecto se enmarca en el *Programa Interamericano de Datos y Algoritmos* apoyado por el International Development Research Center (IDRC), buscando profundizar en el tema. El objetivo de este proyecto de investigación es analizar y comprender cómo funcionan los sistemas de intercambio de datos a nivel nacional en Brasil, Colombia, y Uruguay. Estos 3 estudios de caso nos permitieron identificar un conjunto de buenas prácticas que pueden ser inspiración para otros países de la región e identificar los retos y áreas de oportunidad para este campo de estudios.

Cada caso de estudio buscó conocer los marcos normativos, la infraestructura de datos y sus características, los procesos y la implementación, y la participación de actores diversos (públicos, privados y de la sociedad civil) en esos procesos de intercambio de datos a nivel nacional/federal. Estas investigaciones son la continuación de un conjunto de Informes de Gobernanza de Datos realizados en Colombia, México y Uruguay en 2022, y fueron complementados con una serie de estudios jurídicos sobre el intercambio de datos realizados por bufetes jurídicos especializados en cada país, que contribuyeron de manera pro bono a través de la conexión facilitada por TrustLaw, la red pro bono legal de la Thomson Reuters Foundation.

El proyecto busca aportar un diagnóstico y posibles pasos a seguir en materia de gobernanza de datos, lo cual también podrá ser un insumo de utilidad para la futura gobernanza de la IA en la región. Este esfuerzo no solo persigue entender las estructuras normativas y técnicas existentes, sino también sentar las bases de un ecosistema sostenible, inclusivo y democrático que promueva la interoperabilidad y el uso ético de las tecnologías basadas en datos.

A continuación se presenta el caso de Uruguay, liderado por el Dr. Javier Barreiro y el despacho jurídico Ecija Uruguay. Uruguay ha logrado posicionarse como un referente regional en materia de gobernanza de datos e interoperabilidad, destacándose por una estrategia digital coordinada y consistente que ha sido respaldada por un marco regulatorio robusto y una infraestructura tecnológica avanzada. Este éxito se debe, en gran parte, a la continuidad institucional de la agenda de gobernanza e intercambio de datos, un aspecto que distingue a Uruguay en la región, donde otros países enfrentan desafíos en cuanto a la permanencia de políticas a largo plazo. La evolución constante del marco legal, especialmente en áreas clave como la protección de datos personales, la seguridad de la información y la interoperabilidad, ha permitido una mejora progresiva en la gestión y el intercambio de datos a nivel gubernamental.

El caso de Uruguay destaca la importancia de contar con una arquitectura digital integrada, como lo demuestra la Plataforma de Interoperabilidad (PDI), que ha facilitado el intercambio eficiente y seguro de datos entre múltiples organismos públicos. Esta plataforma ha sido clave para mejorar la calidad y agilidad de los servicios públicos, promoviendo una colaboración interinstitucional fluida y un acceso más equitativo a los servicios para los ciudadanos. A nivel normativo, Uruguay se ha alineado con estándares internacionales, creando un entorno propicio para la protección de los derechos de los ciudadanos y fomentando la confianza en la gestión de datos personales. Sin embargo, el país aún enfrenta desafíos relacionados con la protección de la privacidad, especialmente en el uso de tecnologías disruptivas como la inteligencia artificial y el reconocimiento facial. Estos avances deben ir acompañados de un marco regulatorio claro y transparente para evitar riesgos como la vigilancia masiva y el abuso de tecnologías, lo cual podría erosionar la confianza pública.

Con este trabajo de investigación desde la Iniciativa Latinoamericana por los Datos Abiertos (ILDA), reafirmamos nuestro compromiso de contribuir al desarrollo del ecosistema de datos regional y a la generación de evidencia que permita robustecer las capacidades y modelos de gobernanza de datos existentes.

1. Introducción

El intercambio de datos (*data sharing*) se refiere al proceso de hacer que los datos sean accesibles para múltiples usuarios, aplicaciones u organizaciones. Esto puede realizarse dentro de una misma organización o entre diferentes entidades y tiene como objetivo mejorar la colaboración, la toma de decisiones y la eficiencia operativa. En este proceso es fundamental garantizar que los datos se compartan de manera segura, respetando la privacidad y las normativas legales vigentes.

De igual modo, el intercambio de datos implica el uso de plataformas tecnológicas que faciliten el acceso controlado y seguro a los datos, así como la implementación de políticas y procedimientos que aseguren que la información compartida sea de alta calidad y relevante para los usuarios.

En los últimos veinte años, Uruguay ha sido testigo de una profunda transformación en el intercambio de datos e interoperabilidad en el sector público, consolidándose como un referente regional en la temática. Este proceso ha sido el resultado de una estrategia digital coordinada y liderada principalmente por la Agencia de Gobierno Electrónico y Sociedad de la Información (AGESIC) creada en 2007.

La misión de AGESIC tal como distintos proyectos de gran impacto que involucraron a diversos actores públicos y privados han sido fundamentales para fomentar la modernización del Estado, la digitalización de los servicios públicos y la creación de un ecosistema de intercambio de datos entre diferentes entidades del sector público y privado.

La Organización para la Cooperación y el Desarrollo Económicos (OCDE) define el **intercambio de datos** como “el acto de facilitar el acceso a los datos para su uso por terceros, con sujeción a los requisitos de uso técnicos, financieros, jurídicos u organizativos aplicables.” (OECD, 2021).

La Unión Europea (UE), por medio del reglamento 2022 / 868 del Parlamento Europeo, lo define como “la facilitación de datos por un interesado o titular de datos a un usuario de datos, directamente o a través de un intermediario y en virtud de un acuerdo voluntario o del Derecho de la Unión o nacional, con el fin de hacer un uso en común o individual de tales datos, por ejemplo, mediante licencias abiertas o mediante licencias comerciales de pago o gratuitas.” (2022, p. 19) [1].

En el marco anterior y con el objetivo de establecer un vocabulario común para este

[1] (2022, 03 de junio). Reglamento (UE) 2022 / 868 del Parlamento Europeo y del Consejo del 30 de mayo del 2022 relativo a la gobernanza europea de los datos y por el que se modifica el reglamento (UE) 2018 / 1724 (Reglamento de gobernanza de datos). Disponible en https://www.colegionotarial.org/es/legislaci%C3%B3n/reglamento-ue-2022868-del-parlamento-europeo-del-consejo-30-mayo-2022-relativo

documento, ha sido necesario sentar algunas definiciones base de **interoperabilidad**:

- La norma ISO / IEC 2382:2015 establece que es la "capacidad de comunicar, ejecutar programas o transferir datos entre varias unidades funcionales de forma que el usuario tenga poco o ningún conocimiento de las características exclusivas de dichas unidades" [2].
- El Institute of Electrical and Electronics Engineers (IEEE), desde el punto de vista técnico, puntualiza que es "la habilidad de dos o más sistemas o componentes para intercambiar información y utilizar la información intercambiada." [3].
- La Comisión Europea, desde una perspectiva de estrategia de gobernanza de datos, determina que es "la capacidad de que las organizaciones interactúen con vistas a alcanzar objetivos comunes que sean mutuamente beneficiosos y que hayan sido acordados previa y conjuntamente, recurriendo a la puesta en común de información y conocimientos entre las organizaciones, a través de los procesos empresariales a los que apoyan, mediante el intercambio de datos entre sus sistemas de TIC respectivos." (Naser, 2011, p. 25) [4].

Estas definiciones pueden complementarse con una visión de cuatro niveles de interoperabilidad: legal o jurídica, técnica, semántica y organizacional.

De acuerdo con el *Libro blanco de interoperabilidad de gobierno electrónico para América Latina y el Caribe* (CEPAL) y la Comisión Europea [5] existen diversos tipos de interoperabilidad como se muestra a continuación:

- **Interoperabilidad técnica:** "cubre las cuestiones técnicas (*hardware*, *software*, telecomunicaciones) necesarias para interconectar sistemas computacionales y servicios, incluyendo aspectos clave como interfaces abiertas, servicios de interconexión, integración de datos y *middleware*, presentación e intercambio de datos, accesibilidad y servicios de seguridad." (UN. CEPAL y Comisión Europea, 2007, p. 13).
- **Interoperabilidad semántica:** "se ocupa de asegurar que el significado preciso de la información intercambiada sea entendible sin ambigüedad por todas las aplicaciones que intervengan en una determinada transacción y habilita a los sistemas para combinar información recibida con otros recursos de información y así procesarlos de forma adecuada." (UN. CEPAL y Comisión Europea, 2007, p. 13).
- **Interoperabilidad organizacional:** "se ocupa de definir los objetivos de negocios, modelar los procesos y facilitar la colaboración de administraciones que desean intercambiar información y pueden tener diferentes estructuras organizacionales y

[2] International Standard. (2015, mayo). *Information technology – Vocabulary*. ISO / IEC 2382:2015. Disponible en https://www.iso.org/standard/63598.html

[3] (1991, 18 de enero). *610 – 1990 – IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries*. IEEE. DOI: 10.1109/IEEESTD.1991.106963

[4] Naser, Alejandra. (Coord.). (2011). "Gobernanza digital e interoperabilidad gubernamental. Una guía para su implementación". *Documentos de proyectos*. (LC / TS. 2021 / 8°), Santiago. Comisión Económica para América Latina y el Caribe (CEPAL). Disponible en https://repositorio.cepal.org/server/api/core/bitstreams/6a12e389-3dcb-4cba-830a-99f038835423/content

[5] UN. CEPAL y Comisión Europea. (2007). *Libro blanco de interoperabilidad de gobierno electrónico para América Latina y el Caribe*. Disponible en Libro blanco de interoperabilidad de gobierno electrónico para América Latina y el Caribe: versión 3.0 (cepal.org)

procesos internos. Además de eso, busca orientar, con base en los requerimientos de la comunidad usuaria, los servicios que deben estar disponibles, fácilmente identificables, accesibles y orientados al usuario." (UN. CEPAL y Comisión Europea, 2007, p. 13).

En la estrategia de aplicación del Marco Europeo de Interoperabilidad [6], en el *Anexo de la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones* se establece:

- **Interoperabilidad jurídica:** "consiste en garantizar que las organizaciones que operan con arreglo a diferentes marcos jurídicos, políticas y estrategias pueden trabajar juntas. Ello podría exigir que la legislación no bloquee el establecimiento de servicios públicos europeos dentro de los Estados miembros y entre estos y que existan acuerdos claros sobre cómo abordar las diferencias en la legislación a través de fronteras, incluida la opción de adoptar nueva legislación." (Comisión Europea, 2007, p. 26 – 27).
- **Interoperabilidad técnica:** "abarca las aplicaciones e infraestructuras que conectan sistemas y servicios. Incluye elementos tales como especificaciones de interfaz, servicios de interconexión, servicios de integración de datos, presentación e intercambio de datos y protocolos de comunicación seguros. […]. La interoperabilidad técnica debe garantizarse, siempre que sea posible, mediante el uso de especificaciones técnicas formales." (Comisión Europea, 2007, p. 30 – 31).
- **Interoperabilidad semántica:** "garantiza que el formato y el significado exacto de la información intercambiada se comprenda y conserven en todos los intercambios entre las partes, es decir, 'que lo que se transmite sea lo que se entiende'. […]. El aspecto semántico se refiere al significado de los elementos de datos y la relación entre ellos, incluye la creación de vocabularios y esquemas para describir los intercambios de datos y garantiza que todas las partes que se comunican entienden de la misma manera los elementos de datos; el aspecto sintáctico se refiere a la descripción del formato exacto de la información que se va a intercambiar en términos de gramática y formato." (Comisión Europea, 2007, p. 29).
- **Interoperabilidad organizacional:** refiere a "la manera en que las administraciones públicas adaptan sus procesos empresariales, responsabilidades y expectativas para alcanzar las metas adoptadas de común acuerdo y mutuamente beneficiosas. En la práctica, la interoperabilidad organizativa implica la documentación y la integración o adaptación de los procesos empresariales y la información pertinente intercambiada. La interoperabilidad organizativa se propone igualmente satisfacer los requisitos de la comunidad de usuarios consiguiendo que los servicios estén disponibles, sean fácilmente identificables, sean accesibles y estén centrados en el usuario." (Comisión Europea, 2007, p. 28).

Una vez complementadas estas definiciones y después de haber atendido cómo se desarrollará este informe, ahora es oportuno presentar de qué manera puede definirse la

[6] Comisión Europea. (2007). *Anexo de la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Marco Europeo de Interoperabilidad – Estrategia de aplicación.* Disponible en https://eur-lex.europa.eu/resource.html?uri=cellar:2c2f2554-0faf-11e7-8a35-01aa75ed71a1.0010.02/DOC_3&format=PDF

gobernanza de datos. En este sentido, según el *Dama – Dmbok: Data Management Body of Knowledge*, la gobernanza de datos se refiere al "control ejercido sobre los datos a lo largo de su ciclo de vida", siendo esta la función que "rige todas las demás actividades de gestión de datos y garantiza su adecuado manejo conforme a políticas y buenas prácticas". Además, define la **gestión de datos** como "el proceso de desarrollar, ejecutar y supervisar planes, políticas, programas y prácticas que aseguren, protejan y aumenten el valor de los activos de datos e información a lo largo de su ciclo de vida".

El presente documento se estructura atendiendo y abordando las definiciones presentadas. En el capítulo 2 se expone el marco regulatorio principal en materia de intercambio de datos en relación directa con la interoperabilidad jurídica que el país considera la base para generar la seguridad normativa y los cimientos para el desarrollo seguro del intercambio de datos. Asimismo, se sintetizan las diferentes leyes, normas y decretos vinculados al intercambio de datos que se han desarrollado.

En el capítulo 3 se aborda la estrategia de gobernanza de datos a nivel nacional y la participación de diferentes actores —sector público, sector privado, academia, sociedad civil— en su construcción. Además, se reúnen aspectos de la implementación concreta de la normativa y de la estrategia de datos, la existencia de los recursos necesarios, así como la infraestructura de datos existentes en Uruguay en tanto herramienta habilitadora para la gobernanza. Adicionalmente, se analiza la existencia de consultas públicas, capacitaciones y procesos de sensibilización e inducción dentro del sector público, coordinaciones entre los niveles nacionales y locales, al igual que eventuales colaboraciones con actores de la sociedad civil y actores internacionales. Finalmente, aquí podrán verse aspectos relacionados con la interoperabilidad organizacional y técnica.

En el capítulo 4 se analizan algunos casos que, por sus características, aportan una visión global de lo expuesto en los capítulos anteriores, identificando algunas oportunidades particulares de mejora.

Por último, en el capítulo 5 se agrupan las principales conclusiones y algunos retos y oportunidades para tomarse en cuenta.

2. Marco regulatorio

Puede afirmarse que Uruguay tiene un sólido marco legal en materia de intercambio, protección de datos personales y seguridad de la información, el cual, a lo largo del tiempo y de los sucesivos gobiernos y las subsecuentes administraciones, se ha continuado, actualizado y potenciado, factor fuertemente destacado en la región. Este proceso positivo de acumulación ha sido progresivo y ha sido orientado a fortalecer la protección de la privacidad, a garantizar la transparencia y a promover la interoperabilidad en los ámbitos público y privado.

A modo de ilustrar esta evolución, en 2008 se promulgó la Ley No. 18.331 [7] que establece el derecho a la privacidad de los datos personales y regula su tratamiento en los sectores público y privado. Esta ley creó la Unidad Reguladora y de Control de Datos Personales (URCDP), responsable de supervisar el cumplimiento de la normativa, de realizar censos de bases de datos y de emitir opiniones sobre sanciones administrativas.

En el mismo año, se promulgó el Decreto No. 664 / 008 [8] que reglamenta la ley y estableció el Registro de Bases de Datos Personales a cargo de la URCDP. Un año después, en 2009, el Decreto No. 414 / 009 [9] definió disposiciones generales sobre los derechos de los titulares de los datos, el régimen registral y las obligaciones de quienes gestionan estas bases.

En 2010, la Ley No. 18.719 [10] otorgó a AGESIC la responsabilidad de dirigir políticas y prácticas de seguridad de la información y la ciberseguridad tanto en el ámbito público como en el ámbito privado vinculados a sectores críticos. También los artículos 157 a 160 de la misma ley establecieron condiciones para la interoperabilidad y el intercambio de información. De igual modo, ese año se publicó el Decreto No. 232 / 010 [11] que promovió la transparencia y el acceso ciudadano mediante la publicación de datos abiertos por parte de entidades públicas.

---

[7] (2008, 18 de agosto). Ley No. 18.331. Ley de protección de datos personales. *Centro de Información Oficial. Normativa y avisos legales del Uruguay*. Disponible en https://www.impo.com.uy/bases/leyes/18331-2008/34

[8] (2009, 05 de enero). Decreto No. 664 / 008. Creación del registro de bases de datos personales. *Centro de Información Oficial. Normativa y avisos legales del Uruguay*. Disponible en https://www.impo.com.uy/bases/decretos/664-2008

[9] (2009, 15 de septiembre). Decreto No. 414 / 009. Reglamentación de la Ley 18.331, relativo a la protección de datos personales. *Centro de Información Oficial. Normativa y avisos legales del Uruguay*. Disponible en https://www.impo.com.uy/bases/decretos/414-2009

[10] (2011, 05 de enero). Ley No. 18.719. Presupuesto nacional de sueldos, gastos e inversiones. Ejercicio 2010 – 2014. *Centro de Información Oficial. Normativa y avisos legales del Uruguay*. Disponible en https://www.impo.com.uy/bases/leyes/18719-2010/149

[11] (2010, 10 de agosto). Decreto No. 232 / 010. Reglamentación de la ley sobre el derecho de acceso a la información pública. *Centro de Información Oficial. Normativa y avisos legales del Uruguay*. Disponible en https://www.impo.com.uy/bases/decretos/232-2010/

En 2012 se aprobó la Ley No. 19.030 [12] que ratificó el Convenio 108 del Consejo de Europa, promoviendo la protección de los datos personales en el contexto del tratamiento automatizado y la trazabilidad de datos. Posteriormente, el Decreto No. 178 / 013 [13] de 2013 reglamentó los artículos 157 a 160 de la Ley No. 18.719 [14].

En 2015, la Ley No. 19.355 [15], en su artículo 76 estableció la obligación para los organismos públicos de no solicitar documentación ya emitida por otras entidades del Estado cuando pudiera accederse a esta información a través de sistemas informáticos. Asimismo, el artículo 82 [16] determinó que AGESIC sería responsable de las normas técnicas sobre datos y sus metadatos.

En 2018, la Ley 19.670 [17] modificó varios artículos de la Ley No. 18.331, ampliando las competencias de la URCDP y ajustando aspectos relacionados con la fiscalización y las sanciones. En 2020, el Decreto No. 64 / 020 [18] proporcionó recomendaciones de seguridad y adoptó el Marco de Ciberseguridad de AGESIC. Ese mismo año, la Ley No. 19.889 alineó la normativa nacional con el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, fortaleciendo los derechos de los titulares de los datos personales y estableciendo mayores obligaciones para quienes gestionan estas bases.

En 2021, se aprobó la Ley No. 19.948 [19] que ratificó el Protocolo de Enmienda del Convenio 108 (Convenio 108+), reafirmando el compromiso del país con la protección de los datos personales. La Ley No. 20.075 [20] de 2022 ajustó varios artículos de la Ley No. 18.331, mejorando la regulación del tratamiento de los datos personales.

---

[12] (2013, 07 de enero). Ley No. 19.030. Aprobación del convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. *Centro de Información Oficial. Normativa y avisos legales del Uruguay*. Disponible en https://www.impo.com.uy/bases/leyes/19030-2012

[13] (2013, 25 de julio). Decreto No. 178 / 013. Reglamentación de los artículos 157 a 160 de la Ley No. 18.719, relativos a la regulación en el intercambio de información entre entidades públicas, estatales o no estatales. *Centro de Información Oficial. Normativa y avisos legales del Uruguay*. Disponible en https://www.impo.com.uy/bases/decretos/178-2013

[14] (2011, 05 de enero). Ley No. 18.719. Presupuesto nacional de sueldos, gastos e inversiones. Ejercicio 2010 – 2014. *Centro de Información Oficial. Normativa y avisos legales del Uruguay*. Disponible en https://www.impo.com.uy/bases/leyes/18719-2010/

[15] (2015, 30 de diciembre). Ley No. 19.355. Presupuesto nacional de sueldos, gastos e inversiones. Ejercicio 2015 – 2019. *Centro de Información Oficial. Normativa y avisos legales del Uruguay*. Disponible en https://www.impo.com.uy/bases/leyes/19355-2015/76

[16] (2015, 30 de diciembre). Ley No. 19.355. Presupuesto nacional de sueldos, gastos e inversiones. Ejercicio 2015 – 2019. *Centro de Información Oficial. Normativa y avisos legales del Uruguay*. Disponible en https://www.impo.com.uy/bases/leyes/19355-2015/82

[17] (2018, 25 de octubre). Ley No. 19.670. Aprobación de rendición de cuentas y balance de ejecución presupuestal. Ejercicio 2017. *Centro de Información Oficial. Normativa y avisos legales del Uruguay*. Disponible en https://www.impo.com.uy/bases/leyes/19670-2018

[18] (2020, 21 de febrero). Decreto No. 64 / 020. Reglamentación de los arts. 37 a 40 de la Ley 19.670 y art. 12 de la Ley 18.331, referente a protección de datos personales. *Centro de Información Oficial. Normativa y avisos legales del Uruguay*. Disponible en https://www.impo.com.uy/bases/decretos/64-2020

[19] (2021, 27 de abril). Ley No. 19.948. Aprobación del protocolo de enmienda del convenio para la protección de las personas con respecto al tratamiento de datos personales, suscrito en Estrasburgo. *Centro de Información Oficial. Normativa y avisos legales del Uruguay*. Disponible en https://www.impo.com.uy/bases/leyes/19948-2021

[20] (2022, 03 de noviembre). Ley No. 20.075. Aprobación de rendición de cuentas y balance de ejecución presupuestal. Ejercicio 2021. *Centro de Información Oficial. Normativa y avisos legales del Uruguay*. Disponible en https://www.impo.com.uy/bases/leyes/20075-2022

En 2023, se emitió el Decreto No. 252/023 [21] que reglamentó el artículo 76 de la Ley No. 19.355 y se promulgó la Ley No. 20.212 [22] que otorgó a la AGESIC la responsabilidad de diseñar una Estrategia Nacional de Datos e Inteligencia Artificial. Esta ley impone obligaciones para las entidades públicas y privadas vinculadas a servicios críticos del país y establece la base tanto para la creación de una estrategia nacional, destacando la importancia del contralor, como para la fiscalización del cumplimiento de estas obligaciones por parte de la AGESIC.

Este resumen muestra claramente que la normativa uruguaya en torno a los datos ha evolucionado significativamente, alineándose con estándares internacionales y enfocándose en la protección de la privacidad, la transparencia y la promoción de un entorno seguro y colaborativo para el intercambio de datos. Esta evolución ha permitido establecer un marco robusto para garantizar la adecuada gestión de los datos en un contexto de creciente digitalización.

Uruguay ha desarrollado un abordaje coordinado y reflejado de primera instancia en la iniciativa Datos 360º [23] impulsada por la AGESIC en 2016. Esta iniciativa "se refiere al enfoque holístico de la gestión de datos desde la administración pública" (AGESIC, s.f.), la cual "busca dar soporte al gobierno digital, mediante el abordaje de los diferentes componentes de una gestión de datos eficiente" (AGESIC, s.f.).

Recientemente con la ya mencionada promulgación de la Ley No. 20.212 que establece la obligación de la AGESIC de desarrollar una Estrategia Nacional de Datos e Inteligencia Artificial, se ha vuelto a fortalecer un enfoque articulado que abarca la regulación de la interoperabilidad y la protección de los datos.

Cabe destacar que esta ley también enfatiza la necesidad de realizar recomendaciones específicas para que las entidades públicas y privadas puedan cumplir con los estándares necesarios para el manejo de datos, factor que de igual modo contribuye a una gobernanza coordinada.

---

[21] (2023, 16 de noviembre). Decreto No. 353 / 023. Reglamentación del art. 76 de la Ley No. 19.355, relativo al procedimiento aplicable por las entidades públicas, a los efectos de simplificar sus trámites, siguiendo los lineamientos de la agesic. Modificación del art. 15 y derogación del art. 13 del decreto No. 178 / 013. *Centro de Información Oficial. Normativa y avisos legales del Uruguay*. Disponible en https://www.impo.com.uy/bases/decretos/353-2023

[22] (2023, 17 de noviembre). Ley No. 20212. Aprobación de rendición de cuentas y balance de ejecución presupuestal. Ejercicio 2022. *Centro de Información Oficial. Normativa y avisos legales del Uruguay*. Disponible en https://www.impo.com.uy/bases/leyes/20212-2023/74

[23] (s. f.). "Iniciativa 'Datos 360°'". "Datos 360°". *Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento.* Disponible en https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/node/3557

3. Gobernanza de datos en Uruguay: antecedentes y actualidad

El Decreto No. 134 / 021 [24], promulgado el 04 de mayo de 2021, aprobó la Agenda Uruguay Digital (AUD) 2025 y encomendó a la AGESIC el monitoreo, la evaluación de avances y resultados, así como la revisión de medio término de la referida agenda.

En el objetivo VI "Datos como activos" de la AUD 2025 [25] se propone optimizar el uso intensivo de datos e información como factor clave para una toma de decisiones eficaz y una gestión pública eficiente, contemplando aspectos de ética, privacidad, responsabilidad, transparencia y no discriminación. A su vez, en la meta 27, para el 2025 se establece el objetivo de fortalecer los procesos de monitoreo y evaluación de políticas públicas, así como la integración, la apertura y la visualización de los datos públicos, impulsando la ciencia de datos.

Por su parte, en el marco de la AUD 2025, la AGESIC definió el 5° Plan de Acción Nacional de Gobierno Abierto 2021 – 2024 [26] donde se aprobó en el punto 1.9 la Estrategia Nacional de Datos Abiertos 2021 – 2024. En el plan de acción se menciona que "por primera vez, convergen en un plan los tres poderes del Estado, integrando simultáneamente iniciativas de Parlamento Abierto, Justicia Abierta, organismos de Administración Central y de Gobiernos Departamentales" (AGESIC, s.f., p. 03). Asimismo, se menciona que "reafirma la estrategia del país de concebir los planes de acción y los procesos de cocreación en Uruguay, como instrumento para generar nuevos espacios de colaboración y construcción colectiva entre las instituciones públicas, las organizaciones de sociedad civil, el sector privado y la academia, impulsando así una agenda transversal a todas las políticas públicas.".

También en el marco de la AUD 2025, en el 2021, la AGESIC definió el Plan de Gobierno Digital 2025 [27] en el cual se incluye el objetivo "Gobierno como plataforma", cuyas finalidades

[24] (2021, 12 de mayo). Decreto No. 134/ 021. Aprobación de la "Agenda Uruguay Digital 2025". *Centro de Información Oficial. Normativa y avisos legales del Uruguay*. Disponible en https://www.impo.com.uy/bases/decretos/134-2021%EF%BB%BF

[25] (2023, 18 de diciembre). Agenda Uruguay Digital 2025 – Sociedad digital resiliente. "Uruguay digital". *AGESIC*. Descarga y disponible en: https://www.gub.uy/uruguay-digital/comunicacion/publicaciones/agenda-uruguay-digital-2025-sociedad-digital-resiliente/agenda-uruguay

[26] (s. f.). 5° Plan de Acción Nacional de Gobierno Abierto 2021 – 2024. *AGESIC y Uruguay Presidencia*. Disponible en https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/book/6187/download

[27] (s. f.). Plan de Gobierno Digital 2025. *AGESIC y Uruguay Presidencia*. Disponible en https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/sites/agencia-gobierno-electronico-sociedad-informacion-conocimiento/files/2021-07/Plan%20de%20Gobierno%20Digital%202025_0.pdf

giran en relación con "promover el desarrollo de plataformas escalables y transversales, para la generación de servicios de valor público por parte de organizaciones públicas y privadas. Universalizar la interoperabilidad e integración de datos en la Administración Pública. Diseñar la arquitectura de gobierno en torno a una red de APIs y componentes compartidos, estándares abiertos y conjuntos de datos, para que los organismos públicos y el sector privado puedan brindar servicios en forma segura, innovadora y responsable" (AGESIC, s. f., p.15). Se destaca en este plan explícitamente la gobernanza sobre el intercambio de datos de organismos públicos y el sector privado.

La Agenda Uruguay Digital 2025 refleja un posicionamiento estratégico de Uruguay acerca de la gobernanza de datos tanto en el sector público como en el sector privado, promoviendo la interoperabilidad, la transparencia y el uso seguro y responsable de la información. De esta manera, la estrategia no solo fortalece el ecosistema digital del país, sino que representa una continuidad con las Agendas previamente elaboradas por Uruguay, reafirmando el compromiso del país con la transformación digital y la gobernanza colaborativa.

A través de objetivos claros y planes de acción concretos como el 5° Plan de Acción Nacional de Gobierno Abierto y el Plan de Gobierno Digital 2025, Uruguay consolida su liderazgo regional en la implementación de estrategias de datos abiertos y la integración digital, apostando por un enfoque transversal e inclusivo que involucra a todos los sectores de la sociedad.

Esta iniciativa se complementa al momento de la confección del presente informe en un proceso de elaboración de una estrategia nacional de datos [28]. Siguiendo la misma línea esgrimida hasta ahora "este proceso contempla el desarrollo de mesas de diálogo, talleres y mecanismo de consulta pública. Asimismo, prevé a lo largo de las distintas instancias la participación de referentes del Estado, la academia, la sociedad civil y el sector privado.".

El resultado de este proceso será la versión final de los documentos de Estrategia de Inteligencia Artificial y Estrategia Nacional de Datos. Puede participarse actualmente de la consulta pública en el siguiente *link*: https://plataformaparticipacionciudadana.gub.uy/processes/estrategia-ia-datos/steps?locale=es

Esta última, de reciente publicación a consulta pública, se enfoca en desarrollar una economía basada en datos, con tres pilares clave: gobernanza de datos, infraestructura y desarrollo económico, fundamentada en un conjunto de principios como la innovación, el foco en el valor de los datos, su calidad y su disponibilidad, alineados con la normativa local e internacional en aspectos de seguridad y de privacidad.

El borrador de estrategia plantea la importancia de crear mecanismos que permitan compartir, integrar y poner a disposición los datos segura y confiablemente tanto a nivel nacional como a nivel transfronterizo. Para lograrlo, se sugiere la creación de espacios de

[28] (2024, 17 de julio). "Proceso de revisión de la Estrategia de Inteligencia Artificial y de elaboración de la Estrategia Nacional de Datos. "Políticas y Gestión". *Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento.* Disponible en https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/politicas-y-gestion/proceso-revision-estrategia-inteligencia-artificial-elaboracion-estrategia

datos con diferentes niveles de apertura, accesibles a todos los sectores de la sociedad, bajo un modelo de gobernanza claro que defina las licencias, los acuerdos y las reglas necesarias para asegurar una participación adecuada y conforme a la normativa vigente.

De manera conjunta, se destaca el apremio por crear espacios transversales que garanticen la integración y el intercambio de datos entre organismos públicos de forma segura y confiable, lo que facilitaría la cooperación entre distintas áreas y sistemas en función de los objetivos estratégicos definidos por las instituciones. Paralelamente, propone impulsar la apertura de datos de modo sostenible, con especial énfasis en sectores estratégicos, fortaleciendo las capacidades, los mecanismos y las herramientas que permitan una apertura eficaz y eficiente.

Otro aspecto clave incorporado en el texto es la creación de un plan nacional de interoperabilidad que aborde los aspectos semánticos y los aspectos organizacionales, normativos, técnicos e infraestructurales. Se indica que este plan debe fomentar un mayor intercambio e integración de datos no solo a nivel interno entre las organizaciones, sino a nivel transfronterizo, asegurando la calidad e integridad de los datos en todo momento.

Por otro lado, a nivel subnacional, Uruguay cuenta con la Estrategia de Datos de Montevideo [29], la cual se centra en mejorar el uso y la gestión de datos para maximizar el impacto en los ciudadanos de la capital del país. La estrategia se estructura en cinco ejes fundamentales:

- **Gobernanza:** establece un Comité de Datos que garantiza la gestión integral de los datos, definiendo roles y responsabilidades para asegurar seguridad, transparencia y documentación.
- **Calidad:** implementa estándares para asegurar la consistencia, precisión y seguridad de los datos mediante un Inventario Único de Datos. Cada departamento de la Intendencia es responsable de actualizar y mantener la información que gestiona.
- **Capacidad:** incluye un Plan de Formación y Capacitación para dotar de habilidades a los equipos de trabajo en la gestión y en el análisis de datos, asegurando la creación de una cultura sostenible de uso de datos en toda la Intendencia.
- **Transparencia:** se enfoca en poner a disposición los datos internos y externos, facilitando el acceso a través de la publicación sistemática de datos abiertos. Los datos se publican respetando un protocolo que asegura la confidencialidad y el cumplimiento de la normativa vigente.
- **Uso:** promueve la toma de decisiones informadas a partir del análisis de datos. Se impulsa el desarrollo de herramientas como plataformas de integración de datos y un tablero de mando para priorizar la gestión pública.

A su vez, esta estrategia subnacional se apoya en tres principios fundamentales:

1. Liderazgo para impulsar el uso de datos en la toma de decisiones diarias.
2. Equipo para promover la capacitación.
3. Trabajo colaborativo y ciudadanía para garantizar la transparencia y la participación

[29] (2023, 18 de mayo). Estrategia de datos de la Intendencia de Montevideo. *Intendencia Montevideo*. Disponible y descarga en https://montevideo.gub.uy/noticias/tecnologia/estrategia-de-datos-de-la-intendencia-de-montevideo

ciudadana en el acceso y uso de los datos.

La estrategia busca consolidar una cultura de datos que mejore la calidad de vida de los habitantes de la Ciudad de Montevideo, incremente la transparencia y permita la cocreación de soluciones a problemas públicos.

Desde la perspectiva de regulación y control, en Uruguay existe un conjunto de órganos desconcentrados en la AGESIC vinculados a la temática la Unidad Reguladora y de Control de Datos Personales (URCDP) y la Unidad de Acceso a la Información Pública (UAIP), las cuales actúan ante denuncias o solicitudes al emitir dictámenes cuando corresponde. Están dirigidos por Consejos Ejecutivos asistidos en sus tareas por Consejos Consultivos, órganos multisectoriales integrados por representantes de los tres poderes del Estado, de la academia y de la sociedad civil. En particular, según se indica en la reglamentación, los Consejos Consultivos deben ser involucrados cuando se ejercen potestades de reglamentación.

En concordancia con la normativa presentada, así como las guías y las recomendaciones técnicas elaboradas, el país ha desarrollado una infraestructura de datos robusta y moderna que sostiene su capacidad de gestionar y compartir datos de manera efectiva entre organismos públicos.

La Plataforma de Interoperabilidad (PDI) [30] es una infraestructura tecnológica que permite la conexión y el intercambio de datos entre sistemas de diferentes entidades públicas segura y eficientemente. Esta plataforma facilita la automatización de procesos, mejora la calidad de los servicios públicos y permite una gestión integrada de la información, asegurando que los datos se compartan con una metodología estandarizada y cumpliendo con normativas de seguridad y protección de datos. La AGESIC aseguró las interoperabilidades técnica y semántica con la confección de la Guía de uso para de la Plataforma de Interoperabilidad [31].

La arquitectura de la PDI está orientada a servicios (SOA), lo que permite la reutilización y la orquestación de estos a través de interfaces estandarizadas, promoviendo el desarrollo eficiente de nuevas soluciones y la evolución autónoma de los sistemas estatales. Dentro de su estructura, cada uno de sus elementos desempeña un rol específico para asegurar la provisión, búsqueda, invocación e integración segura de servicios entre los organismos a través de protocolos estandarizados. Su sistema de control de acceso permite la autenticación y la autorización para el intercambio de datos, actuando como puerta de entrada a la plataforma; esto garantiza que solo usuarios y sistemas autorizados puedan acceder a ellos, reforzando la seguridad del intercambio de información.

A partir de su diseño e implementación en 2008, la PDI ha permitido el desarrollo de diversos proyectos de alto impacto para el Estado uruguayo; por ejemplo, Nacido Vivo, Trámites en Línea, Expedientes Digitales, Notificaciones y Comunicaciones Digitales, la Historia Clínica

[30] (s. f.). Plataforma de Interoperabilidad. *AGESIC y Uruguay Presidencia*. Disponible en https://centrodeconocimiento.agesic.gub.uy/web/ccio/plataforma-de-interoperabilidad

[31] (s. f.). Condiciones de uso de la Plataforma de Interoperabilidad. Especificación técnica. Plataforma de Interoperabilidad. *AGESIC y Uruguay Presidencia*. Disponible y descarga en https://centrodeconocimiento.agesic.gub.uy/documents/80442/88295/PGE-Condiciones-de-uso-Plataforma-v01-21.pdf/7786ceca-21b5-0a1d-254e-1293a1330876?version=1.0

Electrónica Nacional y la Ventanilla Única de Comercio Exterior. Estos proyectos han mejorado significativamente la capacidad de las instituciones públicas para compartir y procesar datos de un modo más competente. La participación de la PDI en estos proyectos se refleja en el crecimiento sostenido de la cantidad de transacciones anuales soportadas por la plataforma, demostrando su estabilidad y su escalabilidad.

Al cierre del 2023, la PDI era utilizada por noventa y ocho organismos de la administración pública uruguaya con el fin de obtener información y compartirla, mientras que veintisiete de ellos publicaban un total de doscientos veintiún servicios disponibles para interoperar datos. Este nivel de adopción subraya la importancia de la PDI como una infraestructura esencial para la interoperabilidad en el sector público uruguayo, promoviendo la integración de datos y la mejora de la eficiencia en la gestión pública [32].

[32] (s. f.). Servicios Digitales Transfronterizos. Programa para el fortalecimiento de las transacciones electrónicas transfronterizas en América Latina y el Caribe. "Bienes Públicos Regionales". *Reagealc*. Disponible en https://www.redgealc.org/site/assets/files/13516/anexo_1_-_servicios_digitales_transfronterizos_-_indice.pdf

4. Casos de análisis

4.1 Intercambio de datos e inteligencia artificial

Los datos y la Inteligencia Artificial (IA) están estrechamente relacionados debido a varias razones cuyo análisis exceden el alcance de este documento. En síntesis, la implementación de IA requiere un enfoque robusto en la protección, la gestión y la gobernanza de datos para asegurar la privacidad y la seguridad de la información manejada al mismo tiempo que las leyes y las regulaciones sobre datos impactan directamente en cómo los datos pueden utilizarse y almacenarse para entrenar y operar sistemas de IA.

Dicho lo anterior, es particularmente relevante el artículo 74 de la Ley No. 20.212, aprobada el 06 de noviembre del 2023 que atribuyó a la AGESIC el cometido de diseñar y desarrollar una estrategia nacional de datos e inteligencia artificial basada en estándares internacionales (en los ámbitos público y privado), encomendándole, a su vez, la elaboración de recomendaciones de regulación de la IA al Poder Legislativo.

En ese marco, en el 2024, AGESIC elaboró y entregó al Poder Legislativo el informe *Artículo 74 de la Ley No. 20.212. Recomendaciones para una regulación de la Inteligencia Artificial (IA) orientada al desarrollo ético, la protección de los derechos humanos y el fomento de la innovación tecnológica* [33] donde se menciona que su elaboración fue con "una metodología predefinida, y a través de un proceso en el que se contó con la participación de funcionarios y consultores de diversos organismos públicos, con quienes luego de distintas reuniones se definió un documento de consulta que fue puesto a disposición de otros actores (organismos y entidades privadas, academia y sociedad civil) previamente identificados, empleando a esos efectos la plataforma de participación ciudadana gestionada por Agesic." (AGESIC, s. f., 09).

Los organismos públicos que realizaron aportes fueron:

- Presidencia de la República (Prosecretaría de la Presidencia y Secretaría de Derechos Humanos).
- Ministerio de Educación y Cultura (Consejo de Derechos de Autor).
- Ministerio de Economía y Finanzas (Unidad Defensa del Consumidor).
- Ministerio de Industria, Energía y Minería (Dirección Nacional de Telecomunicaciones

[33] (s. f.). Informe artículo 74 Ley No. 20.212. Recomendaciones para una regulación de la Inteligencia Artificial (IA) orientada al desarrollo ético, la protección de los derechos humanos y el fomento de la innovación tecnológica. *AGESIC y Uruguay Presidencia*. Disponible en https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/sites/agencia-gobierno-electronico-sociedad-informacion-conocimiento/files/documentos/publicaciones/Art%C3%ADculo%2074%20de%20la%20Ley%20N%C2%BA20.212%20recomendaciones%20para%20una%20regulaci%C3%B3n%20de%20la%20Inteligencia%20Artificial%20%28IA%29_0.pdf

y Dirección Nacional de la Propiedad Industrial).
- Ministerio de Trabajo y Seguridad Social (Inspección General del Trabajo y la Seguridad Social).
- Unidad Reguladora de Servicios de Comunicaciones.
- Agencia Nacional de Investigación e Innovación.
- Programa Uruguay Innovation Hub.
- Unidad Reguladora y de Control de Datos Personales.
- Institución Nacional de Derechos Humanos y Defensoría del Pueblo (INDDHH).

A su vez, en el proceso de consulta realizado se recibieron aportes de:

- Asociación de Escribanos del Uruguay (AEU).
- Laboratorio de Datos y Sociedad (DatySoc).
- DATA Uruguay.
- Cámara Uruguaya de Tecnologías de la Información (CUTI).

Como se evidencia, el proceso de elaboración de las recomendaciones recogidas en el informe tuvo una amplia participación de actores públicos y privados de la más diversa índole en el marco de una temática muy relevante para el país como lo es la estrategia nacional de datos e IA.

Si bien la AGESIC, actor público y de perfil técnico, posee un liderazgo claro y gravitante en la construcción de la estrategia mencionada, también recomienda —en el informe— potenciar los mecanismos de intervención y colaboración de todas las partes interesadas y recoge explícitamente medidas y aportes específicos y sugeridos por los actores participantes (p. ej.: creación de foros y realización de audiencias públicas con la colaboración de diferentes actores, generación de grupos asesores multidisciplinarios con funcionamiento regular, etcétera). Además, en el propio informe se incluyen los aportes completos de la INDDHH, de Data Uruguay, del Laboratorio de Datos y Sociedad (DatySoc) y de la Asociación de Escribanos del Uruguay (AEU) como anexo.

Adicionalmente, dentro de las recomendaciones que plantea este documento, se incluyen aspectos vinculados al intercambio de datos. En particular, en cuanto a las recomendaciones asociadas a la institucionalidad y a la gobernanza, se menciona “habilitar el empleo de la plataforma de interoperabilidad prevista en el Decreto No. 178 / 013 del 11 de junio del 2013, por parte de entidades privadas.” (AGESIC, s. f., p. 100).

Por su parte, vinculado a infraestructura y ciberseguridad, se menciona “en aspectos de sustento normativo para el intercambio de datos en forma segura, resulta recomendable habilitar el uso de la Plataforma de Interoperabilidad creada por el Decreto No 178 / 013 para el consumo de servicios por parte de entidades privadas” (AGESIC, s. f., p. 115).

Ambas recomendaciones (en proceso de elaboración por la AGESIC mientras se realiza este informe) se presentan como habilitadores y catalizadores de un ecosistema público privado que potencia el desarrollo de servicios digitales de calidad sin dejar de presentar desafíos en relación con mantener y asegurar las garantías y las condiciones en aspectos de manejo seguro de datos y respeto por su privacidad.

4.2 Intercambio de datos transfronterizos

Uruguay ha implementado regulaciones específicas sobre las transferencias internacionales de datos personales. La resolución No. 23 / 021 de la URCDP de 2021 [34] establece que los datos pueden ser transferidos a países considerados adecuados; entre ellos podemos nombrar a los estados miembros de la UE y a otros países con un marco legal robusto.

Uruguay fue uno de los primeros países de América Latina en obtener el estatus "adecuado" bajo el GDPR, lo que facilita la transferencia de datos personales hacia y desde la UE sin necesidad de salvaguardas adicionales [35].

Además, Uruguay participa activamente en acuerdos regionales e internacionales que buscan facilitar el flujo de datos entre países, promoviendo la cooperación en áreas clave como el comercio digital y la seguridad de la información [36] [37] [38] [39]. Estos aspectos, se ven reflejados en el borrador de la Estrategia Nacional de Datos 2024 – 2030 donde, como se mencionó, se incluyen aspectos del intercambio transfronterizo como parte de su planteamiento.

En cuanto a la firma digital, Uruguay ha establecido un marco normativo sólido mediante de la Ley No. 18.600 [40] con la que regula el uso de la firma electrónica y establece los estándares de certificación. Esto permite que las firmas digitales tengan el mismo valor legal que las firmas manuscritas, facilitando transacciones electrónicas seguras a nivel nacional e internacional. La UCE es el órgano responsable de supervisar la implementación de estas tecnologías en el país, garantizando su interoperabilidad con sistemas mundiales.

Uruguay participa en espacios de diálogo en la región sobre esta temática que implica un desafío a nivel de adopción de normativa y reglas comunes para los países que suscriben

[34] (2012, 08 de junio). Resolución No. 23 / 021. *Unidad Reguladora y de Control de Datos Personales*. Disponible y descarga en https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-23021

[35] (2024, 15 de enero). La Comisión Europea ratifica el nivel adecuado de Uruguay para la protección de datos. Disponible en *Unidad Reguladora y de Control de Datos Personales*. https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/noticias/comision-europea-ratifica-nivel-adecuado-uruguay-para-proteccion-datos-0

[36] (2023, 13 de diciembre). Nuevo convenio de cooperación técnica en identificación digital entre Uruguay y Paraguay. "Identificación oficial". *Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento.* Disponible y descarga en https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/noticias/nuevo-convenio-cooperacion-tecnica-identificacion-digital-entre-uruguay

[37] (2023, 12 de diciembre). Uruguay y Brasil firman convenio de cooperación técnica en identificación digital. "Identificación oficial". *Unidad de Certificación Electrónica.* Disponible y descarga en https://www.gub.uy/unidad-certificacion-electronica/comunicacion/noticias/uruguay-brasil-firman-convenio-cooperacion-tecnica-identificacion-digital

[38] (2024, 18 de septiembre). Acuerdos de reconocimientos transfronterizos de firma digital. *Unidad de Certificación Electrónica.* Disponible en https://www.gub.uy/unidad-certificacion-electronica/politicas-y-gestion/acuerdos-reconocimientos-transfronterizos-firma-digital

[39] (2024, 03 de abril). Firma transfronteriza en Mercosur. "Firma digital". *Unidad de Certificación Electrónica.* Disponible en https://www.gub.uy/unidad-certificacion-electronica/comunicacion/noticias/firma-transfronteriza-mercosur

[40] (2009,05 de noviembre). Ley No. 18.600. Documento electrónico y firma electrónica. Admisibilidad, validez y eficacia. *Centro de Información Oficial. Normativa y avisos legales de Uruguay*. Disponible en https://www.impo.com.uy/bases/leyes/18600-2009

acuerdos, alianzas o planes de acción comunes. Una muestra es que a nivel de América Latina no existe un espacio de gobernanza similar a la Comisión Europea donde se aborden temáticas, se arriben conclusiones y acuerdos y finalmente se dicte una normativa que deban adoptar obligatoriamente todos los países miembros.

A modo de ejemplo, la Alianza Digital Unión Europea – América Latina y el Caribe (de la cual Uruguay es parte) en mayo del 2024 convocó a un diálogo político para mejorar la cooperación en el aspecto de la administración digital. Como resultado, se establecieron conclusiones operativas, áreas de acción e intervenciones conjuntas en materia de interoperabilidad transfronteriza de datos, identificación digital y firma electrónica.

Uruguay manifestó interés particularmente en las siguientes actividades que ponen la mira en la próxima cumbre 2025 UE – ALC:

Objetivo	Actividad
Fortalecer la comunidad que facilite la cooperación entre *stakeholders*. **Prestar apoyo a la validación de proyectos de interoperabilidad transfronteriza de datos.** **Realizar una prueba de concepto.**	Promover una iniciativa regional para el consentimiento digital (autorización de acceso a datos).
Compartir conocimientos y experiencia sobre interoperabilidad entre ALC y los países de la UE.	Promover estrategias de participación ciudadana y sensibilización sobre los derechos digitales y las implicaciones de la interoperabilidad regional.
Desarrollo del marco regional ALC de identificación digital transfronteriza y firma electrónica.	Identificar referentes en ALC y la UE con experiencia en firma electrónica transfronteriza e identificación digital.
Fortalecer la comunidad para planificar nuevas actividades para el desarrollo y la aplicación de un modelo de reconocimiento transfronterizo para países de ALC.	Crear o reforzar grupos de trabajo en identificación digital y firma electrónica para debatir principios jurídicos, normas internacionales, prácticas comunes y requisitos técnicos comunes.
Compartir conocimientos y experiencias sobre identificación digital y electrónica entre los países de la UE.	Desarrollar la capacidad técnica y la concienciación de las partes interesadas en materia de identificación digital y firma electrónica.

4.3 Salud Digital

Salud Digital [41] es una evolución del programa Salud.uy creado en 2012. Su objetivo es mejorar la eficiencia y la calidad de los servicios de salud por medio de la integración y del intercambio de información en el sistema de salud y es un modelo destacado a nivel regional y parte fundamental de la transformación digital del sistema de salud en Uruguay.

Es destacable la gobernanza potente que se estableció desde el inicio para este programa con amplia y plural participación. Distintos órganos y sus integrantes llevan adelante un conjunto de cometidos para la implementación y el control de objetivos y procesos; entre ellos se destacan el Comité de Dirección, autoridad máxima responsable de definir y aprobar la política y la estrategia, así como controlar y asentir presupuestos e inversiones; el Consejo Asesor, quien facilita el asesoramiento técnico; y diversos Grupos Asesores.

Esta gobernanza tuvo cambios y actualizaciones a lo largo del tiempo, siendo las más importantes:

- Artículo 76 de la Ley No. 20.075 [42] donde se atribuye a la AGESIC los objetivos específicos del programa Salud.uy y se agregan dos Consejos Asesores Honorarios:

  - **Consejo Asesor de Políticas Digitales en Salud** integrado por la Presidencia de la República, el Ministerio de Economía y Finanzas (MEF), el Ministerio de Salud Pública (MSP), la Junta Nacional de Salud (JUNASA), la Agencia de Evaluación y Monitoreo de Políticas Públicas (AEMPP), la Agencia de Evaluación de Tecnologías Sanitarias (AETS) y la Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (AGESIC).
  - **Consejo Asesor de Coordinación Interinstitucional en Políticas Digitales** integrado por la Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (AGESIC), la Administración Nacional de Telecomunicaciones (ANTEL), la Administración de los Servicios de Salud del Estado (ASSE), el Banco de Prevención Social (BPS), el Fondo Nacional de Recursos (FNR), la Red Integrada de Efectores Públicos de Salud (RIEPS), el Hospital de Clínicas, la Sociedad Uruguaya de Estandarización, Intercambio e Integración de Datos e Información de Servicios de Salud (SUEIIDISS), los Gremiales de Prestadores Integrales de Salud (GREMCA), las Emergencias Móviles, la Facultad de Medicina y la Facultad de Ingeniería.

[41] (s. f.). Salud Digital. "Salud Digital". *Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento.* Disponible y descarga en https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/politicas-y-gestion/programas/es-saluduy

[42] (2022, 03 de noviembre). Aprobación de rendición de cuentas y balance de ejecución presupuestal. Ejercicio 2021. *Centro de Información Oficial. Normativa y avisos legales del Uruguay.* Disponible en https://www.impo.com.uy/bases/leyes/20075-2022

- Artículo 77 de la Ley No. 20.212 [43] donde se establece que la AGESIC tendrá el cometido de asesorar al MSP en la aplicación de tecnologías de la información en el ámbito de salud en general, poniendo a disposición del ministerio los medios digitales para el procesamiento de información de salud.

Además de ser ejemplo de gobernanza, también lo es de interoperabilidad en sus cuatro niveles. Para demostrarlo, pueden mencionarse el Decreto 242 / 017 [44] que reglamenta los mecanismos de intercambio de información a través del sistema de HCEN y el Modelo de Referencia de Tecnología [45].

Es así como Salud Digital constituye un caso de éxito, siendo ecosistema existente desde hace doce años donde se realiza intercambio de datos entre actores públicos y privados de información altamente sensible, con una potente gobernanza, una robusta interoperabilidad y con revisiones y mejoras permanentes a lo largo del tiempo.

4.4 Censo 2023

El censo realizado en 2023 en Uruguay estuvo marcado por una serie de tensiones acerca de la privacidad de los datos personales, la percepción sobre la privacidad y el uso de esa información. Pese a los esfuerzos del INE por asegurar la confidencialidad de la información, las preocupaciones en torno al manejo de datos sensibles persistieron. El principal punto controversial tuvo relación con la recolección del dato sensible de la cédula de identidad [46] [47].

DatySoc realizó un extenso análisis del asunto e hizo algunas recomendaciones a los ciudadanos [48]. En relación con eso, cabe mencionar los siguientes puntos:

- El número de cédula era obligatorio en el formato digital, mientras que no lo era en el presencial, lo que generó dudas sobre la equidad en el tratamiento de los ciudadanos según la modalidad elegida.
- Hubo poca claridad sobre el uso específico tanto del número de cédula como de su

[43] (2023, 17 de noviembre). Ley No. 20.212. Aprobación de rendición de cuentas y balance de ejecución presupuestal. Ejercicio 2022. *Centro de Información Oficial. Normativa y avisos legales del Uruguay.* Disponible en https://www.impo.com.uy/bases/leyes/20212-2023#:~:text=Cr%C3%A9ase%20una%20estructura%20integrada%20por,dependientes%20de%20la%20Direcci%C3%B3n%20General

[44] (2017, 07 de septiembre). Decreto No. 242 / 017. Reglamentación del art. 466 de la Ley No., relativo a los mecanismos de intercambio de información clínica con fines asistenciales a través del Sistema de Historia Clínica Electrónica Nacional. Revocación del Decreto No. 396 / 003. *Centro de Información Oficial. Normativa y Avisos legales del Uruguay.* Disponible en https://www.impo.com.uy/bases/decretos/242-2017

[45] (s. f.). Arquitectura de referencia HCEN. *AGESIC y Uruguay Presidencia.* Disponible en https://centroderecursos.agesic.gub.uy/web/arquitectura-salud.uy/inicio/-/wiki/Soluci%C3%B3n+peque%C3%B1os+prestadores/Arquitectura+Tecnol%C3%B3gica

[46] (2023, 20 de abril). Censo 2023: pedirán el número de cédula por primera vez y advierten por protección de datos personales. *El Observador*. Disponible en https://www.elobservador.com.uy/nota/censo-2023-pediran-el-numero-de-cedula-por-primera-vez-y-advierten-por-proteccion-de-datos-personales-2023420154121

[47] (2023, 21 de abril). Censo 2023: preocupación en organizaciones por el pedido de cédula de identidad y la "protección de datos personales". *La diaria.* Disponible en https://ladiaria.com.uy/usuarios/entrar/?article=106064

[48] DatySoc. (2023, 28 de abril). Qué tienes que saber sobre la cédula en el Censo 2023. *DatySoc*. Disponible en https://datysoc.org/2023/04/28/que-tenes-que-saber-sobre-la-cedula-en-el-censo-2023/#:~:text=El%20n%C3%BAmero%20de%20c%C3%A9dula%20de,deben%20responder%20el%20censo%20digital.

integración con otros registros administrativos y su posible vinculación con bases de datos gubernamentales.

- Surgieron temores acerca de que este eventual cruce de datos pudiera abrir la puerta a una mayor vigilancia estatal, ya que el censo podría permitir a las autoridades acceder a información sensible centralizadamente.
- Al solicitar el número de cédula, podría facilitarse la discriminación por parte del gobierno o de terceros si la información recopilada se cruza con otras bases de datos, especialmente en relación con temas como ingresos, salud o características étnicas.
- Aunque la Ley No. 18.331 establezca algunos estándares de protección, se cuestionó si el manejo de la cédula en el censo cumplía completamente con estas normativas.
- Pese a que el INE aseguró que se seguirían las normas de protección de datos, se señaló la falta de información sobre las medidas concretas adoptadas para resguardar los datos recolectados, factor que generó desconfianza entre la población.
- La obligatoriedad de la cédula en el censo digital tiene el riesgo de erosionar la confianza de los ciudadanos en el sistema censal y en las instituciones encargadas de manejar sus datos personales.

A raíz de las críticas, el INE modificó las razones por las cuales se solicitaba obligatoriamente el número de la cédula de identidad y realizó una consulta ante la Unidad Reguladora y de Control de Datos Personales (URCDP), quien emitió un dictamen pretendiendo dar las garantías necesarias en el ámbito de su competencia [49].

De lo expuesto, se desprende, en primer lugar, cómo los diferentes actores y la normativa vigente dispusieron los mecanismos necesarios para la protección de los derechos humanos de los ciudadanos ante este caso concreto. En segundo lugar, plantea una oportunidad de fortalecimiento en los niveles que sean necesarios (normativo, gobernanza, etcétera) a los efectos de superar estas tensiones en el futuro, incluso, aun cuando Uruguay pueda considerarse ejemplo en lo referente al intercambio y a la a gobernanza de datos.

4.5 Reconocimiento facial automatizado, ciberpatrullaje y videovigilancia

En febrero del 2020, el Ministerio del Interior procedió a la adquisición de una plataforma de identificación facial mediante licitación pública.

En diciembre de ese año, la Ley No. 19.924 [50] estableció la creación de una “base de datos de identificación facial para su administración y tratamiento con fines de seguridad pública” (artículos 191 y 192) por parte del Ministerio del Interior. Sin embargo, a pesar de la aprobación de estos artículos, no se ha desarrollado una reglamentación específica ni

[49] (2023, 28 de marzo). Dictamen No. 4 / 023. *Unidad Reguladora y de Control de Datos Personales.* Disponible y descarga en https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/dictamen-n-4023

[50] (2020, 30 de diciembre). Ley No. 19.924. Presupuesto nacional de sueldos, gastos e inversiones. Ejercicios 2020 – 2024. *Centro de Información Oficial. Normativa y avisos legales del Uruguay.* Disponible en https://www.impo.com.uy/bases/leyes/19924-2020

protocolos de uso ni detalle alguno sobre el sistema de reconocimiento facial automatizado, provocando una amplia discrecionalidad sobre el empleo de los datos biométricos.

La sociedad civil, mediante organizaciones como DatySoc, destacan las preocupaciones y desafíos relacionados con el uso del reconocimiento facial en Uruguay.

A modo de antecedente, en noviembre del 2021, DatySoc efectuó un pedido de acceso a información pública al Ministerio del Interior en el marco de la Ley No. 18.381, acerca de la adquisición de la plataforma de identificación facial y el *software* de Reconocimiento Facial Automatizado (RFA), pedido que fue rechazado por el ministerio en diciembre de ese año.

En marzo del 2022 DatySoc publicó el informe *Fuera de control: uso policial del reconocimiento facial automatizado en Uruguay* [51] y ese año demandó al Ministerio del Interior por negarse a dar información mencionada. Incluso la UIAP dictaminó que debía entregarse "la información que es pública, así como clasificar la información reservada." (p. 4) [52]. En 2023 DatySoc publicó un documento ampliatorio del informe con los resultados de la demanda y el juicio contra el ministerio [53].

Sin perjuicio de los resultados concretos y el desenlace del caso presentado, los desafíos están sobre la mesa y pasan por profundizar en la discusión sobre el enrolamiento masivo la población en el sistema de RFA, la prohibición o limitación del uso de RFA como medio de vigilancia, la existencia de regulaciones, protocolos de actuación públicos, mecanismos de análisis de impacto y de evaluación de riesgo, capacitaciones sobre funcionamiento y riesgos, la necesidad de participación ciudadana y la existencia de procesos de transparencia y rendición de cuentas.

En el mismo sentido, DatySoc abordó el ciberpatrullaje en Uruguay y estableció un litigio contra el Ministerio del Interior con características análogas al caso anteriormente descrito a raíz de una nueva negativa de acceso a la información pública [54] y finalmente en junio del 2024 el ministerio debió entregar información que evidenció que realiza recolección de datos personales en fuentes abiertas [55] para la prevención y/o investigación de delitos y que ha realizado y ha aprobado estudios, regulaciones, propuestas de regulaciones o documentos

[51] Díaz, Charquero Patricia. (2022). *Fuera de control. Uso policial del reconocimiento facial automatizado en Uruguay.* Laboratorio de Datos y Sociedad (DatySoc) con el apoyo de INDELA y Derechos Digitales América Latina. Disponible en https://datysoc.org/wp-content/uploads/2022/03/Informe-reconocimiento-facial-automatizado-Uruguay-2022-Datysoc.pdf

[52] Consejo ejecutivo de la unidad de acceso a la información pública. (2022, 03 de junio). "Resolución No. 13 2022 / Expediente No. 2021 – 2 – 10 0000432". Unidad de Acceso a la Información Pública. *AGESIC y Uruguay Presidencia* Disponible en https://www.gub.uy/unidad-acceso-informacion-publica/sites/unidad-acceso-informacion-publica/files/2022-06/RESUAIP22013-%20AA%20con%20MI.pdf

[53] (s. f.). Fuera de control: ampliación del informe y resultados del litigio sobre uso policial del reconocimiento facial automatizado en Uruguay. *DatySoc.* Disponible en https://datysoc.org/fuera-de-control-ampliacion-del-informe/

[54] Díaz, Charquero Patricia y Gemetto, Jorge. (2024, julio). *Ciberpatrullaje: ampliación del informe y resultados del litigio sobre vigilancia policial en Internet.* DatySoc con el apoyo de INDELA y el Fondo de Respuesta Rápida de Derechos Digitales. Disponible en https://datysoc.org/litigio-ciberpatrullaje/

[55] Fuente abierta puede considerarse toda información que sea accesible para cualquier persona sin necesidad de tener credenciales de acceso. En Uruguay, la Ley No. 19.696 (Sistema Nacional de Inteligencia de Estado), en su artículo 3, la define como "aquellas de las cuales se puede obtener un determinado informe, sin más restricción que la tarea que demanda su obtención".

para los cuales se han recopilado datos en fuentes abiertas. A su vez, ratificó que no firmó contratos con empresas privadas que se dediquen a la recopilación y análisis de datos en fuentes abiertas.

De igual modo, para este caso se presentan retos análogos al caso anterior que también han de abordarse y que tienen que ver con la revisión de la Ley No. 19.696 del Sistema Nacional de Inteligencia del Estado y del uso *Social Media Intelligence* (SOCMINT) para recopilar información de fuentes abiertas, diseño de protocolos específicos y públicos para dichas actividades, revisión y/o creación de legislación y trasparencia al establecer contratos relacionados con la adquisición de tecnología que se usa para actividades de vigilancia, entre otros.

En Uruguay fue especialmente trascedente el caso del excustodio del presidente de la República, a partir del cual se difundieron *chats* donde ofrecía a terceros contactos en la Dirección Nacional de Información e Inteligencia (DNII) e intervención de celulares con *software* El Guardián [56]. Inclusive, a pesar de la existencia de un protocolo de actuación para interceptaciones legales de comunicación y un Convenio entre el Ministerio del Interior, la Suprema Corte de Justicia, la Fiscalía General de la Nación y las empresas de telecomunicaciones, aún falta mucho camino por recorrer [57].

[56] Silva, Laura. (2022). Chats de Astesiano con importante empresario agropecuario argentino: ofrecía contactos en Inteligencia, drones, intervención de celulares con El Guardián y vehículos oficiales. *La diaria*. Disponible en https://ladiaria.com.uy/usuarios/entrar/?article=99907

[57] DatySoc. (2022, 24 de noviembre). Sobre el caso de Astesiano y la necesidad de regulación del ecosistema de vigilancia policial. *DatySoc.* Disponible en https://datysoc.org/2022/11/24/sobre-el-caso-astesiano-y-la-necesidad-de-regulacion-del-ecosistema-de-vigilancia-policial/

5. Conclusiones, retos y oportunidades

Uruguay ha logrado posicionarse como un referente regional en materia de gobernanza de datos e interoperabilidad en el sector público; un logro que refleja una estrategia digital coordinada y consistente. Este avance ha sido impulsado por un marco regulatorio sólido y en evolución constante, acompañado por una infraestructura tecnológica robusta y una clara visión de gobernanza de datos.

Dichos aspectos han sido potenciados por la continuidad institucional en la agenda de gobernanza e intercambio de datos, característica en la que Uruguay destaca en la región donde la continuidad de estas políticas enfrenta múltiples y complejos desafíos, pero, sin duda, este logro ha sido el resultado de una visión de políticas a largo plazo que ha sido sostenida y potenciada a través de diferentes gobiernos y administraciones que han permitido una evolución constante y progresiva del marco habilitante en áreas clave como la protección de datos personales, la seguridad de la información y la interoperabilidad.

De todos modos, este diferencial consolidado en un proceso de acumulación positiva que fortalece la transparencia y facilita la colaboración interinstitucional no debe dejar de poner foco que el camino hacia una mayor madurez en el intercambio de datos plantea importantes retos que requerirán atención.

Uno de los aspectos más destacados de la estrategia uruguaya es la creación de una arquitectura digital integrada en el ecosistema de intercambio de datos de la administración pública respaldada por la Plataforma de Interoperabilidad (PDI). Esta herramienta ha permitido que diversos organismos intercambien datos de forma eficiente y segura, lo que ha mejorado la calidad y la agilidad de los servicios públicos.

Además, la colaboración entre actores públicos y privados ha fomentado un ecosistema que ha facilitado el intercambio de datos de alta calidad, impulsando la modernización del Estado y la accesibilidad a más servicios para los ciudadanos con el caso de Salud Digital e Historia Clínica Electrónica Nacional como emblema.

Este caso exitoso puede brindar elementos relevantes para replicarse en otras áreas prioritarias que, si bien presentan buenos niveles de intercambio de datos en el ecosistema público y privado, todavía pueden avanzar y profundizarse. En este sentido, tanto el ecosistema de gobernanza como los ámbitos de discusión técnica o la arquitectura de intercambio diseñada pueden ser una buena referencia para el intercambio de datos en educación, seguridad, logística, previsión social o finanzas.

A nivel normativo, Uruguay tiene un marco legal ajustado a los estándares internacionales,

factor que asegura un ambiente propicio para la protección de los datos personales; por tanto, los ciudadanos tienen garantías legales suficientes para defender sus derechos ante abusos o falta de transparencia, lo que es clave en la construcción de un entorno de confianza en el manejo de la información.

Este marco legal junto con las capacidades tecnológicas del país crea las condiciones necesarias para una gobernanza democrática de datos. Casos recientes como la polémica sobre el censo del 2023 y la solicitud del número de cédula de identidad revelan la importancia de asegurar que los ciudadanos perciban que sus datos estén protegidos y que su privacidad sea respetada con un Estado que comunique proactivamente las decisiones tomadas.

Pese a estos avances, el intercambio de datos plantea varios riesgos que deben ser gestionados con cuidado. En particular, la privacidad y la protección de los datos personales sigue siendo una preocupación especialmente cuando se manejan datos sensibles o en contextos donde las tecnologías como la inteligencia artificial y el reconocimiento facial están en juego.

Estos avances tecnológicos pueden ser disruptivos si no están acompañados de un marco regulatorio transparente y una supervisión clara que prevenga el abuso y la vigilancia masiva. Su uso colectivo en casos como la prevención de delitos añade complejidad al debate sobre los derechos digitales y la privacidad; por lo tanto, estos mecanismos sin una regulación clara y transparente podrían generar un clima de desconfianza y percepción de vigilancia excesiva, erosionando la confianza en las instituciones públicas; por lo que es crucial que cualquier avance tecnológico sea acompañado de políticas robustas de comunicación y discusión, involucrando activamente múltiples actores en el proceso.

En particular, se presenta como relevante y necesario potenciar una perspectiva de construcción de confianza en las nuevas estrategias y esquemas de gobernanza en procesos de elaboración, acompañando las perspectivas tradicionales de calidad, ciclo de vida de datos, etcétera.

Otro desafío radica en la participación del sector privado y la sociedad civil en la gobernanza de datos. Mientras que la AGESIC ha sido un actor clave en la articulación de políticas y prácticas, continúa presentándose espacio para una articulación con el sector privado y con la sociedad civil principalmente en su participación en el seguimiento de las políticas definidas, potenciando mucho más un ecosistema inclusivo, equilibrado y confiable en la toma de decisiones sobre datos. Este aspecto toma principal relevancia ante las iniciativas de incluir al sector privado en el intercambio de datos públicos tal como se ha manifestado en las recomendaciones propuestas por la AGESIC en este informe.

Asimismo, las organizaciones de la sociedad civil han jugado un papel muy importante en el área de la transparencia y los datos abiertos, pero su participación en la gobernanza de datos ha sido más reactiva y limitada por los espacios de diálogo proporcionados por el Gobierno. En consecuencia, se requiere un mayor esfuerzo para generar espacios de participación inclusivos y sostenibles que permitan a estas organizaciones contribuir de manera significativa.

Para consolidar los logros y mitigar los riesgos mencionados, es esencial institucionalizar espacios de gobernanza de datos que aseguren su continuidad en el tiempo, integrando al sector privado, a la academia y a la sociedad civil en los procesos de toma de decisiones. Uruguay tiene la oportunidad de continuar avanzando y solidificando la construcción de un sistema de gobernanza con la participación efectiva y proactiva de distintos actores, es decir, no está condicionada nada más en la creación de espacios de diálogo exclusivamente desde el gobierno en momentos del diseño de políticas. Esto no solo fortalecerá la confianza en el intercambio de datos, sino que fomentará la innovación y el desarrollo de servicios con valor agregado para la sociedad.

De igual modo, es trascendental lograr una efectiva implementación de interoperabilidad de datos entre el sector público y privado, facilitando el intercambio de información mediante la creación de incentivos claros y transparentes. El uso de plataformas tecnológicas como la Plataforma de Interoperabilidad (PDI) por entidades privadas debe estar sujeto a normas estrictas que garanticen la seguridad y la privacidad de los datos. Complementando este punto, la reutilización de datos abiertos generados por instituciones públicas puede potenciarse con nuevos sistemas de incentivos, permitiendo que el sector privado los aproveche para desarrollar nuevas soluciones.

En resumen, Uruguay ha recorrido un largo camino en la construcción de un ecosistema digital que fomenta el intercambio de datos de forma segura y eficiente; sin embargo, el país todavía enfrenta retos importantes en cuanto a la participación de todos los sectores y en la aplicación práctica de las políticas, por lo que es necesario seguir promoviendo una gobernanza de datos que garantice la protección de los derechos de los ciudadanos al tiempo que impulsa la colaboración y la innovación. Procesos de consulta pública como los desarrollados en la Estrategia Nacional de Datos e Inteligencia Artificial son un excelente paso en esta dirección, pero deben ser fortalecidos y ampliados.

A medida que se avanza hacia una mayor integración de tecnologías y se amplían las capacidades de interoperabilidad, los riesgos también aumentan, de manera que es fundamental que el país mantenga un enfoque equilibrado que priorice la innovación tecnológica y la protección de los derechos de los ciudadanos al asegurar que el intercambio de datos siga siendo una herramienta para el desarrollo y la inclusión sin sacrificar la privacidad y la confianza pública, porque solo así será posible alcanzar un equilibrio y una visión sistémica entre la apertura de datos, el intercambio, la seguridad de la información y la protección de la privacidad, construyendo un futuro donde los datos sean un verdadero motor para el desarrollo socioeconómico.

Referencias

(2024, 18 de septiembre). Acuerdos de reconocimientos transfronterizos de firma digital. *Unidad de Certificación Electrónica*. Disponible en https://www.gub.uy/unidad-certificacion-electronica/politicas-y-gestion/acuerdos-reconocimientos-transfronterizos-firma-digital

(2023, 18 de diciembre). Agenda Uruguay Digital 2025 – Sociedad digital resiliente. "Uruguay digital". *AGESIC*. Descarga y disponible en: https://www.gub.uy/uruguay-digital/comunicacion/publicaciones/agenda-uruguay-digital-2025-sociedad-digital-resiliente/agenda-uruguay

Comisión Europea. (2007). *Anexo de la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Marco Europeo de Interoperabilidad – Estrategia de aplicación.* Disponible en https://eur-lex.europa.eu/resource.html?uri=cellar:2c2f2554-0faf-11e7-8a35-01aa75ed71a1.0010.02/DOC_3&format=PDF

(2022, 03 de noviembre). Aprobación de rendición de cuentas y balance de ejecución presupuestal. Ejercicio 2021. *Centro de Información Oficial. Normativa y avisos legales del Uruguay.* Disponible en https://www.impo.com.uy/bases/leyes/20075-2022

(s. f.). Arquitectura de referencia HCEN. *AGESIC y Uruguay Presidencia.* Disponible en https://centroderecursos.agesic.gub.uy/web/arquitectura-salud.uy/inicio/-/wiki/Soluci%C3%B3n+peque%C3%B1os+prestadores/Arquitectura+Tecnol%C3%B3gica

(s. f.). Condiciones de uso de la Plataforma de Interoperabilidad. Especificación técnica. Plataforma de Interoperabilidad. *AGESIC y Uruguay Presidencia*. Disponible y descarga en https://centrodeconocimiento.agesic.gub.uy/documents/80442/88295/PGE-Condiciones-de-uso-Plataforma-v01-21.pdf/7786ceca-21b5-0a1d-254e-1293a1330876?version=1.0

(2023, 20 de abril). Censo 2023: pedirán el número de cédula por primera vez y advierten por protección de datos personales. *El Observador*. Disponible en https://www.elobservador.com.uy/nota/censo-2023-pediran-el-numero-de-cedula-por-primera-vez-y-advierten-por-proteccion-de-datos-personales-2023420154121

(2023, 21 de abril). Censo 2023: preocupación en organizaciones por el pedido de cédula de identidad y la "protección de datos personales". *La diaria.* Disponible en https://ladiaria.com.uy/usuarios/entrar/?article=106064

Consejo ejecutivo de la unidad de acceso a la información pública. (2022, 03 de junio). “Resolución No. 13 2022 / Expediente No. 2021 – 2 – 10 0000432”. Unidad de Acceso a la Información Pública. *AGESIC y Uruguay Presidencia* Disponible en https://www.gub.uy/unidad-acceso-informacion-publica/sites/unidad-acceso-informacion-publica/files/2022-06/RESUAIP22013-%20AA%20con%20MI.pdf

DatySoc. (2023, 28 de abril). Qué tienes que saber sobre la cédula en el Censo 2023. *DatySoc*. Disponible en https://datysoc.org/2023/04/28/que-tenes-que-saber-sobre-la-cedula-en-el-censo-2023/#:~:text=El%20n%C3%BAmero%20de%20c%C3%A9dula%20de,deben%20responder%20el%20censo%20digital.

DatySoc. (2022, 24 de noviembre). Sobre el caso de Astesiano y la necesidad de regulación del ecosistema de vigilancia policial. *DatySoc.* Disponible en https://datysoc.org/2022/11/24/sobre-el-caso-astesiano-y-la-necesidad-de-regulacion-del-ecosistema-de-vigilancia-policial/

(2021, 12 de mayo). Decreto No. 134/ 021. Aprobación de la “Agenda Uruguay Digital 2025”. *Centro de Información Oficial. Normativa y avisos legales del Uruguay*. Disponible en https://www.impo.com.uy/bases/decretos/134-2021%EF%BB%BF

(2009, 05 de enero). Decreto No. 664 / 008. Creación del registro de bases de datos personales. *Centro de Información Oficial. Normativa y avisos legales del Uruguay*. Disponible en https://www.impo.com.uy/bases/decretos/664-2008

(2020, 21 de febrero). Decreto No. 64 / 020. Reglamentación de los arts. 37 a 40 de la Ley 19.670 y art. 12 de la Ley 18.331, referente a protección de datos personales. *Centro de Información Oficial. Normativa y avisos legales del Uruguay*. Disponible en https://www.impo.com.uy/bases/decretos/64-2020

(2017, 07 de septiembre). Decreto No. 242 / 017. Reglamentación del art. 466 de la Ley No., relativo a los mecanismos de intercambio de información clínica con fines asistenciales a través del Sistema de Historia Clínica Electrónica Nacional. Revocación del Decreto No. 396 / 003. *Centro de Información Oficial. Normativa y Avisos legales del Uruguay.* Disponible en https://www.impo.com.uy/bases/decretos/242-2017

(2023, 16 de noviembre). Decreto No. 353 / 023. Reglamentación del art. 76 de la Ley No. 19.355, relativo al procedimiento aplicable por las entidades públicas, a los efectos de simplificar sus trámites, siguiendo los lineamientos de la agesic. Modificación del art. 15 y derogación del art. 13 del decreto No. 178 / 013. *Centro de Información Oficial. Normativa y avisos legales del Uruguay*. Disponible en https://www.impo.com.uy/bases/decretos/353-2023

(2009, 15 de septiembre). Decreto No. 414 / 009. Reglamentación de la Ley 18.331, relativo a la protección de datos personales. *Centro de Información Oficial. Normativa y avisos legales del Uruguay*. Disponible en https://www.impo.com.uy/bases/decretos/414-2009

(2013, 25 de julio). Decreto No. 178 / 013. Reglamentación de los artículos 157 a 160 de la Ley No. 18.719, relativos a la regulación en el intercambio de información entre entidades públicas, estatales o no estatales. *Centro de Información Oficial. Normativa y avisos legales del Uruguay*. Disponible en https://www.impo.com.uy/bases/decretos/178-2013

(2010, 10 de agosto). Decreto No. 232 / 010. Reglamentación de la ley sobre el derecho de acceso a la información pública. *Centro de Información Oficial. Normativa y avisos legales del Uruguay*. Disponible en https://www.impo.com.uy/bases/decretos/232-2010/

Díaz, Charquero Patricia y Gemetto, Jorge. (2024, julio). *Ciberpatrullaje: ampliación del informe y resultados del litigio sobre vigilancia policial en Internet.* DatySoc con el apoyo de INDELA y el Fondo de Respuesta Rápida de Derechos Digitales. Disponible en https://datysoc.org/litigio-ciberpatrullaje/

Díaz, Charquero Patricia. (2022). *Fuera de control. Uso policial del reconocimiento facial automatizado en Uruguay.* Laboratorio de Datos y Sociedad (DatySoc) con el apoyo de INDELA y Derechos Digitales América Latina. Disponible en https://datysoc.org/wp-content/uploads/2022/03/Informe-reconocimiento-facial-automatizado-Uruguay-2022-Datysoc.pdf

(2023, 28 de marzo). Dictamen No. 4 / 023. *Unidad Reguladora y de Control de Datos Personales.* Disponible y descarga en https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/dictamen-n-4023

(2023, 18 de mayo). Estrategia de datos de la Intendencia de Montevideo. *Intendencia Montevideo*. Disponible y descarga en https://montevideo.gub.uy/noticias/tecnologia/estrategia-de-datos-de-la-intendencia-de-montevideo

(2024, 03 de abril). Firma transfronteriza en Mercosur. “Firma digital”. *Unidad de Certificación Electrónica.* Disponible en https://www.gub.uy/unidad-certificacion-electronica/comunicacion/noticias/firma-transfronteriza-mercosur

(s. f.). Fuera de control: ampliación del informe y resultados del litigio sobre uso policial del reconocimiento facial automatizado en Uruguay. *DatySoc.* Disponible en https://datysoc.org/fuera-de-control-ampliacion-del-informe/

(1991, 18 de enero). *610 – 1990 – IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries*. IEEE. DOI: 10.1109/IEEESTD.1991.106963

(s. f.). Informe artículo 74 Ley No. 20.212. Recomendaciones para una regulación de la Inteligencia Artificial (IA) orientada al desarrollo ético, la protección de los derechos humanos y el fomento de la innovación tecnológica. *AGESIC y Uruguay Presidencia*. Disponible en https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/sites/agencia-gobierno-electronico-sociedad-informacion-conocimiento/files/documentos/publicaciones/Art%C3%ADculo%2074%20de%20la%20Ley%20N%C2%BA20.212%20recomendaciones%20para%20una%20regulaci%C3%B3n%20de%20la%20Inteligencia%20Artificial%20%28IA%29_0.pdf

(s. f.). "Iniciativa 'Datos 360°"". "Datos 360°"". *Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento*. Disponible en https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/node/3557

International Standard. (2015, mayo). *Information technology – Vocabulary*. ISO / IEC 2382:2015. Disponible en https://www.iso.org/standard/63598.html

(2024, 15 de enero). La Comisión Europea ratifica el nivel adecuado de Uruguay para la protección de datos. Disponible en *Unidad Reguladora y de Control de Datos Personales*. https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/noticias/comision-europea-ratifica-nivel-adecuado-uruguay-para-proteccion-datos-0

(2013, 07 de enero). Ley No. 19.030. Aprobación del convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. *Centro de Información Oficial. Normativa y avisos legales del Uruguay*. Disponible en https://www.impo.com.uy/bases/leyes/19030-2012

(2021, 27 de abril). Ley No. 19.948. Aprobación del protocolo de enmienda del convenio para la protección de las personas con respecto al tratamiento de datos personales, suscrito en Estrasburgo. *Centro de Información Oficial. Normativa y avisos legales del Uruguay*. Disponible en https://www.impo.com.uy/bases/leyes/19948-2021

(2018, 25 de octubre). Ley No. 19.670. Aprobación de rendición de cuentas y balance de ejecución presupuestal. Ejercicio 2017. *Centro de Información Oficial. Normativa y avisos legales del Uruguay*. Disponible en https://www.impo.com.uy/bases/leyes/19670-2018

(2022, 03 de noviembre). Ley No. 20.075. Aprobación de rendición de cuentas y balance de ejecución presupuestal. Ejercicio 2021. *Centro de Información Oficial. Normativa y avisos legales del Uruguay*. Disponible en https://www.impo.com.uy/bases/leyes/20075-2022

(2023, 17 de noviembre). Ley No. 20212. Aprobación de rendición de cuentas y balance de ejecución presupuestal. Ejercicio 2022. *Centro de Información Oficial. Normativa y avisos legales del Uruguay*. Disponible en https://www.impo.com.uy/bases/leyes/20212-2023/74

(2023, 17 de noviembre). Ley No. 20.212. Aprobación de rendición de cuentas y balance de ejecución presupuestal. Ejercicio 2022. *Centro de Información Oficial. Normativa y avisos*

legales del Uruguay. Disponible en https://www.impo.com.uy/bases/leyes/20212-2023#:~:text=Cr%C3%A9ase%20una%20estructura%20integrada%20por,dependientes%20de%20la%20Direcci%C3%B3n%20General

(2009,05 de noviembre). Ley No. 18.600. Documento electrónico y firma electrónica. Admisibilidad, validez y eficacia. *Centro de Información Oficial. Normativa y avisos legales de Uruguay*. Disponible en https://www.impo.com.uy/bases/leyes/18600-2009

(2008, 18 de agosto). Ley No. 18.331. Ley de protección de datos personales. *Centro de Información Oficial*. *Normativa y avisos legales del Uruguay*. Disponible en https://www.impo.com.uy/bases/leyes/18331-2008/34

(2011, 05 de enero). Ley No. 18.719. Presupuesto nacional de sueldos, gastos e inversiones. Ejercicio 2010 – 2014. *Centro de Información Oficial. Normativa y avisos legales del Uruguay*. Disponible en https://www.impo.com.uy/bases/leyes/18719-2010/149

(2011, 05 de enero). Ley No. 18.719. Presupuesto nacional de sueldos, gastos e inversiones. Ejercicio 2010 – 2014. *Centro de Información Oficial. Normativa y avisos legales del Uruguay*. Disponible en https://www.impo.com.uy/bases/leyes/18719-2010/

(2015, 30 de diciembre). Ley No. 19.355. Presupuesto nacional de sueldos, gastos e inversiones. Ejercicio 2015 – 2019. *Centro de Información Oficial. Normativa y avisos legales del Uruguay*. Disponible en https://www.impo.com.uy/bases/leyes/19355-2015/76

(2015, 30 de diciembre). Ley No. 19.355. Presupuesto nacional de sueldos, gastos e inversiones. Ejercicio 2015 – 2019. *Centro de Información Oficial. Normativa y avisos legales del Uruguay*. Disponible en https://www.impo.com.uy/bases/leyes/19355-2015/82

(2020, 30 de diciembre). Ley No. 19.924. Presupuesto nacional de sueldos, gastos e inversiones. Ejercicios 2020 – 2024. *Centro de Información Oficial. Normativa y avisos legales del Uruguay.* Disponible en https://www.impo.com.uy/bases/leyes/19924-2020

Naser, Alejandra. (Coord.). (2011). "Gobernanza digital e interoperabilidad gubernamental. Una guía para su implementación". *Documentos de proyectos*. (LC / TS. 2021 / 8°), Santiago. Comisión Económica para América Latina y el Caribe (CEPAL). Disponible en https://repositorio.cepal.org/server/api/core/bitstreams/6a12e389-3dcb-4cba-830a-99f038835423/content

(2023, 13 de diciembre). Nuevo convenio de cooperación técnica en identificación digital entre Uruguay y Paraguay. "Identificación oficial". *Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento.* Disponible y descarga en https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/noticias/nuevo-convenio-cooperacion-tecnica-identificacion-digital-entre-uruguay

(s. f.). 5° Plan de Acción Nacional de Gobierno Abierto 2021 – 2024. *AGESIC y Uruguay Presidencia*. Disponible en

https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/book/6187/download

(s. f.). Plan de Gobierno Digital 2025. *AGESIC y Uruguay Presidencia*. Disponible en https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/sites/agencia-gobierno-electronico-sociedad-informacion-conocimiento/files/2021-07/Plan%20de%20Gobierno%20Digital%202025_0.pdf

(s. f.). Plataforma de Interoperabilidad. *AGESIC y Uruguay Presidencia*. Disponible en https://centrodeconocimiento.agesic.gub.uy/web/ccio/plataforma-de-interoperabilidad

(2024, 17 de julio). "Proceso de revisión de la Estrategia de Inteligencia Artificial y de elaboración de la Estrategia Nacional de Datos. "Políticas y Gestión". *Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento.* Disponible en https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/politicas-y-gestion/proceso-revision-estrategia-inteligencia-artificial-elaboracion-estrategia

(2022, 03 de junio). Reglamento (UE) 2022 / 868 del Parlamento Europeo y del Consejo del 30 de mayo del 2022 relativo a la gobernanza europea de los datos y por el que se modifica el reglamento (UE) 2018 / 1724 (Reglamento de gobernanza de datos). Disponible en https://www.colegionotarial.org/es/legislaci%C3%B3n/reglamento-ue-2022868-del-parlamento-europeo-del-consejo-30-mayo-2022-relativo

(2012, 08 de junio). Resolución No. 23 / 021. *Unidad Reguladora y de Control de Datos Personales*. Disponible y descarga en https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-23021

(s. f.). Salud Digital. "Salud Digital". *Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento.* Disponible y descarga en https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/politicas-y-gestion/programas/es-saluduy

(s. f.). Servicios Digitales Transfronterizos. Programa para el fortalecimiento de las transacciones electrónicas transfronterizas en América Latina y el Caribe. "Bienes Públicos Regionales". *Reagealc*. Disponible en https://www.redgealc.org/site/assets/files/13516/anexo_1_-_servicios_digitales_transfronterizos_-_indice.pdf

Silva, Laura. (2022). Chats de Astesiano con importante empresario agropecuario argentino: ofrecía contactos en Inteligencia, drones, intervención de celulares con El Guardián y vehículos oficiales. *La diaria*. Disponible en https://ladiaria.com.uy/usuarios/entrar/?article=99907

UN. CEPAL y Comisión Europea. (2007). *Libro blanco de interoperabilidad de gobierno electrónico para América Latina y el Caribe*. Disponible en Libro blanco de interoperabilidad de gobierno electrónico para América Latina y el Caribe: versión 3.0 (cepal.org)

(2023, 12 de diciembre). Uruguay y Brasil firman convenio de cooperación técnica en identificación digital. "Identificación oficial". *Unidad de Certificación Electrónica*. Disponible y descarga en https://www.gub.uy/unidad-certificacion-electronica/comunicacion/noticias/uruguay-brasil-firman-convenio-cooperacion-tecnica-identificacion-digital

Anexo: Panorama legislativo

Esta sección fue elaborada de manera pro bono por el despacho de abogados **ECIJA Uruguay**, a partir de la conexión facilitada por TrustLaw, la red global legal de **Thomson Reuters Foundation**. Su objetivo es contextualizar el marco jurídico aplicable en materia de data sharing, proporcionando un fundamento legal que enriquece el análisis de este estudio de caso.

Descargo de responsabilidad: Los fines de este informe son puramente informativos. No se trata de una asesoría legal. Se recomienda a los lectores solicitar asistencia de abogados calificados para resolver sus asuntos específicos. Nuestra intención es que el contenido del informe sea correcto y actualizado al momento de su publicación. Sin embargo, no garantizamos su precisión o completitud, especialmente dado un posible cambio de circunstancias luego de la publicación. La Iniciativa Latinoamericana por los Datos Abiertos (ILDA), ECIJA Uruguay y la Thomson Reuters Foundation no son responsables por acciones, omisiones o daños que surjan como consecuencia de haber confiado en el informe o alguna inexactitud que el mismo contenga.

ECIJA Uruguay ha generosamente brindado asistencia pro bono a ILDA. Sin embargo, los contenidos de este informe no se entenderán como un reflejo de la postura de ECIJA Uruguay o de los abogados que contribuyeron con este trabajo.
Del mismo modo, la Thomson Reuters Foundation está encantada de haber apoyado a nuestro miembro de TrustLaw, ILDA mediante el trabajo desarrollado en este informe, lo que incluye la publicación y la conexión pro bono que posibilitó esta investigación legal. Sin embargo, de acuerdo con los principios Thomson Reuters Trust Principles sobre independencia y acciones libres de sesgos, no tomamos postura sobre los contenidos o las opiniones aquí expresadas.

A través de un cuestionario desarrollado conjuntamente, se solicitó a Ecija Uruguay responder a las siguientes preguntas sobre el marco normativo uruguayo:

1- ¿Cuál es el marco legal actual, incluyendo leyes, regulaciones, estrategias y políticas públicas, en torno al uso, recolección y procesamiento de datos en Uruguay?

A) Leyes y reglamentos.

i. En el artículo 72 de la Constitución Nacional[58] se encuentra reconocido el derecho a la protección de datos personales como un derecho inherente a la persona humana.

[58] https://www.impo.com.uy/bases/constitucion/1967-1967

ii. La Ley N°19.948[59] aprobó el Convenio N° 108 del Consejo de Europa para la Protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y su Protocolo Adicional.

iii. La Ley Nº 18.331[60] regula la Protección de Datos Personales y la Acción de Habeas Data, la cual es reglamentada por el Decreto Nº 664/2008 y 414/009.

iv. El Decreto 64/020[61] de La Ley N° 19.670 sobre Presupuesto, regula los artículos 37 a 40 sometida a la Ley N° 18.331, referente a protección de datos personales.

v. La Ley N° 18.381[62] reglamentada por el Decreto 232/010[63] regula el Derecho al Acceso a la Información Pública.

vi. La Ley de presupuesto N°19.355[64] y su Decreto reglamentario 54/017[65], regula el documento técnico llamado "Directrices Técnicas para la Apertura de Datos".

vii. El artículo 159 de la Ley N°18.719[66] junto con su Decreto reglamentario N° 178/013[67] sobre Presupuesto regula el "Intercambio de Información entre Entidades Públicas estatales o no Estatales".

B) Autoridad de la que emanaron tales regulaciones, año de promulgación y modificaciones o regulaciones posteriores.

i. La actual Constitución Nacional de Uruguay se promulgó en 1967, emana de un proceso de redacción llevado a cabo por una Asamblea Constituyente, elegida en 1966. Ha sido modificada en los años 1989, 1994, 1997 y 2004.

ii. La Ley N°19.948, fue emanada por el Poder Legislativo, y se promulgó en 2021 por el Poder Ejecutivo

iii. La Ley Nº 18.331 se promulgó en 2008 y fue emanada por el Poder Legislativo. El Decreto Reglamentario N° 414/009 fue promulgado en el año 2009 y emanado por el Poder Ejecutivo.

iv. La Ley N° 19.670 se promulgó en el año 2018, y emana del poder legislativo, mientras que el decreto reglamentario 64/020 fue en el año 2008, por el Poder Ejecutivo.

v. La Ley N° 18.381 se promulgó en el año 2008 y fue emanada por el Poder Legislativo. El decreto 232/010 se promulgó en el año 2008 y fue emanado por el Poder Ejecutivo.

vi. Ley N°19.355 fue promulgada en el año 2015, y emana del Poder Legislativo, y el decreto 54/017 fue promulgado en el año 2017, emanada del Poder Ejecutivo.

vii. La Ley N°18.719 fue promulgada en el año 2010 y emana del Poder Legislativo, mientras que el Decreto N° 178/013 fue promulgado en el año 2013, y emanado del Poder Ejecutivo.

[59] https://www.impo.com.uy/bases/leyes/19948-2021
[60] https://www.impo.com.uy/bases/leyes/18331-2008
[61] https://www.impo.com.uy/bases/decretos/64-2020
[62] https://www.impo.com.uy/bases/leyes/18381-2008
[63] https://www.impo.com.uy/bases/decretos/232-2010
[64] https://www.impo.com.uy/bases/leyes/19355-2015
[65] https://www.impo.com.uy/bases/decretos/54-2017
[66] https://www.impo.com.uy/bases/leyes/18719-2010
[67] https://www.impo.com.uy/bases/decretos/178-2013

C) Autoridades competentes.

En Uruguay la regulación y el control del uso recolección y procesamiento de datos se encuentran bajo la competencia de dos organismos principales:

1. **Unidad Reguladora y de Control de Datos Personales (URCDP)**[68] Fue creada por el artículo 31 de la Ley N° 18.331, el 11 de agosto de 2008. Es el órgano de control, que cuenta con autonomía técnica, encargado de velar por el cumplimiento de la Ley N° 18.331 de Protección de Datos Personales y Acción de Habeas Data. Entre sus cometidos y potestades, entre otros, se puede mencionar: Dicta las normas y reglamentaciones que se deben observar en el desarrollo de las actividades comprendidas por la ley. Realiza un censo de las bases de datos alcanzadas por la ley y mantiene el registro permanente de los mismos. Supervisa el cumplimiento de la ley por parte de las personas físicas o jurídicas públicas o privadas que traten datos personales Controlar la observancia del régimen legal, en particular las normas sobre legalidad, integridad, veracidad, proporcionalidad y seguridad de datos, por parte de los sujetos alcanzados, pudiendo a tales efectos realizar las actuaciones de fiscalización e inspección pertinentes.Recibe y resuelve denuncias presentadas por los titulares de datos investigando posibles violaciones a sus derechos y adoptando las medidas correspondientes. Brinda orientación a ciudadanos y organizaciones sobre sus derechos y obligaciones en materia de protección de datos. Difunde la cultura de la protección de datos y realiza campañas de concientización sobre la importancia de salvaguardar la privacidad. Su competencia se extiende a todos los sectores tanto público como privado que traten datos personales.

Está dirigido por un Consejo integrado por tres miembros: el Director Ejecutivo de AGESIC y dos miembros designados por el Poder Ejecutivo entre personas que por sus antecedentes personales, profesionales y de conocimiento en la materia aseguran independencia de criterio, eficiencia, objetividad e imparcialidad en el desempeño de su cargo de acuerdo a lo regulado en el artículo 31 de la Ley Nº 18.331. A excepción del Director Ejecutivo de AGESIC, los miembros durarán en sus cargos cuatro años, pudiendo ser designados nuevamente.

2. **Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (AGESIC)**[69] Fue creada por el art. 72 de la Ley N° 17.930 en diciembre de 2005. Es una unidad ejecutora con autonomía técnica, dependiente de Presidencia de la República Oriental del Uruguay. Tiene un enfoque más amplio abarcando la gestión de datos en el marco del gobierno electrónico y la sociedad de la información. Impulsa la transformación digital del Estado promoviendo la utilización de las tecnologías de la información y la comunicación en la gestión pública. Fomenta la transparencia y el acceso a la información pública asegurando que los datos gubernamentales sean accesibles y comprensibles para la ciudadanía. Elabora políticas públicas en materia de tecnologías de la información y la comunicación incluyendo aquellas relacionadas con la gestión de datos. Promueve la seguridad de los sistemas informáticos del Estado y la protección de los datos ante posibles ciberataques. Su competencia se

[68] https://www.gub.uy/unidad-reguladora-control-datos-personales/
[69] https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/

centra principalmente en el sector público, aunque también tiene incidencia en el sector privado a través de sus políticas y estándares.

Su ley de creación estableció un Consejo Directivo Honorario (CDH), encargado de diseñar sus líneas de acción, evaluar su desempeño y los resultados obtenidos, asistido por otros tres consejos honorarios: Consejo para la Sociedad de la Información, Consejo Asesor de Empresas y Consejo Asesor de Informática Pública.

El Decreto 184/015 fija la misión, objetivos y cometidos atribuidos legalmente a la AGESIC. Esta agencia busca innovar y hacer más eficientes las formas en que las personas se relacionan con la administración pública, incorporando tecnologías digitales y mejores formas de trabajar, poniendo el foco en las personas.

Información complementaria:

Datos Abiertos en Uruguay

El artículo 82[70] sobre Datos Abiertos de la Ley N° 19.355 establece que las entidades públicas deberán, como mínimo, publicar en formato abierto la información preceptuada por el artículo 5°[71] de la Ley de Acceso a la Información Pública. También podrán publicar como datos abiertos aquellos que considere útiles para algún sector particular de la sociedad, aunque no estén comprendidos por el referido artículo.

Su Decreto Reglamentario Nº 54/017 fija las directrices técnicas para la publicación de datos y está orientado al personal técnico informático.

El artículo 159[72] de la Ley N°18.719 junto con su Decreto reglamentario N° 178/013 se basan en mejorar el intercambio de información y optimizar la prestación de servicios, alineándose con principios de buena gobernanza y transparencia.

Uruguay ha establecido un marco normativo sólido para el uso, recolección y procesamiento de datos en el sector público. Los datos abiertos son un recurso valioso para fortalecer la democracia, mejorar la gobernanza y fomentar el desarrollo sostenible.

Los datos abiertos permiten a los ciudadanos acceder a información sobre las actividades del gobierno, permitiendo un diálogo informado entre el gobierno y la sociedad. En Uruguay hay bastantes, y existe un Portal de Datos Abiertos[73] que facilita la tarea de encontrarlos. Los datos del sector público de libre disposición suelen incluir información que está disponible para el público y que no está sujeta a restricciones. El Portal ofrece acceso a una variedad de conjuntos de datos como información sobre presupuesto e ingresos públicos, informes de políticas públicas, documentos que analizan la implementación y el impacto de políticas gubernamentales, datos de contrataciones públicas y ambientales.

---

[70] https://www.impo.com.uy/bases/leyes/19355-2015/82
[71] https://www.impo.com.uy/bases/leyes/18381-2008/5
[72] https://www.impo.com.uy/bases/leyes/18719-2010/159#:~:text=Cuando%20proceda%20el%20intercambio%20de,competente%20y%20formalizar%20un%20acuerdo.
[73] https://ckan.montevideo.gub.uy

A continuación se describen algunos ejemplos de datos abiertos en el sector público: El Instituto Nacional de Estadística (INE)[74] publica datos estadísticos sobre la población, economía y sociedad, y se utilizan para investigaciones y políticas públicas. El Ministerio de Salud Pública[75] comparte datos incluyendo estadísticas de enfermedades, vacunación y servicios de salud. La Unidad Nacional de Seguridad Vial (UNASEV)[76] proporciona datos de transporte, tanto accidentes de tránsito como estadísticas de movilidad y seguridad vial en el país. El Consejo de Educación Inicial y Primaria (CEIP)[77] y otras instituciones educativas publican información sobre matrícula, rendimiento académico y otros aspectos del sistema educativo.

Catálogo Nacional de datos abiertos:

Es una herramienta que facilita el acceso a datos abiertos, presentándolos de manera ordenada por categorías, organizaciones y etiquetas entre otras opciones[78]. En cada sección, se indicará si reviste carácter informativo u obligatorio. Las secciones informativas, proveen contexto y definiciones para facilitar la comprensión del documento y las secciones obligatorias, prescriben directrices que deben ser cumplidas por los organismos públicos establecidos en el artículo 82 de la Ley Nº 19.355 mencionada anteriormente.

2- ¿Existen leyes, reglamentos o disposiciones específicas para compartir o intercambiar datos entre organismos o agencias gubernamentales?

A) Ley y reglamentos

Si bien no existe una normativa específica en Uruguay que regule de manera exhaustiva el intercambio de datos entre organismos gubernamentales, diversos cuerpos legales y disposiciones inciden en esta práctica. La Ley N° 18.331 de Protección de Datos Personales establece los principios fundamentales para el tratamiento de datos, incluyendo su transferencia entre entidades públicas. La Ley N° 18.381 de Acceso a la Información Pública garantiza el derecho ciudadano a acceder a la información gubernamental, lo que indirectamente fomenta el intercambio de datos entre organismos. Asimismo, el Decreto N° 134/021 y la Estrategia Nacional de Ciberseguridad establecen lineamientos generales sobre seguridad de la información y colaboración interinstitucional, impactando en las prácticas de intercambio de datos. A pesar de esta diversidad normativa, la falta de una ley marco específica dificulta la armonización y la aplicación uniforme de los principios establecidos.

B) Ámbito de aplicación dentro del sector público.

El ámbito de aplicación del intercambio de datos en el sector público, tal cual está planteado hoy en día en la legislación, abarca todas las interacciones entre los diferentes organismos estatales que involucran la transferencia de información. Esto significa

[74] https://www3.ine.gub.uy/rraa/contacto.html
[75] https://www.gub.uy/ministerio-salud-publica/
[76] https://www.gub.uy/unidad-nacional-seguridad-vial/

[77] https://uruguay.fandom.com/es/wiki/Consejo_de_Educación_Inicial_y_Primaria#:~:text=El%20Consejo%20de%20Educación%20Inicial,al%20ámbito%20de%20su%20competencia.
[78] https://catalogodatos.gub.uy/

que cualquier entidad gubernamental, desde ministerios hasta municipalidades, que necesite compartir datos con otra, está sujeta a las normas y regulaciones establecidas para este fin.

En general, existe una alineación entre las diferentes normas y políticas que regulan el intercambio de datos en el sector público uruguayo. Sin embargo, es importante destacar algunos puntos clave:

- Complementariedad: Las distintas normas se complementan entre sí, estableciendo un marco regulatorio integral. Por ejemplo, la Ley N° 18.331 establece los principios generales para la protección de datos, mientras que la Ley N° 18.381 garantiza el acceso a la información pública, creando un equilibrio entre la protección de datos y la transparencia.
- Desafíos de implementación: A pesar de la existencia de un marco normativo sólido, la implementación efectiva de estas normas presenta desafíos, como la necesidad de inversión en tecnología, capacitación del personal y la coordinación entre diferentes organismos.
- Evolución constante: El marco normativo está en constante evolución, adaptándose a los cambios tecnológicos y a las nuevas necesidades de la administración pública. Esto puede generar cierta complejidad y la necesidad de actualizaciones periódicas.

C) Proceso de articulación para compartir datos entre los órganos o agencias nacionales y los órganos o agencias locales.

Si bien no existe un procedimiento único y estandarizado para el intercambio de datos entre agencias gubernamentales y particulares en Uruguay, sí se cuenta con un sólido marco normativo y político que establece los principios fundamentales y las reglas generales para este tipo de transacciones. Este marco está compuesto por una variedad de leyes, decretos, resoluciones y políticas públicas diseñadas para garantizar la seguridad de la información, proteger la privacidad de las personas, promover la transparencia en los procesos gubernamentales y asegurar la eficiencia en la gestión de los datos.

La Ley de Protección de Datos Personales (Ley N° 18.331) constituye un pilar fundamental en este marco, estableciendo los principios y las reglas para el tratamiento de datos personales. Asimismo, la Ley de Acceso a la Información Pública (Ley N° 18.381) garantiza el derecho de los ciudadanos a acceder a la información pública y promueve la transparencia en la gestión gubernamental. Adicionalmente, diversas normas sectoriales y acuerdos interinstitucionales complementan este marco, estableciendo requisitos específicos para el intercambio de datos en diferentes ámbitos.

Este entramado legal y político busca establecer un equilibrio entre la necesidad de compartir información para mejorar la toma de decisiones y la prestación de servicios públicos, y la protección de los derechos individuales. A través de este marco, se establecen los mecanismos para garantizar que los datos sean tratados de manera lícita, leal y

transparente, y que se adopten las medidas técnicas y organizativas necesarias para protegerlos de cualquier tratamiento no autorizado o ilícito.

Información Complementaria:

Se establece la confidencialidad en el procedimiento para la transmisión de datos, asegurando la protección de la información y definiendo las responsabilidades de las entidades en el manejo de dicha información. Se establece que AGESIC pondrá a disposición de las Entidades Públicas una Plataforma de Interoperabilidad (IPD)[79] donde éstas podrán realizar intercambios de información en soporte electrónico, de forma segura y confiable. Su objetivo es facilitar y promover la implementación de servicios de Gobierno Digital, estableciendo pautas para la interoperabilidad de sistemas, facilitando la recolección y uso eficiente de datos.

El artículo 78 de la Ley Nº 20.212 implementó una Estrategia Nacional de Ciberseguridad, y otra de digitalización llamada "Agenda Uruguay Digital 2025"[80] que incluye el uso de nuevas tecnologías como de plataformas interoperables para el intercambio de datos abiertos entre organismos. Esta iniciativa busca fortalecer el uso de tecnologías de la información (TICs) en el Estado para mejorar la calidad de los servicios públicos y promover el uso de datos abiertos. En cuanto a la Estrategia Nacional de Ciberseguridad, aboga por proteger la información manejada por el Estado, mediante la implementación de protocolos de seguridad frente a posibles ciberataques o accesos no autorizados. El fin es prevenir y mitigar riesgos en el uso de tecnologías. La política digital del país, a través de la Agenda Uruguay Digital 2025, busca impulsar la transparencia en la gestión pública a través de iniciativas de datos abiertos.

La interoperabilidad facilita la eficiencia en el sector público, permitiendo que las instituciones públicas uruguayas compartan información en tiempo real, evitando duplicidades, agilizando los trámites administrativos y mejorando la prestación de servicios de los ciudadanos al interactuar con el Estado.

3- **Acuerdos bilaterales o multilaterales vigentes para el intercambio de datos entre estados**

Uruguay ha firmado acuerdos bilaterales y multilaterales que prevén el intercambio de datos entre Estados, en particular en áreas como la protección de datos personales, la cooperación judicial, la seguridad y la fiscalidad.

79 https://centrodeconocimiento.agesic.gub.uy/documents/80442/88295/PGE-Plataforma-Interoperabilidad-Presentación-Técnica-v01.00.pdf/0ad91823-cd02-7edf-50c7-432c2838c3a7?version=1.0

80 https://www.gub.uy/uruguay-digital/sites/uruguay-digital/files/documentos/publicaciones/Documento%20AUD%202025.pdf

Uruguay se adhiere a los estándares internacionales de la Organización para la Cooperación y el Desarrollo Económico (OCDE), como el Estándar Común de Reporte (CRS), que establece un marco para el intercambio automático de información financiera entre países.[81]

También es parte de Acuerdos sobre Intercambio de Información Tributaria con Estados Unidos[82] y países de la Unión Europea, con el objetivo de combatir la evasión fiscal, los cuales permiten el intercambio de información financiera entre las autoridades fiscales de los Estados firmantes, bajo estrictas normas de confidencialidad y protección de datos.

En el ámbito de Salud se firmaron Acuerdos multilaterales para el intercambio de datos epidemiológicos y sanitarios, particularmente en el contexto de la Organización Panamericana de la Salud (OPS)[83] y la Organización Mundial de la Salud (OMS). Estos Acuerdos facilitan el flujo de información sobre enfermedades infecciosas y emergencias sanitarias, siempre bajo normas que protegen los datos personales sensibles.

En el marco del Mercosur, participó en varios Acuerdos como el Intercambio de Información Tributaria y Método para evitar la doble imposición en el año 2012 [84]

Participó en Acuerdos sobre Cooperación en Seguridad y Justicia, relacionado al intercambio de datos de investigaciones criminales, inmigración y seguridad fronteriza, en Acuerdos de Cooperación Judicial y Penal, incluyendo Tratados de Asistencia Jurídica Mutua y Extradición con países de América Latina y Europa[85]

4- Compromiso con los principios internacionales relacionados con el intercambio de datos, como el Marco Europeo de Interoperabilidad

Uruguay ha demostrado un compromiso creciente con la modernización de sus sistemas gubernamentales y la promoción de la interoperabilidad de los datos. Aunque no ha adoptado formalmente el Marco Europeo de Interoperabilidad, ha implementado diversas iniciativas que se alinean con sus principios.

Avances de Uruguay en el Intercambio de Datos

Convenios de Interoperabilidad: El gobierno uruguayo ha suscrito convenios marco de interoperabilidad entre diferentes instituciones, como el Poder Judicial, el Ministerio del Interior y la fiscalía general de la Nación. Estos acuerdos buscan mejorar la comunicación entre sistemas y facilitar la coordinación interinstitucional.

Plataforma Uruguay.uy: Esta plataforma digital integra diversos servicios gubernamentales, permitiendo a los ciudadanos acceder a trámites y gestiones de manera más eficiente. Si

---

81 https://www.gub.uy/ministerio-relaciones-exteriores/comunicacion/comunicados/uruguay-adhiere-recomendacion-ocde-sobre-inteligencia-artificial

82 https://www.ambito.com/uruguay/se-aprobo-la-ley-intercambio-informacion-financiera-estados-unidos-n6063690

83 https://www.paho.org/sites/default/files/cooperacion-tecnica-ops-uruguay-2022_0.pdf

84 https://www.argentina.gob.ar/normativa/nacional/ley-26758-201049

85 https://www.mercosur.int/ciudadania/estatuto-ciudadania-mercosur/3-cooperacion-judicial-y-consular/

bien no es una adopción directa del Marco Europeo, representa un paso importante hacia la interoperabilidad de los sistemas gubernamentales.

Participación en Foros Internacionales: Uruguay participa activamente en foros internacionales sobre gobierno electrónico y transformación digital, lo que le permite estar al tanto de las últimas tendencias y buenas prácticas en materia de intercambio de datos.

El Reglamento General de Protección de Datos (RGPD)[86] de la Unión Europea ha influido en la legislación uruguaya dado que la Unión Europea ha reconocido a Uruguay como un territorio que garantiza un nivel adecuado de protección de datos personales.[87]

Por otro lado, y atendiendo a otros mecanismos de medición internacionales, según el Barómetro Regional de Datos Abiertos (implementado por ILDA en América Latina)[88] el cual mide tres dimensiones: la preparación referida a la apertura de datos de gobierno; la implementación del conjunto de datos; y su impacto en lo político, social y económico, la posición actual de Uruguay es la siguiente:

- Puesto 64 a nivel mundial.
- Puesto 1 en América del Sur.

5- Jurisprudencia y otra información relevante.

En Uruguay, el concepto de "data sharing" o "compartición de datos" está comenzando a ganar relevancia, especialmente a partir del creciente uso de tecnologías y la importancia de la protección de datos personales. En cuanto a la doctrina y jurisprudencia sobre este tema, es un área en desarrollo influenciada por el marco normativo de protección de datos personales, que tiene como principal fuente la ya referida Ley N.º 18.331 (Ley de Protección de Datos Personales y Acción de Habeas Data), y su reglamentación, que sigue los principios de privacidad y protección de datos establecidos por la Regulación General de Protección de Datos de la Unión Europea (GDPR), en lo que respecta a derechos fundamentales.

Doctrina:

La doctrina uruguaya en relación con el data sharing se ha enfocado principalmente en el análisis de la Ley N.º 18.331, y su compatibilidad con estándares internacionales como el GDPR. Existen estudios y publicaciones que destacan la necesidad de una regulación más detallada sobre la transferencia y compartición de datos entre empresas, entidades públicas, y a nivel transfronterizo. Algunos puntos tratados en la doctrina son:

- Los límites del consentimiento del titular de los datos para su transferencia.
- La responsabilidad de los responsables y encargados del tratamiento de los datos.
- El rol de la Agencia de Gobierno Electrónico y Sociedad de la Información (AGESIC) como autoridad reguladora.

Jurisprudencia:

[86] https://www.boe.es/doue/2016/119/L00001-00088.pdf

[87] https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/noticias/comision-europea-ratifica-nivel-adecuado-uruguay-para-proteccion-datos-0

[88] https://idatosabiertos.org/proyectos/barometro-regional-de-datos-abiertos/

En cuanto a la jurisprudencia, si bien no hay una gran cantidad de fallos judiciales específicamente sobre data sharing, algunos casos han abordado temas que entendemos estan relacionados, y entre los cuales encontramos:
Alcance de la Ley de Protección de Datos Personales: Se han analizado casos que han delimitado el alcance de la ley y los derechos de los titulares de los datos.

- Consentimiento informado: La jurisprudencia ha establecido criterios para determinar cuándo el consentimiento otorgado para el tratamiento de datos personales es válido y eficaz. (Ej. Sentencia definitiva Nro 128/2017, Tribunal de Apelaciones en lo Civil de 7° Turno).
- Derechos de los titulares de los datos: La jurisprudencia ha reconocido y protegido los derechos de los titulares de los datos, como el derecho de acceso, rectificación, supresión y oposición al tratamiento de sus datos. (Ej. Sentencia definitiva Nro 109/2023, Tribunal Apelaciones en lo Civil 1º Turno).
- Responsabilidad de los responsables del tratamiento: Se han establecido criterios para determinar la responsabilidad de las entidades que tratan datos personales y las consecuencias de las infracciones a la ley. (Ej. Sentencia definitiva Nro 43/2018, Tribunal de Apelaciones en lo Civil de 6° Turno).

Por otro lado, si bien no es jurisprudencia en el sentido técnico de la palabra, AGESIC ha emitido guías y recomendaciones que interpretan la normativa en situaciones de tratamiento de datos, como la transferencia internacional de datos o el intercambio de información entre organismos públicos y privados, temas que se vinculan con el data sharing, y que poco a poco son tenidos en cuenta por los jueces a la hora de realizar los fallos.

Si bien Uruguay tiene una legislación avanzada en protección de datos, aún falta mayor desarrollo en cuanto a regulaciones específicas para el data sharing, por lo que la doctrina y jurisprudencia seguirán evolucionando en este tema.