REUTERS/Mike Blake

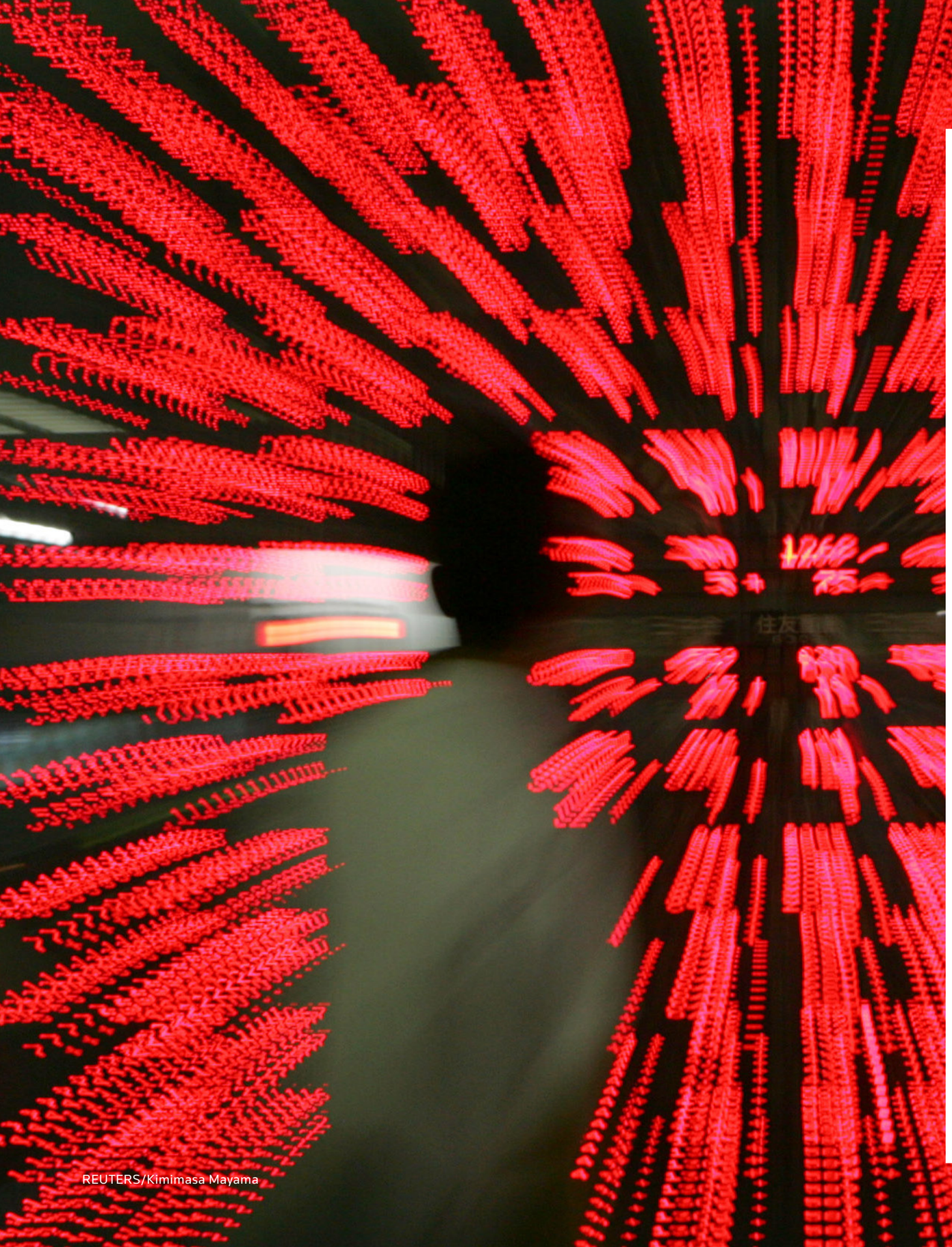
DATA PROTECTION: A LEGAL COMPARATIVE STUDY OF 9 COUNTRIES

PROTECCIÓN DE DATOS: UN ANÁLISIS COMPARATIVO EN 9 PAÍSES

DATA PROTECTION: A LEGAL COMPARATIVE STUDY OF 9 COUNTRIES

PROTECCIÓN DE DATOS: UN ANÁLISIS COMPARATIVO EN 9 PAÍSES

THOMSON REUTERS FOUNDATION
TrustLaw
DEMOCRACIA EN RED



REUTERS/Kimimasa Mayama

ACKNOWLEDGEMENTS
AGRADECIMIENTOS

Thomson Reuters Foundation and Democracia en Red are extremely grateful to the participating law firms for donating their time and expertise to this project. The TrustLaw team is especially grateful to Gomez Pinzón for coordinating this project.

Law firms

- Bruchou Fernandez Madero & Lombardi (Argentina)
- KLA Advogados (Brazil)
- Gomez-Pinzón Abogados (Colombia)
- Dentons Canada LLP (Canada)
- ObradorDigital Legal (Chile)
- Hogan Lovells International LLP (Spain)
- DLA Piper Paris (France)
- Goebel & Muthspiel (Mexico)
- Cervieri Monsuarez (Uruguay)

Researchers

- Franco Raffinetti (Argentina)
- Ana Carolina Cesar (Brazil)
- Luca Lucarini (Canada)
- María José Arancibia and Claudio Villarroel (Chile)
- Andrés Fernández de Castro Muñoz and Andrés Meza Scarpetta (Colombia)
- Santiago de Ampuero, Víctor Mella, Clara Lázaro and Graciela Martín (Spain)
- Denise LEBEAU-MARIANNA, Partner, Divya SHANMUGATHAS, Associate (France)
- Sahoori Rivera (Mexico)
- Lucia Cantera, Viviana Cervieri and Jorge Achard (Uruguay)

Desde Thomson Reuters Foundation y Democracia en Red agradecemos a todas las firmas participantes por donar su tiempo para la elaboración de este valioso documento de legislación comparada. El equipo TrustLaw está especialmente agradecido con Gomez Pinzón por haber coordinado este proyecto.

Firmas

- Bruchou Fernandez Madero & Lombardi (Argentina)
- KLA Advogados (Brasil)
- Gomez-Pinzón Abogados (Colombia)
- Dentons Canada LLP (Canada)
- ObradorDigital Legal (Chile)
- Hogan Lovells International LLP (España)
- DLA Piper Paris (Francia)
- Goebel & Muthspiel (Mexico)
- Cervieri Monsuarez (Uruguay)

Investigadores

- Franco Raffinetti (Argentina)
- Ana Carolina Cesar (Brasil)
- Luca Lucarini (Canada)
- María José Arancibia y Claudio Villarroel (Chile)
- Andrés Fernández de Castro Muñoz y Andrés Meza Scarpetta (Colombia)
- Santiago de Ampuero, Víctor Mella, Clara Lázaro y Graciela Martín (España)
- Denise LEBEAU-MARIANNA, Socia, Divya SHANMUGATHAS, Abogada (Francia)
- Sahoori Rivera (Mexico)
- Lucia Cantera, Viviana Cervieri y Jorge Achard (Uruguay)

DISCLAIMER OF LIABILITY
DESCARGO DE RESPONSABILIDAD

This report is offered for information purposes only. It is not legal advice. Readers are urged to seek advice from qualified legal counsel in relation to their specific circumstances.

We intend the report's contents to be correct and up to date at the time of publication, but we do not guarantee their accuracy or completeness, particularly as circumstances may change after publication. Democracia en Red, Gomez Pinzón; Cervieri Monsuarez; Bruchou, Fernandez Madero & Lombardi; ObradorDigital Legal; KLA Advogados; Goebel & Muthspiel; Hogan Lovells International LLP; Dentons Canada LLP; DLA Piper Paris and the Thomson Reuters Foundation, accept no liability or responsibility for actions taken or not taken or any losses arising from reliance on this report or any inaccuracies herein.

Gomez Pinzón; Cervieri Monsuarez; Bruchou, Fernandez Madero & Lombardi; ObradorDigital Legal; KLA Advogados; Goebel & Muthspiel; Hogan Lovells International LLP; Dentons Canada LLP; and DLA Piper Paris generously provided pro bono research to Democracia en Red. However, the contents of this report should not be taken to reflect the views of Gomez Pinzón; Cervieri Monsuarez; Bruchou, Fernandez Madero & Lombardi; ObradorDigital Legal; KLA Advogados; Goebel & Muthspiel; Hogan Lovells International LLP; Dentons Canada LLP; DLA Piper Paris or the lawyers who contributed.

Similarly, Thomson Reuters Foundation is proud to support our TrustLaw member Democracia en Red with their work on this report, including this publication and the pro bono connection that made the legal research possible. However, in accordance with the Thomson Reuters Trust Principles of independence and freedom from bias, we do not take a position on the contents of, or views expressed in, this report.

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. Democracia en Red; Gomez Pinzón; Cervieri Monsuarez; Bruchou, Fernandez Madero & Lombardi; ObradorDigital Legal; KLA Advogados; Goebel & Muthspiel; Hogan Lovells International LLP; Dentons Canada LLP; DLA Piper Paris y 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.

Gomez Pinzón; Cervieri Monsuarez; Bruchou, Fernandez Madero & Lombardi; ObradorDigital Legal; KLA Advogados; Goebel & Muthspiel; Hogan Lovells International LLP; Dentons Canada LLP; DLA Pipe Paris han generosamente brindado asistencia pro bono a Democracia en Red. Sin embargo, los contenidos de este informe no se entenderán como un reflejo de la postura de Gomez Pinzón; Cervieri Monsuarez; Bruchou, Fernandez Madero & Lombardi; ObradorDigital Legal; KLA Advogados; Goebel & Muthspiel; Hogan Lovells International LLP; Dentons Canada LLP; DLA Piper Paris o de los abogados que contribuyeron con este trabajo.

Del mismo modo, Thomson Reuters Foundation está encantada de haber apoyado a nuestro miembro TrustLaw Democracia en Red 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 libre de sesgos, no tomamos postura sobre los contenidos o las opiniones aquí expresadas.

REUTERS/Edgard Garrido

ABOUT DEMOCRACIA EN RED
SOBRE DEMOCRACIA EN RED

DEMOCRACIA EN RED

Democracia en Red is a non-governmental organisation that uses technology to bring democracy to the 21st century.

Over the last 7 years, it has created and applied strategies to open up public institutions through the design, development, and implementation of digital tools that promote democratic participation. It conducts ssessments on behalf of governments and civil society organisations throughout Latin America to reduce the gap between representatives and constituents and to create public policy with a greater impact. It also stimulates cultural change through communication campaigns and educational tools that promote new habits in the digital era.

Democracia en red es una organización no gubernamental que usa la tecnología para adaptar la democracia al siglo XXI.

Desde hace 7 años genera y aplica estrategias para abrir instituciones públicas a través del diseño, desarrollo e implementación de herramientas digitales que promueven la participación democrática, realiza asesorías para Gobiernos y organizaciones de todo LATAM para reducir la brecha entre representantes y representados y generar políticas públicas con mayor impacto e impulsa el cambio cultural en forma de campañas de comunicación y herramientas educativas que promuevan nuevos hábitos en la era digital.

REUTERS/Daniel Acker

ABOUT TRF / TRUSTLAW
SOBRE TRF / TRUSTLAW

THOMSON REUTERS FOUNDATION

TrustLaw

The Thomson Reuters Foundation is the corporate foundation of Thomson Reuters, the global news and information services company. We work to advance media freedom, raise awareness of human rights issues, and foster more inclusive economies. Through news, media development, free legal assistance and convening initiatives, the Foundation combines its unique services to drive systemic change.

TrustLaw is the Thomson Reuters Foundation's global pro bono legal programme, connecting the best law firms and corporate legal teams around the world with high-impact NGOs and social enterprises working to create social and environmental change. We produce groundbreaking legal research and offer innovative training courses worldwide.

Thomson Reuters Foundation es la fundación corporativa de Thomson Reuters, la compañía global de servicios de noticias e información. Trabajamos para promover la libertad de los medios de comunicación, crear conciencia sobre las cuestiones de derechos humanos y fomentar economías más inclusivas. Por medio de noticias, desarrollo de medios de comunicación, asistencia jurídica gratuita e iniciativas de convocatoria, la Fundación combina sus servicios únicos para impulsar el cambio sistémico.

TrustLaw es el programa legal pro bono global de la Fundación Thomson Reuters, que conecta los mejores despachos de abogados y equipos legales corporativos de todo el mundo con ONGs de alto impacto y empresas sociales que trabajan para crear cambios sociales y ambientales. Producimos investigaciones jurídicas innovadoras y ofrecemos cursos de formación innovadores en todo el mundo.

REUTERS/Kacper Pempel

TABLE OF CONTENTS
ÍNDICE

REUTERS/Rafael Marchante

REUTERS/Russell Boyce

INTRODUCTION
INTRODUCCIÓN

1

Digital assets are increasingly transforming the global economy. Data is the fuel used by large companies to create consumer categories and "profile" consumers for targeted, effective and accurate advertising.

In Argentina, the **Data Protection Law** was enacted in 2000: four years since the surge in popularity of Facebook and seven years since the surge in popularity of Twitter. Initially this law was innovative, but now it is no longer a protective mechanism.

The world has changed, and the law does not reflect those changes. Legislation protecting personal data in Argentina is outdated, centralist and lacks a gender perspective.

In Argentina, **the enforcement authority depends only on the Executive Branch** and, since it was created two decades ago, **protection of sensitive data of women who report gender-based violence is not specifically provided for.**

Democracia en Red wants current legislation to meet the needs the country is facing today. TrustLaw, the Thomson Reuters Foundation's global pro bono service, connected Democracia en Red with nine law firms to produce legal research on legislation on data protection applicable to the public and private sectors locally. This in-depth comparative study covers legislation from Argentina, France, Chile, Colombia, Canada (with a focus on Quebec), Brazil, Spain, Mexico and Uruguay. This report addresses five aspects related to current legislation: main laws and regulations, gender perspective, enforcement authority, government access to personal data and implicit consent.

The full report answers eight questions.

La economía global se basa, cada vez más, en activos digitales. Los datos son el combustible utilizado por enormes empresas para incluirnos en categorías de consumo y para "perfilarnos" hacia publicidad dirigida, efectiva y precisa.

En Argentina **La ley de Protección de Datos Personales** se aprobó en el año 2000: cuatro años antes del estallido de Facebook y siete años antes de la de Twitter. En su momento la ley fue innovadora pero hoy en día, ya no protege lo que buscaba proteger.

El mundo cambió y la ley quedó atrás. La legislación que protege nuestros datos hoy es incompleta, centralista y sin perspectiva de género.

Así, **su órgano de aplicación depende sólo del poder ejecutivo,** y al haber sido redactada en otra época, **no contempla específicamente la protección de los datos sensibles de mujeres denunciantes de violencia machista**.

Democracia en Red busca que la legislación pueda satisfacer las necesidades que el país enfrenta actualmente. Así, TrustLaw, el programa global pro bono de la Thomson Reuters Foundation, conectó a Democracia en Red con nueve firmas legales para llevar a cabo una investigación de normativa sobre protección de datos aplicable a los sectores público y privado a nivel local. Este estudio de derecho comparado analiza normativa de Argentina, Francia, Chile, Colombia, Canadá (con especial foco en Quebec), Brasil, España, México y Uruguay. Además, se exponen cinco aspectos vinculados a la legislación vigente: principales leyes y reglamentos, la perspectiva de género, la autoridad de aplicación, el acceso del estado a los datos personales y la figura del consentimiento tácito.

La totalidad de la investigación contempla ocho preguntas.

SUMMARY OF FINDINGS
RESUMEN DE LOS RESULTADOS

2

Among the countries covered in this study, Argentina and Chile have the oldest data protection laws, while Spain and France – with the application of the General Data Protection Regulation (GDPR) – as well as Brazil – with the General Data Protection Law (LGPD) entering into force in September 2020 – have the most modern legislation, adapted to the global context and the technological advances of recent years.

On gender perspective, none of the data protection laws analyzed in this report has a gender perspective or specific provisions in this regard. The Spanish legislation makes an isolated reference on this topic when regulating notices and publications of administrative acts.

Regarding data protection authorities, the Argentine enforcing authority – the Agency for Access to Public Information (AAIP) – is an autarchic entity that operates independently within the Office of the Chief of Cabinet of Ministers. This is similar in: (i) Colombia with the Superintendence of Industry and Commerce (SIC); (ii) France with the *Commission nationale de l'informatique et des libertés* (CNIL); (iii) Spain with the Spanish Data Protection Agency (AEPD); (iv) Mexico with the National Institute for Access to Public Information and Protection of Personal Data (INAI); and (v) Uruguay with the Agency for the Development of Electronic Government and Information Society and Knowledge (AGESIC). In contrast, the Brazilian authority, the National Data Protection Authority (ANPD), is an entity of the federal public administration, reporting to the Presidency, and so it is not an independent body of the executive branch. Similarly, in Canada, the Office of the Privacy Commissioner of Canada (OPC), overseeing compliance with the federal Personal Information Protection and Electronic Documents Act (PIPEDA), is independent of the government, but reports directly to Parliament. As for the Privacy Commission of Quebec, its members are appointed, on the proposal of the Premier, by a resolution of the legislature. Finally, in Chile there is no enforcing authority responsible for ensuring data protection.

As regards State access to personal data, under most regulations, the State could be exempted from requiring the consent of the data subject for the collection/transfer of their data when it comes to performing the State's own duties and/or in states of "emergency". In France, some purposes and activities related to data processing are subject to stricter requirements, especially when such processing is done on behalf of the State. Also relevant is the decision made by the Supreme Federal Court of Brazil during the COVID-19 pandemic, highlighting the lack of reasons provided by the Brazilian Institute of Geography and Statistics for data processing purposes.

Finally, most laws analyzed in this report require express consent of the data subject for data processing. However, Canada – in its different regulations – and Mexico allow implied consent in some cases.

Entre los países que forman parte de la presente investigación, se destaca que Argentina y Chile tienen las leyes más antiguas en materia de protección de datos personales. España y Francia por la aplicación del Reglamento General de Protección de Datos (RGPD), y Brasil con la entrada en vigencia de la Ley General de Protección de Datos (LGPD) en el mes de septiembre de 2020, receptan las legislaciones más modernas, aggiornadas al contexto global y a los avances tecnológicos de los últimos años.

En lo que respecta a la perspectiva de género, ninguna de las normas de datos personales analizadas cuenta con una perspectiva de género ni previsiones específicas en este sentido. La norma española estipula una referencia aislada sobre este tópico al tratar la notificación y publicación de actos administrativos.

Por otra parte, a partir del año 2017, la autoridad de aplicación argentina en materia de datos personales, la Agencia de Acceso a la Información Pública (AAIP), pasó a ser un ente autárquico con autonomía funcional, en el ámbito de la Jefatura de Gabinete de Ministros de la Nación. Situación con varios puntos en común se da en los siguientes países: (i) Colombia con la Superintendencia de Industria y Comercio (SIC); (ii) Francia con la *Commission nationale de l'informatique et des libertés* (CNIL); (iii) España con la Agencia Española de Protección de Datos (AEPD); (iv) México con el Instituto Nacional de Acceso a la Información Pública y Protección de Datos Personales (INAI); y (v) Uruguay con la Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (AGESIC). En contraposición, la autoridad brasileña, la Autoridad Nacional de Protección de Datos (ANPD), es una entidad de la administración pública federal, perteneciente a la Presidencia, sin independencia del poder ejecutivo. Asimismo, en el caso de Canadá, la Oficina del Comisario de Privacidad de Canadá (OPC), que supervisa el cumplimiento de la ley federal de Protección de la Información Personal y de los Documentos Electrónicos (PIPEDA) es independiente del gobierno, pero depende directamente del Parlamento. En cuanto a la Comisión de Acceso a la Información de Quebec, sus miembros son elegidos por la legislatura, a propuesta del primer ministro. Por último, en Chile no existe una autoridad que vele por la protección de datos personales.

Con relación a la facultad del Estado para acceder a los datos personales, se advierte que la gran mayoría de las regulaciones prevén la posibilidad de que el Estado sea relevado del consentimiento del titular para la recolección/cesión de los datos para funciones propias de Estado y/o por fines de "emergencia". En el caso de Francia, se destaca que determinados fines y tipos de actividades de tratamiento de datos están sujetos a requisitos más estrictos, especialmente cuando las actividades de tratamiento se lleven a cabo en nombre del Estado. Asimismo, resulta relevante lo dictaminado por el Supremo Tribunal Federal de Brasil durante la pandemia de Covid-19, haciendo énfasis en la falta de justificación de la finalidad del tratamiento por parte del Instituto Brasileño de Geografía y Estadística.

Por último, la gran mayoría de las normas objeto del presente documento estipulan un consentimiento expreso para el tratamiento de los datos. Sin embargo, Canadá (en sus distintas normas aplicables) y México prevén el consentimiento tácito en determinadas circunstancias.

REUTERS/Regis Duvignau

MAIN LAWS AND REGULATIONS / PRINCIPALES LEYES Y REGLAMENTOS

3 **What are the main laws and regulations protecting data in each jurisdiction?**

¿Cuáles son las principales leyes y reglamentos que protegen los datos en cada jurisdicción?

ARGENTINA

In Argentina, **Law No. 25.326 on Data Protection** ("LPDP", in Spanish) was enacted in October 2000 and its Regulation No. 1558 was passed in December 2001.

Both regulations establish a protection mechanism for the storing and processing of personal data in records, databases, files and computers with the aim of giving individuals control over their data. This is done through a series of rules and principles setting forth certain applicable standards and the practices that should be followed when dealing with individuals' information, the quality of specific data, consent for data processing, legal actions, restrictions to databases regarding content and time and ways of storing and processing, assignments and transfers to third parties (locally or abroad) and the intervention of government specialised agencies responsible for protecting these rights.

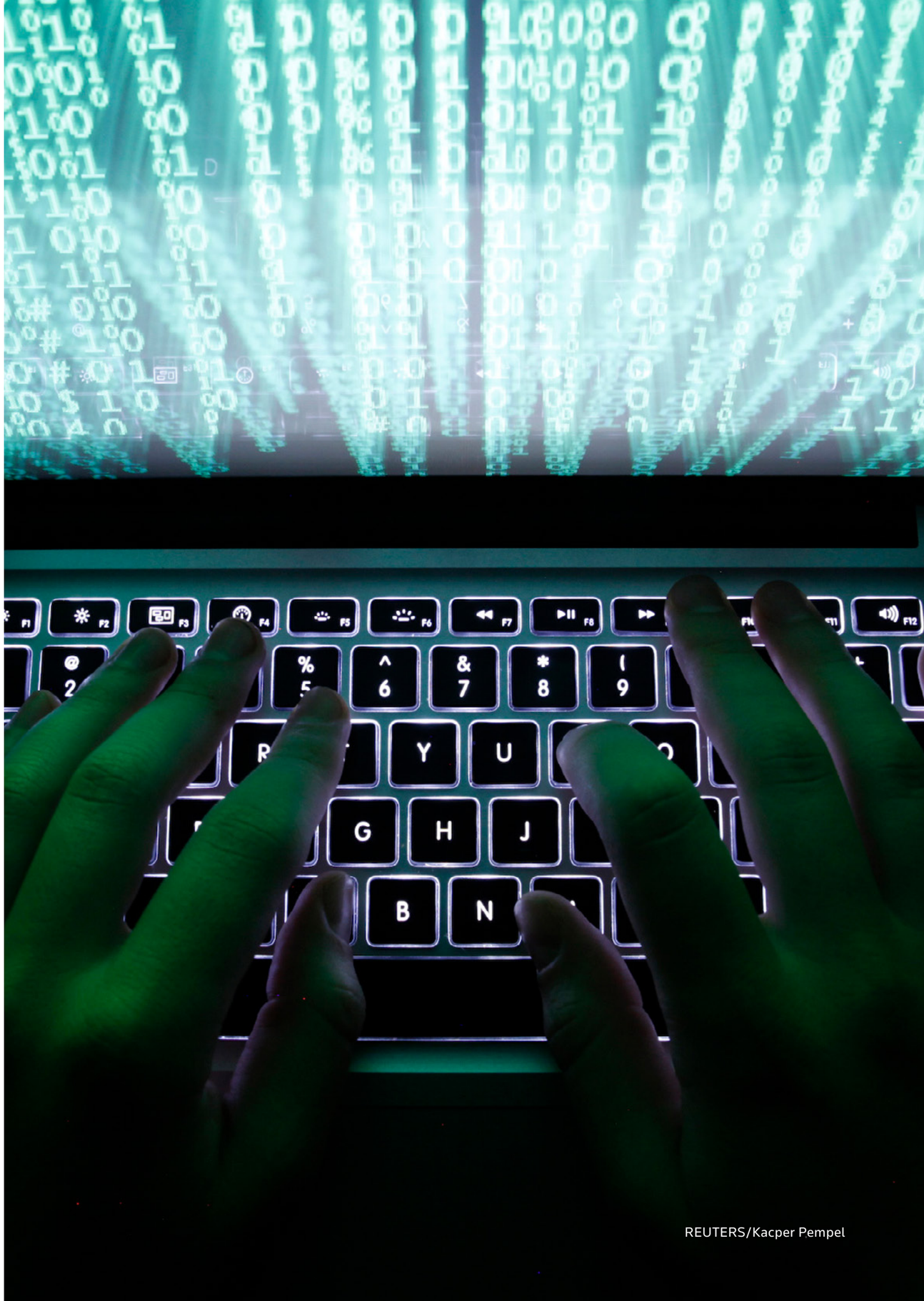
On 2 January 2019, the enactment of Law No. 27.483 was announced in the Official Gazette. Through such law Argentina adhered to the Convention for the protection of individuals regarding the processing of personal data (Convention 108). On 20 September 2019, Argentina signed the amendment to said Convention (Convention 108+), which is still to be ratified.

ARGENTINA

En octubre del año 2000 se promulgó en la Argentina la **Ley N° 25.326 de Protección de Datos Personales** (en adelante, la "LPDP"), y su Decreto Reglamentario Nro. 1558 (diciembre de 2001).

Ambas normas introdujeron un sistema de protección para el almacenamiento y tratamiento de datos personales en registros, bases, archivos y ordenadores, con la finalidad de otorgar a las personas una facultad de control sobre sus datos personales, a través de una serie de reglas y principios que establecen ciertos estándares a ser aplicados y las prácticas que deben seguirse en el manejo de la información sobre personas, la calidad de ciertos datos, el consentimiento para su tratamiento, acciones judiciales, limitaciones a los bancos de datos en su contenido, en el tiempo y en la forma de su almacenamiento y tratamiento, en las cesiones o transferencias a terceros (tanto locales como internacionales) y en la intervención de agencias especializadas del Estado destinadas a tutelar estos derechos, entre otros.

El 2 de enero de 2019, se publicó en el Boletín Oficial la Ley N° 27.483, mediante el cual la Argentina adhirió al Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal (Convenio 108) y el 20 de septiembre de 2019, la Argentina



REUTERS/Kacper Pempel

The LPDP is complimentary to the Rules and Regulations issued by the Access to Public Information Agency, the relevant enforcement authority in Argentina.

A bill on data protection was submitted to the House of Representatives on November 17, 2020. Such bill is an amendment to the current data protection system, similar to the General Data Protection Regulation (GDPR) and the Brazilian General Data Protection Act. It broadens the legal grounds to authorise data processing – including implicit consent – materially increases the value of the fines the control authority can impose, establishes extraterritorial jurisdiction standards and adopts innovative legal devices, such as a data protection delegate, an impact assessment on data protection and the rights of portability and objection.

suscribió una versión modernizada del tratado (Convenio 108+), cuya ratificación aún se encuentra pendiente.

La LPDP se complementa con Resoluciones y Disposiciones que emita la Agencia de Acceso a la Información Pública (AAIP), autoridad de aplicación en la materia.

El 17 de noviembre de 2020 se presentó un proyecto de ley de protección de datos personales ante la Cámara de Diputados de la Nación que propone una modernización del régimen vigente de protección de datos personales, que lo aproxima al Reglamento General de Protección de Datos de la Unión Europea (GDPR) y a la Ley General de Protección de Datos de Brasil y amplía las bases legales que autorizan el tratamiento de datos personales, incluyendo el consentimiento tácito, aumenta sustancialmente la cuantía de las multas que puede imponer la autoridad de control, establece un criterio de jurisdicción extraterritorial e incorpora instituciones novedosas, tales como el delegado de protección de datos, la evaluación de impacto relativa a la protección de datos personales y los derechos de portabilidad y oposición.

BRAZIL

Before the enactment of Federal Law No. 13,709/18, General Data Protection Law ("LGPD", in Portuguese) in August 2018, Brazil had several sectoral and scattered laws that regulated the subject of privacy.

The LGPD entered into force in September 2020 and its sanctions came into force on August 1, 2021.

The LGPD considers the protection of personal data a fundamental right of all natural persons and creates a set of regulations aimed at granting interested parties (only natural persons) located in Brazilian territory greater control and protection over their data.

Since 2022, data protection is considered a fundamental right provided for in the Brazilian Federal Constitution.

Applicable legislation:

- Brazilian Federal Constitution.
- Brazilian Civil Code.
- Brazilian Civil Rights Framework for the Internet, Law no. 12,965, of April 23, 2014, which establishes the principles, guarantees, rights and obligations for the use of the Internet in Brazil.
- Decree no. 8,771, of May 11, 2016, which regulates the Civil Rights Framework for the Internet.
- Decree no. 8,777, of May 11, 2016, which establishes the Open Data Policy of the Federal Government.
- Brazilian General Data Protection Law, Law no. 13,709, of August 14, 2018, which provides for the protection of personal data.

BRASIL

Antes de la promulgación de la Ley Federal n° 13.709/18, Ley General de Protección de Datos ("LGPD") en agosto de 2018, Brasil contaba con varias leyes sectoriales y dispersas que regulaban el tema de la privacidad.

La LGPD entró en vigor en septiembre de 2020 y sus sanciones entraron en vigor el 1 de agosto de 2021.

La LGPD considera la protección de datos personales como un derecho fundamental de todas las personas naturales y crea un conjunto de normas destinadas a otorgar a los interesados (solo personas naturales) ubicados en territorio brasileño un mayor control y protección sobre sus datos.

Desde 2022, la protección de datos es considerada un derecho fundamental previsto en la Constitución Federal brasileña.

Normativa aplicable:

- Constitución Federal Brasileña.
- Código Civil.
- Marco de Derechos Civiles de Brasil para Internet, Ley nº 12.965, de 23 de abril de 2014, que establece los principios, garantías, derechos y obligaciones para el uso de Internet en Brasil.
- Decreto nº 8.771, del 11 de mayo de 2016, que regula el Marco de Derechos Civiles de Brasil para Internet.
- Decreto nº 8.777, del 11 de mayo de 2016, que establece la Política de Datos Abiertos del Gobierno Federal.
- Ley General de Protección de Datos de Brasil, Ley nº 13.709, de 14 de agosto de 2018, que prevé la protección de los datos personales.

FRANCE

In the jurisdiction of France, national and European rules are applied to ensure data protection:

- **The national legislative framework:** France has been a global pioneer in the regulation of data protection, with the first version of its Data Protection Act coming into force in 1978 (**"FDPA"**). The Law has undergone several revisions, notably in 2019 to account for the European Union's General Data Protection Regulation (**"GDPR"**) and the Law Enforcement Directive (**"LED"**) coming into force..

The French legislative framework on data protection is mainly composed of the following:

- Law No. 78-17 of January 6, 1978 relating to information technology, files and liberties, as last amended: the French Data Protection Act.
- The French Civil Code
- Penal Code
- Specific legislation

However, as of 2022, the French Data Protection Law has been amended regarding provisions related to sanctioning procedures of the French Data Protection Authority. For example, the Decree of April 8 has created a simplified sanction procedure applicable to less complex matters that allows the French Data Protection Authority to take further action in relation to processing activities carried out by data controllers and processors.

- **The European legislative framework:** the European Regulation (EU) 2016/679 of April 27, 2016, called GDPR, came into force on May 25, 2018, and is a regulation, meaning it is immediately applicable as law in France. The GDPR replaced the European Union Directive 95/46/EC on the protection of personal data.

The European Directive (EU) 2016/680 of April 27, 2016, called LED, which came into force on May 25, 2018, is a directive. It sets an objective that all EU member states

FRANCIA

En la jurisdicción francesa se aplican normas nacionales y europeas para garantizar la protección de datos:

- **El marco legislativo nacional:** Francia ha sido pionera a nivel mundial en la regulación de la protección de datos, con la entrada en vigor de la primera versión de su Ley de Protección de Datos en 1978 (**"FDPA"**, en inglés). La Ley ha sido objeto de varias revisiones, la última de las cuales ha sido la de 2019 para tener en cuenta la entrada en vigor del Reglamento General de Protección de Datos de la Unión Europea (**"RGPD"**) y la Directiva de Aplicación de la Ley (**"LED"**, en inglés).

El marco legislativo francés en materia de protección de datos se compone principalmente de lo siguiente:

- **Ley nº 78-17 del 6 de enero de 1978 relativa a la informática, los archivos y las libertades, modificada por última vez: la Ley de Protección de Datos francesa.**
- **El Código Civil francés**
- **Código Penal**
- **Legislaciones específicas**

Sin embargo, a partir del 2022 la Ley de Protección de Datos francesa ha sido modificada en lo que respecta a las disposiciones relacionadas con los procedimientos de sanción de la Autoridad de Protección de Datos francesa. Por ejemplo, el Decreto del 8 de abril ha creado un procedimiento simplificado de sanción aplicable a asuntos menos complejos que permite a la Autoridad Francesa de Protección de Datos tomar más medidas en relación con las actividades de tratamiento llevadas a cabo por los controladores y procesadores de datos.

- **El marco legislativo europeo: El Reglamento Europeo (UE)** 2016/679 de 27 de abril de 2016 denominado GDPR que entró en vigor el 25 de mayo de 2018, es un reglamento lo que significa que es inmediatamente aplicable como ley en Francia. El

must achieve, but each member state is free to decide how to transpose the rules into national law. The LED lays down rules on the protection of natural persons regarding the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, including the protection against and the prevention of threats to public security

GDPR sustituyó a la Directiva 95/46/CE de la Unión Europea sobre la protección de datos personales.

La Directiva Europea (UE) 2016/680 de 27 de abril de 2016 denominada LED que entró en vigor el 25 de mayo de 2018, es una directiva. Establece un objetivo que todos los Estados miembros de la UE deben alcanzar, pero cada Estado miembro es libre de decidir cómo transponer las normas a su legislación nacional. La LED establece normas sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de delitos o de ejecución de sanciones penales, incluida la protección contra las amenazas a la seguridad pública y su prevención.

CANADA

There currently are several provincial and federal **laws** governing the protection of personal information in Canada. For the private sector, there is the federal Personal Information Protection and Electronic Documents Act (**"PIPEDA"**) along with substantially similar provincial legislation. The provincial legislation of Quebec, The Private Sector Personal Information Protection Act (the **"Quebec Act"**), has recently been amended and is distinct from other provincial or federal private-sector legislation. For the public sector, there is the federal Privacy Act, which governs Government of Canada institutions. Each province has its own equivalent to the **Privacy Act.**

- The Quebec Act applies to any collection of personal information in Quebec in the private sector by "businesses".
- The Personal Information Protection and Electronic Documents Act (**"PIPEDA"**) is Canada's federal law regulating the privacy of private sector organisations.

PIPEDA applies to all private sector organisations in Canada that collect, use or disclose personal information during a commercial activity (section 4(1)). "Personal information" is defined as "information about an identifiable individual". "Commercial activity" is defined as "any particular transaction, act or conduct, or any regular course of conduct that is commercial in nature," including selling, bartering or renting donor, membership or other fundraising lists" (section 2(1)).

PIPEDA also applies to employee information that an organisation collects, uses, or discloses in connection with the operation of a federal work, enterprise, or business (section 4(2)).

PIPEDA also applies to employee information that an organization collects, uses, or discloses in connection with the operation of a federal work, enterprise, or business (section 4(2)).

- The *Privacy Act* regulates how Government of Canada institutions may collect, use, disclose, retain and dispose of individuals' personal information.

Government of Canada agencies include government departments, ministries, agencies, offices or corporations.

CANADÁ

Actualmente existen **varias leyes** que regulan la protección de datos personales en Canadá. En el sector privado, rige la ley federal de Protección de la Información Personal y de los Documentos Electrónicos ("PIPEDA", en inglés) junto con legislación provincial sustancialmente similar. La legislación provincial de Quebec, esto es, la Ley de Protección de Datos Personales en el Sector Privado (la "Ley de Quebec" o, referida en este documento como la "Ley"), ha sido modificada recientemente y se diferencia de otras normas provinciales y federales aplicables al sector privado. Para el sector público, rige la Ley federal de Privacidad, aplicable a instituciones del gobierno canadiense. Cada provincia cuenta con su propia norma equivalente de la Ley de Privacidad..

- La **Ley** de Protección de Datos Personales en el Sector Privado (la «Ley») se aplica a toda recogida de datos personales en Quebec en el sector privado por parte de «empresas».
- La Ley de Protección de la Información Personal y de los Documentos Electrónicos ("***PIPEDA***", en inglés) es la ley federal de Canadá que regula la privacidad de las organizaciones del sector privado.

La PIPEDA se aplica a todas las organizaciones del sector privado de Canadá que recojan, utilicen o divulguen información personal en el curso de una actividad comercial (artículo 4(1)). "Información personal" se define como "información sobre un individuo identificable". "Actividad comercial" se define como "cualquier transacción, acto o conducta particular, o cualquier curso regular de conducta que tenga carácter comercial", incluyendo la venta, el trueque o el alquiler de listas de donantes, de miembros o de otros tipos de recaudación de fondos" (artículo 2(1)).

La PIPEDA también se aplica a la información de los empleados que una organización recoge, utiliza o divulga en relación con la actividad de un trabajo, empresa o negocio federal (artículo 4(2)).

- La ***Ley de Privacidad*** regula el modo en que las instituciones del Gobierno de Canadá pueden recopilar, utilizar, divulgar, retener y disponer de la información personal de los individuos.

Las instituciones del Gobierno de Canadá incluyen los departamentos, ministerios, organismos, oficinas o empresas gubernamentales.

CHILE

The legal framework applicable to data protection in Chile is the following:

- Political Constitution of the Republic of Chile, article 19 No. 4
- Law 19.628 on the protection of private actions
- Law 20.584 governing patients' rights and obligations

CHILE

El marco normativo aplicable a la protección de datos en Chile comprende:

- Constitución Política de la República artículo 19 N° 4
- Ley 19.628 sobre protección de la vida privada
- Ley 20.584 que regula los derechos y deberes de los pacientes

REUTERS/Lee Smith

COLOMBIA

Colombian law establishes a dual regime for the protection of personal data (jointly, and hereinafter, "**Colombian Privacy Laws**"), as follows:

- **Law 1581** of 2012, **Decree 1377** of 2013, **Title V** of the Single Circular Letter issued by the SIC and other regulations implementing the same (hereinafter, the "General Data Protection Regime") establish the general requirements and obligations for the processing of personal data in Colombia by data controllers and processors.
- **Law 1266** of 2008 and its implementing regulations (hereinafter, the "Financial Habeas Data Regulations"), establish a series of requirements for the processing of financial data and commercial information (mainly credit score reports to credit bureaus).
- On the other hand, **Decree 090** of 2018 and the implementing rules issued by the SIC (mainly contained in Title V of its Single Circular Letter) establish the requirements for the registration of databases in Colombia before the National Database Registry ("RNBD", in Spanish).
- Finally, the Colombian Criminal Code (Law 599 of 2000 as amended by Law 1273 of 2009) establishes certain crimes in relation to the unlawful access or use of personal data, in particular, the following:
  - **Article 269F** establishes that whoever, without being authorised to do so, for his own benefit or that of a third party, obtains, compiles, subtracts, offers, sells, exchanges, sends, purchases, intercepts, discloses, modifies or uses personal codes, personal data contained in files, archives, databases or similar means, shall incur a prison term of forty-eight (48) to ninety-six (96) months and a fine of 100 to 1000 legal monthly minimum wages in force.
  - **Article 269G** establishes that whoever with illicit purpose and without being authorised to do so, designs, develops, traffics, sells, executes, programmes or sends electronic pages, links or pop-up windows, shall incur a prison term of forty-eight (48) to ninety-six (96) months and a fine of 100 to 1000 legal monthly minimum wages in force, provided that the conduct does not constitute a crime punishable by a higher penalty.

COLOMBIA

La legislación colombiana establece un doble régimen de protección de datos personales (conjuntamente, y en adelante, **"Leyes de Privacidad Colombianas"**), así:

- La **Ley 1581** de 2012, el Decreto 1377 de 2013, el Título V de la Circular Única expedida por la SIC y demás normas de desarrollo de la misma (en adelante, el "Régimen General de Protección de Datos") establecen los requisitos y obligaciones generales para el tratamiento de datos personales en Colombia por parte de los responsables y encargados del tratamiento.
- La **Ley 1266** de 2008 y su reglamento de desarrollo (en adelante, el "Régimen de Habeas Data Financiero"), establecen una serie de requisitos para el tratamiento de datos financieros e información comercial (principalmente, reportes de calificación crediticia a los burós de crédito o centrales de riesgo).
- Por otro lado, el **Decreto 090 de 2018** y las normas de desarrollo expedidas por la SIC (principalmente contenidas en el Título V de su Circular Única) establecen los requisitos para el registro de bases de datos personales en Colombia ante el Registro Nacional de Bases de Datos (por su sigla "RNBD")
- Finalmente, el **Código Penal colombiano** (Ley 599 de 2000 modificada por la Ley 1273 de 2009), establece, ciertos delitos en relación con los datos personales, en particular, los siguientes:
  - El **artículo 269F** establece que quien, sin estar autorizado para ello, en beneficio propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o utilice códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios similares, incurrirá en prisión de cuarenta y ocho (48) a noventa y seis (96) meses y multa de 100 a 1000 salarios mínimos legales mensuales vigentes.
  - El **artículo 269G** establece que quien con propósito ilícito y sin estar autorizado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en prisión de cuarenta y ocho (48) a noventa y seis (96) meses y multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena mayor.

SPAIN

In Spain, there is existing legislation at the national and international level that regulates the protection of personal data (understood as all information relating to an identified or identifiable natural person). The following is a list of the main regulations

Data protection regulation in Spain:

- Spanish Constitution ("CE", in Spanish)

Data protection is a fundamental right recognised under article 18.4 of the CE. This right has been also defined by the Constitutional Court of Spain in case law. The CE was a pioneer in recognising data protection as a fundamental right. Such article sets forth that "the law shall limit the use of technology to ensure the protection of the honour and personal and family privacy of all citizens and the full exercise of their rights."

- Organic Law 3/2018, of 5 December, on Data Protection and Digital Rights ("LOPDGDD", in Spanish)

LOPDGDD is the "cornerstone" of the legislation governing data protection in Spain. This is the law by which the Spanish legal system adapted to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April (General Data Protection Regulation or "GDPR").

- Royal Decree 1720/2007, of 21 December, which approves the Regulation implementing Organic Law 15/1999, of 13 December, on the Protection of Personal Data ("**RLOPD**", in Spanish)

RLOPD is a legal provision applicable to all situations that do not contradict GDPR and LOPDGDD. It was enacted to regulate the now repealed Organic Law 15/1999, of 13 December, on the Protection of Personal Data (which incorporated Directive 95/46/EC on the protection of individuals, now also repealed). This law is mostly de facto repealed.

- Decree 389/2021, of June 1, approving the Statute of the Spanish Agency for Data Protection

It establishes the regulatory framework applicable to the relevant Spanish data protection authority. There are also other autonomous data protection authorities (in the Basque Country, Catalonia and Andalusia) with jurisdiction over the processing of data related to public entities in those jurisdictions.

ESPAÑA

En España, existe normativa tanto a nivel nacional como internacional que regula la protección de los datos personales[1] (entendidos como toda información sobre una persona física identificada o identificable). A continuación, se expone un listado de las principales normas:

Normativa de protección de datos en España:

- Constitución Española **("CE")**

La protección de datos es un derecho fundamental protegido bajo el artículo 18.4 CE y que ha sido desarrollado por la doctrina del Tribunal Constitucional de España. La CE fue pionera en el reconocimiento del derecho fundamental a la protección de datos personales. Dicho artículo prevé que "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales **("LOPDGDD")**

La LOPDGDD es la "columna vertebral" de la normativa que regula la protección de datos en España. Es la norma que ha venido a adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016 (el Reglamento General de Protección de Datos o "**RGPD**").

- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal **("RLOPD")**

El RLOPD es una norma que aplica en todo aquello que no contradiga al RGPD y la LOPDGDD. Se trata de una norma que se aprobó para desarrollar la derogada Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (que transponía la ya también derogada Directiva Europea 95/46/CE relativa a la protección de las personas físicas). En su mayor parte se encuentra, de facto, derogada.

- Real Decreto 389/2021, de 1 de junio, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos

Establece el marco regulador de la autoridad española de protección de datos. Asimismo, se debe destacar que

1 Existen otras normas que regulan y protegen otro tipo de información como secretos empresariales, propiedad intelectual, etc.

Other provisions related to data protection:

- Law 34/2002, of 11 July, on Information Society Services and Electronic Commerce – This law is applicable to information society services providers based in Spain and the services they provide. For example, website builders, hosting providers, etc.

On data protection, this law governs, among other things, the sending of electronic advertisements and the use of cookies.

- Law 9/2014, of 9 May, General Telecommunications (currently in the process of being amended) – This law governs telecommunications in Spain, including the operation of networks and the provision of electronic communications services and associated resources. On data protection, this law regulates, among other things, unrequested telephone calls. In relation to this law, Spanish Law 25/2007, of 18 October, on the retention of data related to electronic communications and public communications networks may also be of interest.
- Organic Law 1/1982, of 5 May, on the Civil Protection of the Right to Honour, Personal and Family Privacy and Self-Image – This law specifically regulates the requirements that must be met among other things, to use an individual's image.
- Finally, Law 19/2013, of 9 December, on Transparency, Access to Public Information and Good Governance ("**Transparency Act**") is aimed at broadening and promoting transparency of public activity, regulating and ensuring the right to access to information in relation to such activity and establishing the good governance obligations public officers shall meet.

existen autoridades de protección de datos autonómicas (en País Vasco, Cataluña y Andalucía) que tienen competencias sobre el tratamiento de datos relativo a entidades públicas en dichos territorios.

Otras normas de interés en relación con datos personales:

- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico – Esta ley aplica a los prestadores de servicios de la sociedad de la información establecidos en España y a los servicios prestados por ellos. Por ejemplo, editores de páginas web, proveedores de servicios de alojamiento, etc.

A nivel de protección de datos, esta ley regula, entre otras cuestiones, el envío de comunicaciones comerciales por medios electrónicos o el uso de cookies.

- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones (en proceso de cambio en la actualidad) – Esta ley regula las telecomunicaciones en España, que comprenden la explotación de las redes y la prestación de los servicios de comunicaciones electrónicas y los recursos asociados. A nivel de protección de datos esta ley regula, entre otras cuestiones, las comunicaciones telefónicas no solicitadas. En relación con esta norma, la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones también puede ser de interés.
- Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen – Esta ley regula de manera específica las condiciones que se deben cumplir para, entre otras cuestiones, poder utilizar la imagen de una persona.
- Finalmente, existe la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno ("**Ley de Transparencia**") que tiene por objeto ampliar y reforzar la transparencia de la actividad pública, regular y garantizar el derecho de acceso a la información relativa a aquella actividad y establecer las obligaciones de buen gobierno que deben cumplir los responsables públicos.

MEXICO

In Mexico, the protection of personal data is a fundamental right recognized by the **Federal Constitution** (articles 6 section II, and 16 section II).

In the public sector, the law governing the protection of personal data in Mexico is the **General Law for the Protection of Personal Data in Possession of Obligated Parties**, as well as the local laws on the subject in each state of the Mexican Republic.

In the private sector, the law governing the protection of personal data in Mexico is the **Federal Law for the Protection of Personal Data in Possession of Private Parties**. There are auxiliary laws that complement this law such as the Regulation of the Federal Law for the Protection of Personal Data in Possession of Private Parties, and the Guidelines of the Privacy Notice.

All individuals and legal entities in the private sector involved in the processing of personal data are governed by the above legislation. Credit information companies and individuals who collect and process personal data exclusively for personal use are exempt from these rules.

URUGUAY

In Uruguay, data protection is governed by Law No. 18.331, known as Data Protection Act, and its regulations No. 414/009 and 64/020, which provide for the scope of application of such law.

The Data Protection Law was enacted on 11 August 2008 by Uruguayan Congress and published on 18 August that year.

- Law No. 18.331
- Regulatory decree No. 414/009
- Regulatory decree No. 64/020

MÉXICO

En México, la protección de datos personales es un derecho fundamental reconocido por la **Constitución Federal** (artículos 6 fracción II, y 16 fracción II).

En el sector público, la ley que rige la protección de datos personales en México es la **Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados**, así como las leyes locales en la materia de cada estado de la República Mexicana.

En el sector privado, la ley que rige la protección de datos personales en México es la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Existen leyes auxiliares que complementan esta ley como el Reglamento de la **Ley Federal de Protección de Datos Personales en Posesión de los Particulares,** y los Lineamientos del Aviso de Privacidad.

Todas las personas físicas y jurídicas del sector privado que participan en el tratamiento de datos personales se rigen por la legislación anterior. Quedan exentos de estas normas las empresas de información crediticia y los particulares que recojan y traten datos personales exclusivamente para uso personal.

URUGUAY

En Uruguay, la protección de datos personales se encuentra regulada por la ley número 18.331 llamada Ley de Protección de Datos Personales, y sus decretos reglamentarios, números 414/009 y 64/020 que establecen el ámbito de aplicación de la ley mencionada.

La ley de protección de datos fue promulgada el 11 de agosto de 2008 por el parlamento uruguayo y publicada el 18 del mismo mes.

- Ley 18.331
- Decreto 414/009
- Decreto 64/020

REUTERS/Gleb Garanich

GENDER PERSPECTIVE / PERSPECTIVA DE GÉNERO

4

Do these laws and regulations adopt a gender perspective? If so, how is it addressed? We would like to know if these laws and regulations include any specific protection for women reporting domestic violence, sexual abuse and other gender-based crimes. We would like to know whether the law addresses this issue.

¿Tienen las leyes y reglamentos una perspectiva de género? En caso afirmativo, ¿cómo se aborda? Queremos saber si las leyes y los reglamentos tienen alguna protección específica para las mujeres que denuncian la violencia doméstica, el abuso sexual y otros delitos de género. Nos gustaría saber si la ley aborda o no esta cuestión.

ARGENTINA

LPDP and its complementary laws and regulations do not adopt a gender perspective. Therefore, there is no specific protection for women reporting domestic violence, sexual abuse and other gender-based crimes. There is also no record of parliamentary debates addressing gender-based data protection.

Notwithstanding the above, Resolution No. 08/2014 issued by the Argentine Directorate for Data Protection ("DNPDP", in Spanish) should be highlighted. In such resolution, the DNPDP, former LPDP enforcement authority, mentioned the "Collaboration Agreement between the Argentine Council for Women and the Argentine Institute for Statistics and Census ("INDEC", in Spanish)", executed on 11 September 2012. Such agreement provides for: (i) the collaboration between the parties to design indicators of violence against women; (ii) the implementation of a Single Register of Cases of Violence Against Women based on administrative records compiling information of different sources of the Public Administration; (iii) the reporting of cases of violence against women; and (iv) the joint disclosure and publication of the outcomes achieved.

ARGENTINA

La LPDP y su normativa complementaria no cuentan con una perspectiva de género. En ese sentido, no se prevé una protección específica para las mujeres que denuncian la violencia doméstica, el abuso sexual y otros delitos de género. Tampoco constan antecedentes parlamentarios donde se haya tratado la protección de datos personales con perspectiva de género.

De todas maneras, se puede destacar el Dictamen N° 08/2014 emitido por la Dirección Nacional de Protección de Datos Personales (ex autoridad de aplicación de la LPDP, en adelante "DNPDP"), en el que se pronunció sobre el "*convenio de Cooperación entre el Consejo Nacional de las Mujeres y el Instituto Nacional de Estadísticas y Censos (INDEC)*", suscripto el 11-09.2012. Dicho convenio tiene como finalidad: (i) la cooperación de las partes para el diseño de indicadores de violencia contra las mujeres; (ii) la implementación de un Registro Único de Casos de Violencia contra las Mujeres sobre la base de registros administrativos provenientes de diversas fuentes de información de la Administración Pública; (iii) el relevamiento de casos sobre violencia contra las mujeres y (iv) la difusión y publicación en conjunto los resultados que se logren.

Through this Resolution and considering the lack of a specific reference to gender-based violence in the LPDP, the DNPDP framed the information gathered as sensitive data. Sensitive data is defined as personal data revealing racial or ethnic origin, political opinions, religious, moral or philosophical beliefs, trade-union membership, health-related data and data concerning a person's sex life or sexual orientation. This data can only be gathered and processed for public interest reasons authorised by law or for statistics or scientific purposes and only if data subjects cannot be identified.

En este Dictámen y ante la ausencia de una referencia específica en la LPDP para los casos de violencia de género, la DNPDP enmarcó la información recolectada dentro del concepto de datos sensibles, es decir, aquellos que revelan el origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual. De este modo, esta información podrá ser recolectada y tratada únicamente cuando medien razones de interés general autorizadas por ley, o ser tratados con finalidades estadísticas o científicas siempre que sus titulares no puedan ser identificados.

BRAZIL

This issue is not considered at all in Brazilian data protection legislation.

BRASIL

Esta cuestión no se considera en absoluto en la legislación brasileña de protección de datos.

Las leyes de protección de datos aplicables vigentes en Brasil no consideran la cuestión de género.

CANADA

The Law: No The Act does not have a gender perspective. There are no laws or regulations under the Personal Information Protection and Electronic Documents Act ("PIPEDA") that provide specific protections for women who report cases of domestic violence or sexual abuse.

- **PIPEDA**: PIPEDA does not address gender-related privacy issues. PIPEDA does not contain laws or regulations that provide specific protections for women who report cases of domestic violence or sexual abuse.
- **Privacy Act**: No.

CANADÁ

La Ley: No. La Ley no tiene una perspectiva de género. No hay leyes ni reglamentos en el marco de la Ley del Sector Privado que prevean protecciones específicas para las mujeres que denuncien casos de violencia doméstica o abusos sexuales.

- **PIPEDA**: La PIPEDA no aborda las cuestiones de privacidad relacionadas con el género. La PIPEDA no contiene leyes ni reglamentos que establezcan protecciones específicas para las mujeres que denuncian casos de violencia doméstica o abusos sexuales.
- **La Ley de Privacidad**: No.

CHILE

The issue of gender is not covered by current legislation in Chile.

CHILE

La cuestión de género no está considerada en la legislación actual.

COLOMBIA

In Colombia, the laws and regulations specifically addressing data protection do not have a gender perspective.

COLOMBIA

En la jurisdicción colombiana, las leyes y reglamentos emitidos específicamente en relación con la protección de datos no tienen una perspectiva de género.

FRANCE

In France, data protection laws and regulations have no gender perspective.

FRANCIA

En la jurisdicción francesa, las leyes y reglamentos sobre protección de datos no tienen ninguna perspectiva de género.

SPAIN

In the Spanish legal framework on data protection, paragraph 2 of the seventh additional provision of the LOPDGDD sets forth that, in relation to the identification of interested parties in notices through announcements and publications of administrative acts, and in order to prevent risks to victims of gender-based violence, the Government will promote the drafting of a collaboration protocol defining safe procedures for the publication and notification of administrative acts, with the involvement of competent authorities. The processing of data related to criminal behavior falls under a special regulation and, in general terms, is banned.

Moreover, the Spanish Data Protection Agency ("AEPD", in Spanish) has a section dedicated to this topic on its website, directing to sources of information and links to reports and regulations on this issue. Last year AEPD also published the guide "Data protection in an employment relationship", which includes guidelines on the application/construction of applicable legislation on data protection in situations involving victims of harassment and gender-based violence in the workplace (please see sections 4.15 and 6.6).

ESPAÑA

En la normativa española de protección de datos, el apartado 2 de la disposición adicional séptima de la LOPDGDD dispone que, en relación con la identificación de interesados en las notificaciones por medio de anuncios y publicaciones de actos administrativos, y a fin de prevenir riesgos para víctimas de violencia de género, el Gobierno impulsará la elaboración de un protocolo de colaboración que defina procedimientos seguros de publicación y notificación de actos administrativos, con la participación de los órganos con competencia en la materia. El tratamiento de datos relativo a comportamientos delictivos tiene una regulación especial y, en general, se prohíbe.

Además, la Agencia Española de Protección de Datos (la "AEPD") tiene una sección en su página web dedicada a esta materia, donde remite a fuentes de información así como a enlaces a resoluciones e informes relativos a este tema. Asimismo, la AEPD publicó el año pasado la guía sobre "La protección de datos en las relaciones laborales" donde ofrece ciertas directrices en relación con la aplicación / interpretación de la normativa aplicable de protección de datos a situaciones que involucren a víctimas de acoso y de violencia de género en el ámbito laboral (véanse secciones 4.15 y 6.6).

MEXICO

The laws covered in section 2.8 of this report do not include specific provisions that address a gender perspective. The laws seek to protect men and women without specifically addressing women, domestic violence, sexual abuse and gender-based crimes.

MÉXICO

Las leyes mencionadas en el punto 2.8 no incluyen disposiciones específicas que aborden la perspectiva de género. Las leyes pretenden proteger a los hombres y a las mujeres sin proteger especialmente a las mujeres, la violencia doméstica, los abusos sexuales y los delitos de género.

URUGUAY

Law No. 18.331 does not include a gender perspective. Instead, it regulates data protection of all natural and legal persons equally on the basis that data protection is a fundamental human right.

However, the protection of personal data of women who are victims of gender-based violence is regulated under section 7 of Law 19.850, also known as Gender-based Violence Against Women Act. Subsection E of such provision provides for the protection of: "confidentiality and privacy of their personal data, that of their offspring and of any other person under their custody or care."

Law 19.580 also regulates the Uruguayan Women Institute, the "enforcement authority for public policies aiming at violence-free life for women". Among its obligations, this authority, under section 11 (J), is responsible for: "Creating records of quantitative and qualitative data about gender-based violence, taking into account data like age, disabilities, racial and ethnic origin, religious beliefs, territory and other factors of discrimination. They must also **ensure the confidentiality of personal data** so that the person they refer to cannot be identified (Law No. 18.331 of 11 August 2008)."

Law No. 19.580

URUGUAY

La ley 18.331 no posee una perspectiva de género, sino que regula a todas las personas tanto físicas como jurídicas por igual, basándose en que la protección de datos personales es un derecho humano fundamental.

Sin embargo, la protección de los datos personales de las mujeres víctimas de violencia de género, se encuentra regulada en el artículo 7 de la ley 19.580, LEY DE VIOLENCIA HACIA LAS MUJERES BASADA EN GÉNERO, que en su inciso E estipula que: "A que se garantice la confidencialidad y la privacidad de sus datos personales, los de sus descendientes o los de cualquiera otra persona que esté bajo su tenencia o cuidado."

A su vez, la ley 19.580 regula el Instituto Nacional de las Mujeres, "órgano rector de las políticas públicas para una vida libre de violencia para las mujeres", que tiene dentro de sus obligaciones, la establecida en el inciso J del artículo 11: "Generar registros de datos cuantitativos y cualitativos sobre violencia basada en género, que contemplen variables tales como edad, situación de discapacidad, origen étnico racial, religión, territorialidad, entre otras dimensiones de la discriminación. Deberán adaptarse medidas a fin de **garantizar la reserva de los datos personales** de forma que no sea identificable la persona a la que refieren (Ley N° 18.331, de 11 de agosto de 2008)."

Ley 19.580

REUTERS/Brittany Hosea

REUTERS/Evgenia Novozhenina

ENFORCEMENT AUTHORITY / AUTORIDAD DE APLICACIÓN

5

Who is the enforcement authority? Is it independent of the Executive Branch? How is it regulated?

¿Quién es la autoridad de aplicación? ¿Es un órgano dependiente o independiente del poder ejecutivo? ¿Cómo se regula esta autoridad?

ARGENTINA

Created in 2017, the Agency for Access to Public Information (Agencia de Acceso a la Información Pública - AAIP) is an autarchic entity that operates independently within the Office of the Chief of Cabinet of Ministers in Argentina and is the enforcement authority for data protection laws. It is also the control authority for Law No. 27.275 (Right to Access to Public Information Act) and Law No. 26.951, which created a "Don't Call" National Record in Argentina.

The LPDP establishes that the AAIP must carry out all necessary actions to ensure compliance with the objectives and all provisions under the law. The AAIP is also vested with the power to assist and advise individuals requesting support on the scope of the LPDP and the legal means available to defend their rights under the LPDP. It also has the power to issue rules and regulations that databases and its administrators must follow, impose administrative sanctions, carry out file censuses, receive claim reports, oversee the satisfaction of legal provisions on the integrity and safety of data, among other powers.

ARGENTINA

Creada el año 2017, la Agencia de Acceso a la Información Pública (AAIP) es un ente autárquico que funciona con autonomía funcional en el ámbito de la Jefatura de Gabinete de Ministros de la Nación y es la autoridad de aplicación en materia de datos personales. También es el órgano de control de la Ley N° 27.275 (Derecho de Acceso a la Información Pública) y la Ley N° 26.951 de creación del Registro Nacional "No Llame".

LPDP prevé que la AAIP deberá realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la normativa, otorgándole facultades para asistir y asesorar a las personas que lo requieran acerca del alcance de la LPDP y de los medios legales de que disponen para la defensa de los derechos que la LPDP garantiza como dictar normas y reglamentaciones que deberán observar las bases de datos y sus responsables, imponer sanciones administrativas, realizar censos de archivos, recibir denuncias, controlar la observancia de las normas sobre integridad y seguridad de datos, entre otras atribuciones.

BRAZIL

The enforcement authority is the National Data Protection Authority (ANPD, in Portuguese), an entity of the federal public administration, reporting to the Presidency of the Republic, so it is not an independent body of the executive branch.

Under the Brazilian General Data Protection Law, the legal nature of the ANPD is transitory and may be transformed by the Executive Branch into an entity of the indirect federal public administration, subject to a special autarchic regime and reporting to the Presidency of the Republic, and the evaluation of this transformation must occur within two (2) years following the date of which it enters into force of the regulatory framework of the ANPD.

BRASIL

La autoridad de aplicación es la Autoridad Nacional de Protección de Datos (ANPD), una entidad de la administración pública federal, perteneciente a la Presidencia de la República, por lo que no es un órgano independiente del poder ejecutivo.

De acuerdo con la Ley General de Protección de Datos brasileña, la naturaleza jurídica de la ANPD es transitoria y puede ser transformada por el Poder Ejecutivo en una entidad de la administración pública federal indirecta, sujeta a un régimen autárquico especial y perteneciente a la Presidencia de la República, y la evaluación de esta transformación deberá ocurrir dentro de los dos (2) años siguientes a la fecha de entrada en vigor del marco normativo de la ANPD.

CANADA

The Privacy Commission of Québec is the enforcement authority for the Quebec Act. It is composed of a supervisory division and an adjudication division. The members of the Commission are appointed, on the proposal of the Premier, by a resolution of the National Assembly (i.e., the legislature of Québec) passed by no less than two-thirds of its members. The Commission must send a report of its activities during the preceding fiscal year to the appointed minister no later than June 30 of each year, which is tabled in the National Assembly.

The Office of the Privacy Commissioner of Canada ("OPC") enforces and monitors compliance with PIPEDA. The OPC is independent of the Government of Canada and is non-partisan but reports directly to Parliament. The OPC is appointed for 7-year terms.

The OPC's organisational structure consists of three sectors: the Compliance Sector, the Policy and Promotion Sector and the Corporate Management Sector. The work of each sector is supervised by a Deputy Commissioner. The three Deputy Commissioners, as well as the Legal Services Directorate, report directly to the Privacy Commissioner. The Commissioner is also supported by the OPC Executive Secretariat.

CANADÁ

La Comisión de Acceso a la Información de Quebec (the Privacy Commission of Quebec) es la autoridad de aplicación. Está compuesta por una división de supervisión y una división de adjudicación. Los miembros de la Comisión son nombrados, a propuesta del primer ministro, por una resolución de la Asamblea Nacional (es decir, la legislatura de Quebec) aprobada por no menos de dos tercios de sus miembros. La Comisión debe enviar un informe de sus actividades durante el año fiscal anterior al ministro designado, a más tardar el 30 de junio de cada año, que se presenta en la Asamblea Nacional.

La Oficina del Comisario de Privacidad de Canadá ("**OPC**", en inglés) aplica y supervisa el cumplimiento de PIPEDA. La OPC es independiente del gobierno de Canadá y no es partidista, pero depende directamente del Parlamento. El OPC se nombra por períodos de 7 años.

La estructura organizativa de la OPC se compone de tres sectores: el Sector de Cumplimiento, el Sector de Política y Promoción y el Sector de Gestión Corporativa. El trabajo de cada sector está supervisado por un Comisario Adjunto. Los tres Comisarios Adjuntos, así como la Dirección de Servicios Jurídicos, dependen directamente del Comisario de Privacidad. El Comisario también cuenta con el apoyo de la Secretaría Ejecutiva de la OPC.

REUTERS/Andrew Kelly

CHILE

In Chile there is no enforcement authority responsible for ensuring data protection. Instead, only civil courts hear Habeas data actions and Appellate Courts can hear actions for constitutional relief.

CHILE

En Chile no existe una autoridad que vele por la protección de datos. Solo los tribunales civiles conocen de Habeas data o bien por medio de recursos de protección ante la Corte de Apelaciones.

COLOMBIA

The enforcement authority in Colombia is the Superintendence of Industry and Commerce ("SIC", in Spanish). Although the SIC exercises its functions independently, it remains an entity attached to the Colombian Ministry of Commerce, Industry and Tourism (which is part of the executive branch).

Therefore, the President of the Republic of Colombia has the power to appoint the Superintendent of Industry and Commerce (or to ratify the person who previously held this position).

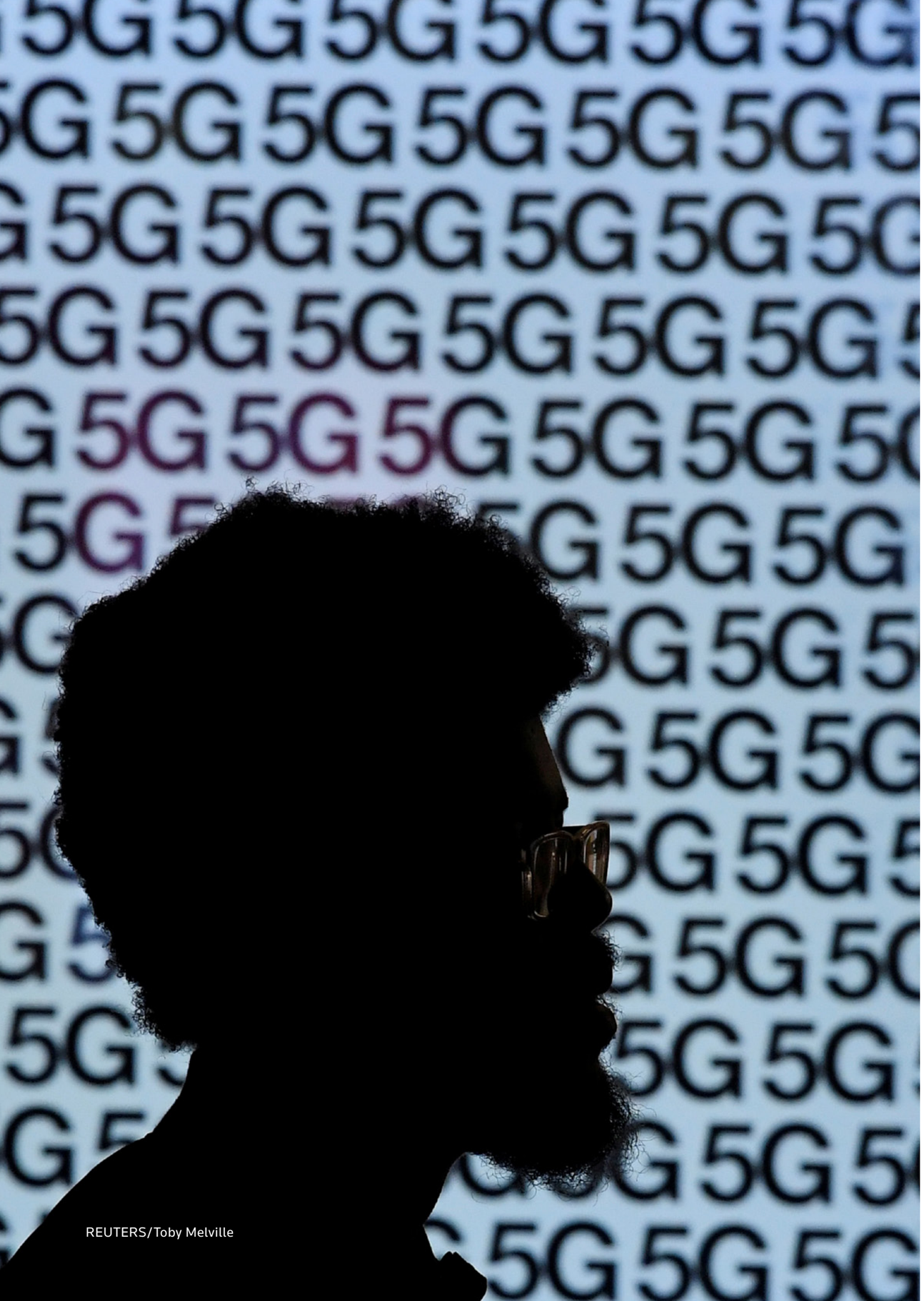
The competences of the SIC are clearly delimited in Decree 4886 of 2011 as the Colombian data protection authority.

COLOMBIA

La autoridad de protección de datos en Colombia es la Superintendencia de Industria y Comercio (SIC). Aunque la SIC ejerce sus funciones de forma independiente, sigue siendo una entidad adscrita al Ministerio de Comercio, Industria y Turismo de Colombia (que forma parte de la rama ejecutiva).

Por lo tanto, el Presidente de la República de Colombia tiene la facultad de nombrar al Superintendente de Industria y Comercio (o de ratificar a la persona que venía desempeñando este cargo anteriormente).

Las competencias de la SIC están claramente delimitadas en el Decreto 4886 de 2011 como autoridad colombiana de protección de datos.



REUTERS/Toby Melville

FRANCE

The Commission nationale de l'informatique et des libertés (CNIL), created by the FDPA in 1978, is an independent administrative authority and its missions are primarily the following:

- To inform data subjects and data controllers of their rights and obligations and to ensure the protection of data subjects' rights
- Support data controllers and processors in complying with data protection legislation and advise them.
- Ensure that the processing of personal data is carried out in accordance with the provisions of the applicable legislation.
- Reflect on the ethical problems and social issues raised by the development of information technology.
- Monitor the processing activities of data controllers and processors and, in the event of non-compliance, to sanction them.

The CNIL is a very active supervisory authority. It has a website on which it regularly publishes information and the sanctions it has adopted (when they are made public) (see). Unfortunately, the CNIL's publications are still mainly in French. However, the authority gradually publishes information in English.

Acts and decisions taken by the CNIL can be appealed directly to the highest French administrative court (Conseil d'État). This applies to sanctions, guidelines or any decision of the CNIL. Decisions of the French High Administrative Court are final and cannot be appealed.

The FDPA also obliges the CNIL to publish an annual report of its activities. Each year, the Commission submits a public report to the President of the Republic and the Prime Minister on the execution of its statutory responsibilities (Article 3 of the FDPA). This obligation is intended to help ensure the transparency and fairness of the CNIL's actions.

FRANCIA

La "Commission nationale de l'informatique et des libertés" (CNIL), creada por la FDPA en 1978, es una autoridad administrativa independiente y sus misiones son principalmente las siguientes:

- Informar a los interesados y a los responsables del tratamiento de sus derechos y obligaciones y garantizar la protección de los derechos de los interesados;
- Apoyar a los responsables y encargados del tratamiento en el cumplimiento de la legislación sobre protección de datos y asesorarlos;
- Garantizar que el tratamiento de los datos personales se realice de acuerdo con lo dispuesto en la legislación aplicable;
- Reflexionar sobre los problemas éticos y las cuestiones sociales que plantea el desarrollo de la informática;
- Controlar las actividades de tratamiento de los responsables y procesadores de datos y, en caso de incumplimiento, sancionarlos.

La CNIL es una autoridad de control muy activa. Dispone de un sitio web en el que publica regularmente información y las sanciones que ha adoptado (cuando se hacen públicas) (véase). Lamentablemente, las publicaciones de la CNIL están todavía principalmente en francés. Sin embargo, la autoridad pública progresivamente información en inglés.

Los actos y decisiones tomadas por la CNIL pueden ser recurridos directamente ante el más alto tribunal administrativo francés (Conseil d'État). Esto se aplica a las sanciones, directrices o cualquier decisión de la CNIL. Las decisiones del Tribunal Superior Administrativo francés son definitivas y no pueden ser recurridas.

La FDPA también obliga a la CNIL a publicar un informe anual de sus actividades. Cada año, la Comisión presenta un informe público al Presidente de la República y al Primer Ministro sobre la ejecución de sus responsabilidades estatutarias (artículo 3 de la FDPA). Esta obligación tiene por objeto contribuir a garantizar la transparencia y la equidad de las actuaciones de la CNIL.

SPAIN

In Spain, the Spanish Data Protection Agency ("AEPD", in Spanish) is the authority responsible for overseeing the enforcement of the LOPDGDD and RGPD and, particularly, performing the duties established under these laws and their provisions of implementation. The AEPD is an independent administrative authority, a legal entity with full private and public capacity, acting independently of branches of government when performing its duties.

Title VII of LOPDGDD regulates the AEPD, in particular, its budget, staff, functions, powers and structure. In addition, Royal Decree No. 389/2021, of 1 June, which approves the statute of the AEPD, governs its operation.

In line with the above, among the functions the AEPD has, the following should be highlighted:

- Oversee the enforcement of RGPD and other data protection legislation.
- Raise the awareness of the public and ensure the understanding of risks, legislation, guarantees and rights related to data processing.
- Advice the executive and legislative branches, as well as other entities, on the protection of individuals' rights and liberties related to data processing.
- Handle claims filed by stakeholders or organisations.
- Carry out investigations on the enforcement of RGPD (upon request or *ex oficio*).

On decisions, under the LOPDGDD, the AEPD is obliged to publish all decisions made by its Head granting or rejecting the enforcement of the rights under articles 15 to 22 of RGPD, ending claim proceedings, closing prior investigations, sanctioning with a warning, granting provisional remedies or other remedies provided for under its statute.

Alongside the AEPD, there are other autonomous data protection authorities in Spain (specifically, the Catalan Data Protection Authority, Basque Data Protection Agency and Andalusian Data Protection Authority). However, their duties and powers are more restricted and focused on data processing by public entities in their respective jurisdictions.

ESPAÑA

En España, la Agencia Española de Protección de Datos (AEPD) es la entidad encargada de supervisar la aplicación de la LOPDGDD y el RGPD y, en particular, de ejercer las funciones establecidas en dichas normas y en sus disposiciones de desarrollo. La AEPD es una autoridad administrativa independiente de ámbito estatal, con personalidad jurídica y plena capacidad pública y privada, que actúa con plena independencia de los poderes públicos en el ejercicio de sus funciones.

El Título VII de la LOPDGDD regula el régimen de la AEPD y, en concreto, su régimen económico presupuestario y de personal, funciones y potestades y estructura. Además, el Real Decreto 389/2021, de 1 de junio, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos regula su funcionamiento.

En línea con lo anterior, y entre las muchas funciones que tiene la AEPD, destacamos las siguientes:

- Controlar la aplicación del RGPD y del resto de la normativa de protección de datos.
- Promover la sensibilización del público y su comprensión de los riesgos, normas, garantías y derechos en relación con el tratamiento de datos personales.
- Asesorar al poder legislativo y ejecutivo, así como a otras instituciones y organismos sobre la protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales.
- Tratar las reclamaciones presentadas por un interesado u organismo.
- Llevar a cabo investigaciones sobre la aplicación del RGPD (a petición o *ex oficio)*.

En relación con las resoluciones, la LOPDGDD impone a la AEPD la obligación de publicar las resoluciones de su Presidencia que declaren haber lugar o no a la atención de los derechos reconocidos en los artículos 15 a 22 del RGPD, las que pongan fin a los procedimientos de reclamación, las que archiven las actuaciones previas de investigación, las que sancionen con apercibimiento, las que impongan medidas cautelares y las demás que disponga su estatuto.

Junto a la AEPD, en España existen autoridades de protección de datos autonómicas (en concreto, la Autoridad de Protección de Datos Catalana, la Agencia Vasca de Protección de Datos y la Autoridad Andaluza de Protección de Datos) aunque con funciones y potestades más restringidas centradas en tratamientos de datos llevados a cabos por entidades públicas en sus respectivos territorios.

MEXICO

The authority in charge of ensuring data protection is the National Institute for Access to Public Information and Protection of Personal Data ("INAI", in Spanish). INAI is an autonomous agency in charge of promoting and disseminating the right of access to public information and the right to data protection in government agencies and individuals. This agency is committed to collaborate with federal, state and municipal authorities to promote data protection in different industries and sectors, such as finance, education and health.

INAI will be the first instance for all data protection proceedings. INAI's resolutions may be challenged before the Federal Judicial Courts. In addition, damages may be sought in the civil courts.

Enforcement of data protection laws tends to be difficult.

URUGUAY

The Agency for the Development of Electronic Government and Information Society and Knowledge ("AGESIC", in Spanish) is the autonomous enforcement authority, reporting to the President of Uruguay, responsible for ensuring the improvement of services for citizens, making use of information technologies and communications. Law No. 18.331 created a body decentralised from the AGESIC, and thus the Executive Branch, called the Data Control and Regulatory Unit ("URCDP", in Spanish), which has technical autonomy to operate.

Although some of the URCDP members are appointed by the Executive Branch, they do not receive orders or instructions when it comes to technical knowledge.

It is responsible for ensuring compliance with the law and has the power to impose different sanctions in the case of any breaches by those responsible for database adminstration.

This control authority is governed by sections 31, 34 and 35 of the law.

AGESIC's website

URCDP's website

MÉXICO

La autoridad encargada de velar por la protección de los datos es el Instituto Nacional de Acceso a la Información Pública y Protección de Datos Personales ("INAI"). El INAI es un organismo autónomo encargado de promover y difundir el derecho de acceso a la información pública y el derecho a la protección de datos en las dependencias gubernamentales y en los particulares. Este organismo se compromete a colaborar con las autoridades federales, estatales y municipales para promover la protección de datos en diferentes industrias y sectores, como el financiero, el educativo y el de la salud.

El INAI será la primera instancia para todo procedimiento de protección de datos. Las resoluciones del INAI podrán ser impugnadas ante los Tribunales Judiciales Federales. Además, se puede solicitar una indemnización por daños y perjuicios en los tribunales civiles.

La aplicación de las leyes de protección de datos tiende a ser dura.

URUGUAY

La Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (AGESIC) es una unidad ejecutora con autonomía técnica dependiente de Presidencia de la República Oriental del Uruguay, que tiene como objetivo procurar la mejora de los servicios al ciudadano, utilizando las posibilidades que brindan las tecnologías de la información y las comunicaciones. La ley 18.331 crea un órgano desconcentrado de la AGESIC, y por lo tanto del poder ejecutivo, llamado Unidad Reguladora y de Control de Datos Personales. La misma cuenta con la más amplia autonomía técnica.

La URCDP se caracteriza porque si bien algunos miembros son designados por el Poder Ejecutivo, no recibirán órdenes ni instrucciones en el plano técnico.

Tiene como cometido controlar el cumplimiento de lo estipulado en la ley, así como la potestad de aplicar sanciones de diversos grados en caso de detectar incumplimientos por parte de los responsables de las bases de datos.

El órgano de control se encuentra regulado por los artículos 31, 34 y 35 de la ley.

Sitio web de AGESIC

Sitio web URCDP

STATE ACCESS TO PERSONAL DATA / ACCESO DEL ESTADO A LOS DATOS PERSONALES

6

How is the issue of data in the possession of the State addressed? What are the State's powers in relation to the use of and access to personal data? For this question, we would like lawyers to address the question of whether the State can access data due to a "public emergency".

¿Cómo se aborda la cuestión de los datos en posesión del Estado? ¿Cuáles son los poderes del Estado en relación con el uso y el acceso a los datos personales? Para esta pregunta, nos gustaría que los abogados abordaran la cuestión de si el Estado está facultado para acceder a los datos en nombre de una "emergencia pública".

ARGENTINA

Pursuant to article 5 of the LPDP, personal data processing is illegal whenever the data subject has not given free, express and informed consent in writing or by similar means. However, a subsection of the article sets forth that consent shall not be required whenever data is collected for branches of government to perform their own duties (or as a result of a legal obligation).

All persons obligated under LPDP have a duty of confidentiality in relation to personal data subject to processing (article 10 of LPDP) and can be dismissed from such duty only by court order or for sufficient reasons of public safety, national defense or public health.

However, consent is not required for the direct transfer of personal data from and to Government bodies, provided it falls within the scope of their powers (article 11 (3.C) of LPDP). Neither is it required for the transfer of health-related data necessary for public health or emergency reasons, etc., provided the identity of the data subjects always remains confidential through anonymity tools.

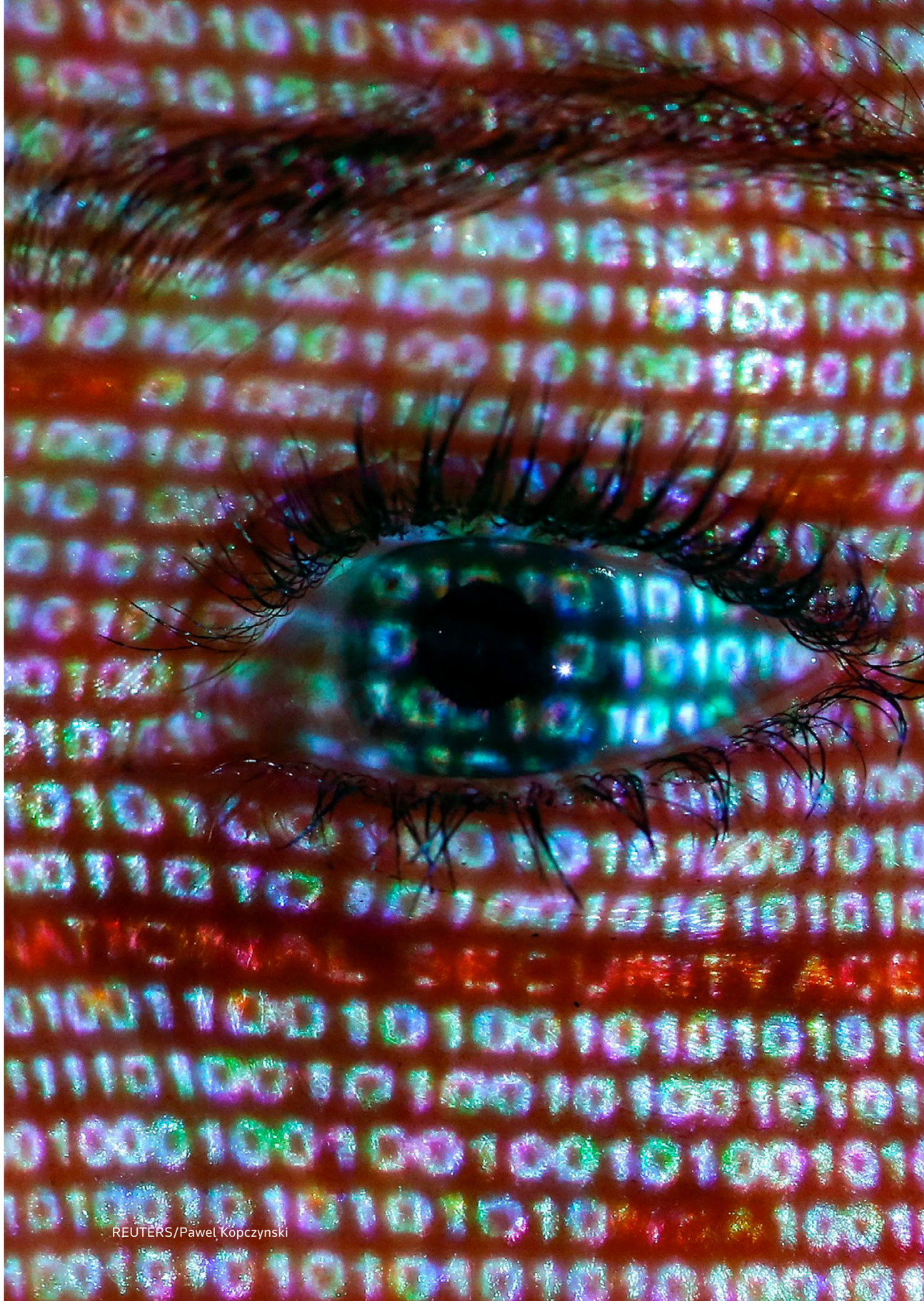
The processing of personal data must always be carried out following the principles of legality, transparency, purpose limitation (protecting individuals' vital/essential interests), accuracy, and data minimisation. On this last point, it should be said that processed data shall

ARGENTINA

Según el art. 5 de la LPDP, el tratamiento de datos personales es ilícito cuando el titular no hubiera prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito o por otro medio que permita se le equipare. Sin embargo, un inciso del mismo artículo establece que no se requerirá del consentimiento cuando se recaben los datos para el ejercicio de funciones propias de los poderes del Estado (o en virtud de una obligación legal).

Todo sujeto alcanzado por la LPDP tiene el deber de confidencialidad de los datos personales objeto de tratamiento (art. 10 de la LPDP) y podrá ser relevado del deber de secreto únicamente por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública.

Sin embargo, no se exige el consentimiento para la cesión de datos personales entre dependencias de los órganos del Estado en forma directa, en la medida del cumplimiento de sus respectivas competencias (art. 11, inc. 3.C LPDP). Lo mismo sucede cuando se trate de datos personales relativos a la salud y sea necesario por razones de salud pública, de emergencia, etc. en tanto se preserve la identidad de los titulares de los datos mediante mecanismos de disociación adecuados.



REUTERS/Pawel Kopczynski

exclusively be that that is necessary for the purposes desired; such processing cannot be extended to other personal data not strictly necessary for said purpose. When the need for that data is over, the data must be destroyed or anonymised.

Finally, article 17 of LPDP establishes specific cases where public database administrators or users are permitted to reject access, rectification or suppression of personal data for the protection of national defense, public order and public safety or the protection of the rights and interests of third parties.

El tratamiento de los datos personales deberá llevarse a cabo en todo momento respetando los principios de licitud, transparencia, limitación de la finalidad (en este caso, salvaguardar los intereses vitales/esenciales de las personas físicas), principio de exactitud y el principio de minimización de datos. Sobre este último aspecto hay que hacer referencia expresa a que los datos tratados habrán de ser exclusivamente los necesarios para la finalidad pretendida, sin que se pueda extender dicho tratamiento a otros datos personales no estrictamente necesarios para dicha finalidad. Cuando finalice la necesidad de contar los datos personales, éstos deberán ser destruidos o anonimizados.

Por último, el art. 17 de la LPDP establece supuestos específicos que le permiten a los responsables o usuarios de bases de datos públicos denegar el acceso, rectificación o la supresión de datos personales. Estos son en función de la protección de la defensa de la Nación, del orden y la seguridad públicos, o de la protección de los derechos e intereses de terceros.

REUTERS/Dado Ruvic

BRAZIL

Brazil's General Data Protection Law sought to establish a balance and harmony between access to information and the protection of citizens' personal data under the guardianship of the public administration and which has a constitutional provision regulated by Law No. 12,527/2011 (Access to Information Act – "LAI", in Portuguese) having limits on the prohibition of providing personal data by the Public Authorities. Therefore, it is necessary to harmonise the principles of data protection and transparency, which are intrinsically connected and have limitations.

According to the Brazilian General Data Protection Act, the processing of personal data shall be done in compliance with its public purpose in the public interest, in order to perform legal functions or perform legal powers of the public service, provided that they:

- Communicate the situations in which, in the exercise of their regulatory powers, they carry out the processing of personal data, providing clear and updated information on the legal basis, purpose, procedures and practices used to carry out these activities in an easily accessible means of communication, preferably on their web pages; and
- appoint a data protection officer when personal data processing operations are carried out.

During the Covid-19 pandemic, the Brazilian Government issued a Provisional Remedy (MP 959/20), which imposed on telecommunications companies the obligation to provide the Brazilian Institute of Geography and Statistics with a structured list of the names, telephone numbers and addresses of their customers. However, the Supreme Federal Court of Brazil flatly suspended the Provisional Remedy, arguing that personal data "comprises (...) the scope of protection of constitutional clauses guaranteeing individual freedom, privacy and the free development of personality". In this line, and warning that the Provisional Remedy lacks further justification as to the purpose of the processing, as well as the indication of safeguard mechanisms for the processing of shared data, the decision reinforces the relevance of the issue of personal data protection, even more so in the pandemic context in which data collection tends to be justified generically.

BRASIL

La Ley General de Protección de Datos de Brasil buscó establecer un equilibrio y armonía entre el acceso a la información y la protección de los datos personales de los ciudadanos bajo la tutela de la administración pública y que tiene una disposición constitucional regulada por la Ley nº 12.527/2011 (Ley de Acceso a la Información - LAI) teniendo límites en la prohibición de proporcionar datos personales por parte de los Poderes Públicos. Por lo tanto, es necesario armonizar los principios de protección de datos y la transparencia, que están intrínsecamente conectados y tienen limitaciones.

De acuerdo con la Ley General de Protección de Datos brasileña, el tratamiento de datos personales se hará en cumplimiento de su finalidad pública en beneficio del interés público, con el fin de realizar funciones legales o desempeñar atribuciones legales del servicio público, siempre que:

- Comuniquen las situaciones en las que, en el ejercicio de sus capacidades normativas, lleven a cabo el tratamiento de datos personales, proporcionando información clara y actualizada sobre la base jurídica, la finalidad, los procedimientos y las prácticas utilizadas para llevar a cabo estas actividades en un medio de comunicación de fácil acceso, preferiblemente en sus páginas web; y
- nombren a un responsable de la protección de datos cuando se realicen operaciones de tratamiento de datos personales.

Durante la pandemia de Covid-19, el Gobierno brasileño emitió una medida provisional (MP 959/20), que imponía a las empresas de telecomunicaciones la obligación de proporcionar al Instituto Brasileño de Geografía y Estadística una lista estructurada con los nombres, números de teléfono y direcciones de sus clientes. Sin embargo, el Supremo Tribunal Federal de Brasil suspendió de plano la vigencia de la Medida Provisional argumentando que los datos personales "comprenden (...) el ámbito de protección de las cláusulas constitucionales que garantizan la libertad individual, la intimidad y el libre desarrollo de la personalidad". En esta línea, y advirtiendo que la Medida Provisional carece de una mayor justificación en cuanto a la finalidad del tratamiento, así como de la indicación de mecanismos de salvaguarda para el tratamiento de los datos compartidos, la decisión refuerza la relevancia del tema de la protección de los datos personales, más aún en el contexto pandémico en el que la recogida de datos tiende a justificarse genéricamente.

CANADA

The Act: The Act does not apply to a public body or to information held on behalf of a public body.

A person carrying on an undertaking may, without the consent of the person concerned, communicate personal information relating to that person, to specified individuals in specified circumstances:

- For the purpose of prosecution or prevention, detection or suppression of crime or legal offenses
- Collection for a program operated by a public agency.
- When the information must be communicated because of the urgency of a situation that threatens the life, health or safety of the person concerned.
- To prevent an act of violence, including suicide.

PIPEDA: PIPEDA does not apply to personal information handled by federal government organisations listed in the Privacy Act, or to provincial or territorial governments and their agents but there may be instances where an organisation that collects, uses or discloses personal information is required to disclose that information to a government institution to comply with a subpoena, court order or warrant.

CANADÁ

La Ley: La Ley no se aplica a un organismo público ni a la información que se tiene en nombre de un organismo público.

Una persona que lleve a cabo una empresa puede, sin el consentimiento de la persona afectada, comunicar información personal relativa a esa persona, a individuos específicos en determinadas circunstancias:

- Para fines de enjuiciamiento o prevención, detección o represión de delitos o infracciones legales
- Recabamiento para un programa gestionado por un organismo público.
- Cuando la información deba ser comunicada por la urgencia de una situación que amenace la vida, la salud o la seguridad de la persona afectada
- Para prevenir un acto de violencia, incluido un suicidio.

PIPEDA: PIPEDA no se aplica a la información personal manejada por las organizaciones del gobierno federal enumeradas en la Ley de Privacidad, ni a los gobiernos provinciales o territoriales y sus agentes, pero puede haber casos en los que una organización que recoge, utiliza o divulga información personal se vea obligada a revelar esa información a una institución gubernamental para cumplir con una citación, orden judicial o mandamiento.

Organisations are authorised (but not required) to disclose personal information without consent to a government institution or investigative agency for purposes such as national security, national defense or terrorism deterrence, law enforcement or in connection with a suspected money laundering offense.

The Privacy Act: The Privacy Act sets limits on the use of personal information by government institutions. In general, the government institution may not use personal information for any purpose other than the reason it was obtained or collected by the institution, unless it specifically obtains consent to do so. However, there are certain exceptions to this rule.

- Where specific legislation or regulation authorises such specific use.
- For any purpose where the public interest in the use of the information clearly outweighs any invasion of privacy that might result from the use, or the use clearly benefits the individual to whom the information relates.

These two exceptions could provide government institutions with the ability to use personal data under their control for "emergency" purposes.

Las organizaciones están autorizadas (pero no obligadas) a revelar información personal sin consentimiento a una institución gubernamental o a un organismo de investigación para fines como la seguridad nacional, la defensa nacional o la disuasión del terrorismo, la aplicación de la ley o en relación con un presunto delito de blanqueo de dinero.

La Ley de Privacidad: La Ley de Privacidad establece límites al uso de la información personal por parte de las instituciones gubernamentales. Y en general, la institución gubernamental no puede utilizar la información personal para ningún otro fin que no sea el motivo por el que fue obtenida o recopilada por la institución, a menos que obtenga específicamente el consentimiento para hacerlo. Sin embargo, hay ciertas excepciones a esta regla.

- Cuando una legislación o un reglamento específico autorice ese uso específico
- Para cualquier propósito en el que el interés público en el uso de la información supere claramente cualquier invasión de la privacidad que pudiera resultar del uso o el uso beneficie claramente al individuo al que se refiere la información.

Estas dos excepciones podrían proporcionar a las instituciones gubernamentales la capacidad de utilizar los datos personales bajo su control para fines de "emergencia".

REUTERS/Alessandro Bianchi

CHILE

The State collects a considerable amount of data that can be requested in the context of the right to petition through the Transparency Act (Law 20.285 on access to public information).

In the case of a public emergency, the State has been collecting data through the "mobility pass" requested to enter places and get in and out of the country.

COLOMBIA

Colombian privacy laws apply to both private and public institutions. Therefore, data protection rules are applicable to any personal data processing activity carried out by the State.

Although Colombian Privacy Laws have as their primary legal basis the prior consent of the data subject, Law 1581 of 2012 establishes certain exceptions to this general rule:

(a) Information required by a public or administrative entity in the exercise of its legal functions or by court order;

(b) Data of a public nature; or

(c) Cases of medical or health emergency.

In this sense, it is legal for Colombian authorities to collect or access personal information (including sensitive data) without the need to obtain the prior consent of the data subjects, based on these exceptions.

In addition, public entities must duly justify why their data processing activities will be based on these grounds and must be able to demonstrate full compliance with Colombian privacy laws.

FRANCE

Data protection legislation is applicable to any processing of personal data carried out by the State. That said, some parts of the FDPA specifically apply to processing carried out by certain authorities and/or the State, which falls outside the scope of the GDPR.

CHILE

El Estado recolecta un gran número de datos que pueden ser solicitados invocando el derecho de petición por medio de la Ley de Transparencia (Ley 20.285 Sobre acceso a la información pública).

En el caso de una emergencia pública el Estado ha recolectado datos por medio del "pase de movilidad" que se solicita para ingresar a lugares, entrar y salir del país.

COLOMBIA

Las Leyes de Privacidad Colombianas se aplican tanto a las instituciones privadas como a las públicas. Por lo tanto, son aplicables a cualquier actividad de tratamiento de datos personales realizada por el Estado.

Aunque las Leyes de Privacidad Colombianas tienen como principal base legal el consentimiento previo de los titulares, la Ley 1581 de 2012 establece ciertas excepciones a esta regla general cuando se trate de:

(a) Información requerida por una entidad pública o administrativa en el ejercicio de sus funciones legales o por orden judicial;

(b) Datos de carácter público; o

(c) Casos de emergencia médica o sanitaria.

En este sentido, es legal que las autoridades colombianas recolecten o accedan a información personal (incluyendo datos sensibles) sin necesidad de obtener el consentimiento previo de los titulares de los datos, con fundamento en estas excepciones.

Además, las entidades públicas deben justificar debidamente por qué sus actividades de tratamiento de datos se basarán en estos motivos y deben poder demostrar el pleno cumplimiento de las Leyes de Privacidad Colombianas.

FRANCIA

La legislación sobre protección de datos es aplicable a cualquier tratamiento de datos personales realizado por el Estado. Dicho esto, algunas partes de la FDPA se aplican específicamente al tratamiento llevado a cabo por determinadas autoridades y/o el Estado, que queda fuera del ámbito de aplicación del RGPD.

REUTERS/Darrin Zammit Lupi

Certain purposes and types of personal data processing activities are subject to stricter requirements, especially when the processing activities are carried out on behalf of the State and relate to public security or law enforcement (Articles 8, 31 and 32 of the FDPA).

These activities, whenever they involve the processing of personal data (regardless of the nationality, residence or capacity of the data subjects), are subject to the following protection measures:

- The processing must be authorised by an order of the competent minister (i.e. an executive authorisation), which must set out the purpose and conditions of the processing.
- The processing must be the subject of a reasoned opinion from the CNIL (the CNIL's opinion is published, in whole or in part, together with the order authorising the processing, but is not binding).
- When the conditions of the processing change or evolve (e.g. new purpose, new data processed), the authorisation must be renewed. A judicial authorisation is not required. The CNIL must be notified by the State in case the processing in question changes or stops.

Each processing operation has been authorised by an order of the Prime Minister. The CNIL has issued its opinions on the intended processing and is since then reviewing the conditions of the processing in accordance with the applicable data protection laws in order to issue an updated opinion.

Determinados fines y tipos de actividades de tratamiento de datos personales están sujetos a requisitos más estrictos, especialmente cuando las actividades de tratamiento se llevan a cabo en nombre del Estado y se refieren a la seguridad pública o a la aplicación de la ley (artículos 8, 31 y 32 de la FDPA).

Estas actividades, siempre que impliquen el tratamiento de datos personales (independientemente de la nacionalidad, residencia o capacidad de los interesados), están sujetas a las siguientes medidas de protección:

- El tratamiento debe estar autorizado por una orden del ministro competente (es decir, una autorización ejecutiva), que debe establecer la finalidad y las condiciones del tratamiento.
- El tratamiento debe ser objeto de un dictamen motivado de la CNIL (el dictamen de la CNIL se publica, total o parcialmente, junto con la orden que autoriza el tratamiento, pero no es vinculante).
- Cuando las condiciones del tratamiento cambian o evolucionan (por ejemplo, nueva finalidad, nuevos datos tratados), la autorización debe renovarse. No se requiere una autorización judicial. La CNIL debe ser notificada por el Estado en caso de que el tratamiento en cuestión cambie o se detenga.

Cada tratamiento ha sido autorizado por una orden del Primer Ministro. La CNIL ha emitido sus dictámenes sobre los tratamientos previstos y, desde entonces, está revisando las condiciones del tratamiento de acuerdo con las leyes de protección de datos aplicables para emitir un dictamen actualizado.

SPAIN

Public entities and government institutions are subject to LOPDGDD and the GDPR and therefore, they can only process data in compliance with data protection regulations and within the scope of their powers. Generally, they process data in compliance with a law or for public interest purposes. Also, public entities and government institutions are subject to the Transparency Act, which ensures transparency in their activities and regulates the right to access to public information for all citizens.

Although they are granted with some privileges, they are also subject to the sanctions imposed by AEPD upon breach of the law. Particularly, they cannot be fined, but they can be warned and given instructions on how to comply with the law.

In states of emergency, they can access personal data always following the LOPDGDD and the GDPR. That is, they cannot "suspend" such laws. However, in these situations, different authorities or bodies can issue rules and regulations allowing data processing by these entities.

ESPAÑA

Las entidades públicas y cuerpos gubernamentales están sujetos a la LOPDGDD y al RGPD, por lo que solo pueden tratar datos personales en cumplimiento con lo previsto en la normativa de protección de datos y en el marco de sus competencias. En términos generales, tratan datos personales sobre la base del cumplimiento con una norma que las regula, o cuando concurre un interés público. Además, las entidades públicas y entidades gubernamentales están sujetas a la Ley de Transparencia que garantiza la transparencia en su actividad y regula el derecho de acceso de los ciudadanos a la información pública.

También están sujetos al régimen sancionador de la AEPD en caso de incumplimiento con la norma, si bien tienen ciertas prerrogativas a este respecto. Principalmente, no quedan sujetos a la imposición de multas, si no que pueden ser apercibidos y recibir indicaciones de cómo cumplir con la normativa.

En casos de emergencia pueden acceder a datos personales siempre que se cumpla con la LOPDGDD y el RGPD. Esto es, no tienen capacidad para "suspender" dichas normas, sin embargo, en dichas situaciones las autoridades o cuerpos pueden emitir leyes que den amparo al tratamiento de datos por estas entidades.

MEXICO

In the public sector, the law that governs the protection of personal data in Mexico is the General Law for the Protection of Personal Data in Possession of Obligated Parties, as well as the local laws that address the subject in each state of the Mexican Republic.

The General Law for the Protection of Personal Data establishes specific obligations for public entities when they obtain personal data from individuals. Pursuant to section 22, subsection VI, the State is exempt from obtaining the consent of the data subject when there is a public emergency that may involve harm to the data subject. In addition to this provision, there are no specific details to regulate public emergencies due to force majeure events.

URUGUAY

Law No. 18.331 governs all aspects related to personal data recorded in any medium that makes it subject to processing, and any later use of such data by private or public entities. Therefore, all data held by the State falls within this law, except for some cases provided for in section 3(B): "Safety of the State and its actions regarding criminal matters, investigations and crime punishment."

Another tool the law granted to the State with respect to data processing is the provision setting forth that the State is exempted from obtaining prior consent from the data subject whenever the data "is collected for branches of government to perform their own duties or as a result of a legal obligation."

MÉXICO

En el sector público, la ley que rige la protección de datos personales en México es la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, así como las leyes locales que abordan el tema en cada estado de la República Mexicana.

La Ley General de Protección de Datos Personales establece obligaciones específicas para los entes públicos cuando obtienen datos personales de particulares. De acuerdo con el artículo 22, fracción VI, el Estado está exento de obtener el consentimiento del titular de los datos personales cuando exista una emergencia pública que pueda implicar un daño para el titular. Además de esta disposición, no hay detalles específicos para regular las emergencias públicas por eventos de fuerza mayor.

URUGUAY

La ley 18.331 regula todo lo concerniente a datos personales registrados en cualquier soporte que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los ámbitos público o privado. Por lo cual se encuentran comprendidos todos los datos en posesión del Estado, exceptuando ciertos casos que se estipulan en el artículo 3 letra B: "seguridad del Estado y sus actividades en materia penal, investigación y represión del delito."

Otra herramienta que la ley brinda al Estado para su tratamiento de datos es la estipulación de que el mismo se encuentra excepcionado de necesitar consentimiento previo de los individuos cuando "se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal."

REUTERS/Dado Ruvic

IMPLICIT CONSENT / CONSENTIMIENTO TÁCITO

7

How is consent regulated under the law? Does implicit consent exist? If so, how is it regulated?

¿Cómo se aborda el consentimiento en la ley? ¿Existe el consentimiento tácito? Si es así, ¿cómo se aborda?

ARGENTINA

The LPDP establishes that data processing is legal when the data subject has given their free, express and informed consent in writing or other similar means, depending on the circumstances. The law does not provide for implicit consent by data subjects for the use of their data.

Furthermore, the LPDP establishes that data subjects shall be clearly and expressly informed about the purposes for which their data will be processed, who the recipients of their data will be, if they would be able to access the data and exercise their right to access, rectify and suppress data, the consequences of providing the data, etc.

However, it also states that express consent will not be needed when (i) data is obtained from unrestricted publicly available sources; (ii) data is collected for branches of government to perform their own duties; (iii) data comes from lists only containing the name, ID, tax payer or retirement identifications, occupation, date of birth and address; (iv) data derives from a contractual, scientific or professional relationship with the data subject and is needed for the development and performance of such relationship; and (v) data comes from transactions of financial institutions and the information received by their clients under section 39 of Law No. 21.526.

ARGENTINA

La LPDP establece que el tratamiento de datos es lícito cuando el titular hubiere prestado su consentimiento libre, expreso e informado, el cual deberá ser prestado por escrito o por otro medio que se le equipare, de acuerdo a las circunstancias. La normativa no prevé la posibilidad de que los titulares consientan tácitamente el uso de los datos.

Más aún, la LPDP dispone que deberá informarse a sus titulares en forma clara y expresa la finalidad para la cual serán tratados los datos, quiénes pueden ser los destinatarios de tales datos, la posibilidad del titular de acceder a tales datos y de ejercer los derechos de acceso, rectificación y supresión de datos, las consecuencias de proporcionar tales, datos, etc.

No obstante, se prevé que el consentimiento expreso no será necesario cuando (i) los datos se obtengan de fuentes de acceso público irrestricto; (ii) se recaben para el ejercicio de funciones propias de los poderes del Estado; (iii) se trate de listados cuyos datos se limiten a nombre, DNI, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio; (iv) deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento; y (v) se trate de operaciones que realicen las entidades

It should be noted that the fact that the law etsablishes some exceptions to the consent requirement, this does not mean that in all cases data could be processed even if the data subject objected to it. What the law does in these cases is to assume consent was given, but this does not prevent the data subject from objecting to the processing of their data.

It is important to highlight that, under Resolution 4/2019, the database administrator shall ensure that the person giving the consent is the actual data subject of the required data and not someone else, using effective identity validation mechanisms.

financieras y de las informaciones que reciban de sus clientes conforme las disposiciones del art. 39 de la Ley N° 21.526.

Debe advertirse que el hecho de que la ley establezca algunas excepciones al requisito del consentimiento no implica per se que en todos los casos esos datos puedan tratarse aun mediando oposición por parte del titular, ya que lo que la ley hace en los supuestos de excepción es presumir ese consentimiento, lo que no obsta a que aún en esas situaciones el titular pueda tener derecho en algunas circunstancias a oponerse al tratamiento de sus datos.

Es importante resaltar que en virtud de la Resolución AAIP 4/2019, el responsable de la base de datos debe acreditar que quien haya prestado tal consentimiento sea efectivamente el titular de los datos requeridos y no otra persona, esto es, que cuente con mecanismos de validación de identidad eficaces.

BRAZIL

For consent to be valid under the Brazilian General Data Protection Law, it must be a free, informed and unequivocal statement by which the data subject agrees to the processing of personal data for a specific purpose and shall be given in writing or by other means that can demonstrate the statement of the data subject's will.

However, in some situations, the requirement of consent is waived for such data that the data subject has manifestly made public, safeguarding the rights of the data subject and the principles provided for in the Law.

BRASIL

Para que el consentimiento sea válido según la Ley General de Protección de Datos brasileña debe ser una manifestación libre, informada e inequívoca por la que el interesado acepta su tratamiento de datos personales para una finalidad determinada, y se dará por escrito o por otro medio que pueda demostrar la manifestación de la voluntad del interesado.

No obstante, en algunas situaciones se prescinde del requisito del consentimiento para los datos que el interesado haya hecho públicos de forma manifiesta, salvaguardando los derechos del interesado y los principios previstos en la Ley.

CANADA

The law: Requires valid consent to collect, use and disclose personal information about individuals. Individuals must be informed of the purpose of the collection, the use or uses to which the information collected will be put, the categories of individuals who will have access to it within the company, where the file will be kept, and the individual's rights of access and rectification. Consent must be specific to each use of personal information. Express consent is the norm, and "implied" (i.e., tacit) consent is acceptable only under certain conditions. For example, implied consent cannot be invoked for the processing of sensitive personal information. Express consent is required in these circumstances.

- Under **PIPEDA:** organisations must obtain meaningful consent for the collection, use and disclosure of personal information. Consent is considered meaningful when individuals receive clear information that explains what organisations are doing with their information (Annex 1, Principle 3). Consent can be express or implied (in Canadian privacy legislation, the term is "implied"). Whether express or implied consent is permitted depends on the sensitivity of the information, the potential risk of harm to the individual if the information is misused, and the individual's reasonable expectations.
- However, there are also circumstances in which personal information may be collected, used or disclosed without the individual's consent (section 7). It is important to note that this section uses permissive language. Therefore, organisations are permitted to collect, use or disclose personal information without consent in the circumstances outlined, but are not required to do so.
- **Privacy Act:** does not require the individual's consent for the institution to collect, use or disclose his or her personal information. Instead, institutions must only use personal information consistent with the purposes for which it was collected (with a number of exceptions). However, an individual may consent to any other use. In this sense, consent constitutes an exception to the restrictions imposed on institutions subject to the Privacy Act. The Privacy Act does not distinguish between express and implied consent.

CANADÁ

La ley: Exige un consentimiento válido para recabar, utilizar y divulgar la información personal de los individuos. Las personas deben ser informadas del objeto de la recabación, del uso o usos que se dará a la información recabada, de las categorías de personas que tendrán acceso a ella dentro de la empresa, del lugar donde se conservará el fichero y de los derechos de acceso y rectificación del individuo. El consentimiento debe ser específico para cada uso de la información personal. El consentimiento expreso es la norma, y el consentimiento "implícito" (es decir, tácito) sólo es aceptable en determinadas condiciones. Por ejemplo, el consentimiento implícito no puede ser invocado para el tratamiento de información personal sensible. El consentimiento expreso es necesario en estas circunstancias

- En virtud de la **PIPEDA**: las organizaciones deben obtener un consentimiento significativo para la recabación, uso y divulgación de información personal. Se considera que el consentimiento es significativo cuando los individuos reciben información clara que explica lo que las organizaciones están haciendo con su información (anexo 1, principio 3). El consentimiento puede ser expreso o tácito (en la legislación canadiense sobre privacidad, el término es "implícito"). El hecho de que se permita el consentimiento expreso o implícito depende de la sensibilidad de la información, el riesgo potencial de daño para el individuo si la información se utiliza de forma indebida y las expectativas razonables del individuo.
- Sin embargo, también hay circunstancias en las que se puede recoger, utilizar o divulgar información personal sin el consentimiento de la persona (sección 7). Es importante señalar que esta sección utiliza un lenguaje permisivo. Por lo tanto, las organizaciones están autorizadas a recoger, utilizar o revelar información personal sin consentimiento en las circunstancias señaladas, pero no están obligadas a hacerlo.
- **La Ley de Privacidad:** no exige el consentimiento del individuo para que la institución recabe, utilice o divulgue su información personal. Por el contrario, las instituciones sólo deben utilizar la información personal en consonancia con los fines para los que se recogió (con una serie de excepciones). Sin embargo, una persona puede dar su consentimiento para cualquier otro uso. En este sentido, el consentimiento constituye una excepción a las restricciones impuestas a las instituciones sujetas a la Privacy Act. La Privacy Act no distingue entre consentimiento expreso y tácito.

CHILE

Law No. 19.628 (on protection of private life) establishes that personal data processing can only be done whenever this is authorised by the law or other legal provisions, or the data subject expressly gives their consent. In this case, the data subject shall give their consent with an understanding of the purpose for the storage of their data and the potential disclosure to the public. The data subject's consent must be given in writing.

Similarly, the law provides for a purpose principle by means of which the data gathered can only be used for the purposes for which it was collected.

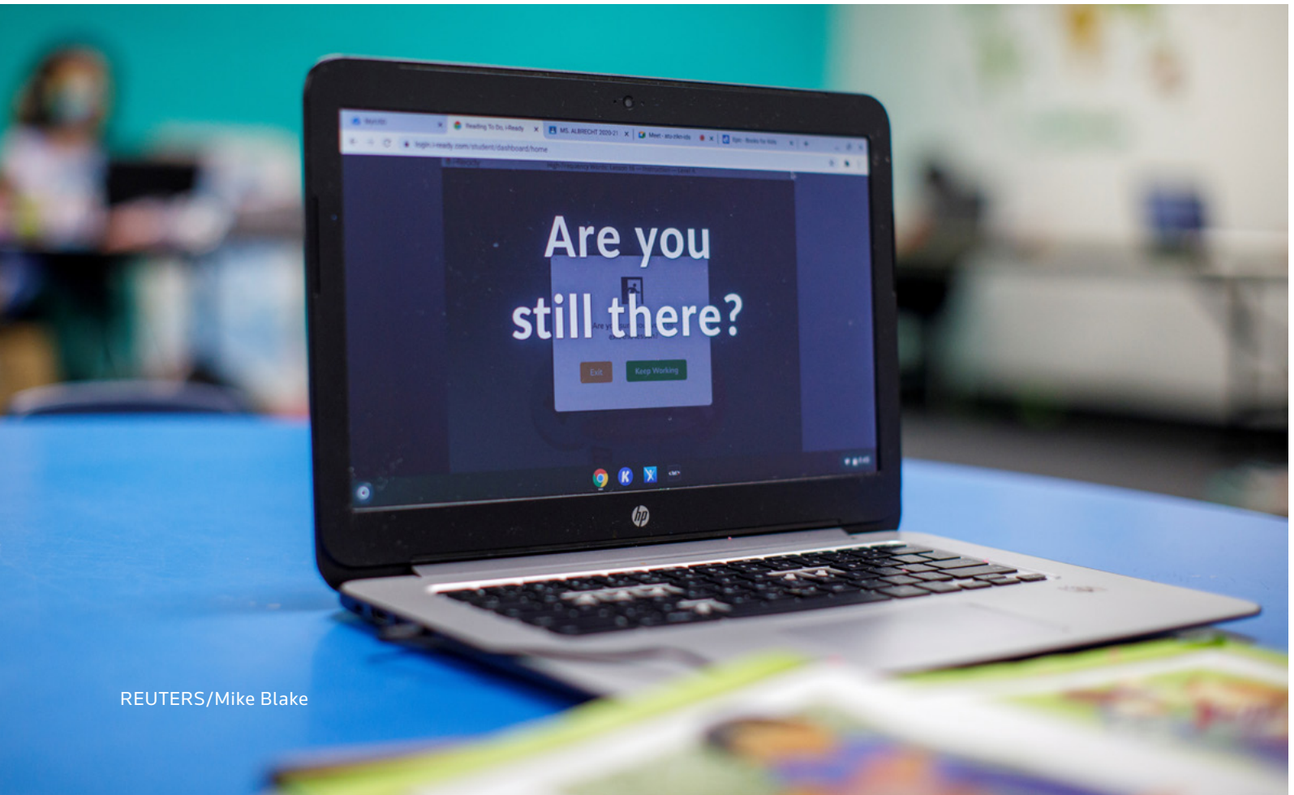
Exceptionally, express consent will not be required whenever the data is collected or comes from publicly available sources; is of an economic, financial, or commercial nature; is contained in a list of a group of individuals sharing their background information, such as belonging to such group, profession or occupation, levels of education, address, or date of birth; or is needed for direct response marketing communications or direct purchases and sales of goods and services.

CHILE

La ley 19.628 (Sobre Protección de la Vida Privada) establece que el tratamiento de los datos personales únicamente puede realizarse cuando la misma ley, u otras disposiciones legales lo autoricen, o el titular de dicha información consienta expresamente en ello. En el último caso, la persona autorizante debe prestar su consentimiento con conocimiento del propósito del almacenamiento de dicha información, así también como la posible comunicación de ella al público. La autorización del titular de tal información debe constar por escrito.

De igual forma, el mismo cuerpo legal consagra un principio de finalidad en virtud del cual, la información recolectada únicamente puede ser utilizada para los objetivos para los cuales fueron recolectados.

De manera excepcional, no será necesaria esta autorización expresa en aquellos casos en que la información sea recolectada o provenga de fuentes accesibles al público, cuando dichos datos sean de carácter económico, financiero, bancario, comercial, se contengan en listados relativos a una categoría de personas que se limiten a indicar antecedentes tales como la pertenencia del individuo a ese grupo, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento, o sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios.



REUTERS/Mike Blake

COLOMBIA

Consent is the main legal basis for the processing of personal data in Colombia and must be secured prior to processing, through a clear statement and a positive act of the data subject. The data controller must provide certain minimum information to data subjects when requesting their consent (e.g., their rights under Colombian privacy laws, the scope and purposes for the processing, among others).

In order to comply with the provisions of section 9 of Law 1581 of 2012, data controllers must establish mechanisms to secure prior consent from data subjects or whoever has authorisation ensuring their subsequent consultation. These mechanisms may be predetermined through technical means that facilitate the automated manifestation to the data subject.

It shall be understood that the consent complies with these requirements when it is provided (i) in writing, (ii) orally or (iii) through an unequivocal conduct of the data subject that allows a reasonable conclusion that they provided their consent.

However, in no case may silence be equated to unequivocal conduct, and consent for the processing of sensitive data (e.g., health data, biometric data, or any type of data that may cause discrimination to the data subject) cannot be provided through unequivocal conduct.

COLOMBIA

El consentimiento es la base legal principal para el tratamiento de datos personales en Colombia y debe ser solicitado antes del tratamiento, mediante una declaración clara y un acto positivo del titular. El responsable del tratamiento debe proporcionar cierta información mínima a los titulares de los datos al momento de solicitar su consentimiento (por ejemplo, sus derechos bajo las Leyes de Privacidad Colombianas, el alcance y los fines para el tratamiento, entre otros).

Para dar cumplimiento a lo establecido en el artículo 9 de la Ley 1581 de 2012, los responsables del tratamiento deben establecer mecanismos para obtener el consentimiento previo de los titulares de los datos o de quien esté legitimado que garanticen su consulta posterior. Estos mecanismos podrán ser predeterminados a través de medios técnicos que faciliten la manifestación automatizada al titular de los datos.

Se entenderá que la autorización cumple con estos requisitos cuando se preste (i) por escrito, (ii) oralmente o (iii) mediante una conducta inequívoca del titular que permita concluir razonablemente que otorgó su consentimiento.

No obstante, en ningún caso el silencio podrá asimilarse a una conducta inequívoca, y el consentimiento para el tratamiento de datos sensibles (por ejemplo, datos de salud, datos biométricos o cualquier tipo de datos que puedan causar discriminación al titular) no podrá suministrarse mediante conductas inequívocas.

FRANCE

The GDPR and the FDPA (which refers to the GDPR) define consent as *"any freely given, specific, informed and unambiguous indication by which the data subject signifies his agreement, by a statement or a clear affirmative act, to the processing of personal data relating to him"* (Articles 6 and 7 of the GDPR and Article 5 of the FDPA). The GDPR imposes several conditions for consent to be considered valid and must be:

- **Free:** consent must not be forced or influenced.
- **Specific:** consent must relate to a single processing operation, for a specific purpose. Thus, for a processing operation involving several purposes, individuals must be able to give their consent independently for any of these purposes.

FRANCIA

El GDPR y la FDPA (que remite al GDPR) definen el consentimiento como *"toda indicación libre, específica, informada e inequívoca por la que el interesado manifiesta su conformidad, mediante una declaración o un acto positivo claro, con el tratamiento de datos personales que le conciernen"* (artículos 6 y 7 del GDPR y artículo 5 de la FDPA). El GDPR impone varias condiciones para que el consentimiento se considere válido y debe ser:

- **Libre:** el consentimiento no debe ser forzado ni influenciado.
- **Específico:** el consentimiento debe corresponder a una única operación de tratamiento, para un fin específico. Por lo tanto, para una operación de tratamiento que incluya varios fines, las personas

- **Informed:** to be valid, consent must be accompanied by certain information communicated to the individual before they give their consent (e.g. the identity of the processor, the category of data collected, etc.).
- **Unambiguous:** consent must be given by a clear statement or other positive act. There can be no ambiguity as to the expression of consent. For example, "pre-ticked" boxes are prohibited.

The following safeguards to consent can be noted:

- **Right of withdrawal:** the individual must be able to withdraw consent at any time, through a simple and equivalent method to that used to collect it (e.g., if consent was given online, it must be possible to withdraw it online as well).
- **Proof of consent**: the controller must be able to demonstrate at all times that the individual has given valid consent.
- **Explicit consent:** the importance of obtaining explicit consent is recalled several times by the CNIL, in particular regarding cookie practices. Indeed, consent must be given by a positive action of the data subject, who has been previously informed of the consequences of their choice and who has the means to accept, refuse and withdraw their consent. Appropriate systems must therefore be put in place to collect consent in a practical way that allows Internet users to benefit from user-friendly solutions. Furthermore, the CNIL regularly reminds that consent to general terms and conditions of use cannot be a valid way of collecting consent.

In addition, under the FDPA, a minor may consent on their own to the processing of their personal data in connection with the direct provision of information society services from the age of 15. Below this age, the processing of data for the direct provision of information society services (e.g., the creation of an Instagram account) is lawful only if consent is given jointly by the minor and the minor's legal guardian.

deben poder dar su consentimiento de forma independiente para cualquiera de estos fines.

- **Informado:** para ser válido, el consentimiento debe ir acompañado de cierta información comunicada a la persona antes de que dé su consentimiento (por ejemplo, la identidad del encargado del tratamiento, la categoría de los datos recogidos, etc.)
- **Sin ambigüedades:** el consentimiento debe darse mediante una declaración clara u otro acto positivo. No puede quedar ninguna ambigüedad en cuanto a la expresión del consentimiento. Por ejemplo, están prohibidas las casillas "marcadas previamente".

Se pueden señalar las siguientes garantías al consentimiento:

- **Derecho de retirada:** la persona debe poder retirar el consentimiento en cualquier momento, a través de un método sencillo y equivalente al utilizado para obtenerlo (por ejemplo, si el consentimiento se ha dado en línea, debe ser posible retirarlo también en línea).
- **Prueba del consentimiento:** el responsable del tratamiento debe poder demostrar en todo momento que la persona ha dado su consentimiento válido.
- **Consentimiento explícito:** la importancia de obtener un consentimiento explícito es recordada varias veces por la CNIL, en particular en lo que respecta a las prácticas de las cookies. En efecto, el consentimiento debe otorgarse mediante una acción positiva del interesado, que ha sido informado previamente de las consecuencias de su elección y que dispone de los medios para aceptar, rechazar y retirar su consentimiento. Por lo tanto, deben implementarse sistemas adecuados para recoger el consentimiento de una manera práctica que permita a los usuarios de Internet beneficiarse de soluciones fáciles de usar. Asimismo, la CNIL recuerda periódicamente que el consentimiento a las condiciones generales de uso no puede ser una forma válida de recoger el consentimiento.

Además, según la FDPA, un menor puede consentir por sí solo el tratamiento de sus datos personales en relación con la prestación directa de servicios de la sociedad de la información a partir de los 15 años. Por debajo de esta edad, el tratamiento de datos para la prestación directa de servicios de la sociedad de la información (por ejemplo, la creación de una cuenta de Instagram) sólo es lícito si el consentimiento lo dan conjuntamente el menor y el tutor legal de éste.

SPAIN

Under the LOPDGDD, in line with the GDPR, consent means *"any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."*

Consent is one of the six legitimising grounds under the GDPR for personal data processing; it cannot be implicit, but rather it must always be express. For it to be valid, the GDPR requires that consent be:

- Free: consent must not be forced or influenced, and the data subject must be able to withdraw it at any time.
- Specific: consent must relate to a single processing operation, for a specified purpose.
- Informed: to be valid, consent must be accompanied by certain information communicated to the individual before they give their consent (e.g. the identity of the processor, the category of data collected, etc.).
- Unambiguous: consent must be given by a clear statement or other positive act. There can be no ambiguity as to the expression of consent. For example, "pre-ticked" boxes are prohibited.

Also, consent is associated with certain rights/guarantees, summarised as follows:

- Right of withdrawal: the individual must be able to withdraw consent at any time, through a simple and equivalent method to that used to collect it (e.g., if consent was given online, it must be possible to withdraw it online as well).
- Proof of consent: the controller must be able to demonstrate at all times that the individual has given valid consent.
- Explicit consent: consent must be given by a positive action of the data subject, who has been previously informed of the consequences of their choice and who has the means to accept, refuse and withdraw their consent. Appropriate systems must therefore be put in place to validly collect consent.

In addition, the LOPDGDD establishes the following in relation to consent:

ESPAÑA

La LOPDGDD, en línea con el RGPD, entiende por consentimiento *"toda manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen"*.

El consentimiento es una de las seis bases legitimadoras reconocidas bajo el RGPD en el que se puede basar el tratamiento de datos personales; no puede otorgarse de forma tácita, sino que debe ser siempre expreso. Para que éste sea válido, el RGPD exige que el consentimiento sea:

- Libre: el consentimiento no debe ser forzado o influenciado y se debe poder revocar en todo momento;
- Específico: el consentimiento debe referirse a un único tratamiento de datos, a una finalidad en particular;
- Informado: para que sea válido, el consentimiento debe ir acompañado de determinada información comunicada a la persona antes de que otorgue su consentimiento (por ejemplo, la identidad del responsable del tratamiento, la categoría de los datos recogidos, etc.); e
- Inequívoco: el consentimiento debe otorgarse mediante una declaración clara u otra acción afirmativa. No puede existir ambigüedad alguna en cuanto a la expresión del consentimiento. Por ejemplo, están prohibidas las casillas "pre-marcadas".

Además, el consentimiento lleva asociadas una serie de garantías/derechos (en resumen):

- Derecho a revocar el consentimiento: la persona debe poder retirar su consentimiento en cualquier momento, a través de un método sencillo y equivalente al utilizado para otorgarlo (por ejemplo, si el consentimiento se ha dado de forma telemática, debe ser posible retirarlo telemáticamente);
- Prueba del consentimiento: el responsable del tratamiento debe poder demostrar en todo momento que la persona ha otorgado su consentimiento; y
- Consentimiento explícito / expreso: el consentimiento debe otorgarse mediante una acción afirmativa del interesado, que deberá haber

- For a processing operation involving several purposes, individuals must be able to give their specific and unambiguous consent independently for any of these purposes.
- Performance of an agreement cannot be subject to the individual's consenting to data processing for purposes unrelated to the preservation, development and control of the contractual relationship.
- As a general rule, data protection consent shall only be valid if given by individuals over the age of 14. Below that age, consent will only be valid if given jointly with their parents or guardians.

Consent is governed by sections 6 and 7 of the LOPDGDD and 4(11), 7 and 8 of the GDPR.

MEXICO

The processing of personal data requires the consent of the data subject, unless such processing falls under one of the exceptions specifically set forth in the laws and regulations. Some of the exceptions to consent are: a) when the personal data is contained in publicly available sources; b) when the personal data is anonymised; c) when the personal data is processed for the purpose of fulfilling obligations arising from a legal relationship between the data subject and the controller; among others.

sido informado previamente de las consecuencias de su elección y debe disponer de los medios para aceptar, rechazar y retirar el consentimiento. Por lo tanto, las organizaciones deben implementar sistemas adecuados para recoger el consentimiento de forma legítima.

Además, la LOPDGDD ha matizado lo siguiente en torno al consentimiento:

- Cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades, será preciso que conste de manera específica e inequívoca que dicho consentimiento se otorga para cada una de ellas;
- No podrá supeditarse la ejecución del contrato a que el afectado consienta el tratamiento de los datos personales para finalidades que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual; y
- Como regla general, solo serán válidos los consentimientos otorgados a efectos de protección de datos por mayores de 14 años. Serán válidos los de menores de 14 años si consta el consentimiento del titular de la patria potestad o tutela.

El consentimiento se regula en los artículos 6 y 7 LOPDGDD y 4(11), 7 y 8 RGPD

MÉXICO

El tratamiento de datos personales requiere el consentimiento del interesado, a menos que dicho tratamiento esté comprendido en una de las excepciones específicamente establecidas en las leyes y reglamentos. Algunas de las excepciones al consentimiento son: a) cuando los datos personales estén contenidos en fuentes de acceso público; b) cuando los datos personales estén anonimizados; c) cuando los datos personales se traten con el fin de cumplir las obligaciones derivadas de una relación jurídica entre el interesado y el responsable del tratamiento; entre otras.

REUTERS/Evgenia Novozhenina

URUGUAY

Informed consent is one of the main pillars of the law. Along with the protection of processed data, this is one of the two fundamental rights that data controllers must respect. Informed consent must be prior to the data processing and, upon any change in the terms and conditions governing the data processing or disclosure, such change must be notified to the data subject for them to give their consent.

Section 9 of the law provides for the prior and informed consent principle, as well as its exceptions, and establishes that consent must be "**expressly** and clearly" given.

URUGUAY

En la ley, el consentimiento informado es tomado como uno de los principios pilares de la misma, ya que junto con la protección de los datos que son tratados, son los dos hechos fundamentales que quien trate los datos de un individuo debe cerciorarse. El consentimiento informado debe ser previo al inicio del tratamiento de datos, y en caso de modificarse alguna cláusula que regule el tratamiento o la comunicación de datos, la misma debe ser notificada al propietario de los datos para que brinde su consentimiento.

El artículo 9 de la ley, regula el principio del consentimiento informado previo, así como sus excepciones, y establece que el mismo "deberá figurar en forma **expresa** y destacada"

REUTERS/Mike Blake

THOMSON REUTERS FOUNDATION

TrustLaw