

Protección de datos

Con fecha 30 de noviembre de 2024, el Ministerio de Justicia y Derechos de Perú aprobó mediante el Decreto Supremo 016-2024-JUS un nuevo [Reglamento de la Ley 29733 de Protección de Datos Personales](#).

El documento permitirá que el país cuente con un marco normativo moderno y sólido que garantice una adecuada tutela de los derechos de los ciudadanos frente a los riesgos generados para los datos personales a partir de las nuevas tecnologías digitales.

Entre otras cuestiones, introduce novedades relativas a las obligaciones en caso de que se den incidentes de seguridad, a la figura del Oficial de Datos Personales, a la portabilidad de los datos o a la implementación de nuevas infracciones.

El Reglamento está alineado con la Directiva Europea de Protección de Datos y entrará en vigor el 30 de marzo de 2025. Las obligaciones referidas a la designación del Oficial de Datos Personales entrarán en vigencia progresivamente a partir del 30 de noviembre de 2025, en base a las ventas anuales.

Por su parte, en Chile también se publicó recientemente la [Ley 21719 que regula la Protección y el Tratamiento de los Datos Personales](#), tras muchos años en periodo de consulta pública.

Entre las modificaciones más destacadas se incluyen la creación de la Agencia de Protección de Datos, la asignación de mayores obligaciones a los responsables del tratamiento de datos, el fortalecimiento de los derechos ARCO de los titulares y la implementación de sanciones significativas y efectivas, que pueden alcanzar hasta 20.000 UTM (US\$1.400.000 aproximadamente).

El nuevo texto de la ley entrará en vigor en un plazo de 24 meses.

Inteligencia artificial y Transformación Digital 2030

El mes de julio fue en Perú el de la promoción de las nuevas tecnologías. Comenzó con la aprobación de la **Ley que Promueve el Uso de la Inteligencia Artificial**, que tiene por objeto fomentar el uso de la inteligencia artificial en el marco del proceso nacional de transformación digital, teniendo en cuenta a la persona y el respeto de los derechos humanos, con el fin de fomentar el desarrollo económico y social del país, en un entorno seguro que garantice su uso ético, sostenible, transparente, replicable y responsable.

Desarrollo y uso de la inteligencia artificial

La ley contempla los siguientes principios para el desarrollo y uso de la inteligencia artificial:

Enfoque basado en riesgo

Debate plural para el desarrollo de políticas de regulación

Gobernanza de internet por parte del Estado, instituciones del sector privado y la sociedad civil

Valoración y promoción de la sociedad digital
Promoción y desarrollo ético para una inteligencia artificial responsable
Protección y promoción de la privacidad



Por otro lado, define los siguientes conceptos: inteligencia artificial, sistema basado en inteligencia artificial, tecnologías emergentes, algoritmo; y establece que la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros es la autoridad técnico-normativa competente a nivel nacional responsable de dirigir, evaluar y supervisar el uso y la promoción del desarrollo de la inteligencia artificial y las tecnologías emergentes, a través de las siguientes acciones:

- El desarrollo de la inteligencia artificial
- La formación de profesionales para el uso de la inteligencia artificial
- La creación y el fortalecimiento de la infraestructura digital
- El desarrollo de una infraestructura de datos
- La adopción de lineamientos éticos
- Un ecosistema de colaboración a nivel nacional e internacional

Política de Transformación Digital 2030

Por otro lado, días después se publicó la **Política Nacional de Transformación Digital al 2030**, con los siguientes objetivos: i) Garantizar el acceso inclusivo, seguro y de calidad al entorno digital a todas las personas; ii) Vincular la economía digital a los procesos productivos sostenibles del país; iii) Garantizar la disponibilidad de servicios públicos digitales inclusivos, predictivos y empáticos con la ciudadanía; iv) Fortalecer el talento digital en todas las personas; v) Consolidar la seguridad y confianza digital en la sociedad; y vi) Garantizar el uso ético y adopción de las tecnologías exponenciales y la innovación en la sociedad.

Protección de datos personales en Cuba

El pasado 14 de mayo el Parlamento cubano aprobó una ley para la protección y acceso de datos personales durante la quinta sesión extraordinaria.

Esta Ley establece los principios y definiciones fundamentales para garantizar a la persona natural el derecho a la protección de sus datos personales que consten en registros, ficheros, archivos, bases de datos, u otros medios técnicos de tratamiento de datos, físicos o digitales de carácter públicos o privados. Asimismo vela por el debido respeto a la intimidad personal y familiar, la propia imagen y voz, honor e identidad personal y contribuye a promover, fomentar y difundir una cultura sobre su protección en la sociedad. Entre los aspectos más significativos destacan los siguientes:

Datos personales

Según dispone la norma, son datos personales “la información concerniente a una persona natural identificada o identificable, que pueden llevar a su identificación”. A este respecto, la norma aclara que una persona es identificable, cuando su identidad puede determinarse directa o indirectamente a través de cualquier información.

Los datos personales que se protegen son aquellos relacionados con el sexo, edad, imagen, voz, género, identidad de género, orientación sexual, color de la piel, origen étnico, clasificación migratoria, discapacidad, creencias religiosas, principios ideológicos, estado civil, domicilio, datos médicos o de salud, económico-financieros, académicos, de empleo, judiciales y administrativos, entre otros; y cualquier información relacionada con estos datos, que pueden llevar a la identificación de una determinada persona, recopilados a partir de registros, ficheros, archivos y bases de datos.

Tratamiento de datos personales

La Ley dispone que existe tratamiento, en las operaciones y procedimientos sistemáticos que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relación, evaluación, bloqueo o destrucción, y en general, el procesamiento de datos personales, así como su cesión a terceros a través de comunicaciones, consultas, interconexiones y transferencias

Principios

La norma recoge los principios de calidad de los datos, finalidad, limitación de uso, legitimación, transparencia de la información, consentimiento, responsabilidad y legalidad.

Además, incluye otros principios como el llamado “participación individual”, según el cual solo podrán obtenerse datos personales con la participación individual de su titular, o el de “grados de reserva de la información” que exige ser titular de los datos personales a los que se accedan, o tener un interés legítimo acreditado para ello.

Consentimiento e información

Según exige la Ley, la persona que realice un tratamiento de datos personales ha de contar con el consentimiento de su titular, salvo excepciones.

A diferencia de las últimas tendencias en esta materia, el consentimiento puede ser tácito cuando, una vez informado el titular de los propósitos del tratamiento de sus datos, no manifiesta su voluntad en sentido contrario.

En todo caso habrá de informar al titular, de manera comprensible y pertinente, sobre la licitud y finalidad específica de los datos que se solicitan, y tiene derecho a conocer los destinatarios o clase de destinatarios de aquellos, el carácter facultativo u obligatorio de proporcionarlos, lugar de almacenamiento, a qué tratamiento pueden someterse, las consecuencias de aportarlos o no y de su inexactitud, así como su régimen de conservación.

Datos personales sensibles

La norma define los datos personales sensibles como aquellos cuyo uso indebido pueda dar lugar a discriminación, implique distinción lesiva a la dignidad humana o conlleve un riesgo grave para su titular. Entre esta categoría de datos, se incluyen: los datos que pueden revelar el sexo, género, identidad, identidad de género, orientación sexual, origen étnico y color de piel, el estado de salud, discapacidad, información genética, creencias religiosas e ideológicas, antecedentes policiales y penales.

Derechos de las personas sobre sus datos personales

Al igual que en resto de legislaciones, se reconoce el derecho que tiene el titular de acceso, rectificación, corrección, modificación y actualización de sus datos personales. Tendrá asimismo el derecho a la cancelación de sus datos personales (cuando considere que el fin para el que fueron obtenidos se ha cumplido, o que se hace un tratamiento inadecuado de los datos), y a la oposición al tratamiento de los mismos, cuando le pueda causar un daño o perjuicio, o afectar de forma significativa sus derechos o legítimos intereses.

Transferencias internacionales de datos

Se autoriza la transferencia de datos personales dentro del territorio nacional a solicitud de los responsables o encargados de tratamiento de datos, en los casos siguientes: a) Intercambio de datos de carácter médico, sanitario o de investigación cuando sea necesario para el tratamiento del titular, o por interés colectivo; b) cuando la transferencia de datos tenga como objeto la seguridad colectiva, el bienestar general, el respeto al orden público, y el interés de la defensa; c) en casos de transferencias bancarias, en cuanto a las transacciones respectivas; d) para facilitar el ejercicio del derecho al sufragio respecto a la conformación del registro de electores; y e) por otras razones que de manera significativa así lo ameriten.

Protección de datos en el resto de Latinoamérica

La mayor parte de países latinoamericanos han ido adaptando sus ordenamientos jurídicos a las nuevas tendencias normativas internacionales y tomando como ejemplo concreto el Reglamento (UE) 2016/679 relativo a la protección de datos de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos (Reglamento General de Protección de Datos o RGPD) comentado en [Progreso 7](#).

Tomando en consideración los países en los que la Fundación Microfinanzas BBVA tiene presencia, Panamá es un ejemplo de ello; con la [Ley 81](#) comentada en [Progreso 19](#) y que fue reglamentada por el [Decreto 285](#) de mayo de 2021.

Además, otros de estos países cuentan con normativa no tan reciente, si bien modificada parcialmente durante los últimos años, o con nueva normativa sectorial que contempla los últimos estándares internacionales. En este sentido, Chile cuenta con la [Ley 19628](#) cuya última modificación tuvo lugar en agosto de 2020; o Colombia, en el que rige la [Ley 1581-12](#), y donde recientemente fue aprobada la denominada Ley de borrón y cuenta nueva o de habeas data financiero, comentada en [Progreso 27](#). Y Perú, que a pesar de tener la [Ley 29733](#) del año 2011, ha ido adaptando su normativa a las nuevas realidades; ejemplo de ello es la [Resolución](#) del Ministerio de Justicia y Derechos Humanos sobre el Tratamiento de Datos Personales mediante Sistemas de Videovigilancia.

Por su parte, República Dominicana regula la protección de los datos personales en la [Ley 172-13](#) que no ha sufrido modificaciones sustantivas desde su aprobación y ya se comenta la necesidad de actualizar la norma.

Esta norma aprobada por el Parlamento cubano constituye la primera ley de la República en regular esta materia, refuerza las garantías institucionales a la intimidad de las personas.

Tratamiento de datos personales

El pasado 16 de abril el Ejecutivo uruguayo promulgó la Ley 19.948 por la que se aprueba el Protocolo de enmienda del Convenio 108 del Consejo de Europa, para la Protección de las Personas con respecto al Tratamiento de Datos Personales[1].

Con la promulgación de la Ley 19.948 se ratifica la adhesión de Uruguay al modelo de protección de datos personales seguido por los países europeos y constituye un hecho de relevancia considerando los hitos ya realizados por Uruguay en esta materia.

Protección de datos en Uruguay

Uruguay ha seguido la tendencia de la Unión Europea y es uno de los países de la Región con mayor regulación en materia de protección de datos personales. En el año 2008 aprobó la [Ley 18.331](#) sobre Protección de datos Personales en la que se reconocían expresamente una serie de principios que protegen este tipo de datos y se exigía la limitación de su uso por parte de terceros. Cinco años después y mediante la [Ley 19.030](#), Uruguay se convirtió en el primer país no europeo en incorporar a su ordenamiento jurídico el Convenio N° 108 junto con su Protocolo Adicional[2].

Estos antecedentes permitieron a Uruguay obtener en el año 2012, mediante la Decisión N° 2012/484/EU, el estatus de país adecuado en los términos de la Comisión Europea y así hacer posible los flujos transfronterizos de datos entre la Unión Europea y Uruguay sin restricciones adicionales.

Además, cabe destacar que a nivel regional europeo se aprobó el Reglamento (UE) 2016/679 relativo a la protección de datos de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos (Reglamento General de Protección de Datos)[3]. Una norma que ha generado impactos directos e indirectos en la forma en que se realiza el tratamiento de datos

personales en países fuera de la Unión Europea, todos ellos tomados en cuenta por el Ejecutivo uruguayo para considerar la aprobación del Protocolo de enmienda.

Protección de datos en el resto de Latinoamérica

Aunque a día de hoy tan solo México y Argentina han ratificado el Convenio 108, la mayor parte de países latinoamericanos han ido adaptando sus ordenamientos jurídicos a las nuevas tendencias normativas internacionales.

Tomando en consideración los países en los que la Fundación Microfinanzas BBVA tiene presencia, Panamá es un ejemplo de ello; con la [Ley 81](#) comentada en [Progreso 19](#) y que, aunque fue publicada en el año 2019, ha entrado en vigor recientemente y espera ser reglamentada en los próximos meses.

Además, otros de estos países cuentan con normativa no tan reciente, si bien modificada parcialmente durante los últimos años, o con nueva normativa sectorial que contempla los últimos estándares internacionales. En este sentido, Chile cuenta con la [Ley 19628](#) cuya última modificación tuvo lugar en agosto de 2020; o Colombia, en el que rige la [Ley 1581-12](#), y donde asimismo está en trámite el [Proyecto de Ley\[4\]](#) sobre habeas data financiero que fue comentada en [Progreso 20](#)-. Y Perú, que a pesar de tener la [Ley 29733](#) del año 2011, ha ido adaptando su normativa a las nuevas realidades; ejemplo de ello es la [resolución](#) del Ministerio de Justicia y Derechos Humanos sobre el Tratamiento de Datos Personales mediante Sistemas de Videovigilancia.

Por su parte, República Dominicana regula la protección de los datos personales en la Ley [172-13](#) que no ha sufrido modificaciones sustantivas desde su aprobación y ya se comenta la necesidad de actualizar la norma.

Protocolo de enmienda del Convenio 108

El Protocolo de enmienda del Convenio pretende modernizar las disposiciones contenidas en el Convenio 108 ante nuevas realidades, y así hacer frente a los desafíos derivados del uso de nuevas tecnologías en materia de protección de datos personales. Se trata de una actualización con fines similares a la realizada en febrero de 2020 y comentada en [Progreso 22](#), fecha en la que se reglamentó [Ley 19.670](#) que introduciendo modificaciones a la Ley de Protección de datos para brindar a las personas un nivel de protección acorde a los nuevos desarrollos tecnológicos y formas de tratamiento de los datos personales.

Entre los aspectos más relevantes contenidos en el Protocolo de enmienda destacan:

Garantizar el derecho de protección de los datos personales, sin importar su nacionalidad o residencia.

Se incluye la referencia al tratamiento no automatizados de datos, y se excluye del ámbito del Convenio el tratamiento doméstico de datos personales.

Se abandonan conceptos como el de archivo modificándolo por el de tratamiento.

Se extiende el catálogo de datos sensibles para incluir los genéticos y biométricos, entre otros.

Se procura facilitar el libre flujo de datos entre Partes.

Se regulan aspectos relacionados a la seguridad de los datos y transparencia en su tratamiento.

Se establece la posibilidad de que se controle el cumplimiento del Convenio por parte de las signatarias.

Con esta Ley que aprueba el Protocolo de enmienda del Convenio 104, Uruguay vuelve a estar a la vanguardia de la protección y regulación de datos personales y aunque ya cuenta con el estatus de

país adecuado será relevante para el mantenimiento del mismo.

[1] El Convenio n. 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal fue el primer instrumento internacional jurídicamente vinculante adoptado en el ámbito de la protección de datos. Tiene como fin garantizar a cualquier persona física el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona. Con el Protocolo que ha modificado el Convenio se pretende ampliar su ámbito de aplicación, aumentar el nivel de protección de los datos y mejorar su eficacia

[2] Protocolo Adicional con Respecto al Tratamiento Automatizado de Datos de Carácter Personal, a las Autoridades de Control y a los Flujos Transfronterizos de Datos adoptado en Estrasburgo, el 8 de noviembre de 2001.

[3] Con aplicación a partir del 25 de mayo de 2018 y que deroga la Directiva 95/46/CE

[4] Ley tiene por objeto modificar y adicionar la Ley 1266 de 2008, fortaleciendo el derecho al hábeas data.

Tecnologías financieras y transformación digital

Teniendo en cuenta el contexto actual y la revolución tecnológica en que vivimos, el Congreso y Gobierno de Colombia han implementado distintas medidas para regular las últimas innovaciones en tecnología financiera y reducir la brecha digital.

En este sentido cabe destacar en primer lugar, el Proyecto de Ley 063 de 2019, que tiene como fin la promoción del uso de las Sociedades Especializadas en Depósitos y Pagos Electrónicos (SEDPEs), entendidas como nuevas tecnologías financieras, mejorando y ampliando de esta manera la provisión de microcréditos a sectores productivos. Es decir, las SEDPEs otorgarán créditos a través de plataformas digitales fomentando la inclusión financiera por un lado y reduciendo las brechas de desigualdad regional, ampliando la oferta en los servicios de financiación.

Por otro lado, la Superintendencia Financiera de Colombia (SFC) ha emitido la Circular Externa 029 de 2019, que contiene instrucciones precisas para las entidades vigiladas relacionadas con requerimientos mínimos de seguridad y calidad en la realización de operaciones, información al consumidor financiero y uso de factores biométricos.

Estas nuevas instrucciones implican el fortalecimiento del uso de canales digitales para la prestación de servicios financieros en condiciones de seguridad y con apego a estándares internacionales en la materia.

Los aspectos regulados por la Circular son los siguientes:

Gran abanico de posibilidades existentes para mejorar la prestación de servicios financieros ofrecidos por las entidades vigiladas a los consumidores y optimizar sus procesos: realidad aumentada, internet de las cosas, blockchain, inteligencia artificial, machine learning, big data, robots, entre otras.

Requerimientos mínimos para la implementación y uso de biometría como factor de autenticación electrónica.

El deber de las entidades de establecer los parámetros a partir de los cuales se requerirán mecanismos fuertes de autenticación para las transacciones realizadas mediante la utilización de los medios de pago (tarjetas débito) con o sin contacto.

La posibilidad que tienen las Entidades para que la información actualizada de los productos, canales, puntos de atención, servicios y tarifas, sea puesta a disposición de terceros desarrolladores de API (Application Programming Interface).

Por último, el Gobierno ha elaborado la Política Nacional para la transformación digital e inteligencia artificial para potenciar la generación de valor social y económico en el país a través del uso estratégico de tecnologías digitales en el sector público y el sector privado, impulsando la productividad y favoreciendo el bienestar de los ciudadanos.

Esta Política aborda los retos específicos de la transformación digital, así como de la conectividad, y permite reducir la brecha digital entre zonas rurales y zonas urbanas.

Entre los aspectos más destacados de la Política, los cuales han sido denominados por el Gobierno como planes de acción, se encuentran los siguientes:

Disminución de barreras relacionadas con la falta de cultura y el desconocimiento ante la transformación digital en el sector privado.

Desarrollo y ajustes normativos e institucionales para favorecer la adopción de la transformación digital en componentes clave de la productividad empresarial.

Ejecución de iniciativas de alto impacto apoyadas en la transformación digital.

Esta política contribuirá a la generación de las redes de conectividad rural que hasta ahora constituyen un barrera para el acercamiento de los servicios financieros al sector rural del país.

Actualización de las medidas europeas sobre ciberseguridad

El 27 de junio entró en vigor el Reglamento de la Unión Europea del Parlamento Europeo relativo a la Agencia de la Unión Europea para la Ciberseguridad y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación.

La norma, que deroga el anterior Reglamento sobre la Ciberseguridad del 2013, tiene como aspiración alcanzar un nivel elevado de ciberseguridad, ciberresiliencia y confianza dentro de la Unión Europea.

A continuación destacamos los dos bloques fundamentales del documento:

Agencia Europea para la Ciberseguridad

En primer lugar, el Reglamento establece los objetivos y aspectos organizativos de la nueva Agencia Europea para la Ciberseguridad (ENISA), y le asigna las siguientes tareas:

Contribuir a la elaboración y ejecución de la política y del derecho de la Unión en el ámbito de la ciberseguridad

Asistir a los Estados en la creación de capacidades de ciberseguridad

Apoyar la cooperación entre los países miembros, las instituciones, órganos y organismos de la Unión y entre las partes interesadas

Promover el desarrollo y la aplicación de la política de la UE en materia de certificación de la ciberseguridad de productos, servicios y procesos TIC

Analizar las tecnologías emergentes y preparar evaluaciones sobre los efectos esperados, de tipo social, jurídico, económico y reglamentario, de las innovaciones tecnológicas

Sensibilizar al público sobre los riesgos relacionados con la ciberseguridad y facilitar orientaciones sobre buenas prácticas

Asesorar a las instituciones, órganos y organismos de la Unión y a los Estados miembros sobre las necesidades y prioridades de la investigación en el ámbito de la ciberseguridad y las tecnologías de la información, y a utilizar eficazmente las tecnologías de prevención del riesgo

Promover la cooperación internacional en relación con los problemas que se refieren a la ciberseguridad

Certificación de la ciberseguridad

Por otra parte, aborda la definición de un marco para la creación de esquemas europeos de certificación de la ciberseguridad, a efectos de garantizar un nivel adecuado de ciberseguridad de los productos, servicios y procesos de las tecnologías de la información y la comunicación (TIC) y de crear un mercado único digital para estos productos, servicios y procesos.

Este marco define un mecanismo destinado a instaurar esquemas europeos de certificación de la ciberseguridad y a confirmar que los productos, servicios y procesos de TIC que hayan sido evaluados con arreglo a dichos esquemas, cumplen los requisitos de seguridad especificados. De esta manera se trata de proteger la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o procesados o las funciones o servicios que ofrecen.

La Comisión Europea publicará un programa de trabajo evolutivo para los esquemas europeos de certificación que definirá las prioridades estratégicas para los futuros esquemas e incluirá una lista de productos, servicios y procesos de TIC, o de categorías de los mismos, que pudieran beneficiarse de su inclusión en el ámbito de aplicación de un esquema europeo de certificación de la ciberseguridad.

Promoción de la Inclusión financiera y transacciones

electrónicas

Colombia, consciente de la importancia de la inclusión financiera en estos tiempos de avances e innovaciones tecnológicas, está llevando a cabo importantes medidas para facilitar el acceso a productos financieros a todos los ciudadanos. Estas medidas tienen por objeto aprovechar estas nuevas tecnologías para reducir las brechas financieras existentes. En este sentido, cabe destacar los siguientes documentos:

◦ Proyecto de documento técnico sobre inclusión financiera

La Unidad de Regulación Financiera (URF), entidad adscrita al Ministerio de Hacienda y Crédito Público de Colombia, presentó para comentarios del público en general un proyecto de documento técnico denominado “Canales y productos financieros”, en el cual analiza la evolución de los corresponsales, de los productos pasivos simplificados (depósitos electrónicos, cuentas de ahorro de trámite simplificado y cuentas de ahorro electrónicas) y del crédito de bajo monto, y propone modificaciones a su marco regulatorio, con el fin de aprovechar en mejor medida las nuevas tecnologías e innovaciones y seguir aumentando la inclusión financiera mediante una mayor densidad, calidad, y eficiencia a nivel tanto de oferta como cobertura financiera, especialmente en la ruralidad.

APPs o plataformas digitales

Entre los aspectos contenidos en el Proyecto se encuentra el desarrollo de contratos de corresponsalía entre entidades financieras y terceros que provean servicios no financieros mediante APPs o plataformas digitales, con interfaces amigables y sencillos que sirvan como herramienta transaccional y de vinculación de productos, habilitando además los pagos y recaudos off line, y con ello, la corresponsalía móvil.

De la misma manera, la URF propone la interoperabilidad entre las distintas redes de corresponsales, la flexibilidad de los requisitos contractuales con los corresponsales, y la modificación de los contratos con los corresponsales sin que se requiera autorización previa de la Superintendencia Financiera de Colombia, como hoy ocurre.

Otras propuestas

Por otro lado, para los productos pasivos simplificados, el Proyecto propone aumentar el monto de saldos y retiros, eliminar la restricción de montos cuando la procedencia de los recursos es conocida, y ampliar los grupos de población que puedan acceder a estos productos.

Asimismo, en cuanto a el crédito de bajo monto, se plantea un aumento del monto máximo establecido para este producto, la realización del desembolso a cuentas de trámite simplificado, y ampliar el plazo que las entidades financieras tienen para reportar ante las centrales de riesgos o burós de crédito la realización de cada desembolso, (actualmente es de un día), lo cual podría afectar la calidad de la información con la que cuentan otros oferentes de créditos y por ende, conllevar a un sobre endeudamiento de los clientes y a una desmejora de la calidad de la cartera.

◦ PL 109 de 2019 sobre promoción de transacciones electrónicas

El Congreso de la República, por su parte, se encuentra debatiendo el Proyecto de Ley 109 de 2019,

que busca promover el uso y acceso a medios electrónicos para pagos y reducir el uso del dinero efectivo; todo ello dentro de la iniciativa de crear una Banca de Oportunidades.

El acceso a los productos financieros en Colombia tiene algunas limitaciones, que deberían ser superadas si se busca disminuir algunas brechas tecnológicas y financieras existentes. Dentro de los aspectos evaluados para llevar a cabo esta iniciativa se tuvieron en cuenta estudios realizados por el Banco de la República, que muestran que cerca del 56% de la población tenía una cuenta de ahorro con un algún establecimiento de crédito finalizando el año 2012, sin embargo, el 48% no habían sido utilizadas en el último semestre de 2014.

El Proyecto de Ley tiene como objetivo principal reducir el uso del dinero en efectivo, promover las transacciones electrónicas y la formalización comercial en el territorio nacional y fomentar la educación financiera. Además, contempla lo siguiente:

Las transacciones de dinero que superen los 100 millones de pesos colombianos (29.420 € aprox.) deberán realizarse exclusivamente por medios electrónicos.

El Gobierno tendrá a cargo la promoción de la educación financiera y la bancarización de todos los ciudadanos colombianos para garantizar el manejo correcto de medios electrónicos en el sistema financiero.

En los establecimientos públicos, medios de transporte masivos y demás entidades del orden nacional, se fomentará el uso de los medios electrónicos sobre el efectivo

Las personas jurídicas que promuevan el uso de transacciones electrónicas en el territorio nacional recibirán incentivos a discreción del Gobierno por dicha labor durante los primeros tres años en caso que se apruebe y entre en vigencia el Proyecto de Ley.

Nueva legislación sobre el desarrollo de Tecnologías Financieras

En línea con el [Decreto 2443 de 2018](#) publicado por el Ministerio de Hacienda y Crédito Público colombiano, se presentó a comienzos de enero el Proyecto de Ley 223 de 2018 con el objeto de promover el uso de las nuevas tecnologías financieras para impactar de manera positiva el desarrollo regional, disminuyendo las desigualdades sociales existentes, facilitando el otorgamiento de créditos, reduciendo la utilización de efectivo y, sobretodo, promoviendo la inclusión financiera. Así, el Proyecto de Ley busca que las autoridades financieras colombianas tengan la facultad de emitir regulaciones que faciliten el desarrollo de las FinTech o empresas de tecnología financiera.

Adicionalmente, delimita los servicios que podrían prestar las Sociedades Especializadas en Depósitos y Pagos Electrónicos (SEDPE): entidades financieras, reguladas en Colombia desde 2014, que captan recursos solamente a través de depósitos electrónicos, entre otras; y, especialmente, establece que las entidades de microcrédito podrán generar acuerdos de participación y cofinanciamiento con las mencionadas SEDPE, con el fin de que las zonas rurales alejadas de las ciudades cuenten con la tecnología necesaria para acceder a nuevas formas de microcrédito.

Por otra parte, el Proyecto busca regular ciertos aspectos del funcionamiento de las instituciones de financiamiento colectivo o *crowdfunding*, con el fin de que puedan desarrollarse en Colombia a través de valores representativos de deuda, valores representativos de capital social y copropiedad o regalías.

Por último, respecto de las areneras o *sandboxes*, indica que las empresas de tecnología financiera deberán ponerse a prueba con el fin de propiciar el ecosistema necesario para que las micro, pequeñas y medianas empresas de innovación financiera puedan consolidar su nicho de emprendimiento.

Inversión de entidades financieras en compañías de tecnología e innovación

Las entidades financieras a nivel mundial se encuentran en un proceso de transformación de sus operaciones mediante el uso de nuevas tecnologías, para ofrecer sus productos y servicios de manera innovadora, facilitar la inclusión financiera y prestar servicios a poblaciones y territorios que tradicionalmente no tenían acceso al sector financiero.

Por todo lo anterior, el Ministerio de Hacienda y Crédito Público de Colombia expidió recientemente el Decreto 2443 de 2018, con el cual abre la posibilidad a los establecimientos de crédito, las sociedades de servicios financieros y las sociedades de capitalización de invertir en sociedades dedicadas al desarrollo de innovación y tecnologías financieras.

De esta forma, las entidades financieras en Colombia podrán tener acciones o cuotas en compañías, nacionales o internacionales, cuyo objeto social exclusivo sea desarrollar o aplicar innovaciones y tecnologías conexas al desarrollo del objeto social de las entidades financieras inversoras. Estas sociedades se denominarían “sociedades de innovación y tecnología financiera”.

Protección de Datos Personales

El pasado 19 de septiembre el Ejecutivo argentino sancionó la nueva Ley de Protección de Datos Personales que deroga la vigente Ley 25.326 y su modificatoria, la Ley 26.343.

La norma introduce numerosas novedades con el fin de adaptarse al nuevo contexto internacional en protección de datos personales y adecuarse a los avances tecnológicos. A continuación se destacan los aspectos que más inciden en los sistemas de gobernanza de los sujetos obligados por la Ley:

Objeto y ámbito de aplicación

La Ley tiene por objeto la protección integral de los datos personales para garantizar el ejercicio pleno de los derechos a sus titulares. La Ley excluye de su alcance al tratamiento de datos efectuados por una persona física para su uso exclusivamente privado o en el ámbito familiar y no ampara a las

personas jurídicas por no considerarlas como titulares de derechos fundamentales.

Siguiendo las últimas tendencias internacionales, y en concreto el Reglamento General de Protección de Datos Personales del Parlamento Europeo y del Consejo del 27 de abril de 2016, la Ley es de aplicación incluso en los supuestos en los que los responsables del tratamiento no se encuentren en territorio nacional, otorgando así una mayor protección.

Nuevos conceptos y principios

Se introducen nuevos conceptos como el de *datos biométricos*, *datos genéticos*, *disociación de datos* o *incidente de seguridad de datos personales* y redefine otros ya existentes como *datos personales**, *datos sensibles* o *base de datos*.

Por otro lado, se dota de especial relevancia a los principios de lealtad y transparencia, seguridad y plazo de conservación de datos, y al principio de licitud del tratamiento de los datos, incluyendo como novedad los principios de minimización de datos y de responsabilidad proactiva. A estos efectos, cabe destacar:

Plazo de conservación: los datos personales no se conservarán más allá del tiempo estrictamente necesario para el cumplimiento de la finalidad del tratamiento. Podrán conservarse durante periodos más largos siempre que se traten con fines de archivo en interés público, fines de investigación o fines estadísticos.

Responsabilidad proactiva: se establecen las acciones necesarias para el cumplimiento de la responsabilidad proactiva, entre ellas: la obligación de adoptar políticas de privacidad o la adhesión a mecanismos de autorregulación vinculantes. La adhesión a estos mecanismos es voluntaria y puede traducirse en códigos de conducta, de buenas prácticas, normas corporativas vinculantes, sellos de confianza o certificaciones.

Licitud: la norma regula exhaustivamente el consentimiento del titular de los datos y, a diferencia de la última regulación europea, se permite un consentimiento tácito para ciertos supuestos. En este sentido, existe además una previsión específica para el tratamiento de datos de menores, siendo válido su consentimiento cuando se aplique al tratamiento de datos vinculados al uso de servicios de la sociedad de la información específicamente diseñados para ellos. En estos casos, el consentimiento será lícito cuando el menor tenga un mínimo de 13 años. En caso contrario el tratamiento solo será lícito si el consentimiento fue otorgado por sus padres o tutores.

Derechos de los titulares y obligaciones de los responsables

La norma regula los derechos básicos de acceso, rectificación, oposición y supresión. Reconoce la inclusión del derecho al olvido dentro del de supresión y contempla el nuevo derecho a la portabilidad de los datos.

En lo que a las obligaciones se refiere, la Ley incluye el deber que tiene el responsable del tratamiento de informar al titular de los datos sobre los fines del tratamiento, la identidad y datos de contacto del responsable del tratamiento, los medios para ejercer los derechos anteriormente citados, las cesiones y posibles transferencias internacionales, el derecho a revocar su consentimiento y a presentar una denuncia, entre otros.

Como novedad en este aspecto, la norma introduce:

Protección de datos desde el diseño y por defecto: el responsable del tratamiento debe aplicar medidas tecnológicas y organizativas antes y durante el tratamiento de los datos garantizando, adicionalmente, que solo sean objeto de tratamiento de aquellos datos personales que sean necesarias para cada uno de los fines del tratamiento.

Realización de una evaluación de impacto: previa al tratamiento de datos que por su naturaleza o

alcance sea probable que entrañe un alto riesgo de afectación a los derechos de los titulares de los datos. Esta evaluación será obligatoria para supuestos de tratamiento de datos automatizado o elaboración de perfiles y para tratamientos de datos sensibles a gran escala o relativos a antecedentes penales.

Delegado de Protección de Datos

Siguiendo las tendencias internacionales, la Ley argentina introduce la figura del Delegado de Protección de Datos, siendo obligatoria su designación para aquellos supuestos en que los responsables y encargados sean organismos públicos, realicen el tratamiento de datos sensibles o tratamiento de datos a gran escala.

Esta figura, que podrá asimismo designarse de manera voluntaria, ejercerá sus funciones sin recibir instrucciones y solo responderá ante el más alto nivel jerárquico de la organización debiendo reunir los requisitos de idoneidad, capacidad y conocimientos específicos para el ejercicio de las mismas.

Esta Ley no entrará en vigor hasta dos años después de su publicación en el Boletín Oficial.

* Información de cualquier tipo referida a personas humanas determinadas o determinables, inclusive los datos biométricos. Se entenderá por determinable la persona que pueda ser identificada mediante algún identificador o por uno o varios elementos característicos de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

Consejo de Coordinación de Inclusión Financiera

El pasado 27 de julio, mediante Resolución 121-E/2017, el Gobierno argentino creó, bajo la dependencia del Ministerio de Finanzas, el Consejo de Coordinación de la Inclusión Financiera (Consejo). La República se suma así a la lista de países como Chile, Uruguay, Colombia, Perú o México, comprometidos a aumentar de manera significativa la inclusión financiera.

Objeto

El Consejo, cuya composición y funcionamiento será regulado reglamentariamente, tiene por objeto elaborar e implementar una estrategia de inclusión financiera en el país y desarrollar políticas de acceso universal a servicios financieros y bancarios. Estas políticas podrán ser a corto medio y largo plazo y facilitarán el acceso universal a dichos servicios de manera eficiente.

Funciones del Consejo

Entre las funciones del Consejo, se incluyen las de: i) articular procesos participativos entre los distintos actores públicos y privados, ii) proponer la ejecución de planes para impulsar el crédito, microcrédito y la educación financiera, o iii) elaborar proyectos regulatorios que faciliten la implementación de los planes y programas definidos, asegurando la protección de los derechos de los consumidores.

Adicionalmente el Consejo deberá asesorar al Gobierno argentino en lo que a la inclusión financiera se refiere, y diseñar bases de datos sobre acceso, uso y calidad de los servicios financieros con el fin de cuantificar el progreso de los programas y planes propuestos por el ejecutivo. Todo ello a fin de promover un sistema financiero eficiente y transparente que utilice la tecnología más novedosa .

Dividendos digitales. Panorama General

El Banco Mundial ha publicado el “Informe sobre el Desarrollo Mundial 2016: Dividendos digitales”.

Los dividendos digitales son el crecimiento económico, la creación de empleo y la prestación de servicios financieros y no financieros; beneficios que se derivan de la utilización de las tecnologías digitales.

El informe analiza el impacto de Internet, la telefonía móvil y otras tecnologías conexas en el Desarrollo mundial, advirtiendo que si bien se han extendido muy rápidamente, no ha ocurrido lo mismo con los dividendos digitales.

El documento reconoce el acceso universal a Internet como una prioridad mundial, que requiere del desarrollo de otros factores, cuales son: (i) marco regulatorio que incentive el mercado y proteja a los consumidores; (ii) habilidades técnicas que permitan a los trabajadores, empresarios y funcionarios aprovechar las nuevas tecnologías, e (iii) instituciones responsables, que utilicen Internet para empoderar a sus ciudadanos. A estos factores los denomina “complementos analógicos”.

El informe concluye en que la conectividad universal sigue siendo un gran desafío y en que el desarrollo de los complementos analógicos es fundamental para garantizar mayores dividendos digitales: mayor crecimiento, más empleo y mejores servicios.