

# EL DERECHO DIGITAL Y DE LAS NUEVAS TECNOLOGÍAS: SU IMPORTANCIA EN EL GOBIERNO Y EN LA EMPRESA

## DIGITAL LAW AND NEW TECHNOLOGIES: ITS IMPORTANCE IN THE GOVERNMENT AND IN THE COMPANY

Julio Núñez Ponce

Universidad Nacional Mayor de San Marcos, Perú

<https://orcid.org/0000-0002-6524-2241>

### Resumen

El derecho digital y de las nuevas tecnologías tiene incidencia e importancia en la sociedad automatizada y global, donde el ritmo tecnológico permite a personas de todo el mundo utilizar las nuevas tecnologías de la información y de las comunicaciones. En este trabajo se analizan los distintos ámbitos de aplicación e interrelación entre el derecho y la tecnología: personas, acto jurídico, matrimonio por Internet, conciliación por medios electrónicos, ley de firmas y certificados digitales, promoción de banda ancha, delitos informáticos. Asimismo, se analiza la Ley de Gobierno Digital y la transformación digital del Poder Judicial. En el acápite «El enfoque digital y el derecho corporativo» se trata la protección de datos personales, el teletrabajo, la afectación tributaria de los servicios digitales y la protección al consumidor en el comercio electrónico. En las conclusiones se resalta la importancia y trascendencia de la disciplina.

**Palabras clave:** derecho digital, derecho de nuevas tecnologías, gobierno digital, derecho corporativo

### Summary

Digital Law and New Technologies has incidence and importance in the automated and global society, where the technological rhythm allows everyone

in the world to use the new information and communication technologies. We proceed to the analysis of the different areas of application between Law and Technology: people, legal act, internet marriage, conciliation by electronic means, law of digital signatures and certificates, promotion of broadband, computer crimes. Likewise, the Digital Government Law and the Digital Government Law and the Digital transformation of the Judiciary are analyzed. The Digital Approach and Corporate Law section deals with the protection of personal data, teleworking, the tax impact of digital service and consumer protection in Electronic Commerce. The conclusions highlight the importance and significance of the discipline.

**Keywords:** Digital Law, New Technologies Law, Digital Government, Corporate Law

## 1. Introducción

El derecho digital y de las nuevas tecnologías tiene incidencia e importancia en la sociedad automatizada y global, donde el ritmo tecnológico permite a personas de todo el mundo utilizar las nuevas tecnologías de la información y de las comunicaciones.

Debe tenerse en cuenta que «la sociedad tecnológica plantea al jurista nuevos y complejos problemas [...]. Entre los aspectos novedosos de las nuevas tecnologías, que reclaman la capacidad programadora del jurista, ocupa un lugar destacado la necesidad de establecer nuevos marcos teóricos...»<sup>1</sup> que sustenten las normas jurídicas y la jurisprudencia que aplica a los hechos que vinculan el derecho con la tecnología.

«En efecto jueces, abogados y juristas de empresa deben enfrentar cada vez con más frecuencia problemas jurídicos incomprensibles para quien no posee las nociones técnicas de base para comprenderlos»<sup>2</sup>. El *hardware*, el *software*, los datos, la información deben ser comprendidos y aprendidos, de forma coherente y sistemática, en esta nueva sociedad tecnológica.

---

1 Antonio Enrique Pérez Luno, *Manual de informática y derecho* (Barcelona: Ariel, 1996), 17.

2 Mario G. Losano, «El derecho frente a la sociedad informatizada», en *El derecho de las TIC en Iberoamérica*, dir. Marcelo Bauzá Reilly (Montevideo: La Ley, 2019), 10.

Los diversos ámbitos de interacción humana se ven favorecidos por el uso de Internet y la tecnología. Las nuevas relaciones jurídico-digitales originan diversas consecuencias: así como aumenta la calidad de vida en beneficio de las personas, también crecen de forma paralela los riesgos y perjuicios derivados de conductas socialmente inaceptables que causan perjuicios a bienes jurídicamente protegidos.

El objetivo de este aporte académico es analizar los diversos tópicos de la disciplina para evidenciar la importancia que el derecho digital y de las nuevas tecnologías tiene en el Gobierno y la empresa. Asimismo, se busca mostrar los resultados de la reflexión jurídico-digital realizada en las aulas universitarias, «fruto de un trabajo serio, riguroso y continuado [...] para conocer todo lo que rodea al complejo mundo del derecho de las Tecnologías de la Información y Comunicaciones (TIC)»<sup>3</sup>.

## 2. Derecho digital y de las nuevas tecnologías

Se analizan en este acápite los distintos ámbitos de aplicación e interrelación entre el derecho y la tecnología.

En lo concerniente al derecho de las personas, la situación es diferente, según se trate de personas naturales o jurídicas. En el caso de las primeras, son temas recurrentes la capacidad, la identidad digital, el daño a la persona en Internet. En lo que se refiere a las personas jurídicas —y específicamente a las sociedades de beneficio e interés colectivo (BIC)<sup>4</sup>—, estas pueden priorizar actividades propias de su naturaleza que coadyuven al logro de los objetivos de desarrollo sostenible (ODS) de la Agenda 2030 aprobada por la ONU, entre los que se encuentra promover la transformación digital y el uso de las tecnologías digitales en la sociedad.

Con respecto al acto jurídico, el artículo 141-A del Código Civil establece que los actos jurídicos pueden llevarse a cabo por medios electrónicos; en lo que corresponde a las obligaciones, ocurre lo mismo con las prestaciones de

---

3 Davara Rodríguez, Miguel Ángel, *Anuario de derecho de las tecnologías de la información y comunicaciones (TIC) 2006* (Madrid: Fundación Vodafone, 2006), XIII

4 Mediante Decreto Supremo 004-2021-PRODUCE, publicado el 23 de Febrero de 2021, se ha aprobado el Reglamento de la Ley 31072 de la Sociedad de Beneficio e Interés Colectivo (Sociedades BIC).

dar, no dar, hacer o no hacer. En este orden de ideas, mediante Ley 31057<sup>5</sup> se declaró de necesidad pública e interés nacional el uso de medios de pago electrónicos, con el objetivo de facilitar el intercambio de bienes y la prestación de servicios, así como de disminuir los riesgos de contagio en la coyuntura de la pandemia de la covid-19. Se busca crear, de esta manera, una cultura de pago seguro, rápido, simplificar la vida de los ciudadanos y evitar el contacto personal entre proveedores y consumidores.

En lo que concierne al derecho de familia, se puede mencionar la posibilidad de contraer matrimonio o de divorciarse por Internet. En el caso de la Municipalidad Metropolitana de Lima, las parejas que deseen casarse pueden, en efecto, iniciar sus trámites mediante el registro en línea que dicho municipio<sup>6</sup> ha implementado en el sitio web [www.munlima.gov.pe](http://www.munlima.gov.pe). Desde la opción «Trámites» se accede a la Plataforma de Operaciones Virtuales, donde los contrayentes validarán sus datos y adjuntarán los documentos necesarios para la apertura del expediente. Después de que este sea revisado y aprobado por los especialistas de la comuna, se citará a la pareja y a sus testigos para proceder a las firmas correspondientes, de manera presencial y con todas las medidas de prevención necesarias. Hecho esto, se confirma la fecha del matrimonio y se procede al pago respectivo. La ceremonia se lleva a cabo a través de la plataforma Google Meet. Por otro lado, en la misma Plataforma de Operaciones Virtuales existe una opción para tramitar el divorcio; los interesados podrán completar las respectivas declaraciones juradas y subir la documentación necesaria para iniciar dicha gestión. Los especialistas verificarán la validez de todos los documentos enviados y, una vez que hayan dado su visto bueno, se abonará el pago correspondiente al derecho de trámite. Se generará, de esta manera, un único número de expediente que se utilizará en todo el procedimiento de divorcio.

En el desarrollo del derecho digital y de las nuevas tecnologías, «nuestra intención debe ser diseñar un derecho para la sociedad digital»<sup>7</sup> que permita afirmar que el derecho está acorde con la realidad. Y con la finalidad de darles

---

5 *El Peruano*, 22 de octubre de 2020.

6 [https://www.munlima.gov.pe/noticias/item/40776-municipalidad-de-lima-implementa-procedimientos-virtuales-para-matrimonios-y-divorcios?fbclid=IwAR20f-XGu2\\_wS5TXTOII MaFe9ldBcOImUyIbDBbWbtFm3qmb-a2-snnSxg8/](https://www.munlima.gov.pe/noticias/item/40776-municipalidad-de-lima-implementa-procedimientos-virtuales-para-matrimonios-y-divorcios?fbclid=IwAR20f-XGu2_wS5TXTOII MaFe9ldBcOImUyIbDBbWbtFm3qmb-a2-snnSxg8/)

7 Michel Vivant, «El derecho digital: entre una aproximación técnica y una reflexión societal», en *El derecho de las TIC en Iberoamérica*, dir. Marcelo Bauzá Reilly (Montevideo: La Ley, 2019), 1312.

seguridad jurídica y técnica al matrimonio, a los contratos o a cualquier otro acto jurídico que se realice vía Internet, se recurre a las firmas y certificados digitales.

Al respecto, cabe señalar que la Ley 27269<sup>8</sup> regula la utilización de la firma electrónica, para lo cual le otorga la misma validez y eficacia jurídica que una firma manuscrita u otra análoga que conlleve manifestación de voluntad. Se entiende por *firma electrónica* cualquier símbolo basado en medios electrónicos que es utilizado o adoptado por una de las partes con la intención precisa de vincularse o autenticar un documento; para esto, cumple todas o algunas de las funciones características de una firma manuscrita.

Este marco legal se aplica a aquellas firmas electrónicas que, puestas sobre un mensaje de datos o añadidas o asociadas lógicamente a ellos, tengan la capacidad de vincular e identificar al firmante, así como garantizar la autenticación e integridad de los documentos electrónicos.

La firma digital es aquella firma electrónica que utiliza una técnica de criptografía asimétrica basada en un par único de claves; en este van asociadas una clave privada y otra pública relacionadas matemáticamente entre sí, de tal forma que las personas que conocen la clave pública no puedan derivar de ella la clave privada. Conforme al Reglamento<sup>9</sup> de la Ley de Firmas y Certificados Digitales, se reconoce la variedad de modalidades de firmas electrónicas, la diversidad de garantías que ofrecen, los diversos niveles de seguridad y la heterogeneidad de las necesidades de sus potenciales usuarios. La Infraestructura Oficial de Firma Electrónica no excluye ninguna modalidad, ni combinación de modalidades de firmas electrónicas.

Se reconocen las siguientes tres modalidades de firma electrónica:

- a) Simple. Es un dato en formato electrónico anexo a otros datos electrónicos o asociado de manera lógica con ellos.
- b) Avanzada. Cumple con las siguientes características: i) está vinculada de manera única al firmante, ii) permite la identificación de este, iii) ha sido elaborada utilizando datos de creación de firmas que el firmante puede utilizar bajo su control, y iv) está vinculada con los datos firmados de modo tal que cualquier modificación posterior de estos es detectable.

---

8 *El Peruano*, 28 de mayo de 2000, p. 187067.

9 Decreto Supremo 052-2008-PCM, Reglamento de la Ley de Firmas y Certificados Digitales, diario oficial *El Peruano*, 19 de julio de 2008. Modificado por Decreto Supremo 029-2021-PCM, Reglamento de la Ley de Gobierno Digital, diario oficial *El Peruano*, 19 de Febrero de 2021.

- c) Cualificada o digital. Es aquella firma electrónica avanzada que cumple con lo establecido en el capítulo II del mencionado reglamento.

Para cada modalidad de firma electrónica, la aplicación de la carga de la prueba varía conforme a lo siguiente:

- a) En caso de controversia sobre la autoría de la firma electrónica simple o avanzada, la carga de la prueba recae en quien la invoque como auténtica.  
b) En caso de controversia alrededor de una firma electrónica cualificada, la carga de la prueba se invierte; así, quien niegue la autoría deberá demostrar que la firma es apócrifa.

La firma digital generada dentro de la Infraestructura Oficial de Firma Electrónica tiene la misma validez y eficacia jurídica que una manuscrita. En tal sentido, cuando la ley exija la firma de una persona, dicho requisito se entenderá cumplido en relación con un documento electrónico si se ha utilizado una firma digital generada en el marco de la Infraestructura Oficial de la Firma Electrónica. Las disposiciones establecidas en el citado reglamento no excluyen el cumplimiento de las formalidades específicas que se exigen para los actos jurídicos y el otorgamiento de fe pública.

Por otra parte, la reciente Ley 31165<sup>10</sup> modifica la Ley de Conciliación de manera que se permite la celebración de audiencias por medios electrónicos, garantizando la identificación, capacidad y comunicación de las partes, así como la autenticidad del acuerdo conciliatorio que se alcance. Este contiene la firma digital del conciliador, las de las partes intervinientes o sus representantes legales.

Lo tratado anteriormente en el ámbito del derecho digital y de las nuevas tecnologías lleva a la siguiente reflexión: «La nueva ciencia y la nueva tecnología enfrentan al derecho con una realidad diferente. Y ello supone el nacimiento de nuevos problemas, que deben ser pensados de una manera diferente en términos jurídicos, con incluso repercusiones morales»<sup>11</sup>. Esta nueva visión jurídico-digital permite tratar temas diversos bajo un solo centro de imputación: la tecnología de información. Desde esta perspectiva, se con-

---

10 Ley 31165, Ley que modifica la Ley 26872 de Conciliación, diario oficial *El Peruano*, 13 de abril de 2021.

11 Fernando de Trazegnies Granda, «El derecho frente a los desafíos que plantea la ciencia y la tecnología moderna», en *Homenaje al Doctor Carlos Torres y Torres Lara* (Lima: El Buho, 2018), 495.

tinuarán desarrollando temas relevantes, como los delitos informáticos y la promoción de la banda ancha.

La Ley de Promoción de la Banda Ancha y Construcción de la Red Dorsal de Fibra Óptica (Ley 29904<sup>12</sup>) define *banda ancha* como:

... la conectividad de transmisión de datos, principalmente a Internet, en forma permanente y de alta velocidad, que le permite al usuario estar siempre en línea, a velocidades apropiadas para la obtención y emisión interactiva de información multimedia, y para el acceso y utilización adecuada de diversos servicios y aplicaciones de voz, datos y contenidos audiovisuales.

En tiempos de pandemia, la conectividad relacionada con la velocidad de conexión resulta determinante para el teletrabajo, la salud, la educación, las relaciones sociales virtuales, así como para la libertad de información, empresa y comercio. Y la Ley de Banda Ancha se propone impulsar el desarrollo, utilización y masificación de dicha conectividad en todo el territorio nacional, tanto en la oferta como en la demanda por este servicio. Con esta finalidad, promueve el despliegue de infraestructura, servicios, contenidos, aplicaciones y habilidades digitales como medios que favorecen y facilitan la inclusión social, el desarrollo socioeconómico, la competitividad, la seguridad del país y la transformación organizacional hacia una sociedad de la información y del conocimiento.

Otro tema relevante es el de los delitos informáticos. Para garantizar la lucha eficaz contra la ciberdelincuencia, la Ley 30096<sup>13</sup> previene y sanciona las conductas ilícitas que, recurriendo a las tecnologías de la información o de la comunicación, afectan los sistemas y datos informáticos, así como otros bienes jurídicos de relevancia penal.

En relación con el bien jurídico protegido —datos y sistemas informáticos— los delitos de acceso ilícito y atentados contra la integridad de datos y sistemas informáticos se tipifican de la siguiente forma:

- a) Acceso ilícito: «El que deliberada e ilegítimamente accede a todo o en parte de un sistema informático, siempre que se realice con vulneración

---

12 Ley 29904, Ley de promoción de banda ancha y construcción de la red dorsal de fibra óptica, diario oficial *El Peruano*, 20 de julio de 2012

13 Ley 30096, Ley de Delitos Informáticos, diario oficial *El Peruano*, 22 de octubre de 2013.

de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa». El acceso ilícito puede ser total o parcial, y la condición tipificante es que exista vulneración de las medidas de seguridad establecidas para impedirlo, sea a nivel físico (instalaciones, *hardware*), lógico (*software*, sistemas, *firewall*, otros), organizativos (privilegios de acceso, otros) o legales (reglamentos, disposiciones normativas).

Otro supuesto que establece el artículo es: «Será reprimido con la misma pena, el que accede a un sistema informático excediendo lo autorizado». Aquí se parte del supuesto de que el acceso está autorizado y que el agente (puede ser un empleado, un dependiente, un locador, entre otros) excede los límites establecidos en la autorización formulada de manera expresa por la persona, autoridad o empleador competente.

- b) Atentado contra la integridad de datos informáticos: «El que deliberada e ilegítimamente daña, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa». El daño a los datos puede ser ocasionado por un *malware*; la introducción de datos falsos, que pueden ser numéricos, textuales o de otro tipo; asimismo, el borrado, alteración o supresión de datos de registro que puede ocasionar modificación o extinción ilegítima de obligaciones, multas, sanciones.
- c) Atentado contra la integridad de sistemas informáticos: «El que deliberada e ilegítimamente inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa». Todos hemos observado, al menos una vez, la falta de atención de servicios bancarios, comerciales u otros por falla del sistema. Cuando esta interrupción se produce en forma deliberada e ilegítima, se configura el delito.

Los delitos contra los datos y sistemas informáticos se incluyen entre los delitos en el ámbito tecnológico que se hallan tipificados en nuestro ordenamiento jurídico. Además, cabe mencionar los delitos de suplantación de identidad, interceptación de datos informáticos, fraude informático, vulneración de derechos de autor de *software*, tráfico ilegal de datos, entre otros.



Otro tema relacionado con los delitos informáticos es la adhesión del Perú al Convenio sobre la Ciberdelincuencia del Consejo de Europa (Convenio de Budapest), que es el acuerdo internacional de uso más extendido para el desarrollo de la legislación de combate al cibercrimen. El tratado ha sido ratificado por sesenta Estados, incluidos Estados Unidos, Canadá, Australia, Japón y los países que integran la Unión Europea. El Perú se adhirió mediante Resolución Legislativa 30913, el 13 de febrero de 2019.

La convención, en síntesis, tiene como objetivo armonizar la legislación relativa al cibercrimen, mejorar las capacidades de investigación de este tipo de delitos y establecer un régimen efectivo de cooperación y asistencia internacional. Entre sus principales disposiciones destacan la obligación de tipificar delitos contra la integridad de los sistemas o datos informáticos y su contenido, y establecer procedimientos que faciliten la investigación penal. El acuerdo resuelve también los aspectos de la cooperación y asistencia internacional en materias como extradición, acceso y consentimiento transfronterizo, así como el establecimiento de un equipo experto en una red 24/7 como punto de contacto localizable las 24 horas del día.

### **3. Derecho y tecnología en la Ley de Gobierno Digital y en el Poder Judicial**

La Ley de Gobierno Digital (Decreto Legislativo 1412) tiene por objeto establecer el marco de gobernanza digital para la adecuada gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos, así como el régimen jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales por parte de las entidades de la Administración Pública en los tres niveles de gobierno.

El reglamento de la Ley de Gobierno Digital (Decreto Supremo 029-2021-PCM) define el marco de identidad digital del Estado Peruano, que comprende la gestión de la identidad digital de peruanos y extranjeros. Los principios específicos son inclusión, identificador único, no discriminación y equivalencia funcional de la verificación de la identidad.

Definimos el Gobierno Inteligente como el aprovechamiento de los datos, información y conocimiento como activos de gobierno para optimizar los servicios di-

giales que creen valor público. Concebimos el Gobierno Digital confiable a aquel que incluye como fases de desarrollo anteriores: al Gobierno cercano, abierto, inteligente, eficiente e integrado en un ecosistema digital que fortalezca la ciberseguridad, promueva la gestión de riesgos y continuidad operativa y universalice la identidad digital, dentro de un marco jurídico adecuado<sup>14</sup>.

Los ciudadanos digitales son aquellas personas naturales que cumplen, como mínimo, los siguientes requisitos: a) tienen atributos de identidad inherentes, b) poseen una casilla electrónica y c) cuentan con credenciales de autenticación emitidas, entregadas o habilitadas.

Los objetivos del gobierno digital son:

- a) Normar las actividades de gobernanza, gestión e implementación en materia de tecnologías digitales, identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos.
- b) Coordinar, integrar y promover la colaboración entre las diversas entidades de la Administración Pública.
- c) Promover la investigación y el desarrollo en la implementación de tecnologías digitales, identidad digital, servicios digitales, interoperabilidad, seguridad digital y datos.
- d) Promover y orientar la formación y capacitación en materia de gobierno digital y tecnologías digitales en todos los niveles de gobierno.

La gobernanza digital es el conjunto de roles, estructuras, procesos, herramientas y normas necesarias para articular, dirigir, evaluar y supervisar la adopción y el uso de las tecnologías digitales y datos en el Estado Peruano, así como el proceso de transformación digital en el país, de conformidad con el artículo 3 de la Ley de Gobierno Digital. Por su parte, el gobierno digital consiste en el uso estratégico de las tecnologías digitales y datos en la Administración Pública con la finalidad de crear valor público, de conformidad con lo establecido en el artículo 6 de la referida norma legal.

La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, es la entidad responsable de ejercer la gobernanza digital del uso transversal y de la adopción estratégica de las tecnologías digitales y datos en el Estado Peruano, así como del proceso de transformación digital en

---

14 Julio Núñez Ponce, «Identidad digital, derecho y gobierno inteligente: hacia el fortalecimiento del gobierno digital», en *El derecho de las TIC en Iberoamérica*, dir. Marcelo Bauzá Reilly (Montevideo: La Ley, 2019), 1213.

el país y de los marcos de identidad digital, interoperabilidad, servicios digitales, datos, gobernanza, gestión y reestructuración de modelos de datos, seguridad digital y arquitectura digital del Estado Peruano. Igualmente, emite las normas, lineamientos, especificaciones, guías, directivas y estándares que deben ser aplicadas por las diversas entidades de la Administración Pública.

La interoperabilidad es la capacidad de interactuar que tienen las organizaciones. El marco de interoperabilidad del Estado se gestiona a través de los niveles organizacional, semántico, técnico y legal.

En el sector público, el Poder Judicial ha iniciado un proceso de transformación digital con la mesa de partes virtual, el expediente judicial electrónico y la casilla electrónica. Al respecto, y en cumplimiento de la Ley 30229<sup>15</sup> se incorporan al Texto Único Ordenado de la Ley Orgánica del Poder Judicial —aprobado por Decreto Supremo 017-93-JUS— los artículos 155-A, 155-B, en los términos siguientes:

#### Artículo 155-A. Notificación electrónica

La notificación electrónica es un medio alternativo a la notificación por cédula y se deriva a casilla electrónica de manera obligatoria en todos los procesos contenciosos y no contenciosos tramitados ante los órganos jurisdiccionales del Poder Judicial. La notificación electrónica debe contar con firma digital y debe ser utilizada en el marco de la Ley 27269, Ley de Firmas y Certificados Digitales, su reglamento, así como la normativa relacionada.

#### Artículo 155-B. Requisito de admisibilidad.

Es un requisito de admisibilidad que las partes procesales consignen en sus escritos postulatorios la casilla electrónica asignada por el Poder Judicial, extendiéndose dicho requisito al apersonamiento de cualquier tercero en el proceso.

Estas disposiciones han sido aplicadas por el Poder Judicial como parte de su proceso de transformación digital.

---

15 Ley 30229, Ley que adecúa el uso de las tecnologías de información y comunicaciones en el sistema de remates judiciales y en los servicios de notificaciones de las resoluciones judiciales, diario oficial *El Peruano*, 12 de julio de 2014.

#### 4. El enfoque digital y el derecho corporativo

El enfoque digital aplicado al derecho corporativo tiene entre sus tópicos la protección de datos personales, el teletrabajo, la tributación de servicios digitales, la protección al consumidor en Internet.

Con respecto a la protección de datos personales, la Ley 29733 —modificada por Decreto Legislativo 1353— establece su aplicación a los datos personales contenidos o destinados a ser almacenados en bancos de datos personales de administración pública y privada cuyo tratamiento se lleva a cabo en el territorio nacional. Son objeto de especial protección los datos sensibles.

La actuación de los titulares, encargados y, en general, de toda persona que intervenga en el tratamiento de datos personales debe ajustarse a los principios rectores de legalidad, consentimiento, finalidad, proporcionalidad, calidad, seguridad, disposición de recurso, nivel de protección adecuado. Esta relación de principios rectores es enunciativa.

Los principios rectores señalados sirven, igualmente, como criterios interpretativos para resolver las cuestiones que puedan suscitarse en la aplicación de la mencionada ley y de su reglamento; también son útiles como parámetros para la elaboración de otras disposiciones y suplir vacíos en la legislación sobre la materia.

Tanto el titular como el encargado del tratamiento de datos personales deben realizar el flujo transfronterizo de estos solo si el país destinatario mantiene niveles de protección adecuados conforme a la norma legal en cuestión. En caso de que en el país en cuestión no exista un nivel de protección adecuado, el emisor del flujo transfronterizo debe garantizar que el tratamiento de los datos personales se efectuará conforme a lo dispuesto por la ley.

Por otra parte, el titular de los datos personales tiene derecho a la actualización, inclusión, rectificación y supresión de estos cuando sean parcial o totalmente inexactos, incompletos, cuando se haya advertido omisión, error o falsedad, o bien en el caso de que hayan dejado de ser necesarios o pertinentes para la finalidad por la cual fueron recopilados o cuando haya vencido el plazo establecido para su tratamiento. Si previamente a las acciones mencionadas los datos personales han sido objeto de transferencia, el encargado del tratamiento de los datos debe comunicar la actualización, inclusión, rectificación o supresión correspondientes a quienes los hayan transferido. El destinatario deberá proceder igualmente a la actualización, inclusión, rectificación o supresión, según corresponda.

Durante el proceso de actualización, inclusión, rectificación o supresión de datos personales, el encargado de su tratamiento debe bloquearlos, con lo cual queda impedido de permitir que terceros accedan a ellos. El bloqueo, sin embargo, no se aplica a las entidades públicas que requieren dicha información para el adecuado ejercicio de sus competencias establecidas por ley; deben ser informados de que se encuentra en trámite cualquiera de los mencionados procesos.

El titular de los datos personales puede oponerse al tratamiento de estos cuando existan motivos fundados y legítimos relativos a una situación personal concreta, siempre que la ley no disponga lo contrario y cuando no haya prestado consentimiento. En caso de que exista una oposición justificada, el titular o el encargado del tratamiento de datos personales debe proceder a su supresión conforme a ley.

Tanto el titular como el encargado de tratamiento de datos personales tienen, según sea el caso, las siguientes obligaciones:

- 1) Efectuar el tratamiento de datos personales solamente con el previo consentimiento informado, expreso e inequívoco del titular, salvo ley autoritativa, con excepción de los supuestos consignados en el artículo 14 de la mencionada Ley.
- 2) No recopilar datos personales a través de medios fraudulentos, desleales o ilícitos.
- 3) Recopilar datos personales que estén actualizados y que sean, asimismo, necesarios, pertinentes y adecuados con relación a finalidades determinadas, explícitas y lícitas para las cuales se hayan obtenido.
- 4) No utilizar los datos personales objeto de tratamiento con fines distintos de aquellos que motivaron su recopilación, salvo que medie algún procedimiento de anonimización o disociación.
- 5) Almacenar los datos personales de manera que a su titular le sea posible ejercer los derechos que le corresponden.
- 6) Suprimir y sustituir o, en su caso, completar los datos personales objeto de tratamiento cuando tenga conocimiento de su carácter inexacto o incompleto, sin perjuicio de los derechos del titular en la materia.
- 7) Suprimir los datos personales objeto de tratamiento cuando hayan dejado de ser necesarios o pertinentes para la finalidad por la cual fueron recopilados o haya vencido el plazo para su tratamiento, salvo que medie algún procedimiento de anonimización o disociación.

- 8) Proporcionar a la Autoridad Nacional de Protección de Datos Personales, cuando esta —en ejercicio de sus funciones y dentro de un procedimiento administrativo en curso solicitado por la parte afectada— se lo requiera, la información relativa al tratamiento de datos personales; igualmente, permitirle el acceso a los bancos de datos personales que administren.

«El advenimiento de Internet en la sociedad trae grandes modificaciones en la forma de comunicación e interacción del ser humano. También trae consigo una nueva sociedad (digital), creando así nuevos desafíos, dilemas, relaciones jurídicas y consecuentemente nuevos problemas»<sup>16</sup>. El enfoque digital para resolver estos problemas en el ámbito del derecho corporativo incluyen la protección de datos personales, el teletrabajo, la afectación tributaria de los servicios digitales y la protección al consumidor.

Con respecto al teletrabajo —que está incluido dentro del concepto de trabajo remoto en tiempo de pandemia—, se caracteriza, según la Ley 30036, por el desempeño subordinado de labores sin la presencia física del trabajador (al que se le denomina «teletrabajador») en la empresa con la que mantiene vínculo laboral, a través de medios informáticos, de telecomunicaciones y análogos; mediante estos, a su vez, se ejercen el control y la supervisión de las labores. La provisión por el empleador de medios físicos e informáticos, la dependencia tecnológica y la propiedad de los resultados, entre otros, son elementos que coadyuvan a tipificar el carácter subordinado de esta modalidad de trabajo.

Cuando los equipos sean proporcionados por el empleador, el teletrabajador es responsable de su correcto uso y conservación, para lo cual evita que los bienes sean utilizados por terceros ajenos a la relación laboral. Cuando el teletrabajador aporte sus propios equipos o elementos de trabajo, el empleador debe compensar la totalidad de los gastos, incluidos los de comunicación, sin perjuicio de los mayores beneficios que pudieran pactarse por acuerdo individual o convenio colectivo. Si el teletrabajador realiza sus labores en una cabina pública de Internet o en un equipo proporcionado por terceras personas, el empleador asume los gastos que esto conlleva. El reglamento establece la forma en la que se efectuará esta compensación de condiciones de trabajo.

---

16 Amanda García Perraro, «Sociedade digital: novos desafios para o direito», en *Direito digital: novas teses jurídicas*, coords. Coriolano Almeida Camargo y Cleórbete Santos (Río de Janeiro: Lumen Juris, 2018), 36.

El teletrabajador tiene los mismos derechos y obligaciones establecidos para los trabajadores del régimen laboral de la actividad privada. Pueden utilizarse todas las modalidades de contratación establecidas para dicho régimen. En todos los casos, el contrato de trabajo debe constar por escrito.

De conformidad con el Decreto Supremo 017-2015-TR, Reglamento de la Ley de Teletrabajo, son principios que orientan la aplicación de la modalidad de teletrabajo los siguientes:

- a) Voluntariedad. El empleador o entidad pública, por razones debidamente sustentadas, puede variar la prestación de servicios a la modalidad de teletrabajo, para lo cual debe contar con el consentimiento del trabajador o servidor civil.
- b) Reversibilidad. El empleador o entidad pública puede reponer al teletrabajador a la modalidad de prestación de servicios anterior al teletrabajo si se acredita que bajo la modalidad de teletrabajo no se alcanzan los objetivos establecidos.
- c) Igualdad de trato. En cuanto a las condiciones de trabajo, el empleador o entidad pública debe promover la igualdad de trato de los teletrabajadores en relación con el que se da a quienes laboran presencialmente.
- d) Conciliación entre la vida personal, familiar y laboral. Promover a través de la modalidad de teletrabajo un equilibrio entre las actividades realizadas en los ámbitos personal, familiar y laboral de los trabajadores o servidores civiles. En tal sentido, deberá existir una adecuada correspondencia entre la carga de trabajo y la jornada laboral o de servicios asignada.

El origen y desarrollo del derecho Telemático se encuentran asociados a la espectacular evolución de las telecomunicaciones potenciadas por la informática potenciadas en los últimos años, singularizada por la globalización, el cambio tecnológico y la reestructuración de los servicios<sup>17</sup>.

El derecho digital y de las nuevas tecnologías incluye al derecho telemático en su desarrollo. Con respecto al teletrabajo y el trabajo remoto, se ha incluido en nuestro ordenamiento jurídico el derecho a la desconexión digital<sup>18</sup>.

---

17 Carlos E. Delpiazzo y María José Viega, *Lecciones de derecho telemático* (Montevideo: Fondo de Cultura Universitaria, 2004), 67.

18 Decreto de Urgencia 127-2020, Disposición Final, diario oficial *El Peruano*, 1 de noviembre de 2020.

En efecto, el teletrabajador podrá desconectarse de su conexión de Internet o celular durante sus horas de descanso o cuando haya suspensión de labores.

Con respecto a la afectación tributaria de los servicios digitales, conforme a la Ley del Impuesto a la Renta, están sujetas al impuesto la totalidad de las rentas gravadas que obtengan los contribuyentes que, conforme a las disposiciones de dicha Ley, se consideran domiciliados en el país, sin tener en cuenta la nacionalidad de las personas naturales, el lugar de constitución de las jurídicas, ni la ubicación de la fuente productora. En caso de contribuyentes no domiciliados en el país, de sus sucursales, agencias o establecimientos permanentes, el impuesto recae solo sobre las rentas gravadas de fuente peruana.

Se consideran rentas de fuente peruana aquellas que se han obtenido mediante servicios digitales prestados a través de Internet o de cualquier adaptación o aplicación de los protocolos, plataformas, o bien de la tecnología utilizada por Internet o cualquier otra red a través de la que se presten servicios equivalentes, cuando el servicio se utilice económicamente, use o consuma en el país.

Conforme el reglamento, se entiende por *servicio digital* todo servicio que se pone a disposición del usuario a través de Internet o de cualquier adaptación o aplicación de los protocolos, plataformas; o bien de la tecnología utilizada por Internet o cualquier otra red a través de la cual se presten servicios equivalentes mediante accesos en línea; se caracteriza por ser esencialmente automático y no viable en ausencia de la tecnología de la información. Para efecto del reglamento, las referencias a *página de Internet*, *proveedor de Internet*, *operador de Internet* o *Internet* comprenden tanto a Internet como a cualquier otra red, pública o privada.

Se consideran servicios digitales, entre otros, los siguientes:

1. Mantenimiento de *software*
2. Soporte técnico al cliente en red
3. Almacenamiento de información (*Data warehousing*)
4. Aplicación de hospedaje (*Application hosting*)
5. Provisión de servicios de aplicación (*Application Service Provider ASP6*).
6. Almacenamiento de páginas de Internet (*website hosting*)
7. Acceso electrónico a servicios de consultoría
8. Publicidad (*Banner ads*)
9. Subastas en línea
10. Reparto de información.
11. Acceso a una página de Internet interactiva



12. Capacitación interactiva

13. Portales en línea para compraventa

Conforme al Código de Protección y Defensa del Consumidor, son consumidores las personas naturales o jurídicas que, en calidad de destinatarios finales, adquieren, utilizan o disfrutan productos o servicios materiales e inmateriales en beneficio propio o de su grupo familiar o social, actuando, de esta manera, en un ámbito ajeno a una actividad empresarial o profesional. Según dicha norma legal, no se considera consumidor a quien adquiere, utiliza o disfruta del producto o servicio normalmente destinado para los fines de su actividad como proveedor.

También son consumidores los microempresarios que evidencien una situación de asimetría informativa con el proveedor respecto de aquellos productos o servicios que no formen parte del giro propio del negocio. En caso de duda sobre el destino final de un determinado producto o servicio, se califica como consumidor a quien lo adquiere, usa o disfruta.

En el documento de trabajo sobre protección al consumidor en el comercio electrónico<sup>19</sup> elaborado por Indecopi, se propone incluir el siguiente texto:

Las relaciones comerciales concertadas a través del intercambio de mensajes de datos entre consumidor y proveedor se entenderán como contratos de consumo de comercio electrónico. En los contratos de consumo celebrados a través de canales digitales, tratándose de productos no relacionados con las necesidades ordinarias, el proveedor debe tomar las medidas posibles para verificar la edad del consumidor, por lo que el proveedor debe dejar constancia de la autorización expresa y previa de los padres, tutor o apoderado para realizar la transacción en soporte duradero.

En esta propuesta se regulan los contratos de consumo de comercio electrónico estableciendo precisiones y obligaciones que deben ser analizadas a la luz del derecho digital y de las nuevas tecnologías.

Asimismo, se propone que los contratos celebrados por canales digitales se perfeccionan cuando el proveedor recibe la aceptación por el consumidor de las condiciones propuestas, las cuales deben estar a disposición de las partes en soporte duradero. Dicho perfeccionamiento se materializa cuando se

---

19 <https://prcp.com.pe/wp-content/uploads/2021/04/Documento-de-Trabajo-Comercio-electronico-version-finalF.pdf.pdf>

recibe la confirmación de la compra en línea. La simple visita al sitio de Internet o plataforma virtual en el cual se ofrecen determinados servicios o productos no impone al consumidor obligación alguna. Las condiciones pactadas en el contrato son respetadas por ambas partes.

Se propone que exista consentimiento del consumidor cuando concurren los siguientes supuestos:

- a) Ha tenido previamente acceso a las condiciones generales del contrato, las cuales deben estar expresadas en términos claros, comprensibles e inequívocos.
- b) Ha contado con la posibilidad de leerlas completamente, almacenarlas digitalmente o imprimirlas.
- c) Ha manifestado su voluntad de forma inequívoca a través de los canales digitales que el proveedor ha puesto a su disposición.

## 5. Conclusiones

Con respecto a la importancia del derecho digital y de las nuevas tecnologías, todo lo señalado en los acápites anteriores lleva a la siguiente reflexión: «Para el jurista y para el abogado operador de nuestros días, su campo de trabajo ya no es solamente el dominio de las reglas generales... hoy además, sus horas de labor debe dedicarlas en gran parte a informarse sobre las normas, los hechos y los efectos de la relación entre ambas»<sup>20</sup>.

Para ello el abogado conoce en forma sistémica la regulación aplicable con un enfoque digital que le permite conocer e interpretar los hechos de la realidad y las normas jurídicas relacionadas, en forma coherente e integral, por lo que el derecho digital y de las nuevas tecnologías tiene un papel preponderante en la formación del abogado en derecho corporativo.

El derecho digital y de las nuevas tecnologías se interrelaciona con los derechos de la persona, la protección de datos personales, las firmas y certificados digitales, la sociedades BIC en transformación digital, la conciliación por medios electrónicos, la legislación de gobierno digital, confianza digital, delitos informáticos, la justicia digital, la ley del teletrabajo, la afectación tributaria de los servicios digitales, *fintech*, inteligencia artificial, arbitraje en lí-

---

20 Carlos Torres y Torres Lara, *Testimonio en informática jurídica* (Lima: Asesorandina, 2004), 46.

nea, procesos electrónicos, entre otros temas. El centro de imputación es el componente tecnológico digital que permite una visión sistémica de la problemática y propone una solución holística, eficiente e integral.

En la Política 35 del Acuerdo Nacional sobre Sociedad de la Información y Sociedad del Conocimiento está presente el compromiso de impulsar una sociedad de la información orientada al desarrollo humano integral y sostenible con base en el ejercicio pleno de las libertades y derechos de las personas con un enfoque jurídico digital. El derecho digital y de las nuevas tecnologías sustenta jurídicamente esta política, de ahí su importancia y trascendencia tanto en el ámbito gubernamental como en el empresarial.

### Referencias

- Davara Rodríguez, Miguel Ángel. *Anuario de derecho de las tecnologías de la información y comunicaciones (TIC) 2006*. Madrid: Fundación Vodafone, 2006.
- De Trazegnies Granda, Fernando. «El derecho frente a los desafíos que plantea la ciencia y la tecnología moderna». En *Homenaje al Doctor Carlos Torres y Torres Lara*. Lima: El Búho, 2018.
- Delpiazzo, Carlos E. y Viega, María José. *Lecciones de derecho telemático*. Montevideo: Fundación de Cultura Universitaria, 2004.
- García Ferraro, Amanda: «Sociedade digital: novos desafios para o direito». En *Direito digital: novas teses jurídicas*, coordinado por Coriolano Almeida Camargo y Cleórbete Santos, 23-40. Río de Janeiro: Lumen Juris, 2018.
- Losano, Mario G. «El derecho frente a la sociedad informatizada». En *El derecho de las TIC en Iberoamérica*, dirigido por Marcelo Bauzá Reilly, 1-10. Montevideo: La Ley, 2019.
- Núñez Ponce, Julio. «Identidad digital, derecho y gobierno inteligente: hacia el fortalecimiento del gobierno digital». En *El derecho de las TIC en Iberoamérica*, dirigido por Marcelo Bauzá Reilly, 1213-1218. Montevideo: La Ley, 2019.

Pérez Luno, Antonio Enrique. *Manual de informática y derecho*. Barcelona: Ariel, 1996.

Torres y Torres Lara, Carlos. *Testimonio de informática jurídica*. Lima: Asesorandina, 2004.

Vivant, Michel. «El derecho digital: entre una aproximación técnica y una reflexión societal». En *El derecho de las TIC en Iberoamérica*, dirigido por Marcelo Bauzá Reilly, 1311-1320. Montevideo: la Ley, 2019.

### **Sobre el autor**

Doctor en Derecho y Ciencias Políticas por la Universidad Nacional Mayor de San Marcos (UNMSM). Magíster en Derecho Empresarial y abogado por la Universidad de Lima. Profesor de Tesis y del Taller de Herramientas Tecnológicas para la Investigación Jurídica en la Maestría en Ciencias Penales en la UNMSM, también profesor de Derecho de las Nuevas Tecnologías en la carrera de Derecho Corporativo de la Universidad ESAN, y de Legislación en Medios Digitales en la Escuela de Posgrado de la UPC.