enaTIC
ABOGACIA DIGITAL

ASOCIACIÓN DE EXPERTOS NACIONALES DE LA ABOGACÍA TIC

DERECHO COMPARADO EN PROTECCIÓN DE DATOS: PERÚ Y LA UNIÓN EUROPEA

ESTUDIOS DE INVESTIGACIÓN EN DERECHO DIGITAL

Registro de versiones

Versión	Fecha	Páginas afectadas	Notas / motivos de cambio
V 1.0	07/03/2022		

ÍNDICE

En este estudio han colaborado:

Jesús Alejandro Robles Salas (Perú)

Abogado por la Universidad Particular de San Martín de Porres (Perú). Máster en Derecho Digital y Sociedad de la Información por la Universidad de Barcelona (España). Con estudios de especialización en Derecho Administrativo por la Universidad de Valladolid (España) y Pontificia Universidad Javeriana de Colombia. Consultor, Investigador y Docente en Derecho Administrativo en entidades públicas y privadas del Perú.

Boris Armando Castillo (Perú)

Abogado especializado en Protección de Datos. Delegado de Protección de Datos (DPD) del BBVA en Perú. Máster en Derecho Digital y Sociedad de la Información por la Universidad de Barcelona (España).

Eduardo López Román (España)

Abogado especializado en Derecho Digital, ciberseguridad y "Compliance". Abogado colegiado en el Ilustre Colegio de la Abogacía de Barcelona (ICAB). Coordinador y profesor del Máster en Derecho Digital y Sociedad de la Información de la Universidad de Barcelona – IL3 (España). Coordinador y profesor del Máster en Accesibilidad Digital de la Universidad de Barcelona (España). Coordinador y profesor del Curso de Formación para Delegados de Protección de Datos del ICAB.

Coordinador:

Eduardo López Román

Vocal de la Junta Directiva de ENATIC

RÉGIMEN JURÍDICO DE PROTECCIÓN DE DATOS EN PERÚ: ESTUDIO COMPARATIVO CON LA UE

1.- INTRODUCCIÓN

Vivimos un mundo **autopoyético** (cuya traducción del griego significa autocreación), en donde con claridad podemos afirmar que "*en el Siglo XX vivíamos en una sociedad del riesgo, sin embargo, a principios del Siglo XXI, vivimos en una sociedad del desconocimiento".* Si tratamos de hacer una breve reflexión sobre esta corta, pero significativa frase, podemos concluir que vivimos no sólo en un mundo hiperconectado, globalizado, digital, disruptivo, siliconizado, sino que además pese a tener todo a la mano, no sabemos de nada a la vez, como ya lo decía el gran filósofo griego Sócrates.

En ese orden, sabemos que lo retos que viven los países de Latinoamérica son diversos como, por ejemplo, gobernanza en Inteligencia Artificial, Recursos Humanos, Educación, Infraestructura, Regulación, Ética, Ecosistema de Datos, y es sobre este último punto donde deseamos detenernos, ya que ante un Tsunami de tecnologías nos hacemos la siguiente pregunta: ¿Cuál es la vinculación de las normativas en protección de datos con los estándares internacionales?, ¿Realmente contamos con normas pro-ciudadano para la protección de datos personales?, ¿Las normas son eficaces para combatir las amenazas en protección de datos personales?., por citar algunas interrogantes.

Ahora bien, es prácticamente un dogma de fe señalar que la protección de los datos personales es un derecho fundamental que le permite a toda persona preservar su intimidad frente a cualquier tratamiento que resulte desproporcionado, abusivo o irregular con sus datos personales; en ese sentido, tampoco es un tabú saber que la globalización ha venido impactando de una manera notable es la sociedad y realidad, la cual los derechos de las personas no son ajenos, más aún si las distintas tecnologías disruptivas han puesto en clara evidencia que el clásico modelo Hobesiano o estatocéntrico de tutelas de derechos y libertades resultan totalmente insuficiente para afrontar nuevos desafíos que podrían poner en peligro bienes jurídicos tutelados como es el de la protección de los datos personales de las personas.

Es por ello, que el presente artículo pretender brindar elementos para comprender la magnitud que ostenta el derecho de la protección de datos en Perú, así como las similitudes y diferencias que existen entre la norma local y su referente internacional como es el Reglamento General de Protección de Datos Personales (RGPD), a fin de poder saber si Perú podría ser calificado por la Comisión Europea con un nivel equivalente a los estándares exigidos por la Unión Europea.

Régimen Jurídico de Protección de Datos Personales en el Perú

Sobre el particular, es correcto empezar señalando que la Constitución Política del Perú en su numeral 6 artículo 2 nos recuerda que toda persona tiene derecho a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad

personal y familiar.

En caso lo anterior sea vulnerado, el Código Procesal Constitucional determina en su numeral 2 del artículo 61, que toda persona puede acudir al proceso constitucional de habeas data para conocer, actualizar, incluir y suprimir o rectificar la información o datos referidos a su persona que se encuentren almacenados o registrados en forma manual, mecánica o informática, en archivos, bancos de datos o registros de entidades públicas o de instituciones privadas que brinden servicios o acceso a terceros.

Esto es perfectamente concordante con lo dispuesto en el artículo 200 inciso 3, de la Carta Magna, la cual nos indica que la acción de habeas data procede contra el hecho u omisión, por parte de cualquier autoridad, funcionario persona, que vulnera o amenaza los derechos a que se refiere el artículo 2, incisos 5[1] y 6[2] de la Constitución; siendo tales artículos los mismos que regulan los derechos de acceso a la información pública y protección de datos personales, respectivamente.

Asimismo, y ahondando en el Habeas Data podemos destacar que a nivel Jurisprudencial, el Tribunal Constitucional, adoptó por decirlo así una especie de tipología con base a los artículos 200, inciso 3 y 2 de la Constitución y en las normas del Código Procesal Constitucional, delineando de esta manera distintos tipos de Habeas Data vigentes en el Perú (Expediente N° 06164-2007-HD/TC), del cual textualmente se expresa de los siguientes: Hábeas Data Puro[3], Hábeas Data de Cognición[4], Hábeas Data Informativo[5], Hábeas Data Inquisitivo[6], Hábeas Data Teleológico[7], Hábeas Data de Ubicación[8], Hábeas Data Manipulador[9], Hábeas Data Aditivo[10], Hábeas Data Correctivo[11],

[1] **CONSTITUCIÓN POLÍTICA DEL PERÚ**
TÍTULO I
DE LA PERSONA Y DE LA SOCIEDAD
CAPÍTULO I
DERECHOS FUNDAMENTALES DE LA PERSONA
(…)
Artículo 2.- Derechos Fundamentales de la Persona. Toda persona tiene derecho:
(…)
5. A solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal, con el costo que suponga el pedido. Se exceptúan las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional.

[2] **CONSTITUCIÓN POLÍTICA DEL PERÚ**
TÍTULO I
DE LA PERSONA Y DE LA SOCIEDAD
CAPÍTULO I
DERECHOS FUNDAMENTALES DE LA PERSONA
(…)
Artículo 2.- Derechos Fundamentales de la Persona. Toda persona tiene derecho:
(…)
6. A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar.

[3] ***Hábeas Data Puro:*** Reparar agresiones contra la manipulación de datos personalísimos almacenados en banco de información computarizados o no.

[4] ***Hábeas Data de Cognición:*** No se trata de un proceso en virtud del cual se pretende la manipulación de datos, sino efectuar una tarea de conocimiento y supervisión sobre la forma en que la información personal almacenada está siendo utilizada.

[5] ***Hábeas Data Informativo.*** Está dirigido a conocer el contenido de la información que se almacena en el banco de datos (qué se guarda).

[6] ***Hábeas Data Inquisitivo.*** Para que se diga el nombre de la persona que proporcionó el dato (quién).

[7] ***Hábeas Data Teleológico.*** Busca establecer los motivos que han llevado al sujeto activo a la creación del dato personal (para qué).

[8] ***Hábeas Data de Ubicación.*** Tiene como objeto que el sujeto activo del poder informático responda dónde está ubicado el dato, a fin de que el sujeto pasivo (el accionante) pueda ejercer su derecho (dónde).

Hábeas Data Supresorio[12], Hábeas Data Confidencial[13], Hábeas Data Desvinculador[14], Hábeas Data Cifrador[15], Hábeas Data Cautelar[16], Hábeas Data Garantista[17], Hábeas Data Interpretativo[18], Hábeas Data Indemnizatorio[19], Hábeas Data Impuro[20], Hábeas Data de Acceso a la Información Pública[21].

Punto concordante y que merece a su vez la pena también hacer mención es respecto al derecho de autodeterminación informativa el cual, la Constitución Política del Perú, en su artículo 2, inciso 6, ha recogido del siguiente modo el derecho a la autodeterminación informativa: *"toda persona tiene derecho a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar"*. Por su parte, el artículo 61, inciso 2, del Código Procesal Constitucional ha recogido una definición más amplia del referido derecho: *"Toda persona puede acudir al [proceso de hábeas data] para conocer, actualizar, incluir y suprimir o rectificar la información o datos referidos a su persona que se encuentren almacenados o registrados en forma manual, mecánica o informática, en archivos, bancos de datos o registros de entidades públicas o de instituciones privadas que brinden servicio o acceso a terceros. Asimismo, a hacer suprimir o impedir que se suministren datos o informaciones de carácter sensible o privado que afecten derechos constitucionales"*.

Ahora bien y sobre este derecho de autodeterminación informativa se puede indicar que el Tribunal ha establecido que: *"el derecho a la autodeterminación informativa consiste en la serie de facultades que tiene toda persona para ejercer control sobre la información personal que le concierne, contenida en registros ya sean públicos, privados o informáticos, a fin de enfrentar las posibles extralimitaciones de los mismos. Se encuentra estrechamente ligado a un control sobre la*

[9] ***Hábeas Data Manipulador.*** No tiene como propósito el conocimiento de la información almacenada, sino su modificación.

[10] ***Hábeas Data Aditivo.*** Agrega al banco de datos una información no contenida. Esta información puede consistir: en la actualización de una información cierta pero que por el paso del tiempo se ha visto modificada; también puede tratarse de una información que tiene como objeto aclarar la certeza de un dato que ha sido mal interpretado; o incorporar al banco de datos una información omitida que perjudica al sujeto pasivo.

[11] ***Hábeas Data Correctivo.*** Tiene como objeto modificarlos datos imprecisos y cambiar o borrar los datos falsos.

[12] ***Hábeas Data Supresorio.*** Busca eliminar la información sensible o datos que afectan la intimidad personal, familiar o cualquier otro derecho fundamental de la persona. También puede proceder cuando la información que se almacena no guarda relación con la finalidad para la cual ha sido creado el banco de datos.

[13] ***Hábeas Data Confidencial.*** Impedir que las personas no autorizadas accedan a una información que ha sido calificada como reservada. En este tipo, se incluye la prohibición de datos que por el paso del tiempo o por sentencia firme se impide su comunicación a terceros.

[14] ***Hábeas Data Desvinculador.*** Sirve para impedir que terceros conozcan la identificación de una o más personas cuyos datos han sido almacenados en función de determinados aspectos generales como la edad, raza, sexo, ubicación social, grado de instrucción, idioma, profesión.

[15] ***Hábeas Data Cifrador.*** Tiene como objeto que el dato sea guardado bajo un código que sólo puede ser descifrado por quien está autorizado a hacerlo.

[16] ***Hábeas Data Cautelar.*** Tiene como propósito impedir la manipulación o publicación del dato en el marco de un proceso, a fin de asegurar la eficacia del derecho a protegerse.

[17] ***Hábeas Data Garantista.*** Buscan el control técnico en el manejo de datos, a fin de determinar, si el sistema informativo, computarizado o no, garantiza la confidencialidad y las condiciones mínimas de seguridad de los datos y su utilización de acuerdo con la finalidad para la cual han sido almacenados.

[18] ***Hábeas Data Interpretativo.*** Tiene como objeto impugnar las valoraciones o conclusiones a las que llega el que analiza la información personal almacenada.

[19] ***Hábeas Data Indemnizatorio.*** Aunque no está estipulado en nuestro ordenamiento jurídico, este tipo de habeas data consiste en solicitar la indemnización por el daño causado con la propalación de la información.

[20] ***Hábeas Data Impuro.*** Solicitar el auxilio jurisdiccional para recabar una información pública que le es negada al agraviado.

[21] ***Hábeas Data de Acceso a la Información Pública.*** Consiste en hacer valer el derecho de toda persona a acceder a la información que obra en la Administración Pública, salvo las que estén expresamente prohibidas por la Ley.

información, como una autodeterminación de la vida íntima, de la esfera personal. Mediante la autodeterminación informativa se busca proteger a la persona en sí misma, no únicamente en los derechos que conciernen a su esfera personalísima, sino a la persona en la totalidad de ámbitos; por tanto, no puede identificarse con el derecho a la intimidad, personal o familiar, ya que mientras éste protege el derecho a la vida privada, el derecho a la autodeterminación informativa busca garantizar la facultad de todo individuo de poder preservarla ejerciendo un control en el registro, uso y revelación de los datos que le conciernen (…). En este orden de ideas, el derecho a la autodeterminación informativa protege al titular delmismo frente a posibles abusos o riesgos derivados de la utilización de los datos, brindando al titular afectado la posibilidad de lograr la exclusión de los datos que considera "sensibles" y que no deben ser objeto de difusión ni de registro; así como le otorga la facultad de poder oponerse a la transmisión y difusión de los mismos" (STCs 04739-2007-PHD/TC, FF.JJ. 2-4 y 0746-2010-PHD/TC, FJ. 4).

Posteriormente, la Ley Nº 29733, Ley de Protección de Datos Personales, publicada el 03 de julio de 2011[22], y su correspondiente Reglamento, aprobado por Decreto Supremo N° 003-2013-JUS, y publicado el 22 de marzo de 2013, son los ejes concéntricos que regulan este derecho comentado. Asimismo, y con el fin de fortalecerlo, es en el año 2017, que se publicó el en Diario Oficial El Peruano, el Decreto Legislativo N° 1353 – Decreto Legislativo que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, Fortalece el Régimen de Protección de Datos Personales y la Regulación de la Gestión de Intereses.

Atendiendo a la Ley de Protección de Datos Personales peruana, esta precisa los derechos que corresponden al titular de datos personales, esto es, los supuestos protegidos por el derecho de autodeterminación informativa, los cuales corresponden a los siguientes:

"**Artículo 18. Derecho de información del titular de datos personales [*Hábeas Data de Cognición*]**
El titular de datos personales tiene derecho a ser informado en forma detallada, sencilla, expresa, inequívoca y de manera previa a su recopilación, sobre la finalidad para la que sus datos personales serán tratados; quiénes son o pueden ser sus destinatarios, la existencia del banco de datos en que se almacenarán, así como la identidad y domicilio de su titular y, de ser el caso, del encargado del tratamiento de sus datos personales; el carácter obligatorio o facultativo de sus respuestas al cuestionario que se le proponga, en especial en cuanto a los datos sensibles; la transferencia de los datos personales; las consecuencias de proporcionar sus datos personales y de su negativa a hacerlo; el tiempo durante el cual se conserven sus datos personales; y la posibilidad de ejercer los derechos que la ley le concede y los medios previstos para ello (…).

Artículo 19. Derecho de acceso del titular de datos personales
El titular de datos personales tiene derecho a obtener la información que sobre sí mismo sea objeto de tratamiento en bancos de datos de administración pública o privada, la forma en que sus datos fueron recopilados, las razones que motivaron su recopilación y a solicitud de quién se

[22] Aunque su entrada en vigor fue en el año 2013, ello conforme a la Duodécima Disposición Complementaria Final de la Ley de Protección de Datos Personales, su vigencia plena se dio a los 30 días hábiles de publicado el Reglamento de la Ley antes indicada.

realizó la recopilación, así como las transferencias realizadas o que se prevén hacer de ellos.

Artículo 20. Derecho de actualización, inclusión, rectificación y supresión [*Hábeas Data Manipulador*]
El titular de datos personales tiene derecho a la actualización, inclusión, rectificación y supresión de sus datos personales materia de tratamiento, cuando estos sean parcial o totalmente inexactos, incompletos, cuando se hubiere advertido omisión, error o falsedad, cuando hayan dejado de ser necesarios o pertinentes a la finalidad para la cual hayan sido recopilados o cuando hubiera vencido el plazo establecido para su tratamiento (…).

Artículo 21. Derecho a impedir el suministro [*Hábeas Data Cautelar*]
El titular de datos personales tiene derecho a impedir que estos sean suministrados, especialmente cuando ello afecte sus derechos fundamentales. El derecho a impedir el suministro no aplica para la relación entre el titular del banco de datos personales y el encargado del banco de datos personales para los efectos del tratamiento de estos.

Artículo 22. Derecho de oposición
Siempre que, por ley, no se disponga lo contrario y cuando no hubiera prestado consentimiento, el titular de datos personales puede oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En caso de oposición justificada, el titular o el encargado del banco de datos personales, según corresponda, debe proceder a su supresión, conforme a ley.

Artículo 23. Derecho al tratamiento objetivo [*Hábeas Data Interpretativo*]
El titular de datos personales tiene derecho a no verse sometido a una decisión con efectos jurídicos sobre él o que le afecte de manera significativa, sustentada únicamente en un tratamiento de datos personales destinado a evaluar determinados aspectos de su personalidad o conducta, salvo que ello ocurra en el marco de la negociación, celebración o ejecución de un contrato o en los casos de evaluación con fines de incorporación a una entidad pública, de acuerdo a ley, sin perjuicio de la posibilidad de defender su punto de vista, para salvaguardar su legítimo interés.

Artículo 24.- Derecho a la tutela
En caso de que el titular o el encargado del banco de datos personales deniegue al titular de datos personales, total o parcialmente, el ejercicio de los derechos establecidos en esta Ley, este puede recurrir ante la Autoridad Nacional de Protección de Datos Personales en vía de reclamación o al Poder Judicial para los efectos de la correspondiente acción de hábeas data (…).

Artículo 25. Derecho a ser indemnizado [*Hábeas Data Indemnizatorio*]
El titular de datos personales que sea afectado a consecuencia del incumplimiento de la presente Ley por el titular o por el encargado del banco de datos personales o por terceros, tiene derecho a obtener la indemnización correspondiente, conforme a ley (…)".

Ante todo lo dicho, Perú, si bien cuenta con una normativa de protección de datos personales y su

correspondiente reglamento, creemos que es totalmente insuficiente, si es que no se acude a la cooperación internacional, ya que tomando como referencia las palabras del premio nobel Joseph Stiglitz: *"esta crisis no la superaremos con actitudes individualistas, ni con egoísmos"*.

Asimismo, si bien las leyes son necesarias, estas tampoco son determinantes, ya que junto con la norma debe existir una comprensión y/o educación digital por parte de los ciudadanos, por ello es menester y responsabilidad del Estado maximizar lo que muchos autores denominan "la alfabetización o catequesis digital" en temas de privacidad y protección de datos personales. Por ello, creemos firmemente que uno de los modelos a imitar sería en de la Unión Europea la cual empodera a sus ciudadanos en la tutela de derechos y la protección de sus correspondientes datos personales, promoviendo una verdadera cultura democrática que se fundamenta en la "autodeterminación informativa". Más aún si sabemos que el mundo digital nace de la relación de autoayuda entre unos y otros. Ciudadanía cooperativa. Y no una capitalización o una empresa que nos trata a los seres humanos como "simples datos".

2.- TABLA COMPARATIVA DE LA NORMATIVA DE PROTECCIÓN DE DATOS: DEFINICIONES, PRINCIPIOS, DERECHOS, OBLIGACIONES DEL RESPONSABLE Y ENCARGADO, COMPETENCIAS DE LAS AUTORIDADES DE SUPERVISIÓN, FUNCIONES DEL DPD Y RÉGIMEN DE TRANSFERENCIAS INTERNACIONALES (ANÁLISIS BASADO DE LOS ANEXOS 1 Y 2).

Definiciones:

Datos Personales (RGPD, LPDP, RLPDP).
Sobre el particular podemos indicar que tanto la normativa europea de protección de datos como la legislación peruana sobre la materia confluyen en directrices tutelares similares ya que ambas direccionas la protección teleológica de la persona humana.

Responsable del Tratamiento (RGPD, LPDP, RLPDP).
En lo que atañe a este concepto podemos dejar constancia que la normativa europea es mucho más completa en lo que refiere a su definición, más no en su ejecución; ya que respecto de la primera el RGPD enumera a los responsables, lo cual no hace la ley peruana; pero al momento de definir las acciones que determinan quien es considerado responsable, ambas leyes sí lo hacen, bajo el acápite: *responsable es quien decide o determina el tratamiento de los datos personales*.

Encargado del Tratamiento (RGPD, LPDP, RLPDP).
Vemos que ambas normativas, tanto la europea como la peruana, extienden subjetivamente y de modo expreso el alcance de quien debe ser considerado como encargado del tratamiento de los datos personales.

Delegado de Protección de Datos (RGPD, LPDP, RLPDP).
Acá notamos que la normativa europea tiene una actuación estelar en el modelo de cumplimiento del RGPD, el mismo que ostenta de encargado de tratamiento de las obligaciones legales en materia de protección de datos personales. Por otro lado, y en lo que respecto a la legislación peruana sobre protección de datos personales podemos indicar que actualmente esta figura no se encuentra contemplada de manera normativa; lo más cercano que podemos encontrar es lo que señala el Decreto Legislativo 1412 – Ley del Gobierno Digital, el cual indica que las instituciones públicas deben designar a un oficial de datos personales (ODP), pero no se indica nada respecto de las empresas privadas u otras alternas.

Evaluación de impacto (RGPD, LPDP, RLPDP)
Una diferencia latente es lo referente a la evaluación de impacto sobre protección de datos, la misma que en la legislación peruana no se encuentra positivizado ni en la LPDP (Ley de Protección de Datos Personales), ni en el RLPDP (Reglamento de la Ley de Protección de Datos Personales); caso contrario sucede en el Reglamento General de Protección de Datos europeo, el cual tiene notable importancia ya que obliga a las autoridades de control a establecer listas orientativas de tratamientos que no requieren el EIPD, así como también de tratamientos que si requieren su correspondiente realización.

Privacidad desde el Diseño y por Defecto (RGPD, LPDP, RLPDP).
Con la protección de datos desde el diseño el Reglamento General de Protección de Datos pretende incluir los principios de protección de datos dentro de las organizaciones en el devenir de toda la vida del tratamiento; asimismo con la protección por defecto se establece que deberán aplicarse medidas técnicas y organizativas que sean apropiadas, ello con el objeto de que se efectúen los tratamientos que realmente sean necesarios para los fines del tratamiento; ambas situaciones de privacidad vemos y notamos que no se encuentran positivizadas en la normativa de protección de datos peruana.

Notificación y comunicación de brechas de seguridad (RGPD, LPDP, RLPDP).
El RGPD señala taxativamente que tan pronto el responsable del tratamiento tenga conocimiento de que se ha producido una brecha de datos personales se deberá de efectuar la correspondiente notificación a la autoridad de control competente, estableciendo un plazo legal de 72 horas para su cumplimiento. Asimismo, la normativa antes señalada establece una obligación para comunicar a los afectados cuyos datos personales se hayan visto afectados por una brecha de seguridad y que hayan comprometido su integridad, confidencialidad y/o disponibilidad. En la normativa peruana sobre el tema de estudio, notamos que legislativamente no existe tal obligación legal.

Definiciones: Autoridad de Control (RGPD, LPDP, RLPDP).
RGPD. Autoridad de Control: la autoridad independiente establecida por un Estado miembro con arreglo a lo dispuesto en el artículo 51.
LPDP. Entidad pública. Entidad comprendida en el artículo I del Título Preliminar de la Ley 27444, Ley del Procedimiento Administrativo General, o la que haga sus veces.
RLPDP. Dirección General de Protección de Datos Personales: Es el órgano encargado de ejercer a Autoridad Nacional de Protección de Datos Personales a que se refiere el artículo 32 de la Ley, pudiendo usarse indistintamente cualquiera de dichas denominaciones.

Tratamiento Transfronterizo (RGPD, LPDP, RLPDP)
Si bien la normativa y el reglamento de la ley peruana tratan acápites referidos al tratamiento transfronterizo de datos personales; es correcto señalar que no existe un nivel de idoneidad para la correcto aplicación y cumplimiento del mismo; situación que si sucede en el RGPD, ya que por ejemplo esta última cuenta con una clasificación sobre la materia, lo cual no sucede en la normativa expuesta en primer lugar.

Servicio de la Sociedad de la Información (RGPD, LPDP, RLPDP)
Sabemos que con el uso del internet y las tecnologías de la información se ha provocado una expansión de la sociedad de la información con su correspondiente protección de los derechos digitales, siendo uno de ellos, la protección de los datos personales; en tal medida notamos que el RGPD detalla y conceptualiza lo que se debe de entender por el servicio de sociedad de la información; situación distinta sucede en la ley peruana de protección de datos personales, el cual no es definido, ni conceptualizado.

Autoridad de control (RGPD, LPDP, RLPDP)
Aunque podemos observar que las autoridades de control tanto de la Unión Europea y de Perú

que se encuentran encargadas de velar por el cumplimiento de la normativa sobre protección de datos personales, así como garantizar y tutelar este derecho fundamental a favor de sus ciudadanos; sin embargo notamos que el RGPD le otorga a sus autoridades una mayor amplitud de actuación como por ejemplo el hecho exigir a sus sujetos fiscalizados el cumplimiento de la privacidad desde el diseño y por defecto.

Elaboración de perfiles (RGPD, LPDP, RLPDP)

Cuando se lleva a cabo un tratamiento de datos personales, la referencia a aspectos que se analizan o evalúan pueden ser por ejemplo a la personalidad del interesado o de su correspondiente comportamiento, así como sus intereses y hábitos; por ello la elaboración de un perfil puede implicar un tratamiento analítico de datos personales masivos; en ese sentido si bien el RGPD detalla postulados al respecto, la normativa peruana de protección de datos personales no lo estipula legislativamente.

3.- ANÁLISIS DE LOS REQUISITOS DE TRANSFERENCIAS INTERNACIONALES DE DATOS: DE LA UE A PERÚ.

Según el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos o RGPD), las transferencias internacionales de datos suponen un flujo de datos personales desde los países de la Unión Europea (UE) y Espacio Económico Europeo (EEE)a destinatarios establecidos en países fuera de dichos territorios.

Cuando las entidades receptoras de los datos se encuentren en un país, un territorio o uno o varios sectores específicos de ese país u organización internacional que hayan sido declarados de nivel de protección adecuado por la Comisión Europea se considerarán transferencias equiparables con un nivel de adecuación de los estados de la UE y EEE.

Hasta la fecha los países y territorios están declarados como adecuados:

- Suiza. Decisión 2000/518/CE de la Comisión, de 26 de julio de 2000
- Canadá. Decisión 2002/2/CE de la Comisión, de 20 de diciembre de 2001, respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos
- Argentina. Decisión 2003/490/CE de la Comisión, de 3 de junio de 2003
- Guernsey. Decisión 2003/821/CE de la Comisión, de 21 de noviembre de 2003
- Isla de Man. Decisión 2004/411/CE de la Comisión, de 28 de abril de 2004
- Jersey. Decisión 2008/393/CE de la Comisión, de 8 de mayo 2008
- Islas Feroe. Decisión 2010/146/UE de la Comisión, de 5 de marzo de 2010
- Andorra. Decisión 2010/625/UE de la Comisión, de 19 de octubre de 2010
- Israel. Decisión 2011/61/UE de la Comisión, de 31 de enero de 2011
- Uruguay. Decisión 2012/484/UE, de la Comisión, de 21 de agosto de 2012.
- Nueva Zelanda. Decisión 2013/65/UE de la Comisión, de 19 de diciembre de 2012
- Japón. Decisión de 23 de enero de 2019.
- Reino Unido. Decisión de 28 de junio de 2021
- Corea del sur. Decisión de 17 de diciembre de 2021

Por otro lado, el Tribunal de Justicia de la Unión Europea (TJUE) invalidó la Decisión (UE) 2016/1250 de la Comisión, de 12 de julio de 2016, conocida como el Escudo de Privacidad para las transferencias de datos a los estados Unidos. En este supuesto y en aquellos otros con destinatarios sin nivel adecuado, a falta de decisión de adecuación se deberán ofrecen garantías adecuadas, que podrán ser aportadas a través de:

a. Un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos
b. Normas corporativas vinculantes
c. Cláusulas tipo de protección de datos adoptadas por la Comisión.
d. Cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión
e. Códigos de conducta, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas las relativas a los derechos de las personas interesadas
f. Mecanismos de certificación, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas las relativas a los derechos de las personas interesadas.

Con fecha 4 de junio de 2021, la Comisión Europea publicó el nuevo conjunto de cláusulas contractuales tipo que, además de sustituir a sus predecesoras, pretenden poder abarcar las transferencias entre responsables, entre responsable y encargado, entre encargados y entre encargado y responsable.

Las nuevas cláusulas se adaptan al RGPD incorporando los principios de responsabilidad proactiva y tratan de adoptar los criterios señalados por el Tribunal de Justicia de la Unión Europea (TJUE) en la sentencia del caso Schrems II.

No obstante, es necesario que el exportador de los datos, en su caso ayudado por el importador, analice el impacto que la legislación y/o la práctica vigente en el país del importador, en este caso Perú, pueda tener en el nivel de protección proporcionado, de forma que sea esencialmente equivalente al que proporciona el marco europeo. Además, adicionalmente, deberán tenerse en cuenta las directrices del Comité Europeo de Protección de Datos sobre **las medidas suplementarias** que se consideren adecuadas adoptar para garantizar ese nivel de protección equivalente.

Las medidas suplementarias se detallan en la Recomendación 01/2020 del CEPD. Dicho documento establece de forma general, además de las medidas suplementarias, todos los pasos que debe seguir el exportador con la colaboración del importador de los datos con la finalidad de poder considerar que se garantiza un nivel de protección equivalente a la UE en el tratamiento de los datos transferidos.

A continuación se detallan los seis pasos:

1.-*Como primer paso, la CEPD les aconseja a los exportadores, que conozcan sus transferencias.* *Mapear todas las transferencias de datos personales a terceros países puede ser un ejercicio difícil. Sin embargo, es necesario saber adónde van los datos personales para garantizar que se les proporcione un nivel de protección esencialmente equivalente dondequiera que se procesen. También debe verificar que los datos que transfiere son adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.*

2.-*Un segundo paso es verificar la herramienta en la que se basa su transferencia, entre las enumeradas en el Capítulo V del RGPD*. *Si la Comisión Europea ya ha declarado adecuado el país, región o sector al que estás transfiriendo los datos, a través de una de sus decisiones de adecuación en virtud del artículo 45 del RGPD o en virtud de la anterior Directiva 95/46, siempre y cuando la decisión siga vigente, no necesitará realizar ningún otro paso, aparte de controlar que la decisión de adecuación siga siendo válida. En ausencia de una decisión de adecuación, debe confiar en una de las herramientas de transferencia enumeradas en los artículos 46 del RGPD. Solo en algunos casos podrá acogerse a una de las excepciones previstas en el artículo 49 del RGPD si cumple las condiciones. Las excepciones no pueden convertirse en "la norma" en la práctica, sino que deben restringirse a situaciones específicas.*

3.-*Un tercer paso es evaluar si hay algo en la ley o las prácticas vigentes del tercer país que pueda afectar la eficacia de las garantías adecuadas de las herramientas de transferencia en las que confía*, *en el contexto de su transferencia específica. Su evaluación debe centrarse ante todo en la legislación de un tercer país que sea relevante para su transferencia y la herramienta de transferencia del artículo 46 del RGPD en la que confía. Examinar también las prácticas de las autoridades públicas del tercer país permitirá para verificar si las garantías contenidas en la herramienta de transferencia pueden garantizar, en la práctica, la protección efectiva de los datos personales transferidos. Examinar estas prácticas será especialmente relevante para su evaluación cuando:*

> *i) la legislación del tercer país, que cumple formalmente las normas de la UE, no se aplica/no se cumple manifiestamente en la práctica;*
> *(ii) existen prácticas incompatibles con los compromisos de la herramienta de transferencia cuando se carece de la legislación pertinente en el tercer país;*
> *(iii) sus datos transferidos y/o el importador caen o podrían caer dentro del alcance de la legislación problemática (es decir, infringiendo la garantía contractual de la herramienta de transferencia de un nivel de protección esencialmente equivalente y no cumpliendo con los estándares de la UE sobre derechos fundamentales, necesidad y proporcionalidad).*

En las dos primeras situaciones, deberá suspender la transferencia o implementar las medidas complementarias adecuadas si desea continuar con la misma.

En la tercera situación, a la luz de las incertidumbres que rodean la posible aplicación de legislación problemática a su transferencia, puede decidir: suspender la transferencia; implementar medidas complementarias para proceder con la misma; o alternativamente, puede decidir proceder con la transferencia sin implementar medidas complementarias si considera y puede demostrar y documentar que no tiene motivos para creer que la legislación relevante y problemática se interpretará y/o aplicará en la práctica para cubrir sus datos transferidos e importador.

Para evaluar los elementos que deben tenerse en cuenta al evaluar la ley de un tercer país que trata el acceso a los datos por parte de las autoridades públicas con fines de vigilancia, se deben consultar las recomendaciones de Garantías Esenciales Europeas del CEPD.

Se debe realizar esta evaluación con la debida diligencia y documentarla minuciosamente. Las autoridades de control y/o judiciales competentes podrán solicitarla documentación de la evaluación correspondiente y por lo tanto, responsabilizar por cualquier decisión que tome el exportador sobre esa base.

4.-*Un cuarto paso es identificar y adoptar las medidas complementarias que sean necesarias para llevar el nivel de protección de los datos transferidos al estándar de la UE de equivalencia esencial.* *Este paso solo es necesario si su evaluación revela que la legislación y/o las prácticas del tercer país inciden en la eficacia de la herramienta de transferencia del artículo 46 del RGPD en la que confía o en la que pretende confiar en el contexto de su transferencia.*

Como es el caso de las salvaguardas apropiadas contenidas en las herramientas de transferencia del Artículo 46, algunas medidas complementarias pueden ser efectivas en algunos países, pero no necesariamente en otros. El exportador será responsable de evaluar su efectividad en el contexto de la transferencia, y a la luz de las leyes y prácticas del tercer país y la herramienta de transferencia en la que se basa, ya que será responsable de cualquier decisión que tome sobre esa base. Esto también puede requerir que se combine varias medidas complementarias. Es posible que, en última instancia, se descubra que ninguna medida complementaria puede garantizar un nivel de protección esencialmente equivalente para su transferencia específica. En aquellos casos en los que no proceda ninguna medida complementaria, se deberá evitar, suspender o terminar la transferencia para no comprometer el nivel de protección de los datos personales. También se deberá realizar esta evaluación de medidas complementarias con la debida diligencia y documentarla.

5.-*Un quinto paso es realizar los pasos procesales formales que pueda requerir la adopción de su medida complementaria, según la herramienta de transferencia del artículo 46 del RGPD en la que se base.* *Es posible que se deba consultar a las autoridades de supervisión competentes del exportador sobre algunas de ellas.*

6.-El sexto y último paso es reevaluar, en intervalos apropiados, el nivel de protección otorgado a los datos personales que se transfieren a terceros países y monitorear si ha habido o habrá cambios que puedan afectarlos. *El principio de responsabilidad proactiva requiere una vigilancia continua del nivel de protección de los datos personales.*

Se debe tener en cuenta que las autoridades de control siempre continuarán ejerciendo su mandato para monitorear la aplicación del RGPD y hacerlo cumplir. Las autoridades de control prestan la debida atención a las acciones que toman los exportadores para garantizar que los datos que transfieren reciban un nivel de protección esencialmente equivalente. Como recuerda el Tribunal de Justicia de la UE, las autoridades de control podrán suspender o prohibir las transferencias de datos en aquellos casos en los que, tras una investigación o una denuncia, comprueben que no puede garantizarse un nivel de protección esencialmente equivalente.

Por ello, las autoridades de control desarrollan la orientación para los exportadores y se coordinan en sus acciones con el CEPD para garantizar la coherencia en la aplicación de la ley de protección de datos de la UE.

4.- CONCLUSIONES

- El Reglamento General de Protección de Datos de la Unión Europea posee un amplio abanico de elementos que empoderan mejor a sus ciudadanos respecto de las leyes peruanas, como por ejemplo el principio de responsabilidad proactiva, la obligación de comunicar brechas de seguridad, derecho al olvido entre otros.

- Actualmente, el Perú si bien positiviza el derecho de protección de datos como uno de corte constitucional, así como cuenta con leyes que exteriorizan su respectivo cumplimiento, ello todavía no es suficiente para ser considerado por la Unión Europea como un país con nivel adecuado de protección de datos como sí lo ostentan Argentina y Uruguay. Motivo por el cual el Perú debería de actualizar sus respectivas normas para lograr su credencialización en la UE.

- La seguridad de la información tiene como objetivo asegurar su confidencialidad, disponibilidad e integridad, a fin de proteger los datos personales de los usuarios y/o consumidores ya sea por empresas o entidades públicas, ya que hay que tener presente que sin seguridad no hay protección de datos personales.

- Las transferencias internacionales de datos personales, cuando el país que recibe una transferencia internacional no goza de la certificación internacional, por ejemplo, el Perú, requerirá de garantías que proporcionen un nivel de protección adecuado aprobadas por instrumentos jurídicos vinculantes como lo detalla los seis pasos establecidos en la Recomendación 01/2020 del Comité Europeo de Protección de Datos (CEPD).

- Si bien es complicado lograr que países de múltiples culturas y variados regímenes legales encuentren normas comunes que todos decidan aceptar, existe también la posibilidad de celebrar acuerdos o tratados multilaterales para la facilitación del comercio transfronterizo que establezcan ciertos parámetros mínimos para facilitar el flujo de datos personales que como ya se evidenció, es vital para realizar negocios (y especialmente negocios que usen internet en algún paso del proceso transaccional o de distribución del producto).

- Atendiendo a la fecha de emisión, si bien la normativa peruana puede ser calificada como una ley post digital, esto difiere cuando revisamos su estructura y cuerpo legal, la misma que puede ser calificada como una ley pre digital debido a la falta de instituciones y mecanismos que exige la actualidad jurídica; lo que en ocasiones puede dar lugar a dudas sobre su interpretación pues requieren prestar atención a la necesidad de una aplicación adecuada considerando, claro está, los avances que se producen en los ámbitos social, económico y tecnológico.

- Se distinguen distintos tipos de regulaciones como la regulación existente, actualizada y a la medida; en ese sentido, la práctica señala que los países con niveles más altos de aprobación en protección de datos suelen tener regulaciones actualizadas en vez de

regulaciones a medida, ya que de esta forma las leyes existentes se modifican para responder de forma más rápida a las nuevas situaciones que nos propone la sociedad de la información, siendo que en el caso del Perú se recomienda adoptar lo diseñado por el RGPD.

- El fenómeno del IoT, el Big Data, la Inteligencia Artificial, el Machine Learning, Blockchain, entre otros proponen grandes retos a las normativas de protección de datos personales en la medida en que se requieren formas ágiles de lograr el cumplimiento de los principios neurálgicos y derechos consubstancial a favor de los ciudadanos como los propone el RGPD; el cual el Perú debería tomar como referencia teleológica en favor de sus pobladores.

- Por todo ello, se debe fomentar una más estrecha colaboración de ambos continentes entre profesionales en Derecho Digital y, de forma especial, en privacidad y protección de datos para lograr objetivos comunes en el marco de garantías de la protección de datos personales con la finalidad de impulsar los beneficios de la sociedad de la información y del conocimiento.

ENATIC, como la asociación referente en Europa y gran parte de Latinoamérica en la promoción de la abogacía TIC (tecnologías de la información y comunicación) y el Derecho Digital, trabajamos para crear puentes entre profesionales de ambos continentes para un mayor entendimiento de todas las sociedades a través de la difusión y debate de los derechos digitales como la privacidad y la protección de datos personales.

ANEXO 1: TABLA COMPARATIVA EN NORMATIVAS DE PROTECCIÓN DE DATOS

	UE (RGPD)	LEY 29733 (LPDP) /REGLAMENTO DE LA LPDP
Definiciones	Art. 4	Art. 2 LPDP / Art. 2 RLPDP
Objeto y alcance	Arts. 1-3	Arts. 1 y 3 LPDP / Art. 1, 3, 4 Y 5 RLPDP
Principios	Art. 5	Arts. 4 – 11 LPDP /Arts. 6-10 RLPDP
Bases de licitud	Art. 6	Arts. 13.4, 13.5 Y 13.8 LPDP / Art. 11 RLPDP
Condiciones del consentimiento	Art. 7	Art. 13 LPDP / Art. 11 -12 RLPDP
Categoría especial de datos	Art. 9	Art. 14 RLPDP
Derechos	Arts. 12-23	Arts. 18-25 LPDP /Arts. 47-72 RLPDP
Responsable	Arts. 24-26	Art. 28
Encargado	Arts. 27-28	Art. 28
Registro de actividades de tratamiento	Art. 30	Art. 29 LPDP /Arts. 76-88 RLPDP
Privacidad desde diseño y por defecto	Art. 25	No se encuentra positivizado ni en la LPDP (Ley de Protección de Datos Personales), ni en el RLPDP (Reglamento de la Ley de Protección de Datos Personales).
Medidas de seguridad	Art. 32	Art. 16-17 LPDP / Arts. 39-46 RLPDP
Notificación y comunicación de brechas de seguridad	Arts. 34 y 34	No se encuentra positivizado ni en la LPDP (Ley de Protección de Datos Personales), ni en el RLPDP (Reglamento de la Ley de Protección de Datos Personales).
Evaluación de impacto	Arts. 35 y 36	No se encuentra positivizado ni en la LPDP (Ley de Protección de Datos Personales), ni en el RLPDP (Reglamento de la Ley de Protección de Datos Personales).
Delegado de protección de datos	Arts. 37-39	No se encuentra positivizado ni en la LPDP (Ley de Protección de Datos Personales), ni en el RLPDP (Reglamento de la Ley de

		Protección de Datos Personales). Pero sí en el Decreto Legislativo 1412 – Ley de Gobierno Digital), donde se establece que las instituciones públicas deben designar a un Oficial de Datos Personales (ODP).
Códigos de conducta	**Arts. 40-43**	**Art. 31 LPDP /Arts. 89-97 RLPDP**
Transferencias internacionales de datos	**Arts. 44-50**	**Arts. 15 LPDP / Arts. 18-20, 24-25 RLPDP**
Autoridades de control	**Arts. 51-59**	**Arts. 32-36 LPDP / Art. 115 RLPDP**
Reclamaciones, Infracciones y régimen sancionador	**Arts. 77-84**	**Arts. 37-40 LPDP /Arts. 98-133 RLPDP**

ANEXO 2: TABLA COMPARATIVA DE DEFINICIONES

	UE (RGPD) Artículo 4	LEY 29733 (LPDP) /REGLAMENTO DE LA LPDP
Datos personales **(SIMILITUD) Aunque la definición del RGPD es más completa**	toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona	Toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados. (ART. 2.4. LPDP).
Tratamiento **(SIMILITUD) Aunque la definición del RGPD es más completa**	cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso,	Cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales" (Art. 2.19 LPDP).

	cotejo o interconexión, limitación, supresión o destrucción	
Limitación del tratamiento **(DIFERENCIA)**	el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro	Las limitaciones al ejercicio del derecho fundamental a la protección de datos personales solo pueden ser establecidas por ley, respetando su contenido esencial y estar justificadas en razón del respeto de otros derechos fundamentales o bienes constitucionalmente protegidos. (Art. 13.2 LPDP)
Elaboración de perfiles **(DIFERENCIA) Entendiendo que la normativa peruana no lo conceptualiza de manera positiva (es decir, en Ley)**	toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física	**No lo señala taxativamente ni la Ley de Protección de Datos Personales, ni su Reglamento.**
Seudonimización **(DIFERENCIA) Entendiendo que la normativa peruana no lo conceptualiza de manera positiva (es decir, en Ley)**	el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos	**No lo señala taxativamente ni la Ley de Protección de Datos Personales, ni su Reglamento.**

	personales no se atribuyan a una persona física identificada o identificable	
Fichero **(SIMILITUD)**	todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica	Conjunto de datos de personas naturales no computarizado y estructurado conforme a criterios específicos, que permita acceder sin esfuerzos desproporcionados a los datos personales, ya sea aquel centralizado, descentralizado o repartido de forma funcional o geográfica (Art. 2.1 RLPDP)
Responsable del tratamiento **(SIMILITUD) Aunque la definición del RGPD es más completa y tutelar a favor del ciudadano**	la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros	Es aquél que decide sobre el tratamiento de datos personales, aun cuando no se encuentren en un banco de datos personales. (Art. 2.14 RLPDP)
Encargado del tratamiento **(SIMILITUD)**	la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento	Entrega por parte del titular del banco de datos personales a un encargado de tratamiento de datos personales en virtud de una relación jurídica que los vincula. Dicha relación jurídica delimita el ámbito de actuación del encargado de tratamiento de los datos personales (Art. 2.8. LPDP)
Destinatario **(SIMILITUD)**	la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no	Toda persona natural, persona jurídica de derecho privado o entidad pública que sola o actuando conjuntamente con otra realiza el tratamiento de los datos

	de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento	personales por encargo del titular del banco de datos personales en virtud de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación. Incluye a quien realice el tratamiento sin la existencia de un banco de datos personales. (Art. 2.7 LPDP)
Tercero **(SIMILITUD)**	persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado	Es toda persona natural, persona jurídica de derecho privado o entidad pública, distinta del titular de datos personales, del titular o encargado del banco de datos personales y del responsable del tratamiento, incluyendo a quienes tratan los datos bajo autoridad directa de aquellos. (Art. 2.15 RLPDP).
Consentimiento del interesado **(SIMILITUD)**	toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen	el tratamiento de los datos personales es lícito cuando el titular del dato personal hubiere prestado su consentimiento libre, previo, expreso, informado e inequívoco. No se admiten fórmulas de consentimiento en las que éste no sea expresado de forma directa, como aquellas en las que se requiere presumir, o asumir la existencia de una voluntad que no ha sido expresa. Incluso el consentimiento prestado con otras

		declaraciones, deberá manifestarse en forma expresa y clara (Art. 7 LPDP)
Violación de la seguridad de los datos personales **(SILIMITUD)**	toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos	En atención al principio de seguridad, en el tratamiento de los datos personales deben adoptarse las medidas de seguridad que resulten necesarias a fin de evitar cualquier tratamiento contrario a la Ley o al presente reglamento, incluyéndose en ellos a la adulteración, la pérdida, las desviaciones de información, intencionales o no, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado (Art. 10 RLPDP) Cuando se trate de personal ajeno, el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto a los datos que el personal hubiera podido conocer con motivo de la prestación del servicio (Art. 46. Párrafo 2 RLPDP)
Datos genéticos **(SIMILITUD) Aunque la definición del RGPD es más completa**	datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona	Datos personales relacionados con la salud: Es aquella información concerniente a la salud pasada, presente o pronosticada, física o mental, de una persona, incluyendo el grado de discapacidad y su información genética. (Art. 2.5 RLPDP)
Datos biométricos **(SIMILITUD)**	datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas,	Datos personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos

	fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos	económicos; opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual. (Art. 2.5 LPDP)
Datos relativos a la salud **(SIMILITUD) Aunque la ley peruana incluye la información genética dentro de este acápite**	datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud	Es aquella información concerniente a la salud pasada, presente o pronosticada, física o mental, de una persona, incluyendo el grado de discapacidad y su información genética. (Art. 2.5 RLPDP)
Establecimiento principal **(DIFERENCIAS)**	a)en lo que se refiere a un responsable del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión, salvo que las decisiones sobre los fines y los medios del tratamiento se tomen en otro establecimiento del responsable en la Unión y este último establecimiento tenga el poder de hacer aplicar tales decisiones, en cuyo caso el establecimiento que haya adoptado tales decisiones se considerará establecimiento principal; b)en lo que se refiere a un encargado del tratamiento con establecimientos en más de un Estado miembro,	Sea efectuado en un establecimiento ubicado en territorio peruano correspondiente al titular del banco de datos personales o de quien resulte responsable del tratamiento (Art. 5.1. RLPDP) Sea efectuado por un encargado del tratamiento, con independencia de su ubicación, a nombre de un titular de banco de datos personales establecido en territorio peruano o de quien sea el responsable del tratamiento (Art. 5.2. RLPDP) En el caso de personas naturales, el establecimiento se entenderá como el local en donde se encuentre el principal asiento de sus negocios, o el que utilicen para el desempeño de sus actividades o su domicilio. (Art. 5.4. párrafo cuarto RLPDP) Tratándose de personas jurídicas, se entenderá como el establecimiento el local en el que se encuentre la administración principal del negocio. Si se trata de personas jurídicas residentes en el

	el lugar de su administración central en la Unión o, si careciera de esta, el establecimiento del encargado en la Unión en el que se realicen las principales actividades de tratamiento en el contexto de las actividades de un establecimiento del encargado en la medida en que el encargado esté sujeto a obligaciones específicas con arreglo al presente Reglamento;	extranjero, se entenderá que es el local en el que se encuentre la administración principal del negocio en territorio peruano, o en su defecto el que designen, o cualquier instalación estable que permita el ejercicio efectivo o real de una actividad. (Art. 5.4. párrafo quinto RLPDP) Si no fuera posible establecer la dirección del domicilio o del establecimiento, se le considerará con domicilio desconocido en territorio peruano (Art. 5.4. párrafo sexto RLPDP)
Representante **(SIMILITUD)**	persona física o jurídica establecida en la Unión que, habiendo sido designada por escrito por el responsable o el encargado del tratamiento, represente al responsable o al encargado en lo que respecta a sus respectivas obligaciones en virtud del presente Reglamento	Para estos efectos, el responsable deberá proveer los medios que resulten necesarios para el efectivo cumplimiento de las obligaciones que imponen la Ley y el presente reglamento y designará un representante o implementar los mecanismos suficientes para estar en posibilidades de cumplir de manera efectiva, en territorio peruano, con las obligaciones que impone la legislación peruana (Art. 5 RLPDP)
Empresa **(DIFERENCIAS)**	persona física o jurídica dedicada a una actividad económica, independientemente de su forma jurídica, incluidas las sociedades o asociaciones que desempeñen regularmente una actividad económica	En el caso de grupos económicos conformados por empresas que son consideradas sujetos obligados a informar (Art. 14.11 LPDP)
Grupo empresarial **(DIFERENCIAS)**	grupo constituido por una empresa que ejerce el	En el caso de transferencias de datos personales dentro de grupos

	control y sus empresas controladas	empresariales, sociedades subsidiarias afiliadas o vinculadas bajo el control común del mismo grupo del titular del banco de datos personales o responsable del tratamiento, o a aquellas afiliadas o vinculadas a una sociedad matriz o a cualquier sociedad del mismo grupo del titular del banco de datos o responsable del tratamiento, se cumple con garantizar el tratamiento de datos personales, si se cuenta con un código de conducta que establezca las normas internas de protección de datos personales (Art. 21 RLPDP)
Normas corporativas vinculantes **(DIFERENCIAS) Entendiendo que la normativa peruana no lo conceptualiza de manera positiva (es decir, en Ley)**	las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta	**No lo señala taxativamente ni la Ley de Protección de Datos Personales, ni su Reglamento.**
autoridad de control **(SIMILITUD) Ambas tienen competencia para el desarrollo de sus funciones tutelares**	la autoridad pública independiente establecida por un Estado miembro con arreglo a lo dispuesto en el artículo 51	Es el órgano encargado de ejercer la Autoridad Nacional de Protección de Datos Personales a que se refiere el artículo 32 de la Ley, pudiendo usarse indistintamente cualquiera de dichas denominaciones (Art. 2.8. RLPDP)
Autoridad de control interesada	la autoridad de control a la que afecta el tratamiento	La Autoridad Nacional de Protección de Datos Personales

(DIFERENCIAS) No existe en la normativa peruana una clasificación como sí lo tiene el RGPD	de datos personales debido a que: a)el responsable o el encargado del tratamiento está establecido en el territorio del Estado miembro de esa autoridad de control; b)los interesados que residen en el Estado miembro de esa autoridad de control se ven sustancialmente afectados o es probable que se vean sustancialmente afectados por el tratamiento, o c)se ha presentado una reclamación ante esa autoridad de control;	ejerce las funciones administrativas, orientadoras, normativas, resolutivas, fiscalizadoras y sancionadoras (Art. 33 RLPDP)
Tratamiento transfronterizo **(DIFERENCIAS) No existe en la normativa peruana una clasificación como sí lo tiene el RGPD**	a)el tratamiento de datos personales realizado en el contexto de las actividades de establecimientos en más de un Estado miembro de un responsable o un encargado del tratamiento en la Unión, si el responsable o el encargado está establecido en más de un Estado miembro, o b)el tratamiento de datos personales realizado en el contexto de las actividades de un único establecimiento de un responsable o un encargado del tratamiento en la Unión,	Transferencia internacional de datos personales a un destinatario situado en un país distinto al país de origen de los datos personales, sin importar el soporte en que estos se encuentren, los medios por los cuales se efectuó la transferencia ni el tratamiento que reciban. (Art. 2.10 LPDP)

	pero que afecta sustancialmente o es probable que afecte sustancialmente a interesados en más de un Estado miembro;	
Objeción pertinente y motivada **(DIFERENCIAS) Entendiendo que la normativa peruana no lo conceptualiza de manera positiva (es decir, en Ley)**	la objeción a una propuesta de decisión sobre la existencia o no de infracción del presente Reglamento, o sobre la conformidad con el presente Reglamento de acciones previstas en relación con el responsable o el encargado del tratamiento, que demuestre claramente la importancia de los riesgos que entraña el proyecto de decisión para los derechos y libertades fundamentales de los interesados y, en su caso, para la libre circulación de datos personales dentro de la Unión	**No lo señala taxativamente ni la Ley de Protección de Datos Personales, ni su Reglamento.**
Servicio de la sociedad de la información **(DIFERENCIAS) Entendiendo que la normativa peruana no lo conceptualiza de manera positiva (es decir, en Ley)**	todo servicio conforme a la definición del artículo 1, apartado 1, letra b), de la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo	**No lo señala taxativamente ni la Ley de Protección de Datos Personales, ni su Reglamento.**
Organización internacional **(DIFERENCIAS) Entendiendo que la normativa**	una organización internacional y sus entes subordinados de Derecho internacional público o cualquier otro organismo	**No lo señala taxativamente ni la Ley de Protección de Datos Personales, ni su Reglamento.**

peruana no lo conceptualiza de manera positiva (es decir, en Ley)	creado mediante un acuerdo entre dos o más países o en virtud de tal acuerdo	

enaTIC
ABOGACIA DIGITAL

Asociación Expertos Nacionales Abogacía TIC
Paseo de Recoletos 13
28004 - MADRID