Universidad Internacional de La Rioja

Facultad de Derecho

Máster Universitario en Derecho Digital

El Tratamiento de Datos Personales en el *Score* TELCO: Análisis comparativo entre Ecuador y España

Trabajo fin de estudio presentado por:	Krizia Valeria Valero Zambrano
Tipo de trabajo:	Trabajo de Fin de Máster
Director/a:	Enrique Ortega Burgos
Fecha:	07 de diciembre de 2023

Resumen

El *Score* TELCO es una alternativa al *scoring* crediticio tradicional. Desde la arista comercial, existe una oportunidad de negocio para el Operador, empleando la analítica, *machine learning* e inteligencia artificial para el tratamiento de *big data* generada por los clientes, siendo posible procesar la información para predecir su voluntad y capacidad de pago. Por el lado social, los clientes del Operador que correspondan al sector no bancarizado contarían con una herramienta que les permite adquirir bienes y servicios a los que no tendrían acceso por no contar con un historial crediticio.

Este fenómeno implementado en España ha manifestado el deseo de ser replicado en Ecuador, teniendo legislación incipiente en la materia; de manera que, para determinar el correcto tratamiento de los datos personales de los abonados, se realiza un análisis comparativo de ambas normativas para determinar aquellas figuras reproducibles para garantizar un efectivo estándar de protección.

Palabras clave: *Score*, telecomunicaciones, datos, personales, crediticios.

Abstract

The TELCO Score is an alternative to traditional credit scoring. From the commercial side, there is a business opportunity for the Operator, using analytics, machine learning and artificial intelligence to process big data generated by customers, making it possible to process the information to predict their willingness and ability to pay. On the social side, the Operator's clients who correspond to the unbanked sector would have a tool that allows them to acquire goods and services to which they would not have access due to not having a credit history.

This phenomenon implemented in Spain has expressed the desire to be replicated in Ecuador, with incipient legislation on the matter; so, to determine the correct treatment of subscribers' personal data, a comparative analysis of both regulations is carried out to determine those reproducible figures to guarantee an effective standard of protection.

***Keywords**: Score, telecommunications, data, personal, credit.*

Índice de contenidos

Índice de figuras

1. Introducción

Hoy en día, existe un auge en la oferta comercial de productos corporativos que emplean inteligencia artificial para el tratamiento de *big data*; ello se debe a la necesidad que tienen las empresas de tomar decisiones más perspicaces, comprender mejor a los clientes y aprovechar oportunidades de crecimiento y eficiencia que les otorguen una ventaja competitiva. Uno de estos productos presente en el ámbito de las telecomunicaciones es el *Score* TELCO, concebido como una plataforma de entrega de calificaciones crediticias alternativas, producto del análisis de macrodatos originados de la prestación del servicio por parte de las Operadoras a sus abonados.

El uso de esta herramienta innovadora trae consigo la posible afectación de derechos y libertades fundamentales del Usuario TELCO, considerando que sus datos personales atraviesan varias fases de tratamiento hasta el momento de la consulta por el destinatario del *scoring*; situación que deviene en la necesidad de generar el ambiente propicio para el desarrollo de soluciones comerciales capaces de generar resultados rentables, éticos y legalmente viables, al cumplir con el derecho a la protección de datos personales que asiste al titular.

La característica principal del *Score* TELCO que genera profunda preocupación en el espectro del Derecho Digital, reside en determinar cómo se debe efectuar un correcto tratamiento de los datos personales por parte del Operador en su calidad de responsable; ya que se verá beneficiado económicamente al incorporar dicha solución a su portafolio y será quien tome las decisiones más importantes del ciclo de vida de los macrodatos tratados.

Este producto se ha hecho presente mayormente en sectores de África y Asia, en los cuales se ha requerido un desarrollo acelerado de mecanismos que permitan la progresiva inclusión financiera de la población, particular que es posible al construirse un historial de tipo crediticio con el *scoring* de telefonía. Tal situación se extendió hasta Europa con la visión de ampliar las oportunidades de crédito a los abonados que no contaren con suficientes antecedentes bancarios o que carezcan de estos; tal es el caso de España.

Por ello, existiendo la necesidad en Ecuador de implementar este tipo de soluciones corporativas por los operadores y, considerando la reciente normativa de protección de datos personales, resulta menester el estudio del tratamiento de datos personales en el *Score* TELCO

desde la óptica del Operador a través de una comparación de la legislación española con la ecuatoriana; habiéndose escogido estos países por las similitudes en el modelo de Estado, sistema jurídico y la histórica impronta del desarrollo jurídico de España sobre el ordenamiento jurídico del Ecuador.

Con este trabajo se busca profundizar en la figura del *Score* TELCO para conocer detalladamente sus componentes y fases para estudiar el alcance de las obligaciones en materia de protección de datos personales que revisten a toda la solución; para ello, se revisará la normativa española y europea que resulte aplicable y se extrapolará al caso ecuatoriano, pudiendo así detectar similitudes, diferencias y determinar la factibilidad de replicar en Ecuador aquellos aspectos que ya hayan sido solventados en España.

Para cumplir este propósito, se hará un recorrido de tres fases que vislumbrarán la óptica española y ecuatoriana de este tipo de *scoring*. Se abordará la definición del producto, su historia y el marco normativo, lo cual ofrecerá el contexto suficiente para avanzar al estudio del flujo de tratamiento de los datos personales; para ello, se identificará el tipo de datos a ser tratados y los macro tratamientos a los que estarán expuestos los datos personales del Usuario TELCO. Finalmente, se ahondará en las obligaciones del Operador TELCO, determinando la causal más apropiada de legitimación del tratamiento de acuerdo con el giro del negocio, las consideraciones regulatorias que debe cumplir y las particularidades que surgen en la tutela de los derechos del titular.

Diversos autores han abordado previamente temas relacionados con los ficheros tradicionales de crédito y en el tratamiento de datos personales de forma general o en el espectro de la analítica; sin embargo, no se cuenta con un referente que converja dichos conocimientos y los aplique de forma concreta en este producto, por lo que en las siguientes páginas, este trabajo presentará una guía de fácil entendimiento, tanto para el Operador de telecomunicaciones que desee implementar nuevas soluciones en el mercado ecuatoriano, como para el titular que requiere conocer el alcance de sus derechos y que desea ser capaz de determinar si sus datos cuenta con el grado de protección que ameritan.

1.1. Justificación del tema elegido

Como indicado, el *Score* TELCO es una figura que está tomando auge en países de bajo desarrollo económico e inclusión financiera de su población. En estos países, los clientes se destacan por ser, en su mayoría, del segmento prepago y no formar parte del segmento bancarizado. Ante esta realidad, el *Score* TELCO les permite acceder a bienes y servicios al proporcionar una calificación que genere confianza en el posible acreedor.

En este proceso entran en conflicto el interés económico de las operadoras telefónicas y el beneficio social que se deriva de un score basado en datos de telecomunicaciones. Asimismo, considerando que la normativa en protección de datos es reciente y en muchos países donde se aplica el *Score* TELCO, apenas existente, no es clara la forma en que se deben tratar los datos personales para que el negocio sea viable y, a la vez, el cliente se encuentre protegido.

En consecuencia, este trabajo busca desarrollar el correcto tratamiento de los datos personales en la elaboración y venta de un *Score* TELCO para que sea un producto seguro, con bajo nivel de contingencia ante posibles sanciones regulatorias, no obstantes los riesgos inherentes a dicho modelo de negocios en materia de protección de datos personales.

1.2. Problema y finalidad del trabajo

En el contexto antedicho, el desarrollo de modelos de negocio basados en la transferencia de datos personales procesados conlleva la implementación de medidas que garanticen la protección de los derechos de los propietarios de dichos datos. Tal es el caso del *Score* TELCO, en el cual se ha normalizado la recolección de datos a título gratuito y su posterior transferencia a título oneroso.

Este particular se suma a que en dicho modelo de negocio intervienen hasta cuatro partes en la cadena de tratamiento de datos. Adicionalmente, existen dificultades propias a las jurisdicciones españolas, diferencias de desarrollo normativo de 30 años entre ambos países y, en el caso de Ecuador, la ausencia, a octubre 2023, de Asamblea Nacional y a enero de 2024, de una Superintendencia de Protección de Datos en funciones, a pesar de la existencia de una Ley de Protección de Datos Personales expedida en 2021 y de su Reglamento, en 2023. Cabe

señalar que la Asamblea en mención asumió funciones a fines de noviembre de 2023, sin haberse pronunciado en materia de datos personales hasta la fecha de cierre de este trabajo.

En consecuencia, este trabajo está dirigido al análisis del tratamiento de datos en el *Score* TELCO en Ecuador y en España, con corte a diciembre de 2023, para discernir la causal óptima de legitimación del tratamiento de datos del cliente e identificar las soluciones desarrolladas en el ordenamiento jurídico español que podrían ser replicables en el Ecuador, sin que ello implique una afectación a las necesidades comerciales de las operadoras de telecomunicaciones. Dicha dirección se concretiza en los objetivos que se detallan, por consiguiente.

1.3. Objetivos

Objetivo General:

Identificar las soluciones desarrolladas en el ordenamiento jurídico español, y aplicables en el ordenamiento jurídico ecuatoriano, que otorguen al Operador TELCO una causal óptima de legitimación y un correcto tratamiento de datos personales de los usuarios en el producto *Score* TELCO.

Objetivos específicos:

1. Analizar la figura del *Score* TELCO desde la perspectiva de la aplicación de tecnologías al procesamiento de *big data*, ahondando en la historia del producto y su perfil normativo comparado entre Ecuador y España, determinando la causal de legitimación aplicable;
2. Identificar la tipología de los datos recolectados y las particularidades del flujo del tratamiento en la elaboración de un *Score* TELCO, a través de cinco macro-procesos: recolección, almacenamiento, procesamiento, consulta y eliminación;
3. Determinar el alcance de las obligaciones que posee el Operador TELCO en el modelo de *Score* TELCO, desde las consideraciones regulatorias hasta la tutela de los derechos ARCO, señalando las figuras jurídicas españolas replicables en territorio ecuatoriano.

2. Marco teórico y desarrollo

Como indicado anteriormente, el objetivo del presente trabajo es identificar las soluciones españolas, aplicables en Ecuador, al problema del uso legítimo por el Operador de los datos personales de sus clientes en el producto *Score* TELCO. A este fin, se empezará estableciendo el contexto en el que surge dicho problema (2.1.), para luego detallar los datos tratados y sus procesos de tratamiento de datos en el producto *Score* TELCO, en contraste con la normativa aplicable (2.2.). De este contraste se destilarán las obligaciones que se imponen al Operador y las soluciones aportadas por el ordenamiento jurídico español, desde una perspectiva comparatista (2.3).

2.1. El *Score* TELCO

El primer paso hacia evaluar las soluciones aportadas al problema planteado es entender el contexto en el que surge dicho problema. En el marco de este trabajo, este contexto consiste en el auge de la implementación del producto *Score* TELCO. Se empezará por precisar la noción de *Score* TELCO (2.1.1.) y evocar su evolución histórica en varios casos de estudio (2.1.2.), para luego describir el marco normativo que se ha desarrollado a su alrededor (2.1.3.) y determinar la base legitimadora (2.1.4.).

2.1.1. ¿Qué es el *Score* TELCO?

El concepto central en este trabajo es sin duda el *Score* TELCO, por lo que conviene definirlo y detallar el proceso y sus intervinientes, con sus respectivos roles.

2.1.1.1. Definición

El *Score* TELCO es una herramienta que proporciona evaluaciones crediticias, ofreciendo soluciones de inteligencia financiera para obtener una calificación crediticia alternativa. Se basa en el análisis de grandes volúmenes de datos de telecomunicaciones para estimar la disposición y capacidad de un individuo para cumplir con servicios crediticios, como préstamos. (KT GLOBAL BUSINESS GROUP 2019).

Este sistema alternativo de calificación crediticia sirve para que las empresas que comercializan bienes o prestan servicios con financiamiento directo, puedan tener una base

de información acerca del comportamiento crediticio del posible cliente no bancarizado o para reforzar la información proporcionada por un *score* crediticio tradicional.

También es un sistema empleado por entidades del sector financiero, auxiliares o afines, cuyo giro del negocio está principalmente centrado en el crédito y que requieren de fuentes de información confiables para analizar el perfil del posible cliente, reduciendo la posibilidad de un crédito impago.

En el modelo de negocio del *Score* TELCO, existen los siguientes intervinientes: a) El usuario del servicio de telecomunicaciones; b) La Operadora de telecomunicaciones; c) El *Bureau* Crediticio (según la legislación donde se entregue el servicio); y, d) La institución o negocio que brinda el crédito o financiamiento directo (KT GLOBAL BUSINESS GROUP 2019).

El flujo del proceso se puede describir de la siguiente forma:

- El posible cliente se acerca a la institución de, o relacionada con, el sistema financiero, o a un negocio que ofrece productos y/o servicios con crédito o financiamiento directos.
- La institución o negocio le pide el *Score* TELCO a un *Bureau* Crediticio o a la Operadora de Telecomunicaciones.
- En el supuesto de haber un *Bureau* Crediticio como intermediario, este le pide a la Operadora el *Score* TELCO.
- La Operadora le remite la información al *Bureau* Crediticio a la institución o negocio que haya solicitado el *score* (generalmente un *retail*).
- La institución o negocio recibe el *Score* TELCO del posible cliente y analiza si es sujeto de crédito o financiamiento directo.

2.1.1.2. Partes intervinientes

Para mayor comprensión, se procederá a desglosar el rol de cada interviniente:

<u>El Usuario TELCO</u>

De acuerdo con el derecho español, precisamente en el Anexo II, numeral 83 Ley 11/2022, el usuario final (a efectos de este trabajo, “Usuario TELCO”), es aquel que no provee redes de comunicaciones electrónicas públicas, servicios de comunicaciones electrónicas abiertos al público o no los vende; definición compartida en su esencia por la legislación ecuatoriana.

Dicho usuario, que generalmente consiste en una persona natural, consume servicios de telecomunicaciones que pueden ser, a manera de ejemplo, servicios móviles como llamadas, mensajes, internet, *roaming*; o, servicios fijos, como, según sus siglas en inglés, *IPTV* (televisión por protocolo de internet), *WTTX* (*wireless* para el hogar), *OTT* (servicio de transmisión libre), *HFC* (internet por fibra híbrida), *GPON* (internet por fibra óptica), entre otros. El Usuario TELCO ocupa el rol de titular de los datos.

El Operador TELCO

En el numeral 45 *eiusdem* se hace referencia a una persona o entidad legal que proporciona redes públicas de comunicaciones electrónicas o presta servicios de comunicaciones electrónicas accesibles al público, y ha notificado el inicio de sus actividades al Registro de Operadores o se encuentra registrado en él. Dicho Operador TELCO recibirá constantemente información generada por el Usuario TELCO mediante el uso permanente de los servicios móviles y/o fijos que tenga contratados como, por ejemplo, el uso de datos o la conducta de pago de los servicios.

Para que el Operador pueda generar un *Score* TELCO, deberá contar con los siguientes elementos a) Análisis de inteligencia financiera de *big data* de telecomunicaciones, para derivar los mejores datos candidatos para el modelado de calificación crediticia; b) Tecnologías de modelado de puntaje crediticio y modelos que estiman la posibilidad de riesgo de incumplimiento; y, c) Plataforma de aplicaciones que implementan análisis de *big data*, modelado de puntaje crediticio y entrega de información crediticia (KT GLOBAL BUSINESS GROUP 2019).

El *Bureau* Crediticio

En países como Corea (KT GLOBAL BUSINESS GROUP 2019), el *Score* TELCO solo puede ser entregado al cliente final por un *Bureau* Crediticio, definido por el Banco de España como una entidad que se dedica a gestionar una base de datos que centraliza casi la totalidad de la información relativa a préstamos, créditos, avales y riesgos que las instituciones financieras mantienen con sus clientes. Dicha base refleja los datos que las entidades financieras almacenan en sus propias bases acerca de sus clientes (BANCO DE ESPAÑA sin fecha).

La Institución o Empresa (*Retail*)

Es la institución financiera, auxiliar del sistema financiero, relacionada con el sistema financiero, *retail* o negocio en general, al que acude el Usuario TELCO con la finalidad de adquirir un bien o servicio a plazo. A efectos de evaluar la capacidad y voluntad de pago del posible cliente, consulta su información crediticia financiera y/o alternativa (*Score* TELCO), para lo cual requiere efectuar un tratamiento de datos personales.

2.1.2. Historia

Históricamente, el mercado relevante para el desarrollo del *Score* TELCO residió en África y Asia, destacados por tener un alto porcentaje de población sin acceso a instituciones financieras, lo que llevó al surgimiento de soluciones como el dinero electrónico, la billetera móvil y un flujo constante de recargas de servicios prepago de telefonía. Estos datos, que se encuentran bajo el control de las compañías de telecomunicaciones, ofrecen una visión completa de los movimientos financieros de un usuario de tarjeta *SIM*. (SAFARICOM 2023).

Un caso de éxito en *Score* TELCO es la empresa Tiaxa, que desde 2010 ofrece nano créditos a Usuarios TELCO bajo el esquema de un producto crediticio de uso extendido, se dirige a usuarios de telefonía móvil con planes prepago que se quedan sin minutos para realizar llamadas, y en estos casos, reciben una asignación inmediata de minutos adicionales. Normalmente, estos adelantos consisten en cantidades reducidas. Tiaxa proporciona 50 millones de estos pequeños adelantos de minutos de comunicación cada mes a varios operadores de telefonía móvil (CHEN, FAZ 2015).

Otro caso notable se encuentra en África, específicamente en Kenia, materializado en el producto denominado M-PESA: M-SHWARI (SAFARICOM sin fecha), lanzado en 2012 por la operadora Safaricom. Este producto se presenta como una colaboración entre Safaricom, un operador de telefonía móvil, y el Banco Comercial de África. Se evalúa el uso de los dispositivos móviles de aquellos que buscan acceder a un préstamo, lo que permite establecer un límite de crédito inicial (CHEN, FAZ 2015).

Se puede observar que, con el paso de los años, el *Score* TELCO se ha desarrollado hasta constituir un sistema crediticio alternativo al sistema financiero, que le permite al Usuario TELCO desarrollar un historial lo suficientemente sólido para, en lo posterior, poder convertirse en cliente del sistema financiero y de sus servicios auxiliares. En este orden, el

Usuario TELCO será sujeto de un *Score* TELCO y con base al resultado de dicho análisis, podría solicitar un nano crédito.

Claro ejemplo de este sistema es Timiza, un servicio de crédito a corto plazo implementado en Tanzania en asociación con Airtel, el cual se vale de datos digitales para evaluar posibles oportunidades. A través de la información recopilada por el operador de telefonía móvil, se identifican posibles clientes a quienes se les ofrecen préstamos de pequeñas sumas. El comportamiento de pago y las solicitudes subsiguientes de préstamos se utilizan como una base a largo plazo para ajustar el límite de crédito, los costos y la duración del servicio crediticio a lo largo del tiempo (CHEN, FAZ 2015).

Actualmente se puede constatar que, en 2023, el producto *Score* TELCO sigue siendo subutilizado. Si bien los países que lo implementaron más de diez años atrás se encuentran en una fase de banca móvil, fuera de Asia y África el *Score* TELCO no se encuentra mayormente disponible como parte de la oferta comercial corporativa de las Operadoras TELCO por desconocimiento del alcance en materia regulatoria y de protección de datos personales; sin perjuicio de lo cual se verá el caso del Grupo Telefónica en España, el cual se ha deseado replicar en Ecuador por operadores locales, como es el caso de CONECEL.

2.1.3. Marco normativo

El concepto de Score Telco definido, y su evolución histórica presentada por ejemplos de casos de éxito, se procederá a continuación a desarrollar los principales parámetros normativos que rigen al tratamiento de datos personales en el producto *Score* TELCO. Para ello, se analizarán las semejanzas y diferencias entre Ecuador y España con respecto al modelo de estado, sistema jurídico y figuras esenciales presentes en este *scoring*.

2.1.3.1. Ordenamiento jurídico español

Se tomará como premisa el siguiente marco normativo aplicable: la Ley 3/2018, el Reglamento (UE) 279/2016, el RDL 1720/2007, el RDL 1/2007, la Ley 11/2022, las resoluciones de la AEPDP y del Comité Europeo de Protección de Datos, la jurisprudencia y la doctrina.

El marco normativo nacional del *Score* TELCO es muy interesante, porque se presta a una labor interpretativa para determinar qué normas rigen a esta figura. La primera impresión sería que su ordenamiento jurídico aplicable es el de una calificación crediticia que debería ser emitida

por una agencia de calificación debidamente registrada; sin embargo, ¿la naturaleza del *Score* TELCO se adecua a este supuesto?

El Reglamento 1060/2009, sobre las agencias de calificación crediticia, en su artículo 3, numeral 1, literal a), hace referencia a la evaluación crediticia como un juicio sobre la capacidad financiera de una entidad, deuda u obligación financiera, o cualquier otro instrumento financiero. Se emite mediante un sistema establecido y definido de categorías de clasificación.

Como se abordará en el próximo capítulo, el Operador TELCO desarrolla esta herramienta tratando datos personales y no personales generados por el Usuario TELCO durante el uso de los servicios de telecomunicaciones. El público objetivo del *Score* TELCO es, trascendentalmente, el segmento masivo prepago, el cual, para acceder a los servicios que presta la Operadora TELCO, realiza la compra de un paquete de servicios o de una recarga y hace uso de estos hasta que se agote su cupo, pagan mayormente en efectivo y no suelen contar con tarjetas de crédito o débito; por lo tanto, el tratamiento no implica mayormente a las obligaciones financieras.

La misma norma, en su literal b) define a las agencias de calificación crediticia como una persona jurídica cuya actividad principal es emitir evaluaciones crediticias de manera profesional.

En el *Score* TELCO, la Operadora ha desarrollado una plataforma con algoritmos que realizan minería de *big data*, pero sigue siendo una Operadora TELCO. Los datos que está procesando se van generando segundo a segundo por el Usuario TELCO y el resultado que se pueda obtener de este *scoring* no es netamente financiero, por lo que no se hablaría de una calificación crediticia profesional, pero sí se trata de un tratamiento regulado.

La Ley 11/2022, aborda, en su artículo 60, numeral 1, la protección de datos de carácter personal, estableciendo que el Operador tiene la responsabilidad de asegurar que solo el personal autorizado acceda a los datos personales para propósitos permitidos por la ley, protegiendo la información contra tratamientos, accesos o divulgaciones no autorizadas o ilegales, y garantizando la implementación efectiva de una política de seguridad para el tratamiento de datos.

Como usuarios de dispositivos móviles inteligentes, a más de datos de tráfico de internet, se cuenta con datos de localización. Es un hecho que la Operadora TELCO tiene conocimiento de la ubicación del abonado de acuerdo con la radiobase a la que se va conectando mientras se desplaza. La norma antedicha, en su artículo 66, numeral 2, literal c), se pronuncia al respecto, manifestando que la gestión de datos de localización, excluyendo los datos de tráfico, solo se llevará a cabo una vez que hayan sido anonimizados o con el consentimiento del usuario, y únicamente en la medida y durante el tiempo necesario para proporcionar, si procede, servicios de valor agregado. Ejemplos de servicios de valor añadido son los mensajes multimedia, el buzón de voz, música, juegos, *gps, tv* móvil, redes sociales, etc. (PIEDRAS 2011)

Establecido esto, se procederá a analizar qué tipo de servicio es el *Score* TELCO. Se sabe que el *scoring* se obtiene producto de una consulta (acción) y, como consecuencia, se obtiene la respuesta. Si no se hace la consulta, esa información no se va a generar y para poder consultar, la Institución o Negocio deberá ingresar a una plataforma, sea una aplicación o página web.

El RDL 1/2007, define los servicios digitales en su artículo 59 bis, literal o), como aquellos que habilitan a los consumidores o usuarios para generar, procesar, guardar o consultar información en formato digital. Esta premisa permite ubicar al *Score* TELCO como un servicio digital y cubierto por la ley que regula la protección a los consumidores, según quién efectúe la consulta.

El ordenamiento jurídico ofrece varias causales de tratamiento legítimo de datos, empezando por el consentimiento. La LO 3/2018, indica en su artículo 6 la legitimación del Tratamiento basado en el consentimiento del afectado; y, en su artículo 8, establece el tratamiento por obligación legal, interés público o ejercicio de poderes públicos.

Lógicamente el *Score* TELCO no consiste en una potestad o un servicio públicos cuya prestación le es delegada a un Operador TELCO; sin embargo, es un servicio de interés público, por lo que el artículo 20 *ibidem*, numeral 1, establece que el tratamiento de datos personales relacionados con el impago de obligaciones financieras, de crédito o de pago a través de sistemas de información crediticia se presume como legítimo. Sin embargo, esta presunción no se extiende a situaciones en las que la entidad a cargo del sistema asocie la información crediticia con datos adicionales u obtenidos de otras fuentes.

En el Reglamento (UE) 2016/679, artículo 6, numeral 1, literal f), se habla del interés legítimo como causal de tratamiento. Tal artículo debe interpretarse en concordancia con el artículo 10, numeral 2, del RDL 1720/2007, que incluye al interés legítimo como justificación del tratamiento o cesión de datos sin la obtención del consentimiento.

En consecuencia, se puede ver que el consentimiento es la fuente tradicional para legitimar el tratamiento de datos personales, mas no la única. El *Score* TELCO puede alimentarse de datos legítimamente tratados por diferentes causales, de acuerdo con la fase que corresponda al flujo de tratamiento y a las partes intervinientes en el modelo de negocio desde cuya óptica se analice.

2.1.3.2. Comparación con Ecuador

Ahora se procederá a establecer semejanzas y diferencias generales, aplicables al tratamiento de datos en el *Score* TELCO entre la normativa española y la normativa ecuatoriana, de acuerdo con los siguientes ejes, que permitirán conocer si dicho producto admite analogías en la aplicación de su marco regulador: modelo de estado, sistema jurídico, tratamiento de datos crediticios, transferencia o cesión de datos y autoridad en la materia.

<u>Modelo de Estado y sistema jurídico</u>

A efectos de comparar la legislación española con la ecuatoriana, se parte desde la concepción del modelo de Estado y su sistema jurídico. Con respecto a España, la doctrinaria María José Roig (2002), indica que la Constitución de 1978 estableció un modelo de organización distinto en el ámbito legal y político, que posteriormente se ha identificado como el Estado constitucional de Derecho; particular que se complementa con el pronunciamiento del Reino de España (sin fecha), el cual dicta que dentro de los sistemas jurídicos actuales, el sistema español se adscribe al modelo continental, caracterizado por la preeminencia de la legislación y el derecho escrito; de igual modo, las fuentes del sistema legal español, tal como se establecen en el Código Civil, comprenderían la ley, la costumbre y los principios generales del derecho; además, la jurisprudencia desempeñaría un papel complementario en el ordenamiento legal junto con la doctrina.

En Ecuador, de acuerdo con la Constitución de la República del Ecuador del 2008, en su artículo 1, se trata de un Estado constitucional de derechos y justicia; y, sobre su sistema jurídico, el tratadista Ocampo (2017), explica que el sistema legal ecuatoriano tiene raíces históricas que

se remontan al Derecho Romano, el cual influyó a través del Derecho español. En este sistema legal, la ley ocupa una posición preeminente como fuente principal del derecho, siguiendo una tradición de origen latino-romano.

Notando que coinciden en modelo y sistema, se precisa que, en materia de protección de datos, luego de la norma constitucional, se tiene puntualmente, la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional (LOGJCC /2009), la Ley Orgánica de Protección de Datos Personales (LOPDP /2021), la Ley Orgánica de Telecomunicaciones (LOT /2015), la Ley Orgánica de Defensa al Consumidor (LODC /2000), el Reglamento General a la Ley Orgánica de Protección de Datos Personales (RGLOPDP /2023), la jurisprudencia y la doctrina.

Tratamiento de datos crediticios

En la Ley 3/2018, artículo 20, numeral 3, de España, establece una presunción de licitud del tratamiento de estos datos, los cuales alimentan la base que será procesada para elaborar el *Score* TELCO; no obstante, la presunción no es absoluta por intervenir diferentes tipologías de datos, lo cual devendrá en obligaciones adicionales como caso del sopesamiento, para demostrar que existe una debida protección a los datos personales. Dicho criterio se replica en Ecuador, específicamente en la LOPDP /2021, artículo 28; incluyendo la obligación de realizar acciones adicionales por parte del Operador TELCO dado el uso de *big data*.

Como particularidad ecuatoriana, producto del RGLOPDP /2023, cualquier puntualización en cuanto al alcance de la protección de los datos crediticios, será adoptada por Junta de Política y Regulación Financiera y por la Superintendencia de Bancos. Se desconoce si abarcarán los ficheros de solvencia no tradicionales.

Transferencia o cesión

En los términos de la LOPDP /2021, artículo 33, se le da a la llamada cesión de datos en España la denominación de transferencia de datos, pudiendo esta ser nacional o internacional. La particularidad de este tratamiento, y el motivo por cual son sinónimos, es que el destinatario de los datos no se encuentra en obligación de destruir o devolver los datos comunicados. Sin perjuicio de ello, existe una diferencia expresa al incorporarse en el art. 82 *ibidem* un pronunciamiento expreso por el cual el uso comercial de datos personales (la cesión para consulta del destinatario) debe estar precedido de la obtención del consentimiento del titular.

En cuanto al encargo, este es denominado acceso, como dictan los artículos 34 y 35 de LOPDP /2021 de Ecuador.

Con respecto a la corresponsabilidad, en Ecuador, esta figura no existía en rango legal; no obstante, fue incorporada mediante el RGLOPDP /2023, artículo 37, incluyendo la novedad de que todos quienes constituyan una corresponsabilidad serán solidariamente responsables ante la Superintendencia de Protección de Datos Personales y ante los titulares en el ejercicio de sus derechos.

En este producto, cada transferencia de datos es puntual, proveniente de una solicitud expresa del destinatario, para lo cual deberá garantizar y declarar que ha obtenido el consentimiento del titular previo a efectuar la consulta. Por el giro del negocio, el Operador TELCO traslada el cumplimiento de esta obligación al destinatario, ya que la consulta se efectúa por una solicitud del titular al destinatario para aplicar a un financiamiento.

Si bien la prospección de una relación contractual es una causal de legitimación, por tratarse de una transferencia de datos en manos de un tercero que ostenta la calidad de prestador de servicio de telecomunicaciones, al tenor del cumplimiento de norma expresa, el Operador TELCO deberá plasmar este requisito dentro del contrato que efectúe con el *retail*, previo a entregarle claves de acceso al software.

Autoridad en Protección de Datos Personales

En España, de acuerdo con la Ley 3/2018 en sus artículos 44, numeral 1 y artículo 48, numeral 3, el ente regulador es la Agencia Española de Protección de Datos, la cual se caracteriza por un órgano administrativo e independiente, cuya máxima autoridad es un presidente, el cual es nombrado a propuesta del Ministerio de Justicia; en cambio, en Ecuador, se trata de una Superintendencia de Protección de Datos y su representante es elegido de entre una terna propuesta por el presidente del país.

En este orden, se puede notar que en Ecuador el ente regulador tendría un esbozo político, pese a no ser parte de la estructura del Estado, y, al compararlo con otras instituciones públicas, se desprende que, al tener el carácter de Superintendencia, no estará vinculada a un Ministerio. En cuanto a las atribuciones, ambas legislaciones coinciden en el marco de actuación, con la diferencia de que, en Ecuador, no se verá una repercusión directa de

normativa comunitaria que pudiere marcar pautas para la Autoridad de Control distintas a las ya previstas en la Ley.

Se observa que el marco normativo analizado brinda claridad para el desarrollo de los siguientes capítulos, en tanto ahora se conoce que el *Score* TELCO no es una calificación crediticia propiamente dicha, que el Operador TELCO no se encuentra obligado a constituirse como agente calificador acreditado, que se trata de un servicio digital y que el tratamiento de los datos puede tener varias causales de legitimación, pudiendo inclusive cederse los datos siempre que se cumplan los presupuestos de Ley.

2.1.4. Legitimación del tratamiento de datos personales

Se observa que la causal de legitimación de tratamiento denominada interés legítimo se presenta en ambas legislaciones. Siendo el presente trabajo un análisis desde la óptica del Operador TELCO, se profundizará en el siguiente apartado que ambas causales de legitimación coinciden en significado, pero difieren en el alcance de las obligaciones que ello representa para el Operador como responsable del tratamiento; y, siendo este el punto de partida para adentrarse en la figura, es menester desarrollarlo en un capítulo.

2.1.4.1. Definición de interés legítimo

En la prestación de servicios de telecomunicaciones el Operador TELCO recolectará y almacenará datos, en muchas ocasiones, de forma involuntaria, por medio de las radiobases o en cumplimiento de obligaciones legales como el empadronamiento de líneas; sin embargo, tal tratamiento se encuentra legitimado solo para determinados fines. Ello no justifica el tratamiento para fines ulteriores. En este orden, el *Score* TELCO necesita su propia causal de legitimación.

Coincidiendo en que, para el Operador TELCO, sí se está hablando del tratamiento de datos personales y que la generación de un servicio de *scoring* amerita su propia finalidad debidamente legitimada, cabe indicar cuál sería aquella que responda a la naturaleza del servicio y al tipo de titular, ante lo cual se desarrollará en este capítulo que el Operador TELCO efectuará el tratamiento justificado en el interés legítimo.

Ordenamiento jurídico español

En España esta causal estará, a más de en la Ley 3/2018, en el RDL 1720/2007, artículo 10, numeral 2 y en el Reglamento (UE) 679/2016, artículo 6, numeral 1, literal f. Por otro lado, se verá que en Ecuador se encuentra en la LOPDP /2021, artículo 7, numeral 8.

¿Qué es el interés legítimo? A nivel normativo español no existe una definición de esta causal de legitimación, por lo que, analizando la definición efectuada en la Dict. GT29, de 9 de abril de 2014, se puede colegir que un interés legítimo debe ser legal, en conformidad con las leyes españolas y de la Unión Europea aplicables; debe expresarse de manera clara para facilitar la prueba de sopesamiento frente a los intereses y derechos fundamentales del titular; y debe consistir en un interés real y presente.

Desde el punto de vista doctrinal, se amplía esta idea al distinguirla del interés simple. Para entenderlo mejor, es útil dividirlo en sus partes: 1) el interés, que se refiere a la utilidad, bienestar, valor y disfrute, y va más allá de un sentido meramente económico o material; y 2) el reconocimiento y protección de este interés por parte del derecho. Esta característica lo diferencia del interés simple, que carece de importancia desde una perspectiva normativa. (CONTRERAS y TRIGO 2019).

Se desprende que, en España, el Operador TELCO, para efectuar un *scoring*, requerirá un interés real y actual, específico, lícito y sopesado frente a los derechos del interesado, lo que fundamentaría su tutela por parte del derecho.

Ordenamiento jurídico ecuatoriano

Ahora bien, ¿el interés legítimo significa lo mismo en Ecuador? De la revisión de las fuentes del derecho ecuatoriano en protección de datos personales no se encuentra una definición del este; inclusive, el término ha sido recientemente acuñado por la LOPDP /2021, cuya promulgación recién data de 2021 con un régimen sancionatorio cuya vigencia teórica comenzó en 2023, pero que no se ha ejercido por cuanto sigue pendiente la creación institucional de la Autoridad de Control.

A falta de definición, la interpretación de la ley de acuerdo con el Código Civil /2005, art. 18, numeral 2, lleva a buscar el sentido natural y obvio, esto es, la definición de la Real Academia de la Lengua Española y el Diccionario Panhispánico; como consecuencia, en Ecuador se habla de la inclinación del ánimo (del responsable del tratamiento) hacia algo (datos personales del

titular) y deseo de conseguirlo con base en una justificación legal (ej., derecho constitucional a la libertad de desarrollar actividades económicas, respetando los lineamientos contenidos en las leyes especiales).

Siendo definiciones con un grado de similitud elevado, los elementos diferenciadores recaerían en la especificidad y el sopesamiento. Sin embargo, se verá en lo posterior que la normativa ecuatoriana en protección de datos necesariamente se va a complementar con la normativa constitucional, lo que llevará a definiciones prácticamente idénticas del interés legítimo.

2.1.4.2. Aplicación: sopesamiento y ponderación

La Ley 3/2018 de España se pronuncia en sus considerandos, indicando que el Título IV incluye normas para tratamientos específicos, sin pretender ser una lista completa de tratamientos cuya licitud se presume. La legalidad de aquellos tratamientos no estaría excluida si no se cumplen estrictamente las condiciones; sino que el responsable debe realizar la ponderación legalmente requerida.

¿Qué implica la ponderación a la que hace referencia la ley? En el Dict. GT29 del 9 de abril de 2014 se encuentra un análisis más exhaustivo a nivel español sobre este particular, en el cual se aclara que la finalidad de esta es impedir un impacto negativo desproporcionado sobre el interesado.

De acuerdo con el numeral iii.3.4., de dicho documento, las categorías que conforman la prueba de sopesamiento son: 1) la evaluación del interés legítimo del responsable del tratamiento; 2) el impacto sobre los interesados; 3) el equilibrio provisional; y, 4) las garantías adicionales. Para entender la razón de esta clasificación, es necesario comprender el alcance de cada una y en qué forma contribuyen a determinar un interés legítimo.

<u>La evaluación del interés legítimo del responsable del tratamiento</u>

Incluye el análisis de: i) el ejercicio de un derecho fundamental; ii) el interés público o el interés de la comunidad en general; iii) otros intereses legítimos; y, iv) reconocimiento jurídico y cultural o social de la legitimidad de los intereses.

Se puede extraer de estos parámetros que el Operador TELCO va a requerir que su interés englobe un derecho contenido en un rango constitucional o supranacional en materia de derechos humanos, el cual debe ser proporcionado y necesario para el fin perseguido.

Asimismo, adquiere fuerza si se complementa con un interés de la comunidad o si ha sido desarrollado a través de pronunciamientos de la agencia reguladora en materia de protección de datos personales.

Es decir, que, si el interés en su sentido neto correspondería con el derecho constitucional de libertad de desarrollar actividades económicas, de contratación y de propiedad, este alcanzará su plena legitimidad al aplicarse el *test* de sopesamiento en la legislación española, o *test* de ponderación en la legislación ecuatoriana.

El impacto sobre los interesados

Comprenderá el análisis de: i) la evaluación del impacto; ii) la naturaleza de los datos; iii) el modo en que se tratan los datos; iv) las expectativas razonables del interesado; v) la posición del responsable del tratamiento y del interesado.

El Operador TELCO requerirá efectuar una matriz de riesgos para conocer el impacto positivo y negativo de la calificación crediticia, detectar el umbral de riesgo y tomar las medidas que lo eliminen o mitiguen. En este aspecto también surgirá una realidad propia del *Score* TELCO, esto es, que no es una expectativa razonable del interesado que sus datos se traduzcan en una predicción de comportamiento crediticio; a lo cual se suma la posición de poder que tendría el operador por sobre el Usuario TELCO, ya que el número de operadoras telefónicas en una misma jurisdicción es reducido y probablemente este servicio sea prestado por aquellas con mayor cuota de mercado y, por tanto, con acceso a *big data*.

Equilibrio provisional

El tratamiento deberá cumplir con los parámetros de: i) proporcionalidad; ii) transparencia; iii) reducción del impacto e injerencia; y, iv) cumplimiento de medidas legales.

A efectos de poder cumplir con este requisito, es imperioso que el Operador genere un algoritmo que le permita obtener un resultado fiable y equitativo, haciendo uso únicamente de aquellos datos que le puedan proporcionar una referencia genuina de la capacidad de endeudamiento y voluntad de pago del Usuario TELCO. Asimismo, deberá encontrarse en cumplimiento estricto de todas aquellas obligaciones que por ley o por resolución de los diferentes entes reguladores a los que está sujeto, le sean exigibles, a saber, las instituciones que regulen los derechos de los consumidores, el poder de mercado, las telecomunicaciones y el tratamiento de datos personales.

Garantías adicionales

Las garantías adicionales deben ser: i) adecuadas; ii) suficientes; y, iii) propias a reducir la repercusión para los interesados. El Operador TELCO que adopte medidas que excedan las mínimas legalmente exigibles se encuentra en ventaja con respecto a garantizar la legitimidad del tratamiento para la finalidad del *Score* TELCO. Este punto servirá para equilibrar la balanza que pudiere haberse visto afectada por las expectativas razonables y la posición del responsable en el segundo eje del *test*; criterio que se encuentra avalado por la AEPD en su Informe Núm. 0156-2014.

Ejemplos de dichas garantías podrían ser medidas técnicas y organizativas, certificaciones de calidad, medidas de ciberseguridad, facilidad para el ejercicio de los derechos ARCO y, en general, una alta protección desde el diseño, mismos que pueden ser aplicados por el Operador TELCO, dado que debe contar con ellos para la prestación ordinaria de sus servicios y sustentado en su alta capacidad económica para invertir en estos aspectos.

Estos cuatro ejes del *test* de sopesamiento, conforme con el Dict. GT29, de 9 de abril de 2014, se considerarán en conjunto con los siguientes parámetros: i) el principio de responsabilidad y transparencia; ii) el derecho de oposición; y, iii) la exclusión voluntaria. En consecuencia, el Operador TELCO que, sin estar obligado, ponga a disposición del Usuario TELCO un extracto de fácil comprensión sobre su *test* de ponderación; que cuente con un proceso fácil para el ejercicio de derechos ARCO, en particular el derecho de oposición; y, que, a falta de una justificación suficiente del interesado le permita la exclusión voluntaria del *scoring*, consolidarán el interés legítimo del Operador TELCO.

En Ecuador, la LOPDP /2021, en su artículo 9, fija únicamente cuatro requisitos para la constitución de un tratamiento por interés legítimo: i) finalidad; ii) necesidad; iii) transparencia; y, de manera opcional, iv) un informe de amenazas concretas en contraposición con las expectativas legítimas.

En esta legislación, aunque no existe el *test* de sopesamiento, se cuenta con la figura de la ponderación contenida en la LOGJCC /2009, artículo 3, numeral 3; y cuya finalidad es permitir una interpretación jurídica que dirima una colisión de derechos. Como en el interés legítimo subyace un derecho que asiste al Operador TELCO, y el Usuario TELCO posee un derecho constitucional a la protección de datos personales, previo a la publicación del RGLOPDP /2023,

era menester recurrir a las técnicas que el ordenamiento jurídico ponía a disposición para dirimir el conflicto (RUÍZ y VICUÑA 2020).

A falta de desarrollo normativo del *test* de ponderación, en Ecuador, a criterio doctrinal y jurisprudencial se consideraba pertinente la aplicación del *test* de acuerdo con los parámetros del doctrinario Robert Alexy, esto es:

- Ley de la ponderación. - Se divide en tres pasos: i) definir el grado de la no satisfacción o de afectación de uno de los principios; ii) definir la importancia de la satisfacción del principio de juega en sentido contrario; y, iii) definir si la importancia de la satisfacción del principio contrario justifica la afectación o la no satisfacción del otro.
- Fórmula del peso. - Se compone de tres variables: 1) intensidad de afectación vs intensidad de satisfacción; 2) el peso abstracto de los principios en colisión; y 3) Seguridad de las premisas epistémicas.
- La carga argumentativa. - Cuando, después de calcular el peso de los derechos, se obtiene el mismo resultado para los derechos en disputa, es necesario resolver el conflicto mediante el uso de argumentos adicionales.

En cuanto al derecho del interesado que entraría en conflicto, la doctrina internacional coincide en que se trata del derecho a la protección de datos, aduciendo que el Tribunal Constitucional ha establecido la idea de la protección de datos personales como un derecho fundamental a través de varias sentencias, lo que ha llevado al reconocimiento de este derecho como independiente (PLANA 2014).

Sin perjuicio de ello, en Ecuador, para que el análisis sea equitativo, podría hacerse con un enfoque en el derecho a la privacidad, ya que el derecho a la protección de datos personales no se encuentra muy desarrollado. Resultaría desigual el enfrentamiento entre derechos ampliamente tratados que pudieren marcar una diferencia considerable al asignarles un valor, pudiendo devenir en la aplicación del interés legítimo como un abuso del derecho.

Esta diferencia en cuanto a la fórmula para ejercer la ponderación cambió, al menos en alto nivel, producto de la publicación del RGLOPDP /2023, puesto que, en su artículo 7.3, fija los mismos cuatro parámetros que el *test* de sopesamiento de España. No obstante, se desconoce si se replicará todo el sistema desarrollado o si se llegaría a un punto medio, considerando que la ponderación se ha aplicado en Ecuador siguiendo los parámetros mencionados

previamente y que, como se verá en el siguiente numeral, siguen siendo aplicados en la jurisprudencia.

Por lo expuesto, se extrae que, desde la óptica del Operador, en ambas legislaciones, es perfectamente posible legitimar el tratamiento de datos personales en el *Score* TELCO justificado en el interés legítimo, siempre que tomen las medidas necesarias desde el diseño y, que hasta que exista un pronunciamiento oficial sobre la forma en que este debe ser aplicado, la tendencia normativa será compatible con el régimen Español, pudiendo aprovecharse las bondades de la doctrina emitida por la Agencia Española de Protección de Datos.

2.1.4.3. Resoluciones de la AEPD y jurisprudencia ecuatoriana

En España se cuenta con un ente rector en materia de protección de datos desde 1993, por lo que existen pronunciamientos expresos que dan claridad a la forma en que se ha plasmado la doctrina contenida en el apartado precedente.

Se cuenta con el Procedimiento Nº: PS/00259/2020 AEPD 07/2021 contra BANKIA S.A.; caso perdido al sustentar la legitimidad del tratamiento en el interés legítimo, siendo el interés alegado de carácter financiero cuando la política de privacidad especificaba que la legitimación empleada para *marketing* directo es el consentimiento. En este caso, existió una contradicción del responsable en su base legitimadora y en la determinación del interés del que se veía asistido, lo cual atañe al primer filtro del *test* de sopesamiento, de manera que no hubo necesidad de analizar el reclamo con mayor profundidad, generando una sanción al responsable.

En el Procedimiento Nº: PS/00406/2020 AEPD 03/2021, contra EQUIFAX IBÉRICA, se trató de una inclusión en fichero de morosidad sin existir deuda y sin previo aviso al titular. Si bien el *Score* TELCO no es un fichero oficial de solvencia, bien podría aplicarse por analogía el deber de informar la posibilidad de una afectación en su calificación. Esto estaría amparado en el Dict. GT29, de 9 de abril de 2014 sobre las recomendaciones adicionales al *test* de sopesamiento, aumentando las posibilidades de emplear el interés legítimo como causal suficiente del tratamiento.

En el Procedimiento Nº: PS/00221/2020 AEPD 11/2020 contra LVCENTVM LEGAL S.L., la comunicación se produjo en el marco de un procedimiento judicial civil de reclamación de

derechos de propiedad intelectual, acreditando su interés con base en la defensa de sus derechos legales. No obstante, en su política de privacidad al efectuar una notificación de cobro con datos obtenidos de terceros, obvió comunicar al titular sus derechos ARCO, incumpliendo una obligación regulatoria. En consecuencia, el interés legítimo no se configura cuando existe un incumplimiento de medidas horizontales. Asimismo, del caso se desprende que hubo una extralimitación en la finalidad del tratamiento, perdiendo la legitimación.

De los casos en mención se desprende que, en España, el responsable del tratamiento tiende a presentar dificultades para justificar la finalidad del tratamiento, de manera que no se llega a efectuar el *test* de necesidad ni el *test* de equilibrio. En Ecuador, por otra parte, el desarrollo ha recaído en la justicia constitucional, siendo a la fecha el único órgano con capacidad de resolver la posible contraposición entre un interés legítimo contenido en un derecho y los derechos fundamentales del interesado, a través del ejercicio de una acción denominada *hábeas data*.

El doctrinario Alejandro Mogroviejo Gavilanes (2020) se pronuncia en este orden, manifestando que la Corte Constitucional no ha delimitado la diferencia entre un juicio de ponderación y uno de proporcionalidad, de manera que la jurisprudencia ha ido construyendo gradualmente este último, elevándolo al estatus de principio constitucional e instrumento legal. Posteriormente, se le ha atribuido la característica de razonabilidad como salvaguarda de un orden justo.

Como consecuencia, se estará ante el mismo principio de proporcionalidad comprendido como el examen de la idoneidad, la necesidad y una ponderación en sentido estricto, pero menos riguroso. Esto da a pensar que la forma en que se realiza la ponderación judicial será, en la práctica, la que se termine adoptando en materia de protección de datos personales, plasmándose en las resoluciones que llegare a emitir la Superintendencia. Sin perjuicio de lo último, se considera que una aplicación por analogía del *test* de sopesamiento sería de gran utilidad en Ecuador, generando una protección más efectiva al tratamiento de los datos del Usuario TELCO.

En las páginas que anteceden, se ha definido la noción de *Score* TELCO y su evolución histórica, al igual que descrito generalmente sus procesos, actores, marco normativo y legitimación. En las páginas siguientes se ahondará en los procesos *Score* TELCO y en los datos tratados a esta ocasión, a fin de identificar los problemas inherentes relativos a la protección de dichos datos.

2.2. El flujo de tratamiento de datos

Como anunciado, luego de haber introducido la noción de *Score* TELCO, corresponde detallar los tipos de datos tratados (2.2.1.) y los tipos de tratamientos a los que están sujetos (2.2.2), a fin de describir los problemas en los macroprocesos que se presentan, dirigiéndose a la solución a la cual este trabajo busca contribuir.

2.2.1. Tipos de datos

Para comprender mejor la figura del Score TELCO y su relación con el tratamiento de datos personales, se procederá a estudiar los datos que el Operador recolecta del Usuario TELCO y cómo estos datos, debidamente procesados, son capaces de brindar información de la capacidad y voluntad de pago de un posible cliente. Los datos se clasifican, esencialmente en dos grupos: datos de telecomunicaciones (2.2.1.1.) y datos de atención al cliente (2.2.1.2.).

2.2.1.1. Datos de telecomunicaciones

Datos de uso

Empezando por los datos que conciernen estrictamente a los servicios de telecomunicaciones, existen los "Datos de uso", que se obtienen a través del *CDR* o registro de llamadas. Si se visualiza el registro de llamadas en nuestros dispositivos móviles, se notará que queda un registro de la hora, la fecha, la duración, el número al que se realizó la llamada o del cual la se recibió; se verá que hay llamadas salientes, entrantes, llamadas perdidas, números frecuentes, llamadas devueltas.

El *CDR* inclusive ha evolucionado por la amplitud de datos que procesa a medida que las redes soportan mayor tecnología. En ocasiones, los registros de red más amplios se conocen como registros de datos genéricos (*XDR*) o registros de uso de datos (*UDR)*. Estos registros contienen datos sobre mensajes de texto *SMS*, la utilización de internet y registros de administración de la movilidad (MACMILLAN, GARVEY 2021).

Datos de localización

Existen también los "datos de localización", que van a ser tratados por el Operador TELCO por ser indispensables para la prestación del servicio, puesto que el dispositivo móvil, una vez que esté en funcionamiento, iniciará un proceso de conexión mediante el uso de su identidad de suscriptor móvil internacional (*IMSI*) para registrarse en la red móvil correspondiente y

comprobar el estado de la suscripción (MACMILLAN, GARVEY 2021). Si el Usuario TELCO desactiva su *GPS*, igual podrá ser localizado, ya que el dispositivo se irá conectando y desconectando de los equipos de red permanentemente, de acuerdo con sus desplazamientos físicos.

Datos de red y aplicaciones

Otra fuente de datos son los "datos de red y aplicaciones". Al igual que los equipos móviles del Usuario TELCO, el Operador TELCO cuenta con equipos que le permiten prestar sus servicios, entiéndase, la infraestructura de la red. Dichos equipos registran errores en la red, caídas en el servicio, calidad de la señal, etc. En cuanto a las aplicaciones, los datos que registren dependerán de la aplicación utilizada, por ejemplo, un mensaje dejado en el buzón de voz receptará la grabación de voz.

Datos generados por máquinas

Los "datos generados por máquinas" provienen de los dispositivos móviles, los dispositivos de *internet of things (IOT)*, decodificadores de televisión de señal analógica o digital, *routers,* etc.

Datos de actividad en línea

Por otro lado, los "datos de actividad en línea" provienen de la interacción del Usuario TELCO en los navegadores de internet y en el uso de las aplicaciones que haya descargado en su dispositivo. Poniendo un ejemplo muy concreto que engloba ambos tipos de datos, el dispositivo móvil del Usuario TELCO puede tener descargada una aplicación que permita controlar su lavadora de ropa y otros datos socioeconómicos.

2.2.1.2. Datos de atención al cliente

La otra cara de los servicios del Operador TELCO consiste en la atención al cliente, que dentro del giro del negocio de las telecomunicaciones implica un trabajo permanente, que debe cubrir a todos los usuarios en la mayor cantidad de canales posibles (los detalles dependerán de las condiciones de su contrato de concesión).

La atención al cliente de una operadora puede ser, sin perjuicio de nuevos canales que se vayan desarrollando, mediante un centro de atención al cliente, *contact center*, fuerza de venta (vendedor en calle), distribuidor autorizado o canal digital. Dicha atención podrá ser con fines de activación de servicios o por gestión *backoffice*, también llamada de soporte.

Datos de identificación del suscriptor

El primer grupo de datos que se pueden obtener, son los "datos de identificación del suscriptor", que son datos básicos de una persona natural, como los que constan en su documento nacional de identificación: número único, nombres y apellidos, género, país, ciudad, estado civil; a ello se le agregan datos que son necesarios para activar determinados servicios, como el domicilio, correo electrónico y la copia de algún documento como la misma cédula o una planilla de servicios básicos.

Datos de pedido y facturación

El segundo grupo de datos está conformado por los "datos de pedido y facturación", los cuales varían según la modalidad del Usuario TELCO. Si es un cliente pospago, se contará con información de facturación frecuente y de un consumo estable, ceñido a su plan contratado.

En el caso de clientes prepago, se obtendrá información acerca de las elecciones que los suscriptores hacen en cuanto a los planes de llamadas y datos, así como la frecuencia y el monto de las recargas.

En ambos escenarios, el Operador TELCO tendrá un registro de los equipos y servicios que adquiera el Usuario TELCO (los "pedidos"), por ejemplo, productos *IOT*, licencias de software, accesorios, seguros por robo de dispositivo, etc.

Datos del dispositivo

Por último, están los "datos del dispositivo", que pueden ser captados por la red de telecomunicaciones o alimentados manualmente en el *CRM* del Operador TELCO. Para brindar el servicio, la red es capaz de identificar todos los aspectos del dispositivo que solicita la señal, incluyendo su sistema operativo. Estos datos del dispositivo, vistos como activos, posibilitan la deducción de información relacionada con la capacidad de gasto del Usuario TELCO. Además, la red puede identificar si múltiples dispositivos se conectan desde la misma dirección y si presentan rasgos que los relacionen con el mismo Usuario TELCO (MACMILLAN, GARVEY 2021).

El Operador TELCO en muchas ocasiones no contará con datos netamente crediticios, mas la vasta pluralidad de fuentes de datos de diversa naturaleza le permiten contar con *big data*, o información en bruto, que, con los algoritmos apropiados, puede transformar en un *scoring* que sirve en sí mismo o como complemento de un *SCORE* tradicional.

En España existe un ejemplo de *Score* TELCO de la operadora Telefónica, en cuya descripción denota pautas del tratamiento, como el empleo de *big data*, inteligencia artificial, *internet of things*, *open data*, red TELCO, algoritmos; todo ello compele al desglose del flujo del tratamiento de datos personales para llegar a determinar el correcto tratamiento en cada una de sus fases.

En este punto, se destaca que en artículo 24 del RGLOPDP/ 2023, los datos tratados por un Operador TELCO y que han sido identificados en este apartado, tienen un régimen especial en cuanto a la notificación de vulneraciones de seguridad. Esto deberá tomarse en cuenta puesto que existe la obligación legal de notificar al titular, a la SPDP y a la ARCOTEL en aquellos casos en que exista un riesgo de vulnerabilidad; ello implica un monitoreo permanente en cada macroproceso del tratamiento de datos, el cual se desarrollará en el título siguiente.

2.2.2. Tipos de tratamientos

Es relevante mencionar que, en el flujo de vida de los datos señalados, se producen diversos tratamientos necesarios para la prestación del servicio de *Score* TELCO; por ello, para una mejor comprensión, se analizan los tratamientos elementales de recolección (2.2.2.1.), almacenamiento (2.2.2.2.), procesamiento (2.2.2.3.), consulta (2.2.2.4.) y eliminación (2.2.2.5.). Se abordarán estos procesos desde su reglamentación respectiva en el orden jurídico español; puesto que no han sido abordados en la legislación ecuatoriana aplicable a la materia.

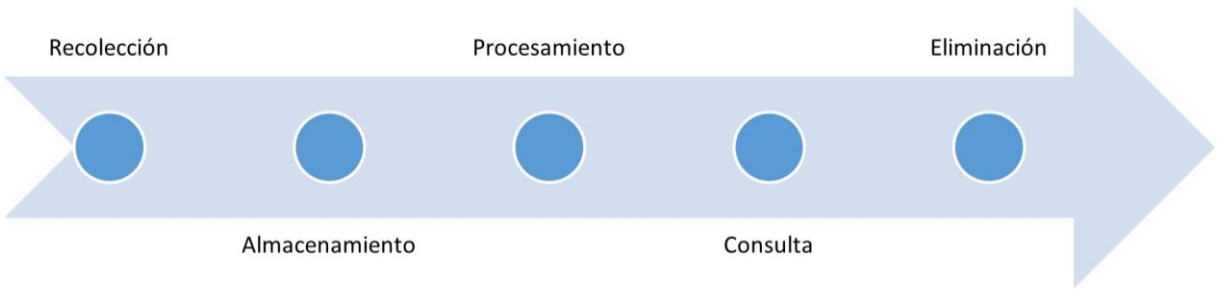

Figura 1. "Macroprocesos del flujo del tratamiento". (Elaboración propia 2023)

2.2.2.1. Tratamiento "Recolección"

El primer paso en el flujo de tratamiento consiste en la recolección. Se ha podido identificar que existen datos recolectados con el consentimiento del Usuario TELCO, como los datos del

CRM, IOT y *Cookies*, y se cuenta con datos obtenidos sin el consentimiento de este, como los recolectados por *DNS*, memoria *Caché* y *CDR*.

CRM, IOT y Cookies

El Reglamento (UE) 2016/679, en su artículo 11, define el consentimiento del interesado como cualquier expresión libre, específica, informada e inequívoca de su voluntad, ya sea a través de una declaración o una acción clara y afirmativa, en la que acepta el tratamiento de sus datos personales. Dicha norma debe interpretarse en concordancia con el Art. 7, numerales 1 y 2 *eiusdem*, que fijan la obligación del responsable del tratamiento de poder demostrar el consentimiento obtenido y establece el presupuesto de solicitar el consentimiento de manera que sea claramente discernible de otros temas, sea fácilmente comprensible y accesible, y se utilice un lenguaje natural.

Ahora bien, es interesante que, aunque se pide una acción afirmativa de parte del Usuario TELCO, el numeral 2 del artículo 14 del RDL 1720/2007 ofrece una alternativa para recabar el consentimiento, indicando que el responsable puede comunicarse con la persona afectada, proporcionándole información y otorgándole un plazo de treinta días para expresar su rechazo al tratamiento. Asimismo, se le advierte que, en caso de no emitir una respuesta en contra, se considerará que consiente el tratamiento de sus datos personales.

La opción que se recomienda siempre será la del consentimiento previo mediante una acción afirmativa, cuando el tipo de datos así lo requiera, mas es importante tomar en consideración que, si no fuere posible recabarlo oportunamente, existe la salvedad que se acaba de plantear. Un ejemplo de aplicación de esta salvedad podría ser la actualización de la política de privacidad o de la política de cookies, ya que la cantidad de Usuarios TELCO no permite una gestión individual del consentimiento, además que generaría la paralización de las consultas en el *Score* TELCO.

Se debe tener en cuenta que el Operador TELCO recolecta los datos mencionados en este trabajo de manera permanente, para cumplir y mejorar diversos aspectos de sus servicios; por tanto, el tratamiento ulterior que efectúe con ellos con la finalidad de generar un *Score* TELCO, no requiere de un esfuerzo adicional en el tratamiento recolección.

DNS, Caché y *CDR*

En cuanto a los datos recolectados con los métodos *DNS*, memoria Caché y *CDR,* estos están cubiertos por el numeral 1 del artículo 8 de la Ley 3/2018 de Protección de Datos, en el cual se alega que el tratamiento solo puede considerarse justificado por el cumplimiento de una obligación legal aplicable al responsable cuando así lo establezca la normativa de la Unión Europea o una norma con jerarquía de ley.

Esto, en concordancia con el artículo 10, numeral 3, literal b), del RDL 1720/2007, aclara que los datos provenientes de dichas fuentes pueden ser recolectados sin el consentimiento del Usuario TELCO por ser tratados en el contexto de una relación contractual o precontractual, o de la existencia de una relación comercial, laboral o administrativa en la que el afectado sea parte, y los datos son necesarios para su mantenimiento o cumplimiento.

Inclusive, si se habla de los Usuarios TELCO del segmento masivo prepago, el artículo 153, numeral 1 *ibidem*, prevé la posibilidad de obviar el deber de informar sobre el tratamiento de los datos, por ser imposible o exigir esfuerzos desproporcionados, pudiendo el Operador TELCO subsanarlo mediante una cláusula informativa en, por ejemplo, su página web.

2.2.2.2. Tratamiento “Almacenamiento”

Una vez recolectados los datos, estos deben ser almacenados para poder ser procesados ulteriormente. En relación con este almacenamiento, se analizará subsiguientemente ciertas categorías de organización del almacenamiento de los datos recolectados, y ciertos métodos de almacenamiento aplicables al *Score* TELCO.

Organización del almacenamiento.-

En cuanto al almacenamiento de datos, este puede realizarse por ficheros, en vista de establecer un perfil del Usuario TELCO.

El artículo 6 del Reglamento (UE) 2016/679, define los ficheros como cualquier conjunto organizado de datos personales, accesibles según criterios específicos, ya sea de forma centralizada, descentralizada o distribuida funcional o geográficamente.

Tal fichero puede ser o no automatizado, este último es definido en el RDL 1720/2007 como cualquier agrupación de datos personales organizados manualmente y estructurados de

acuerdo con criterios específicos relacionados con personas físicas. Esto simplifica el acceso a sus datos personales sin necesidad de esfuerzos desproporcionados.

Tales definiciones llevan a comprender el tratamiento inmediato que van a recibir los datos recolectados, que pasarán de ser datos en bruto a datos estructurados. Siguen siendo varias fuentes de datos; no obstante, algunas fuentes son en sí mismas un fichero y otras conforman un fichero al ser interpretadas en su conjunto. A manera de ejemplo, el *CRM* es un fichero en sí mismo, pero las *cookies* y la memoria caché requieren de un esfuerzo adicional para constituirse en un fichero. Producto de estas fuentes, se generará el fichero "final": el *Score* TELCO, entendido como la plataforma.

La existencia de ficheros generará obligaciones especiales al responsable y al encargado del tratamiento de datos personales, al propiciar el proceso de identificación del Usuario TELCO. El Reglamento (UE) 2016/679, artículo 13, numeral 2, literal f), establece la obligación de informar al interesado que sus datos serán tratados para la elaboración de perfiles. No obstante, el artículo 22, numeral 2, literal a), el Operador TELCO podría obviar dicha obligación cuando resulta indispensable para la firma o ejecución de un contrato entre el titular y un responsable del tratamiento, o está permitida por la legislación de la Unión Europea o de uno de sus miembros.

En este orden, si el Operador TELCO estableciera el perfilado de los Usuarios TELCO como parte del proceso comercial o *backoffice* en la prestación de los servicios de telecomunicaciones, no necesitaría informarle al Usuario TELCO de la existencia de ficheros. No obstante, se considera que queda descubierto el fichero más importante y sobre el cual se requerirá seguir profundizando: la plataforma de *scoring*.

Con respecto a los datos que pueden ser almacenados en ficheros para el posterior perfilamiento del Usuario TELCO, el artículo 38 RDL 1720/2007 fija limitaciones a la inclusión de los datos crediticios en el *Score* TELCO que incluyen la existencia previa de una deuda cierta, vencida, exigible e impagada, sin reclamación, que no hayan pasado seis años desde la fecha de pago o vencimiento y la necesidad de un requerimiento de pago previo.

Estos requisitos implican un control constante por parte del Operador TELCO, ya que, al ser un negocio de alcance nacional, contar con varios canales de atención y tener disposiciones

financieras como la venta de cartera vencida, debe tener un grado de diligencia que lo mantenga en el cumplimiento de estos lineamientos.

Nótese que son medidas lógicas, aplicables a todo *scoring*, mas existe un límite normativo que sí afecta directamente al *Score* TELCO y que se halla plasmado en la Disposición Adicional Sexta de la Ley 3/2018, el cual consiste en que las deudas de un monto inferior a cincuenta euros no serán incluidas en los sistemas de información crediticia. Tomando en cuenta el precio de los paquetes de recargas automáticas y de los planes más activados, se pierde mucha información útil para aumentar la efectividad del *scoring*. Esta limitación no existe en Ecuador, por lo que la calificación reflejaría con mayor fidelidad la capacidad de endeudamiento y predisposición al pago.

Métodos de almacenamiento.-

Dentro del flujo de tratamiento de datos recolectados por las operadoras, se presentan diversos métodos de almacenamiento de los datos que se procesarán directamente para generar una calificación crediticia basada en el uso de los servicios del Operador por parte del Usuario TELCO. Entre estos métodos, cabe destacar:

Servidores propios

Algunos datos pueden ser almacenados en servidores ubicados en las instalaciones de la propia empresa de telecomunicaciones. Estos servidores están físicamente en la sede de la empresa o en sus centros de operación.

Centros de datos privados

Las empresas de telecomunicaciones a menudo utilizan centros de datos privados para alojar servidores y sistemas de almacenamiento. Estos centros de datos proporcionan infraestructura de alta disponibilidad, seguridad y conectividad.

Almacenamiento en la nube

Muchas empresas de telecomunicaciones utilizan servicios de almacenamiento en la nube, como *Amazon Web Services (AWS), Microsoft Azure* o *Google Cloud Platform*, para alojar y gestionar datos. La nube ofrece escalabilidad, redundancia y flexibilidad.

De acuerdo con RED HAT (2023), se pueden encontrar nubes públicas, privadas e híbridas. Para efectos del tratamiento de datos personales obtenidos de la actividad del Usuario TELCO

en las redes sociales o información proporcionada en campañas específicas de mercadeo o deducibles de los mensajes *bulk* que los clientes corporativos del Operador TELCO le hace llegar al Usuario TELCO, se recomienda el uso de una nube privada.

La nube privada presenta una serie de ventajas que permiten una adecuada protección: control, seguridad, personalización, rendimiento, privacidad, escalabilidad comprobada, disponibilidad y facilita la conformidad con las regulaciones legales. Para las empresas que se desenvuelven en sectores altamente regulados, como la salud o las finanzas, las nubes privadas surgen como una alternativa propicia; agilizan el cumplimiento de normativas y regulaciones específicas al conferir un control completo sobre la seguridad y el acceso a los datos (CADLAN 2023).

Sistemas de almacenamiento distribuido

Algunas empresas de telecomunicaciones utilizan sistemas de almacenamiento distribuido, como sistemas de archivos distribuidos o bases de datos *NOSQL*, para gestionar grandes volúmenes de datos de manera eficiente.

- Sistema de archivos distribuidos.- Se denomina distribuido cuando sus contenidos están ubicados en varias máquinas o nodos, operando con un espacio de nombres compartido (CIFUENTES 2018). Su principal utilidad es lograr recuperar datos en caso de falla en uno de los medios de almacenamiento;
- Bases de datos *NOSQL*.- es un tipo de sistema de gestión de bases de datos diseñado para almacenar, recuperar y gestionar datos que no se ajustan bien a las bases de datos relacionales tradicionales (*SQL)* que utilizan tablas con filas y columnas para almacenar datos. Por ejemplo, HBase y Cassandra (RODRÍGUEZ, RODRÍGUEZ, DÍAZ 2016).

Backups y recuperación de desastres

Los datos suelen respaldarse regularmente y se almacenan en ubicaciones seguras como parte de las estrategias de recuperación de desastres. Existen diferentes tipos de respaldos de bases de datos: uno completo que guarda todos los archivos de datos, uno parcial que cubre solo una parte específica, uno integral que copia todos los bloques de datos en uno o más archivos, y uno incremental que registra los cambios desde el último respaldo (CARREÑO 2017).

Se recomienda realizar copias de seguridad completas de manera regular. En caso de no ser factible efectuar respaldos en tiempo real, se debería considerar mínimo un respaldo semanal para asegurar la integridad, disponibilidad y veracidad de los datos personales almacenados.

Almacenamiento temporal (caché)

Algunos datos, como los registros de actividad de la red, pueden almacenarse temporalmente en caché antes de ser procesados o archivados en sistemas de almacenamiento a largo plazo.

La infraestructura de red que rodea a las antenas de telecomunicaciones, como los equipos de conmutación y enrutamiento en el centro de datos del Operador, puede tener memoria caché y sistemas de almacenamiento temporal para optimizar el rendimiento de la red y reducir la carga en los servidores y enlaces de datos.

En términos generales, el tipo de almacenamiento utilizado en empresas de telecomunicaciones se vincula con su operación cotidiana. La información para las evaluaciones crediticias de usuarios, especialmente en el segmento prepago, se obtiene mayormente de datos generados automáticamente durante el uso de servicios de telecomunicaciones. Solo un pequeño porcentaje de abonados llega al número máximo de líneas que requiere un empadronamiento y consecuente intervención en campañas de mercadeo, deviniendo en el almacenamiento de sus datos personales en formatos estructurados específicos.

2.2.2.3. Tratamiento “Procesamiento”

En vista de establecer el *Score* TELCO, los datos recolectados y almacenados deben ser procesados por medio de metodologías de procesamiento, generalmente patentadas. Esto implica que no existe una base única que permita comprender cómo se llega desde los datos extraídos y almacenados hasta la calificación que se muestra en el software utilizado por el sector *retail*. Sin embargo, se reconoce que, a un nivel más abstracto, se emplearía la ciencia de datos con este propósito.

El *data science* implica la gestión de datos que integra disciplinas como estadística, métodos científicos, inteligencia artificial y análisis con el objetivo de extraer valor de la información. Esto incluye la preparación de datos mediante procesos como limpieza, agregación y manipulación para llevar a cabo análisis complejos (HILBCK y BUENO 2022).

Cabe señalar que, de forma específica, la Agencia Española de Protección de Datos (2020) en su obra Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial – Una Introducción, habla de varios sub-tratamientos comprendidos en el flujo de vida del dato: 1) desarrollo/entrenamiento, 2) validación, 3) despliegue/explotación (compuesto por inferencia/perfilado, decisión y evolución), y 4) retirada; de los cuales los tres primeros pueden catalogarse dentro del tratamiento "procesamiento"; particular que se puntualiza para comprender el grado de exhaustividad al que se puede llegar si se abarca este tratamiento desde una óptica informática.

Figura 2. "Tratamiento Procesamiento". (Elaboración propia 2023)

Para mayor comprensión del flujo de datos personales, se procederá a describir algunos algoritmos y métodos comunes utilizados para la fase de procesamiento:

Análisis de regresión

El análisis de regresión se utiliza para identificar relaciones estadísticas entre variables. En el contexto de la calificación crediticia basada en telecomunicaciones, puede utilizarse para determinar cómo ciertos comportamientos, como la consistencia en el pago de facturas o la duración de la relación con un proveedor, se relacionan con el riesgo crediticio.

Análisis de series temporales

El análisis de series temporales se utiliza para detectar patrones y tendencias a lo largo del tiempo en los datos de consumo de telecomunicaciones. Puede ayudar a identificar cambios en el comportamiento del usuario que podrían ser indicativos de problemas financieros.

Aprendizaje automático

Los algoritmos de aprendizaje automático, como las máquinas de soporte vectorial (*SVM)*, bosques aleatorios (*Random Forests*) y redes neuronales, pueden ser entrenados utilizando datos de consumo de telecomunicaciones y datos crediticios históricos para predecir la solvencia crediticia de un individuo o entidad.

- Soporte vectorial.- Se trata de un proceso donde un conjunto de instrucciones especiales se utiliza para cambiar la forma en que se ven los datos de entrenamiento originales. Esto ayuda a encontrar la mejor línea imaginaria que divide de manera más clara los elementos de un grupo de los de otro grupo, como si fuera una frontera que los separa (VARGAS 2015).
- Bosques aleatorios.- Se trata de un algoritmo que fusiona los resultados de múltiples árboles de decisión con el fin de obtener un resultado único. Cada uno de estos árboles se entrena con una selección aleatoria de los datos y, en ocasiones, con un subconjunto aleatorio de las variables disponibles (IBM 2023).
- Redes neuronales.- De acuerdo con la doctrinaria Elena Esteve (2005), son modelos que buscan imitar el funcionamiento del cerebro. Como tal, simplifican el sistema identificando los elementos relevantes, ya sea debido a la abundancia o redundancia de la información disponible

Análisis de clústeres

El análisis de clústeres agrupa a los individuos o entidades en segmentos o grupos con comportamientos similares en función de sus patrones de consumo de telecomunicaciones. Esto puede ayudar a identificar segmentos de alto y bajo riesgo crediticio. Ej. Algoritmo *K-Means.*

Análisis de redes sociales

En algunos casos, se pueden utilizar algoritmos de análisis de redes sociales para evaluar las conexiones y relaciones de un individuo en función de su actividad de telecomunicaciones. Esto puede proporcionar información adicional sobre su solvencia crediticia. Ej. algoritmo *NLP* (procesamiento de lenguaje natural), *Page Rank* (relevancia de páginas), *LDA* (asignación latente Dirichlet).

Técnicas de minería de datos

La minería de datos implica explorar grandes conjuntos de datos en busca de patrones y relaciones ocultas. Puede utilizarse para identificar características clave en los datos de consumo de telecomunicaciones que están correlacionadas con el riesgo crediticio. Ej. detección de anomalías, análisis de componentes principales.

Existen casos en los cuales el proceso de "recolección" se fusiona con el proceso de "procesamiento" sin necesidad de un almacenamiento debido a la rapidez de la transacción. Esto dependerá del tipo de dato que se está extrayendo. Por ejemplo, se puede encontrar datos personales almacenados en el *CRM* principal del Operador TELCO, mientras que los datos extraídos del uso de redes sociales se analizan de manera instantánea. Producto de ello, es posible afirmar que el procesamiento de datos personales se puede dividir en dos categorías: simple (proveniente de fuentes estructuradas) y compuesto (proveniente de fuentes no estructuradas).

2.2.2.4. Tratamiento “Consulta”

Una vez procesados los datos, el *Score* TELCO sería en principio consultable. A menudo, este tipo de servicios son ofrecidos a través de dos medios principales: los servidores *web* (*web servers*) y las interfaces de programación de aplicaciones (*API*). Cada uno de estos enfoques tiene sus propias ventajas; sin embargo, corresponde analizar si existe un medio idóneo para la exposición de la calificación crediticia producto del tratamiento de datos personales, considerando que serán objeto de consultas masivas por parte de terceros (*retail)*.

Interfaz de programación de aplicaciones (*API*)

Una *API* es un conjunto de instrucciones que controla el funcionamiento de un *software* y permite transferir datos entre diferentes partes del programa. Estas interfaces posibilitan que una aplicación extraiga archivos o datos preexistentes de un *software* y los utilice en otro programa o en uno de sus componentes.

El término "*API*" proviene de las siglas en inglés de "*application programming interface*" o interfaz de programación de aplicaciones. Cada *API* tiene un destino al que debe enviar los datos extraídos, conocido como "punto de terminación de *API*", que puede tomar la forma de una aplicación móvil, un sitio web o un sistema de gestión de datos.

Existen tres conceptos necesarios para entender el funcionamiento de una *API*: llamada, intermediación y aplicación:

a) La llamada.- es una instrucción que permite extraer información de otra sección del mismo programa o de una herramienta externa que pueda ser integrada. Por lo general, se manifiesta como una línea de código donde se solicita la biblioteca, fragmento de código o base de datos necesarios;

b) La intermediación.- implica extraer la información requerida y luego integrarla en el código del nuevo programa; y,
c) La aplicación.- se refiere a la ejecución de la información como parte de la nueva programación. Las *API*s son útiles para aplicar formatos, estilos o importar datos desde diferentes fuentes.

Asimismo, existen diversos tipos de *API* (COPPOLA 2023), las cuales se pueden clasificar en:

i) API Pública: Disponible para cualquier usuario;
ii) *API* Privada/Cerrada: Son herramientas a las que solo pueden acceder los usuarios autorizados. Estas cuentan con *gateways* o puertas cerradas que restringen el acceso a usuarios específicos;
iii) *API HTTP*: Las *HTTP API* o *web API* son interfaces diseñadas para ser utilizadas en el desarrollo de sitios web a través del protocolo de transferencia de hipertexto;
iv) *SOAP*: Las *API* de protocolo simple de acceso a objetos constan de una serie de instrucciones que permiten a un programa acceder a información básica desde otra ubicación; y,
v) *RESTful API*: Las *RESTful API* o *API* de transferencia de estado representacional son interfaces diseñadas para interactuar con una arquitectura de *software* específica basada en contenido multimedia. Ejemplo: *API* para aplicaciones móviles.

Servidor *web*.-

Los servidores web son un componente esencial de los sistemas de servidor y tienen la tarea principal de almacenar todos los archivos relacionados con una página *web,* como imágenes, texto y videos, y luego transmitirlos a los usuarios a través de los navegadores mediante el protocolo *HTTP* (Protocolo de Transferencia de Hipertexto) (DE SOUZA 2019).

Para que el servidor *web* funcione correctamente, debe recibir solicitudes de navegadores. En otras palabras, cuando se realiza una solicitud desde una dirección *IP*, esta se envía a la dirección *IP* del servidor que alberga los archivos del sitio web en cuestión.

Una vez que recibe la solicitud, el servidor *web* busca la información solicitada en sus archivos, interpreta el código correspondiente y envía el resultado de vuelta al navegador que realizó la solicitud.

La decisión en cuanto a la elección entre un servidor *web* y una *API* dependerá de múltiples factores, como los objetivos de la aplicación, los requisitos de seguridad y regulación, la arquitectura del sistema y las necesidades de integración. A efectos del *Score* TELCO como producto que trata datos personales, se recomienda emplear una *API;* ya que permite el uso de múltiples plataformas, soporta planes de escalabilidad, mejora la experiencia del usuario y permite la implementación de mayores medidas de seguridad y control de accesos.

2.2.2.5. Tratamiento "Eliminación"

Eliminar datos personales que ya no son necesarios para los fines del tratamiento o cuya supresión debe ejecutarse producto del ejercicio de los derechos ARCO, es una práctica esencial que debe ser garantizada por el Operador TELCO para proteger la privacidad del Usuario TELCO, cumplir con el régimen regulatorio, reducir costos de almacenamiento, mejorar la eficiencia en la gestión de datos y mantener la confianza de los abonados. El Operador TELCO debe implementar políticas y prácticas que incluyan la eliminación segura y oportuna de datos que ya no son relevantes.

La Agencia Española de Protección de Datos (2020) en su Guía de Protección de Datos por Defecto, puntualiza que la implementación del principio de minimización en el plazo de retención establece que, si un dato personal deja de ser necesario después de completar una fase del tratamiento, deberá eliminarse (lo que en ciertos casos podría implicar el bloqueo o la anonimización). Toda retención debe estar objetivamente justificada y fundamentada.

A efectos de comprender la mejor forma en que el Operador TELCO puede efectuar la eliminación de los datos, se recomienda cumplir con un proceso de borrado seguro, es decir, aquel diseñado para eliminar permanentemente la información personal almacenada en dispositivos electrónicos o sistemas de almacenamiento. La expectativa de implementarlo es que los datos eliminados no puedan ser recuperados, incluso mediante softwares diseñados para recuperación de datos.

El método de borrado seguro dependerá del tipo de almacenamiento que se utilice. Se pueden considerar opciones como trituración, incineración o el uso de químicos para almacenamiento físico. Para almacenamiento magnético, se puede optar por sobreescritura, desmagnetización o destrucción física. En el caso de almacenamiento óptico, la destrucción física es una opción. Para almacenamiento óptico regrabable, se recomienda usar sobreescritura o destrucción

física. En el caso de almacenamiento de estado sólido, la sobreescritura y la destrucción física son alternativas válidas. Si se trabaja con almacenamiento en la nube, la medida consistirá en contar con un contrato de servicio con políticas de copias de seguridad y respaldos (BECERRA 2017).

En Ecuador, la LOPDP /2021 y el RGLOPDP /2023 disponen, en su artículo 15 y 9, respectivamente, que, en aquellos casos en que proceda la eliminación de los datos, esta podrá efectuarse a través de métodos de eliminación propiamente dicha, bloqueo, anonimización, hacer ilegible o irreconocibles los datos personales. Asimismo, el RGLOPDP / 2023, en su artículo 11, permite la implementación de estándares internacionales para la eliminación de los datos; ello vuelve admisible la implementación de las medidas sugeridas por la AEPDP (2020) sobre tratamientos que involucran inteligencia artificial.

En el *Score* TELCO se deberá prestar especial atención, ya que existen datos de tratamiento obligatorio (referentes a la prestación técnica del servicio de telecomunicaciones) y datos que deben permanecer almacenados para la defensa de acciones legales. En este sentido, si el Operador elimina los datos y dentro de los diez años subsiguientes que opera la prescripción de las acciones en Ecuador, el titular desea ejercer sus derechos por considerar que se vio afectado en una calificación crediticia de hace nueve años, el Operador debe tener claridad absoluta de los datos tratados y del resultado obtenido.

El Operador TELCO podrá escoger, de acuerdo con sus necesidades y conveniencia, si este proceso ha de efectuarlo directamente o por medio de un encargado. En ambos casos, el departamento de Aseguramiento de Ingresos y Control de Accesos, o el que hiciere sus veces, realizará la verificación del cumplimiento de la obligación de eliminar la data, debiendo requerir evidencia documental y, de ser posible, audiovisual, que le sirva de soporte ante el Ente Regulador en materia de Datos Personales.

2.3. Obligaciones del Operador TELCO

Comprendidos los tipos de datos y de tratamientos que se efectúan a los datos personales del Usuario TELCO para la obtención del Score TELCO, se procede a estudiar como última instancia las obligaciones que debe cumplir el Operador TELCO para garantizar un adecuado nivel protección; por ello, se evaluará el avance normativo español y se destacarán figuras jurídicas replicables en Ecuador en los ámbitos de consideraciones regulatorias (2.3.1.), relaciones

contractuales (2.3.2.), política de privacidad (2.3.3.) y el ejercicio de los derechos ARCO (2.3.4.).

2.3.1. Consideraciones regulatorias

Tomando como punto de partida que, tanto Ecuador como España, cuentan con normativa en protección de datos, con una autoridad que ejerce el papel de ente regulador del cumplimiento y que el Operador TELCO ejerce la prestación de un servicio concesionado altamente escrutado, conviene indagar en las consideraciones regulatorias que el Operador debe tomar en cuenta para poder ofrecer el servicio de *scoring* de forma sostenible en el tiempo. Ante ello, se analiza la obligación de efectuar una correcta gestión del riesgo (2.3.1.1.) y una evaluación de impacto (2.3.1.2.).

2.3.1.1. Gestión del riesgo

La AEPDP (2021), en su informe Gestión del riesgo y evaluación de impacto en tratamientos de datos personales, fija estos dos parámetros como indispensables para los tratamientos que conllevan riesgos considerables. La gestión de riesgos se compone de una serie de medidas organizadas y estructuradas con la finalidad de supervisar las posibles repercusiones que una actividad puede tener sobre un conjunto de activos que requieren protección, considerando tanto la probabilidad como la magnitud de los impactos. La evaluación de impacto, en cambio, constituye un componente de dicha gestión que toma fuerza en tratamientos que aplican nuevas tecnologías, como el *Score* TELCO.

El Reglamento (UE) 679/2016 manifiesta en su artículo 24, numeral 1, que, dado el tipo de datos, el alcance del tratamiento, la situación específica y los propósitos involucrados, el responsable del tratamiento tomará medidas adecuadas para proteger los derechos y libertades de las personas. Tal disposición se debe analizar en concordancia con el Art. 35, numeral 2, literal a), que fija la obligatoriedad de efectuar una evaluación de impacto en los casos de elaboración de perfiles que sean utilizados posteriormente en la toma de decisiones, lo cual ocurre en una calificación de solvencia.

Teniendo como base legitimadora el tratamiento de datos fundado en el interés legítimo, el informe de la AEPD (2021) en mención habla de seis fases que debe cumplir un correcto proceso de gestión del riesgo, sobre todo en este escenario en que se efectuó un sopesamiento con los derechos y libertades del titular. Estas fases deben definir claramente

los fines, describir los tipos de tratamiento, evaluar el riesgo, anticipar posibles brechas de seguridad, aplicar controles, verificaciones y un régimen de reevaluación.

Ahora bien, dichos aspectos dentro de un tratamiento que emplea IA, de acuerdo con la AEPD (2020a), comprenden la evaluación del riesgo determinando su graduación, la evaluación de impacto de la privacidad de los datos, la transparencia, precisión, limitación, seguridad, el análisis de la proporcionalidad y necesidad del tratamiento, así como procesos de auditoría.

En estos casos de tratamientos que aplican nuevas tecnologías, se presentan riesgos acordes a los métodos empleados en el flujo de vida del dato personal; por ejemplo, dentro del análisis se requerirá categorizar riesgos que solo son posibles por el uso de determinada tecnología, como el caso de los sesgos en la programación de algoritmos destinados a decidir sobre las personas o a discriminarlas. También se deberán incluir los riesgos derivados y colaterales que pudieren producirse.

La AEPD (2020a) emite una recomendación bastante acertada al decir que, cuando el procesamiento automatizado implica la creación de perfiles y la toma de decisiones, es necesario identificar todas estas decisiones en las diferentes etapas del proceso, proporcionar detalles, analizar los parámetros operativos, como los márgenes de error, y evaluar minuciosamente sus efectos en las partes involucradas. Se considera que tal nivel de detalle conllevará la toma de medidas específicas y adecuadas, capaces de mitigar en gran medida el impacto y viabilizar el tratamiento.

2.3.1.2. Evaluación de impacto

En cuanto a la evaluación de impacto, hasta este momento se podría considerar que se podría obviar en caso de no existir un alto riesgo inherente o residual. No obstante, tal suposición quedó deslegitimada luego que la AEPD (2019) se pronuncie expresamente, dictaminando que ésta es un requisito para el *Score* TELCO por las particularidades que lo revisten.

El Operador TELCO, en su rol de responsable del tratamiento, deberá efectuar, previo al inicio del tratamiento, un estudio de la necesidad del tratamiento y su proporcionalidad en comparación con los fines perseguidos. Para ello, a más de asesorarse por el delegado de Protección de Datos, puede consultar la opinión de los interesados, minimizando las posibles objeciones que pudieren surgir en lo posterior. También se recomienda contar con un código

de conducta y con certificaciones oficiales. El resultado de la evaluación de impacto deberá traducirse en una reforma al tratamiento de los datos.

Finalmente, se debe tomar en consideración la aplicación de una consulta previa si existiere alguna duda remanente sobre los pormenores del tratamiento. Este proceso pudiere ser complejo, pero se justifica por ser un tratamiento permanente y de gran escala. Por el procesamiento de datos blandos, deberá sumarse a esto una evaluación de impacto algorítmica.

La evaluación de impacto en el *Score* TELCO se ve afectada directamente por el informe de la AEPD (2020a) denominado Adecuación del reglamento de tratamientos que incorporan inteligencia artificial, el cual inicia aclarando que para estas situaciones corresponde efectuar pruebas basadas en el riesgo (*RBT* por sus siglas en inglés). Concluido ese proceso, se evalúa el riesgo residual y se ejercen actividades de control.

Se recomienda que el Operador TELCO busque un punto medio que le permita cumplir con la transparencia requerida mientras procura salvaguardar sus derechos de propiedad intelectual e industrial, siendo una buena opción la obtención de certificaciones como la norma ISO/IEC 27001 o la Certificación europea *GDPR* (*General Data Protection Regulation*) por las cuales puede disminuir la cantidad de detalles que pudieren revelar los secretos empresariales que hacen posible el funcionamiento del producto.

En este contexto se vuelve imperioso contar con un delegado de Protección de Datos. Esta afirmación que parece obvia, no lo es tanto, ya que en Ecuador no es un requisito para el Operador TELCO contar con un delegado; inclusive, no requiere contar con un Oficial de Cumplimiento ni con un responsable de seguridad. Afortunadamente, las buenas prácticas hacen que las empresas de telecomunicaciones se adelanten a estos requerimientos.

Este particular podría cambiar por la publicación del RGLOPDP /2023, puesto que en su artículo 53 describe un escenario de obligatoriedad de designar un delegado muy similar al que se presenta en el tratamiento de datos en el *Score* TELCO, por lo que se espera que la Superintendencia se pronuncie expresamente a través de una resolución.

Adicionalmente, existen amenazas y medidas de seguridad que deben formar parte de la gestión del riesgo específicamente en el tratamiento de datos personales que usan *IA*. Producto de ello, en el Código de Buenas Prácticas en Proyectos de *Big data* de la AEPDP

(2017), se recomienda implementar 1) prácticas de privacidad como anonimización, cifrado, gestión de accesos y rastreabilidad; 2) técnicas, como responsabilidad proactiva, transparencia, consentimiento, supervisión y control; y, 3) acciones para fortalecer la confianza, como el desarrollo de códigos de conducta, mecanismos de certificación, y sellos y etiquetas de protección de datos.

Habiendo visto el desglose exhaustivo de una gestión del riesgo de acuerdo con la normativa española, se procederá a comparar los requisitos que la legislación ecuatoriana impone para cumplir la misma tarea. Así, en la LOPDP /2021, en su artículo 40, se encuentra un esbozo de los parámetros para efectuar una gestión del riesgo; se trata de las particularidades del tratamiento, las características de los involucrados, las categorías de datos y su volumen.

Dicha norma debe aplicarse en concordancia con el artículo 10, literal k) *Ibidem*, en el que se incluye el principio de responsabilidad proactiva por el cual el Operador TELCO debería emplear estándares, mejores prácticas, esquemas de autorregulación y corregulación, códigos de protección, sistemas de certificación, sellos de protección de datos personales, o cualquier otro enfoque apropiado para la mitigación del riesgo.

Adicionalmente, la gestión del riesgo conlleva la rendición de cuentas al Usuario TELCO y a la Superintendencia de Protección de Datos Personales, cuando esta estuviere operativa. De igual manera, su matriz de riesgos deberá revisarse de forma periódica, puesto que la implementación de tecnología lleva implícito el carácter evolutivo del procesamiento de los datos. Asimismo, se debe aplicar este artículo en conjunto con el Art. 39 que habla de la protección de datos desde el diseño y por defecto, que, en breves rasgos, comparte las nociones de la legislación española.

Por último, la norma ecuatoriana en su artículo 42, literal a), habla de la evaluación de impacto, declarándola obligatoria para el caso de un análisis detallado y sistemático de datos personales, realizado a través de procesos automatizados como la creación de perfiles, y que resulta en decisiones con consecuencias legales para el titular.

Por tanto, para esta jurisdicción la evaluación sí será indispensable para la viabilidad del *Score* TELCO, puesto que da una definición lo suficientemente amplia que se puede encasillar en este producto, es decir, la elaboración de un perfil del Usuario TELCO producto de un

algoritmo y que dará como resultado del análisis de sus datos personales, una calificación sobre su posible capacidad de endeudamiento y predisposición de pago.

Debido a la publicación del RGLOPDP /2023, en Ecuador se han emitido los lineamientos superficiales que deberá cumplir la evaluación de impacto, contenidos en el artículo 32 *ibidem*, correspondiendo a la descripción del tratamiento, finalidades, necesidad, proporcionalidad, evaluación del riesgo e implementación de medidas. Ello no brinda más información, siendo más exhaustivo el análisis requerido para justificar la causal de legitimación del tratamiento.

Es posible inferir que en ambos países se requiere de un análisis de riesgo para efectuar el tratamiento de datos que devenga en la elaboración de perfiles sobre los cuales se vayan a tomar decisiones que generen un impacto en el titular de los datos. No obstante, en España se requiere de una gestión del riesgo adaptada específicamente a tratamientos en los que se procesa *big data* y se aplique inteligencia artificial, requiriendo inclusive una evaluación de impacto algorítmica y la aplicación de un código de buenas prácticas, mientras que, en Ecuador, este análisis solo implicaría el cumplimiento de las obligaciones legales del responsable del tratamiento. Por tanto, conviene la aplicación de los avances españoles para que el tratamiento se adecue a las particularidades tecnológicas del *Score* TELCO.

2.3.2. Relaciones contractuales en el flujo del tratamiento

En el ciclo de vida del dato personal a través del flujo del tratamiento se cuenta con diversas fases o macroprocesos, las cuales se habían determinado en un sentido estricto como recolección, almacenamiento, procesamiento, consulta y eliminación. Sin embargo, para este apartado, se procederá a puntualizar los aspectos críticos que deben contener los documentos que rigen las relaciones contractuales que surgen en cada fase, para lo cual se tomará como referencia el informe de la AEPD (2020a) denominado Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial.

2.3.2.1. Contrato con el encargado

Si bien, en todo el flujo del tratamiento, que a su vez constituyen tratamientos en sí mismos, pueden darse diversas interacciones contractuales con terceros por la magnitud de la data que se traducirá en el *Score* TELCO, se verá que existe una tabla explicativa que proporciona la AEPD (2020a) y da mayor visibilidad de la participación del rol del encargado en el

macroproceso de "procesamiento" de datos, en las etapas de desarrollo, entrenamiento, despliegue, inferencia/perfilado, decisión y evolución. Estos tratamientos, si fueren delegados por parte del Operador TELCO a un tercero, sea o no parte de su grupo empresarial o aliado estratégico, consistirá en un encargo y, en consecuencia, estará sujeto a un contrato de acceso a datos por terceros.

Dichos contratos deberán contar con medidas de seguridad de nivel básico y medio, tal como lo dictamina el Reglamento 1720/2008, artículo 81.2, literal f), ya que este es un producto que se encuadra como una especie de fichero que incluye datos que definen las características o la personalidad de los ciudadanos y que posibilita la evaluación de aspectos específicos de su identidad o comportamiento.

Asimismo, el contrato del encargado debe contemplar la obligación de elaborar un documento de seguridad que, de acuerdo con Reglamento 1720/2008, contenga responsabilidades y deberes del personal, registro de incidentes, restricción de acceso, manejo de documentos y archivos, verificación de identidad y autenticación, así como copias de seguridad y recuperación. Adicionalmente, debe contar con un responsable de seguridad y efectuar auditorías bienales. Por el uso de inteligencia artificial a estas obligaciones se le agregan el registro de los accesos y aplicación de cifrado en las etapas en que fuere posible.

En el caso particular de España, el Operador TELCO deberá agregar una cláusula por la cual el encargado declare que el tratamiento será efectuado en dicho país o dentro de la Unión Europea y, en el supuesto de que fuere estrictamente necesario contar con proveedores de otras jurisdicciones, se deberán implementar las medidas propias de una transferencia internacional de datos personales del Usuario TELCO.

Una obligación imprescindible es el control de los usuarios que, de parte del encargado, efectuarán el tratamiento y, en consecuencia, tendrán acceso a los datos personales. Dicho control a nivel contractual se respaldará mediante la obtención por parte del encargado de la suscripción de un acuerdo de confidencialidad y de un documento que contemple todas las disposiciones que rijan el contrato de acceso a datos por terceros, delimitando el alcance de sus atribuciones y fijando responsabilidades.

En Ecuador, en la LOPDP /2021 solo se verán lineamientos para las medidas de seguridad aplicables al responsable del tratamiento y, al ser las mismas exigibles al encargado de

acuerdo con lo indicado en el artículo 47 de este cuerpo normativo, las medidas que deben replicarse en los contratos de encargo deben considerar las tipologías y la cantidad de datos personales, el estado actual de la técnica, medidas eficaces de seguridad, y los costos asociados. También es necesario identificar la posibilidad de riesgos, efectuar un proceso de revisión continua, demostrar la efectividad de las medidas y reducir el impacto de los riesgos identificados.

El artículo *ibidem* recomienda (es facultativo) tomar medidas de anonimización, seudonomización, cifrado; medidas para preservar los datos en caso de incidentes; medidas de fortalecimiento a infraestructuras físicas, técnicas, a la estructura administrativa y regulación jurídica relacionados con los datos personales tratados; e incita a la aplicación de estándares internacionales, sistemas de seguridad de la información y códigos de conducta avalados por una autoridad competente en protección de datos.

Esto debe aplicarse en concordancia con el artículo 41, en el cual se manifiesta que las medidas deben responder al resultado del análisis de riesgo (equivalente a la evaluación de impacto), la tipología de los datos, las características del responsable y el titular, y los antecedentes de afectaciones negativas en el tratamiento de datos personales.

El artículo 35 del RGLOPDP /2023 agrega una particularidad a las obligaciones del Operador TELCO en Ecuador, siendo que la onerosidad de las medidas que deban ser aplicadas para garantizar un adecuado nivel de protección no será motivo de justificación para su incumplimiento o laxitud. Por tanto, el Operador que deseare implementar el producto *Score* TELCO, deberá contemplar un presupuesto suficiente para cubrir aspectos relacionados con datos personales y deberá limitarse a licitar con proveedores cuya capacidad financiera les permita acatar dichos estándares.

2.3.2.2. Contrato con el titular

La relación contractual con el titular / Usuario TELCO, estará enmarcada en el contrato de adhesión debidamente aprobado por el Ente Regulador de las Telecomunicaciones y la legislación específica en esta materia; y, si el usuario corresponde al segmento prepago, su relación contractual estará sujeta a los términos y condiciones, política de privacidad y aviso legal que son informados al titular de los datos y a los que se adscribe al momento de contratar los servicios con el Operador TELCO. En consecuencia, las cláusulas que le son aplicables se

encuentran en la legislación de telecomunicaciones, defensa al consumidor y protección de datos personales, además de todas aquellas resoluciones que vayan emitiendo los entes reguladores.

2.3.2.3. Contrato con el destinatario

El Operador TELCO debe suscribir con el Destinatario de los datos (*retail*/institución privada) un contrato de cesión de datos personales por la prestación del servicio de consulta al *Score* TELCO. El *retail*, a su vez, luego de recibir estos datos, se torna responsable del tratamiento de los datos cedidos para el cumplimiento de sus propios fines. Producto de esta cesión, el *retail* puede consultar los datos tratados, imprimirlos, almacenarlos, elaborar sus propios análisis; en fin, efectúa diversos tratamientos que debe legitimar con el Usuario TELCO, sin perjuicio de lo cual se reitera que para el *Score* TELCO requerirá del consentimiento del titular de los datos, al ser un requisito para la data obtenida del uso del servicio de telecomunicaciones.

En el contrato de cesión se recomienda sumar medidas de responsabilidad proactiva, lo cual se puede observar en un claro ejemplo de un *scoring* que se emplea en España para el sector inmobiliario, en el cual incorporan la obligación del destinatario de obtener el consentimiento del titular en una forma que permite trazabilidad y remisión al responsable del tratamiento en línea para acceder a la plataforma.

El futuro arrendatario recibirá un correo electrónico con un archivo, llamado declaración informada, que le avisa sobre la consulta en *bureau*. El solicitante tiene la opción de firmar electrónicamente la declaración desde su teléfono o computadora, garantizando un proceso simple y legal (IDEALISTA 2023). Esta metodología garantiza al responsable del tratamiento el cumplimiento de la obligación legal contemplada en el Real Decreto 1720/2007, artículo 10, al ser consultas individuales controladas.

Adicionalmente, en el contrato se debe especificar los datos que son cedidos, los cuales deberán constar en un registro de actividad de tratamiento. También se deberá contemplar en dicha cláusula la finalidad específica para la cual se está efectuando la cesión, siendo esta la única legitimada e informada al titular de los datos a través de los mecanismos que establece la normativa en protección de datos.

2.3.2.4. Contratos con bases de datos

En el *Score* TELCO no se utilizan datos obtenidos de terceros, ya que toda la información ha sido proporcionada o generada por el Usuario TELCO. No obstante, si llegase a ser el caso en que el Operador TELCO decidiera emplear información de terceros, por ejemplo, de otra empresa del grupo, debería suscribir un contrato de corresponsabilidad del tratamiento; mismo que, de acuerdo con el artículo 37 del RGLOPDP /2023 de Ecuador, se caracterizaría por un régimen de responsabilidad solidaria frente al titular y a la Superintendencia.

2.3.2.5. Contrato con colaboradores

Por último, los colaboradores del Operador TELCO que se dediquen a ejecutar las facultades del responsable del tratamiento deberán firmar un acuerdo de confidencialidad, código de conducta, código de ética y política de privacidad que lo pongan en pleno conocimiento del alcance de sus funciones dentro del flujo del tratamiento. Igualmente, el colaborador estará sujeto a las obligaciones y sanciones contempladas en el reglamento interno de trabajo.

En Ecuador se notará que la cesión de datos es denominada una transferencia. En este sentido, la relación con el encargado de protección de datos se mantiene, tomando la definición simple de "contrato de encargo del tratamiento". La relación con el titular sigue siendo a través del contrato de adhesión y/o política de privacidad de acuerdo con el segmento al que pertenezca el Usuario TELCO. La relación con el destinatario se regirá por un contrato de transferencia de datos. Finalmente, la relación con los colaboradores del Operador TELCO seguirá las mismas directrices de confidencialidad y de normativa corporativa y laboral.

En conclusión, en ambas jurisdicciones las relaciones contractuales se sintetizan en 1) el contrato de acceso a datos por terceros a efectos del encargo del tratamiento; 2) el contrato de adhesión y política de privacidad para el Usuario TELCO en su calidad de titular; 3) el contrato de cesión / transferencia de datos para la relación con el destinatario de los datos, sea *retail* o institución privada; 4) el contrato de corresponsabilidad si hubiere el uso de una base de datos proveniente de terceros; y, 4) los contratos de confidencialidad con los colaboradores del Operador TELCO que vayan a intervenir activamente en el tratamiento de datos para el *Score* TELCO.

2.3.3. La política de privacidad del Operador TELCO

En el *Score* TELCO la política de privacidad y el ejercicio de los derechos ARCO adquieren un rol protagónico, puesto que la mayoría de los usuarios TELCO que van a alimentar la base de datos a ser procesada van a estar relacionados contractualmente con el Operador TELCO mediante un contrato de prestación de servicios no suscrito, y, en materia de datos personales, específicamente con la política de privacidad.

Es importante enfatizar que la política de privacidad se encuentra íntimamente ligada al derecho a la información del Usuario TELCO en su calidad de titular, pues, es en este documento en el que tendrá claridad sobre el alcance del tratamiento al que estaría sujeto en caso de decidir adquirir los servicios del Operador.

De acuerdo con la AEPDP (2023), una política de privacidad correctamente elaborada estará compuesta de dos capas, brindando un mayor nivel de profundidad. En Ecuador, la política de privacidad no exige doble capa; sin embargo, se entiende que deberá incorporar todas aquellas obligaciones de informar contenidas en la LOPDP /2021.

Para mejor entendimiento, se ha procedido a comparar el contenido de las políticas de privacidad de dos compañías con sede en España y Ecuador, cuya fusión de objetos daría lugar al *Score* TELCO*:* Equifax y Telefónica. De la revisión del contenido de ambas políticas, resulta interesante la forma en que la misma compañía la comunica en sus diferentes jurisdicciones, de manera que se observa el uso de un lenguaje asertivo y concreto sobre cada aspecto que compone la política en la filial española; en cambio, la filial ecuatoriana emplea un lenguaje de compromiso genérico inspirados en el código de conducta, sin respuestas concretas para cada aspecto de la política.

Equifax desarrolla su política de privacidad únicamente sobre el acceso al fichero de morosidad por cuanto él desarrolla, gestiona y mantiene la plataforma. No es el acreedor del usuario, es un tercero; y, por tanto, su política se limita a ese tratamiento específico. En este sentido, la política de privacidad está dirigida al destinatario de los datos que, generalmente, no es el titular.

En cambio, en el *Score* TELCO, el Operador es quien centraliza el tratamiento, salvo que requiera de un tercero para el desarrollo, implementación o mantenimiento de la plataforma. Siendo el Operador TELCO quien proporciona los datos recabados directamente de sus

usuarios y quien presta el servicio de *scoring*, su política de privacidad deberá ser más extensiva, abarcando todo el flujo del tratamiento en los diversos servicios que le presta al Usuario TELCO en calidad de cliente y titular de los datos. Esta política puede materializarse en un contrato de transferencia o cesión si el destinatario fuere plenamente identificable o, si se trata de una plataforma de acceso individual con alcance masivo, se optaría por una política de privacidad como la que emplea Equifax.

En cuanto a la empresa Telefónica, se logra identificar que ambas filiales clasifican los fines del tratamiento de acuerdo con la base legitimadora. De esta particularidad surge una novedad que se considera tiene su razón de ser por el aparataje societario que distingue a ambas organizaciones. Estando Movistar España directamente vinculado al Grupo Telefónica, de la misma jurisdicción, se puede notar que el tratamiento se diversifica entre los miembros de dicho grupo. En cambio, en Movistar Ecuador, se cuenta con una sola razón social en el mismo Estado y es esta en la que se concentra el tratamiento.

Ahondando en los fines legitimados por la causal de interés legítimo, en Movistar Ecuador se encuentra que los ficheros y posible analítica fijan como destinatario al mismo titular de los datos. Sin embargo, la redacción da a entender que se usará para fines de mercadotecnia -aunque también puede interpretarse como que la mercadotecnia a favor de terceros es uno de los fines, ya que no está totalmente claro-. Ello no implica que la compañía evite su uso para el sector comercial corporativo, sino que debe interpretarse en el sentido de que aplican técnicas de anonimización para que no se encuentre sujeto a protección de datos personales.

En el caso de Movistar España, existe una política de privacidad robusta, aunque un poco confusa, que lleva a navegar por las políticas de las diferentes empresas que conforman el Grupo Telefónica para tener una visión completa del tratamiento de datos personales. Ello responde a que diversas empresas del grupo efectúan distintos tratamientos con base en la misma data, la cual complementan entre sí.

En este orden, se identifica que en el tratamiento por interés legítimo declarado no se menciona explícitamente la elaboración de “perfiles” ni “ficheros” o su cesión a terceros, salvo la comunicación a otras empresas del grupo telefónica, a saber: Telefónica *Iot* & *Big data Tech*, S.A.U., y es a través de esta compañía que efectúan el *scoring* (*Score* TELCO) bajo un régimen de corresponsabilidad, cediendo los datos Telefónica y estos, a su filial Telefónica *Tech.*

Nótese que el término empleado por Movistar Ecuador para el procesamiento algorítmico de los datos del titular es el de analítica prescriptiva; misma que, de acuerdo con el doctrinario Sebastián Maldonado (2021), evalúa de manera efectiva distintos resultados y situaciones, con el objetivo de tomar la decisión más acertada; además, cuenta con la capacidad de calcular la probabilidad asociada a estas situaciones, permitiendo una evaluación precisa del nivel de riesgo. Para los fines pertinentes, es el tipo de análisis que se usa en el *Score* TELCO, debido a que permite determinar la capacidad de endeudamiento y predisposición de pago del Usuario TELCO.

Un aspecto que forma parte de la legislación española y que se ha introducido en Ecuador con la LOPDP /2021 en su artículo 58, numeral 3, es la obligación de comunicar los casos de transferencia internacional cuando se apliquen normas corporativas vinculantes, que deberán contener una descripción detallada de las compañías subsidiarias que, junto con el responsable del tratamiento, forman parte del mismo grupo empresarial. También, proporcionar información sobre la estructura y los datos de contacto del grupo y de cada miembro. En el caso de Movistar Ecuador no se observa dicho desglose, lo cual estaría justificado por no existir a la fecha una Autoridad en funciones a la cual remitir las normas.

En Ecuador, la política de privacidad no requiere que se incluya la lógica utilizada al elaborar el perfilamiento, las normas corporativas ni las categorías de datos cuando estos no son obtenidos del abonado. Por ello, se puede determinar que el avance en la legislación tiene un impacto directo en el grado de transparencia que reviste la información que recibe el Usuario TELCO.

Es así como se recomienda replicar en Ecuador la política de doble capa que coadyuvará a que mayor cantidad de usuarios revisen los aspectos esenciales del tratamiento. Asimismo, se recomienda reforzar el contenido de esta política, incluyendo aquellos aspectos que la legislación ecuatoriana deja de lado, pero que la legislación española incluye con gran acierto.

2.3.4. Ejercicio de los derechos ARCO

Como último aspecto a analizar, se analizará el ejercicio de los derechos de protección de datos personales que asisten al titular de los datos (Usuario TELCO). Para el ámbito español, la guía serán las Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento (UE) 679/2016, emitidas por el Grupo de Trabajo Sobre

Protección de Datos del artículo 29 (GT29) (Direct. GT29, de 3 de octubre de 2017), que desglosan la aplicación de estos derechos en el ámbito que atañe al *Score* TELCO; y, de parte de Ecuador, se empleará la LOPDP /2021 y el RGLOPDP /2023.

Acceso

En el derecho de acceso, al igual que en los derechos subsiguientes, no se efectuará un análisis de su definición, ya que en ambas legislaciones el nombre del derecho corresponde a su sentido natural y obvio (por ejemplo, acceso: acceder); en cambio, se abarcarán las particularidades que se pueden presentar en cada uno considerando la finalidad del tratamiento.

Es así como la Direct. GT29, de 3 de octubre de 2017 ofrece una recomendación totalmente válida para el *Score* TELCO, indicando que el Operador podría considerar la puesta en producción de un sistema que habilite a los titulares la verificación de su perfil, ofreciendo información detallada sobre los datos y las fuentes utilizadas en su elaboración.

Ello se puede complementar con el artículo 12 del RGLOPDP /2023 de Ecuador, en el cual fomentan el uso de canales informáticos simplificados; de manera que el Usuario TELCO se vería correctamente protegido en este derecho con un perfil digital intuitivo en la página *web* o *app* del Operador.

Rectificación

Para el derecho de rectificación, la Direct. GT29, de 3 de octubre de 2017, habla de una configuración avanzada del perfil propuesto, de manera que exista una funcionalidad en línea para que el titular gestione su panel de privacidad y que se aplique tanto los datos personales utilizados para crear el perfil (datos de entrada) como la información resultante, ya sea el perfil en sí o la puntuación asignada a la persona (datos de salida).

En Ecuador, ni en la LOPDP /2021 ni en el RGLOPDP /2023, se hace mayor énfasis a este derecho. No obstante, se aclara que debe ser ejercido ante el Operador en su calidad de responsable y que, por analogía al tratamiento de datos crediticios, si hubiese que generarse una consulta sobre el usuario requirente mientras se gestiona la admisibilidad de su derecho, el reporte deberá incluir una leyenda manifestando que los datos están siendo objeto de revisión.

Oposición

Con respecto al derecho de oposición, la Direct. GT29, de 3 de octubre de 2017 determina que este derecho debe mostrarse visiblemente en el sitio web del responsable. Este aporte goza de novedad con respecto a la normativa ecuatoriana.

También efectúan una puntualización que coincide con la LOPDP /2021 de Ecuador, artículo 16, por la que, en caso del ejercicio de este derecho, se deberá efectuar una segunda ponderación considerando la causal invocada por el titular; asimismo, aclara que el Operador TELCO deberá demostrar los motivos imperiosos -al no determinarse el alcance de la palabra imperioso, se procede a verificar el Diccionario de la Real Academia Española (2023), quien lo califica como indispensable, inmediato, imperativo -o la necesidad de continuar el tratamiento para fines procesales, razones por las cuales no habría lugar a la oposición, aunque podría caber una limitación.

Supresión o eliminación

El derecho a la supresión también cuenta con causales taxativas para su ejercicio por parte del titular. La LOPDP /2021 de Ecuador, en su artículo 15, indica que solo procederá cuando el tratamiento infrinja la Ley; cuando no sea necesario; se haya cumplido la finalidad o vencido el plazo; exista una afectación a los derechos y libertades del titular; se revoque el consentimiento; o, exista obligación legal.

Por revocación del consentimiento podría ser, por ejemplo, una supresión del resultado del *scoring* para el tratamiento de consulta que hace el destinatario, si esta no fuere ejecutada en línea. No se perciben diferencias para el ejercicio de este derecho.

Portabilidad

El derecho a la portabilidad sí goza particular atención, ya que tanto la Direct. GT29, de 3 de octubre de 2017 como la LOPDP /2021 de Ecuador en su artículo 17 coinciden en que se pueden portar los datos de entrada, pero no los datos de salida, aduciendo que es un derecho no aplicable cuando los datos han sido procesados para su adaptación individualizada, sugerencia, clasificación o elaboración de perfiles; en consecuencia, el resultado del *scoring* no es objeto de portabilidad.

Limitación o suspensión

Con respecto al derecho a la limitación, la Direct. GT29, de 3 de octubre de 2017 aclara que esta puede efectuarse en los casos de suspensión cautelar del tratamiento para resolver una reclamación del titular, cuando el interesado pida específicamente la limitación porque solo está de acuerdo con ciertos fines, o cuando se requiera su conservación para la defensa administrativa o procesal. A nivel de Ecuador, se comparten los lineamientos.

Información

El derecho a la información comprenderá el desglose de los ítems vistos en el apartado de la política de privacidad, con el énfasis determinado en la Direct. GT29, de 3 de octubre de 2017 con respecto a que es necesario comunicar al usuario que sus datos serán empleados tanto para crear perfiles como para tomar decisiones basadas en este, y, por parte de la LOPDP /2021, artículo 12, numeral 10), deben informarse las transferencias de datos, con la diferencia de que en Ecuador se refieren a mencionar los destinatarios de forma genérica, sin pedir datos de contacto como en el caso español.

No ser objeto de decisiones automatizadas

Con el derecho a no ser objeto de decisiones automatizadas, España tiene una diferencia notoria que recae en las decisiones tomadas totalmente de forma automatizada, lo cual estaría mayormente del lado del destinatario de los datos, ya que el Operador TELCO efectúa un análisis algorítmico que generará una calificación, la cual en sí misma no produce ningún efecto. Sin embargo, como medida de seguridad proactiva, puede incluir en su contrato de cesión de datos una cláusula por la cual se reitere que el *scoring* es un elemento a ser considerado por el destinatario, mas no constituye una respuesta en sí misma.

Para garantizarlo, se recomienda que la cláusula incluya el pronunciamiento de la Direct. GT29, de 3 de octubre de 2017, la cual indica que se debe garantizar el derecho a la intervención humana, expresar su opinión, recibir una explicación de la decisión que se ha tomado después de la evaluación, y el derecho recurrir la decisión. Si hay decisiones automatizadas con efectos legales, durante la evaluación de impacto, el responsable debe detectar y registrar el grado de participación humana en la toma de decisiones; así como dejar constancia del momento en que se suscita dicha participación.

Sin perjuicio de la utilidad de tal pronunciamiento, y haciendo énfasis en el equilibrio que debe generarse entre el Operador y el titular, la LOPDP /2021 de Ecuador, en su artículo 20, aunque incrementan el alcance de este derecho a las decisiones basadas parcialmente en valoraciones automatizadas, también eximen al responsable de aplicar este derecho si hubiere un mandato motivado de la Autoridad en Datos Personales o si no hubiere un impacto grave para el titular.

Es decir que, en Ecuador, por medio de una opinión consultiva y una gestión integral del riesgo con evaluación de impacto, se lograría viabilizar el producto si llegase a ser el caso de suscitarse este tipo de decisiones, evitando una observación cuando el servicio se encuentre en etapa de producción.

Nótese que las medidas propuestas por la Direct. GT29, de 3 de octubre de 2017, referentes un portal autogestionado por el titular, pueden fortalecer la legitimación del tratamiento al disminuir la posible afectación a derechos y libertades. Sin embargo, deben emplearse con debidas precauciones comerciales para que exista un equilibrio entre la protección del titular y la ventaja competitiva del producto que requiere datos verificados, actualizados y completos, cuyo procesamiento emita una calificación fidedigna que sea de utilidad para el Usuario TELCO frente al *retail*.

Dar autonomía total en el perfil podría afectar la calidad del dato, por ello, se considera que se puede optar por un perfil de funcionalidades limitadas y que posea una interfaz sencilla e intuitiva que muestre solo información relevante como para que el titular determine la necesidad o no de activar el ejercicio de sus derechos Arco cuando lo considere necesario.

En cuanto a una diferencia general pero trascendente en la forma de ejercitar los derechos ARCO, se destaca que el tiempo de respuesta en Ecuador se reduce a la mitad -quince días-, dificultando dar contestación oportuna a aquellos casos que requieran de un análisis pormenorizado, considerando la complejidad que puede revestir el *Score* TELCO al ser un servicio que utiliza *big data* y mecanismos de inteligencia artificial en el procesamiento de datos.

De lo expuesto se puede extraer que existe gran similitud entre los requisitos de la normativa ecuatoriana y la española y se evidencia que la mayor diferencia en este apartado se encuentra en el alcance de las acciones que debe ejecutar el Operador, prevaleciendo el caso español por el vasto desarrollo que ha efectuado la AEPD.

Es así como, para que la protección al titular sea superior en territorio ecuatoriano, se pueden replicar las recomendaciones españolas en cuanto al ejercicio de los derechos a través de un perfil digital intuitivo, de autogestión limitada, que permita el ejercicio de derechos ARCO con rapidez y trazabilidad.

De igual modo, sería de utilidad replicar la figura de la opinión consultiva para garantizar que las medidas de seguridad aplicadas cuenten con el respaldo de la SPDP, reduciendo el riesgo de efectividad del *Score* TELCO ante el ejercicio del derecho a la suspensión del tratamiento en la toma de decisiones parcialmente automatizadas.

3. Conclusiones

Se procede a presentar las conclusiones del estudio exhaustivo sobre la protección de datos personales en relación con el producto *Score* TELCO, desde la perspectiva del Operador. En este análisis, se ha llevado a cabo una comparativa detallada entre la legislación española y ecuatoriana, identificando aquellas figuras jurídicas y buenas prácticas implementadas en España que pueden ser replicadas en Ecuador.

Primera.- La plataforma *Score* TELCO es una herramienta que proporciona evaluaciones crediticias, ofreciendo soluciones de inteligencia financiera para calificación crediticia alternativa. Se basa en el análisis de grandes volúmenes de datos de telecomunicaciones para estimar la disposición y capacidad de un individuo para cumplir con servicios crediticios, como préstamos. No se trata de una calificación crediticia convencional, lo que significa que el Operador no está obligado a actuar como un agente calificador acreditado.

Segunda.- En el modelo de negocio de *Score* TELCO, participan los siguientes actores: a) El usuario del servicio de telecomunicaciones, que actúa como titular de los datos personales sujetos a tratamiento; b) El Operador, que asume el papel de responsable del tratamiento; c) El *Bureau* Crediticio, de acuerdo con la legislación del país donde se presta el servicio, desempeñando el papel de corresponsable; y, d) La entidad o empresa que ofrece el crédito o financiamiento directo (*retail*), desempeñando la función de destinatario del *scoring*. En algunos casos, también puede estar presente el desarrollador, actuando como encargado del tratamiento.

Tercera.- En el marco normativo del Score TELCO, Ecuador y España comparten similitudes y diferencias. Ambos países cuentan con un modelo de Estado constitucional y un sistema jurídico que otorga primacía a la Ley. Existe una presunción de interés legítimo para el tratamiento de datos crediticios en ambas jurisdicciones; sin embargo, se requiere una ponderación debido a la integración con otras tipologías de datos. En Ecuador, la cesión de datos se denomina transferencia. Recientemente, se ha introducido la figura de la corresponsabilidad en Ecuador, aplicable cuando interviene un *Bureau*. En relación con la autoridad en protección de datos, España cuenta con una Agencia, mientras que Ecuador tiene una Superintendencia que aún no se ha posesionado, marcando diferencias en el nivel de independencia política.

Cuarta- Para la legitimación del tratamiento se requerirá un interés legítimo. En España, el Operador TELCO requerirá un interés real, actual, específico, lícito y sopesado frente a los derechos del interesado, lo que fundamentaría su tutela por parte del Derecho. En Ecuador, significa la inclinación del ánimo del responsable del tratamiento hacia los datos personales del titular y su deseo de conseguirlo con base en una justificación legal. La diferencia reside en el grado de especificidad requerido y el alcance del sopesamiento.

Quinta.- Una vez identificado el interés legítimo, se requiere de una prueba que permita contraponerlo con los derechos del interesado. En España es el *test* de sopesamiento que está conformado por las siguientes categorías: 1) la evaluación del interés legítimo del responsable del tratamiento; 2) el impacto sobre los interesados; 3) el equilibrio provisional; y, 4) las garantías adicionales. En Ecuador, este mismo análisis toma el nombre de *test* de ponderación. A falta de desarrollo por la SPDP, se recomienda replicar en Ecuador la incorporación al *test* del principio de responsabilidad y transparencia, el derecho de oposición y de exclusión voluntaria fijados en el Dict. GT29, de 9 de abril de 2014.

Sexta.- La tipología de datos a ser tratados, denominados datos TELCO, se clasifican en datos de telecomunicaciones y datos de atención al cliente. Los primeros están conformados por datos de uso del servicio, datos de localización, datos de red y aplicaciones, datos generados por máquinas y datos de actividad en línea; en cambio, los segundos se encuentran constituidos por datos de identificación, datos de pedido y facturación y datos del dispositivo. Estos datos son obtenidos tanto del Usuario TELCO, como de su comportamiento de uso de los servicios de telecomunicaciones.

Séptima.- Desde el punto de vista jurídico, en el tratamiento de recolección de datos para el producto *Score* TELCO, se destaca la importancia de obtener el consentimiento claro y específico del Usuario TELCO para datos receptados a través de *CRM, IOT y Cookies*, conforme al Reglamento (UE) 2016/679. Se señala la alternativa de un plazo para que el usuario manifieste su negativa. En cuanto a los datos obtenidos mediante *DNS*, memoria Caché y *CDR*, se establece la base legal en el cumplimiento de obligaciones legales, permitiendo la recolección sin consentimiento en situaciones contractuales. Se destaca también la posibilidad de obviar el deber de informar de manera individual en ciertos casos, como en el segmento masivo prepago.

Octava.- El almacenamiento de datos para el *Score* TELCO se basa generalmente en la organización de información en ficheros, regulados por el Reglamento (UE) 2016/679, los cuales son esenciales para transformar datos brutos a estructurados. En cuanto a los métodos de almacenamiento, estos incluyen el uso de servidores propios, centros de datos privados, almacenamiento en la nube y sistemas distribuidos. Además, la normativa del RDL 1720/2007 impone restricciones al tratamiento de datos netamente crediticios y la Disposición Adicional Sexta de la Ley 3/2018 establece la exclusión de deudas inferiores a cincuenta euros, particular que no aplica en Ecuador; todo esto debe ser tomado en cuenta en el tratamiento de datos.

Novena.- En el tratamiento procesamiento de la *big data* generada por el Usuario TELCO, el Operador TELCO emplea metodologías de inteligencia artificial. La AEPDP identifica en esta fase los sub-tratamientos de desarrollo/entrenamiento, validación y despliegue/explotación. Para generar el *scoring*, se emplean algoritmos como análisis de regresión, series temporales, aprendizaje automático, análisis de clústeres, análisis de redes sociales y técnicas de minería de datos. En consecuencia, existen procesamientos simples o compuestos y su aplicación técnica es universal, no existiendo diferencias entre Ecuador y España.

Décima.- En el tratamiento consulta, el *Score* TELCO se caracteriza por ser un servicio prestado en línea. A menudo, este tipo de servicios son ofrecidos a través de servidores web o de interfaces de programación de aplicaciones. A efectos del *Score* TELCO, se recomienda emplear una API; ya que permite el uso de múltiples plataformas, soporta planes de escalabilidad y permite la implementación de mayores medidas de seguridad de la información y un control eficiente de los accesos.

Undécima.- En la eliminación de los datos, la Guía de Protección de Datos por Defecto destaca la aplicación del principio de minimización en el plazo de retención, admitiendo excepciones solo en caso de justificación objetiva. Tanto la legislación española como la ecuatoriana admiten la aplicación del boqueo o anonimización de datos. Se recomienda replicar la diligencia española en la destrucción de datos, lo cual se traduce en la ejecución de técnicas de borrado seguro de acuerdo con el tipo de soporte, como la sobreescritura o la celebración de contratos con proveedores, que contengan una política de copias de seguridad.

Duodécima.- En cuanto a las obligaciones del Operador, las consideraciones regulatorias señalan la importancia de la gestión del riesgo y la evaluación de impacto para el tratamiento de datos, en *Score* TELCO. Ambos países reconocen la importancia de gestionar los riesgos de

manera proactiva, considerando las particularidades del tratamiento, las partes involucradas y el volumen de datos personales. Para mejorar la efectividad de la legislación ecuatoriana, se recomienda adoptar aspectos específicos de la normativa española, como la aplicación de medidas técnicas y organizativas avanzadas y específicas a tratamientos que procesan *big data* usando inteligencia artificial, la evaluación de impacto algorítmica y la implementación de códigos de buenas prácticas.

Decimotercera.- En ambas jurisdicciones las relaciones contractuales se sintetizan en el contrato de acceso a datos por terceros a efectos del encargo del tratamiento; el contrato de adhesión y política de privacidad para el Usuario TELCO en su calidad de titular; el contrato de cesión / transferencia de datos para la relación con el destinatario de los datos; contrato de corresponsabilidad si hubiere el uso de una base de datos proveniente de terceros; y, contratos de confidencialidad con los colaboradores que vayan a intervenir activamente en el tratamiento. Se sugiere adoptar ciertos elementos de la legislación española, como la especificación detallada de medidas de seguridad en los contratos con encargados, la inclusión de cláusulas sobre la ubicación del tratamiento y la introducción de directrices sobre la corresponsabilidad en el caso de uso de bases de datos de terceros.

Decimocuarta.- Con respecto al alcance de la política de privacidad, conviene replicar en Ecuador la implementación de una política de doble capa, lo que facilitaría que un mayor número de usuarios revisen los elementos esenciales del tratamiento. Además, se recomienda fortalecer el contenido de dicha política, incorporando aquellos aspectos que la legislación ecuatoriana omite pero que la legislación española aborda de manera efectiva, como la inclusión de la lógica empleada en la elaboración del perfilamiento, las normas corporativas y las categorías de datos cuando no son obtenidos del abonado.

Decimoquinta.- Producto del análisis comparativo entre las normativas española y ecuatoriana, se destaca el avance de la normativa española en la doctrina sobre los derechos ARCO, especialmente en tratamientos de grandes volúmenes de datos. Se sugiere la adopción en Ecuador de figuras y prácticas recomendadas por el GT29 y la AEPDP, como la configuración avanzada de un perfil intuitivo de autogestión, la aplicación de la opinión consultiva para reducir riesgos y el replanteamiento del plazo de respuesta a 30 días, similar a la legislación española, para asegurar respuestas fundamentadas a todas las solicitudes.

Referencias bibliográficas

Bibliografía básica

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción*. Febrero de 2020a. Disponible en: https://www.aepd.es/documento/adecuacion-rgpd-ia.pdf. [Consultado el 25 de octubre 2023].

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Código de buenas prácticas en protección de datos para proyectos de big data.* Mayo de 2017. Disponible en: https://www.aepd.es/documento/guia-codigo-de-buenas-practicas-proyectos-de-big-data.pdf. [Consultado el 25 de octubre 2023].

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Derecho de información*. Última modificación 10 de noviembre de 2023. Disponible en: https://www.aepd.es/derechos-y-deberes/conoce-tus-derechos/derecho-de-informacion. [Consultado el 25 de octubre 2023].

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Gestión del riesgo y evaluación de impacto en tratamientos de datos personales*. Junio de 2021. Disponible en: https://www.aepd.es/documento/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf. [Consultado el 25 de octubre 2023].

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Guía de protección de datos por defecto.* Octubre de 2020b. Disponible en: https://www.aepd.es/documento/guia-proteccion-datos-por-defecto.pdf. [Consultado el 25 de octubre 2023].

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Listas de tipos de tratamientos de datos que requieren evaluación de impacto relativa a protección de datos (art 35.4)*. Mayo de 2019. Disponible en: https://www.aepd.es/documento/listas-dpia-es-35-4.pdf. [Consultado el 25 de octubre 2023].

AMAZINUM. *What is NLP and how it is Implemented in Our Lives.* ©2019-2023. Disponible en: https://amazinum.com/insights/what-is-nlp-and-how-it-is-implemented-in-our-lives/. [Consultado el 25 de octubre 2023].

AÑON ROIG, María José. Derechos fundamentales y Estado constitucional. *Cuadernos constitucionales de la cátedra Fadrique Furió Ceriol,* 2002, núm. 40, pp. 25-36.

CADLAN. *Nubes privadas: Ventajas y desventajas.* ©2020. Disponible en: https://www.cadlan.com/noticias/nubes-privadas/. [Consultado el 25 de octubre 2023].

CARREÑO BORDA, Yesica Paola. Backup y protección de datos. *Repositorio Universidad Libre* [en línea]. 2017. Disponible en: https://repository.unilibre.edu.co/bitstream/handle/10901/11200/MonografiaYesicaCarre%c3%b1o.pdf?sequence=1&isAllowed=y. [Consultado el 25 de octubre 2023].

CIFUENTES FERNANDEZ, Jorge. *Estudio del estado del arte de sistemas de almacenamiento distribuido ara el almacenamiento de datos de red.* Junio 2018. Trabajo de fin de grado para la obtención del grado en ingeniería informática por la Universidad autónoma de Madrid - Escuela politécnica superior. Disponible en: https://repositorio.uam.es/bitstream/handle/10486/688123/cifuentes_fernández_jorge_tfg.pdf?sequence=1&isAllowed=y. [Consultado el 25 de octubre 2023].

CLOUDFLARE. *¿Qué es DNS? | Cómo funciona*. ©2023. Disponible en: https://www.cloudflare.com/es-es/learning/dns/what-is-dns/. [Consultado el 25 de octubre 2023].

CONTRERAS VÁSQUEZ, Pablo y TRIGO KRAMCSÀK Pablo. Interés legítimo y tratamiento de datos personales: Antecedentes comparados y regulación en Chile. *Revista Chilena de Derecho y Tecnología,* 2019, vol. 8, núm. 1, pp. 69-106. Disponible en: https://www.scielo.cl/pdf/rchdt/v8n1/0719-2584-rchdt-8-1-00069.pdf. [Consultado el 25 de octubre 2023].

DIAZ OCAMPO, Eduardo y ANTÚNEZ SÁNCHEZ, Alcides. LAS FUENTES DEL DERECHO EN EL DERECHO DEL ECUADOR. *Revista jurídica directo & Paz*, 2017, 2do semestre, núm. 37, pp. 349-375. Disponible en: http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_informativo/bibli_inf_2006/6FC84302E6C2238BE050A8C0DD0104CB. [Consultado el 25 de octubre 2023].

ESTEVE LOPEZ, Elena María. *Modelo mixto de Credit Scoring construído con Análisis discriminante y el Algoritmo de Kohonen. Valoración de las componentes de riesgo según Basilea II.* Memoria para la obtención del grado de Doctor por la Universidad de Sevilla - Departamento de Economía aplicada III. Febrero 2005. Disponible en:

https://idus.us.es/bitstream/handle/11441/24067/Original_M_TD-0541.pdf?sequence=1&isAllowed=y. [Consultado el 25 de octubre 2023].

GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29. *Dictamen sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE*. (844/14/ES. WP 217). 9 de abril de 2014. Disponible en: https://www.aepd.es/documento/wp217_es_interes_legitimo.pdf. [Consultado el 25 de octubre 2023].

GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29. *Directriz del sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679* (17/ES WP251). 03 de octubre de 2017. Disponible en: https://www.aepd.es/sites/default/files/2019-12/wp251rev01-es.pdf. [Consultado el 25 de octubre 2023].

HILBCK RÍOS, Mauricio y BUENO TORRES Micaela. Data science y el scoring crediticio en el sistema financiero. *Revista ALIDE*, Julio-Septiembre 2022, pp. 25-28. Disponible en: https://www.alide.org.pe/wp-content/uploads/2022/11/Data-science-y-el-scoring.pdf. [Consultado el 25 de octubre 2023].

IBM. *¿Qué es un bosque aleatorio?*. Disponible en: https://www.ibm.com/es-es/topics/random-forest#:~:text=El%20algoritmo%20de%20bosque%20aleatorio%20es%20una%20ampliaci%C3%B3n%20del%20m%C3%A9todo,correlacionado%20de%20%C3%A1rboles%20de%20decisiones. [Consultado el 25 de octubre 2023].

KINSTA. *Cómo Borrar la Cache Para los Principales Navegadores*. Última actualización 8 de agosto de 2023. Disponible en: https://kinsta.com/es/base-de-conocimiento/como-borrar-la-cache-del-navegador/. [Consultado el 25 de octubre 2023].

KT GLOBAL BUSINESS GROUP. *Telecom big data monetization. Credit scoring solution based on telecom data. CRDP & K-TELCO Score™*. 2019. Disponible en: https://corp.kt.com/eng/attach/area/A000000561/C000003656v5.pdf [Consultado el 03 de noviembre de 2023].

LORENZO, José Antonio. *Conoce todo lo que tu operador de Internet puede recopilar sobre ti.* Última actualización 14 de noviembre de 2023. Disponible en:

https://www.redeszone.net/tutoriales/redes-cable/recopilacion-datos-operador-internet-navegacion/. [Consultado el 25 de octubre 2023].

MALDONADO, Sebastián. Prescriptive analytics: La última frontera de las capacidades analíticas. *Revista Contabilidad Y Sistemas*, segundo semestre 2021. Disponible en: https://www.contabilidadysistemas.cl/revistas/r20/R20-6.pdf. [Consultado el 25 de octubre de 2023] pp. 46-59.

MARTÍNEZ VILLASECA, Marisa. El interés legítimo como base legitimadora del tratamiento de datos de carácter personal. *Actualidad administrativa*, diciembre 2019, núm. 12, p. 10.

MOGROVEJO GAVILANES, Alejandro Raúl, et al. Aplicación del Principio de proporcionalidad en la Jurisprudencia de la Corte Constitucional del Ecuador. *Iustitia Socialis: Revista Arbitrada de Ciencias Jurídicas*, 2020, vol. 5, núm. 8, pp. 91-116. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=7408541. [Consultado el 25 de octubre 2023].

PIEDRAS, Ernesto. S*ervicios de valor agregado en los dispositivos móviles*. EL ECONOMISTA. 03 de noviembre de 2021, 03h28. Disponible en: https://www.eleconomista.com.mx/opinion/Servicios-de-valor-agregado-en-los-dispositivos-moviles-20111103-0009.html. [Consultado el 25 de octubre 2023].

PLANA ARNALDOS, María Carmen. El derecho fundamental a la protección de datos personales y los ficheros privados: el interés legítimo en el tratamiento de datos (The fundamental right of personal and private files protection: the legitimate interest in the data processing). *Comunitania Revista Internacional de Trabajo Social y Ciencias Sociales*, enero 2014, núm. 7, pp. 69-89. Disponible en: https://revistas.uned.es/index.php/comunitania/article/view/13007/12000. [Consultado el 25 de octubre 2023].

REAL ACADEMIA ESPAÑOLA y ASOCIACIÓN DE ACADEMIAS DE LA LENGUA ESPAÑOLA. *Diccionario panhispánico de dudas (DPD)*, 2a. edición (versión provisional) [en línea]. Disponible en https://www.rae.es/dpd/interés. [Consultado el 25 de octubre 2023].

REAL ACADEMIA ESPAÑOLA. Diccionario de la lengua española [en línea]. Versión 23.6. Disponible en: https://dle.rae.es. [Consultado el 25 de octubre 2023].

RECHE, José Manuel. SQL, NoSQL, NewSQL. Qué son, historia y elección. *IThink UPC.* 22 de junio de 2016. Disponible en: https://www.ithinkupc.com/es/blog/sql-nosql-newsql-que-son-historia-y-eleccion. [Consultado el 25 de octubre 2023].

REINO DE ESPAÑA. Sistemas de Justicia nacionales - España - Organización de la Justicia. Sistemas judiciales - Administración de Justicia. [En linea]. Última actualización el 04 de julio de 2022. Disponible en: https://e-justice.europa.eu/content_judicial_systems_in_member_states-16-es-es.do?member=1. [Consultado el 25 de octubre 2023].

RODRÍGUEZ PÉREZ, Aylin, RODRÍGUEZ HERNÁNDEZ, Dairon, DÍAZ MARTÍNEZ, Elizabeth. Selección de Base de Datos No SQL para almacenamiento de Históricos en Sistemas de Supervisión. *Revista Cubana de Ciencias Informáticas* [en linea], 2016, 10(3), pp. 85-96. Disponible en: https://www.redalyc.org/articulo.oa?id=378346436012. [Consultado el 25 de octubre 2023].

SAFARICOM. *Safaricom and CBA Launch Ambitious Plan to Grow M-Shwari Customers.* Disponible en: https://www.safaricom.co.ke/media-center-landing/press-releases/safaricom-and-cba-launch-ambitious-plan-to-grow-m-shwari-customers. [Consultado el 25 de octubre 2023].

TELEFÓNICA TECH. *AI of Things. Scoring. Optimiza el rendimiento de tu negocio de crédito al consumo*. Disponible en: https://aiot.telefonicatech.com/hubfs/product_es/ficha_scoring_es.pdf. [Consultado el 25 de octubre 2023].

VILLACRESES VALENCIA, Carlos Andrés. El Tercero Interesado en el Régimen de Competencia Ecuatoriano, un Análisis Comparativo Crítico (The Interested Third Partie in the Ecuadorian Competition Law, a Critical Comparative Analysis). *USFQ Law Working Papers*, 2022/03. Disponible en: https://ssrn.com/abstract=4051015. [Consultado el 25 de octubre 2023].

WONDER.LEGAL. *Diferencias entre el acceso y la cesión de datos personales a terceros*. 05 de julio de 2022. Disponible en: https://www.wonder.legal/es/guide/diferencias-entre-el-acceso-cesion-datos-personales-terceros. [Consultado el 25 de octubre 2023].

Bibliografía complementaria

ALBARRÁN SÁNCHEZ, Oscar Sánchez; VIVANCOS GIMÉNEZ, Cristina; ALSINA DÍAZ, Carlos. Protección de Datos Personales: el interés legítimo, guía para poder utilizar los datos de los clientes sin su consentimiento. *La Ley privacidad*, 2021, núm. 9, p. 22.

ANDRADE SANTAMARÍA, Danilo Rafael; ALCÍVAR BASURTO, Frowen Bolívar; ARAUJO ESCOBAR, Esperanza del Pilar y SOXO ANDACHI Jorge Washington. La ponderación de derechos para las decisiones judiciales en Ecuador. *Estudios del Desarrollo Social: Cuba y América Latina*, 2020, vol. 8, núm. Especial, núm. 2. Disponible en: https://revistas.uh.cu/revflacso/article/view/4463. [Consultado el 25 de octubre 2023].

BANCO DE ESPAÑA. Central de Información de Riesgos. Disponible en https://www.bde.es/bde/es/secciones/servicios/Particulares_y_e/Central_de_Infor/Central_de_Info_04db72d6c1fd821.html [Consultado el 25 de octubre 2023].

BASE DE DATOS DE MOROSIDAD INMOBILIARIA. *Condiciones de Contratación de BDMI*. 18 de junio de 2023. Disponible en https://www.idealista.com/ayuda/articulos/condiciones-servicio-base-datos-inquilinos-morosos/. [Consultado el 25 de octubre 2023].

BECERRA GUTIÉRREZ, Juan Armando. *Guía para el borrado seguro de datos personales*. Propuesta de solución empresarial para obtener el grado de maestro en derecho de las tecnologías de la información y comunicación. Disponible en https://infotec.repositorioinstitucional.mx/jspui/bitstream/1027/147/4/INFOTEC_MDTIC_JABG_09092019.pdf. [Consultado el 25 de octubre 2023].

CARRASCO RUIZ Ximena Lucía y TRELLES VICUÑA Diego Fernando, La ponderación en la tutela de los derechos fundamentales en el Ecuador. *Polo del Conocimiento: Revista científico-profesional*, 2020, vol. 5, núm. 8, pp. 320-352. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=7554362. [Consultado el 25 de octubre 2023].

CHAYA. Random Forest Regression. *LevelUp Coding*. 8 de junio de 2020. Disponible en: https://levelup.gitconnected.com/random-forest-regression-209c0f354c84. [Consultado el 25 de octubre 2023].

CHEN, Gregory; FAZ, Xavier. El potencial de los datos digitales: ¿Hasta qué punto pueden fomentar la inclusión financiera?. *Enfoques*, enero de 2015. Disponible en:

https://www.cgap.org/sites/default/files/Focus-Note-The-Potential-of-Digital-Data-Jan-2015-Spanish.pdf [Consultado el 25 de octubre 2023].

CONDE ORTIZ, Concepción. *La protección de datos personales: un derecho autónomo con base en los conceptos de intimidad y privacidad* [online]. Madrid: Dykinson, 2005. Disponible en: https://rodin.uca.es/handle/10498/26396. [Consultado el 25 de octubre 2023].

COPPOLA, María Eugenia. ¿Qué es una API? Definición, tipos y ejemplos. *Hubspot*. 8 de octubre de 2023 13h25. Disponible en: https://blog.hubspot.es/website/que-como-usar-api. [Consultado el 25 de octubre 2023].

DE SOUZA, Iván. ¿Qué es un servidor web y para qué sirve en Internet? *Rockcontent*. 14 de junio de 2019. Disponible en: https://rockcontent.com/es/blog/que-es-un-servidor/. [Consultado el 25 de octubre 2023].

MACMILLAN, Rory y GARVEY, Scott. *Use of telecommunications data for digital financial inclusion*. Financial inclusion global initiative (FIGI), 2021. Disponible en: https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-DFS-2021-5-PDF-E.pdf. [Consultado el 25 de octubre 2023].

REDHAT. ¿Qué es y para qué sirve el almacenamiento en la nube? *Redhat.com*. 07 de febrero de 2023. Disponible en: https://www.redhat.com/es/topics/data-storage/what-is-cloud-storage#:~:text=Existen%20tres%20tipos%20de%20nubes,en%20bloques%2C%20archivos%20u%20objetos. [Consultado el 25 de octubre 2023].

VARGAS OROZCO, Carlos Alberto. *Un modelo de credit scoring utilizando inteligencia artificial para el fondo de empleados de salud en Risaralda - Feser*. Trabajo de grado para optar al título de Ingeniero de Sistemas y Computación por la Universidad tecnológica de Pereira - Facultad de ingenierías - Ingeniería de sistemas y computación. 18 de Noviembre de 2015. Disponible en: https://hdl.handle.net/11059/6111. [Consultado el 25 de octubre 2023].

VILLACRECES BRITO, Gustavo Andrés. La «persona interesada» y el «tercero interesado» en el control de concentraciones económicas del derecho de competencia ecuatoriano. *USFQ Law Review*, 2022, vol. 9, no 2, pp. 57-92.

VON JHERING, Rudolf. *L'esprit du droit romain: dans les diverses phases de son développement.* Paris: A. Marescq, Aîné. 1880.

Legislación citada

Código civil. *Registro Oficial*, núm. 46, del 24 de junio de 2005.

Constitución de la República del Ecuador. *Registro oficial,* 05 de enero de 2008, núm. 449. Última modificación el 25 de enero de 2021.

Ley 11/2022 General de Telecomunicaciones. 28 de junio de 2022. *Boletín oficial del estado* del 29 junio 2022, núm. 115, pp. 91253-91411. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2022-10757.

Ley orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales. 05 de diciembre de 2018. *Boletín oficial del Estado* del 06 de diciembre 2018, núm. 294, pp. 119788-119857. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673.

Ley Orgánica de Defensa al Consumidor. *Registro oficial*, del 10 de julio de 2000, núm. 116.

Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional. R*egistro oficial*, 22 de octubre de 2009, núm. 52, segundo suplemento*,* pp. 2-35. Última modificación el 07 de febrero de 2023.

Ley Orgánica de Protección de Datos Personales. *Registro oficial*, 26 de mayo de 2021, núm. 549, quinto Suplemento. Última modificación el 26 de mayo de 2021.

Ley Orgánica de Telecomunicaciones. *Registro oficial*, 18 de febrero de 2015, núm. 439, tercer suplemento. Última modificación el 29 de marzo de 2023.

Real Decreto Legislativo 1/2007 por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias. 16 de noviembre de 2007*. Boletín oficial del Estado* del 30 de noviembre de 2007, núm. 287, pp. 49181-49215. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2007-20555.

Reglamento (CE) 1060/2009 del Parlamento Europeo y del Consejo sobre las agencias de calificación crediticia. 16 de septiembre de 2009, última versión consolidada del 01 de enero de 2019. Diario Oficial de la Unión Europea del 17 de noviembre de 2009, L 302, pp. 1-31. Disponible en: https://eur-lex.europa.eu/eli/reg/2009/1060/oj.

Reglamento General de la Ley Orgánica de Protección de Datos Personales. 06 de noviembre de 2023. Registro oficial, 13 de noviembre de 2023, núm. 435, pp. 4-41. Disponible

en:http://esacc.corteconstitucional.gob.ec/storage/api/v1/10_DWL_FL/eyJjYXJwZXRhIjoicm8iLCJ1dWlkIjoiMGYxZjliNDctODQzNC00ZmExLTgwNDYtN2UyZGVlZDNiNzMzLnBkZiJ9.

Jurisprudencia referenciada

Resolución de procedimiento sancionador PS-00221-2020 de la Agencia española de protección de datos (AEPD), del 30 de noviembre de 2020, contra LVCENTVM LEGAL, S.L., p. 3. Disponible en: https://www.aepd.es/documento/ps-00221-2020.pdf.

Resolución de procedimiento sancionador PS-00259-2020, de la Agencia española de protección de datos (AEPD), del 08 de julio de 2021 contra Bankia S.A. p. 38. Disponible en: https://www.aepd.es/documento/ps-00259-2020.pdf.

Resolución de procedimiento sancionador PS-00406-2020 de la Agencia española de protección de datos (AEPD), del 09 de marzo de 2021, contra EQUIFAX IBERICA, S.L., p. 9. Disponible en: https://www.aepd.es/documento/ps-00406-2020.pdf.

Sentencia de la Corte Constitucional del Ecuador del 04 de septiembre de 2013, Caso 0179-12-CN y ACUMULADOS, Núm. 048-13-SCN-CC. Disponible en: http://doc.corteconstitucional.gob.ec:8080/alfresco/d/d/workspace/SpacesStore/f155c871-2655-4c78-b8ec-5516262ef7c5/0179-12-cn.pdf?guest=true.

Sentencia de la Corte Constitucional del Ecuador del 24 de Agosto de 2010, Caso 0022-2009-CN, 024-10-SCN-CC, Disponible en: http://esacc.corteconstitucional.gob.ec/storage/api/v1/10_DWL_FL/e2NhcnBldGE6J3RyYW1pdGUyMDIzJywgdXVpZDonZjVmYzRjMzItZDA4Yi00MTJjLThiNGEtZWMzZTY1ODM2MDk5LnBkZid9.

Sentencia de la Corte Constitucional del Ecuador del 27 de enero de 2021, Caso 2064-14-EP. Disponible en: http://esacc.corteconstitucional.gob.ec/storage/api/v1/10_DWL_FL/e2NhcnBldGE6J3RyYW1pdGUnLCB1dWlkOic1MDM5NmI5Ny1hZmFiLTQ1OWEtYWRlMC1jNjdmNzM1NTMzYjAucGRmJ30=#:~:text=2064%2D14%2DEP.&text=implica%20que%20no%20existiendo%20prueba,la%20vulneración%20de%20de.

Listado de abreviaturas

AEPD: Agencia Española de Protección de Datos Personales

APP: Application

ARCO: Acceso, Rectificación, Cancelación y Oposición

ARCOTEL: Agencia de Regulación y Control de las Telecomunicaciones

Art: Artículo

AWS: Amazon Web Services

CC: Código Civil

CDR: Call Detail Record

CRM: Customer Relationship Management

DNS: Domain Name System

Ej. Ejemplo

GDPR: General Data Protection Regulation

GPON: Gigabit Passive Optical Network

GPS: Global Positioning System

GT29: Grupo de Trabajo Sobre Protección de Datos del Artículo 29

HFC: Hybrid Fiber-Coaxial

HTTP: Hypertext Transfer Protocol

IMSI: International Mobile Subscriber Identity

IOT: Internet of Things

IP: Internet Protocol

IPTV: Internet Protocol Television

LDA: Latent Dirichlet Allocation

LODC: Ley Orgánica de Defensa al Consumidor

LOGJCC: Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional

LOPDP: Ley Orgánica de Protección de Datos Personales

LOT: Ley Orgánica de Telecomunicaciones

NLP: Natural Language Processing

NOSQL: Not Only SQL

Núm: Número

OTT: Over-The-Top

RBT: Risk-Based Reliability

RGLOPDP: Reglamento General a la Ley Orgánica de Protección de Datos Personales

SIM: Subscriber Identity Module

SMS: Short Message Service

SOAP: Simple Object Access Protocol

SPDP: Superintendencia de Protección de Datos Personales

SQL: Structured Query Language

SVM: Support Vector Machine

TELCO: Telecomunicaciones

UDR: User Data Repository

WTTX: Wireless-To-The-X

XDR: Extended Detection and Response