PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
FACULTAD DE DERECHO Y SOCIEDAD

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR FACULTAD DE DERECHO Y SOCIEDAD CARRERA DE DERECHO

TRABAJO DE INTEGRACIÓN CURRICULAR PREVIO A LA OBTENCIÓN DEL TÍTULO DE ABOGADO

Uso de datos personales en el contrato de factoring en el Ecuador

ESTUDIANTE: Paula Eduarda Coronel Iza
DIRECTOR: Mtr. José Paredes

Quito, D.M., 2024

Resumen

El escenario regulatorio en protección de datos resulta insuficiente en el tratamiento de datos dentro del contrato de factoring mercantil en el Ecuador. Al ser una implementación normativa reciente, al igual que en el resto de países latinoamericanos, en comparación con la trayectoria de protección de datos en la UE. Este trabajo analizará si existe un cumplimiento de estándares internacionales de protección de datos dentro del tratamiento proporcionado interno y externo por parte de las instituciones involucradas en el cobro de cartera de facturas comerciales negociables.

Palabras Claves: datos personales, cesión de derechos, contrato de factoring mercantil.

Abstract

The regulatory framework for data protection proves to be insufficient when it comes to the handling of personal data within commercial factoring agreements. As is the case in most Latin American countries, the implementation of such regulations is relatively recent when compared to the longstanding data protection frameworks in the European Union.This thesis analyzes whether the internal and external processing of personal data by institutions involved in the collection of negotiable and tradable invoice portfolios complies with international data protection standards.

Keywords: personal data, assignment of rights, factoring contract.

Tabla de contenido

1.1. Introducción.....4
1.2. Evolución normativa de datos personales en la UE.....7
1.2.1. Surgimiento y regulación de los datos personales en el marco del desarrollo comercial y tecnológico.....7
1.2.2. Comparación entre la Directiva 95/46/CE y el RGPD.....14
1.3. Evolución normativa de la protección de datos personales en el Ecuador.....19
2.1. Naturaleza jurídica del contrato de factoring mercantil..... 24
2.1.1. Cláusulas esenciales de cesión de datos en el contrato de Factoring Mercantil.. 28
2.1.2. Otros medios de obtención de los datos de los deudores en bases o sistemas informáticos ajenos a la empresa de factoring.....36
2.1.3. Uso de datos de los deudores desde la base de legitimidad de la Ley de Protección de Datos.....37
2.1.4. Medidas de gestión de riesgo y manejo de seguridad de datos personales y crediticios.....39
3. Conclusiones.....45
4. Bibliografía.....46

1.1. Introducción

Las implicaciones comerciales de un mundo moderno sintonizan en el mercado transnacional a países que den cumplimiento a estándares internacionales de protección de datos. En la actualidad, los datos personales son ahora los activos más importantes de las empresas; por tanto, las empresas que manejen dichos activos en cumplimiento de normativa serán relevantes y podrán ser parte de implicaciones comerciales en el mercado transnacional. Esto, debido a que la conectividad digital abarca un enfoque transfronterizo por el acceso e innovación creciente de tecnologías que crean nuevos espacios comerciales, mercantiles, y financieros. Donde el intercambio de información dentro de estos espacios ha proporcionado e implementado herramientas en negocios que dan uso de datos personales de los usuarios.

Los datos, al ser los activos más importantes, actualmente cuentan con una mayor fuente de obtención de los mismos implementados por empresas y Estados. Esto se ha dado a razón de la implementación de sistemas de generación y recolección de datos desde el uso de plataformas virtuales bancarias, de servicios, de pagos de cualquier tipo. Al tener los datos más fuentes de recolección generada por interacción de los titulares o usuarios de sus cuentas nacionales e internacionales, estos deben de contar con un margen de protección mayor.

Este escenario no se limita únicamente a actividades previsibles, como el acceso a una cuenta mediante el registro biométrico para la realización de pagos. Sino que abarca la simplificación de las interacciones entre los usuarios y las entidades financieras. Estas dinámicas, cada vez más frecuentes en un entorno digitalizado, incluyen la aceptación de condiciones y términos por parte de los usuarios, los cuales derivan directamente de dichas interacciones y configuran un marco de tratamiento de datos personales en el que convergen aspectos tecnológicos, jurídicos y comerciales.

Ampliando el margen de protección de datos personales, donde los parámetros de seguridad adquieren una relevancia central para garantizar un manejo adecuado de los datos personales en el ámbito financiero y comercial. Entre los principales desafíos se encuentran la prevención del acceso no autorizado a la información, y el establecimiento de mecanismos efectivos de control sobre los datos por parte de los usuarios titulares. Implicando de esta forma la necesidad de la conformación de una infraestructura normativa sólida, teniendo un enfoque estratégico que permita equilibrar la eficiencia operativa con los principios de transparencia, resiliencia, privacidad y protección de los derechos de los usuarios. En este sentido, el tratamiento de datos por parte de las instituciones financieras representa la ampliación de la gestión de parámetros de seguridad de la información. Creando a su vez una necesidad de implementación de una cultura institucional por parte de instituciones financieras de protección de datos.

La regulación de los datos personales encuentra su origen como un derecho fundamental, de tercera generación. Que por el dinamismo tecnológico se ha ampliado la necesidad de un margen de protección; en sentido del reciente uso de tecnologías que permiten la recopilación masiva de información. En Ecuador, la normativa en esta materia ha transitado por un proceso evolutivo, influenciada tanto por instrumentos nacionales como por estándares internacionales, entre los cuales destacan los desarrollos normativos de la Unión Europea, como el Reglamento General de Protección de Datos (RGPD). Estos marcos normativos han establecido principios y obligaciones esenciales para el tratamiento adecuado de datos personales. Viendo por primera vez la incursión en el reconocimiento del derecho de protección de datos personales en la normativa interna en el 2008 en el art. 66.19 de la Constitución. En este sentido, a pesar de dar reconocimiento a la protección de datos como un derecho constitucional, no fue hasta

2017 que la DINARDAP empezó a trabajar en un proyecto de ley. Mismo que en 2019 fue presentado ante la Asamblea Nacional, y aprobado en 2021; obteniendo de esta forma la actual Ley de Protección de Datos Personales, con su Reglamento de Protección de Datos.

En el ámbito mercantil, los contratos de factoring representan un caso particular de estudio debido al manejo especializado de datos personales que requieren. Este instrumento financiero, que permite la cesión de derechos de crédito, implica la incorporación de cláusulas específicas para regular la transferencia, y protección de los datos de deudores y terceros involucrados. La naturaleza jurídica de la gestión de la información por parte de instituciones financieras, y empresas de cobro de cartera exigen medidas de seguridad avanzadas; además, de obligaciones sistemáticas para garantizar la transparencia y la protección de los derechos de los titulares de la información.

Asimismo, en este trabajo reflexiona sobre las fases de inclusión normativa y la importancia de fomentar una mayor concienciación sobre la seguridad de la información, particularmente en sectores estratégicos como el financiero. Donde el manejo de datos adquiere implicaciones tanto jurídicas, desde una perspectiva comparativa, se analizarán las normativas ecuatoriana y europea. Considerando aspectos como la evolución legal de la protección de datos, los instrumentos internacionales aplicables, y los desafíos regionales en América Latina en esta materia.

De este modo, la investigación aborda de manera integral la protección de datos personales en Ecuador, con especial énfasis en su relación con el comercio y la tecnología. Asimismo, se examinan los desafíos que surgen en el contexto de los contratos de factoring mercantil, con el objetivo de sentar las bases para una gestión

normativa más eficiente. Misma que dé respuesta a las necesidades actuales del entorno digital dentro del espacio mercantil, manteniendo coherencia con los estándares internacionales.

SECCIÓN 1: MARCO TEÓRICO

1.2. Evolución normativa de datos personales en la UE

1.2.1. Surgimiento y regulación de los datos personales en el marco del desarrollo comercial y tecnológico.

La implementación normativa en protección de datos personales, se ha desarrollado de forma sostenida y dinámica en el tiempo. Esto a fin de poder gestionar los riesgos que devienen de nuevas realidades, donde los datos personales, son el activo inmaterial más importante en dinámicas comerciales. La obtención de datos personales tiene lugar en espacios físicos y virtuales, que a su vez, son una constante presente en el desarrollo de la vida del ser humano; esto tomando en cuenta la hiperconectividad a la que como especie estamos sujetos.

Para poder realizar un análisis del contenido y enfoque actual del marco regulatorio en protección de datos; es necesario examinar las bases en las que va tomando forma este derecho. La formación de este derecho, tiene sus cimientos en los derechos de primera generación de la privacidad e intimidad. En sentido, que el contenido de estos derechos se estaban vinculando con la esfera privada del "honor del individuo y de su familia" (Brandeis, L., Warren S., 1890, página 194). Adicionalmente, el derecho a la intimidad fue establecido como un derecho fundamental en dos ocasiones, siendo la primera en 1948 en la Declaración de los Derechos Humanos, y la segunda en 1950 en la Convención Europea de Derechos Humanos.

Conviene mencionar que el surgimiento de relacionar la formación de un nuevo derecho con el derecho a la intimidad, inició en 1890 en Estados Unidos. Posteriormente este

concepto jurídico, se iría acuñado en normas europeas, que en la actualidad han encaminado la implementación normativa de protección de datos desde un enfoque de "gobernanza global de la privacidad" (Cazzuro, V., 2020, pág. 9). En este apartado se conceptualiza el origen de este derecho, en contraste con la normativa internacional europea desde sus comienzos hasta la actualidad.

Este concepto nace dentro del ámbito académico en Estados Unidos en 1890 con el artículo "The Right of Privacy" de los abogados Louis Brandeis y Samuel D. Warren. Donde el derecho de privacidad es definido como el "derecho que lo dejen a uno en paz" (Cotino Hueso et al. , 2020), esto significando la existencia de una esfera privada, que no debía ser propensa a injerencias de terceros. Cabe señalar que en el mismo año el juez Brandeis utilizaría este término para emitir una sentencia, donde se dimensiona el alcance de este derecho en una obligación negativa de la "abstención para terceros y poderes públicos, que otorgaba garantías frente a injerencias" (Cotino Hueso et al. , pág. 18). Adicionalmente en el artículo académico de 1890 se reconoce que la privacidad nace como un principio derivado de la "protección de la persona y de la propiedad" (Brandeis, L., Warren S., 1890, página 193), que cubre "la dimensión moral o espiritual de la persona" (Huerta, P., 2017, página 59).

Para generar un entendimiento integral del desarrollo del marco normativo en protección de datos de la Unión Europea, resulta útil separar el análisis de forma histórica en tres momentos. Siendo un primer momento previo a la formación de la UE, analizando el origen normativo de algunos de los países que posteriormente serían miembros de la UE; posteriormente se realizará un análisis en acuerdos regionales y tratados internacionales como instrumentos jurídicos que promovieron la cooperación estatal entre países que serían futuros miembros de la UE; como último punto se abordará la consolidación de un marco jurídico común dentro de la Unión Europea.

En este primer momento se realizará un abordaje individual sobre la implementación progresiva de normativa en protección de datos antes de la formación de la UE. Siendo Alemania en 1970 con la emisión de la *Datenschutzgesetz* (Ley de Protección de Datos), el primer país en el mundo en implementar normativa donde se reconoce "el derecho de los ciudadanos a controlar el uso de sus datos personales hacia el Gobierno de ese estado" (L., Mieres y M., Vilasau, 2018, pág. 7). En el contenido de esta ley, se establecía que todo tipo de documento que contenían datos de usuarios debían de estar cubiertos por una protección legal. En esta sentencia, se desarrolla que las autoridades públicas deben de almacenar y procesar datos únicamente bajo el cumplimiento de fines específicos de uso. Posteriormente en 1977 en Alemania se aprueba de la *Bundesdatenschutszgestez* (Ley General de Protección de Datos), provocando que también exista la aplicación de la protección de datos para el sector privado.

Ahora bien, en Suiza en 1973 se aprobó la *Datalagen* (Ley de Protección de Datos) como una disposición complementaria de la *Datakungörelse* que era un reglamento donde se solicitaba "la autoridad administrativa de exploración y creación de archivos de datos personales" (*Datalagen,* 1973, art. 2). Esto con el fin de prevenir el riesgo de que un tercero de forma no autorizada diere uso de los archivos de las personas. La implementación normativa en protección de datos en países europeos, continuó en Francia en 1978, año en el que se aprobó la *Loi relative à l'informatique, aux fichiers et aux libertés* (Ley relativa a la informática, los archivos y las libertades civiles o Ley de Protección de Datos).

El marco legal de protección de datos, no solo estaba formado del ámbito normativo. En 1983 en Alemania el Tribunal Constitucional Federal desarrolló el "derecho a la autodeterminación informática" en base al derecho a la personalidad. Esta sentencia se

da en razón de que en 1982 se aprueba la Ley de Censo, donde el gobierno no solo se limitaba a la recopilación de datos generales de sus ciudadanos, sino accedía a la esfera personal de los mismos; esto causando un descontento social civil. En esta sentencia se determina que debe de existir un tratamiento de uso de datos. Y que para su implementación práctica, se debía de realizar una clasificación previa del tipo de dato que se buscaba usar. Esta sentencia, desarrolló no sólo la existencia de un tratamiento, sino que el tratamiento se debía de adecuar a la clasificación del dato. Las clasificaciones que se contemplaron son dos y están relacionadas con su fin de uso. La primera clasificación, atiende a los datos que se recolectan con fines estadísticos; aquí se puntualiza que " no se puede exigir de forma estrecha y concreta de que los datos estén vinculados a un fin determinado" (Schwabe, J., 2009, pág. 94). Mientras que en la segunda clasificación, tenemos a los vinculados a la persona, mismos "que son recaudados y analizados en forma individualizada, no anónima, y aquellos que se encuentran destinados a fines estadísticos" (Schwabe, J., 2009, pág. 94). En esta sentencia, se determina que no toda recopilación de datos estatal es contraria al derecho de libertad, esto al entender que esta recolección es necesaria para vivir en comunidad. La recopilación de datos contempla dentro de la sentencia la finalidad de convivencia. Y determina que, para cumplir con la organización social dentro de un Estado, es necesario aplicar restricciones a la autodeterminación de los ciudadanos. La aplicación de estas restricciones en cuanto al uso de datos de ciudadanos debe necesariamente cumplir con un propósito de recolección y un tratamiento determinado que sea de conocimiento ciudadano.

Ahora se va a puntualizar en la creación de acuerdos regionales y tratados internacionales como instrumentos jurídicos que promovieron la cooperación estatal, entre países que serían futuros miembros de la UE.

Es así que en 1980 la Organización para la Cooperación y el Desarrollo Económico (OCDE) aprueba las Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales, cabe mencionar que estas directrices no tenían fuerza vinculante. Estas directrices se formaron con el propósito de "expansión del comercio del comercio mundial sobre una base multilateral" (OCDE, 1980). Y su desarrollo se vió enmarcado en la identificación de la necesidad de protección de datos personales dentro de flujos transfronterizos. Donde se reconoce y define la existencia de un inspector de datos dentro de cada país y que la legislación local podría generar confusión en su tratamiento.

Como establece la OCDE (1980), estas directrices tenían como fin la estandarización de los principios básicos de tratamiento de protección de datos en los territorios de sus países miembros. Los principios que contemplaron dentro del contenido de estas directrices son:

Principio	**Contenido**
Principio de limitación de recogida	Establece que deben existir límites legales sobre la recolección de los datos, siendo un requisito consentimiento informado por parte del titular.
Principio de calidad de los datos	El uso de datos debe de tener fines concretos de uso, dichos usos deben ser completos, correctos y actualizados.
Principio de especificación de los fines	Desde la recolección de los datos debe de brindarse al usuario información sobre el uso específico de sus datos. Este uso debe

	ser limitado y si existe alguna variante de deberá de ser informada y actualizada para tratamiento.
Principio de limitación de uso	Debe de haber un uso limitado del dato, no habrán usos externos a los descritos, deberá de existir cumplimiento de disposiciones legales
Principio de salvaguardar la seguridad	La protección de los datos debe de ser oportuna, adoptando medidas contra riesgos de su uso o tratamiento dentro de todo su ciclo.
Principio de transparencia	Previa a la recolección del dato, debe de existir una política de tratamiento del dato.
Principio de participación individual	Toda persona física tiene derecho a acceder a su información, a "dentro de un plazo razonable, con una tarifa (...), de manera razonable y de forma que pueda entender fácilmente" (Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales, pág. 5-6)
Principio de responsabilidad	Los inspectores de datos deben adoptar medidas para el cumplimiento e incumplimiento de los principios.

Nota: tabla realizada con las Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales.

Si bien estas directrices surgen como softlaw, posteriormente fueron usadas como un marco referencial entre países; esto con el fin de fomentar el comercio con buenas prácticas internacionales de generación de estándares mínimos de tratamiento de datos.

En esta misma línea el 28 de enero de 1981, se desarrolla la *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (Convenio 108 del Consejo de Europa). Esta convención es considerada como el primer instrumento internacional con fuerza vinculante en materia de tratamiento automatizado de datos personales en flujos transfronterizos en sectores públicos y privados. En este convenio se recogen algunos de los principios desarrollados anteriormente en las Directrices. El fin de este Convenio, era "establecer una regulación homogénea en su ámbito de vigencia territorial" (Rebollo, L., 2020, pág. 61).

En palabras de Antonio Troncoso (2020) el desarrollo del derecho de protección de datos, fue uno de los principales medios de cumplimiento del objetivo clásico de la creación de la Unión Europea (UE) que es la libre circulación entre países miembros. En sentido que al existir un intercambio de información adecuado, se permitió sentar los cimientos de funcionamiento de esta unión geopolítica. Cabe aclarar que actualmente hay países externos a la Unión Europea que han ratificado dicho instrumento. El Convenio en un contexto histórico, permitió cimentar las bases que formaron y fortalecieron a la UE; más en la actualidad, este no puede ser implementado, al no estar adaptado al desarrollo tecnológico. Es por esto, que el 18 de mayo de 2018, se adopta el protocolo CETS No. 223 para modernizar este instrumento, que actualmente es conocido como Convenio 108.

Como tercera etapa de análisis el Tratado de Maastricht se firma en 1992 y entra en vigor en 1993, dando vida a la Unión Europea. Esto con el fin de "asegurar el buen funcionamiento del mercado único, así como, entre otras cosas, un desarrollo armonioso, equilibrado y sostenible de las actividades económicas" (Parlamento Europeo, 2024). En este tratado se sientan las bases de desarrollo de política y normativa en respeto de los derechos fundamentales. Siendo uno de estos derechos el

derecho a la privacidad, mismo que sería base para el posterior desarrollo de tratados y políticas en protección de datos ya en un ámbito transfronterizo comunitario.

1.2.2. Comparación entre la Directiva 95/46/CE y el RGPD

Con el nacimiento de la UE era necesario armonizar la normativa aplicable en protección de datos, para reducir "la diversidad legislativa existente en los distintos Estados de la Unión" (L., Mieres y M., Vilasau, 2018, pág. 9) y fortalecer el mercado comunitario. Ante esto, en 1995 varios Estados de la UE adoptan la Directiva 95/46/CE del Parlamento Europeo, que tenía disposiciones relativas a "al tratamiento de datos personales y a la libre circulación de estos datos " (Directiva sobre protección de datos, 1995). Cabe señalar que esta normativa sería aplicada de acuerdo al actual desarrollo de la sociedad según el considerando 14 de la directiva. En esta normativa se incluyeron los principios relativos al tratamiento de datos del Convenio 108 y se hace mención a la necesidad de existencia de autoridades de control nacionales, también se establece que los datos son lícitos cuando:

> El interesado ha dado inequívocamente su consentimiento; o el tratamiento es necesario para el cumplimiento de un contrato en el que sea parte el interesado; o el tratamiento es necesario para el cumplimiento de una obligación legal del responsable del tratamiento; o el tratamiento es necesario para proteger los intereses vitales de la persona de cuyos datos se trate; o el tratamiento es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero, o el tratamiento es necesario para los fines de interés legítimo del responsable del tratamiento o de un tercero, siempre que sobre dichos intereses no prevalezcan los intereses del interesado en el ámbito de los derechos y libertades que requieren protección (EUR-Lex, 2025).

Este Convenio también desarrolló los derechos de los titulares de los datos, que contemplaban la obtención, el acceso y oposición a la información. Para la

implementación del ejercicio de estos derechos, el Estado en esta normativa tiene la obligación de brindar a los titulares de datos recursos administrativos ante la autoridad de control competente.

Adicionalmente, uno de los fines de la directiva era establecer un sistema de protección de datos de aplicación general. Al ser un instrumento de aplicación indirecta, cada Estado a través del carácter de discrecionalidad adaptó dichas disposiciones dentro de cuerpos normativos nacionales. Hay que aclarar que este instrumento no es aplicable cuando el tratamiento del dato haya sido:

> Efectuado por una persona física en el ejercicio de actividades exclusivamente particulares o domésticas; aplicado al ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, tales como la seguridad pública, la defensa o la seguridad del Estado (EUR-Lex, 2025).

Esta directiva por los cambios derivados de la realidad tecnológica y económica del mundo en 2018 fue sustituida por el Reglamento Europeo (UE) 2016/679. Este reglamento se forma, según Moritz y Gibello (2017), en el 2015 por medio de una de las comisiones de la Comisión Europea que agrega como objetivo el desarrollo del mercado digital alineado al libre mercado y el respeto de derechos fundamentales. Adicionalmente, en 2012 se realiza el debate de una reforma a la Directiva 95/46/CE, esto para adaptar dicha regulación ante los "actores de este mercado único digital" (Moritz, M., Gibello, V., 2017, pág. 2). En este año hubo un proceso de negociación entre el Parlamento Europeo y el Consejo de la Unión Europea. Más no es hasta 2016 que esta reforma sería publicada en el Diario Oficial de la UE, dando así el nacimiento del REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 "relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y

por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)". Esta reforma fomentó la adaptación normativa a la realidad para fomentar el crecimiento del mercado. Con el fin de terminar con la disparidad normativa existente de los países miembros, se instauró una base sólida normativa unificada para la protección de datos. El reglamento al ser de obligatorio cumplimiento y con efectos inmediatos para todos los miembros que lo hubieren ratificado, tuvo una implementación eficiente en la normativa de sus países miembros. Esto implicando que dichos países debieron adaptar su normativa interna a las disposiciones del reglamento y; por tanto, derogar aquella que no estuviere a fin de este. En el 2018, este instrumento entra en vigor, a partir de esta fecha se deroga la Directiva de Protección de Datos.

El contenido de este reglamento, según el Consejo Europeo (2024), contempla los "derechos fundamentales de las personas en la era digital, las obligaciones de los encargados de tratamiento de datos, los métodos para garantizar el cumplimiento y las sanciones para quienes infrinjan las normas" (pág. 1). Además, determina que para que exista control del cumplimiento del reglamento, deben de existir autoridades administrativas concernientes a cada Estado. Las autoridades de control estarán sujetas al secreto profesional y de confidencialidad, mientras que el Comité Europeo de Protección de Datos revisará el correcto cumpliento.

A continuación se mostrará un cuadro comparativo entre la Directiva 95/46/CE y el RGPD:

Tema a analizar	**Directiva 95/46/CE**	**RGPD**
Año de ratificación	1995	Adoptada en 2016, más hay que tomar en cuenta que con la derogación de la Directiva 95/46/CE en 2018, desde este año

		pasa a ser de aplicación directa.
Países que ratificaron de la UE	15 Estados miembros de la UE	Aplicación directa de todos los Estados miembros (28 países), tomando en cuenta que este reglamento entró en vigencia antes del Brexit.
Ámbito de aplicación	Los países que ratificaron dicha directiva tuvieron que adaptar su normativa de acuerdo al tratado.	Este reglamento buscaba acabar con el problema de la disparidad normativa interna de cada Estado, tratando de unificar el derecho de protección de datos, teniendo como resultado la obligación de los Estados de la adaptación de su normativa interna a las directrices contenidas en el reglamento.
Principios reconocidos	● Principio de licitud, lealtad y transparencia (art. 6). ● Principio de limitación de la finalidad (art.6.1.b). ● Principio de minimización de datos (dentro de los principios generales). ● Principio de exactitud (art.6.1.d). ● Principio de limitación del plazo de conservación (art. 6.1.e). ● Principio de integridad y	● Principio de licitud, lealtad y transparencia (art. 5.1.a). ● Principio de limitación de la finalidad (art.5.1.b). ● Principio de minimización de datos (art. 5.1.c). ● Principio de exactitud (art. 5.1.d). ● Principio de limitación del plazo de conservación (art. 5.1.e). ● Principio de integridad y confidencialidad (art. 5.1.f, y art. 32). ● Principio de responsabilidad proactiva

	confidencialidad (art. 17).	(art. 5.2) ● Principio de protección desde el diseño y por defecto (art. 25)
Derechos de los usuarios	● Derecho de información (arts. 10 y 11). ● Derecho de acceso (art. 12). ● Derecho de rectificación, cancelación o bloqueo (art. 12b). ● Derecho de oposición (art. 14). ● Derecho a no ser objeto de decisiones automatizadas (art. 15).	● Derecho a la información (art. 13 y 14). ● Derecho de acceso (art. 15) ● Derecho de rectificación (art. 16). ● Derecho al olvido (art. 17). ● Derecho a la limitación del tratamiento (art. 18). ● Derecho a la portabilidad (art. 20). ● Derecho de oposición (art. 21).

Nota: tabla realizada con la Directiva 95/46/CE y el RGPD.

En conclusión, la derogatoria de la Directiva 95/46/CE y la adopción del RGPD buscó una unificación normativa para generar homogeneidad de aplicación normativa de los países miembros de la UE. Esto permitió salvaguardar el cumplimiento transfronterizo del tratamiento automatizado de datos. Por medio de este reglamento también se desarrolla en mayor medida el contenido de: (i) derechos de los usuarios y se implementó el derecho de portabilidad, y; (ii) los principios implementando tres principios siendo éstos los de responsabilidad, protección desde el diseño y el de privacidad. La adopción de este reglamento era una forma de adaptarse a la nueva

realidad y necesidad de regular espacios nuevos donde los datos, son tratados como activos intangibles, cobrando más relevancia dentro del mercado.

1.3. Evolución normativa de la protección de datos personales en el Ecuador

La forma en la que se ha abordado la protección de datos en Ecuador inició de forma indirecta, con el desarrollo de los derechos de intimidad y privacidad. Al igual que en los países europeos pioneros en contemplar la protección de datos como un derecho, desde la base estos derechos fundamentales. La base filosófica que justifica la existencia normativa de los derechos de intimidad y privacidad, es reconocer que el ser humano tiene una esfera personal. Al tener una esfera personal estos derechos, tienen una dimensión amplia, donde se sitúa al ser humano desde el resguardo de su privacidad. Un ejemplo del alcance de la dimensión de este derecho, es la inviolabilidad del domicilio, al ser este un espacio privado.

El derecho de libertad en el Ecuador se estableció por primera vez en la Constitución de 1830. En la Constitución se aborda este derecho de libertad, desde un deber de abstención de inmiscuirse en la vida privada de las personas. Este derecho fue uno de los primeros donde se vinculaba la propiedad de un individuo como un asilo inviolable. El derecho de libertad, desde la primera constitución, fue vinculado dentro de la esfera personal del ciudadano.

Cabe señalar que al igual que este derecho existieron otros como la inviolabilidad de la correspondencia y el derecho al honor, que fueron formando la noción del plano privado dentro de la vida de un ciudadano. Posteriormente en 1967 aparece el derecho a la intimidad como un derecho constitucional.

Pero no es hasta la reforma constitucional de junio de 1996, R.O. 969, que la garantía jurisdiccional del hábeas data aparece. Esta garantía jurisdiccional contemplaba la protección de los derechos de acceso, “actualización, rectificación, eliminación o

anulación" (Puccinellli citado por Gárate et. al, 2021) de la información. Posteriormente, en la Constitución de 1998 en su art. 94 que establecía el hábeas data, por primera vez aparecía el término datos personales. No como un derecho, pero sí como parte de una obligación legal a entidades que manejaran "archivos relacionados con la defensa nacional" (Constitución, 1998, art. 94) de desarrollar procedimientos especiales para acceder a datos personales.

La protección de datos como derecho constitucional en Ecuador, aparece por primera vez en la Constitución 2008, en el que se reconoce como derecho fundamental al derecho de protección de datos. Este derecho contenido en el art. 66.19, el capítulo sexto de derechos de libertad establecía:

> Se reconoce y garantizará a las personas:
>
> (...)
>
> 19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley (CRE, 2008, art.66.19).

En palabras de Luis Enríquez (2017), el reconocimiento de un derecho no hace efectiva su protección, con la implementación normativa del derecho de datos personales existían razones por las que en la práctica no se podía exigir este derecho. Esto, en primer lugar, al no establecer una definición de datos personales, ni el margen de aplicabilidad de esté derecho. Aquí es importante señalar que en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos de 2002 sí existía una definición de datos personales. Pero esta definición se da en un contexto específico que es el ámbito electrónico. El derecho de protección de datos además, fue implementado sin la existencia de un sistema de tratamiento que vincule al dato desde su ciclo de vida. Adicionalmente, el enfoque normativo en protección de datos cubría una esfera

únicamente nacional, más por el desarrollo tecnológico resulta que la aplicación de este derecho era insuficiente al contar con problemas transnacionales en esta materia. Por último, no se establecen órganos competentes ni autoridades que aseguren la observancia de este derecho.

Posteriormente, en 2017, la DINARDAP empieza a trabajar en el desarrollo de un proyecto de Ley de Protección de Datos. Esto a razón que en 2016 el Ecuador suscribe el Protocolo de Adhesión al Acuerdo Comercial Multipartes con la Unión Europea. En este acuerdo el Ecuador se compromete con "desarrollar un nivel de protección adecuado para el flujo transfronterizo de datos personales" (Roldán, F., 2021, pág. 4). Esto teniendo en cuenta que en el 2016 ya se había promulgado el RGPD, este un nuevo estándar en protección de datos con enfoque transfronterizo. Adicionalmente, se debe tener en cuenta que los países que fueran adecuando su marco regulatorio en protección de datos en cumplimiento de los estándares internacionales; se les abriría el "mercado para inversiones internacionales y actividades empresariales que implican la transferencia de datos personales" (Roldán, F., 2021, pág. 5).

Finalmente, en 2021 se aprueba la Ley Orgánica de Protección de Datos Personales, esto representando para el país mayor cobertura en esta materia. Dla Piper (2025) realizó un informe donde se clasifica el marco normativo de protección de datos de 160 países, situando al Ecuador como un país con regulación moderada, al igual que Colombia y Perú. Una vez señalado esto se procederá a realizar un cuadro comparativo de la normativa en protección de datos en el Ecuador y en la Unión Europea:

Tema a analizar	**LOPDP (2021- Ecuador)**	**RGDP (2018- Unión Europea)**
Año	Se aprueba en 2021	Se ratifica en 2018
Territorialidad	Ecuador, y ciudadanos ecuatorianos fuera del país.	Países dentro de la UE, se aplica a empresas que ofrezcan bienes y servicios a ciudadanos de los países de la UE.

Terminología normativa	**Datos personales:** "Información que identifica o hace identificable a una persona natural" (LOPDP, 2021, art. 5). **Tratamiento de datos personales:** "Cualquier operación sobre datos personales: recolección, almacenamiento, uso, difusión, etc " (LOPDP, 2021, art. 5). **Consentimiento:**"Manifestación libre, específica, informada e inequívoca"(LOPDP, 2021, art. 12).	**Datos personales:** "Toda información sobre una persona física identificada o identificable" (RGPD, 2018, art.4.1). Tratamiento de datos personales: "Cualquier operación sobre datos personales", esto desde su recolección, registro, consulta, difusión, conservación, destrucción. (RGDP, 2018, art.4.2). "Todo tratamiento de datos personales debe ser lícito y leal. Para las personas físicas debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados" (RGDP, 2018, art.39). **Consentimiento**: "El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal (...)" (RGPD, 2018, art.32).
Clasificación de datos personales	**Dato personal:** "Dato que identifica o hace identificable a una persona natural, directa o indirectamente" (LOPDP, 2021, art. 4). **Datos personales crediticios:** "Datos que integran el comportamiento económico de personas naturales, para analizar su capacidad financiera"(LOPDP, 2021, art. 4). **Datos relativos a la salud** (LOPDP, 2021, art. 4). **Datos sensibles:** "Datos relativos a: etnia, identidad de género, identidad cultural, religión,	**Datos personales:** "el respeto de la vida privada y familiar, del domicilio y de las comunicaciones, la protección de los datos de carácter personal, la libertad de pensamiento, de conciencia y de religión, la libertad de expresión y de información, la libertad de empresa, el derecho a la tutela judicial efectiva y a un juicio justo, y la diversidad cultural, religiosa y lingüística"(RGPD, 2018, art. 4). Categorías especiales de datos personales:

	ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, salud, datos biométricos, datos genéticos y aquellos cuyo tratamiento indebido pueda dar origen a discriminación, atenten o puedan atentar contra los derechos y libertades fundamentales"(LOPDP, 2021, art. 4). **Datos anonimizados** (LOPDP, 2021, art. 2.c). **Datos seudonomizados** (LOPDP, 2021, art. 4).	● **Datos sensibles:** No hay una definición específica sobre este tipo de datos, más se establece que "Estados miembros especifiquen sus normas, inclusive para el tratamiento de categorías especiales de datos personales («datos sensibles»)" (RGPD, 2018, art. 10). ● **Datos relativos a temas penales**(RGPD, 2018, art. 19). ● **Datos anonimizados** (RGPD, 2018, art. 26). ● **Datos seudonomizados** (RGPD, 2018, art. 26 y 28).
Autoridades de Control	Superintendencia de Protección de Datos Personales, misma que fue creada en 2023.	Comité Europeo, en coordinación con las autoridades nacionales competentes dentro de cada país.
Derechos ARCO	Acceso Rectificación Cancelación (olvido) Oposición Portabilidad	Acceso Rectificación Cancelación (olvido) Oposición Portabilidad
Mecanismos preventivos	Evaluaciones de impacto del uso de datos personales: Cabe señalar que este tipo de tratamiento deberá ser implementado previo el tratamiento del dato, "-El responsable realizará una evaluación de impacto del tratamiento de datos personales cuando se haya identificado la probabilidad de que dicho tratamiento, por su naturaleza, contexto o fines, conlleve un alto riesgo para los derechos y libertades del titular o cuando la Autoridad de Protección de Datos Personales lo requiera" (LOPDP, 2021, art. 42). Se establece que este tipo de evaluaciones son obligatorias cuando: 1) cuando el titular de los datos, por	Evaluaciones de impacto: "Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares" (RGPD, 2018, art. 35). Cabe señalar que en el RGPD se establece que será facultad de cada entidad de control determinar en

	tratamiento de sus datos tenga efectos jurídicos; 2) cuando los datos son categorizados como especiales; y 3) cuando haya una observancia sistémica de acceso público.	qué casos se requerirá evaluaciones de impacto.

Nota: tabla realizada con la LOPDP y el RGPD

SECCIÓN 2: EL TRATAMIENTO DE DATOS PERSONALES EN EL CONTRATO DE FACTORING

2. Manejo de datos personales en el Contrato de Factoring Mercantil en el Ecuador

2.1. Naturaleza jurídica del contrato de factoring mercantil

El Factoring mercantil es un tipo de contrato nominado desde 2019 con la entrada en vigencia del Código de Comercio. Este contrato busca brindar una herramienta financiera de liquidez inmediata para empresas por medio de la compra de facturas, reduciendo el riesgo del impago de las mismas. Cabe puntualizar que las actividades relacionadas al cobro anticipado de cualquier tipo de obligación, incluyendo el cobro de facturas antes de 2019 estaban previstas para su operatividad desde el sector financiero desde 2014 en el Código Orgánico Monetario y Financiero.

En este contrato doctrinariamente existe una empresa denominada cedente, misma que cede a una entidad financiera denominada como factor, los derechos de cobro de sus facturas comerciales negociables (FCN) a cambio de una financiación anticipada. El factor se encarga de gestionar el cobro de la deuda y asume, en algunos casos, el riesgo de insolvencia de los deudores (Uribe, H., 2015, pág. 5-6). Con la definición doctrinaria, hay que puntualizar que la regulación en el Código de Comercio del contrato de factoring confunde su alcance al cobro al de cualquier tipo de obligación, esto al regular este contrato de la siguiente forma:

> El **contrato de compra de cartera o factoring** es una operación por la cual las compañías de comercio legalmente constituidas, que incluyan en su objeto social la realización profesional y habitual de operaciones o factoring o descuento de facturas comerciales negociables, cesión de cualquier tipo de derechos de cobro y sus operaciones conexas, de conformidad con las regulaciones que para el efecto emita la autoridad competente en la materia, adelantan fondos a sus clientes, quienes a cambio le **ceden títulos de crédito o facturas comerciales negociables**; asumiendo el adquirente, respecto de los créditos cedidos, al menos una de las obligaciones siguientes:
>
> a) Gestionar el cobro de los créditos;
>
> b) Financiar al proveedor; y,
>
> c) Asumir el riesgo de insolvencia de los deudores (Énfasis me pertenece)(Código de Comercio, 2019, art. 667).

Si bien existe esta confusión normativa, al extender el alcance a cualquier título de crédito, por **confusión** en la forma de regulación hay que entender que el contrato de factoring mercantil no es más que una especie dentro del género de compra de cartera. Y que, como establece Idrovo y Baraona (2021) "se limitan exclusivamente a los créditos por cobrar retenidos en facturas comerciales negociables" (pág. 432). Las facturas comercial negociables, a su vez, son un título valor de circulación comercial que su emisión puede ser física o electrónica y estas sirven de "comprobantes de venta físicos o electrónicos que el vendedor de un bien o derecho o prestador de un servicio emite con ocasión de la transferencia del bien o derecho o la prestación del servicio u otra negociación" (Ordoñez, M., 2019). Este título valor, puede ser a su vez de naturaleza ejecutiva si cumple con lo establecido en el Código de Comercio:

> "Las facturas comerciales constituyen (...) títulos ejecutivos cuando contengan una orden incondicional de pago, cuya aceptación sea suscrita por el comprador o adquirente de bienes, derechos o servicios, o su delegado, con la declaración expresa de que los ha recibido a su entera

> satisfacción, o que hubieren sido aceptadas tácitamente y siempre que cumplan con las reglas dispuestas en este capítulo" (2019, art. 203).

Si estas constituyen un título ejecutivo, adicionalmente como requisitos normativos del Código de Comercio, tendrían que no haber sido reclamadas o devueltas y encontrarse actualmente exigibles para que la vía idónea judicial sea el procedimiento ejecutivo.

Uno de los elementos esenciales tenemos que este contrato es bilateral, estando este contrato conformado por el cedente o factorado y el factor.
El cedente es la persona natural o jurídica en capacidad de emisión de facturas comerciales negociables. Esta parte, cede sus derechos de cobro contenidos en la factura comercial negociable; con el fin de obtención de liquidez brindada por parte del factor para dar continuidad a sus actividades comerciales. Por otro lado, el factor es quien compra los derechos de crédito contenidos en la factura comercial negociable. Para el factor, poder realizar actividades de factoring, tendrá que ser una persona jurídica, que dentro de su objeto social contemple la de "la realización profesional y habitual de operaciones o factoring o descuento de facturas comerciales negociables, cesión de cualquier tipo de derechos de cobro y sus operaciones conexas" (Código de Comercio, 2019, art. 667). Es por esto, que pueden existir dos tipos de factores siendo las IFIS (instituciones financieras) y las compañías con objetos sociales que cumplan las disposiciones del art. 447 del Código de Comercio, el factor adquiere dos obligaciones principales, siendo estas: 1) En el momento de la compra de los derechos de crédito, el factor tiene la obligación de pagar al cedente tomando en cuenta que el cálculo de valor a pagar será en base al "descuento por sus servicios y el riesgo del cobro" (Idrovo y Baraona, 2021, pág. 428); y 2) Una vez adquiridos los derechos de crédito, la obligación del cobro de crédito al deudor.

Ahora bien, si este contrato es de naturaleza bilateral, tenemos a un tercero involucrado directamente en el contrato a pesar de no ser una parte contractual, quien es el deudor. Dentro del contrato de factoring, el deudor pasa a tener un nuevo acreedor quien es el factor. Bajo la normativa ecuatoriana, no es necesaria la notificación y aceptación de la cesión del derecho de crédito por parte del cedente al factor; más, por la libertad contractual de las partes es un término que se podría pactar.

Ahora bien, como características generales derivadas de este tipo de contrato son las siguientes: nominado, conmutativo, de contenido flexible, oneroso, típico, consensual, bilateral (Rodríguez, 2024). Mientras que, como estructura base del contrato se establecen los siguientes elementos:

Elementos estructurales del contrato de factoring
1. Nombre, razón o denominación social y domicilio de las partes
2. Plazo de duración del contrato
3. Identificación de los instrumentos que son objeto de factoring o, de ser el caso, precisar los criterios que permitan identificar los instrumentos respectivos.
4. Identificación clara del precio a ser pagado por los instrumentos y la forma de pago.
5. En caso de ser una comisión, la retribución correspondiente al factor.
6. Se debe de establecer cuál de las partes asume la gestión de actividades derivadas del cobro de la deuda.
7. Se establece desde qué momento el factor asume el riesgo crediticio de los deudores.

Los elementos descritos, son esenciales para la formación de la estructura base del contrato de factoring mercantil. Este contrato, al ceder un derecho de crédito tiene un fin comercial que el factor pueda ser beneficiario del valor adeudado.

2.1.1. Cláusulas esenciales de cesión de datos en el contrato de Factoring Mercantil.

En este contrato, al pactarse una cesión del derecho de crédito y ser un contrato de naturaleza comercial, se deberá pactar la forma en la que el factor y el factorado se encuentran obligados en el contenido de derechos. El factor previa suscripción contractual deberá de evaluar la capacidad de riesgo de los deudores, esto en sentido de que esta parte podría asumir la insolvencia del deudor. Para poder realizar esta acción el el factor necesariamente deberá de tener acceso a los datos crediticios del deudor. Generalmente, por el tipo de riesgo a asumir no se realiza una compra única de FCN, sino se compra la cartera de FCN de personas naturales o jurídicas.

Por otra parte, los derechos de crédito conllevan la realización de una serie de actividades operativas financieras que permitan al factor poder ejecutar el cobro. Para poder realizar esta operación de forma efectiva, será necesario poder establecer contacto con el deudor. Algunos de los datos personales del deudor que podrían ser usados antes, durante y posterior a la suscripción de este contrato. Esto será posible porque la cesión de los derechos crediticios al tener como fin el cobro, tendrá que gestionar la operatividad de actividades para llegar al pago de la deuda. Algunas de las fuentes de obtención de datos personales del deudor son el contrato, de la misma FCN y de fuentes con acceso público externo en uso del operador de las actividades de cobro.

Para el perfeccionamiento de este contrato, existen dos escenarios que dependen de la forma en la que se transfieren los derechos de crédito. Una de las formas es la cesión de derechos, en esta opción nos encontramos ante un acto bilateral, que para que este perfeccione necesita cumplir con los requisitos del Código Civil, donde se contempla notificación del traspaso del crédito. En la notificación se deberá de exhibir el título al deudor, donde se establecerá e identificará al cesionario y al cedente; una vez exhibido

el título, la aceptación por parte del deudor puede ser tácita o expresa, bastará con la realización por parte del mismo con "un hecho que la suponga" (Código Civil, art. 1845). Por otro lado, como una segunda forma de cesión de derechos tenemos el endoso, donde como se mencionó *ut supra* no es necesaria la notificación y aceptación por parte del deudor para el perfeccionamiento del contrato de factoring.

En el primer escenario donde existe una cesión de derechos que se perfecciona por la notificación y aceptación al deudor; el modo del título, se contempla desde una perspectiva meramente civil y mercantil. Cabe señalar que con el título se ceden los datos personales y datos crediticios del deudor. Con la cesión de derechos crediticios no se contempla el margen de consentimiento de cesión de datos por el deudor. Esto tomando en cuenta que dependiendo de cómo se establecen las obligaciones del contrato de factoring, se podrían consecuentemente establecer cambios en el tratamiento de sus datos personales, en cuanto al encargado, el responsable, y el destinatario.

La finalidad del tratamiento de datos dentro del contrato de factoring es ejecutar el cobro total de la deuda. La forma en la que se persigue la ejecución es variada y proporcional a quien asume la gestión de cobro y operaciones conexas dentro del contrato. Como regla general salvo estipulación contractual contraria quien asume este tipo de gestiones es el factor, éste deberá de brindar un tratamiento de datos del deudor bajo el cumplimiento del fin antes mencionado. Para esto será necesario identificar que ahora el encargado de proteger el derecho de protección de datos es el factor. Adicionalmente, se deberán de identificar las personas naturales o jurídicas que participarán en las operaciones conexas derivadas del fin de ejecución de cobro usando los datos personales y personales crediticios del deudor. Estas personas dentro del tratamiento de protección de datos serán conocidos como encargados.

Los datos personales crediticios tienen como margen de regulación general la LOPDP y el Reglamento de esta ley; más este marco regulatorio por la especificidad del dato, se extiende al desarrollo normativo de la Superintendencia de Bancos y la Junta de Política y Regulación Financiera.

Ahora bien, el factoring mercantil constituido desde el endoso o desde la cesión no requiere del consentimiento como un requisito para la cesión de datos personales. Esto entendiendo que el consentimiento fue otorgado previamente al cedente, quien al ceder sus derechos de crédito al factor lo posicionó como un nuevo acreedor, quien resulta ser beneficiario de la cesión de todos los derechos derivados de la deuda por cobrar. Es de este modo, que la aceptación de la acción de cesión no es necesaria para el perfeccionamiento del contrato de factoring. El deudor no estaría informado hasta que exista un acto manifiesto por parte del factor, quien al ser el nuevo acreedor en ejercicio de sus derechos diera a conocer al deudor su posición como nuevo acreedor.

Como se mencionó con anterioridad, este contrato cede al factor datos personales y datos personales crediticios. Para mayor comprensión se debe de puntualizar que los datos personales crediticios son una especie de datos personales. Esto en razón de que los datos personales vuelven identificables a una persona; y que por otro lado, los datos crediticios permiten identificar a una persona y su comportamiento dentro del sistema financiero. La información objeto de estos tipos de datos, tiene que ser manejada con fines específicos y tener un tratamiento de datos. Dependiendo del tipo de dato, la normativa y las entidades que regulan su tratamiento cambian; es por esto que es necesario puntualizar diferencias en cuanto al tratamiento de acuerdo al tipo de dato tratado.

Los datos crediticios en el Ecuador, a modo de registro histórico normativo, han estado regulados desde 1994 con la publicación de Ley General de Instituciones del Sistema

Financiero. Esta ley surge al margen de la necesidad normativa comercial financiera, de posicionar el sistema financiero ecuatoriano como un sistema establecido sólido en seguridad de privacidad de usuarios suficiente. Esta ley buscaba implementar procesos de seguridad para tratamientos de datos. Esta norma fue un primer acercamiento en el ámbito regulatorio de protección de datos crediticios; posicionando al sistema financiero como uno de los primeros sectores que empezaron a dar un tratamiento normativo institucional a los datos obtenidos de sus clientes y usuarios.

Posteriormente, dentro del marco regulatorio del sistema financiero se implementaron normas, reglamentos internos dentro de las IFIS. Se expidieron resoluciones por parte de las entidades competentes como la Superintendencia de Bancos. Estas normas de protección de datos se fueron implementando por entidades autorizadas a funcionar como burós de créditos Una de las resoluciones más importantes, que daba dimensión al derecho de acceso a la información de los clientes y usuarios sobre sus datos fue la resolución No. JB-2010-1782 de la Junta Bancaria, misma que fue derogada por el Código Orgánico Monetario Financiero, donde se establecía el Código de Derechos del Usuario Financiero, que daba dimensión al derecho de acceso de la siguiente forma:

> 13.1 Exigir información y documentación de todos los actos que respalden la negociación, contratación, ejecución y terminación del contrato, y/o de la prestación de productos y servicios financieros ya sea al obligado directo o indirecto;
>
> 13.2 Derecho a obtener los documentos que han sido debidamente cancelados o endosados por haberse subrogado en la obligación en calidad de garante; y,
>
> 13.3 Conocer si en las bases de datos de las instituciones del sistema financiero existe información sobre sí mismo y acceder a ella sin restricción alguna; a conocer la fuente de dicha información; y, a exigir de la misma la rectificación de los datos personales cuando dicha información sea inexacta o errónea (2010, art. 13)

Ahora bien, entendiendo que la implementación normativa de datos crediticios es más antigua, que la normativa en general de protección de datos al ser la Ley de Protección de Datos publicada en 2021; la misma Ley Orgánica de Protección de Datos prevé que la protección de datos personales crediticios estará sujeta a lo previsto en "la presente ley, en la legislación especializada sobre la materia y demás normativa dictada por la Autoridad de Protección de Datos Personales" (2021, art. 28).

Los datos personales crediticios desde una definición normativa, como establece el Código Orgánico Monetario y Financiero, abarcan la información de una persona dentro del sistema financiero, teniendo acceso a datos de IFIS públicas y privadas. Una persona en el Ecuador, empieza a tener un perfil crediticio cuando la misma cumple la mayoría de edad; esto con el fin específico, de poder analizar la situación financiera y el riesgo de crédito de la misma. Por otro lado, en la Ley Orgánica de Protección de Datos establece que son datos crediticios aquellos que "integran el comportamiento económico de personas naturales, para analizar su capacidad financiera" (2021, art. 4).

Este tipo de datos, al estar inmersos dentro del sistema financiero, tienen como responsable de la administración de los mismos a la Superintendencia de Bancos. En el Código Orgánico Monetario y Financiero, en su libro I, se establece el acceso de datos crediticios como un servicio prestado por la "Superintendencia de Bancos y personas jurídicas autorizadas por la Superintendencia" (2014, art. 357). A las instituciones que presten este servicio, como determina la Codificación de las Normas de la Superintendencia de Bancos en su Libro I del Sistema Financiero, en su título IX, art. 4 se les denomina como burós crediticios. Estas entidades se verán obligadas a responder dentro del margen de su actuación a la Codificación anteriormente mencionada, a la Ley Orgánica de Protección de Datos y a las resoluciones emitidas por la Junta de Política y Regulación Monetaria y Financiera. Actualmente, como instituciones autorizadas para

funcionar como burós de créditos por parte de la Superintendencia de Bancos encontramos a las empresas Equifax, Aval Buró Ecuador e IFIS.

Si bien es cierto que el servicio general es el de acceso, también se establecen como servicios relativos a los datos crediticios "la entrega de reportes de información crediticia, modelos de riesgos, scores de crédito o en general diversas metodologías, procesamiento de información o servicios de valor agregado" (Código Orgánico Monetario y Financiero, 2014, art. 357).

En el caso de los datos crediticios, la Ley Orgánica de Protección de Datos puntualiza el fin con el que pueden ser recolectados los datos crediticios siendo este que "permitan evaluar la concertación de negocios en general, la conducta comercial o la capacidad de pago del titular de los datos" (2021, art. 28). Mientras que, los fines específicos de recolección abarcan los siguientes aspectos: "permiten evaluar la concertación de negocios en general, la conducta comercial o la capacidad de pago del titular de los datos" (2021, art. 28).

Para que el acceso a los datos crediticios pueda ser posible, el titular de la información crediticia, es el responsable de solicitar el acceso, o a su vez, autorizar a un tercero, estas dos formas de acceso tienen que contar con la autorización expresa del titular. Generalmente, los solicitantes de datos crediticios son las mismas instituciones financieras que usan los datos crediticios de una persona para poder medir su capacidad crediticia y ver la idoneidad de cumplimiento de la persona natural o jurídica de sus obligaciones financieras. Adicionalmente, se establecen como requisitos normativos en el Código Orgánico Monetario y Financiero, que el acceso del titular o un tercero autorizado a sus datos crediticios, debe de estar justificado de forma expresa, indicando los fines por los cuales se busca la autorización de acceso.

En este aspecto, una vez la entidad o el titular solicitante tenga acceso a los datos crediticios, estos estarán obligados a la protección y confidencialidad de la información obtenida, enmarcando sus actividades propiamente para el fin del análisis crediticio. Esto genera también, una prohibición expresa del fin de uso de datos con fines comerciales; delimitando las actuaciones por parte de las entidades a abstenerse de la venta de los datos personales obtenidos. En este mismo sentido, hay que señalar que no toda la información dentro de los burós crediticios puede ser de acceso para sus titulares o terceros autorizados. Esta información es conocida como información prohibida, misma que corresponde a la siguiente:

> 11.1. Aquella que pueda considerarse de carácter personal de conformidad con la Constitución de la República; el Código Orgánico Monetario y Financiero; y, otras leyes conexas, como por ejemplo características físicas, morales o emocionales de una persona, o cualquier otra información relacionada con circunstancias de su vida afectiva o familiar, hábitos personales y de consumo, ideologías, opiniones políticas, creencias o convicciones religiosas, estados de salud físico o psicológico, vida sexual o información genética, así como toda información que suponga una violación al derecho a la intimidad personal y familiar; y, a los derechos y garantías previstos por la Constitución de la República y las leyes, tratados y convenios internacionales relacionados con este tema;
>
> 11.2. La información que de conformidad con el Código Orgánico Monetario y Financiero, se encuentre protegida por el sigilo bancario; y,
>
> 11.3. La información del patrimonio personal y familiar del titular de la información,
>
> las cuales solo pueden ser entregadas por expresa orden judicial. (Codificación de las Normas de la Superintendencia de Bancos en su Libro I del Sistema Financiero, título IX, 2018, art. 11).

En este mismo sentido, dentro de cada entidad existe un responsable de brindar tratamiento a datos crediticios para articular, proporcionar y adecuar el tratamiento existe una subclasificación de los datos. Este tipo de acciones de clasificación, están

amparadas en el principio de seguridad, mismo que está regulado en la Ley Orgánica de Protección de Datos Personales, en el art. 37. Donde se establece que para brindar seguridad dentro del tratamiento de datos personales, no solo se debe contemplar el tipo de dato a tratar, sino la cantidad de datos, las particularidades del tratamiento y las partes involucradas. A modo de ejemplificar, la forma en la que se subclasifican los datos crediticios, se va a tomar la determinada en la Política de Privacidad de Equifax:

Tipo de dato crediticio	**Contenido**
Datos Identificativos	Son aquellos que permiten identificar a una persona, como son los "nombres, apellidos, documento de identidad" (Política de Privacidad de Equifax, 2025, apartado 2.3.1.).
Datos de Contacto	Son aquellos que permiten el contacto de la persona, como son la "dirección, teléfono, correo electrónico" (Política de Privacidad de Equifax, 2025, apartado 2.3.1.).
"Datos económicos, financieros o de seguros" (Política de Privacidad de Equifax, 2025, apartado 2.3.1.).	Estos datos versan sobre el ámbito patrimonial de la persona en interacción con los sectores "económico, financiero o de seguros" son recabados de instituciones públicas o privadas (Política de Privacidad de Equifax, 2025, apartado 2.3.1.).
Datos de riesgo crediticio	Este tipo de datos, "incluye todos los tipos de datos actuales e históricos identificados por la normativa antes citada y que permiten identificar adecuadamente a una persona y evaluar su riesgo crediticio, determinar sus niveles de endeudamiento, solvencia económica, así como su capacidad de endeudamiento y pago de obligaciones" (Política de Privacidad de Equifax, 2025, apartado 2.3.1.).

Nota: tabla realizada en base a la Política de Privacidad de Equifax.

2.1.2. Otros medios de obtención de los datos de los deudores en bases o sistemas informáticos ajenos a la empresa de factoring.

La información obtenida de los burós crediticios no es el único medio usado por las instituciones financieras, sino que, como señala Mancero (2024), estas "se han visto en la necesidad de desarrollar internamente procesos que permitan realizar una investigación más profunda sobre el posible cliente" (pág. 16).

Las fuentes de información para la construcción y actualización de perfiles crediticios, son medios de consulta que cumplen fines específicos. Primero, se debe de puntualizar que no existe una fuente única de obtención de datos, ni se constituye un solo proceso de recopilación; sino que, es un "proceso continuo que involucra múltiples partes y fuentes" (Faster Capital, 2025). Los actores dentro del sistema de obtención de este tipo de datos personales está conformado de la siguiente forma:

> Las entidades del sistema financiero nacional, del sector comercial y de servicios, del sector público, las compañías de seguro y reaseguro, las entidades sin fines de lucro que poseen información de riesgo crediticio y otras instituciones en las que registren obligaciones de pago (Mancero, S., 2024, pág. 11).

De forma general podemos establecer que existen dos tipos de fuentes de datos personales crediticios: "fuentes de acceso público o procedentes de informaciones facilitadas por el acreedor" (Ley Orgánica de Protección de Datos, 2021, art. 28). Las fuentes de acceso público, como su nombre lo indica no necesitan de la intervención del consentimiento del acreedor para su acceso. Mientras que las fuentes facilitadas por el usuario o titular, necesitan de forma obligatoria el consentimiento del acreedor para su acceso. Doctrinariamente, a las fuentes de acceso público también se les conoce como fuentes de obtención directa, mientras que, a las fuentes necesitan el consentimiento del usuario para su acceso como fuentes de acceso autorizado.

Ahora bien, dentro de este segundo tipo de fuentes, no basta con solicitar el acceso de la información del usuario o titular . Sino que es necesario, que la manifestación de de la voluntad cumpla con los siguientes requisitos:

Elemento de la voluntad	**Descripción del elemento**
Libre	La manifestación de la voluntad debe de estar "exenta de vicios del consentimiento" (2018, art. 18).
Específico	La manifestación de la voluntad debe de ser "concreta de los medios y fines del tratamiento" (2018, art. 18).
Informado	La manifestación de la voluntad debe de cumplir el principio y derecho de transparencia.
Inequívoco	En la manifestación de la voluntad, "no se deben de presentar dudas sobre el alcance de la autorización otorgada por el titular" (2018, art. 18).

Nota: tabla realizada en base la Codificación de las Normas de la Superintendencia de Bancos en su Libro I del Sistema Financiero, título IX, 2018, art. 8

Cabe señalar que el titular o usuario en cualquier momento podrá revocar su consentimiento, sin la necesidad de manifestar los motivos que justifiquen la revocatoria. "El tratamiento realizado antes de revocar el consentimiento es lícito, en virtud de que este no tiene efectos retroactivos" (Codificación de las Normas de la Superintendencia de Bancos en su Libro I del Sistema Financiero, título IX, 2018, art. 8).

2.1.3. Uso de datos de los deudores desde la base de legitimidad de la Ley de Protección de Datos.

Previa suscripción del contrato de factoring o endoso, por la naturaleza comercial del contrato, el posible factor debe contar con una evaluación de la gestión de riesgo de los derechos crediticios que va a adquirir. Esta evaluación, no solo permitirá identificar si es

existente o no la idoneidad comercial del contrato, sino le permitirá evaluar el tipo de acciones que este deberá de realizar para poder efectuarse el cobro del valor contenido en la o las facturas comerciales negociables. En virtud que, como lo contempla el Código de Comercio, este tipo de contrato cubre la "cesión de cualquier tipo de derechos de cobro y sus operaciones conexas" (2019, art. 667).

Una vez el factor se ha posicionado como parte contractual, será éste quien jurídicamente se encuentre en el rol de ser un nuevo acreedor, desplazando al cedente. Con el contrato o endoso, también se transfieren los datos personales, esto con el fin de dar cumplimiento al cobro de la factura. Con este rol, será necesario que el factor cuente con los recursos que permitan identificar al deudor; para esto, "el cedente o endosante no tiene responsabilidades con los pormenores relacionados con la identificación del deudor, salvo que el adquirente demuestre dolo en los datos proporcionados" (Código de Comercio, 2019, art. 669).

La legitimidad de la cesión de datos personales dentro del contrato de factoring, no sólo encuentra su respaldo, al mencionar que en este tipo de contrato en el Código de Comercio, cede al factor el derecho de cobro y operaciones relacionadas a este derecho. Es por la naturaleza de la cesión de derechos, que se transfiere que se transfiere su titularidad. Al ser el factor, el nuevo acreedor dentro de una deuda, también se vuelve el nuevo encargado del tratamiento de protección de datos. Este tratamiento, tiene que respaldar un fin legítimo, que en este caso sería el cobro de la cartera de facturas negociables comerciables.

Ahora bien, la legitimidad como principio estructural en las actuaciones por parte de los encargados de suministrar datos personales, permite dimensionar al derecho a la protección de datos como derecho fundamental, con requisitos de cumplimiento de tratamiento y limitaciones. Las instituciones que manejen datos personales deberán de

sustentar sus actuaciones respecto al tratamiento durante el ciclo de vida del dato de "forma leal y ampararse en una base jurídica de legitimación para dicho tratamiento" (Barrio, M., 2024, pág. 6). Al tener su base en el derecho de intimidad, debe cumplir con los "fines legítimos específicos y explícitos"(RGPD, art. 5, apdo. 1, letra b) para los que fueron recolectados. En el caso de una cesión de derecho de crédito, la finalidad legítima del factor es que el deudor cumpla con su obligación de pago derivada de la factura o facturas negociables comerciables.

2.1.4. Medidas de gestión de riesgo y manejo de seguridad de datos personales y crediticios

El fin por el que los datos fueron recopilados por el cedente no ha cambiado al ser adquiridos por el factor. Cabe señalar que para que exista cumplimiento normativo, no solo es necesario contar con un fin legítimo; sino que, obligatoriamente, debe de implementarse al tratamiento una gestión de riesgos. Esto con el objetivo principal de salvaguardar los derechos de los deudores, quienes fungen el rol de titulares en cuanto a su derecho de protección de datos. Otro de los objetivos, se enmarca dentro establecer y posteriormente preservar la imágen empresarial de la empresa de factoraje o IFIS, frente a empresas nacionales o internacionales, sobre el correcto funcionamiento interno ante la implementación y cumplimiento de buenas prácticas. Esto entendiendo, que en el ámbito de interacción empresarial se busca mitigar riesgos cuando existen asociaciones; y el cumplimiento de estándares en protección de datos recubre la imagen de una empresa o IFIS de seguridad jurídica y social para realizar una asociación empresarial.

Como partes involucradas y obligadas a realizar e implementar medidas que mitiguen el riesgo del tratamiento son los responsables y encargados del tratamiento. Que, al subsumir la norma en el funcionamiento del contrato de factoring, podríamos señalar que son, en el caso del responsable, la empresa que ha comprado la cartera de facturas

comerciales negociables, esta puede ser una empresa habilitada para actividades de factoraje o una IFIS. Mientras que, como encargados del tratamiento, tenemos que establecer el contexto del margen de actuación empresarial, en el que el factor derive a terceros el acceso de datos con el fin de cobrar la obligación pendiente. Este acceso por parte de los encargados debe permitir la gestión de los servicios.

Aquí hay que puntualizar que la gestión de riesgo debe de ser conjunta, informada e interdependiente entre responsables y encargados de tratamiento de datos. Esto al entender que por medio de una gestión de riesgo se busca "disminuir la incertidumbre para tomar decisiones informadas en la implementación de medidas de seguridad en el tratamiento de datos personales" (Guía de Gestión de Riesgos e Impacto de Inversión, 2025, pág. 11). Para que se pueda implementar de forma correcta una gestión de riesgos, se deben de contemplar 5 etapas de implementación, mismas que son, "establecimiento del contexto, identificación de riesgos, análisis de riesgos, evaluación de riesgos y tratamiento de riesgos" (Guía de Gestión de Riesgos e Impacto de Inversión, 2025, pág. 11).

En cada etapa, se deberán de implementar parámetros de evaluación de la gestión del riesgo. Algunos de los parámetros en España por la Agencia Española de Protección de Datos (AEPD) y en Ecuador por la Superintendencia de Datos utilizados como métricas en la gestión de riesgos son:

Clasificación de parámetros de metraje en la gestión de riesgo de los datos personales	
Agencia Española de Protección de Datos (AEPD)	Superintendencia de Protección de datos (SPDP)
Tipo de factor de riesgo y la posibilidad de que el riesgo se materialice	Tipo de estándares de privacidad y seguridad interna. Este parámetro hace referencia no solo al cumplimeito

Clasificación de parámetros de metraje en la gestión de riesgo de los datos personales	
	normativo, sino a que las empresas o instituciones manejen “estándares de mejores prácticas” (SPDP, 2025, pág. 11) como sistemas de seguridad, un ejemplo de estándar, es el cumplimiento de las normas ISO/IEC 27001.
Nivel de impacto en caso de concretarse el riesgo y su nivel de afectación a los derechos de los usuarios.	Identificación de responsables y encargados en la gestión de riesgos
Identificación de factores de riesgo por áreas	“Integración de la gestión de riesgos para la protección de derechos y libertades” (SPDP, 2025, pág. 11): Este parámetro hace referencia a los tipos de seguridad que son considerados para la gestión de riesgo. Algunos tipos de seguridad pueden ser en los sistemas de almacenamiento y en temas jurídicos
Extensión y alcance del tratamiento	Grado de interdependencia e integración en áreas encargadas de gestionar el riesgo
Categoría del dato a tratar	Escenarios de riesgo y respuestas frente a que estos se concreten
Medios de almacenamiento físicos o virtuales de datos	Clasificación de tipo de dato
Departamentos encargados de la gestión del tratamiento en cualquiera de sus etapas	Clasificación de tipos de riesgo
Este parámetro contempla la evaluación continua de los parámetros en cada etapa se proporciona un seguimiento oportuno desde la “evolución de la probabilidad” (AEPD, 2021, pág. 96)	Tipos de auditorías aplicadas y establecimiento de periodos de auditorías.

Cabe señalar, que estos parámetros forman parte de las guías de gestión de riesgo emitidas por la AEPD y la SPDP. En las prácticas las instituciones y empresas que manejen datos podrán implementar los mismos o diferentes parámetros de metraje de la

gestión de riesgos; esto siempre que se cumplan los principios generales en protección de datos y los de gestión de riesgos en el manejo de datos personales.

Los parámetros utilizados pueden variar dependiendo de la estructura interna de cada institución y los fines de uso de los datos. Autores como Freund, J., Jones, J. (2015), consideran que para evaluar el riesgo hay que considerar 5 factores principales:

- Identificación del problema que se constituye como un riesgo.
- Analizar el área de afectación y su impacto.
- Identificar opciones de tratamiento para mitigar o tratar el problema del riesgo.
- Sobre las opciones identificadas, seleccionar cuáles responderían como la mejor opción de implementación.
- Generar una comunicación interdependiente de los resultados y recomendaciones de los parámetros anteriores (pág. 6).

Para la verificación de una correcta gestión de riesgos, deben de realizarse obligatoriamente auditorías periódicas, permanentes, jurídicas, organizacionales y técnicas, según la Guía de Gestión de Riesgo y Evaluación del Impacto del Tratamiento de Datos Personales, misma que fue emitida por la Superintendencia de Datos en 2025. Ahora bien, la gestión de riesgo dentro de la normativa de la Ley Orgánica de Protección de Datos Personales, establece como obligaciones las siguientes:

Tipo de obligación	**Persona sobre la que recae la obligación**	**Contenido**	**Agentes de control y regulación**
Obligación de implementar medidas de seguridad para el tratamiento	Responsable y encargado del tratamiento de datos	Para el tratamiento de protección de datos el responsable o encargado deberá de aplicar al tratamiento el principio de seguridad, donde en cada etapa se deberá de evaluar “las categorías y volumen de datos personales, el estado de la técnica, mejores prácticas de	Autoridad de Protección de Datos Personales

		seguridad integral y los costos de aplicación de acuerdo a la naturaleza, alcance, contexto y los fines del tratamiento, así como identificar la probabilidad de riesgos" (LOPDP, 2021, art. 37).	
Obligación de implementación del principio de privacidad desde el diseño y por defecto	Responsable del tratamiento de datos	El principio de privacidad desde el diseño y por defecto deberá ser implementado en todo el ciclo de vida del dato. Se entiende desde el diseño a " el deber del responsable del tratamiento de tener en cuenta, en las primeras fases de concepción y diseño del proyecto" (LOPDP, 2021, art. 39). Mientras que por defecto, "hace referencia a que el responsable debe aplicar las medidas técnicas y organizativas adecuadas con miras a que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines del tratamiento, en los términos del reglamento" (LOPDP, 2021, art. 39).	Autoridad de Protección de Datos Personales
Obligación de obligación de impacto del tratamiento de datos personales	Responsable del tratamiento de datos	Esta obligación surge ante los posibles escenarios: 1) cuando la Autoridad de Protección de Datos lo solicite; 2) cuando el tratamiento pueda implicar un "alto riesgo para los derechos y libertades del titular"(LOPDP, 2021, art. 42); 3) el tratamiento de datos vaya a implicar "Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado"(LOPDP, 2021, art. 42); 4) el tratamiento de datos que se vaya a efectuar es a "gran escala de categorías especiales de datos" (LOPDP,	Autoridad de Protección de Datos Personales

		2021, art. 42) y 5) “Observación sistemática a gran escala de una zona de acceso público” (LOPDP, 2021, art. 42).	
Obligación de inventariar el tratamiento y sistemas de soporte	Responsable del tratamiento de datos	Esta obligación se encuentra inmersa en el “Registro Nacional de protección de datos personales”. El contenido de esta obligación es “reportar y mantener actualizada la información ante la Autoridad de Protección de Datos Personales” (LOPDP, 2021, art. 51)	Autoridad de Protección de Datos Personales
Obligación de comunicación cuando exista una violación de la seguridad	Responsable del tratamiento del dato	En caso de producirse una vulneración a la seguridad, el responsable tendrá la obligación de “ notificar la vulneración de la seguridad de datos personales a la Autoridad de Protección de Datos Personales y la Agencia de Regulación y Control de las Telecomunicaciones, tan pronto sea posible, y a más tardar en el término de cinco (5) días después de que haya tenido constancia de ella” (LOPDP, 2021, art. 43). Mientras que, la notificación al titular deberá ser de inmediato o en un término de 3 días después de haber tenido constancia de la vulneración (LOPDP, 2021, art. 46).	Autoridad de Protección de Datos Personales y Agencia de Regulación y Control de Telecomunicaciones

3. Conclusiones

3.1. En el contrato de factoring con los derechos crediticios se ceden también datos de los deudores. En el proceso de esta cesión o endoso no se debe de contar como requisito el consentimiento por parte del deudor. Esto al entender, que el consentimiento se dió previamente dentro de facturas comerciales negociables. Y en cumplimiento del fin de poder ejecutar el cobro de la deuda contenida en el título valor. Que la cesión sea legítima, hace que el factor sea el nuevo responsable en salvaguardar los derechos de los deudores, haciendo de este responsable de la gestión de riesgo del dato personal. Esto hace necesario que el factor deba de cumplir con parámetros de gestión de riesgo que deberán de ser evaluados de forma continua hasta la ejecución del cobro.

3.2. La ejecución del cobro hace necesaria la implementación de operaciones conexas que permitan este fin. Para que estas operaciones conexas sean realizadas, se deberán de manejar datos de los deudores. Donde terceros al factor serán encargados del tratamiento de datos con el fin de gestión del cobro. Estas empresas de forma interdependiente con el factor deberán de tomar decisiones conjuntas para salvaguardar el cumplimiento de parámetros de seguridad, implementando protocolos específicos Estas acciones deberán de ser realizadas con equipos multidisciplinarios para asegurar la cobertura efectiva del riesgo.

3.3. Los datos que son manejados con el fin de ejecutar la deuda son de tipo crediticios y personales. El tratamiento que se debe de suministrar por parte de responsables y encargados deben de ser afines al cumplimiento de la normativa de las Superintendencias de Datos, Superintendencia de Bancos y la Junta de Política y Regulación Financiera. Esto implica que debe de existir un manejo interinstitucional de control para este tipo de contratos. Este manejo interinstitucional debe de darse de forma continua durante todas las etapas del ciclo del dato, hasta que en la etapa final el dato sea archivado o destruido por parte de las empresas responsables y encargadas.

4. Bibliografía

4.1.1. Accessnow, La creación de un marco para la protección de datos: una guía para los legisladores sobre qué hacer y qué no, (2018).

4.1.2. Agencia Española de Protección de Datos. (junio de 2021). Gestión del riesgo y evaluación de impacto en tratamientos de datos personales (Guía). AEPD. https://www.aepd.es/sites/default/files/2021-06/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf

4.1.3. Agencia Española de Protección de Datos (AEPD). (2020). Guía para la implementación de la protección de datos desde el diseño y por defecto. https://www.aepd.es/guias/guia-proteccion-datos-por-defecto.pdf

4.1.4. Asamblea Constituyente de Ecuador. (1830). Constitución Política de la República del Ecuador [1830]. Ministerio de Gobierno de Ecuador. Art. 56 https://www.ministeriodegobierno.gob.ec/wp-content/uploads/downloads/2014/03/CONSTITUCIO%CC%81N-POLI%CC%81TICA-DEL-AN%CC%83O-1830.pdf

4.1.5. Asamblea Nacional del Ecuador. (1998). Constitución Política de la República del Ecuador (Registro Oficial Suplemento No. 1, 11 de agosto de 1998).

4.1.6. Asamblea Nacional del Ecuador. (2019). Código de Comercio. RO 497 de 29 de mayo de 2019.

4.1.7. Asamblea Nacional del Ecuador. (2021). Ley Orgánica de Protección de Datos Personales.

4.1.8. Asociación de Bancos Privados del Ecuador (ASOBANCA). (2023). *Política de protección de datos personales* [PDF]. https://asobanca.org.ec/wp-content/uploads/2023/09/Politica-de-Proteccion-de-Datos.pdf

4.1.9. Barrio Andrés, M. (2024, febrero). Los principios estructurales del Reglamento General de Protección de Datos. Actualidad Jurídica Iberoamericana (N.º 20), 1322–1341. https://revista-aji.com/wp-content/uploads/2024/02/AJI20_Art_42.pdf

4.1.10. Cotino Hueso, L., García Mahamut, R., Medina Guerrero, M., Lucas Murillo de la Cueva, P., Rallo Lombarte, A., Rebollo Delgado, L., Troncoso Reigada, A., & Vidal Fueyo, M. del C. (2020). Encuesta sobre la protección de datos personales. *Teoría y Realidad Constitucional*, (46), 15–118.

4.1.11. Counsil of Eupore (2018). Convention for the protection of individuals with regard to the processing of personal data. Enlace de acceso: 16808b36f1 (coe.int)

4.1.12. Consejo de la Unión Europea. (s.f.). Los Tratados de Maastricht y Ámsterdam. Parlamento Europeo.

https://www.europarl.europa.eu/factsheets/es/sheet/3/los-tratados-de-maastricht-y-amsterdam

4.1.13. Datenschutzgesetz vom 7. Oktober 1970 [Ley de protección de datos de 7 de octubre de 1970]. GVOBl. HE I, 12 de octubre 1970, Nr. 41, p. 625.

4.1.14. Datalagen, 1973 [Ley de protección de datos de 1973], art. 6.

4.1.15. DLA Piper. (2025). Ecuador. En Data Protection Laws of the World (14ª ed.). Recuperado de https://www.dlapiperdataprotection.com

4.1.16. European Union. (n.d.). Treaty on European Union (Maastricht Treaty) – 1992. En Founding agreements [sitio web de la UE]. (Consultado el 28 abril de 2025).

4.1.17. Equifax Ecuador C.A. (s. f.). *Política de privacidad y protección de datos personales*. Recuperado el 4 de julio de 2025, de https://www.equifax.ec/legal/politica-de-privacidad/

4.1.18. FasterCapital. (2025). Datos crediticios: cómo recopilar y gestionar sus datos crediticios de forma eficaz. Recuperdado en julio de 2025 de, https://fastercapital.com/es/contenido/Datos-crediticios--como-recopilar-y-gestionar-sus-datos-crediticios-de-forma-eficaz.html

4.1.19. Gibello, V., & Moritz, M. (2017). El Reglamento Europeo (UE) 2016/679: análisis de un claroscuro. Foro, (27), 115–128. Universidad Andina Simón Bolívar. https://repositorio.uasb.edu.ec/bitstream/10644/5948/1/08-TC-Moritz-Gibello.pdf

4.1.20. Huerta, P. P. (2016). La génesis del derecho fundamental a la protección de datos personales (Doctoral dissertation, Universidad Complutense de Madrid).

4.1.21. J. Schwabe (comp.) (2009). Jurisprudencia del Tribunal Constitucional Federal Alemán (págs. 94-102), (pág. usada 94). Berlín: Ed. Konrad Adenauer Stiftung.

4.1.22. Cruz Villalón, P. (1989). Formación y evolución de los derechos fundamentales. Revista Española de Derecho Constitucional, 9(25), 45-78.

4.1.23. Principios Unidroit sobre los Contratos Comerciales Internacionales (2016). Enlace de acceso: Microsoft Word - Black-letter rules Spanish.docx (unidroit.org) (softlaw).

4.1.24. European Union. (n.d.). Treaty on European Union (Maastricht Treaty) – 1992. En Founding agreements [sitio web de la UE]. (Consultado el 28 abril de 2025).

4.1.25. Freund, J., & Jones, J. (2014). Measuring and managing information risk: A FAIR approach (1.ª ed.). Butterworth-Heinemann. ISBN 978-0124202313

4.1.26. UNED. Teoría y Realidad Constitucional, Encuesta sobre la protección de datos personales. núm. 46, 2020, ISSN 1139-5583, pp. 15-118
4.1.27. Organización de los Estados Americanos – OEA. (2021). Principios actualizados sobre la privacidad y la protección de datos personales (OEA/Ser.D/XIX.20). Departamento de Derecho Internacional, Secretaría de Asuntos Jurídicos.
4.1.28. Organización para la Cooperación y el Desarrollo Económicos (OCDE). (2013). Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales. https://www.oas.org/es/sla/ddi/docs/Directrices_OCDE_privacidad.pdf
4.1.29. OECD, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data,2023.
4.1.30. Idrovo, E. y Barona, K. (2021). El contrato de factoring: una herramienta subestimada en el Ecuador. Revista Ruptura de la Asociación Escuela de Derecho PUCE. Edición 2021, p (411-460).
4.1.31. Presidencia de la República del Ecuador. (13 de noviembre de 2023). Decreto Ejecutivo No. 904: Reglamento General de la Ley Orgánica de Protección de Datos Personales. Tercer Suplemento del Registro Oficial No. 435.
4.1.32. Unión Europea. (s.f.). Protección de datos - RGPD. Europa.eu. https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_es.htm
4.1.33. Martínez Pérez, O., Freire Gaibor, E. F., & Alzate Peralta, L. A. (2024). Desafíos del habeas data en la protección de datos personales en el ordenamiento jurídico ecuatoriano. European Public & Social Innovation Review, 1–21. https://doi.org/10.31637/epsir-2024-1842
4.1.34. Mayorga-Jácome, T. C., Carrión-Jumbo, J. L., García-Jiménez, M., Yarad-Jeada, P. V., & Duret-Gutiérrez, J. F. (2019). Historia de la normativa reguladora de la protección de datos de carácter personal en distintos países latinoamericanos. Dominio de las Ciencias, *5*(1), 518–537. http://dx.doi.org/10.23857/dom.cien.pocaip.2019.vol.5.n.1.518-537
4.1.35. Mazzeo, J. V., Moyano Ruiz, M. L., & Nara, C. N. (2012). Factoring: liquidez para las empresas (Trabajo final de grado). Universidad Nacional de Cuyo, Facultad de Ciencias Económicas. Disponible en https://bdigital.uncu.edu.ar/5156
4.1.36. Mieres, L., & Vilasau, M. (2018). Introducción al marco legal de la protección de datos: Módulo didáctico 1 - El nacimiento y la evolución del derecho a la protección de datos. Universitat Oberta de Catalunya (UOC). https://openaccess.uoc.edu/bitstream/10609/140786/1/Introducci

%c3%b3n%20al%20marco%20legal%20de%20la%20protecci%c3%b3n%20de%20datos_M%c3%b3dulo%20did%c3%a1ctico%201_El%20nacimiento%20y%20la%20evoluci%c3%b3n%20del%20derecho%20a%20la%20protecci%c3%b3n%20de%20datos.pdf

4.1.37. Moscoso León, J. D. (2025). Evaluación jurídica de riesgos y vulnerabilidades en la protección de datos en instituciones financieras del Ecuador bajo la Ley Orgánica de Protección de Datos Personales (Tesis de grado, Universidad Católica de Cuenca). https://dspace.ucacue.edu.ec/server/api/core/bitstreams/de4b613c-519b-4f9c-9852-8d18ac21e733/content

4.1.38. Naranjo Godoy, L. (2019). El contenido esencial del derecho a la protección de datos personales en el Ecuador a la luz de los modelos europeo, norteamericano y latinoamericano [Tesis doctoral, Universidad Pablo de Olavide].

4.1.39. Naranjo Godoy, L. (2017). El dato personal como presupuesto del derecho a la protección de datos personales y del hábeas data en Ecuador. FORO. Revista de Derecho.

4.1.40. Roldán Carrillo, F. N. (2021). Los ejes centrales de la protección de datos: consentimiento y finalidad. Críticas y propuestas hacia una regulación de la protección de datos personales en Ecuador. Universitas. Revista de Ciencias Sociales y Humanas, *8*(1). https://doi.org/10.18272/ulr.v8i1.2184

4.1.41. Rosas-Lanas, G., & Pila-Cárdenas, G. (2023). La protección de datos personales en Ecuador: Una revisión histórica-normativa de este derecho fundamental en el país suramericano.

4.1.42. Samaniego Nugra, E., Reina Cunín, J., & Loyola Moreano, K. (2021). Habeas Data: origen y evolución. Lex: Revista de la Facultad de Jurisprudencia, 4(13), 197–210. https://doi.org/10.33996/revistalex.v4i13.82

4.1.43. Superintendencia de Bancos. (2018). Codificación de las normas de la Superintendencia de Bancos. Libro I del Sistema Financiero, Título IX. Quito, Ecuador.

4.1.44. Superintendencia de Protección de Datos Personales. (mayo de 2025). *Guía de gestión de riesgos y evaluación de impacto del tratamiento de datos personales* (Versión 1). SPDP. https://spdp.gob.ec/wp-content/uploads/2025/05/GUIA-DE-GESTION-DE-RIESGOS-E-IMPACTO-VERSION-1.pdf

4.1.45. Universidad Regional Autónoma de los Andes. (2025). *La protección de datos personales crediticios y la administración del riesgo operacional* (Trabajo de titulación vía DSpace, UA-MCL-EAC-013-2025). https://dspace.uniandes.edu.ec/bitstream/123456789/18758/1/UA-MCL-EAC-013-2025.pdf

4.1.46. Uribe Vargas, H. (2015). El contrato de factoring: apuntes y comentarios. Criterios: Cuadernos de Ciencias Jurídicas y Política Internacional, 8(2), 19–70.
4.1.47. Ordóñez Pineda, L. O. (2020). El derecho fundamental a la protección de datos personales en Ecuador. Situación actual y presupuestos para la formulación de un marco jurídico que asegure un nivel adecuado de protección [Tesis doctoral, Universidad de Cádiz].
4.1.48. Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. Harvard Law Review, 4(5), 193-220. https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf