
COMPLIANCE Y PROTECCIÓN DE DATOS EN COLOMBIA

Régimen Nacional, Marco Europeo y Perspectiva Norteamericana

*Tratado sistemático sobre el cumplimiento normativo, la responsabilidad de las personas
jurídicas y el tratamiento de datos personales en perspectiva comparada*

1ra edición 2026

I.S.B.N 978-628-7920-11-8
I.S.B.N Digital 978-628-7920-12-5

© André Alfaro Rodríguez 2026
© Editorial Diké S.A.S. 2026
www.editorialdike.co

Editorial Diké S.A.S.

Cel.: 301 242 7399 - e-mail: dikesascomercial@gmail.com
Medellín - Colombia

Bogotá D.C. Librería

Calle 23 sur # 27- 41 Barrio Santander
Cel.: 301 242 7399 - e-mail: dikesasgerencia@gmail.com

San José de Costa Rica

Teléfono: 83 02 10 54 - Telefax: 22 14 25 23
e-mail: jadguzman@yahoo.com
editorialdike@hotmail.com

Caracas-Venezuela

Av. Urdaneta, esq. Ibarras, edf. Pasaje la Seguridad, P.B. Local 19, Caracas 1010 / info@paredes.com.ve / Tels.: 58 (212) 564-15-05 / 563-55-90/06-04
RIF: J-30797099-5

Panamá

Calle Parita, Bulevar Ancón, Casa 503, Corregimiento de Ancón, Ciudad de Panamá.
Tel.: 50767814196 / borisbarrios@lawyer.com

Diseño y diagramación

Lucio F. Chunga Cheng
e-mail: dikesas.diagramacion@gmail.com

Diseño de portada

Sandra Marcela Londoño Restrepo. Cel: 315 427 6687
email: sandramarcela03@gmail.com

Compliance y Protección de datos en Colombia. Régimen Nacional, Marco Europeo y Perspectiva Norteamericana. Tratado sistemático sobre el cumplimiento normativo, la responsabilidad de las personas jurídicas y el tratamiento de datos personales en perspectiva comparada 1ra edición impresa en septiembre del 2026.

La impresión de esta obra se terminó en los talleres de Editorial Diké S.A.S. Calle 23 Sur # 27- 41 Barrio Santander. Cel.: 301 242 7399 e-mail: dikesasgerencia@gmail.com -- www.editorialdike.co

Reservados todos los derechos. No se permite la reproducción total o parcial de esta obra, ni su incorporación a un sistema informático, ni su transmisión en cualquier forma o por cualquier medio, sin la autorización previa y por escrito del titular del copyright.

Advertencia sobre la fecha de cierre. Esta obra fue cerrada con la legislación, la jurisprudencia y la doctrina disponibles a comienzos de 2026. El proyecto de reforma de la Ley Estatutaria 1581 de 2012, examinado en la Parte Segunda, se hallaba en trámite legislativo a la fecha de cierre; su contenido definitivo, sujeto al procedimiento estatutario y al control previo de constitucionalidad, deberá verificarse en el momento de la consulta.

Autor

ANDRÉ ALFAR RODRIGUES

COMPLIANCE Y PROTECCIÓN DE DATOS EN COLOMBIA

Régimen Nacional, Marco Europeo y Perspectiva Norteamericana

*Tratado sistemático sobre el cumplimiento normativo, la responsabilidad de las personas
jurídicas y el tratamiento de datos personales en perspectiva comparada*

1ra edición 2026



Editorial Diké S.A.S.

Eduardo Quiceno Álvarez
Presidente Honorario del Comité Editorial

Tabla de Contenido

Parte Preliminar

Fundamentos del compliance y de la autodeterminación informativa	17
---	-----------

Capítulo I.

El compliance como categoría jurídica: concepto, evolución y funciones	19
1. Aproximación terminológica y problema de la traducción del concepto	19
1.1. «Compliance», «cumplimiento normativo» y «debido control»: delimitación semántica	19
1.1.1. <i>La insuficiencia de la traducción literal y sus consecuencias dogmáticas</i>	19
1.1.2. <i>El compliance como concepto funcional y no meramente escriptivo</i>	20
1.2. Compliance en sentido estricto y en sentido amplio	21
2. Génesis histórica: del mundo anglosajón a la recepción en el civil law	22
2.1. Los orígenes en el Derecho estadounidense de la regulación económica	22
2.1.1. <i>Las Federal Sentencing Guidelines de 1991 como punto de inflexión</i>	22
2.1.2. <i>La influencia del escándalo corporativo y la Sarbanes-Oxley Act de 2002</i>	23
2.2. La difusión europea y la construcción del criminal compliance	23
2.3. La recepción latinoamericana y el caso colombiano	24
3. Fundamento y funciones del sistema de cumplimiento	25
3.3.1. <i>La función preventiva y la gestión anticipada del riesgo jurídico</i>	25
3.1. La función de detección temprana y de reacción interna	25
3.2. La función de confirmación del Derecho y de refuerzo de la cultura de legalidad	26
3.3. La dimensión reputacional y su valor económico	27
4. La función de cumplimiento en la estructura organizativa	27
4.1. Autonomía, independencia y suficiencia de recursos	27
4.2. Líneas de reporte y posición del compliance officer	28
4.3. El «tone at the top» y la responsabilidad del órgano de administración	29

Capítulo II.

Fundamentos constitucionales y axiológicos en el ordenamiento colombiano	31
1. El Estado social de derecho y la actividad empresarial	31
1.1. Libertad de empresa y función social de la iniciativa privada (art. 333 C.P.)	31
1.2. Intervención del Estado en la economía y regulación del riesgo	32

2.	Garantías constitucionales en el ejercicio del ius puniendi administrativo	32
2.1.	Debido proceso, legalidad y tipicidad en el derecho administrativo sancionador	32
2.2.	Culpabilidad, proporcionalidad y non bis in idem	33
3.	El bloque de constitucionalidad y la recepción de estándares internacionales.....	34
3.1.	Concepto y alcance del bloque de constitucionalidad	34
3.2.	Convenios anticorrupción y su fuerza normativa interna.....	34

Parte Primera

El régimen de compliance en Colombia.....	37
--	-----------

Capítulo III.

La responsabilidad de las personas jurídicas como presupuesto del compliance	39
1. El debate dogmático sobre la responsabilidad del ente colectivo	39
1.1. El principio <i>societas delinquere non potest</i> y su erosión.....	39
1.1.1. <i>Objeciones dogmáticas: acción, culpabilidad y pena</i>	40
1.1.2. <i>Respuestas de la doctrina y modelos de superación</i>	40
2. El sistema colombiano de responsabilidad de la persona jurídica.....	42
2.1. La responsabilidad administrativa como eje del modelo colombiano.....	42
2.2. La discusión sobre la responsabilidad penal de la persona jurídica en Colombia.....	43
2.3. Responsabilidad de administradores y deberes fiduciarios (Ley 222 de 1995)..	43
3. El defecto de organización y el valor eximente o atenuante del programa	44

Capítulo IV.

Los marcos normativos sectoriales de cumplimiento en Colombia.....	47
1. El régimen de prevención de LA/FT/FPADM: visión de conjunto.....	47
1.1. Marco internacional: GAFI y las 40 Recomendaciones.....	47
1.2. Arquitectura institucional: UIAF, Superintendencias y régimen de reporte	48
2. El SAGRILAF de la Superintendencia de Sociedades	48
2.1. Ámbito de aplicación y empresas obligadas	48
2.2. Elementos del sistema y debida diligencia	49
2.3. El oficial de cumplimiento en el SAGRILAF	50
2.4. Régimen de reportes y operaciones sospechosas	50
3. El SARLAF en el sector financiero vigilado.....	51
3.1. Origen y evolución del SARLAF.....	51
3.2. Etapas de administración del riesgo	51
3.3. Debida diligencia intensificada y personas expuestas políticamente	52
4. Los Programas de Transparencia y Ética Empresarial (PTEE).....	52

4.1.	Fundamento y destinatarios.....	52
4.2.	Relación con el riesgo de soborno transnacional	53
5.	La responsabilidad por soborno transnacional: la Ley 1778 de 2016	53
5.1.	Conducta típica y sujetos responsables	53
5.2.	Régimen sancionador y criterios de graduación.....	54
5.3.	El programa de cumplimiento como circunstancia relevante.....	55
6.	El Estatuto Anticorrupción (Ley 1474 de 2011) y su desarrollo posterior	55
6.1.	Medidas administrativas, penales y disciplinarias.....	55
6.2.	Articulación con la contratación estatal.....	56

Capítulo V.

Los elementos del programa de cumplimiento efectivo.....	57
1. El compromiso de la alta dirección y el gobierno corporativo.....	57
1.1. Deberes del órgano de administración en materia de cumplimiento.....	57
1.2. Comités de auditoría y de riesgos.....	58
2. La evaluación y la matriz de riesgos	58
2.1. Metodologías de identificación, medición y control	58
2.2. El riesgo residual y el apetito de riesgo.....	59
3. Políticas, códigos de conducta y controles internos	59
4. El oficial de cumplimiento: estatuto, deberes y responsabilidad.....	60
4.1. Requisitos, nombramiento e independencia	60
4.2. Régimen de responsabilidad personal del compliance officer.....	61
5. La debida diligencia de terceros y de la cadena de valor	61
6. Los canales de denuncia y la protección del denunciante	62
6.1. Diseño, confidencialidad y prohibición de represalias	62
6.2. Tratamiento de datos personales en los canales de denuncia	63
7. Las investigaciones internas	63
7.1. Garantías del investigado y valor probatorio.....	63
7.2. Conflicto con derechos fundamentales y con la protección de datos	64
8. Formación, comunicación, monitoreo y mejora continua	65

Parte Segunda

La protección de datos personales en Colombia	67
--	-----------

Capítulo VI.

El derecho fundamental al habeas data y su desarrollo legislativo.....	69
1. Fundamento constitucional: el artículo 15 de la Constitución de 1991.....	69
1.1. Intimidad, buen nombre y autodeterminación informativa	69
1.1.1. <i>La triple dimensión del artículo 15.....</i>	<i>69</i>
1.1.2. <i>La autodeterminación informativa como derecho autónomo</i>	<i>70</i>

1.2.	La jurisprudencia constitucional configuradora del habeas data	71
1.2.1.	<i>Las sentencias fundacionales</i>	71
1.2.2.	<i>La acción de tutela como cauce procesal del habeas data</i>	71
2.	El doble régimen: Ley 1266 de 2008 y Ley 1581 de 2012	72
2.1.	El habeas data financiero (Ley 1266 de 2008)	72
2.1.1.	<i>Ámbito: información financiera, crediticia y comercial</i>	72
2.1.2.	<i>El principio de caducidad del dato negativo</i>	72
2.2.	El régimen general de protección de datos (Ley 1581 de 2012)	73
2.2.1.	<i>Naturaleza estatutaria y control previo de constitucionalidad</i>	73
2.2.2.	<i>Desarrollo reglamentario: Decreto 1377 de 2013 y Decreto 1074 de 2015</i>	73

Capítulo VII.

El régimen sustantivo del tratamiento de datos personales	75
1. Ámbito de aplicación y definiciones legales	75
1.1. Ámbito material y territorial.....	75
1.2. Dato personal, dato sensible y dato semiprivado	76
1.2.1. <i>La categoría del dato personal</i>	76
1.2.2. <i>Los datos sensibles y su régimen reforzado</i>	76
1.2.3. <i>La clasificación tripartita heredada de la jurisprudencia: público, semiprivado y privado</i>	77
1.3. Responsable, encargado y titular	78
2. Los principios rectores del tratamiento	78
2.1. Legalidad, finalidad y libertad	78
2.1.1. <i>El principio de finalidad como eje del sistema</i>	78
2.1.2. <i>El principio de libertad y el papel del consentimiento</i>	79
2.2. Veracidad, transparencia y acceso restringido	79
2.3. Seguridad y confidencialidad	80
3. La autorización del titular como base del tratamiento.....	80
3.1. Requisitos, forma y prueba del consentimiento	80
3.2. El tratamiento de datos sensibles y de menores de edad	81
3.2.1. <i>La prohibición matizada del dato sensible</i>	81
3.2.2. <i>El interés superior del menor en el tratamiento de sus datos</i>	81
4. Deberes de responsables y encargados	82
5. Los derechos del titular y los mecanismos de garantía	83
5.1. Conocer, actualizar, rectificar y suprimir.....	83
5.2. El reclamo y la consulta como mecanismos administrativos	83
5.3. La acción de tutela como garantía constitucional.....	84
6. El Registro Nacional de Bases de Datos	84
7. Transferencias y transmisiones internacionales de datos	85
7.1. Distinción entre transferencia y transmisión	85

7.2. El principio de nivel adecuado de protección.....	85
7.3. La declaración de conformidad de la Superintendencia de Industria y Comercio	86

Capítulo VIII.

La autoridad de control y el régimen sancionador	87
1. La Superintendencia de Industria y Comercio como autoridad de datos	87
1.1. La Delegatura para la Protección de Datos Personales	87
1.2. Funciones de instrucción, decisión y sanción.....	88
2. El procedimiento administrativo sancionador	88
3. Tipología de infracciones y criterios de graduación de la sanción.....	89
3.1. El catálogo de sanciones.....	89
3.2. Los criterios de dosificación	89

Capítulo IX.

La reforma en curso: el proyecto de modernización de la Ley 1581 de 2012.....	91
1. Contexto y justificación de la reforma.....	91
1.1. El diagnóstico: trece años de vigencia y transformación digital	91
1.2. Los Proyectos de Ley 214 y 274 de 2025 y su acumulación.....	92
1.3. Estado del trámite a la fecha de cierre de esta obra.....	92
2. Los ejes de la reforma y su aproximación al RGPD	93
2.1. Ampliación del ámbito de aplicación y criterio de destino	93
2.2. Nuevas bases de licitud: interés legítimo y ejecución contractual	93
2.3. Nuevos derechos: portabilidad, oposición y decisiones automatizadas	94
2.3.1. <i>El derecho a la portabilidad de los datos</i>	94
2.3.2. <i>El derecho de oposición</i>	94
2.3.3. <i>El derecho a no ser objeto de decisiones automatizadas</i>	94
2.4. Protección reforzada de niñas, niños y adolescentes	95
2.5. Fortalecimiento del régimen sancionador	95
3. Valoración crítica y prospectiva	96

Capítulo X.

La intersección entre compliance y protección de datos	99
1. El dato personal como activo y como fuente de riesgo	99
2. El privacy compliance y el principio de responsabilidad demostrada.....	100
3. Seguridad de la información, incidentes y notificación.....	100
4. El delegado de protección de datos y su articulación con el compliance officer	101

Parte Tercera

El marco europeo como estándar de referencia	103
---	------------

Capítulo XI.

El Reglamento General de Protección de Datos (RGPD).....	105
1. Génesis y arquitectura del Reglamento (UE) 2016/679	105
1.1. Del Convenio 108 a la Directiva 95/46/CE.....	105
1.1.1. <i>El Convenio 108 del Consejo de Europa y su modernización</i>	<i>105</i>
1.1.2. <i>La Directiva 95/46/CE y sus limitaciones.....</i>	<i>106</i>
1.2. La reforma de 2016 y la elección del instrumento reglamento	107
1.2.1. <i>La fragmentación como problema</i>	<i>107</i>
1.2.2. <i>Las razones de la opción por el reglamento</i>	<i>107</i>
1.3. El ámbito territorial y el criterio de destino.....	108
2. Principios y bases de licitud del tratamiento	108
2.1. Los principios del artículo 5 y la accountability	108
2.1.1. <i>Licitud, lealtad, transparencia y minimización</i>	<i>108</i>
2.1.2. <i>La responsabilidad proactiva como clave de bóveda</i>	<i>109</i>
2.2. Las bases jurídicas del artículo 6 y el interés legítimo.....	110
2.2.1. <i>El elenco de bases de licitud.....</i>	<i>110</i>
2.2.2. <i>La ponderación en el interés legítimo</i>	<i>110</i>
3. Los derechos del interesado.....	110
3.1. Información, acceso, rectificación y supresión.....	110
3.1.1. <i>El derecho al olvido y la sentencia Google Spain</i>	<i>110</i>
3.2. Portabilidad, oposición y decisiones automatizadas	111
3.2.1. <i>El derecho a la portabilidad</i>	<i>111</i>
3.2.2. <i>El derecho de oposición</i>	<i>111</i>
3.2.3. <i>Las decisiones individuales automatizadas y la elaboración de perfiles</i>	<i>112</i>
4. Responsable, encargado y delegado de protección de datos	112
4.1. El contrato de encargo del tratamiento	112
4.2. El estatuto del delegado de protección de datos	113
5. Privacidad desde el diseño y evaluación de impacto (DPIA).....	113
5.1. La privacidad desde el diseño y por defecto.....	113
5.2. La evaluación de impacto relativa a la protección de datos	114
6. Las transferencias internacionales tras la sentencia Schrems II	114
6.1. El régimen de transferencias del Capítulo V	114
6.1.1. <i>Decisiones de adecuación.....</i>	<i>114</i>
6.1.2. <i>Cláusulas contractuales tipo y normas corporativas vinculantes</i>	<i>115</i>
6.2. La sentencia Schrems II y sus consecuencias.....	115
6.2.1. <i>La invalidación del Escudo de Privacidad</i>	<i>115</i>
6.2.2. <i>La evaluación caso por caso y las medidas suplementarias</i>	<i>115</i>

6.3.	El Marco de Privacidad de Datos UE-EE. UU.....	116
7.	El régimen sancionador y el sistema de autoridades de control.....	116
7.1.	Los umbrales sancionadores del artículo 83.....	116
7.2.	Las autoridades de control y el Comité Europeo de Protección de Datos.....	117

Capítulo XII.

El compliance en el Derecho de la Unión Europea	119
1. Cumplimiento normativo y responsabilidad de la empresa en la Unión.....	119
1.1. La ausencia de un régimen penal general del ente	119
1.2. Los deberes de organización en el Derecho derivado	119
2. La Directiva (UE) 2019/1937 sobre protección de los denunciantes	120
2.1. Ámbito y canales de denuncia obligatorios.....	120
2.2. La prohibición de represalias.....	120
2.3. La articulación con la protección de datos	120
3. La debida diligencia en sostenibilidad: la Directiva CSDDD	121
3.1. Deberes de diligencia sobre la cadena de valor	121
3.2. Del compliance preventivo a la gestión responsable.....	121

Capítulo XIII.

El «efecto Bruselas» y la influencia europea sobre Colombia.....	123
1. El concepto de efecto Bruselas y su mecánica	123
1.1. La atracción del mercado como fuente de poder regulatorio	123
1.2. El efecto Bruselas de facto y de iure	123
2. La adecuación como incentivo regulatorio para Colombia.....	124
2.1. La aspiración de la declaración de adecuación.....	124
2.2. La reforma de la Ley 1581 como manifestación del fenómeno	124

Parte Cuarta

La perspectiva norteamericana	127
--	------------

Capítulo XIV.

El compliance en los Estados Unidos de América	129
1. La Foreign Corrupt Practices Act (FCPA).....	129
1.1. Origen y estructura de la ley.....	129
1.2. Disposiciones antisoborno y de contabilidad	130
1.2.1. Las disposiciones antisoborno	130
1.2.2. Las disposiciones contables y de controles internos	130
1.3. Alcance extraterritorial y enforcement conjunto DOJ-SEC	131
2. Las Federal Sentencing Guidelines y el programa de cumplimiento efectivo	132
2.1. El capítulo octavo y la reducción de la culpabilidad.....	132

2.2.	Los elementos del programa efectivo.....	132
3.	Los criterios del Departamento de Justicia para evaluar programas	133
3.1.	La guía «Evaluation of Corporate Compliance Programs».....	133
3.1.1.	<i>Las tres preguntas fundamentales</i>	133
3.1.2.	<i>La actualización de 2024: inteligencia artificial y denunciantes</i>	134
3.2.	Acuerdos de enjuiciamiento diferido (DPA) y de no persecución (NPA).....	134
4.	La responsabilidad penal corporativa en el modelo estadounidense	135
4.1.	La doctrina del respondeat superior	135
4.2.	El programa como factor de la decisión de perseguir	135

Capítulo XV.

La protección de datos en los Estados Unidos	137
1. El modelo sectorial y la ausencia de una ley federal general	137
1.1. Un modelo fragmentario.....	137
1.2. Regímenes sectoriales: HIPAA, GLBA y COPPA.....	137
1.3. La matriz constitucional de la privacy.....	138
2. La legislación estatal: California como estándar de facto	138
2.1. La CCPA y su reforma por la CPRA	138
2.2. La proliferación de leyes estatales y el mosaico regulatorio	139
3. El enforcement de la Federal Trade Commission.....	139
3.1. La Sección 5 y las prácticas desleales o engañosas.....	139
3.2. Los consent decrees como fuente de doctrina	140
4. Contraste estructural con el modelo europeo y colombiano.....	140

Parte Quinta

Síntesis comparada y propuestas	143
--	-----

Capítulo XVI.

Convergencias y divergencias entre los tres modelos		145
1.	Compliance: del enforcement estadounidense a la autorregulación regulada europea y su recepción colombiana.....	145
1.1.	El origen estadounidense y su lógica de enforcement.....	145
1.2.	La reelaboración dogmática europea.....	146
1.3.	La síntesis administrativa colombiana.....	146
2.	Protección de datos: modelo de derechos fundamentales frente a modelo de mercado.....	147
2.1.	El modelo europeo de derecho fundamental	147
2.2.	El modelo estadounidense de mercado.....	147
2.3.	La adscripción colombiana al modelo europeo	148
3.	El papel del programa de cumplimiento como puente entre ambas materias	148

3.1. La convergencia metodológica.....	148
3.2. Los puntos concretos de intersección.....	149

Capítulo XVII.

Hacia un programa integrado de compliance y protección de datos en Colombia.....	151
1. Bases para un modelo integrado de gestión del riesgo jurídico	151
1.1. La unidad de la función de gestión del riesgo	151
1.2. La metodología común de gestión del riesgo.....	151
1.3. La integración organizativa	152
2. Recomendaciones de política legislativa.....	152
2.1. La culminación de la reforma y su articulación con el compliance	152
2.2. La racionalización de los regímenes sectoriales.....	153
2.3. El reforzamiento de la autoridad de control	153
3. Recomendaciones para la práctica empresarial	154
3.1. La adopción de programas integrados.....	154
3.2. La articulación de las funciones de control	154
3.3. La formación y la cultura de cumplimiento integrada.....	154
Conclusiones generales	157
Bibliografía	159
1. Doctrina	159
2. Instrumentos normativos	160
2.1. Colombia	160
2.2. Unión Europea.....	160
2.3. Estados Unidos	161
2.4. Instrumentos internacionales y estándares técnicos	161
3. Jurisprudencia.....	161
3.1. Colombia	161
3.2. Unión Europea y Alemania	162
3.3. Estados Unidos	162

