PROTECCIÓN DE DATOS PERSONALES DE NIÑOS NIÑAS Y ADOLESCENTES

En el marco de la juridificación y prevención del riesgo digital en Colombia

LUCERO GALVIS CANO

UNIVERSIDAD SANTO TOMAS
PRIMER CLAUSTRO UNIVERSITARIO DE COLOMBIA

DOCTORADO EN DERECHO

BOGOTÁ

Diciembre de 2019

PROTECCIÓN DE DATOS PERSONALES DE NIÑOS NIÑAS Y ADOLESCENTES

En el marco de la juridificación y prevención del riesgo digital en Colombia

LUCERO GALVIS CANO

Tesis presentada para optar el título de Doctor en Derecho

DIRECTOR

JHEISON TORRES ÁVILA

Doctor en Derecho

FACULTAD DE DERECHO

BOGOTÁ

2019

Agradecimientos

En este proceso investigativo materializado en la presente tesis doctoral, si bien ha requerido de esfuerzo y mucha dedicación por parte de la autora y su director de tesis, no hubiese sido posible su finalización sin la cooperación desinteresada de todas y cada una de las personas que a continuación refiere y muchas de las cuales han sido un soporte importante en cada de las etapas de su construcción y consolidación.

A Dios, por su infinita bendición espiritual y material reflejada en los dones de sabiduría, templanza y fortaleza que me acompañaron en el camino recorrido durante todo el periodo de estudio.

A mis padres Jose Vicente Galvis Pereira (Q.E.P.D.) y Abigail Cano de Galvis, quienes sembraron en mi la perserverancia y disciplina constante para construir y alcanzar las metas propuestas. A mis hermanos y amigos gracias por su apoyo incondicional.

Y en especial, al Doctor Jheison Torres Avila, por su acertada dirección, orientación, soporte y discusión crítica que me permitió comprender el significado sistémico de la investigación jurídica, acercándome a un campo innovador y de trascendencia para los derechos de los niños, niñas y adolescentes cuyos objetivos fueron posibles gracias a su invaluable sabiduría.

Contenido

Pág.

Introducción 17

Capítulo introductorio: Fundamento metodológico 21

1.Planteamiento del Problema 21

1.1. Justificación 24

1.2. Formulación del Problema 37

2. Objeto de la investigación 38

3. Hipótesis 39

4. Enfoque Metodológico 40

Capítulo I: Génesis del Derecho a la Protección de Datos Personales de Niños, Niñas y Adolescentes a Nivel Internacional 45

1.1. Referente Histórico del "Derecho a la Privacidad y la Protección de Datos Personales" 47

1.1.1. La privacidad como derecho individual, humano, global y tecnológico 47

1.1.2. La protección de datos personales como un derecho proactivo basado en el enfoque de los derechos humanos 55

1.2. Referente Conceptual del "Derecho a la Privacidad y la Protección de Datos Personales". 64

1.3. Reconocimiento del Derecho del Niño a la Privacidad y el Tratamiento de Datos Personales 89

1.4. Marco Teórico del Derecho a la Protección de Datos Personales de los Niños en la Era Digital 96

1.4.1 Fundamento de la teoría sistémica: Sistema social y tecnología 97

1.4.2 El pensamiento sistémico y el riesgo de seguridad digital de los datos personales 101

Capítulo II: Modelos y Estándares de Protección de Datos Personales Fuente de Regulación en Colombia 113

2.1. Modelo Centralizado de Protección de Datos Personales: Unión Europea 114

2.1.1. Gdt29: Estudio de la "privacidad de los menores en internet" 122

2.1.2. Un nuevo horizonte de la protección de los datos personales de NNA en la UE 127

2.2. Modelo Sectorial de Protección de Datos Personales: Estados Unidos de Norteamérica .. 137

2.2.1. Ley de Protección de la Privacidad en Línea de Los Niños: "The Children's Online Privacy Protection Act" (COPPA, 1998): 140

3.2.1.1. Ámbito de aplicación 142

3.2.1.2. Principios 143

2.2.2. Inspección y propuesta de modificación de las normas de desarrollo de la COPPA 145

2.2.3. Logro: Puerto seguro de la privacidad EU – EE. UU 148

2.3. Modelo Híbrido de Protección de Datos Personales: Colombia 151

2.4. Armonización y Estándares Internacionales de Protección de Datos Personales y la Privacidad de los Niños 154

2.4.1. Estándares de protección de la privacidad en el tratamiento de datos personales a nivel europeo 158

2.4.2. Estándares de protección de datos personales de los Estados Iberoamericanos 160

Capítulo III: Tratamiento Jurídico de Datos Personales de los Niños en Colombia y su Adecuación a los Estándares De Protección 168

3.1. Naturaleza Constitucional del Derecho a la Privacidad de Datos Personales de los Niños 169

3.2. Tratamiento Legal de Datos Personales de los Niños a Nivel General y Sectorial 188

3.2.1. Tratamiento de datos personales de niños en el ámbito empresarial 212

3.2.2. Tratamiento de datos personales de los menores de edad en el ámbito penal 215

3.2.3. Tratamiento de datos personales de niños en el ámbito educativo 221

3.2.4. Tratamiento de datos personales de los niños en el sector público y de las Tecnologías de la información y las comunicaciones 224

3.3. Control del Tratamiento de Datos Personales por Parte de la Superintendencia de Industria y Comercio 226

3.4. Nivel de Adecuación del Tratamiento de la Privacidad de Datos Personales de los Niños a los Estándares De Protección 242

3.4.1. Primeros estándares Internacionales de Protección de la privacidad de los niños en el tratamiento de datos de carácter personal 243

3.4.2. Estándares Iberoamericanos para el tratamiento de datos personales de los niños 268

Capítulo IV: Medidas Proactivas de Gestión Integral de Datos Personales de Niños, Niñas y Adolescentes 276

4.1. Fundamento Teórico 277

4.2. Política para la Ciberseguridad y Ciberdefensa de Datos Personales de los Niños 280

4.3. Juridificación del Tratamiento de Datos Personales y el Sistema Informático 290

4.3.1. Fases y variables de regulación de datos personales en el sistema informático 291

4.3.2. Propuesta de tratamiento jurídico de datos personales online de los niños, niñas y adolescentes 299

4.4. Gestión de Riesgos de Seguridad Digital y Privacidad de Datos Personales de los Niños 310

4.4.1 Sistema de protección de datos personales de la infancia y adolescencia 310

4.4.2. Programa integral de gestión de datos personales de los niños (PIGD) en las entidades públicas y privadas 314

5. Conclusiones 316

Referencias Bibliográficas 325

Apéndices 355

Apéndice A. Derechos de petición 355

Apéndice B. Resumen de entrevistas estructuradas 358

Lista de Figuras

Figura 1. Unos niños en la escuela St. Columba's en Delhi, India, con un teléfono móvil. © UNICEF/UN036675/Sharma – 2017…….……18

Figura 2. Indicador estadístico digital de Colombia……28

Figura 3. Proporción de personas de 5 y más años de edad que usaron internet en cualquier lugar y desde cualquier dispositivo. (2017)……29

Figura 4. "Proporción de personas de 5 y más años de edad que usaron computador en cualquier lugar según rangos de edad." (2016 – 2017)…….…..….30

Figura 5. "Proporción de personas que usaron internet en cualquier lugar, según nivel educativo" (2016 – 2017)……..…..…31

Figura 6. Registro de denuncias por cibercrimen en Colombia…….…..32

Figura 7. Protectio……33

Figura 8. Registro de quejas y sanciones de la SIC por violación de datos personales……...35

Figura 9. Línea del tiempo de los instrumentos normativos en materia de privacidad y protección de datos personales…….56

Figura 10. Mapa mundial de protección de datos personales……...…58

Figura 11. Dimensiones de estudio del derecho a la protección de datos personales……...77

Figura 12. Mapa mental de la Teoría de Sistemas. Se incopora la teoría de Teubner……..98

Figura 13. Escenarios relacionados con el sistema social y la tecnología……..100

Figura 14. Acoplamiento normativo de la protección de datos personales……102

Figura 15. Mapa legislativo de protección de datos personales a nivel sectorial……..…..115

Figura 16. Medidas de protección de datos personales plasmadas en el Reglamento Europeo……134

Figura 17. Principios de la ley COPPA……...143

Figura 18. Escenarios constitucionales del derecho a la intimidad……186

Figura 19. Escenarios constitucionales del derecho a la privacidad y protección de datos personales de los niños, niñas y adolescentes:……..……..188

Figura 20. Regulación de la protección de datos personales en Colombia……..…...191

Figura 21. Tipos de datos personales……..196

Figura 22. Sujetos titulares de derecho según la ley 1098 de 2006……218

Figura 23. 1581 vs 1266 crecimiento anual……...…….227

Figura 24. Motivos sanción Ley 1581 (2012-2018)……..….228

Figura 25. Motivos sanción 1266 año 2019……....228

Figura 26. Motivos sanción 1581 año 2019…….…...229

Figura 27. Motivos sanción Ley 1266 (2009-2018)……...230

Figura 28. Motivos sanción Ley 1581 (2012-2018)…….……..230

Figura 29. Trámites nuevos Ley 1581 vs 1266 (2019)…….……..231

Figura 30. Las redes sociales…….252

Figura 31. Telaraña jurisprudencial sobre la protección de datos personales de NNA en el ámbito digital……...265

Figura 32. Menores y protección de datos en redes sociales…….277

Figura 33. Variables de la protección de datos personales de NNA…….279

Figura 34. Estado actual de los Sistemas de Información de Justicia. Ejemplo:

Sistema de Responsabilidad Penal Adolescente Modelo de Gestión Pública

Eficiente al Servicio del Ciudadano……..284

Figura 35. . Índice de Penetración de Internet dedicado por Departamento…….……286

Figura 36. Modelo de Gestión Pública Eficiente al Servicio del Ciudadano……287

Figura 37. Comienza una nueva era en el tratamiento y protección de los datos

Personales…….……....289

Figura 38. Protección del derecho a la privacidad de los niños en la era digital……..291

Figura 39. Diagrama causal l……..……...…297

Figura 40. La ONU declara el acceso a Internet como un derecho humano……..……...300

Figura 41. Sistema de protección de datos personales de NNA……311

Figura 42. Código binario del título de la Tesis Doctoral…….……316

Lista de Tablas

Pág.

Tabla 1. Abreviaturas……..17

Tabla 2. Glosario…….19

Tabla 3. Etapas de reconocimiento del derecho a la vida privada ……..49

Tabla 4. Instrumentos legales de carácter universal del derecho a la vida privada…….53

Tabla 5. Instrumentos normativos de protección de datos personales de la Unión Europea…..57

Tabla 6. Países que han regulado la protección de datos personales 1970 – 2018…….59

Tabla 7. Reconocimiento de la tecnología como derecho humano…….62

Tabla 8. Conceptos de intimidad…….65

Tabla 9. Niveles de derechos fundamentales relacionados con la intimidad en Estados Unidos…….72

Tabla 10. Instrumentos internacionales sobre derechos humanos que reconocen los derechos de la infancia y el derecho a la vida privada……..90

Tabla 11. Instrumentos normativos de protección de datos personales en la Unión Europea (UE)……117

Tabla 12. Característica del modelo de protección de datos personales en la Unión Europea…129

Tabla 13. Normativa del derecho a la privacidad en Estados Unidos (a nivel federal)……..…137

Tabla 14. Marco normativo de la privacidad y la protección de datos personales de niños en los Estados Unidos……..140

Tabla 15. Comparativo del nivel adecuado de terceros países frente a la reglamentación - Comunidad Europea de protección de datos personales…….148

Tabla 16. Estados Unidos reconoce los principios de protección de datos personales……...150

Tabla 17. Análisis comparativo de modelos de protección de datos personales…….152

Tabla 18. Principales organizaciones internacionales que han emitido documentos sobre tratamiento de datos personales……..…155

Tabla 19. Estándares Iberoamericanos para el tratamiento de datos personales de NNA……...166

Tabla 20. Postulado normativo del derecho a la vida privada en Colombia antes de 1991…..…169

Tabla 21. Primeros instrumentos de protección de los derechos del niño y el derecho a la vida privada antes de la Constitución Política de 1991……..…….170

Tabla 22. Normativa de reconocimiento de la Convención de los Derechos del Niño y su derecho a la vida privada en Colombia…….…...172

Tabla 23. Protección constitucional de la intimidad e información personal de los NNA…..…175

Tabla 24. Transición Línea jurisprudencial de la Corte Constitucional: Derecho fundamental de la protección a la privacidad e información personal……..178

Tabla 25. Instrumentos legales de protección de los datos personales antes de 1991……189

Tabla 26. Principios del tratamiento de datos personales en Colombia…….…....197

Tabla 27. Instrumentos legales de protección del derecho a la privacidad y protección legal de NNA en Colombia…….…..200

Tabla 28. Desarrollo normativo de la protección de los NNA en el ámbito empresarial……..213

Tabla 29. Instrumentos de protección de datos personales en el ámbito penal……..…217

Tabla 30. Estudios estadísticos de las denuncias en materia de delitos informáticos en Colombia a 2017……..219

Tabla 31. Denuncias y capturas Colombia 2014-2017 ……..…220

Tabla 32. Usuarios impactados en el periodo 2014-2017……..221

Tabla 33. La protección de datos personales de NNA en el sector educativo……...222

Tabla 34. La protección de datos personales en el sector de las Tecnologías de la información y las comunicaciones……..……..224

Tabla 35. Exigencia internacional de protección de los datos personales de NN..……243

Tabla 36. Leyes y lineamientos de protección de datos personales de niños EE. UU – UE y Colombia……..244

Tabla 37. Comparativo de los principios regulados en instrumentos internacionales de protección de datos personales y la normativa en Colombia…….…..……...257

Tabla 38. Cumplimiento del Memorándum de Montevideo para el marco legal sobre la protección de datos personales y la vida privada en las redes sociales en internet de NNA en Colombia……...……258

Tabla 39. Comparativo de los principios regulados en instrumentos internacionales de protección de datos personales y la normativa en Colombia……...…..269

Tabla 40. Estándares Iberoamericanos del tratamiento de datos personales de NNA en Colombia……...….272

Tabla 41. Sistema teórico…….....294

Tabla 42. Variable Nº 01: Protección de la información……..…….....….294

Tabla 43. Variable Nº 02: Seguridad de la información personal ……..…….....…295

Tabla 44. Variable No. 3: Probabilidad de afectación de la información personal de NNA…….…..295

Tabla 45. Variable No. 4: Implementación de un modelo de gestión integral de datos online para NNA en Colombia…….……..…296

Tabla 46. Componentes del Sistema de protección de datos personales de la infancia y adolescencia…….……..312

Lista de Apéndices

Pág.

Apéndice A. Derechos de petición **355**

Apéndice B. Resumen de entrevistas estructuradas **358**

Abreviaturas

Tabla 1.

Abreviaturas

Sigla	Significado de la abreviatura
AEPD	Agencia Española de Protección de Datos
APEC	Foro de Cooperación Económica Asia – Pacífico
ARCO	Acceso, Rectificación, Cancelación y Oposición
CE	Consejo de Europa
CARU	Children's Advertising Review Unit
CC	Código Civil
CIF	Código de la Infancia y la Adolescencia Ley 1098 de 2006
CEDH	Convenio Europeo de Derechos Humanos
CIDH	Carta Internacional de los Derechos Humanos
COPPA	Children's Online Privacy Protection Act (1998)
CONPES	Consejo Nacional de Política Económica y Social
DDHH	Derechos Humanos
DRLEPDP	Decreto reglamentario 1377 de 2013 de 27 de Junio, de la Ley estatutaria de protección de datos personales
DRLEPDP	Decreto reglamentario 1074 de 2015 de 26 de Mayo, del sector comercio industria y turismo
DUDH	Declaración Universal de Derechos Humanos
FTC	Federal Trade Commision
IWGDPT	International Working Group on Data Protection In Telecommunications
IUS	Termino en latin que significa Derecho Objetivo
LEPDP	Ley Estatutaria 1581 de 2012 de 17 de octubre, para la Protección de Datos Personales
LOPD	Ley orgánica 15 /1999, de 13 de diciembre, de Protección de Datos de Carácter Personal
LOPH	Ley orgánica 1/1982, de 5 de mayo, de Protección civil de los derechos la honor, intimidad personal y familiar y propia imagen
LOPJM	Ley orgánica 1/1996, de 15 de enero, de Protección Jurídica del menor
NNA	Niños, niñas y adolescents
OCDE	Organización para la Cooperación y el Desarrollo Económico
OEA	Organización de Estados Americanos
ONU	Organización de Naciones Unidas

Sigla	Significado de la abreviatura
PDP	Protección de Datos Personales
PSSI	Prestadores de servicios de la sociedad de la información
RLOPD	Real decreto 1720/2007 de 21 de diciembre, por el cual se aprueba el reglamento de desarrollo de LOPD
RNBD	Registro Nacional de Base de Datos
RSR	Red social real
RSV	Red social virtual
SCC	Sentencia de la Corte Constitucional de Colombia
SIC	Superintendencia de Industria y Comercio
STEDH	Sentencia del Tribunal Europeo de Derechos Humanos
TICs	Tecnologías de la información y comunicaciones
TJCE	Tribunal de justicia de las comunidades europeas
TJUE	Tribunal de justicia de la Unión Europea
UNICEF	United Nations Children's Fund

Glosario

Tabla 2.

Glosario

Término	Definición
Dato de carácter personal	Cualquier información que identifica o puede llegar a identificar a una persona física por diferentes medios razonablemente utilizados.
Tratamiento	Cualquier operación o conjuntos de operaciones, sean o no automatizadas, que se aplique a datos de carácter personal, en especial su recogida, conservación, utilización, revelación o supresión.
Interesado	Persona física cuyos datos de carácter personal sean objeto de tratamiento
Prestador de servicios de tratamiento:	Persona física o jurídica, distinta de la persona responsable, que lleve a cabo un tratamiento de datos de carácter personal por cuenta de dicha persona responsable.
Extimidad	Hace referencia a la tendencia que tienen las personas de hacer pública su intimidad.
Proscribir	Excluir o prohibir el uso de un uso o de una costumbre.
Juridificación	Regular en derecho una situación que anteriormente no se encontraba prevista en las normas.
Gromming	Es un tipo de acoso por parte de pedófilos y pederastas que consiste en todas las conductas o acciones que realiza un adulto para ganarse la confianza de un menor de edad, con el objeto de obtener un beneficio sexual.
Sexting	Es aquel acto de emitir mensajes, fotografías y videos con alto contenido sexual a través de un teléfono móvil.
Nativo digital	Hace referencia a una persona que se encuentra cómoda con la tecnología al punto de ser asumida como un complemento
Privacidad por diseño	La privacidad por diseño se refiere a la aplicación de las garantías necesarias para la protección de datos, desde la fase de planificación de cualquier desarrollo tecnológico.
Privacidad por defecto	Hace referencia a ofrecer las máximas garantías de privacidad por defecto de esas tecnologías que vayan a tratar con datos personales

Creación basada en los instrumentos normativos

Introducción

> En un mundo digital, sus voces son cada vez más más importantes, y se oyen más alto que nunca. Se trata de un mundo que no solamente ellos van a heredar, sino que están contribuyendo a configurar. (Anthony Lake, UNICEF, 2017)

En virtud de la innovación que ofrece la sociedad del conocimiento, las tendencias de las Tecnologías de la Información y las Comunicaciones –TIC y la digitalización, durante los siglos XX y XXI, los niños acceden con mayor velocidad a los distintos sistemas informáticos, dispositivos de alta tecnología que irrumpen en las redes de internet, tales como: celulares, Ipads, tablets, computadoras portátiles y otros escenarios digitales de diferente aplicación; herramientas que hacen de las comunicaciones un elemento dinámico de gran evolución e información, pero que a su vez, presenta grandes desafíos jurídicos frente al inadecuado tratamiento de la información personal de los individuos en especial de los menores de edad.

Los niños, son identificados para este estudio indistintamente por los términos: "niños, niñas, adolescentes (en adelante NNA) y menores de edad", con fundamento en la Convención sobre los Derechos del Niño, base de su reconocimiento internacional: "(…) se entiende por niño todo ser humano menor de dieciocho años de edad" (CDN, 1989 artículo 1), como sujetos de derecho de especial interés y protección efectiva por parte de los Estados frente a la falta de autodeterminación informativa y la autorregulación en el mundo de la ciencia, la innovación y la tecnología de la datificación circulante de forma prevalente y sin control en una sociedad de la transparencia que

incorpora algoritmos desconocidos que a la vez representa riesgos de seguridad al ejercicio del derecho y deber de respeto de la privacidad de la información personal de sí mismo, de su familia, su entorno económico, político y social, bajo en el enfoque de la garantía de los derechos humanos.

El objeto del presente trabajo parte del análisis de los dilemas conceptuales, los constructos normativos, la aproximación a los modelos y estándares de tratamiento de datos personales, los desafíos de la regulación frente a los riesgos de la privacidad de los niños en internet y la necesidad de adecuar el ordenamiento jurídico para superar la fragmentación técnica del derecho con el ecosistema digital, como lo refiere algunos estudios recogidos por UNICEF:

> "Es importante recordar que los derechos de la infancia son universales y aplicables en todo el mundo por igual, independientemente de la edad o el género del niño, de que vayan al colegio o no, y de que sean ricos o pobres. Y lo mismo se debe aplicar en el caso de internet. ¿Por qué deberíamos pensar que los derechos van a ser diferentes cuando se trate de internet?" (Byrne, 2016, p. 9)

Figura 1. Unos niños en la escuela St. Columba's en Delhi, India, con un teléfono móvil. © UNICEF/UN036675/Sharma - 2017.

Fuente: UNICEF https://www.unicef.org/paraguay/spanish/UN0150440.pdf

Atendiendo la estructura capitular y con el fin de desarrollar cada uno de los objetivos planteados en la presente investigación se desarrolla en el siguiente esquema histórico, teórico, sistémico y deductivo:

El capítulo introductorio de la tesis presenta el fundamento metodológico.

El primer capítulo de la tesis presenta una aproximación a la génesis del derecho a la protección de datos personales de niños, niñas y adolescentes, la conceptualización del derecho a la intimidad, la vida privada y la protección de datos personales, marco teórico del derecho a la privacidad de los datos personales de los niños; así como los aspectos teóricos relacionados con los riesgos de seguridad de la información personal de los niños en la sociedad de la digitalización.

El segundo capítulo identifica los modelos de protección de datos personales que han inspirado el tratamiento jurídico de la privacidad de la información de los niños en Colombia, tales como el modelo europeo y el modelo Estadounidense, que han sido referentes en la construcción del derecho a la protección de los datos personales e incorporan los principios y conceptos que fundamentan el reconocimiento de la privacidad y la autodeterminación informativa de los niños, niñas y adolescentes frente a los riesgos de la era digital.

El tercer capítulo establece el tratamiento jurídico de la privacidad y la información personal de los niños en Colombia, respecto a la naturaleza constitucional y estructura legal del derecho a la protección de datos personales, así como su tratamiento y adecuación a los Estándares De Protección de Datos Personales de los Estados Iberoamericanos.

Y el cuarto capítulo analiza las medidas de seguridad del tratamiento de la privacidad de datos personales de los niños, niñas y adolescentes en Colombia respecto de los Estándares de Protección de Datos Personales para los Estados Iberoamericanos y el Modelo de Gestión de Seguridad

Digital de los niños basado en el enfoque de los derechos humanos frente a los desafíos y paradigmas que representa la sociedad de la información tecnológica en virtud de la responsabilidad proactiva de los Estados para emprender programas integrales de administración, transparencia, confidencialidad, seguridad y privacidad de la información personal, y así mismo, el uso de herramientas jurídicas apropiadas que regulen el uso del internet y de la tecnología para los menores de edad; instrumentos jurídicos que aseguren la autorregulación de los operadores digitales, la seguridad de los riesgos digitales, análisis de incidentes y sanciones por la falta de control en los contenidos y servicios de los ciudadanos digitales.

Capítulo introductorio: Fundamento metodológico

1. Planteamiento del problema

Gestionar los datos personales con calidad y adecuada protección se ha convertido en uno de los hándicaps y debates en la juridificación de los derechos en internet, con distintas iniciativas legislativas de carácter global que buscan consolidar principios normativos armonizados en este campo, con ocasión de la metamorfosis que experimenta la intimidad o también denominada privacidad. Así como, el alto grado de extimidad del individuo en la web, la proliferación de herramientas de tecnología propias de la era de la sociedad del conocimiento, la brecha informática, el marketing sin control promovido por diferentes operadores online y offline de información, la exposición a riesgos y la violación de los derechos de los menores (la vida privada) en la era digital, merece ser analizado desde una perspectiva sociojurídica.

Dada la complejidad de la presente investigación propia del escenario técnico jurídico que rodea la dogmática de la privacidad de la información personal producto de múltiples intereses, resulta necesario analizar cómo la creación del derecho y la protección del sujeto de derecho en entornos digitales, presenta enfoques multidisciplinarios propios del entorno empresarial, bancario, marketing, electoral, asistencia sanitaria, las telecomunicaciones, el transporte de personas, las relaciones paterno-filiales, la gobernanza digital, la inteligencia artificial, la actividad administrativa, la gestión tributaria entre otros diversos subsistemas propios de la sociedad del conocimiento.

Subsistemas que se conectan con la tecnología y la digitalización en escenarios propios del sistema jurídico, cuyos derechos incorporan: la intimidad, el buen nombre, la información, la igualdad, la seguridad y la defensa, el secreto e interceptación de las comunicaciones, las peticiones, el libre desarrollo de la personalidad, la participación, la libertad de expresión; la función jurisdiccional y los relacionados con los diferentes mecanismos de participación ciudadana que fundamentan una democracia que experimenta la innovación de la modernidad líquida y reconoce la garantía de los derechos humanos en contextos virtuales desde la génesis del tratamiento jurídico de datos personales.

Desde una perspectiva transnacional, es necesario en forma progresiva integrar el enfoque sistémico y cibernético en el marco de la globalización del derecho; caracterizado por una normativa internacional armónica y homogenizada con las comunicaciones mundiales como lo plantea la Comisión Europea. Por lo tanto, replantear el sistema de derechos fundamentales en todas las dimensiones de la información, la contextualización de normas, la protección de la información para el dominio público, se constituye un desafío jurídico que debe ser tratado de manera prioritaria por parte de todos los Estados.

Principalmente, en el contexto del régimen jurídico de los datos personales de los menores de edad en internet se requiere de un exigente nivel de protección integral, en virtud de la falta de autorregulación y la ausencia de pautas educativas de conducta, dado su imaginario intangible de privacidad que le permite compartir su información personal sin límites (fotos, gustos, viajes, intereses, ubicaciones de su familia nuclear, entre otros) en ambientes digitales sin control, que desconocen la realidad de los hilos invisibles de las multinacionales que le dan tratamiento a esta información con grandes dividendos gracias al consumo y negociación comercial de los datos personales (prácticas de consumo, viajes, localización, intereses familiares, publicidad e imágenes

relevantes para el marketing), como lo refiere UNICEF en uno de sus últimos referentes sobre el internet y los derechos de la infancia: “Hacer del Internet y las tecnologías móviles más seguras para la infancia, así como para que puedan utilizar ambas herramientas como vehículos de aprendizaje, crecimiento y acceso a la información.” (2016, p. 2)

Los niños son uno de los titulares de información más vulnerables en el mundo digital que incursionan sin ninguna restricción en los portales electrónicos de la Web (*Redes sociales de carácter personal*: Facebook, MySpace, Twitter, Instagram, Whatsapp. *Redes sociales profesionales*: Xing, Ploxy, Linkedin. *Redes sociales temáticas*: Pinterest, YouTube, Tumblr y r*edes sociales de escala local*: Tuenti, Hyves) como medios de comunicación para el aprendizaje informal que le permite crear contenidos que pueden llegar a situaciones de vulneración de derechos fundamentales, por la falta de educación del adecuado uso de las tecnologías de la información y las comunicaciones (en adelante TIC) y el conocimiento de los riesgos a los que se expone al ingresar a internet.

Así mismo, los menores pueden ser víctimas del cibercrimen por perder o facilitar información personal o confidencial de los miembros de su familia a personas totalmente desconocidas para ellos y ser objeto de situaciones de vulnerabilidad al intercambiar sus datos con supuestos amigos que se muestran con perfiles falsos. Por lo general, los dispositivos digitales que hacen parte de los bienes de la familia no cuentan con sistemas de seguridad idóneos que les brinden protección a sus datos personales, convirtiéndose en presa fácil de los ciberdelincuentes, los piratas del internet, los depredadores sexuales, y las mafias que promocionan la pornografía infantil, robo de identidad o el consumo de alucinógenos, como lo refiere Ornelas en los siguientes términos:

> “El derecho a la vida privada es un valor que toda sociedad democrática debe respetar. Por tanto, a efectos de asegurar la autonomía de los individuos para decidir los alcances de su vida

privada, debe limitarse el poder del Estado como de las organizaciones privadas, de cometer intromisiones ilegales o arbitrarias en dicha esfera personal. En particular, debe protegerse la información que niños, niñas y adolescentes proporcionan e intercambian en Internet a efectos de impedir su utilización inadecuada con fines distintos para los cuales ellos la proporcionaron." (2010, p. 155).

Es decir, el valor de la privacidad de la información personal de NNA en todos los entornos ya sea físicos, online, offline deben ser protegidos de manera prevalente y especial, dado el interés superior de este sujeto de derecho, que exige mayor intervención en el ámbito preventivo y proteccionista, en cuanto, a la gobernanza de sus datos personales. Como, por ejemplo el derecho a la libertad de expresión en internet, el derecho al olvido, el derecho al honor, la imagen, deben ser protegidos en justa proporción con el derecho al habeas data de los niños a fin de garantizar el principio de la dignidad humana, en razón a su expectativa razonable de intimidad y debido a que desconoce la vigilancia, monitoreo y riesgos a la hora exhibir su información personal en ambientes virtuales.

1.1. Justificación

Frente al acelerado aumento de casos de vulneración de los derechos humanos con ocasión del inadecuado uso y funcionamiento de las plataformas digitales, en un alto porcentaje de los países del mundo, UNICEF evidencia que el 70.6% de los adolescentes de 15 a 24 años conectados a internet ha sufrido algún tipo de violencia digital, y con mayor preocupación las víctimas de ciberacoso, son menores que se encuentran en un rango de edad, cada vez más reducido con ocasión de la facilidad en el acceso a diferentes herramientas tecnológicas sin control parental,

institucional, estatal y social, lo cual conlleva a diferentes dilemas jurídicos frente a los contextos digitales que afectan la seguridad, la privacidad, el desarrollo de la personalidad y la dignidad humana de los niños.

En la sociedad de la información automatizada, el determinismo tecnológico se convierte en un desafío socio político y jurídico entorno a una política de privacidad acorde con los derechos humanos en el ámbito digital, después de tres décadas de reconocimiento internacional de la "Convención sobre los Derechos del Niño" y del surgimiento de la World Wide Web, como la oportunidad de intercambio generacional de conocimiento interactivo que crea contenidos en la Web 2.0. en tránsito a la revolución tecnológica 4.0 mediada por la inteligencia artificial, que a la vez, se traduce en una herramienta técnica de exposición constante de riesgos de seguridad digital y desconocimiento de los valores de fraternidad, igualdad y libertad, con ocasión de la falta de autodeterminación informativa de los internautas deseosos de compartir imágenes de su interés en milésimas de segundos micro y macro datos en Internet como un medio de complementar las actuales relaciones sociales, económicas, culturales, religiosas, recreativas de los más jóvenes en línea.

En particular, existen múltiples riesgos y la falta de garantías de los derechos concernientes a la vida privada de los niños, niñas y adolescentes como un derecho humano que ha evolucionado en el sistema de internet y el régimen jurídico internacional frente a las nuevas tecnologías de la información y las comunicaciones, que exigen un tratamiento jurídico y de cooperación global en virtud del interés superior, el derecho a la libertad y los principios reconocidos por el ordenamiento constitucional y legal acorde con los tratados internacionales.

La protección del "interés superior del niño" en la interacción digital, se pone a prueba en los eventos en que se presentan casos de riesgo o vulneración de derechos, ocasionados por la

inseguridad desde la misma arquitectura o concepción del sistema que desconoce su garantía prevalente y proactiva, y que a la vez, representa diferentes formas del ejercicio de sus derechos que apremia el control y acceso a la información adecuada para la edad, por parte de los operadores y responsables de la información a nivel público y privado. El compromiso internacional es la responsabilidad proactiva de los diseñadores de los códigos binarios y otros sistemas propios del mundo de internet, relacionados con las plataformas digitales como herramienta de búsqueda de identidad e información y perfilación en comunidades virtuales tales como: Google, Youtube, Yahoo entre otros; los blogs, correo electrónico y las redes sociales, como por ejemplo: Twitter, Instagram, Facebook, Whatsapp por medio de las cuales circulan libremente datos y megadatos personales propios de una sociedad sujeta al panoptismo de transparencia y consumo online.

Como lo señala Aba Catoira (2011), la forma actual de relacionarse entre los menores no se concibe sin las herramientas tecnológicas por cuanto, son sujetos de derecho digitales e interactivos que acceden a la información en línea con facilidad, crean y comparten datos como usuarios y como consumidores de información personal que permite la elaboración de perfiles digitales en un mundo analógico y con apariencia inofensiva así como la sobreexposición voluntaria de la información personal a los ojos del mundo virtual y real.

A nivel internacional, los Estados se han venido acoplando al modelo de protección comunitario de consenso global enfocados al entendimiento del sistema informático y de la conectividad con la garantía de derechos tales como la igualdad jurídica, los derechos fundamentales y la dignidad humana que dinamiza la autorregulación, la legalidad del consentimiento, la responsabilidad parental, la exigencia de la privacidad por diseño y por defecto, códigos de conducta y lenguaje informático en razón a la capacidad de comprensión propia de la edad y madurez del niño y la

rendición de cuentas de los diferentes operadores y responsables del tratamiento de la información personal.

Uno de los principales referentes normativos vigentes en la actualidad, es el Reglamento Europeo 679 UE: “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, por el que se deroga la Directiva 95/46/CE" (2016), y hace alusión a los principios de integridad y dignidad humana de cara a las nuevas tendencias tecnológicas, de acuerdo al siguiente considerando:

> “El tratamiento de datos personales debe estar concebido para servir a la humanidad. El derecho a la protección de los datos personales no es un derecho absoluto, sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo a los principios de proporcionalidad” (Reglamento 679 UE, No. 4, 2016).

Servir a la humanidad, de manera especial es reconocer la importancia de proteger a los niños, niñas y adolescente frente al uso de las TIC en especial cuando refiere:

> “Los niños merecen una protección específica de sus datos personales, ya que pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales. Dicha protección específica debe aplicarse en particular, a la utilización de datos personales de niños con fines de mercadotecnia o elaboración de perfiles de personalidad o de usuario y a la obtención de datos personales relativos a niños cuando se utilicen servicios ofrecidos directamente a un niño. El consentimiento del titular de la patria potestad o tutela no debe ser necesario en el contexto de los servicios preventivos o de asesoramiento ofrecidos directamente a los niños” (Reglamento 679 (UE), No. 38, 2016).

El régimen jurídico y preventivo del tratamiento de datos personales de los niños en la sociedad de la información se encuentra en un proceso de transición que exige modelos de gestión de seguridad digital con programas y alianzas educativas en materia de autorregulación, privacidad por diseño y por defecto, responsabilidad proactiva, derecho al olvido, código de buenas prácticas, políticas de privacidad y calidad de datos, que son y serán importantes para evitar impactos negativos frente al desconocimiento de los derechos de la infancia y la adolescencia.

Colombia, en los últimos tres años ha evidenciado un panorama acelerado de accesibilidad a internet a través de los dispositivos móviles (54.29 millones) y como consecuencia mayor conectividad de la población a través de las redes sociales, generando una oportunidad valiosa de conocimiento y comunicación, pero a su vez mayores riesgos sin control (2018).

Figura 2. Indicador estadístico digital de Colombia.
Fuente: Hootsuite (2018)

De acuerdo con el informe del DANE, entre los años 2016 y 2017 se evidenció un aumento paralelo en el acceso de internet por parte de la población que inicia su uso a partir de los 5 años de edad independiente de si es en las grandes ciudades o regiones apartadas de Colombia.

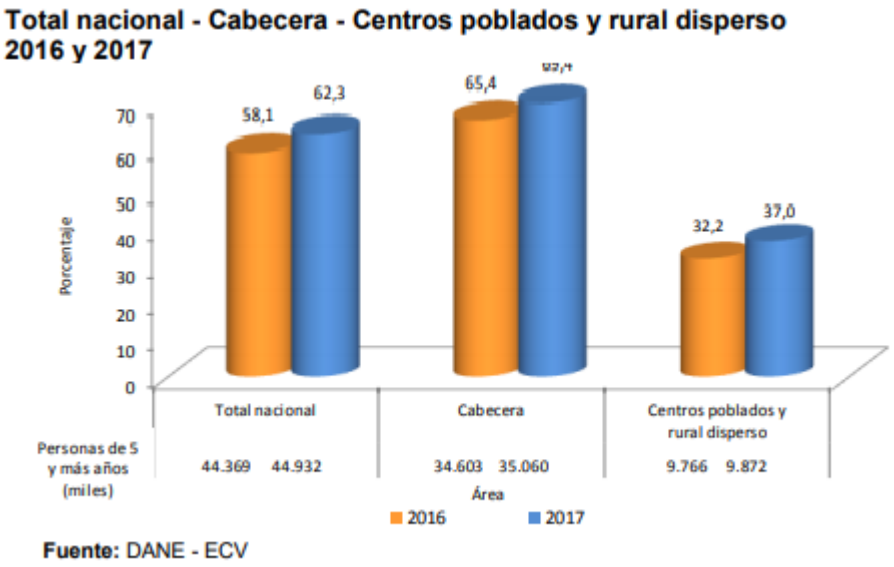


Figura 3. Proporción de personas de 5 y más años de edad que usaron internet en cualquier lugar y desde cualquier dispositivo. (2017)
Fuente: DANE ECV.

Otro componente de revisión es el rango de edad que más accede a internet entre los que sobresale de 5 a 24 años, los cuales están por encima de la media nacional, incluyendo a los niños, niñas y adolescentes que son los que utilizan al dispositivo de información para acceder a la web por encima del promedio nacional dependiendo de su capacidad de comprensión.

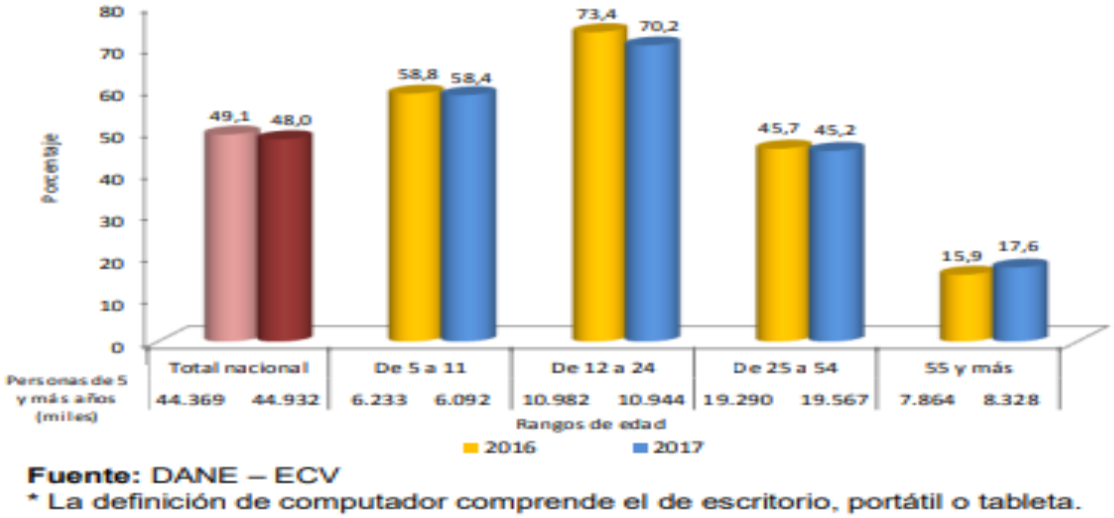
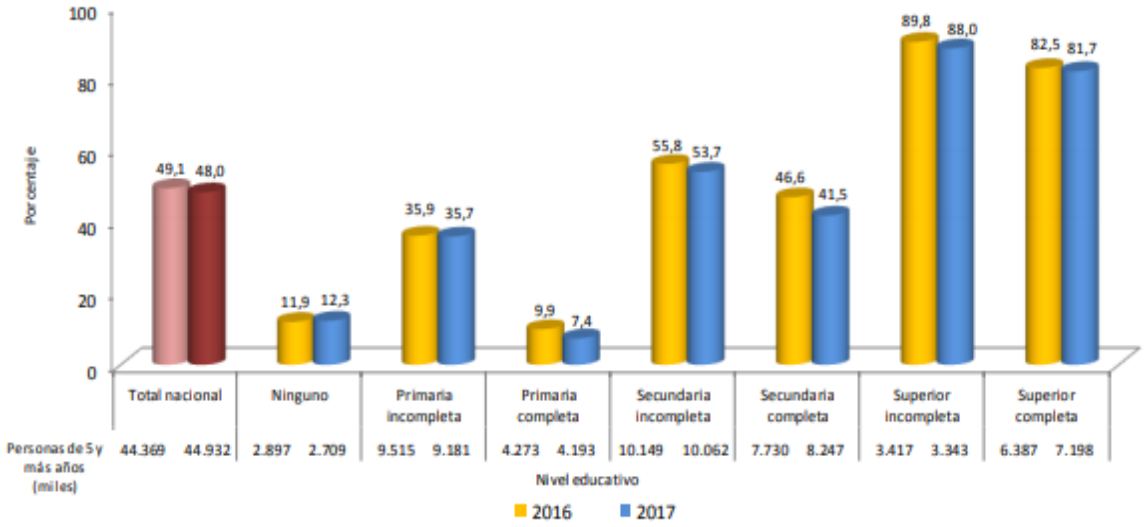


Figura 4. "Proporción de personas de 5 y más años de edad que usaron computador en cualquier lugar según rangos de edad." (2016 – 2017)

Fuente: DANE ECV

El promedio de acceso a internet por parte de los nativos digitales aumenta de acuerdo con los requerimientos que exige el nivel educativo, los intereses sociales, económicos, familiares, culturales, recreativos entre otros.



Fuente: DANE – ECV
* La definición de computador comprende el de escritorio, portátil o tableta.

Figura 5. "Proporción de personas que usaron internet en cualquier lugar, según nivel educativo" (2016 – 2017)
Fuente: DANE ECV

Las estadísticas muestran un alto índice de uso de dispositivos e internet a nivel nacional, que avanza de acuerdo con el nivel educativo de los ciudadanos digitales y el acceso a la tecnología que ofrece las grandes ciudades, sin embargo, existen altos niveles de riesgo de seguridad digital para la comunidad en general y de manera particular, para los menores de edad que presentan mayor vulnerabilidad frente a la garantía de sus derechos fundamentales por la inadecuada gestión informática y tratamiento ilegal de su datos.

El Centro Cibernético Policial de Colombia, presenta un panorama preocupante en el informe Balance Cibercrimen en Colombia, en la medida en que aumentó el 28.30% el índice de delitos informáticos, que responde al reporte de denuncias por delitos informáticos relacionados con el tratamiento ilegal de la confidencialidad en bases de datos personales online relacionado con la compra y venta de información personal de interés, el uso de las redes sociales que vulneran

derechos y de manera particular la incidencia de la ciberdelincuencia en la afectación de la privacidad de los niños: “gromming y sextortion”. (Policía Nacional, 2017, p. 1):

El estudio de la tipología cibercriminal en Colombia muestra un alto índice de casos reportados en relación con la inseguridad digital que involucra en segundo lugar el tratamiento ilegal de los datos personales en el año 2017 Colombia registra datos de: “11.618 denuncias por violación a la Ley 1273 de 2009” (Policía Nacional, 2017, p. 8):

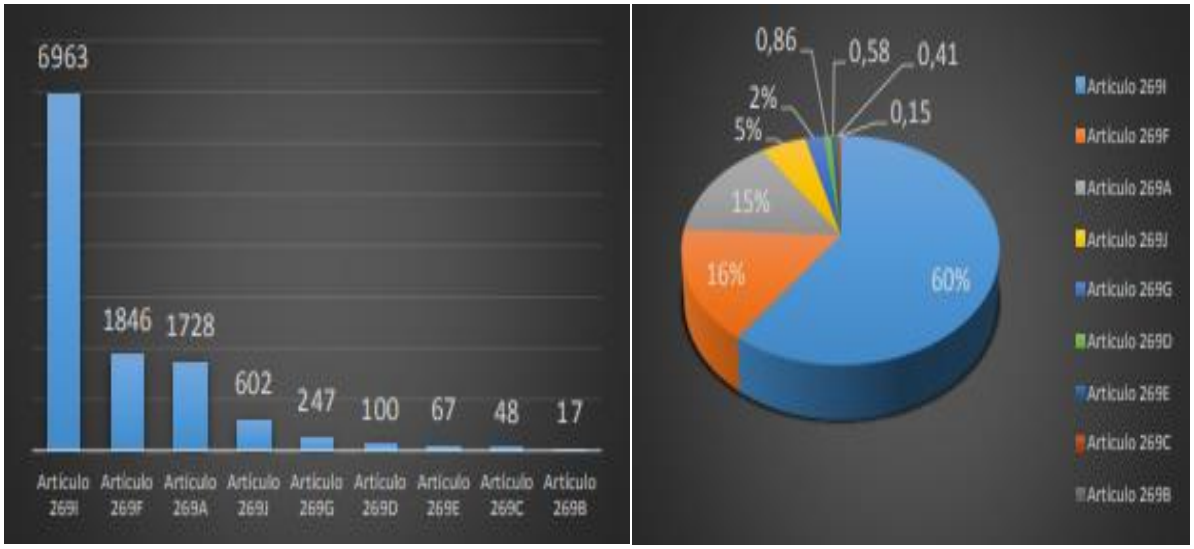


Figura 6. Registro de denuncias por cibercrimen en Colombia
Fuente: Centro Cibernético Policial Colombia, 2017.

La vulneración de datos personales se muestra en la figura 2 del registro de denuncias en un tercer lugar de mayores reportes: “Siendo el “artículo 269I. Hurto por medios informáticos y semejantes” la tipología criminal de mayor frecuencia, equivalente al 60%, seguido del “artículo 269F Violación de datos personales” con 16% y “artículo 269A. Acceso abusivo a un sistema informático.” (Centro Cibernético Policial de Colombia, 2017, p. 8).

Otro registro de interés sobre la suplantación de identidad de NNA está relacionado con la pornografía en la web con fines económicos que amerita la atención del Estado frente a una problemática que cobra más importancia en el mundo. “Durante el año 2017, el CAI Virtual atendió 280 incidentes asociados a la modalidad de GROOMING (la suplantación de un NNA - Niño, Niña y/ Adolescente en la red).” (Centro Cibernético Policial de Colombia, 2017, p. 8).

En la actualidad se hacen esfuerzos por crear aplicaciones como herramientas de gestión de los riesgos de las plataformas digitales en dispositivos móviles para proteger, vigilar y controlar a los menores de edad en forma oportuna y constante como el aplicativo Protectio ideado para ser instalado en los móviles de los niños, niñas y adolescentes, lo cual ha permitido conocer e identificar los moviles de los cibercrimenes e individualizar a los victimarios y victimas.

Figura 7. Protectio.
Fuente: Colombia, Centro Cibernético de la Policia Nacional, Protectio (2019).

Así mismo, el estudio con enfoque diferencial sobre la realidad del uso y apropiación de las TIC, realizado por el Ministerio de las TIC muestra el empoderamiento que ha tenido los ciudadanos frente a la participación online en diversos asuntos de connotación privada o pública

que conlleva a repensar los paradigmas y retos del derecho preventivo y la formación personal de los nativos digitales en esta dimensión:

> "El 10% de los menores entre los 12 y 17 años afirma tener un amigo o familiar que practica sexting"[1]; de otra parte respecto al uso de las redes sociales "el 59% de los colombianos accede a ellas al menos diez veces al día, mientras el 8.1% ingresa más de 50 veces"; de igual manera el aprendizaje de los colombianos respecto al uso de internet muestra que "el 42% lo hizo de manera autodidacta, mientras que el 14% manifestó haber aprendido de un hijo, nieto o sobrino, es decir de la generación de nativos digitales que nació después de 1995." (Min TIC, 2017)

De manera alarmante la investigación evidencia los múltiples riesgos a los que está sometido un niño por falta de conocimiento y acompañamiento en el uso de las tecnologías:

> "A pesar de que el 66% de los colombianos no cree que los menores de edad a su cargo estén seguros cuando navegan en internet, el 64% no los acompaña o asesora, quedando expuestos a riesgos como el gromming, el sexting y el ciber-acoso, entre otros, y además el 72% de los encuestados no están familiarizados con estos términos. (Ministerio de la Tecnología de la Informacion y de las Comunicaciones." (MinTIC, 2017).

Como se observa, existe un alto porcentaje de riesgo o amenaza por la falta de alfabetización digital de los padres, tutores o responsables de los niños y la falta de compromiso de las empresas intermediarias o responsables de la información respecto a la protección de la seguridad de la información personal y la privacidad de los menores de edad con ocasión de los nuevos avances tecnológicos y más aún cuando aumenta de forma exponencial el acceso a internet o disminuye cada vez más la edad de acceso a las redes sociales u otras tecnologías de última generación.

[1] Con el fin de denunciar los abusos contra menores de edad en internet el Estado colombiano habilita canales de prevención contra delitos informáticos como En TIC Confío y Te Protejo (MinTIC-2016) Recuperado: http://www.mintic.gov.co/portal/604/w3-article-15041.html

La Superintendencia de Industria y Comercio (en adelante SIC) muestra un aumento en el reporte de quejas y sanciones a nivel empresarial, por el incumplimiento del adecuado tratamiento de datos personales de los consumidores, usuarios online e incluso niños, niñas y adolescentes que al igual tienen la calidad de consumidor (2019):

Figura 8. Registro de quejas y sanciones de la SIC por violación de datos personales
Fuente: SIC, 2019.

La estadística muestra un significativo aumento de quejas y sanciones ante la SIC, por motivos de falta de autorización del titular del dato, calidad de los datos, desconocimiento de los principios e implementación de políticas de privacidad en el sector empresarial adecuadas al ecosistema digital, con el objeto de lograr una protección integral de todos los ciudadanos, incluyendo de manera especial a los niños que también poseen la condición de consumidores.

Es de resaltar que el modelo de tratamiento de datos personales en Colombia, muestra significativos avances de reconocimiento del derecho a la protección de datos como un derecho fundamental y autónomo que busca salvaguardar la privacidad de la información personal de forma expresa y general en la Constitución Política de 1991. Derecho que integra: "la recolección, tratamiento y circulación de datos" (artículo 15) y el derecho a la información (artículo 20) en escenarios tradicionales que a su vez integran el mundo del internet y los derechos fundamentales de los NNA en virtud del interés superior y prevalente de la familia, la sociedad y el Estado (artículo 44); así como la Ley 1098 de 2006 consagra el derecho a la intimidad de los niños en los diferentes contextos que incluye la interacción sociotecnológica. (artículo 33)

El tratamiento de datos personales presenta un reconocimiento conceptual en el ámbito financiero, comercial y general desde el año 2008 a 2019; sin embargo, cuando se trata de la seguridad de la información que identifica a menores de edad, con sus correlativos derechos, se evidencia grandes vacíos de juridificación con respecto a la garantía del principio de interés superior y mecanismos de protección y prevención integrales que involucra la falta de corresponsabilidad parental en la protección de la intimidad y la educación de NNA.

Ahora bien, como lo refiere Remolina Angarita (2010), se debe acoger los estándares internacionales y lineamientos emitidos por la ONU, la Unión Europea, los Estados Iberoamericanos y los organismos internacionales reconocidos por Colombia, en procura de lograr

mayor pertinencia en la garantía de régimen de gestión y seguridad digital prodata, mediante la homogenización del corpus normativo garantista de un país proactivo frente a la ausencia de autorregulación por parte de los diversos actores y titulares de la información en la red.

De establecer instrumentos jurídicos en el plano nacional que frene o límite a los contenidos en los sistemas tecnológicos y las comunicaciones digitales a los que pueden acceder los menores. Si no existe una autorregulación controlada por el Estado, no existe un marco normativo eficaz de seguridad de la privacidad de la información personal online de los menores, por lo tanto, estos quedan expuestos a contenidos infantiles llenos de violencia, al lenguaje subliminal de consumo de productos de las grandes cadenas, tales como cigarrillos, alcohol, sustancias psicotrópicas o alucinógenos, y a un desarraigo de los valores sociales; que todo en conjunto afecta la personalidad de menores de edad interactivos en la digitalización.

1.2. Formulación del problema

La presente investigación responde a una pregunta problema armonizada en un contexto jurídico y tecnológico que rodea la privacidad de los menores de edad como sujetos de derecho de especial tratamiento de acuerdo con las siguientes categorías:

¿En qué medida el tratamiento de datos personales de los niños, niñas y adolescentes que consagra el ordenamiento jurídico colombiano, se adecua a los “Estándares de Protección de Datos Personales para los Estados Iberoamericanos” en el marco de la “Convención sobre los derechos del niño”, el derecho a la privacidad como derecho humano y la gestión de riesgos de seguridad digital?.

2. Objeto de la investigación

El objeto del presente estudio investigativo se basa en el análisis del régimen de protección de datos personales de niños, niñas y adolescentes de Colombia frente a los estándares de protección de datos personales para los Estados Iberoamericanos mediante el estudio del marco histórico - jurídico, dogmático, descriptivo y documental, del desarrollo del derecho a la privacidad como derecho humano, los modelos y referentes jurídicos internacionales y la gestión del riesgo de la seguridad digital.

Como guía para el desarrollo específico del trabajo se describe la génesis del derecho al tratamiento de datos personales de niños, niñas y adolescentes bajo el enfoque basado en los derechos humanos y las nuevas tecnologías de la información; la identificación de los modelos de tratamiento de datos personales y estándares internacionales de protección de datos personales que han fundamentado la construcción del tratamiento de datos personales en Colombia, y en particular el régimen de tratamiento de datos personales de los niños; la adecuación del tratamiento de datos personales en Colombia a los “Estándares de Protección de Datos Personales para los Estados Iberoamericanos” y los mecanismos proactivos de gestión integral de la seguridad digital de los datos personales de los menores de edad.

3. Hipótesis

Para el desarrollo de esta investigación se ha planteado la siguiente hipótesis:

Hi: El régimen jurídico de datos personales de los menores de edad consagrado en el ordenamiento jurídico colombiano, no se adecua a los “Estándares De Protección de Datos Personales de los Estados Iberoamericanos” en el marco de la juridificación y la gestión del riesgo digital.

No obstante, existe un avance normativo significativo en el tratamiento de los datos personales de carácter general, que se refleja en los instrumentos legales vigentes, por medio del reconocimiento constitucional del carácter autónomo del derecho a la protección de datos personales con una mirada garantista frente a las tecnologías de la información y las comunicaciones; sin embargo, se requiere de mecanismos jurídicos acordes a la protección integral e interés superior del niño con relación al derecho a la privacidad de su información personal en la era digital. Es por ello, que se requiere armonizar la legislación a los “Estándares Internacionales de Tratamiento de Datos Personales de los Estados Iberoamericanos” que posibiliten la implementación de programas integrales de gestión de datos personales de niños, niñas y adolescentes con el fin de contrarrestar los riesgos propios de la era digital.

4. Enfoque metodológico

El presente trabajo acoge el tipo de investigación sociojurídica, basado en el método sistémico, en cuanto parte de una "precomprensión"[2] del lenguaje informático jurídico desde la perspectiva social, que se acerca a la dimensión histórica y desarrollo del "derecho a la privacidad y la protección de datos personales" de los niños en un contexto relacionado con las nuevas tecnologías de la información frente al riesgo digital. Como lo refiere Troncoso Reigada al plantear soluciones equilibradas a problemas concretos del inadecuado e ilegal tratamiento de datos personales que se presentan en la realidad tecnológica:

> "a llevar a cabo una labor de ponderación y a aplicar el principio de proporcionalidad. Esto supone desterrar los fundamentalismos y las posiciones extremas, que se han dado entre los defensores de la protección de datos, pero también entre los que mantienen otros planteamientos". (2010, p. 35-36).

Se presenta el análisis de la naturaleza jurídica del tratamiento de la privacidad y los datos personales con base en el estudio del derecho positivo actual y los estándares de protección internacionales de datos personales relacionados con los niños, niñas y adolescentes en el marco de los derechos humanos y las garantías de protección por parte de los Estados, como lo ilustra Giraldo:

[2] "Precomprensión" a la luz de Larenz con relación a la interpretación de las normas jurídicas: "no sólo contienen una regulación que pretende validez jurídica, sino que regulan determinadas relaciones sociales, procesos y modos de comportamiento, en los que la circunstancia de ser regulados por el Derecho muestra a su vez sólo uno de los aspectos bajo los que se manifiestan. El jurista que no llega a ver nada de otros aspectos, tampoco comprenderá su relación jurídica". (1979. p. 196-199)

> “El objeto en la investigación sociojurídica son los comportamientos sociales prescritos en las normas, entendidas éstas como las hipótesis que formula el Estado acerca de las conductas que hay que realizar, o las instituciones que hay que crear, para alcanzar los fines políticos que se propone en un momento histórico determinado, teniendo en cuenta las condiciones situacionales concretas en que el proceso se debe realizar.” (2010, p 107)

Por lo tanto, la investigación utiliza el proceso cualitativo y descriptivo de las variables objeto de estudio tales como estándares, directivas y mecanismos de protección, conceptos, teorías y paradigmas propios de la interacción con comunidades tecnológicas o cualquier otro fenómeno que sea sometido a análisis con el propósito de reconocer y describir los contextos sociales y jurídicos en las que se desenvuelven e interactúan los niños como factores determinantes de la responsabilidad proactiva.

Y acoge el pensamiento sistémico como el método científico guía, característico de acuerdo al planteamiento metodológico que representa la realidad que a su vez brinda orientación en entornos transdisciplinarios; además de las características holísticas fundamentadas en las relaciones del individuo y la sociedad mediante la cual se fomente un ambiente de relación y comunicación social.

En este orden de ideas, desde un contexto evolucionista ha de traerse a colación al biólogo Austriaco Karl Ludwig von Bertalanffy (1968), a quien se le atribuye la primera denominación de la “Teoría General de Sistemas”; la cual corresponde a un mecanismo de integración, articulación, armonía e interdependencia entre las ciencias naturales y sociales. Es decir, se crea con el propósito de explicar y comprender los principios que rigen la composición de la fenomenología de la naturaleza y hoy se aplica a diferentes áreas del conocimiento relacionados con la socio tecnología. (Hernández, 1989).

No obstante, el método sistémico fue estudiado por varios autores (Von Bertanlaffy, Beer, Ackoff, Forrester, Checkland, etc.), aunque finalmente es atribuido a Peter Senge, cuyo propósito buscaba corroborar herramientas metodológicas e innovadoras mediante las cuales permita modificar las prácticas sociales de manera organizada en un entorno integrado, holístico y sistémico. Por lo tanto, el pensamiento sistémico se define a través del constructo mental que comprende la razón de ser del funcionamiento de un sistema de brinda solución a una problemática que se compone de elementos emergentes. Pensamiento holístico que integra el conjunto en su todo y sus integrantes, al igual que su conectividad. (1990).

La aplicación del pensamiento sistémico ha tomado especial importancia en la actualidad, toda vez, que ha sido considerado un elemento de evolución social fundamentado en la "dinámica de sistemas", desarrollada por Jay Forrester y algunos académicos en el MIT (Massachusetts Institute of Technology) para explicar la dinámica de sistemas, que permite la comprensión de lo complejo de las relaciones humanas a gran dimensión.

Sistemas de gran escala que son estudiados, de acuerdo a los métodos en la investigación jurídica como lo refiere Villabella Armengol (2015), al referirse al significado del método sistémico-estructural-funcional en el contexto de los casos complejos como aquel conjunto de partes que se relacionan y se articulan entre sí para formar una unidad que es el sistema y que de forma cualitativa permite aclarar la pirámide de jerarquía de los componentes del tema de investigación y las interconexiones intra o intersistémicas en la dinámica de interpretación de los principios dogmáticos como es el régimen jurídico internacional y nacional de la protección de la privacidad y la información personal de los menores de edad.

De otra parte, la presente investigación aplica la técnica documental relacionada con la exploración, identificación, recolección e interpretación bibliográfica en físico y bases de datos,

elaboración de fichas bibliográficas que se traducen en sistematización de la información, elaboración de diversas tablas, gráficos y conclusiones que se presentan en el desarrollo del tema, gracias a las fuentes primarias y secundarias consultadas y analizadas sobre su tratamiento a nivel nacional e internacional.

La técnica exploratoria de las ciencias sociales para la obtención de información clave que ayuda al investigador a aproximarse a las fuentes de conocimiento y la experiencia investigativa de temas tan novedosos como el derecho frente a las tecnologías, se gestiona con la aplicación de entrevistas estructuradas (grabadas) a la Superintendencia Delegada para la Protección de Datos Personales de la Superintendencia de Industria y Comercio como ente de inspección, vigilancia y control de su tratamiento y a expertos académicos de Colombia y España; el ejercicio de consulta a las entidades públicas de Colombia tales como el Ministerio de las Tecnologías de la Información y las Comunicaciones, el Instituto Colombiano de Bienestar Familiar y la Fiscalía General de la Nación que evidencian registros del desarrollo e implementación del tratamiento de los datos personales a la luz de la Política Nacional de Seguridad Digital.

La participación a los Congresos Internacionales de Protección de Datos Personales, organizados por la Superintendencia de Industria y Comercio[3] y la estancia académica internacional a la Universidad de Valencia en España, permitieron ahondar en el estudio de los paradigmas, desafíos y retos que representa el tratamiento jurídico de la protección de datos personales a nivel global, la implementación de programas integrales de gestión de datos personales de la infancia en la era digital, incidentes de seguridad, la responsabilidad demostrada

[3] Los congresos Internacionales de Protección de Datos Personales organizados por la Superintendencia de Industria y Comercio en Colombia se han venido desarrollando anualmente desde el año 2013, como un escenario de intercambio de conceptos y teorías respecto a los desafíos y retos del adecuado tratamiento de la información personal y su relación con la garantía de los derechos fundamentales, económicos, sociales y culturales, incluso derechos colectivos relacionados con experiencias empresariales.

(Accountability) como un principio consagrado en los estándares internacionales de protección y las guías de privacidad impulsado por la Comunidad Europea y la Red Iberoamericana de Protección de Datos Personales.

Así como, la elaboración y publicación de artículos de investigación permitió un acercamiento a la comprensión del contexto iusinformático en su orden: Galvis, (2012) Protección de Datos Personales en Colombia: Avances y Retos, No. IV, Revista Lebret USTA, P. 195-214, Galvis, (2018); El panóptico digital de la protección de datos personales en Colombia, Revista Temas USTA, Galvis y Salazar (2018); Alcance del derecho al olvido en el tratamiento de datos personales en Colombia. Revista Verba Iuris p. 45-63 y un Capítulo del libro titulado: La Cuarta Revolución y el Derecho: Galvis, L. (2019) Panóptico digital de la libertad de expresión en las redes sociales p. 315 – 335.

Capítulo I: Génesis del derecho a la protección de datos personales de niños, niñas y adolescentes a nivel internacional

La revolución tecnológica y la expansión global de internet han permitido un giro ontológico y autopoiético de la privacidad, tanto en la reconstrucción de las relaciones del hombre en su interior, para con sus pares y para con la naturaleza misma de manera plurifacética y autoreferencial, en cuanto se facilita y complejiza a la vez la comunicación y el acceso a la información superando los límites de modo, tiempo y lugar de interacción en internet de manera exponencial en la sociedad de la transparencia y sin control absoluto de la gobernanza digital.

Porque como lo refiere Byun- Chul Han:

> "En la modernidad se renuncia cada vez más a la distancia teatral a favor de la intimidad. El mundo no es hoy ningún teatro en el que se representen y lean lecciones y sentimientos, sino un mercado en que se exponen, venden y consumen intimidades. El teatro es un lugar de representación, mientras que el mercado es un lugar de exposición." (2018, p. 68)

Esta metamorfosis incide de manera significativa en los sistemas jurídicos por su principal justificación: La paz y la seguridad como principal preocupación de los Estados por conseguirla como fundamento de una historia colectiva, cuyo símbolo emblemático es la "sociedad de la información", o la "sociedad informatizada", como lo señala Perez Luño, en cuanto al diseño de nuevos instrumentos de análisis y marcos conceptuales de orden jurídico apropiados para una sociedad en constante transformación (1986).

Frente a uno de los debates técnicos jurídicos que surgen de un cúmulo de problemas de carácter fundamental propios del mundo de la comunicación digital, es el relacionado con la protección a la privacidad de la información personal de NNA que se encuentra en proceso de construcción y consolidación de la arquitectura como derecho y de especial protección en la era tecnológica que advierte el reconocimiento y cooperación de los Estados para garantizar el adecuado tratamiento jurídico, técnico y administrativo de los datos en el ámbito público y privado de acuerdo a los estándares internacionales de privacidad y gestión integral.

La exigibilidad del derecho de acceso a internet como lo refiere Torres Ávila (2015), implica la protección de otros derechos entre los que sobresale "la protección de datos personales", como una herramienta para el desarrollo de otros derechos y valores constitucionales, tales como: habeas data, la intimidad, el buen nombre, la seguridad social, la salud, el trabajo, la libertad de cátedra, la libertad de expresión, la propiedad entre otros relacionados con el acceso y uso de las TIC.

En este capítulo se analiza la génesis y construcción del "derecho a la protección de datos personales" en el marco de los derechos humanos y la sociedad de la tecnología frente a la seguridad de la información personal de los menores en la era digital. Para ello hay que acotar la investigación a aquellas teorías, instrumentos internacionales y nacionales relacionados con la garantía del derecho a la vida privada e intimidad del niño en el ámbito de la visión ius-informática de la privacidad, no en el sentido de regulación de una tecnología concreta (evidentemente, antes de los ordenadores no podía existir normas jurídicas que regularan su uso), sino en el de su finalidad, propósito o "ratio", que es controlar el uso de la información personal para que los ciudadanos digitales no se les vulnere sus derechos, su dignidad, sus bienes o sus intereses legítimos y posibiliten el ejercicio de su derecho de autodeterminación informativa.

1.1. Referente histórico del "derecho a la privacidad y la protección de datos personales"

El contexto histórico y dogmático del derecho a la protección de datos personales presenta un acercamiento a la primera manifestación doctrinal de la Privacy de Warren y Brandéis: *"el derecho a ser dejado solo"* entre otras reformulaciones conceptuales, la construcción normativa a nivel internacional del derecho a la vida privada como un derecho humano en el marco del tratamiento de datos personales y los primeros referentes de la privacidad de datos personales de los niños en Colombia.

1.1.1. La privacidad como derecho individual, humano, global y tecnológico

La idea de intimidad basada en el enfoque de privacidad como se percibe en el tratamiento de los datos personales surge y evoluciona desde el siglo XIX, con ocasión del proceso de los primeros orígenes de la tecnología (1960 – 1970), la construcción de la teoría del liberalismo, la burguesía y el individualismo, con ocasión de un entorno dialéctico de lo público y lo privado, como lo refiere Parejo:

> "el sustrato y el fundamento, pues, de la intimidad actual no es otro que el largo proceso histórico de radical transformación de la conciencia que comienza con la contrarreforma, sigue con la desvalorización de la conciencia religiosa por los filósofos del siglo XVII (Hobbes, Locke, J.S. Mill, Descartes, Spinoza) y desembocan en la construcción de la conciencia moral, preparada por Thomasius y concluida por Kant". (1994, p. 293).

Al igual que enfatiza Garriga respecto a la fenomenología del derecho a la intimidad éste se construye de la mano con lo público bajo una proclama de libertad y autonomía:

> "En su evolución histórica, lo íntimo y lo privado se han ido desarrollando a costa de lo público" … La vida íntima y privada ha ido creciendo a medida que se ha ido limitando el ansia expansionista del poder político. Así, de la idea de la confrontación de la idea de libertad frente al omnipresente poder público". (2009, p. 20).

De ahí que, de la confrontación entre la idea de libertad frente al poder político, aparece el derecho a la intimidad como ese dominio privado que permite la realización humana, en un contexto de: "un conjunto de poderes y facultades para garantizar la exclusión del Estado en el ámbito más propio del individuo". (Garriga, 2009, p. 20).

Y es así que una de las dinámicas emergentes de la sociedad contemporánea reconoce el derecho a la vida privada como un derecho humano producto de un proceso de múltiples cambios, como lo resalta Travieso:

> "Es así que los cambios del sistema económico produjeron el capitalismo y el auge de la burguesía que impulsó el desarrollo, la generalización e internacionalización de los derechos humanos. Los cambios en el poder político generaron el Estado caracterizado como un poder racional, centralizado y burocrático, sin el cual no hay derechos humanos." (Travieso, 2014, p. 49)

En este orden, se hace necesario asimilar el proceso evolutivo del derecho a la vida privada como derecho humano en conexidad con la tecnología, el carácter dinámico respecto a la proyección de la informática y el estructuralismo, el cual busca construir una ciencia de los derechos humanos y su consecuente delimitación conceptual en el ámbito de la metodología filosófica, la cibernética e informática. (Pérez Luño, 2003).

Ahora bien, las etapas evolutivas del derecho a la vida privada; conquista de un derecho de carácter individual a un derecho humano construido en un contexto multidisciplinario y evolutivo del sistema social se visibiliza en el siguiente contexto:

Tabla 3.

Etapas de reconocimiento del derecho a la vida privada

Aspecto	**Siglo XVIII**	**Finales del siglo XIX y mitad del siglo XX**	**Ultima mitad del siglo XX y siglo XXI**
Instrumentos normativos	Declaración de Derechos de Virginia (1776, goce de la vida) la Declaración de Independencia de los Estados Unidos (1776) y las sucesivas Declaraciones de los Derechos del Hombre y del Ciudadano de la Revolución Francesa. (1789) Derechos Civiles y políticos.	Declaración Universal de Derechos Humanos Resolución 217 A (III), París, 10 de diciembre de 1948. Convenio para la protección de los Derechos Humanos y las Libertades fundamentales - 1950 Derechos económicos, sociales y culturales	Pacto Internacional de Derecho Civiles y Políticos Resolución 2200 – 1966 – 1976 Declaración de Viena, 1993) Reafirmación del derecho al desarrollo en búsqueda de la realización del ser humanos y de los pueblos Derechos globales y tecnológicos
Reconocimiento de la vida privada y otros derechos	"Preconizaba la autonomía como principal distintivo del ser humano", cuya proclama era la libertad, configurándose así "derechos relativos al aislamiento, entre ellos: el derecho al honor, a la vida, a la integridad personal" e incluso de forma rudimentaria el propio	Garantiza "el bienestar económico, el acceso al trabajo, la educación y a la cultura, de tal forma que asegure el desarrollo de los seres humanos y de los pueblos." "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona	"No. 1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia… 2. Toda persona tiene derecho a la protección de la ley…" en conjunto al desarrollo del derecho a la información. Artículo 19 No. 2 "Toda persona tiene derecho a la libertad de expresión;" (Artículo

Aspecto	Siglo XVIII	Finales del siglo XIX y mitad del siglo XX	Ultima mitad del siglo XX y siglo XXI
	derecho a la intimidad personal.	tiene derecho a la protección de la ley contra tales injerencias o ataques." (Declaración Universal de los Derechos Humanos, 1948, Artículo 12). Establece "toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y correspondencia". (Convenio para la protección de los derechos humanos y las libertades fundamentales, 1950, Artículo 8 No. 1)	17 Pacto Internacional de Derecho Civiles y Políticos Resolución 2200 – 1966 – 1976) "Las nuevas relaciones que conllevan los fenómenos citados, con la naturaleza y de los seres humanos entre sí, propician la aparición de un nuevo tipo de Derechos Humanos que, sin olvidar los anteriores, recoja las preocupaciones y retos que dichas tecnologías y movimientos sociales representan para el mundo actual"

Fuente: Creación propia basada en Ornelas (2004) y Álvarez - Cienfuegos (2007), Travieso, J. (2014), Subrayado fuera de texto.

La etapa del siglo XVIII, muestra en primera instancia el reconocimiento del derecho a la vida privada como un derecho de carácter individual muy personal, cuyo rasgo característico es la autonomía del individuo, la perspectiva de libertad para todos los seres humanos y de singular protección con una mirada integral, interdependiente y complementaria frente a la materialización de los derechos y su respectiva garantía frente a la ‘‘libertad de’’, la ‘‘libertad para’’ y la ‘‘libertad con’’ los demás." (Álvarez-Cienfuegos Fidalgo, 2007, p.13).

De otra parte, las nociones de libertad expuestas por John Locke, entendidas como un estado que permite a cada individuo: "(...) ordene sus acciones y disponga de posesiones y personas como

juzgue oportuno, dentro de los límites de la ley de la naturaleza, sin pedir permiso ni depender de la voluntad de ningún otro hombre" (Locke, 2006, p. 10).

Es decir, el ámbito privado entendido como el espacio más apropiado para el libre desarrollo del pensamiento y de las acciones individuales libre de interferencias externas. La privacidad entendida como la esfera y centro de la autonomía del individuo en palabras de Kant:

> "El concepto de autonomía articula la idea de libertad individual. Pues, refiere «la voluntad como universalmente legisladora» que desarrolla «la idea de dignidad de un ser racional que no obedece a ninguna otra ley que aquella que él se da a sí mismo». «La autonomía es, pues, el fundamento de la dignidad de la naturaleza humana y de toda naturaleza racional" (Kant, 1983, pp. 92-94).

Zona privada en la que el individuo es soberano e independiente y cuyo conjunto permite reflejar materialmente la libertad de conciencia, de pensamiento y de expresión, como también la libertad de elegir y decidir sobre nuestras preferencias e intereses y la libertad de asociación, como lo refiere Mill, haciendo hincapie de lo privado y su motivo de existencia ligado directamente con el sentido del reconocimiento y ejercicio público de las libertades básicas para la sociedad. (1981).

Es decir, los límites al control o panóptico clásico sobre el ejercicio arbitrario del poder público en la esfera privada del individuo:

> "Los derechos humanos son concebidos como derechos de defensa de las libertades del individuo que exigen la no injerencia de los poderes públicos en su vida privada; la acción del Estado, entonces, queda limitada a preservar el orden público, algo así como una mera policía administrativa". Travieso, J. (2014)

A finales del siglo XIX el derecho a la intimidad o privacy se expresa como una categoría doctrinal e independiente en la comunidad anglosajona y su gran desarrollo normativo

internacional se da en el transcurso del siglo XX con el reconocimiento de la Declaración Universal de los Derecho Humanos ONU 1948, la construcción constitucional en Europa, en la cual sobresale Portugal (1976) con la primera Constitución que refiere al derecho a la intimidad (Art. 26.1), algunos ejemplos como la Constitución Española (1978, Art. 18), Ley fundamental de Bonn (1949, Art. 2) y la Constitución Italiana (1947, Art. 2), entre otras diversas regulaciones garantistas, que muestran un proceso de evolución del derecho a la privada en concordancia con el desarrollo de la tecnología.

Se reconoce "*ya no una mera igualdad formal, igualdad ante la ley, sino una igualdad de contenidos,* que podría ser equiparada a la libertad positiva, a una ''libertad para'', de tal forma que esta es concebida no sólo como el resguardo frente a la acción del Estado, sino que le exige al poder político la creación de unos mínimos sociales comunes a todos sus ciudadanos." Travieso, J. (2014) (Cursiva fuera de texto)

Ahora bien, el siglo XX y XXI se traduce en el reconocimiento de la vida privada en consonancia con los derechos sociales económicos y culturales de la era de la tecnología y la información, los cuales han tenido origen en la misma época, como lo expresa Travieso. Se incentiva el progreso social con base en la dimensión tecnocientífica que fundamentan la creación de nuevos derechos de carácter global, con una visión de multiculturalidad y civilidad propia de la modernidad contemporánea de todos los Estados. (2014)

Y denotan al igual que señala Garriga, los primeros cimientos del derecho a la protección de datos personales, el cual se circunscribe en el derecho a la vida privada enmarcado en los derechos y libertades del hombre en sus relaciones sociales y con el status de derecho humano, a partir del 10 de diciembre de 1948 con la Declaración Universal de Derechos Humanos de las Naciones

Unidas y otros instrumentos internacionales de especial relevancia e inspiración a los Estados para su fundamentación:

Tabla 4.

Instrumentos legales de carácter universal del derecho a la vida privada

Organización y país	Año	Instrumentos normativos
Organización de Naciones Unidas (ONU)	1948	**Declaración Universal de Derechos Humanos (**en adelante DUDH), señala el inicio normativo del derecho a la protección de los datos personales con el reconocimiento del derecho a la vida privada: "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques" (ONU, DUDH, artículo 12). Subrayado fuera de texto
Colombia – Bogotá	1948	**Declaración Americana de los Derechos y Deberes del Hombre (**en adelante DADDH**) señala**: "Toda persona tiene derecho a la protección de la Ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar." (DADDH, artículo V.)
Consejo de Europa en Roma	1950	**"Convenio para la protección de los Derechos Humanos y las Libertades fundamentales" reconoce por primera vez el derecho a la intimidad en Europa**: "toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y correspondencia". (Artículo 8 No. 1)
Nueva York	1966	**Pacto Internacional de Derecho Civiles y Políticos** "1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia…2. Toda persona tiene derecho a la protección de la ley…". De igual manera se da paso al reconocimiento expreso al derecho a la información (Artículo 17) y "Toda persona tiene derecho a la libertad de expresión; …" (Artículo 19 No. 2)
Asamblea del Consejo de Europa	1968	Recomendación 68/509 sobre "los derechos humanos y los nuevos logros científicos y tecnológicos"

Organización y país	Año	Instrumentos normativos
Costa Rica (San José de Costa Rica)	1969	**Convención Americana de Derechos Humanos:** "Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación." (Articulo 11 No. 2, enmarcado en el Derecho a la honra y la dignidad)

Fuente: Creación propia basada en la normatividad de la vida privada como derecho humano 1948 - 1969

Cada regulación responde al nivel de concordancia con el reconocimiento internacional del derecho a la vida privada como derecho humano desde 1948 con un enfoque reactivo frente a las arbitrariedades o abusos de poder que afecten la reputación y la dignidad humana personal, familiar, domicilio y las comunicaciones relacionadas con la correspondencia, así como la protección de su entorno social y los logros científicos y tecnológicos propios de finales del siglo XX.

De otra parte, el Derecho Internacional de los Derechos Humanos ha sido el medio para encarar esta lucha entre el derecho y la tecnología que surge de la necesidad de proteger la información personal ante la realidad tecnológica actual, que exige el reconocimiento de la protección de la privacidad como derecho indiscutible de la persona humana. (Hassemeer & Chirino, 1997)

Los principios del Derecho Internacional de Derechos Humanos fundamentan la salvaguarda universal de las garantías judiciales, siendo de especial prevalencia en la sociedad interactiva y con mayor determinación la exclusión e inclusión en el mundo de la digitalización, la privatización y génesis de redes globales como lo refiere Travieso:

> "Surge la necesidad de proteger adecuadamente los derechos humanos de la sociedad democrática que debe realizar un delicado equilibrio entre la transparencia de la información y

el respeto de los ámbitos de privacidad, ubicado esta última dentro de un amplio concepto social. La privacidad será entendida, en consecuencia, no como un derecho de una sociedad individualista y disgregada. Será, en fin, un derecho que se fundamente en la integración social dentro de la sociedad democrática que dará lugar a la nueva disciplina de la protección de datos personales con una presencia real de los seres humanos en la organización social y política." (2014, p. 6).

Hoy, la sociedad de la información requiere de diseños tecnológicos que reconozcan el derecho a la autodeterminación personal como un derecho humano de integración social, que respondan al derecho a superar la ignorancia digital, a repensar paradigmas, variables y categorías propias de las realidades y redes tecnológicas: Skype, Facebook, YouTube, Twitter entre otras inimaginables.

1.1.2. La protección de datos personales como un derecho proactivo basado en el enfoque de los derechos humanos

En el siglo XX, los Estados en su mayoría iniciaron un proceso de reconocimiento del derecho a la vida privada como un derecho humano (1948), el cual cimentó el reconocimiento del derecho a la protección de datos personales (1970 a 1973) con las primeras normas de Alemania y Suecia, que luego trascienden a nivel global de acuerdo a los desarrollos de la ciencia, la tecnología e innovación.

Figura 9. Línea del tiempo de los instrumentos normativos en materia de privacidad y protección de datos personales.

Fuente: Creación propia basada Travieso y los instrumentos normativos PDP a (2018). (Aclaración Latinoamérica recoge la normativa vigente de 2000 a 2008).

El tratamiento jurídico de los datos personales a nivel mundial ha sido progresivo bajo un enfoque de protección a la vida privada como un derecho humano de reconocimiento internacional y de valoración legal por cada Estado en particular bajo un modelo centralista y/o sectorial de protección.

Uno de los referentes normativos importantes en la construcción de derecho a la protección de datos personales ha sido la Unión Europea, el cual se ha consolidado desde 1970 a través de resoluciones, directivas y reglamentos que han sido fuente de inspiración frente a la regulación local del derecho fundamental a la intimidad del niño en un escenario informativo tecnológico:

Tabla 5.

Instrumentos normativos de protección de datos personales de la Unión Europea

Organización y país	Año	Instrumentos normativos
Asamblea consultiva del Consejo de Europa	1970	Resolución 428, indica que la intimidad debe protegerse frente a la injerencia arbitraria de la tecnología
Consejo de Europa	1973	Resolución de 1973: Fijó pautas para la protección de datos en el sector público y se detallaron los principios básicos de operación de datos, como el de exactitud, finalidad y licitud en la obtención de la información, el derecho al acceso por parte del ciudadano, el régimen estricto de conducta para quienes operan la información y la aplicación de mínimos de seguridad.
Unión Europea	1981 1995	El primer convenio internacional de protección de datos fue firmado en 1981 por Alemania, Francia, Dinamarca, Austria y Luxemburgo. Es conocido como “Convenio 108” o “Convenio de Estrasburgo”. Se crea una norma común que se denominó Directiva 95/46/CE, referente a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
Unión Europea	2016	El Parlamento Europeo y del Consejo establece “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” e incorpora de manera particular el alcance de

Organización y país	Año	Instrumentos normativos
		la protección de datos personales de los menores de edad. (Reglamento (UE) 2016/679).

Fuente: Creación propia basada en la normativa de PDP UE

La normativa reconoce el deber de los Estados de garantizar la privacidad, confidencialidad, tecnología y seguridad que caracteriza la sociedad de la información y donde el valor de los datos transversaliza las relaciones personales, sociales, comerciales, culturales y políticas independientes de su fuente y naturaleza.

Por lo tanto, alrededor de más de 100 países en el mundo han acogido con diversas denominaciones el tratamiento jurídico de datos personales, ya sea por norma constitucional o por legislación específica, como se presenta en las siguientes gráficas y tabla (Banisar, 2016):

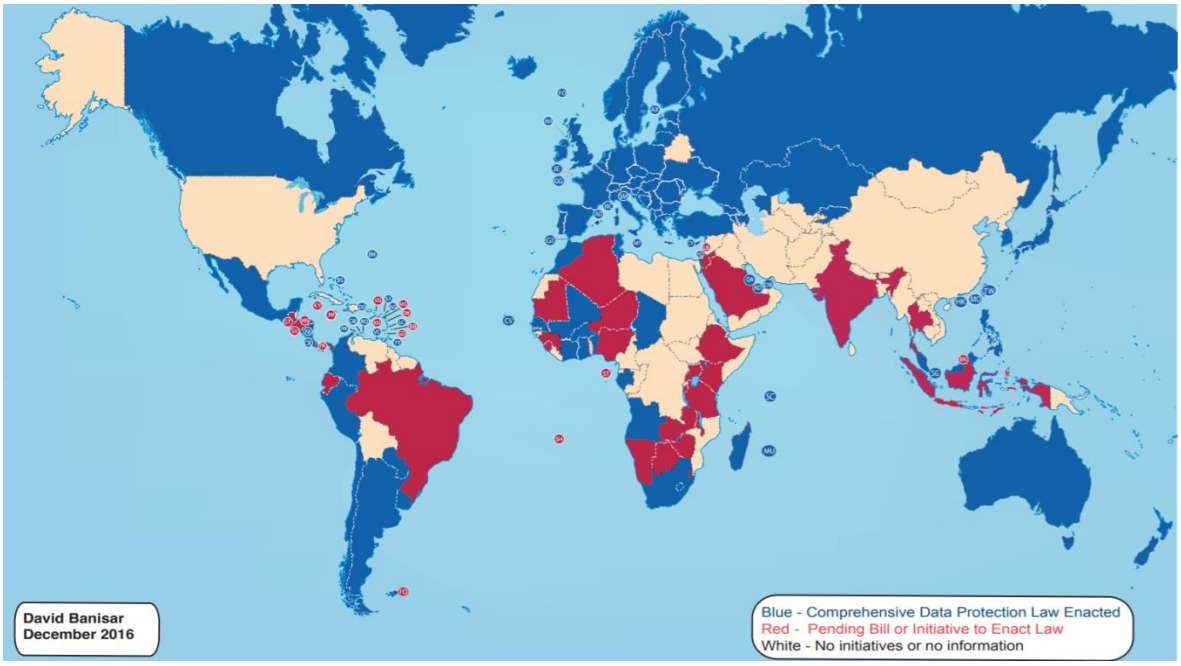


Figura 10. Mapa mundial de protección de datos personales

Fuente: Creación Banisar David (2016)

- Azul: Promulgada una Ley integral de protección de datos,
- Rojo: Pendiente de esfuerzo u obligación de promulgar leyes
- Blanco: Ninguna Ley

Se evidencia un significativo avance en la juridificación de la protección de datos personales como una proclama de contrarrestar toda arbitrariedad y salvaguardar la privacidad, el libre desarrollo de la personalidad, la autodeterminación informativa de todos los seres humanos independientemente de su condición, raza e ideología. Sin embargo, existen aún un amplio número de países que muestra desconocimiento y desinterés por su regulación y adecuada protección.

La línea del tiempo normativa de protección de datos personales parte del reconocimiento jurídico de un derecho humano identificado como: Vida privada que con la incidencia de las tecnologías de la sociedad de la información se autoreferencia en un ecosistema social e informático donde sobresale el principio de confidencialidad, datos sensibles, legalidad del consentimiento del titular y la responsabilidad proactiva frente al derecho a la información desde la privacidad por diseño y por defecto, la autorregulación y gestión de riesgos de seguridad digital.

Tabla 6.

Países que han regulado la protección de datos personales 1970 - 2018

Organización y país	Año	Ley de privacidad y protección de datos personales
Alemania	1970 - 1977	Primer régimen legal para el tratamiento de datos en el Estado de Hesse Alemania. Se faculta al "Comisario parlamentario de protección de datos para velar por la confidencialidad en el manejo de los datos", cuyo objetivo fue proteger las personas naturales frente a la injerencia de las autoridades y servicio de inteligencia estatal respecto al tratamiento informatizado de los datos de las personas, así como otros entes sujetos al control estatal. (Ley Datenschutz 1970 y Ley Federal Bundesdatenschutzgesetz 1977)

Organización y país	Año	Ley de privacidad y protección de datos personales
Suecia	1973	Una de las primeras regulaciones que prohíbe la "creación de registros de datos sensibles frente a las personas" (Ley No. 289)
Estados Unidos de Norteamérica	1974	Busca proteger a la persona frente a datos de índole personal, que se ponen en conocimiento del público o de terceros sin el consentimiento del afectado" (Privacy Act)
Portugal	1976	El derecho a la información y el uso de bases de datos (La Constitución de Portugal)
Reino Unido	1981	Registro de información de las personas ante organismo gubernamental (Data Protection Act.)
España	1999	La ley Orgánica 15 de 1999, establece la Protección de Datos de Carácter Personal. Latinoamérica ha utilizado esta ley como referente importante del modelo europeo
Rusia	2006	Ley de protección de datos personales.
América Latina	2000-2018	En América Latina surgen las leyes de protección de datos personales con ocasión de la influencia iusinformática del modelo europeo y dado los requerimientos de la revolución tecnológica, los riesgos y afectaciones a los derechos de las personas en diferentes dimensiones. Argentina la Ley 25.326 (2000), Chile (1999), Panamá (2002), Brasil (1997), Paraguay (2000), Uruguay (2008), Perú La ley 29.733 del 2 de julio de 2011, "Ley Federal de Protección de Datos Personales en Posesión de Particulares" (Diario Oficial de la Federación, 2010 - 2012) y Colombia (2008) La Ley 1266 Habeas Data Financiero, Crediticio y Comercial y Ley Estatutaria de Protección de Datos Personales de Carácter General (2012) 1581 y sus decretos reglamentarios y sectoriales a 2018

Fuente: Creación basada en Travieso, J. (2014) y actualizada a 2018

El avance en la regulación a nivel mundial ha sido progresivo y continúo, el proceso de adecuación se encuentra en una etapa de consolidación de acuerdo a los estándares internacionales de tratamiento de datos personales, siendo Alemania uno de los primeros países que estructuró su normativa con base en la confidencialidad y la protección de la persona titular de la información.

Para el caso colombiano cuenta con la Ley Estatutaria de Protección de Datos Personales (2012) que se identifica ampliamente con el modelo europeo (centralizado) y en más limitada proporción con el modelo de Estados Unidos (sectorial), por su aporte normativo, órganos de control y vigilancia, principios, responsabilidad demostrada, derechos y deberes de los operadores y cooperación internacional entre los distintos Estados para proteger los derechos humanos en el contexto tecnológico.

Cada Estado adoptó los lineamientos dados por los modelos de protección de datos personales desarrollados y de mayor avance tales como: El modelo centralizado de protección y el modelo sectorial de protección, sirvieron de base para estructurar el modelo híbrido de protección de los datos personales en Colombia, el cual adoptó la categoría de derecho fundamental de rango constitucional (modelo centralizado) y la responsabilidad demostrada (modelo sectorial); los cuales se encuentran en proceso de consolidación y estandarización global con el objeto de brindar mayor seguridad y cooperación tecnológica.

Vivimos tiempos de múltiples paradigmas, según Thomas S. Kuhn los cuales se replantean a través de modelos de problemas y a la vez soluciones con un carácter científico universalmente reconocidas, donde la tecnología irrumpe cada vez más en la vida cotidiana y así lo advierte la relación entre ésta y los derechos humanos, cuenta un nuevo factor de la vida moderna: el hecho de que la vida privada ha entrado en el mercado como una mercancía, como un objeto intercambiable, como un objeto cualquiera. (2004).

Un caso paradigmático lo plantea Travieso J. A. (2014) en los países de la unión europea con posturas diferentes como es el caso de Finlandia que en forma unilateral avanzó en la legislación y declaró la banda ancha como derecho humano. Contrario sensu, la ratificación por parte del gobierno francés de Nicolás Sarkozy de la negativa del acceso a internet como derecho

fundamental. Y sin olvidar que se está gestando la “cloud computing” (computación en la nube), equipamiento informático y todos los datos se están depositando en ficheros de datos globalizados en el que la soberanía es absolutamente trivial.

La Asamblea General de las Naciones Unidas le reconoce al derecho a internet el estatus de derecho humano, en virtud del derecho al desarrollo de los pueblos, la promoción y protección de todos los derechos humanos, civiles, políticos, económicos, sociales, culturales, así como el derecho a la privacidad en la era digital y las “tecnologías de la información y las comunicaciones”:

Tabla 7.

Reconocimiento de la tecnología como derecho humano

Resolución	Proclama
Resoluciones 12/16, de 2 de octubre de 2009,	Derecho a la libertad de opinión y de expresión
Resoluciones del Consejo 20/8, de 5 de julio de 2012	Derecho a la libertad de opinión y de expresión
Resoluciones 26/13, de 26 de junio de 2014	Derecho sobre la promoción, la protección y el disfrute de los derechos humanos en Internet
Resoluciones 69/166, de 18 de diciembre de 2014 Resoluciones 28/16, de 24 de marzo de 2015	Derecho a la privacidad en la era digital
Resoluciones 70/184, de 22 de diciembre de 2015	Derecho de las tecnologías de la información y las comunicaciones para el desarrollo
ONU Resolución 32/16	Derecho sobre la promoción, la protección y el disfrute de los derechos humanos en Internet

Fuente: ONU, 2016

Como se observa, la tendencia internacional de aseguramiento de la protección y promoción del derecho de las tecnologías se presenta en mayor medida en aspectos relacionados con:

- “La libertad y la libertad en internet”

- "…las violaciones y abusos de los derechos humanos"
- "…la importancia de la privacidad online"
- "…promover la educación de las mujeres y los niños en aspectos importantes de la tecnología" (ONU Resolución 32/16)

Y lo reitera Travieso cuando presenta su estudio en el ámbito internacional 2.0:

"Cada vez que hacemos click en una computadora e ingresamos en internet, debemos tener en cuenta que estamos en condiciones de circunnavegar la tierra en milésimas de segundos. La World Wide Web (www.), por esencia, es internacional. Tan internacional como lo son los satélites que transmiten informaciones, los cables submarinos que permiten la difusión con una fibra óptica de un ínfimo espesor, entre 10 y 300 micrones, y que transportan mensajes con haces de luz a enormes velocidades." (2012, p. 165)

Promover y facilitar la cooperación internacional para educar a los ciudadanos, operadores y el mismo Estado representado en sus entidades públicas sobre el uso responsable de la tecnología de la información y comunicación es una proclama que debe responder a un tratamiento jurídico de datos personales armonizado y garante del principio de la dignidad humana en una democracia digital.

1.2. Referente conceptual del “derecho a la privacidad y la protección de datos personales”

De acuerdo con las características morfológicas y la técnica propia del derecho al tratamiento de datos personales que ha incidido en su nacimiento es pertinente la pregunta: ¿Es posible un concepto homogéneo de privacidad? Pues bien, la similitud de los conceptos de privacidad e intimidad, es clara, aunque dicho parecido no implica que son idénticos en razón a su contexto de protección, la privacidad abarca un espectro de aplicación más genérico y amplio, la intimidad involucra la esfera interna del individuo de manera específica.

El término privacidad no hace referencia a la “vida privada”, sino a conceptos mas actuales que en su mayoria surgieron a finales del siglo XIX, sin embargo cada uno de los doctrinantes presenta un enfoque propio al tratar de definir lo que es la privacidad. El alcance semántico de la privacidad no es absoluta, y mas cuando se trata de la defensa de los derechos del hombre frente a la informática, es un concepto pluridimensional que no es susceptible de una unica definicion sustantiva por su complejidad en el contexto global del procesamiento de datos de carácter personal y la autodeterminación informativa. (Vazán, 2014)

Sin embargo, se hace una aproximación a la idea de intimidad o privacidad las cuales, han evolucionado de manera inseparable desde sus orígenes y estando presentes en el proceso de construcción del Estado liberal como lo refiere Murillo cuando hace referencia a la idea de intimidad:

> “En efecto, aunque la vuelta al hombre y las actitudes individualistas arrancan con el renacimiento y toman un decidido impulso con la Reforma protestante, es en diversos autores ingleses donde brotan – en el seno del debate político y filosófico – las nociones de libertad y autonomía que, a la postre, conducen a la intimidad. Thomas Hobbes, John Locke, Robert Price y John Stuart Mill han efectuado las aportaciones más importantes.” (1990 p. 49).

En ese orden, se muestra los conceptos de intimidad que ilustran los autores Thomas Hobbes y John Locke, respecto a una postura clásica de la libertad del individuo y la injerencia pública a diferencia de una noción más amplia, reflexiva y de contexto de Robert Price en cuanto a la facultad del individuo de autorregular su conducta, así como la mirada de John Stuart Mill respecto a la importancia de la moral en noción de privacidad, como se presenta en el siguiente esquema:

Tabla 8.

Conceptos de intimidad

Autores	Pensamiento
Hobbes Thomas	Utiliza un artificio racional, y por tanto moderno para sostener el absolutismo de otras afirmaciones importantes, percibe la existencia de una esfera privada estrechamente relacionada con la libertad del súbdito
Locke John	La libertad que implica además de la liberación frente a la presión y violencia de los demás la autonomía para disponer como bien le parezca, de su persona, de sus actos, de sus bienes, y de todo cuanto le pertenece sometiéndose a lo que las leyes ordenen. Se identifica el aislamiento como último componente del concepto de libertad (Ensayo sobre el gobierno civil) Concibe la esfera doméstica privada de una persona de una forma tal que desaparece el efecto claudicante que la caracterizaba. En el Leviatán: No hay contradicción entre los intereses públicos y los asuntos domésticos privados. (La carta sobre la tolerancia) La libertad en sus facetas de autonomía, aislamiento y exclusión de intervenciones públicas sirve para configurar el marco propio de la vida privada
Price Robert	Cuatro libertades por luchar: autodirección, autogobierno, capacidad de la persona de autorregular su conducta y al mismo tiempo su conexión con la existencia de una esfera reservada en la vida de cada uno.
Stuart Mill John	Considera al individuo el centro de la moral y el receptáculo de la libertad, mientras que la sociedad y el Estado son sus potenciales enemigos. Considera la privacidad como el espacio de soberanía de un individuo considerado en su dimensión moral.

Fuente: Creación basada en Murillo, P. L. (1990)

Se evidencia la construcción de una noción de privacidad sobre las bases de las conexiones que el individuo presenta con su entorno social, en el cual, sin intimidad, sin el área aislada de la injerencia de la sociedad no hay libertades públicas. Como lo señala Berlín (1988), erigiendo sobre esta premisa filosófica ha pretendido trazar los límites entre la esfera privada y la pública. Distingue "libertad negativa" cuando la esfera privada se libera de las interferencias públicas, que presupone un límite a la actuación de los demás es decir la "conciencia de lo privado, de una zona sagrada", en la que cada individuo decide por derecho propio, establecer y disfrutar de sus relaciones personales y de una "libertad positiva", en el ámbito de la aprobación de lo que se puede hacer.

El concepto de privacidad reconocido históricamente surge en 1890 con la publicación del artículo The Right to Privacy (El derecho a la intimidad) como la primera manifestación de la doctrina anglosajona que aporta elementos de interpretación entorno al procesamiento de información humana con instrumentos de medición en actividades de censo.

La privacidad se define entonces, como el ***"derecho a ser dejado solo",*** esta definición se hizo famosa por dos abogados de Estados Unidos, Samuel Warren (1852 – 1910) y Louis Brandéis (1856 – 1941). Con la aparición de la tecnología de la información surgió la necesidad de adaptar esta definición, y de acuerdo con el enfoque de Westin, se reformula la definición de privacidad como la reclamación de individuos, grupos o instituciones para determinar por sí mismos cuándo, cómo y en qué medida se comunica a los demás la información sobre ellos. Esta afirmación sobre la libre determinación es la esencia del interés de una persona en la privacidad.

Hoy en día, estas dos ideas básicas de privacidad, el derecho a ser solitario y el derecho a controlar la información personal, constituyen el núcleo de la protección de datos. Es lógico que, sin el control sobre la información personal, la privacidad será en gran medida disminuida y en

última instancia podría hasta perderse.

Y es así que el surgimiento y reconocimiento del derecho a la vida privada presenta su primera manifestación por vía doctrinal en consonancia con la vía jurisdiccional y como producto de la configuración teórica que da vida al concepto jurídico de privacy o intimidad; autodeterminación informativa y el derecho al tratamiento de datos personales entendido como una extensión del derecho a la vida privada, cuyo desarrollo promueve la libertad individual.

Para construir la dogmática del derecho a la vida privada basada en la proclama de libertad individual cabe resaltar la obra de Benjamin Constant "De la libertad de los antiguos comparada a la de los modernos" (1819), John Stuart Smill en su obra On liberty (1859) y Samuel Warren y Louis Brandéis con su obra The Rigth to Privacy (1890) en los siguientes postulados:

1. "El goce pacífico y la independencia privada" (Constant, 1988 p. 75).
2. "La única libertad que merece este nombre es la de buscar nuestro propio bien a nuestra propia manera" (Stuart Mill, 2004, pp. 126-152).
3. Derecho a la soledad: "Se sentaron las bases técnico jurídicas de la noción de Privacy" (Warren, & Brandéis, 1995, p. 10-12).

El motivo de su construcción se basa según Prosser, en que Warren estimó que la prensa de Boston el periódico Saturday Evening Gazette, vulneró la vida privada de su hija al divulgar información tan detallada y con una imagen de derroche sobre la fiesta realizada sobre su boda; en consecuencia, junto a Brandéis buscaron una norma que permitiera el reconocimiento del derecho la intimidad de las personas el cual de manera general ya habían precedentes jurisprudenciales en diversos fallos judiciales anteriores de *Right of Privacy*. (1960, pp.383-423).

Pasado relativamente tres (3) años de la publicación de tan famosa obra por primera vez el Tribunal de Nueva York en el cao Marks & Joffra reconoce el concepto de privacy en el caso

relacionado con la publicación del retrato de un estudiante de derecho en un periódico que promovía un concurso del cual Él no estaba de acuerdo, y demanda por irrespeto a la propia imagen, a la falta de consentimiento, y al "derecho a ser dejado en paz". Los argumentos de la sentencia refieren el respeto a los derechos íntimos, deseos, sensibilidad, así como se respeta su propiedad y, por lo tanto, ningún medio de comunicación usará "el nombre o la fotografía de nadie sin su consentimiento". Por lo tanto, su conceptualización surge en la jurisprudencia y la doctrina norteamericana de fines del siglo XIX como el **"***derecho a ser dejado solo"*[4], el cual se amplió más tarde a todos los derechos. (Warren y Brandéis, 1995, p. 11).

Es decir, la concepción técnica jurídica de la vida privada replantea la teoría de Stuart Mill respecto a la independencia soberana del ser humano:

> "…consideraba que los aspectos concernientes al individuo consistían en el derecho a una absoluta independencia, puesto que sobre sí mismo, sobre su cuerpo y mente, el individuo era soberano. Por lo que con Warren y Brandéis, la privacy fue un derecho a la soledad, una facultad "to be lef alone", esto es, una garantía del individuo a la protección de su persona y su seguridad frente a cualquier invasión del sagrado recinto de su vida privada y doméstica. (Garcia, 2007, p. 750).

Y la perspectiva de un concepto autónomo del individuo producto de la sociedad civilizada:

> En consecuencia, al proclamarse el derecho a la búsqueda de la felicidad por parte de los ciudadanos, se buscaba proteger las creencias, los pensamientos, emociones y sensaciones de la persona. Así, en 1890, siendo Brandéis juez de la Suprema Corte de los Estados Unidos, en

[4] Warren S. D, Brandéis L. D, (1890)." Definen la protección de la esfera privada como fundamento de la libertad individual en la era moderna. El incremento de la capacidad del gobierno, la prensa y otros organismos e instituciones invaden la órbita de lo inaccesible de la actividad personal, y por lo tanto, su argumento se basó en que la ley debe evolucionar en respuesta a los cambios tecnológicos". El derecho a estar solo. The right to privacy. Revista de Derecho de Harvard, Vol. IV No. 5 ISBN 1610278402, 9781610278409 USA. Páginas 98 Editor Quid Pro, LLC, 2015 Béjar, H.: "Individualismo, privacidad e intimidad: precisiones y andaduras", Aranguren, J. L.: De la intimidad. Barcelona, Crítica, 1989, pp. 43 y 44

una dissenting opinión considero que frente al gobierno el derecho a la soledad es el más amplio de los derechos y el más estimado por los hombres civilizados" (Garcia, 2007, p. 750).

La doctrina de *Privacy Law*, aportó una reinterpretación de los precedentes en cuanto a la naturaleza y alcance de la protección de la vida privada. Más aún, antes se pensaba que el *Common Law* protegía el derecho de propiedad sobre la persona física o bienes materiales, en cambio, con esta nueva interpretación se reconoció la tutela sobre bienes inmateriales como los pensamientos, las emociones y las sensaciones de una persona física. Y de esa manera el tratamiento del derecho a la vida privada tradicional se expande al derecho a la personalidad inviolable que disfruta de la vida en diversos ámbitos como lo refiere Urabayen:

"debemos concluir que los derechos así protegidos, cualquiera que sea su naturaleza exacta, no surgen de un contrato o de una relación de confianza, sino que son derechos contra todo el mundo. Y, como ya hemos señalado, el principio aplicado para proteger tales derechos no es en realidad el derecho de propiedad privada, a menos que este término sea usado en un sentido amplio o inusual. El principio de la inteligencia o de las emociones, es el derecho a la privacy, y la ley no tiene que formular un nuevo principio cuando extiende esa protección a la apariencia personal, a las expresiones, actos, y a las relaciones personales, domésticas y otras cualesquiera." (1977, p. 99 -129).

Sin embargo, el derecho a la privacy no se constituye en un derecho absoluto, por cuanto, considera excepciones en materia publicitaria de asuntos de índole público o personal dependiendo del grado de los intereses:

"Hay personas que pueden razonablemente reclamar como un derecho la protección de la notoriedad que conlleva convertirse en víctimas de las empresas periodísticas. Hay otros que, en diversos grados, han renunciado al derecho a vivir sus vidas apartados de la observación

pública. Maerias que hombres de la primera clase pueden pretender con justicia que les concierne sólo a ellos, pueden en los de la segunda ser objetos de legítimo intéres de sus conciudadanos." (Urabayen, 1977, p. 99 - 129).

Posterior al aporte doctrinal de Warren y Brandéis, se inicia una etapa de reconocimiento de múltiples casos de violación de la vida privada, en particular sobre protección de los datos personales, por lo que surge la necesidad de dictar normas legales para su protección[5]. Como respuesta, se dictan leyes sectoriales, es decir, regulaciones específicas a cada sector determinado, pero no una ley general de protección de datos aplicable a todos los aspectos de la vida de una persona. Incluso, en este país actualmente el derecho a la protección de datos personales no posee un reconocimiento como derecho independiente al derecho a la vida privada y aunque la Constitución Norteamericana no establece una mención literal de la privacidad, se considera que queda dentro de su ámbito de protección pues establece en las Enmiendas I, III, IV, V y XIV disposiciones que se consideran como protectoras de este derecho[6]:

"Desde el primer momento, una de las aplicaciones más importantes de la informática ha sido el tratamiento y la elaboración de la información, al propiciar inmensas posibilidades de acumulación y manipulación de toda clase de datos, incluidas las informaciones sobre personas. En el año 1884, Herman Hollerith, a quien se considera el precursor del tratamiento automatizado de la información sobre personas, creó la primera empresa de procesamiento automático de información en el mundo, revolucionando de manera radical el análisis de la información del censo. Desarrolló un sistema de cómputo mediante tarjetas perforadas en las que los agujeros representaban el sexo, la edad o raza, entre otros. Gracias a la máquina

[5] Cfr. Ibíd., p.281
[6] Vid. Puente de la Mora, X., "Privacidad de la Información Personal y su protección Legal en Estados Unidos" [en línea] en Alfa- Redi, N° 97, agosto, 2006. Disponible en formato electrónico: http://www.alfa-redi.org/node/9027 (13 de agosto de 2014)

> tabuladora de Hollerith el censo en Estados Unidos de 1890 se realizó en dos años y medio, cinco menos que el censo de 1880. La utilización de tarjetas perforadas en el procesamiento de datos permitía clasificarlas. De esta forma era posible saber cuántas tarjetas cumplían determinados requisitos, por ejemplo, el número de personas de un determinado sexo, raza, Estado civil y edad que vivían en una localidad. Posteriormente, su invento se utilizó para elaborar y organizar estadísticas sanitarias en algunas ciudades y en el ejército" (Garriga, A. 2010, p. 1).

Finalizando el siglo XIX, la vida privada inicia con mayor determinación su especial protección jurídica en el ámbito anglosajón, basado en un enfoque eminentemente liberal, con la determinación de la génesis de la propiedad, enmarcada en el origen de todos los derechos, incluyendo las amenazas a la vida privada, las cuales eran entendidas como incursiones de terceros en su propia territorialidad[7].

A la privacidad, se le contrapuso el derecho a informar y el derecho de ser informado, es decir la exigencia de una información pública. Y a su vez el derecho a esa información se limita por el derecho a la privacidad. Sin desconocer que la privacidad se ubica en el centro de problemáticas complejas tales como interferencias telefónicas, reproducción de la imagen, control de opiniones religiosas y políticas.

El concepto ha sido expuesto en los casos célebres resueltos por la jurisprudencia, como en el ya mencionado de las escuchas telefónicas, y en el del derecho al aborto de Roe Vs. Wade (1973), se refirió a tres *niveles descendientes de derechos fundamentales* como se presenta en la siguiente tabla:

[7] Al respecto John Locke, señalaba que "aunque las cosas de la naturaleza son dadas en común, el hombre, al ser dueño de sí mismo y propietario de su persona y de las acciones y trabajos de esta, tiene en sí mismo el gran fundamento de la propiedad". Cfr. Segundo Tratado sobre el gobierno civil, trad. C. Mellizo, Alianza Editorial, Madrid, 1994, No. 44, p. 70

Tabla 9.

Niveles de derechos fundamentales relacionados con la intimidad en Estados Unidos

Niveles	Derechos fundamentales
1	El derecho de «control automático sobre la propia inteligencia y personalidad
2	La libertad de escoger en las cuestiones básicas sobre la propia vida, como el matrimonio, la procreación y la crianza de los hijos
3	La libre elección de los medios para cuidar su persona y su salud

Fuente: Creación propia basado en Roe Vs Wade, 1973

En este caso la Corte Suprema de Justicia de los EEUU, decidió que la mujer, amparada en el derecho a la privacidad bajo la "cláusula del debido proceso" de la Décimo Cuarta Enmienda podía elegir si continuaba o no con el embarazo, ese derecho a la privacidad se consideraba un derecho fundamental bajo la protección de la Constitución de los EE. UU. Y, por lo tanto, no podía legislarse en su contra por ningún Estado. Cabe resaltar que dichos criterios o niveles de derechos fundamentales no los acoge Colombia, como se analiza en el capítulo tres relacionado con el régimen jurídico de protección de la privacidad e información personal de los niños, en el cual se presenta la naturaleza constitucional del derecho a la intimidad que involucra derechos fundamentales relacionados con la vida privada personal, familiar y datos automatizados de las personas, así como la libertad de iniciativa privada en virtud del Estado Social de Derecho que promueve la prosperidad económica en virtud de la profesionalización del sector empresarial propia de la política de competitividad y productividad.

Al igual, Tocqueville, Constant y otros muchos autores reiteran la relación de dependencia que existe entre la privacidad, la libertad individual y la autonomía moral, aunque "el derecho a estar solo", como ilustraron Warren y Brandéis, reconoce un concepto de privacidad que se perfila a

partir de la idea intrínseca que surge de la condición de ser persona y del respeto de todos los seres humanos en una sociedad democrática y moderna.

Tocqueville, considera como concepto de intimidad que los riesgos derivados de un individualismo pueden llevar a las personas a encerrarse en su vida privada desentendiéndose de la vida pública. No hay más remedio que la búsqueda del equilibrio, dotar a la esfera pública y privada del contenido indispensable para que el individuo pueda ejercer realmente dos dimensiones de la libertad la negativa y la positiva.

Sin embargo, la postura de Rawls, respecto a la justicia como equidad constituye el fundamento de una concepción social que justifica la vida privada de la persona en consideración a su esencia como "fuente auto-originante de la filosofía moral y de toda reflexión política" (1979, p. 654).

Por lo tanto, es preciso como preludio temático tener en consideración la dualidad conceptualizada con respecto a la intimidad y la privacidad en el entorno internacional:

> "La verdadera razón de tanta variedad de criterios y de tantas contradicciones, vacíos, subjetivismos y confusiones, hemos de encontrarla en una proposición muy simple, que será difícil comprobar no existe un concepto único de vida privada, se trata de algo relativo y, por consiguiente, variable conforme a ciertas condiciones. La idea que se tiene de la vida privada varía de una persona a otra, de un grupo a otro, de una sociedad a otra; varía también igualmente, en función de edades, tradiciones y culturas diferentes" (Monreal, 1981, p. 42).

Incluso en el mundo del derecho, un concepto multivariado, que evoluciona y se transforma por las distintas contingencias de la vida social, cuyo estudio se desarrolla por la configuración teórica en la materia como lo ilustra Madrid Conesa (1984) frente a cómo las numerosas definiciones de la privacidad poco han cambiado a lo largo del tiempo y poco dicen de su contenido material,

avivando la búsqueda de elementos efectivos para cimentar un concepto legítimo, que, en consecuencia:

> "Solamente buscando aquello que hic et nunc (aquí y ahora), dentro de nuestro medio y nuestra cultura actual, ha de considerarse como claramente perteneciente a la vida privada del individuo, podremos sortear el escollo de trabajar con un objeto fluctuante, ligado a factores contingentes, cuya apreciación se hace siempre desde bases cargadas de subjetividad, y que por ello se presenta, para su consideración científica, como huidizo y casi inaprehensible." (Monreal, 1981, p. 45).

Conceptuar lo que realmente significa la privacidad, no es tarea fàcil, más aún dentro de campos como la filosofía y la psicosociología; se identifican autores tales como Altman, Newell, Pederson entre otros, sin embargo, se resaltan figuras en el área de la ciencias juridicas como es el caso Thomas Cooley (1888) quien da una noción de privacidad como el "derecho a ser dejado solo", a "ser dejado en paz.".

Los conceptos que mas se deben resaltar en este esfuerzo son las expresadas por Westin, quien establece la privacidad en terminos de autodeterminación; este autor planteó cuatro tipos de privacidad, las cuales mas adelante Perdenson amplía a cinco: *soledad*: se refiere a la situación en la cual las demás personas no pueden ver ni oir a las demás personas esta haciendo, *el aislamiento*: haciendo referencia al alejamiento fisico de los demas, *reserva*: alude al control de la información verbal que suministramos a otros, *intimidad;* hace referencia a estar con un grupo de personas sean con amigos o familiares excluyéndose de esta manera otros grupos y, por último *el anonimato*; calificativo que se da a un individuo que no es identificado entre la multitud.

Frente a estas precisiones resulta necesario establecer una concepción sobre la dignidad humana al estar profundamente ligada con la vulneracion a la vida privada de las personas y que a criterio

de muchos doctrinantes se resalta como una garantia y como parte del pleno desarrollo de las personalidad de las personas, como se expresa en el siguiente postulado:

> “La dignidad humana constituye no sólo la garantía negativa de que la persona no va a ser objeto de ofensas o humillaciones, sino que entraña también la afirmación positiva del pleno desarrollo de la personalidad de cada individuo. El pleno desarrollo de la personalidad supone, a su vez, de un lado, el reconocimiento de la total auto disponibilidad sin interferencias o impedimentos externos, de las posibilidades de actuación propias de cada hombre; de otro, la autodeterminación (selbstbestimmung des Menschen) que surge de la libre proyección histórica de la razón humana, antes que de una predeterminación dada por la naturaleza.” (Pérez Luño, 2005, p. 324).

El principio de la dignidad humana sirve de punto de referencia frente a tratamientos teóricos sobre el honor y la intimidad, los cuales son fundamentales dentro de los planteamientos que se formulan frente a la privacidad de las personas. Por ejemplo, la naturaleza jurídica de la intimidad se apoya en la regulación gubernamental de la empresa privada, contra aquellos que vieron la libertad de contratación y la búsqueda del propio interés económico como aspectos de la libertad individual, tales como la regulación política de las condiciones laborales y la competencia económica.

De igual forma Garriga, plantea los siguientes postulados de autodeterminación informativa, la intimidad y el derecho a la protección de los datos personales con fundamento en el principio de la dignidad humana:

> “La intimidad y el derecho a la protección de datos personales (autodeterminación informativa), son derechos fundamentales directamente ligados a la dignidad humana. El derecho a la intimidad se caracteriza por un eminente contenido negativo para salvaguardar del

> conocimiento ajeno una parte de nuestra vida personal y familiar, es decir, aquella que deseamos tener en el lado más reservado o secreto. El derecho a la autodeterminación informativa, por su parte, tiene un contenido diferente, su ámbito es más amplio y los elementos que lo componen más complejos. El tratamiento de la información personal puede, pero no tiene por qué, afectar a informaciones íntimas o secretas que son el objeto de protección del derecho a la intimidad. De la misma forma, los datos personales informatizados no tienen necesariamente que precipitar un retrato personal que implique una valoración peyorativa u ofensiva de un individuo y que atente contra su buen nombre o fama" (2007, p. 22).

Sobre el particular, la vida privada de los niños no se escapa a múltiples peligros que ofrece la tecnología como lo señala Pérez Luño: "De los asedios y transgresiones a la intimidad no han quedado a salvo los niños, quienes requieren una mayor atención y una tutela específica" (2009, p. 143).

Es decir, se requieren de ¿mayores garantías? ¿mecanismos de tutela efectiva de sus derechos por la utilización masiva de las TIC´s y la aparición de Internet?, la respuesta la determina las estadísticas que reflejan su incidencia en las relaciones del niño: "nativo digital", con su espacio vital, con los demás y para consigo mismo, así como, los mecanismos de protección de los datos personales del menor en cualquier escenario de su vida.

La globalización del derecho ha abierto las puertas hacia el mundo exterior y unificar criterios jurídicos para la solución de los problemas que trascienden las fronteras ha sido el objetivo de los Estados modernos y con prevalencia hacia la protección integral de los niños en el mundo, que exige el reconocimiento de estándares internacionales de soberanía y protección universal, como se observa de manera general en el marco jurídico internacional y nacional del derecho a la privacidad del niño.

En el plano jurídico es inevitable considerar una concepción restrictiva y limitada del derecho a la intimidad que tutela las manifestaciones más reservadas del comportamiento individual y familiar; aunado a la definición de intimidad desde el punto de vista sociológico:

> "La intimidad se entiende como el dominio interno, la esfera más sagrada de la persona" por ello "la intimidad es un concepto sicológico y alude a un mundo que se desarrolla en el propio interior". (Béjar, 1989, p. 64). Por lo tanto, Béjar reconoce que la privacidad contendrá la intimidad.

El siguiente gráfico muestra las esferas de protección de datos personales y autodeterminación informativa que acoge en su orden la privacidad y a su vez ésta acoge la vida privada y la intimidad en un contexto auto referencial y global.

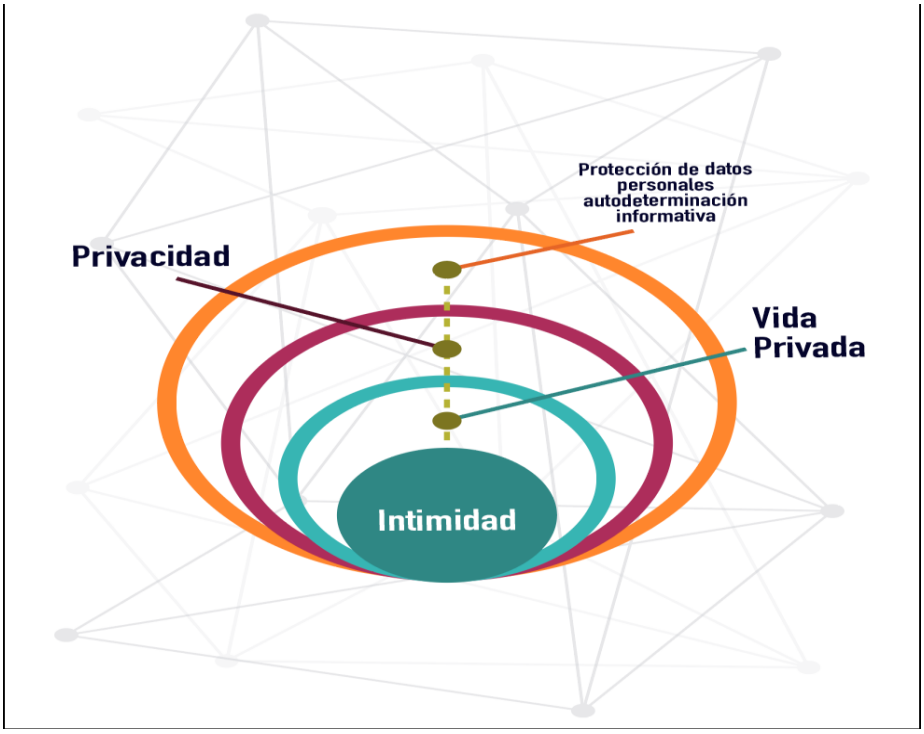


Figura 11. Dimensiones de estudio del derecho a la protección de datos personales.
Fuente: Creación propia (2017).

Como se muestra, existen distinciones entre lo íntimo, lo privado y lo público, como lo refiere Garzón, en cuanto a los rasgos propios que identifican su campo de aplicación, como por ejemplo la noción de intimidad:

> "los pensamientos de cada cual, de la formación de decisiones, de las dudas que escapan a una clara formulación, de lo reprimido, de lo aún no expresado y que quizás nunca lo será, no sólo porque no se desea expresarlo sino porque es inexpresable; es, no pocas veces, el marasmo que tanto suele interesar a los psicoanalistas desde Freud les enseñara a distinguir entre el ello, el ego y el superego" (2003 No. 137 p. 16).

Y que sustenta en la idea de un derecho reconocido por su relación con la moral y la autonomía de la voluntad como se refiere en el postulado:

> "Hay muchos… que desean saber quién soy yo… los cuales, aunque han oído algo o han oído a otros de mí, no pueden aplicar su oído a mi corazón, donde soy lo que soy. Quieren, sin duda, saber por confesión mía lo que soy interiormente, allí donde ellos no pueden penetrar con vista, ni oído, ni la mente" (San Agustín, 1956, Confesiones, Libro X).
>
> Así como: "La intimidad es también un derecho absoluto. Sólo Dios conoce la intimidad: Los teólogos nos aseguran que ni siquiera los ángeles son capaces de percibirla" "la intimidad sería aquella zona espiritual del hombre que considera inespecífica, distinta a cualquier otra, independientemente de que lo sea; y, por lo tanto, exclusivamente suya que tan sólo él puede libremente revelar" (J.M. Desantes, Guanter, 2004, p. 214-215 y 243).

A manera de conclusión, como lo establece Garzón, la intimidad es el ámbito de ejercicio de la autonomía personal de forma plena, en los rasgos de su personalidad es decir: "allí donde soy lo que soy" (2003, No. 137 p.17).

El concepto de vida privada acoge una noción de la libertad individual más amplia de acuerdo a las relaciones sociales:

> "el ámbito donde pueden imperar exclusivamente los deseos y preferencia individuales. Es condición necesaria del ejercicio de la libertad individual. (…) Es el ámbito de lo reservado a un tipo de situaciones o relaciones interpersonales en donde la selección de los participantes depende de la libre decisión de cada individuo" (E. Garzón Valdés, 2003, No. 137 p. 17).

> Y el carácter de reserva que debe respetar el derecho a la información de la vida privada familiar a elección del individuo: "la vida privada, que, si puede ser compartida por varias personas y, por tanto, es predicable de la familia incluso del matrimonio en la mayoría de los aspectos, es, a la vez, reservado y secreta y debe ser respetada por la información". (J.M. Desantes Guanter, 2004, p. 215).

Se afirma la necesidad de introducir en el ordenamiento jurídico el derecho a la autodeterminación informativa, como una derivación a los postulados del derecho a la intimidad tales como:

> "puede ser interpretado de una forma tal que acabe convirtiéndose, en la práctica, casi en un derecho general de la personalidad que subsuma la mayor parte de sus manifestaciones" y por esta vía, es un derecho que "al abarcar mucho, aprieta poco, o lo que es igual, resulta difícil organizar una tutela jurídica eficaz de un bien que, debido a sus contornos imprecisos (…) se hace en cierta medida evanescente o al menos deja en la penumbra los sectores que ha incorporado más recientemente." (Murillo de la Cueva, 1993).

De ahí que para la investigación es necesario, de acuerdo con Murillo de la Cueva (1990), organizar la defensa jurídica del ciudadano, en cuanto, a sus datos personales desde una posición de independencia sistemática en relación con los otros perfiles de la intimidad, e introducir el

estudio del derecho a la autodeterminación informativa en cuanto al derecho de patrimonio y confidencialidad.

El tratamiento de datos personales se ve afectado por el cambio social y la evolución tecnológica:“Un concepto unitario de textura abierta, plural, dinámica y globalizadora” (Pérez, 1994, p.49). Además, posee un sentido tan limitado y jurídicamente ineficaz, porque al jurista le queda poco para elegir, porque o le amplía el campo semántico del término intimidad o bien se utiliza la locución que defina la realidad como “vida privada”, o bien se incorpora, castellanizándola o no.

Para complementar Pérez Luño (1994) identifica la intimidad con la soledad y el aislamiento dejando por sentado la valoración a su raíz etimológica que corresponde al vocablo latino “*intimus”,* que ilustra la idea de lo más interno, la introspección o recóndito y secreto del ser humano.

El tratamiento de datos personales en todas sus etapas de recolección, almacenamiento, circulación, publicación y transferencia nacional e internacional busca como regla general proteger el derecho a la intimidad, porque busca establecer el equilibrio entre dicho derecho y la necesidad de utilizar la información personal por parte de terceros: la libertad informática y el derecho a la información.

En Europa, las ideas de Estados Unidos fueron superadas por la doctrina de la autodeterminación informativa o intimidad informativa, como señala Lucena (2012) que consiste en el derecho de cada persona a determinar en qué medida se puede comunicar a otros una información sobre sí mismo. El denominado derecho a la autodeterminación informativa tiene lugar su nacimiento en la República Federal Alemana con la sentencia del Tribunal Constitucional Federal Alemán (TCFA) en 1983: Ley del Censo, la cual reconoce jurisprudencialmente la

existencia del derecho fundamental a la autodeterminación informativa frente a la técnica moderna de tratamiento de la información:

> "Esta libertad de decisión, de control, supone además que el individuo tenga la posibilidad de acceder a sus datos personales, que pueda, no sólo tener conocimiento de que otros procesan informaciones relativas a su persona, sino también someter el uso de éstas a un control, ya que, de lo contrario, se limitará su libertad de decidir por autodeterminación." (Heredero Higueras, 1983 : 139-159, Documentación administrativa No. 198, Traducción Daranas, M. 1984).

Es decir, la jurisprudencia reconoce según Martínez, que el derecho a la libre personalidad le atribuye al individuo la capacidad de decidir en el ejercicio de su autodeterminación para difundir y dar uso a lo que desea dar a conocer de su propia vida basado en el derecho general de la personalidad frente al tratamiento ilimitado de sus datos. Es más, este concepto permitió concebir por primera vez, la protección de datos como un derecho autónomo e independiente al derecho a la vida privada. (2007 p. 48).

El constructo doctrinal sobre la autodeterminación informativa ha sido cimentado en España por el pensamiento de Perez Luño y Lucas Murillo de la Cueva la falta de límites de preservación de la identidad con ocasión de la estructura automatizada tan compleja y amplia en su argumentación:

> "Ese objetivo se consigue por medio de lo que se denomina técnica de protección de datos, "integrada por un conjunto de derechos subjetivos, deberes, procedimientos, instituciones y reglas objetivas" (Murillo de la Cueva, 1990 p.p. 173-174).

El significado y repercusión de las tecnologías de información en el ámbito de los derechos, en especial las afectaciones del derecho a la vida privada son estudiados bajo el enfoque de la privacidad al igual en los países latinos:

> “La respuesta a la contaminación tecnológica de las libertades se ha formulado el derecho a la autodeterminación informativa, construcción de la doctrina y la jurisprudencia germana, que tiene su equivalente en los países latinos en el derecho a la libertad informática. Tal derecho tiene una importancia decisiva en las sociedades tecnológicas del presente. Su función se cifra en garantizar a los ciudadanos unas facultades de información, acceso y control de los datos personales que les conciernen almacenados en ficheros informatizados.” (Pérez, 2007, p. 85).

Se observa en la denominación de dato personal la correlación que existe con la identificación de la persona física, la identificación de datos automatizados en los diferentes escenarios en los que se desenvuelve y que singularizan su personalidad en los escenarios políticos, sociales, comerciales, culturales, familiares entre otros y que requieren ser protegidos, en lo que concierne a su adecuado tratamiento, la libertad en la gobernanza, los derechos fundamentales de las personas físicas y su honor e intimidad, como señala Davara Fernández (2011) hacia la estandarización de la protección de los datos personales, la propia denominación ya induce a confusión.

> “El dato, en sí mismo, no necesita protección alguna. Sin embargo, cuando el dato se une a una persona, es algo distinto. Ya no protegemos entonces al dato, sino al titular del mismo, a la persona. Es más, cuando el dato se une a la persona se convierte en información personal.” (Fernández, 2013).

La noción de privacidad es conceptualizada de forma diferente por cada individuo dependiendo del contexto, por ejemplo, si es reactivo se tendría una aproximación a la noción norteamericana: «The Justices might not be able to say what privacy is, but they know it when they seeit». RubenFeld, J. (1989) que ilustra como los jueces podrían no ser capaces de decir lo que es la privacidad, pero lo saben cuándo lo ven. Dicha perspectiva está fundamentada en la Enmienda IV, al expresar que la protección a los individuos es válida si tienen unas expectativas razonables de

privacidad.[8] Y como lo expresa Prosser, al enumerar cuatro áreas que perfilan el derecho a la intimidad:

> "l) contra la intrusión en la reclusión o soledad, o en los asuntos privados de uno; 2) contra la revelación de actos privados embarazosos; 3) contra la publicidad que coloca a uno en una falsa imagen ante el público; y 4) contra la apropiación del nombre de uno en beneficio de otro." (1960 pp. 383-423).

De otra parte, se resalta el concepto de protección de datos personales ampliamente ilustrado por las Reglas mínimas para la difusión de información judicial en internet de Heredia como un referente para la regulación del tema por parte de los Estados:

> "Los datos concerniente a una persona física o moral, identificada o identificable capaz de revelar información acerca de su personalidad, de sus relaciones afectivas, su origen étnico o racional, o que esté referida a las características físicas, morales o emocionales, a su vida afectiva y familiar, domicilio físico y electrónico, número racional de identificación de personas, número telefónico, patrimonio, ideología y opiniones políticas, creencias o convicciones religiosas o filosóficas, la condiciones de salud física o mental, las preferencias sexuales, u otras análogas que afectan su intimidad o su autodeterminación informativa. Esta definición se interpreta en el contexto de la legislación local en la materia" (2003, Regla 10).

En el cual se reconoce la gestión de la información personal con fundamento en las características propias de intimidad y autodeterminación del individuo en escenarios online y offline.

[8] El Tribunal Supremo ha interpretado que dicha regla no proporciona protección cuando los individuos comparten información con terceras partes. Ver Stephen Henderson, «Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search» (2010) 55 Catholic University Law Review, disponible en: http://works.bepress.com/cgi/viewcontent.cgi?article=1002&context=stephen_henderson

De otra parte para finalizar en Colombia, el derecho a la intimidad se reconoce constitucionalmente (1991, artículo 15) como un derecho fundamental de carácter autónomo basado en un enfoque garantista a nivel personal, familiar y respecto de su propiedad a no ser molestado, con diversas posiciones frente a las tecnologías de la información y las comunicaciones que amplían el ámbito de regulación identificada como la privacidad y el tratamiento de datos personales que al igual son derechos fundamentales independientes y conectados con su fin salvaguardar la persona de los riesgos y afectaciones a sus derechos.

Así mismo, el derecho a la intimidad no es absoluto, ha sido estudiado por la doctrina y la Corte Constitucional en diversos precedentes jurisprudenciales que ilustran su definición y materialización en diversos contextos así Bautista refiere:

> "No hay suficiente información sobre la trascendencia de la intimidad personal, y ello conduce a que no exista una clara dimensión del ejercicio de este derecho. Hace 10 años, nadie habría considerado interesante un sitio de internet en el que yo tuviera la oportunidad de ver fotos de otros y de los momentos que viven en su día a día; hace 20 años, el concepto de un sistema de información que se basa en comunicar imágenes y emociones de los miembros que son suscriptores de este sistema, quizás habría sido una idea desechada de primera mano; sin embargo, si apreciamos lo que son las redes sociales hoy en día, es fácil entender cómo las cosas realmente han cambiado". (2015, p. 17).

La Corte Constitucional en sus primeros pronunciamientos despúes de 1991, fundamenta los estudios sobre el derecho a la intimidad en la identificación de su núcleo esencial:

> "… por su parte, ha definido el núcleo esencial del derecho fundamental a la intimidad como "el espacio intangible, inmune a las intromisiones externas, del que se deduce un derecho a no ser forzado a escuchar o a ser lo que no desea escuchar o ver, así como un derecho a no ser

escuchado o visto cuando no se desea ser escuchado o visto.” (Corte Constitucional, Sentencia T-530/92).

Y la percepción iusnaturalista del derecho a la intimidad en armonía con la dignidad humana como razón de su existencia:

“Toda persona, por el hecho de serlo es titular a priori del derecho a la intimidad y el único legitimado para permitir la divulgación de datos concernientes a su vida privada. La intimidad es elemento esencial de la personalidad y como tal tiene una conexión imprescindible con la dignidad humana” (Corte constitucional, Sentencia SU 528 de 1993)

De otra parte, la Corte aclara respecto al derecho de habeas data y su vinculación con el sector económico:

“(…) tiene la función primordial de equilibrar el poder entre el sujeto concernido por el dato y aquel que tiene la capacidad de recolectarlo, almacenarlo, usarlo y transmitirlo” y su núcleo esencial “está integrado por el derecho a la autodeterminación informática y por la libertad, en general, y en especial económica” (Corte Constitucional, Sentencia SU-082 de 1995).

Establece su relación con el derecho a la autodeterminación informativa que responde a la autonomía del derecho a la protección de datos personales en relación con el derecho a la intimidad:

“No obstante, y a pesar de que en determinadas circunstancias el derecho a la intimidad no es absoluto, las personas conservan la facultad de exigir la veracidad de la información que hacen pública y del manejo correcto y honesto de la misma. Este derecho, el de poder exigir el adecuado manejo de la información que el individuo decide exhibir a los otros, es una derivación directa del derecho a la intimidad, que se ha denominado como el derecho a la “autodeterminación informativa”. (Corte Constitucional, Sentencia T-552 de 1997).

Es decir, pone límites a la intromisión satelital en los asuntos personales y en la soledad de cada individuo, publicación de asuntos que afecten la imagen de las personas en virtud del derecho a la información, prevenir la suplantación de identidad y el reconocimiento facial para beneficiar a los intermediarios de la información tales como las redes sociales (Facebook, instagram etc), aumento de la utilización de drones sin protocolos de privacidad, son desafíos y dilemas jurídicos que requiere de intervención y conceptualización del derecho a la vida privada en una dimensión tecnológica.

Y así mimo, la Corte Constitucional aclara respecto a los estudios sobre el derecho a la intimidad que:

> "El derecho a la intimidad implica la facultad de exigir de los demás el respeto de un ámbito exclusivo que incumbe solamente al individuo, que es resguardo de sus posesiones privadas, de sus propios gustos y de aquellas conductas o actitudes personalísimas que no está dispuesto a exhibir, y en el que no caben legítimamente las intromisiones externas." (Corte Constitucional, Sentencia T-592-2003).

La protección a la privacidad de datos personales, no valora los datos por sí solos "*per se"*, sino en cuanto, ese dato se asimila e identifica a los titulares de la información. Y por ende el abordaje conceptual del derecho a la protección de los datos personales abarca la dimensión jurídica, informática y tecnológica, que integra tres elementos en su interpretación:

1. La persona,
2. Los datos o información personal
3. La gestión o el tratamiento de los datos.

En este orden de ideas, la conceptualización del derecho a la intimidad, la vida privada y la protección de datos personales de los menores de edad, se analiza en una dimensión hermenéutica

y moderna con nociones afines a la privacidad de acuerdo con la naturaleza de este sujeto de derecho y su relación con la información que lo identifica en el ámbito de su desarrollo cognitivo, emocional, individual y social. Y un ámbito normativo de gobernanza y gestión de los datos frente al significado del «derecho a la vida privada» reconocido por el ordenamiento jurídico que hace alusión a la seguridad de su ámbito privado. (Béjar, 1988).

Por ello, en lo subsecuente y para efectos prácticos se hará referencia a lo largo de esta investigación, al derecho a la vida privada y al derecho a la privacidad, indistintamente en relación con el derecho a la autodeterminación informativa. Por cuanto, la protección de los datos personales, disciplina jurídica que como Puccinelli refiere incluye denominaciones tales como: "libertad informática", "intimidad informática", "derecho a la autodeterminación informativa (o informática)", "information control", "data protection", "datenschutz", "hábeas data", entre otros, y que la legislación prefiere rotular: "derecho a la protección de datos" (2013, p. 1).

Por su parte, los múltiples conceptos de intimidad, privacidad en la sociedad de la transparencia, no se escapa a la cosmovisión autopoiética de la pos privacy frente al valor de uso del dato, el significado de la persona como apariencia que se exhibe, se expone, se visibiliza, se desnuda de manera pornográfica, como lo refiere: "Agamben desconoce que la *exposicion en si* es pornográfica. El capitalismo agudiza el proceso pronográfico de la sociedad en cuanto lo expone todo como mercancía y lo entrega a la hipervisibilidad. Se aspira a maximizar el valor de exposición." (Byun-Chul Han, 2018 p. 51) Y donde la distancia debe desaparecer para darle paso a la "contiguidad epidérmica del ojo y de la imagen" cercana a la piel. (Baudrillard, 1991 p.64).

Es por tanto, a la sociedad de la transparencia que le sigue la sociedad del rendimiento donde el sujeto se explota a "sí mismo", en la medida en que el sujeto activo del derecho a la privacidad

es actor titular de su información y a la vez victima de su propio actuar visible de hipercomunicación, frente a lo cual no se escapan los menores de edad: “nativos digitales”.

Como lo refiere Byun-Chul Han, la iluminación unida al sentido de libertad del individuo moderno según Bentham es reflejo del panóptico digital con un enfoque “moral o biopolítico” con el cambio de las costumbres y mitos con un idea vaga de preservación, cuando hoy la transparencia esta cimentada por un “imperativo económico” donde la explotación de la información contenida en diversos datos de los consumidores mueve las economías y “la hiperiluminación de una persona maximiza la eficiencia económica”. El hombre que se codifica, y se incerta en un algoritmo que invisibiliza su ser y a la vez mora en el panóptico digital que desconoce la esencia de una comunidad con sentido social a una comunidad sujeto a las marcas y a los bienes de consumo. Los datos por lo tanto, se convierten en bienes de uso comercial y el consumidor es importante en la medida funcional de su información como mecanismo de producción. El adulto consumidor no se interroga frente al funcionamiento sistémico de internet y sus implicaciones en la vida social y menos aún los niños consumidores que exponen su información como un juego y reto de imágenes sin control. (2018, p. 93 – 94).

La noción de privacidad y libertad informativa están en consonancia con la idea de iluminación en una sociedad de control y transparencia del individuo que exterioriza su intimidad para existir y relacionarse en una modernidad líquida, que debe ser estudiada por el derecho en procura de proteger al hombre en su humanización o transhumanización desde sus primeros años de vida en un mundo tecnológico y digitalizado.

1.3. Reconocimiento del derecho del niño a la privacidad y el tratamiento de datos personales

El reconocimiento de los derechos del niño por parte de los Estados ha existido un paulatino proceso de regulación internacional y exigencias de protección universal, porque vieron la necesidad de establecer convenios y tratados internacionales para proteger la vida privada de los derechos de los ciudadanos en general y a su vez la protección general de los derechos de los NNA, por medio de la Declaración Universal de los Derechos Humanos, el Pacto de los Derechos Civiles y Políticos, la Convención Americana sobre los Derechos Humanos.

Instrumentos normativos que buscan proteger de manera especial al niño, figura que para la época antigua no se le consideraba como sujeto de protección especial; ya que, en la edad media, los niños eran catalogados como "adultos pequeños". Sin embargo, a mediados del siglo XIX en Francia, surgió la idea de protección especial a los niños (1841, protección a los niños en su lugar de trabajo y 1881 protección del derecho de los niños a una educación); que ha permitido desarrollar progresivamente la protección jurídica de sus derechos. Ya en el siglo XX, comienza a implementarse la protección de los niños en el área social, jurídica y sanitaria en Francia y luego trasciende a Europa. Posteriormente en 1919, gracias a la creación de la Liga de las Naciones (denominada años más tarde ONU), a nivel internacional se visibiliza la importancia de proteger los niños, por medio de instancias colegiadas como el Comité para la Protección de los Niños. (Humanium, 2016).

En virtud del derecho de la Unión Europea, se adopta por regla general la noción de niño establecida en la "Convención sobre los Derechos del Niño" (en adelante CDN) visibiliza al sujeto del derecho que se enmarca en una categoría relacionada con la edad: "menor de 18 años de edad" (CDN, 1989, artículo 8) y en razón al Convenio Europeo de Derechos Humanos y Las Libertades

Fundamentales de 1950 (en adelante CEDH) conmina a los Estados a respetar los derechos "sin distinción alguna" incluyendo a los menores de edad (CEDH, artículo 1). Incluso el Tribunal Europeo de Derechos Humanos (en adelante TEDH) ha conocido de demandas "interpuestas por niños o en representación de estos, independientemente de su edad" (Agencia de los Derechos Fundamentales de la Unión Europea, 2015).

De esta forma, los primeros instrumentos internacionales que reconocen la protección de los derechos del niño y su vida privada surgen en diferentes dimensiones con políticas progresistas, como se ilustra en la siguiente tabla:

Tabla 10.

Instrumentos internacionales sobre derechos humanos que reconocen los derechos de la infancia y el derecho a la vida privada

Instrumento	Disposición
Declaración de Ginebra sobre los Derechos del Niño 1924[9]	**Primera declaración que centra mayor atención al deber de los padres hacia la protección de los derechos del niño** Por primera vez se reconoce y se afirma la existencia de derechos específicos de los niños, así como la responsabilidad de los adultos hacia ellos con mayor énfasis. La normativa se centra en el bienestar del niño y reconoce su derecho a la educación, desarrollo, asistencia, socorro y a la protección.
Declaración Americana de los Derechos y Deberes del Hombre 1948[10]	**En relación a la maternidad, la lactancia y la infancia** Reconoce la protección especial de la maternidad, la lactancia y la infancia, así como el correlativo deber de los padres de cuidar, alimentar, educar y amparar a sus hijos menores de edad. (artículo 7) **Reconoce el derecho a la vida privada** "1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad;

[9] Surge gracias al trabajo del médico polaco Janusz Korczak. Se funda en el pensamiento "la humanidad debe al niño lo mejor que ésta puede darle." (Humanium 2016) En 1947 Se crea el Fondo de las Naciones Unidas para la Infancia (conocido como UNICEF) al cual se le concedió el estatus de organización internacional permanente en 1953

[10] Aprobada en la Novena Conferencia Internacional Americana. Bogotá, abril de 1948.

Instrumento	Disposición
	2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra y reputación; 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques". (artículo 11)
La Declaración Universal de los Derechos Humanos – ONU 1948[11] –	**En cuanto al derecho a la vida privada** Establece que: "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia su domicilio y su correspondencia, ni de ataques a su honra y reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias y ataques" (artículo 12) **Con relación a la maternidad y la infancia** Reconoce que "la maternidad y la infancia tienen derecho a cuidados y asistencia especiales. Todos los niños, nacidos de matrimonio o fuera de matrimonio, tienen derecho a igual protección social." (artículo 25 No. 2)
Declaración de los Derechos del Niño Resolución 1386 (XIV) de 1959 ONU	**Describe los derechos de los niños en 10 principios** Corresponde al primer gran consenso internacional sobre los principios fundamentales de los derechos del niño: 1. "Derecho a la igualdad 2. El derecho a tener una protección especial para el desarrollo físico, mental y social 3. Derecho a un nombre y una nacionalidad 4. Derecho a una alimentación, vivienda y atención médica adecuada 5. El derecho a una educación y tratamiento especial para la discapacidad 6. Derecho a la comprensión y amor de los padres y la sociedad 7. El derecho a actividades recreativas y educación gratuita 8. El derecho a estar entre los primeros en recibir ayuda en cualquier circunstancia, 9. Derecho a la protección de cualquier forma de abandono, crueldad y explotación 10. El derecho a ser criado en armonía y convivencia universal."
El Pacto Internacional de Derechos Civiles y Políticos ONU A/6316 (1966) vigor 1976	**En cuanto a la vida privada ante la publicidad** "1. Todas las personas son iguales ante los tribunales y cortes de justicia**…** La prensa y el público podrán ser excluidos de la totalidad o parte de los juicios por consideraciones de moral, orden público o seguridad nacional en una sociedad democrática, o cuando lo exija el interés de la vida privada de las partes o, en la medida estrictamente necesaria en opinión del tribunal…" (artículo 14)

[11] Adoptada por la Asamblea General de las Naciones Unidas en Resolución 217 A (III), del 10 de diciembre de 1948

Instrumento	Disposición
	En cuanto a la vida privada en general 1. Nadie será objeto de injerencias arbitrarias e ilegales en su vida privada, su familia, su domicilio o su correspondencia ni de ataques ilegales a su honra y reputación. (…)". (artículo 17) **En cuanto a los derechos del niño** Reconocimiento del derecho a la igualdad, identidad y nacionalidad, así como medidas de protección del niño, tanto por parte de su familia como de la sociedad y del Estado. (artículo 24)
El Pacto Internacional de Derechos Económicos, Sociales y Culturales (diciembre 1966) vigor 1976	**En cuanto a los derechos del niño** "Reconocen que se deben adoptar medidas especiales de protección y asistencia en favor de todos los niños y adolescentes, en condiciones de igualdad y contra la explotación económica y social. Establece los límites al trabajo infantil" (artículo 10) "La reducción de la mortinatalidad y de la mortalidad infantil, y el sano desarrollo de los niños" (artículo 12)
Declaración de los Derechos del Niño - Resolución 44/25 ONU 1989 [12] vigencia 1990 (septiembre 2)	**Protección integral los derechos económicos, sociales y culturales del niño** Se ratifica la Convención sobre los Derechos del Niño de 1959 Se reconoce de manera integral los derechos de los niños a gozar de una protección especial, disponer de oportunidades y servicios, en condiciones de libertad, dignidad e interés superior del niño. **En cuanto a la vida privada del niño:** Reconoce de manera particular la protección de la vida privada del niño: "1. Ningún niño será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia ni de ataques ilegales a su honra y a su reputación. 1. El niño tiene derecho a la protección de la ley contra esas injerencias o ataques." (Artículo 16) **En cuanto a la vida privada en materia penal** "Que se respetará plenamente su vida privada en todas las fases del procedimiento." (artículo 40, inc. vii)

Fuente: Creación basaba en la normatividad internacional de vida privada.

[12] Aprobada por la Asamblea General de Naciones Unidas el 20 de noviembre de 1989 y hasta la fecha ha sido firmada por 190 Estados, aunque con algunas reservas por Estados Unidos y Somalia

Todos los postulados orientan a nivel internacional el derecho a la vida privada del niño como un derecho humano, que reconoce la vida privada en un ámbito personal y familiar en relación con la protección de la honra e imagen en instrumentos declarativos, idóneos y representativos de una política pública para la protección de la niñez a nivel mundial y la voluntad de los Estados por la ratificación de los convenios y tratados internacionales que propenden por su garantía universal. Así como, la regulación de la vida privada basada en un enfoque económico de publicidad, social, política y cultural desde 1976.

Dado que desde los inicios del siglos XX existe una proclama universal de cooperar internacionalmente en la consolidación y construcción de instrumentos jurídicos de garantía de los derechos del niño como lo señala la Declaración de Ginebra: "Toda la humanidad debe darle al niño lo mejor" (1924), dicho postulado trasciende en la Convención sobre los Derechos del Niño (tratado internacional - 1989), la cual consagra de manera específica derechos y obligaciones para asegurar el respeto de la infancia en armonía con los de derechos humanos: civiles, culturales, económicos, políticos y sociales (UNICEF, 2006). Y su reconocimiento se basa en la "articulación *ad hoc* para garantizar el respecto de la dignidad humana fundamental de la infancia (menores de 18 años), así como la necesidad de garantizar su protección y desarrollo" (Ornelas, L. 2011, p. 159).

En un proceso concomitante los Estados miembros de la Convención inician un proceso de formalización de los derechos de los niños como titulares de sus propios derechos, bajo el principio de la dignidad humana universalmente reconocido y unificado para proteger el interés superior del menor tanto en la teoría como la práctica siguiendo el pensamiento de Ornelas: "Los Estados, se

comprometen y se responsabilizan ante la comunidad internacional para cumplir con un código de obligaciones vinculantes a favor de la infancia". (2011, p. 159).

En consecuencia, la sociedad en general (las familias, las organizaciones, las instituciones públicas) está llamada a proteger en forma co-garante los derechos de los niños con medidas y políticas adecuadas de acuerdo con la edad y etapa de desarrollo:

> "Los Estados Partes se comprometen a asegurar al niño la protección y el cuidado que sean necesarios para su bienestar, teniendo en cuenta los derechos y deberes de sus padres, tutores u otras personas responsables de él ante la ley y con este fin, tomarán todas las medidas legislativas y administrativas adecuadas." (Naciones Unidas, 2016).

Por lo tanto, la 'primacía del menor', debe ser asumido como el principio presente en la normativa interna de los Estados de manera articulada con la Convención y cumpliendo el mandato internacional de proteger el interés superior del niño: "En este tenor, es la sociedad en su conjunto quien debe asegurar su cumplimiento como una obligación jurídica, un imperativo moral y una prioridad en materia de desarrollo" (Ornelas, 2011, p.159).

Y respecto a toda forma de violencia contra los niños es la misma Convención la que establece la obligación de protección integral como lo señala el artículo 12:

> "1. Los Estados Partes adoptarán todas las medidas legislativas, administrativas, sociales y educativas apropiadas para proteger al niño contra toda forma de perjuicio o abuso físico o mental, descuido o trato negligente, malos tratos o explotación, incluido el abuso sexual, mientras el niño se encuentre bajo la custodia de los padres, de un representante legal o de cualquier otra persona que lo tenga a su cargo.
>
> 2. Esas medidas de protección deberían comprender, según corresponda, procedimientos eficaces para el establecimiento de programas sociales con objeto de proporcionar la asistencia

> necesaria al niño y a quienes cuidan de él, así como para otras formas de prevención y para la identificación, notificación, remisión a una institución, investigación, tratamiento y observación ulterior de los casos antes descritos de malos tratos al niño y, según corresponda, la intervención judicial." (Naciones Unidas Derechos Humanos, 1989).

Las políticas nacionales, al igual que su internacionalización, han evolucionado; el enfoque legal de los derechos de los niños y niñas a lo largo del siglo XX, suponen un cambio en su consideración jurídica. Los niños son reconocidos como sujetos de derecho, como cualquier adulto, en contra de la consideración tradicional de los niños como objetos de derecho. Esta situación permite hablar de una evolución, en cuanto a la consideración autónoma del niño y, por lo tanto, añade algo nuevo a la tradicional postura de hablar de la protección a la infancia. (Hierro, 1999).

Las tecnologías de la información y las comunicaciones, son fuente de la reflexión dogmática respecto a los derechos humanos frente a la privacidad de los niños, conlleva a un análisis detallado que responda al pos-paradigma relacionado con la inclusión digital como lo refiere Ornelas:

> "Es por ello, que gracias al desarrollo generacional de los derechos y a su incorporación el sistema jurídico internacional, ha logrado la visibilidad global de los derechos humanos. Le corresponde al Estado y a la sociedad en su conjunto, el deber de proteger a cada individuo y de manera especial a los niños con el fin garantizar la protección y garantía de los derechos humanos con mayor determinación en la ciberevolución" (2010, p. 158).

Algunos organismos internacionales como la UNICEF han realizado estudios temáticos para contrarrestar los riesgos, amenazas o peligros de los "niños en un mundo digital" como se presentó en uno de los informes por la infancia a nivel mundial:

> "En aquellos Estados que carecen de un marco jurídico adecuado para la protección del derecho del niño a la privacidad y la libertad de expresión, las empresas deberían reforzar los procesos de diligencia debida a fin de garantizar que las políticas y las prácticas estén en consonancia con el derecho internacional." (UNICEF, 2016, P. 8).

Los esfuerzos por armonizar la regulación de cada Estado a los estándares de protección de privacidad y seguridad de la información digital que incluya a los niños como sujetos de especial protección es una proclama que amerita la intervención inmediata tanto en escenarios de juridificación y gestión reactiva como proactiva que deben ser vigilados y controlados en un sentido de gobernanza integral de datos para su adecuada implementación.

1.4. Marco teórico del derecho a la protección de datos personales de los niños en la era digital

La sociedad está influenciada por sistemas tecnológicos de información y comunicación, en una era de reestructuración en la que la globalización se expande en tanto que se incrementan las diferencias y se fragmentan los derechos: la ciencia y la tecnología mejoran la calidad de vida humana, pero tiene incidencias negativas en el comportamiento humano y el conglomerado universal. (Travieso, 2014).

Al respecto Zigmunt Bauman (2004), puntualiza la existencia de un mundo, con modernidad líquida, frágil, desgarrado, heterodoxo en contraposición a la modernidad sólida del siglo XX, que como lo expresa Martínez y Travieso (2014) se está frente a una realidad inabarcable con percepciones distintas de la privacidad y con diversidad de leyes sin reglas comunes o de regulación global armonizadas, al igual que existe innumerables desafíos y retos relacionados con

la protección de datos personales en particular de los menores de edad para ser tratados de manera especial y rigurosa en el ámbito jurídico por el derecho internacional de derechos humanos.

El estudio dogmático y epistemológico del derecho a la vida privada y la protección de los datos personales a partir de enfoques jurídicos y planteamientos sociotecnológicos en el derecho moderno, nutren el conocimiento humano desde diversas disciplinas y perspectivas del derecho reflexivo, como un instrumento que responde a un Estado social e intervencionista del siglo XX, con fines concretos de interacción humana y resolución de conflictos especializados de la evolución social y legal que se traduce en estándares de regulación progresista tales como la teoría sistémica de Gunther Teubner (Morales, 2002).

La presente investigación se identifica con los fundamentos de la teoría sistémica desde el enfoque social y el ecosistema digital, por cuanto, estudia las dinámicas propias del sistema jurídico y la tecnología que responde a la construcción de realidades sociales y sistémicas percibidas de manera novedosa y técnica, más allá del lenguaje común, por cuanto, se enfrenta a desafíos propios de las visiones del derecho moderno a la vida privada digitalizada, el tratamiento de la información personal de niños, niñas y adolescentes en el mundo del internet como fuente de producción normativa en el ámbito de la autorregulación y la gobernanza de datos.

1.4.1 Fundamento de la teoría sistémica: Sistema social y tecnología

Las rutas de la epistemología sociojurídica en el campo de las tecnologías de la información y la hiperconectividad resalta como referente teórico de la Europa Occidental a Michel Foucault con su postulado del post-estructuralismo, Jurgen Habermas desde la teoría crítica y Niklas Luhmann

con la teoría de la autopoíesis quienes comparten la visión del individuo en un proceso comunicativo.

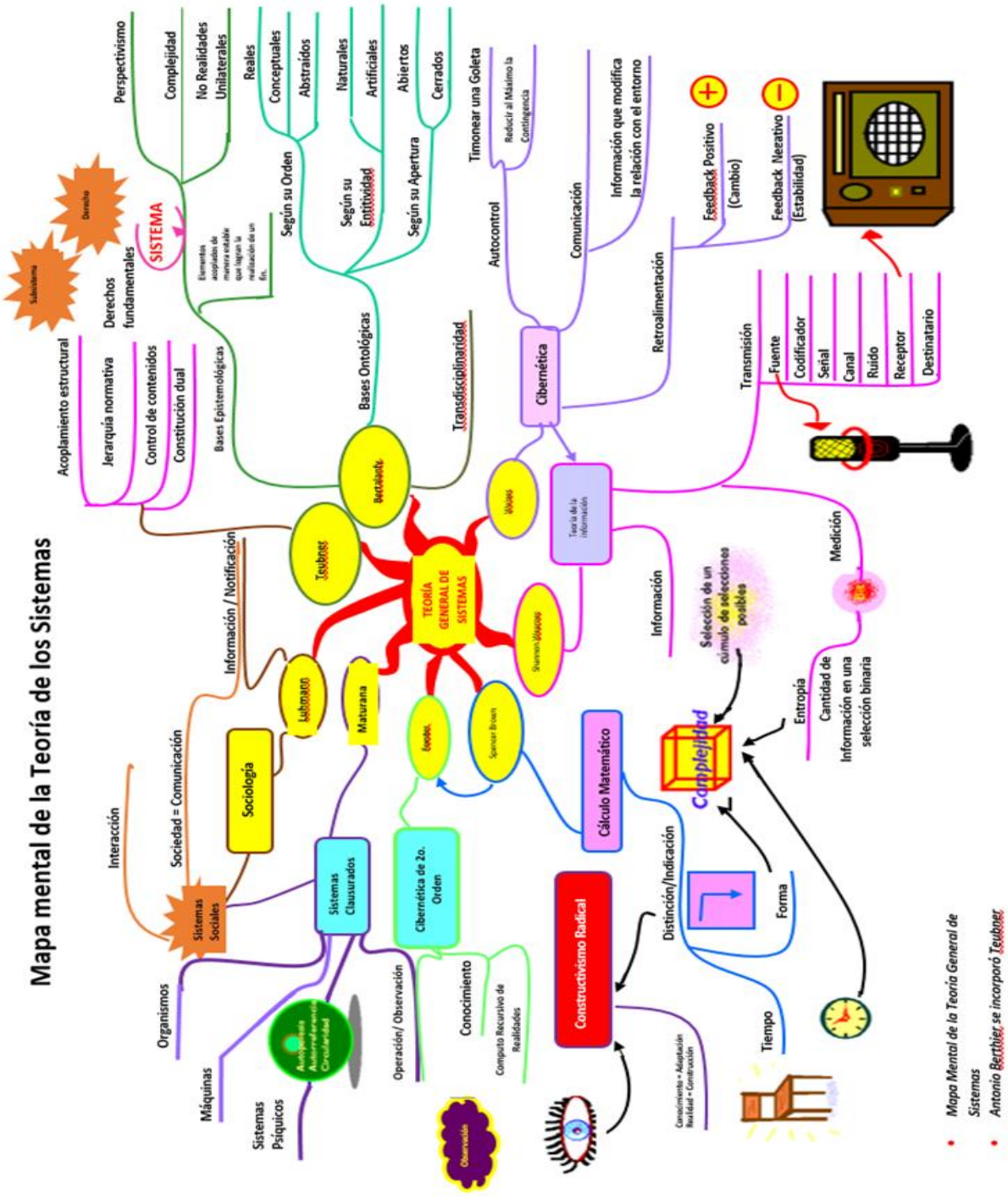


Figura 12. Mapa mental de la Teoría de Sistemas. Se incopora la teoría de Teubner

Fuente: Berthier Antonio, (2018).

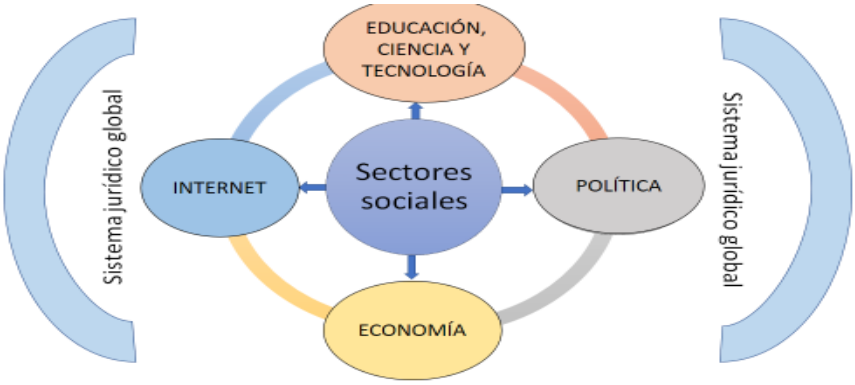
Dentro de los referentes del pensamiento sistémico, Luhmann (1984), ilustra el enfoque de la teoría de los sistemas como un instrumento que facilita la comprensión de un mundo interdisciplinar, deshumanizado y tecnificado que se caracteriza por la *complejidad social*, en la que el hombre se ubica en un amplio y difícil escenario de acciones y de elecciones que suponen riesgos y *límites de la razón humana* para dar respuesta a tan compleja realidad. De ahí la concepción del *sistema como una herramienta técnica y cognitiva* de entendimiento frente a las dinámicas complejas de la sociedad que necesita afianzar y asegurar su estabilidad personal y social. (Montoro Ballesteros, 2007, p. 367).

El sistema está compuesto por una diversidad de subsistemas que presentan su propia estructura y autonomía (familia, educación, empresas, iglesias, mercado, internet) que tiene como fin facilitar el entendimiento del entorno que se transforma y que se comunica a gran escala para dar solución a problemáticas del medio social y tecnológico, el cual se caracteriza por su enfoque autopoiético que acoge Luhmann, capaces de autoregeneración e integración.

> "La autopoíesis (autoproducción) significa que los sistemas sociales, igual que los sistemas psíquicos y orgánicos, tienen la capacidad de producir, ellos mismos, los elementos que los integran, construyendo su propio espacio de operación y reducción de la complejidad". (Montoro Ballesteros, 2007, p. 368).

La sociedad es entendida como un sistema social donde cada uno de sus componentes se relaciona entre si y de producirse un cambio en uno de ellos genera cambio en los demás y en el sistema total, en razón a que las relaciones son recíprocas, se comunican y se retroalimentan unas a otras. Este cibermundo que hace más evidente la separación entre la teoría y la práctica, es decir las disciplinas sociales de las ciencias de la información se transforman en un territorio donde la tecnología ya no es un instrumento sino el sentido de una sociedad articulada con la comunicación.

Respecto a los procesos de digitalización y la implementación de una red promovida por actores globales que se escapan al control de los Estados “constitución mundial de la libertad” cuyo acoplamiento estructural entre la política mundial decentral y el derecho entendido como una red interconectada que produce comunicaciones jurídicas en diferentes sectores y dimensiones que acoge los escenarios descritos por el pensamiento sistémico desarrollado por Gunther Teubner y que se adecua a la presente investigación:



Derecho	Internet
El código propio del derecho: legal e ilegal (normas jurídicas) fundamentales control de la corrupción y la dominación, proceso jurídico autónomo	El código propio de internet (esquema de ordenación específico del subsistema “arquitectura de internet”) Son las estructura de comunicación digitales proceso social autónomo

Figura 13. Escenarios relacionados con el sistema social y la tecnología.
Fuente: Creación propia basado en Teubner (2017).

Los escenarios de protección como primera medida se caracterizan porque requieren del acoplamiento estructural entre el subsistema digital y el derecho como un sistema social autopiético compuesto por comunicaciones jurídicas que incluyen la participación, la información y la comprensión de un mundo con dinámicas y codigos propios. (Gomez Jara Diez & Cancio Meliá, 2005).

Surge el debate si el mundo del internet debe ser regulado a nivel nacional frente a su carácter trasnacional de la comunicación digital? La realidad nos muestra el ascendente proceso de autorregulación dado el contexto arquitectonico y tecnico que involucra beneficios y a la vez amenazas a los derechos de los sujetos de derechos. Es decir todos los actores del sistema social estan llamados a garantizar el derecho a la protección de datos personales como esgrimible *erga omnes* y a responder como: individuo: principal protagonista y transgresor (familiares, el amigo, el extraño, el jefe …); la sociedad y entidades especializadas en información (agencias de transporte, Facebook, los bancos, universidades...) y el Estado (Ministerios, alcaldías, registraduría…) frente al adecuado tratamiento jurídico de cara a las tecnologías que están al alcance de los niños a más temprana edad, como ya en su oportunidad lo señaló Fariñas, respecto a la "fenomenología de la intimidad" y la vida privada (1983, p. 486).

1.4.2 El pensamiento sistémico y el riesgo de seguridad digital de los datos personales

El panóptico de Bentham recurre a la exposición de la soledad como un medio de disciplina para mejorar "ver sin ser visto" [13]a diferencia de la figura de la sociedad de control digital donde: "El panóptico digital del siglo XXI carece de perspectiva en el sentido de que no es vigilado desde el único centro por la omnipotencia de la mirada despótica". (Byun-Chul Han, 2018, p.88).

Las luchas internas en internet como dinámica altamente especializada y entorno a la cyberanarchy (ciberanarquía), a la regulación estatal y la comercialización son conflictos de tipo constitucional y político de primer rango en cuyo decurso caótico lo que lentamente va perfilándose no es otra cosa que el derecho de organización de una constitución digital que de

[13] Bentham, J. Panopticon, Carta V. P.92

acuerdo con el pensamiento de Teubner, decida sobre la vigencia de los derechos fundamentales en el ciberespacio donde las empresas privadas corregulen, definan y establezcan los límites de la libertad de opinión en internet. (Gómez Jara Diez & Cancio Meliá, 2005 pg. 204).

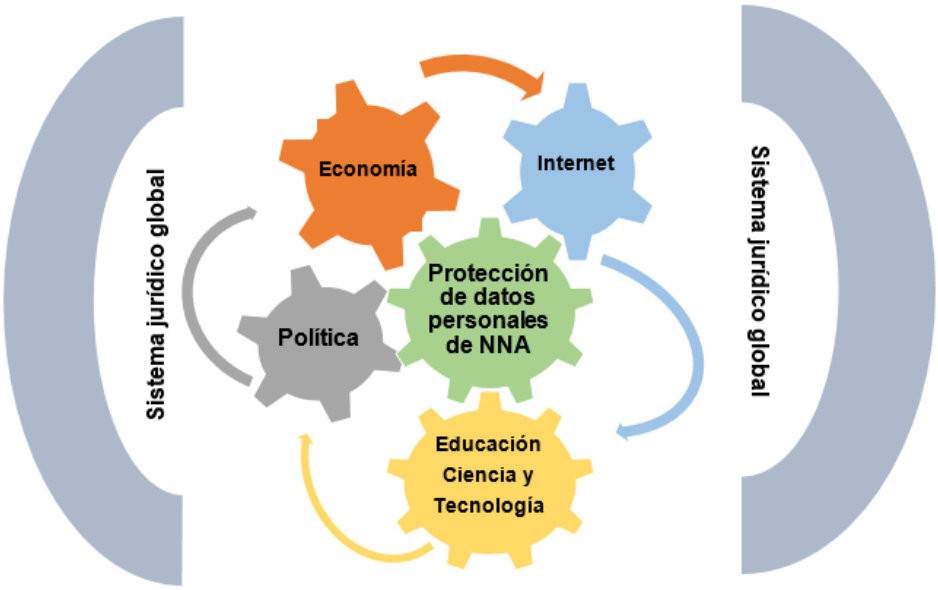


Figura 14. Acoplamiento normativo de la protección de datos personales.
Fuente: Creación propia basado en Teubner (2017).

El sistema jurídico global amerita una jerarquia normativa literal de la comunicación digital, propia de las practicas jurídicas que proclaman autonomía, y que según Teubner, son altamente formalizadas como tercera característica:

> "normas secundarias constitucionales que son capaces de superar la paradoja de vigencia de un derecho digital autoconstruido y deciden de modo selectivo acerca del carácter de norma jurídica de normas sociales" (Gomez Jara Diez & Cancio Meliá, 2005, p. 102).

Una tercera característica está relacionada con el control de contenidos de la norma y los estándares tecnológicos globales con base en criterios de derechos fundamentales, procedimientos

adecuados de contratación internacional, códigos de conducta de corporaciones globales. Como por ejemplo, la materialización digital de normas en el diseño por privacidad y por defecto, es decir el comportamiento en la arquitectura del ciberespacio (Lessig, Reindenberg, 1998).

> Y que lleva a cuestionamientos de regulaciones alternativas tales como: "¿Cuales son los controles de contenido y de procedimiento "código" que son necesarios para poder asegurar derechos fundamentales individuales y la autonomía institucional sectorial frente a las manifestaciones digitales de las normas jurídicas? "(Gomez Jara Diez & Cancio Meliá, 2005, p. 105).

Y la cuarta característica resulta de la tendencia mundial al desarrollo de una constitucion dual en un ambito organizado y en un ambito espontaneo frente a organizaciones estructuradas, es decir:

> "El desafío jurídico constitucional estaría en asegurar tambien en el plano normativo la dualidad de la autonomía social en los subsistemas, como una dinámica de control de ámbito espontáneo y ámbito de organización" "(Gomez Jara Diez & Cancio Meliá, 2005, p. 109).

La digitalización, la privatización y la génesis de redes globales, son tendencias de desarrollo en el conocimiento que a su vez han generado un cúmulo de problemas de carácter social y educativo lo que conlleva al estudio sistémico desde el enfoque de las ciencias sociales y de cómo los Estados responden a los múltiples desafíos que son producto de esta fenomenología incluyente y excluyente a la luz del pensamiento de Teubner. (Gomez Jara Diez & Cancio Meliá, 2005).

Es así que la presente investigación se identifica con la teoría sistémica de Gunther, en razón a los diferentes escenarios y agentes intervinientes de protección del menor de 18 años respecto al uso, tratamiento el intercambio electrónico de los datos que lo identifican como persona natural.

La dinámica de los sistemas de acuerdo a Martin García (2003) se puede aplicar a un sin número de problemas jurídicos y sociales, tales como el relacionado con el tratamiento de datos personales

de niños, niñas y adolescentes, en el cual puede existir un tipo de realimentación de las efectos causados mediante los cuales pueden surgir fenómenos contrarios a los modelos mentales utilizados tradicionalmente como es el caso de la visión ius informática del derecho a la privacidad de los niños y la garantía de los derechos fundamentales en el marco del derecho internacional y del derecho interno.

Así, las organizaciones humanas son consideradas como un sistema que involucra a todos los actores que dinamizan y examinan diferentes posibilidades de los miembros que lo integran y se relacionan con un multidiverso mundo de descripciones y alternativas para dar respuesta a los dilemas del tratamiento adecuado de la información personal de niños, niñas y adolescentes, quienes se ven expuestos a múltiples situaciones complejas y de "multicausalidad creciente" dado el escenario de tecnología e información a gran escala como lo refiere Coletti, y que involucra variables y múltiples espacios de un ecosistema que evoluciona (1997).

Los sistemas dependen de su estructura, la interacción entre el todo y las partes porque se experimentan "relaciones circulares de mutua afectación y de multi-causalidad creciente", el pensamiento sistémico "es circular, es decir, pasa de entender el mundo como un conjunto de objetos relativamente desconectados y con causalidades que preceden linealmente a unos efectos, para concebir que todos sus componentes están interconectados directa o indirectamente" esta indagación se circunscribe a interrogantes de una investigación sistémica, tales como: ¿Por qué el tratamiento de los datos personales de los niños, niñas y adolescentes en Colombia no se ajusta a los estándares internacionales? ¿cómo se protege el interés superior del niño frente a la violación de la información personal de los niños, niñas y adolescentes? y ¿cuál es el nivel de responsabilidad de la familia, del Estado, la industria, y la comunidad en general frente a la protección de los datos personales de NNA?.

Para comprender las transformaciones de los derechos en la sociedad actual desde el principio de la progresividad implica analizar la enorme velocidad que se presenta en el campo de la innovación que refiere Torres Ávila (2015), como expresión de una democracia online:

> "De esta manera los procesos de cambio tecnológico se enmarcan en este camino de adaptación en donde la innovación modifica la forma de entender el mundo, pero implica al mismo tiempo la aplicación de los conceptos de la tradición sobre otros que no lo son. Esta mixtura entre lo viejo y lo nuevo, es la que se plasma en el constitucionalismo de los derechos, y en la doctrina que se desprende de su implementación. La idea de fundamentación basada en la validez universal, similar al imperativo kantiano, no nos es útil para comprender las transformaciones de los derechos y su fundamentación en la sociedad actual. Desde esta perspectiva, los derechos no son lo que descubramos como máximas que atañen a todos los hombres; los derechos son la expresión de una praxis política, con consecuencias jurídicas, como lo deja ver la interpretación misma que hacen los sistemas constitucionales de la democracia." (Torres Ávila, 2015, p. 50 - 51).

Una praxis política cuyo lenguaje se identifica con "la dialéctica de la digitalización" que esta iluminando un mundo de abordaje binario, con la tensión entre el ciberoptimismo y el pesimismo tecnológico; y donde se exige mayor acoplamiento de los sistemas políticos, económicos y tecnológicos, en un entorno más digitalizado y comunicado mediante algoritmos, e incluso con una nueva moneda: los "bitcoins" y donde la privacidad tiene valor económico. ¿Ahora bien qué hacer para ejercer un adecuado control de la privacidad de los NNA en el espacio digitalizado?.

El desafio de los Estados es implementar un verdadero sistema jurídico global en el que exista un acoplamiento normativo de la política, la economía, la educación, la ciencia y tecnología, internet y la familia de cara al constructo autopoiético de los ecosistemas digitales más seguros y

confiables que faciliten el desarrollo integral de los niños como sujetos de derecho, de especial protección y de interés superior para el desarrollo de los Estados como lo refiere Maturana:

> "Toda comunidad existe como una red de procesos, actos, encuentros, conductas, emociones, tecnicas,..que configuran un sistema de relaciones de convivencia que esta presente en todos los aspectos del vivir de los niños y niñas que crecen en ella, en el curso de transformarse en adultos en todas las dimensiones de su hacer y emocionar. Es por esto mismo que la educación como proceso de transformación en la convivencia, ocurre en todas las dimensiones relacionadas con el vivir, tanto en los espacios privados de la familia o del colegio, como en los espacios públicos de la calle, la televisión el cine, el teatro o la radio que, como redes de conversaciones (el entrelazamiento del hacer y el emocionar) definen cotidianamente lo deseable, lo no deseable, lo legítimo y lo ilegítimo, lo hermoso y lo feo, lo honesto y lo deshonesto, lo aceptable y lo no aceptable..el convivir de la comunidad a que los niños y niñas se incorporan."(Maturana, 1999 p. 11).

De otra parte, la Organización para la Cooperación y el Desarrollo Económica OCDE estructura en 1980 las directrices del tratamiento automatizado de datos personales y la privacidad en el marco de intercambio internacional de datos e incorpora la gestión del riesgo digital con el denominado "puerto seguro".

Ahora bien, ¿En qué consiste el riesgo digital? Es una pregunta que responde a entornos de relacionados con amenaza online, ataque cibernético, exposición a la afectación de derechos y que afecta la confianza de los actores en el entorno digital: "Es el efecto de incertidumbres sobre objetivos y puede resultar de eventos en donde las amenazas cibernéticas se combinan con vulnerabilidades generando consecuencias económicas" (Minambiente, 2017).

Hoy el mundo no concibe la vida sin estar conectado a la web; la hiperconectividad se apoderó del hombre y sus relaciones comerciales, sociales, políticas entre otros escenarios que ofrece los servicios de los ciudadanos digitales que viven en la nube bajo las condiciones de esa nube. Existe una dependencia a la conectividad que ha generado conductas adictivas que ponen en riesgo la seguridad personal, familiar, laboral e incluso del mismo sistema.

Los riesgos de la seguridad digital se ha presentado como una película que hay que presenciar de manera visionaria en cine y en hoy el mundo experimenta la vulneración a los sistemas de información de un banco, intercambio de datos con fines políticos, las compras online en portales falsos, suplantación de identidad, dispositivos de entretenimiento para niños que a la vez son utilizados como instrumentos para vigilar a los niños, virus que capturan información de las personas con fines ilícitos atentatorios de sus derechos.

Gestionar el riesgo digital es una premisa importante que se encamina a la necesidad de formar profesionales en ciberseguridad por parte de todos los Estados en la industria, la academia y la investigación frente a los sistemas, el seguimiento y control proactivo de la web.

LA ONU en su informe del Estado Mundial de la Infancia 2017, presenta la preocupación por el aumento de la tecnología: “Las TIC están intensificando los riesgos tradicionales de la niñez, como la intimidación, y fomentando nuevas formas de abuso y explotación infantil, como el material con un contenido de abuso sexual infantil hecho a medida de los usuarios y la transmisión en vivo de actos de abuso sexual infantil.” (UNICEF, 2017 p. 3).

Son multiples los desafíos respecto al alcance y el ámbito de la digitalización, por cuanto, cada vez más se expandan y sus numerosas oportunidades continúen siendo explotadas comercialmente con multivariados “dispositivos digitales, plataformas en línea y aplicaciones disponibles para el uso de los niños” y falta por definir límites respecto al uso del “ internet de

las cosas, la inteligencia artificial y el aprendizaje automático" que si bien representan excelentes oportunidades, también generan multiples riesgos a los derechos de los niños como lo refiere en sus estudios UNICEF.

También hay claros vacíos en el conocimiento de los niños sobre los riesgos en línea, y, a pesar de que el uso de dispositivos ha aumentado rápidamente entre los niños y los adolescentes, muchos de ellos carecen de aptitudes digitales y de la capacidad crítica necesaria para medir la seguridad y la credibilidad del contenido y de las relaciones que confrontan en línea. Esto refleja la necesidad de ofrecer posibilidades mucho más amplias para la alfabetización digital que puedan salvaguardar y empoderar a los niños.

Finalmente, un elemento crucial es que todas estas brechas reflejan y producen lagunas en la formulación de políticas: los marcos que regulan la protección digital, la oportunidad digital, la gobernanza digital y la responsabilidad digital no mantienen el mismo ritmo que el cambiante panorama digital, y pasan por alto las repercusiones únicas que las tecnologías digitales suponen para los niños. Si no se cierran, habrá personas que exploten rápidamente esas brechas en la regulación. Explora algunas de las formas en que la digitalización está cambiando la vida de los niños, para bien o para mal. Las TIC han cambiado la manera en que los niños establecen y mantienen sus amistades, algo que les permite estar en contacto con sus compañeros casi constantemente.

También han transformado la manera en que los niños pasan su tiempo libre, proporcionándoles un suministro constante de videos, actualizaciones de las redes sociales y juegos muy absorbentes. Muchos adultos temen que estos cambios no sean positivos, y les preocupa que el tiempo excesivo frente a la pantalla esté aislando a los niños de sus familias y

de su entorno, acrecentando la depresión e incluso contribuyendo a su obesidad" (UNICEF, 2017 p. 11).

Vásquez Rocca, resalta uno de los riesgos digitales entorno a la explotación neoliberal con fundamento en el pensamiento de Byung-Chul Han:

"El hombre contemporáneo se ha convertido en una fábrica de sí, hiperactiva, hiperneurótica, que agota cada día su propio ser diluyéndolo en un afán competitivo, de allí que el síntoma de nuestra época es el cansancio. El sistema neoliberal ha sido internalizado hasta el punto de que ya no necesita coerción externa para existir. Así mismo, La sociedad de la transparencia lleva a la información total, no permite lagunas de información ni de visión" y acelera el flujo de datos empíricos. El mundo es hoy un mercado en el que se exponen, venden y consumen intimidades." (2017, p. 2).

Otro fenómeno de ciber-riesgo que se visibiliza en los postulados de la sociedad de la transparencia planteados por Byung Chul Han en los siguientes términos:

"La coacción de la transparencia no es hoy un explícito imperativo moral o biopolítico sino, sobre todo, un imperativo económico. El que se ilumina se entrega a la explotación. Iluminación es explotación. La hiperiluminación de una persona maximiza la eficiencia económica. El cliente transparente es el nuevo morador, el hombre sagrado del panóptico digital." (Byun-Chul Han, 2018, p. 93).

Así mismo, los riesgos digitales son generados por la dinámica del sistema de internet, en su técnica y ausencia de control de la información que circula en la web: "la comunicación digital se distingue por el hecho de que las informaciones se producen, envían y reciben sin mediación de los intermediarios. No son dirigidas y filtradas por mediadores. La instancia intermedia es

eliminada para siempre [...]. Medios como blogs, Twitter o Facebook liquidan la mediación de la comunicación, la desmediatizan.” (Han, 2014, p. 33, 34).

Otro de los riesgos socio tecnológicos es la ausencia de la responsabilidad de los intermediarios de los servicios de información en la web para realizar una adecuada gestión y vigilancia de los contenidos y política de seguridad digital (Moncada, 2009).

Con relación a la prevención de riesgos digitales, sobresale el Reglamento Europeo (2016) por incluir la categoría de los riesgos de seguridad digital de los datos personales en el marco de la protección del interés superior de los NNA en aspectos de regulación prevalente tanto en el ámbito de la mercadotecnia y la veracidad del consentimiento en los siguientes considerandos importantes de resaltar:

> “Los niños merecen una protección específica de sus datos personales, ya que pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales. Dicha protección específica debe aplicarse en particular, a la utilización de datos personales de niños con fines de mercadotecnia o elaboración de perfiles de personalidad o de usuario, y a la obtención de datos personales relativos a niños cuando se utilicen servicios ofrecidos directamente a un niño. El consentimiento del titular de la patria potestad o tutela no debe ser necesario en el contexto de los servicios preventivos o de asesoramiento ofrecidos directamente a los niños.” (Reglamento EU 2016/679, Considerando 38).

Su requerimiento, es imperativo a todo nivel la revolución industrial 4.0 que no solo debe estar preoucpada por obtener provecho económico de la información de los consumidores y usuarios, sino proteger los derechos fundamentales de los NNA de manera prioritaria por ser un sujeto de derecho de interés superior iustecnológico.

Al igual el derecho al olvido y el consentimiento del niño como garantía del adecuado tratamiento de sus datos personales refiere el Reglamento Europeo su protección en todas la etapas de desarrollo del ser humano:

> "Los interesados deben tener derecho a que se rectifiquen los datos personales que le conciernen y un «derecho al olvido» si la retención de tales datos infringe el presente Reglamento o el Derecho de la Unión o de los Estados miembros aplicable al responsable del tratamiento. En particular, los interesados deben tener derecho a que sus datos personales se supriman y dejen de tratarse si ya no son necesarios para los fines para los que fueron recogidos o tratados de otro modo, si los interesados han retirado su consentimiento para el tratamiento o se oponen al tratamiento de datos personales que les conciernen, o si el tratamiento de sus datos personales incumple de otro modo el presente Reglamento. Este derecho es pertinente en particular si el interesado dio su consentimiento siendo niño y no se es plenamente consciente de los riesgos que implica el tratamiento, y más tarde quiere suprimir tales datos personales, especialmente en internet. El interesado debe poder ejercer este derecho, aunque ya no sea un niño." (Reglamento EU 2016/679, Considerando 65).

Y sobre la ponderación o valoración del riesgo digital establece un enfoque objetivo en su determinación:

> "La probabilidad y la gravedad del riesgo para los derechos y libertades del interesado debe determinarse con referencia a la naturaleza, el alcance, el contexto y los fines del tratamiento de datos. El riesgo debe ponderarse sobre la base de una evaluación objetiva mediante la cual se determine si las operaciones de tratamiento de datos suponen un riesgo o si el riesgo es alto" (Reglamento EU 2016/679, Considerando 76).

En la actualidad Colombia, estructura la Política Nacional de Seguridad Digital (CONPES 3854, 2016) con una mirada proteccionista desde el Ministerio de Tecnologías de la información y las comunicaciones, el Ministerio de Defensa, la Dirección Nacional de Inteligencia y el Departamento Nacional de Planeación estableció la política nacional de seguridad digital que busca:

> "fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el País" (CONPES, 3854, no. 5.1).

El país experimenta una etapa de adecuación y armonización de su régimen jurídico de tratamiento de datos personales con una visión administrativa de los riesgos de seguridad digital con el Modelo de Nacional de Gestión de Riesgos de Seguridad Digital (MGRSD), con el objeto de identificar, gestionar, tratar y mitigar los riesgos de seguridad digital socioeconómica:

> "alcanzar beneficios sociales y económicos, proveer servicios esenciales, operar infraestructuras críticas, preservar los derechos humanos y los valores fundamentales y proteger a las personas frente a las amenazas de seguridad digital". (MGRSD, Min TIC, 2018).

Para finalizar, hacer parte de la "Red Iberoamericana de Protección de datos Personales" y la "Organización para la Cooperación y el Desarrollo Económicos" (OCDE), es repensar paradigmas o bloqueadores paradigmáticos con el objeto de avanzar en su tratamiento jurídico y gestión del riesgo de seguridad armonizado con los estándares globales de protección integral de datos personales de NNA y la cosmovisión proactiva de garantía de sus derechos en la era digital.

Capítulo II: Modelos y Estándares de Protección de Datos Personales Fuente de Regulación en Colombia

La protección de datos personales es un campo del ordenamiento jurídico particularmente moderno, que parte de las relaciones del derecho y la informática en un marco constitucional y legislativo de carácter internacional, cuyo corpus doctrinal de la informatica se ha cimentado a lo largo de treinta años y la tutela de la vida privada por más de un siglo, pudiera pensarse que carece del recorrido temporal suficiente para justificar un estudio de su historia. Sin embargo, el análisis del conjunto de instituciones que conforman hoy la legislación de protección de datos es no sólo necesario, sino también posible (Martínez, 2004).

Este capítulo describe, como primer referente el modelo centralizado de protección de datos personales propio de la Unión Europea que hace relación a la construcción normativa del derecho fundamental de autodeterminación informativa de las personas frente al tratamiento de su información personal; los estudios especializados realizados por el Grupo de Trabajo del Articulo 29 (GdT29), los ámbitos de protección especial, y el nuevo horizonte en materia de tratamiento de la información personal de los niños de acuerdo al análisis del Reglamentario (EU) 2016/679 del Parlamento Europeo y del Consejo de Europa relativo a la protección de las personas frente al tratamiento de los datos personales.

En segunda instancia se hace una aproximación al modelo sectorial de tratamiento de datos personales de NNA en Estados Unidos, por considerarse el país que cimienta la discusión pública sobre la de existencia de un nuevo derecho con autonomía y dinámico propios de la era de la información tecnológica: La privacidad, caracterizada no por un modelo único de regulación, sino

por un modelo sectorial de regulaciones específicas y mecanismos de autorregulación. Estos planteamientos sientan las bases garantistas de la tutela de este derecho por parte del Tribunal Supremo de los Estados Unidos, para consolidarse en una normativa especial para protección de la privacidad de los niños como modelo garantista en el ámbito preventivo y represivo de la "privacy" desde el punto de vista iusfundamental en la era digital.

Y en una tercera dimensión se hace referencia al modelo híbrido de protección de datos personales que caracteriza al régimen jurídico en Colombia y al proceso de armonización con los estándares de protección de la privacidad y los datos personales de los niños, niñas y adolescentes.

2.1. Modelo centralizado de protección de datos personales: Unión Europea

Como se hizo mención en el primer capítulo, la mayoría de los países en el mundo, fueron incursionando en el tratamiento jurídico del procesamiento de la información automatizada o no automatizada de datos personales desde mediados de los años setenta y con mayor determinación en Europa mediante directivas, leyes y reglamentos generales y en Estados Unidos con una legislación a nivel sectorial como se evidencia en la siguiente figura.

Figura 15. Mapa legislativo de protección de datos personales a nivel sectorial
Fuente: Deimos estadística. Recuperado de http://www.deimosestadistica.com/dia-mundial-la-proteccion-datos/

Para el caso latinoamericano, y en especial Colombia el proceso de regulación del tratamiento de datos personales, toma como base referentes de protección al derecho fundamental de privacidad, del derecho a la autodeterminación informativa, el libre desarrollo de la personalidad, la libertad de expresión y la libertad de iniciativa privada en el marco de la garantía de los derechos humanos como lo refiere la Unión Europea, sin embargo, reconoce el bienestar económico y de seguridad social que ofrece el mundo de la tecnología y la innovación empresarial.

La Unión Europea, ha tenido varios nombres oficiales desde su creación por el tratado de Roma de 1957 como la Comunidad Económica Europea; a pesar, de tener más de 50 años de antigüedad

sigue transcendiendo en la actualización y armonización del tratamiento de datos personales de cara a la era tecnológica y digital.

Durante mucho tiempo, la Unión Europea ha funcionado como un grupo de países que operan bajo un conjunto de normas que han tratado de ser coherentes entre sí para facilitar el flujo de personas y bienes entre los Estados miembros. Esto se ha conseguido aplicando de forma fragmentada los principios de numerosas directivas. En la aplicación del régimen, cada Estado miembro, de hecho, conservó o eligió tomar, mucha independencia y autonomía. Si bien esta estrategia permitió el establecimiento de un sentido de unidad entre países con diferentes culturas, historias e identidades, terminó creando un mosaico de leyes nacionales que tenían cierta semejanza con las directivas básicas de protección de datos, pero también con sus propias identidades.

Ahora bien, la legislación europea relacionada el tratamiento de la vida privada, de NNA, inicialmente se orientaba a resolver cuestiones concretas en relación con las libertades e iniciativas de orden procesal, tales como el derecho a un proceso equitativo:

> "…La sentencia debe ser pronunciada públicamente, pero el acceso a la sala de audiencia puede ser prohibido a la prensa y al público durante la totalidad o parte del proceso en interés de la moralidad, del orden público o de la seguridad nacional en una sociedad democrática, cuando los intereses de los menores o la protección de la vida privada de las partes en el proceso así lo exijan o en la medida en que sea considerado estrictamente necesario por el tribunal, cuando en circunstancias especiales la publicidad pudiera ser perjudicial para los intereses de la justicia. (Convenio Europeo, 1950, art. 6).

Y con el fin de proteger el orden familiar, político y económico a nivel general se consagra la protección del derecho a la vida privada:

"1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.

2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás." (Convenio Europeo, 1950, art. 8).

De acuerdo con la línea del tiempo del tratamiento jurídico de los datos personales en la Unión Europea, existen diversas normas que han protegido el derecho a la privacidad entre los que sobresale de manera específica, las principales disposiciones de regulación de 1980 a 2018:

Tabla 11.

Instrumentos normativos de protección de datos personales en la Unión Europea (UE)

Normativa de protección de datos personales en la Unión Europea	
Año	**Principales documentos**
2016 - 2018	(1) Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo del 27 de abril de 2016, relativo a la protección de personas físicas en lo que respecta al 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); **hace mención específica a la protección de datos personales de los niños**
2001 - 2018	(2) Protocolos adicionales al Convenio 108 del Consejo para la protección de personas respecto al tratamiento automatizado de datos de carácter personal y relativo a la transferencia de datos (2001 y 2018)
2000	(3) "Carta de los Derechos Fundamentales de la Unión Europea" (2000)
1981	(4) Convenio 108 del Consejo para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal (1981)

Fuente: Elaboración propia basada en instrumentos normativos (UE)

El Convenio No. 108 de 1981 del Consejo de Europa por su naturaleza proteccionista de las personas respecto a la administración de datos de carácter personal, se destaca por ser uno de los primeros instrumentos normativos aplicables de manera específica con el fin de garantizar tanto el derecho a la vida privada como a la libertad de información de todos los pueblos. Regulación que se caracteriza por establecer su objeto y fin, definiciones, campo de aplicación, principios básicos, flujos transfronterizos de datos, ayuda mutua, comité consultivo, enmiendas y procedimiento frente al inadecuado tratamiento de los mismos.

Es decir, se constituye en el primer referente que contempla la definición de la calidad de los datos en el escenario de la licitud, lealtad y legitimidad tan proclamado hoy en día en el contexto nacional e internacional por intereses superiores de defensa y seguridad del Estado:

"Los datos de carácter personal que sean objeto de un tratamiento automatizado:

a) Se obtendrán y tratarán leal y legítimamente;

b) Se registrarán para finalidades determinadas y legítimas, y no se utilizarán de una forma incompatible con dichas finalidades;

c) Serán adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado;

d) Serán exactos y si fuera necesario puestos al día;

e) Se conservarán bajo una forma que permita la identificación de las personas concernidas durante un período de tiempo que no exceda del necesario para las finalidades para las cuales se hayan registrado" (Convenio 108, 1981, artículo 5).

De igual manera, en 1995 se destaca en la Directiva 95/46/CE la defensa de las personas físicas en el ámbito del tratamiento de los datos y circulación transfronteriza de estos en espacios cerrados donde los sujetos afectados no tienen normalmente conocimiento del tratamiento de su

información personal y por lo tanto, se requiere mayores mecanismos de seguridad de la información y responsabilidad por parte de los diferentes operadores, así como la exigibilidad de la legalidad del consentimiento y su progresiva implicación: “se exige el consentimiento del interesado, con independencia del grado de sensibilidad de los datos tratados” (Directiva 95, artículos 7, 8 y 14).

Ahora bien, adaptar un proceso de legalidad respecto al consentimiento dirigido a los niños, fue necesario dada la tendencia a la utilización masiva de los dispositivos y herramientas tecnológicas por parte de ellos y su vulnerabilidad por la edad y limitada capacidad de comprensión del mundo digital, así como el fomento de su progresiva implicación. En la implementación de este procedimiento adaptado a niños el primer paso necesariamente implicaría que éste, sea consultado por su representante legal antes de otorgar su consentimiento, posteriormente obtener la autodeterminación del niño, a la par la de su representante legal y finalmente el consentimiento exclusivo del niño adolescente.

En otro ámbito importante de protección, los responsables del tratamiento de los datos personales tienen la obligación de suministrar al titular la información personal necesaria sobre la gestión de sus datos y el fin que se le dará a estos, con el propósito que puedan tomar decisiones debidamente informadas. El reto es adaptar esta interpretación en términos y lenguaje adecuado para la edad de los niños de acuerdo a su nivel de madurez y comprensión. Por lo tanto, esta directiva, visibilizó mayores límites al acceso y suministro de la información tales como: “la finalidad del tratamiento, la identidad y los datos de contacto del responsable del tratamiento” (Directiva, 1995, artículo 10, letras a y b).

Así mismo, se determinó la posibilidad de los interesados de suprimir los datos y ejercer oposición frente al inadecuado tratamiento de los datos que identifican a una persona en escenarios

físicos y online en consonancia con la garantía de todos los derechos fundamentales, y que hoy se ve contextualizado en el derecho al olvido; derecho que ha adquirido una importancia creciente frente a la utilización de las redes sociales y la interacción digital por parte de los niños a más temprana edad y cuya autorregulación se desconoce por la falta de educación, gestión integral de los datos personales y la corresponsabilidad de la familia, el Estado y las diferentes organizaciones responsables y operativas de la información personal.

De igual manera, la unión europea (UE, Carta de los derechos fundamentales, 2000) establece en su regulación, apartes referentes a la protección de los derechos del niño, como es el caso del artículo 24, el cual implementa tres principios básicos de estos derechos:

- “Derecho a la libre expresión de su opinión en función de su edad y madurez”. (artículo 24, apartado 1),
- “derecho a que su interés superior constituya una consideración primordial en todo acto que les concierna” (artículo 24, apartado 2),
- “derecho a mantener relaciones personales y contactos directos, de forma periódica, con sus progenitores" (artículo 24, apartado 3).

Este último principio de vital importancia para el desarrollo integral del niño, que parte del reconocimiento de su sana convivencia y su relación el derecho a la vida privada y familiar de calidad donde: “toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones” (Carta de los Derechos Fundamentales, 2000, artículo 7).

Así mismo, el consentimiento, la legalidad y el derecho de acceso de la información forman parte de los primeros inicios de la regulación general del derecho a la protección de datos de carácter personal en los siguientes términos:

> “Todas las personas tienen el derecho a la protección de sus datos de carácter personal. Frente al tratamiento de los datos personales; éste debe ser para un fin concreto a partir del consentimiento del titular esos datos, de igual forma el tratamiento de estos datos se realiza de forma leal y el titular de estos tendrá derecho acceso a los mismos.” (Carta de los derechos fundamentales, 2000, artículo 8).

Sobresale de manera significativa el grupo de trabajo “protección de datos”, el grupo de trabajo GdT29 cuya creación se fundamenta en el artículo 29 de la Directiva 95/46/CE. El carácter consultivo y de independencia de dicho Grupo frente a la protección de la privacidad y los datos personales, se da desde su conformación por las autoridades de vigilancia y control entre otros. De forma particular, con relación a la privacidad de los menores de edad, en el año 2002, se realizó un estudio técnico y normativo denominado “La privacidad de los menores en Internet: El papel del consentimiento parental” (Grupo de Berlín – Nueva Zelanda) en el cual se precisó:

- La necesidad de legalizar la autorización (representantes legales) para el tratamiento de sus datos personales online del menor y en equilibrio con la libertad de expresión de los niños y el control parental**.**
- La importancia de unificar estándares sobre consentimiento parental.
- Determinar los límites y medidas de intervención respecto a los factores de riesgo relacionados con la falta de madurez propia de la edad (frente a la tendencia de mentir más en un escenario virtual), y la inexperiencia frente a la inteligencia virtual que debe tenerse en cuenta para evitar que sea aprovechada en forma inadecuada por parte de algunos operadores y responsables del tratamiento.
- La exigibilidad de un mayor nivel de responsabilidad por parte de los operadores y responsables de los datos personales de los niños.

- Definir programas de gestión de riesgos.
- Identifica supuestos en los que es adecuado obtener el consentimiento parental. Así, cuando se solicite a un menor (inferior a 16 años de edad) que proporcione datos personales; cuando se vayan a revelar a terceros sus datos personales o vaya a ser utilizados con fines distintos (ej. Marketing directo); o cuando los datos personales vayan a ser publicados en la web.

2.1.1. Gdt29: Estudio de la "privacidad de los menores en internet"

El GdT29, ha tratado el tema de la privacidad y la protección de los datos de los menores en distintos documentos de trabajo[14], tales como en diversos dictámenes relacionados con el ámbito publicitario (Dictámenes 3 / 2003 y 4 / 2010, acerca del Código de conducta europeo de la FEDMA sobre comercialización; Dictámenes 2/2010 y 16/2011, sobre publicidad comportamental en línea); en lo relativo a geolocalización (Dictámenes 5 / 2005 y 13 / 2011); a propósito de los datos biométricos (Dictámenes 3 / 2007 y 3 / 2012); de las redes sociales (Dictamen 5 / 2009); o de las aplicaciones de los dispositivos inteligentes (Dictamen 2/2013)[15]. Así mismo, como una estrategia de protección de la información personal de los niños la implementación de un programa denominado «Hacia una Estrategia de la Unión Europea sobre los Derechos de la Infancia» se elabora el Dictamen 2/2009[16], cuyo objetivo consiste en analizar la pertinencia en el sector educativo.

El GdT29 ha abordado el tema de la publicidad en relación con los menores a propósito del "Código de Conducta Europeo de la FEDMA" en materia de su comercialización, determina un

[14] Puede consultar en http://ec.europa.eu/justice/policies/privacy/workinggroup/index-en.htm
[15] También lo ha hecho en otros documentos generados en relación con la reforma de la Directiva europea de protección de datos
[16] Véase en https://www.apda.ad/system/files/wp160_es.pdf

conjunto de buenas prácticas entorno al tratamiento de los datos personales relacionadas de forma directa con el marketing. Este código resalta la necesidad de proteger con medidas adecuadas de acuerdo a su condición y naturaleza a los menores como sujetos de derechos en su papel de consumidores de la industria tradicional como del comercio electrónico. (Dictamen 3 / 2003, 2017, WP 174).

Entre las medidas referidas se encuentra: El previo consentimiento paterno en el tratamiento de los datos de los niños, límites a la publicidad comportamental en línea por parte de los operadores de las redes de información dirigida a los niños, así como promover la autorregulación, regulación y límite de la edad mínima de 12 años para autorizar el tratamiento de sus datos de personales (Dictamen 16 / 2011, WP 188). Así mismo, establece las siguientes recomendaciones para la protección de la información personal de los niños vía online: Obtener el consentimiento de los representantes legales del menor de manera verificable en las diferentes etapas relacionadas con el tratamiento (incluso cesión o difusión pública de sus datos); adecuado lenguaje en los temas de publicidad cuyos destinatarios sean los niños evitando el engaño y aprovechamiento de su inexperiencia; evitar inducir la extimidad de los menores a través de estímulos disfrazados; prohibido el aprovechamiento de la inocencia del niño para que este facilite la información de sus familiares o de terceros (ej. Padres); tener presente el proceso de madurez de los menores respetando su autonomía privada una vez la adquieran según la edad reglamentaria. (Gómez-Juárez Sidera, 2008).

Respecto a la utilización del servicio de localización de los menores, cuyo valor radica en el análisis de los datos geo-referenciados por parte de los padres utilizando dispositivos móviles, el GdT29 resalta la importancia de limitar su uso ponderando los derechos en juego tales como el derecho a la intimidad del menor como el interés de cuidado por parte de sus representantes legales

en el marco del interés superior del niño. Frente a los múltiples riesgos se debe regular la legalidad del consentimiento del menor, las garantías de su seguridad e identificación y los límites de utilizar dicho servicio por parte de los padres. (Dictamen 5 / 2005, WP115).

Los servicios en aparatos inteligentes, asegura el GdT29 con posterioridad que el abordaje legal debe ser preciso y claro en cuanto la protección de los datos personales con los nuevos servicios de geolocalización (mapas, publicidad basada en la localización, rastreo de amigos, localización de los contenidos de internet, control de menores, entre otros) que ofertan los últimos avances tecnológicos (en particular, teléfonos inteligentes y tabletas). A propósito del consentimiento necesario para el tratamiento de los datos de localización, el Dictamen analiza el prestado por los menores, señalados que, en determinados casos, serán los representantes legales quienes deban otorgar dicho consentimiento. Pero, sobre todo, vuelve a insistir en los problemas derivados de las aplicaciones de geolocalización específicamente destinadas a un control parental.

Tal y como señalara en dictámenes anteriores[17], los menores no deben estar sobre vigilados por razones de seguridad, de manera que se reduzcan su autonomía y su derecho a la intimidad. Este derecho debe garantizarse también para los menores y, en el caso en que las concretas circunstancias aconsejen el uso de estos dispositivos de control, deberá ser informado y participar en la toma de decisión tan pronto como sea posible. (Dictamen 13 / 2011, WP 185).

Se constituye en un verdadero desafío la privacidad en las redes sociales en línea que forman parte del servicio de red social (SRS), en el sentido amplio de su responsabilidad frente al adecuado e inadecuado tratamientos de la información personal de sus usuarios (caso Analytic Cambridge - Facebook). Se recomienda establecer mayor claridad frente a las políticas de privacidad encaminadas a informar de manera transparente, sucinta y ágil al usuario sobre su identidad, la

[17] El Dictamen 5 / 2005, sobre geolocalización, al que se acaba de hacer referencia, o el Dictamen 2 / 2009, sobre protección de los datos personales de los menores

recolección y finalidad del tratamiento de los datos personales, lineamientos de confidencialidad, y de manera proactiva corregir la defectos, hacer recomendaciones sobre su adecuado uso, legalidad y verificación del consentimiento, protección especial de los datos sensibles, actualización o supresión de la cuenta, derecho al olvido y limites en su conservación en virtud del principio rector del ‹‹interés superior del menor››. (Dictamen 5/ 2009, WP 163).

Frente a los riesgos a los cuales se expone el menor cuando no se comprueba su edad y consentimiento parental, el GdT29, recomienda implementar estrategias en diversos ámbitos tales como: programas de formación escolar y sensibilización de los operadores y responsables de la información, herramientas tecnológicas que garanticen un mayor nivel de protección de la intimidad, autorregulación del sector empresarial e industrial (Códigos de buenas prácticas y sanciones disciplinarias) y regulación acorde con el tratamiento eficaz de los datos personales que reduzcan los riesgos y escenarios de vulnerabilidad, así como brindar tratamiento adecuado, gradual, especializado y con un enfoque diferencial a las comunidades de adultos y de niños en virtud del interés superior, así como no involucrar directamente a los niños en actividades de comercialización.

El GdT29 adoptó en el año 2009 un documento denominado "Directrices generales y especial referencia a las escuelas" (Dictamen 2/2009), que analiza el derecho de los niños a un adecuado tratamiento de sus datos personales y su aplicación al sistema educativo, destacando la imperiosa necesidad de garantizar en el ordenamiento jurídico los principios y derechos fundamentales de los menores en concordancia con el Convenio de la ONU sobre los derechos del niño de 1989 y la Directiva 95 / 46/CE con el fin de salvaguardar el "interés superior del niño" como principio rector en la materia[18]. (Andreu, 2014).

[18] Sobre este principio y su significado pueden consultarse, entre otros, Rivero Hernandez, F. (2000) El interés del menor, Dykinson: Madrid, pp. 51 y ss.; CAMPS MIRABET, N. (2007) ‹‹El principio del interés superior del menor;

El estudio se basa en analizar los principios acordes al tratamiento de los datos de los menores en temas tales como: la calidad de los datos, legitimidad, seguridad, proporcionalidad y derechos del titular en eventos tales como:

> "los ficheros de alumnos, señalándose, entre otras cuestiones, los límites a la publicación de los resultados escolares…, la utilización de datos biométricos para el control de accesos …; el uso de videos de vigilancia con fines de seguridad (que deberá responder de manera especial al principio de proporcionalidad, de manera que sólo deben instalarse cuando el objeto no se pueda conseguir con un método menos intrusivo, y deberá hacerse en lugares o momentos que menos afecten al derecho a la intimidad – ej., en las entradas o salidas del colegio, en horarios no lectivos, etc.-); la utilización de fotografías de los menores (que deberá contar con su consentimiento o el de sus representantes legales); o el uso de los teléfonos móviles (advirtiendo a los alumnos sobre las infracciones que para el derecho a la intimidad de terceros pueden suponer las grabaciones de vídeos, audio o fotografías" (Andreu, 2014, p. 110 – 111).

Finalmente, como lo refiere Andreu, respecto a la ponderación de los derechos que se involucran en el tratamiento de los datos personales de los niños deben existir límites para su publicación y criterios proporcionales de utilización en el ámbito escolar:

> "la protección eficaz de los datos personales de los menores, conlleva la aplicación de la legislación sobre protección de datos a la vista del ‹‹interés superior del menor›› y el resto de principios contenidos en los Convenios internacionales de protección de menores. El documento hace especial hincapié en el ámbito escolar, no sólo como el primer nivel en el que el GdT29 ha querido analizar la protección de los datos de los menores, sino también como el

marco normativo internacional y aplicación e el derecho interno››, en PADIAL ALBÄS, A.M y TOLDRÁ ROGA,M.D. (coords.), Estudios jurídicos sobre la protección de la infancia y a adolescencia, Tirant lo Blanch: Valencia, pp.23 y ss.; VILLAGRASA ALCAIDE,G. (2011) ‹‹El interés superior del menor››, en RAVELLAT BALLESTÉ,I. (coord..), Derecho de la persona, Bosch: Barcelona, pp.25 y ss

primer ámbito en el que éstos deben aprender la importancia de la intimidad y protección de sus datos. Para el GdT29, esta materia debería incluirse en los planes de estudio, de manera que en el futuro les permitiera adoptar decisiones informadas sobre qué datos desean o no divulgar, a quién y en qué condiciones. También se destaca un aspecto que consideramos decisivo en la sociedad actual, y es la necesidad de equilibrio, entre la intimidad de los menores y su seguridad. (2014 p. 111).

Por lo tanto, se debe implementar programas educativos de las TIC, TAP Y TEP que faciliten el conocimiento de las tecnologías, la apropiación del conocimiento y empoderamiento del uso adecuado de NNA que evite controles excesivos que ponen límites a su autonomía y autodeterminación informativa.

2.1.2. Un nuevo horizonte de la protección de los datos personales de NNA en la UE

En el año 2009 la Comisión Europea inició un proceso de reforma del actual modelo europeo en materia de protección de datos. La razón principal que se ha aducido para justificar una revisión de la normativa europea en esta materia ha sido básicamente la necesidad de adaptar la regulación a los cambios tecnológicos de los últimos años y a la globalización. Junto a lo anterior, también hay que destacar la búsqueda de una mayor armonización que la que se había conseguido hasta ahora a través de la directiva 95/46/CE, con el fin de potenciar el mercado interior[19]. De hecho, ha

[19] En la Comunicación de la Comisión Europea ‹‹Un enfoque global e la protección de datos personales en la Unión Europea››, de 4 de noviembre de 2010 [COM (2010) 609 final], a la que se ha hecho referencia en la nota anterior, se señalaban como nuevos retos en materia de protección de datos: la necesidad de abordar el impacto de las nuevas tecnologías; el reforzamiento de la dimensión de mercado interior de la protección de datos; la necesidad de hacer frente a la globalización y de mejorar las transferencias internacionales de datos; la consolidación de las instituciones para la aplicación efectiva de las normas en esta materia; y, por último, la mejora de la coherencia del marco jurídico que regula la protección de datos

sido este último aspecto el que ha propiciado que el instrumento jurídico finalmente elegido sea el del Reglamento y no una nueva Directiva sobre protección de datos personales.

La Comisión Europea consideró que un "reglamento", en oposición a una "directiva", era el instrumento jurídico más adecuado para definir el nuevo marco para regular el tratamiento de datos personales por parte de las empresas y agencias gubernamentales en sus operaciones cotidianas. Debido a la naturaleza jurídica de un reglamento en virtud del Derecho de la Unión, la regulación propuesta es el mejor medio para establecer una regla única que se aplique en forma directa y uniforme.

La normativa de la Unión Europea es la forma más directa del Derecho de la Unión Europea. Un reglamento vincula directamente a los Estados miembros y es directamente aplicable en todos ellos. En cuanto se aprueba un reglamento, éste pasa automáticamente a formar parte del ordenamiento jurídico nacional de cada Estado miembro. No es necesario crear nuevos textos legislativos.

Las directivas de la Unión Europea, por otra parte, se utilizan para concertar las diferentes leyes nacionales. Prescriben sólo un resultado final que debe alcanzarse en cada Estado miembro las formas y los métodos de aplicación de los principios enunciados en una directiva son de su competencia, una vez que, se aprueba una directiva a nivel de la Unión Europea, cada uno debe aplicar o "transponer" la directiva en su ordenamiento jurídico, pero puede hacerlo en sus propias palabras.

Las normas en materia de protección de datos, basadas en una serie de directivas, en particular la Directiva 95/46 / CE, la Directiva 2002/58 / CE (modificada) y la Directiva 2006/24 / CE, han demostrado ser el resultado de las discrepancias significativas entre las interpretaciones o implementaciones de cada directiva que se hicieron en los distintos Estados miembros. Al adoptar

una regulación sobre cuestiones de protección de datos, la Comisión Europea tiene la intención de equipar a cada uno de sus Estados miembros con el mismo instrumento jurídico básico que se aplica de manera uniforme a todas las empresas, a todas las organizaciones y a todos los individuos.

En la Unión Europea (UE), la protección de datos personales tiene un significado tan importante que está catalogada como un derecho fundamental en la Carta de los Derechos Fundamentales, caracterizado por la búsqueda de adecuar el tratamiento jurídico de manera armónica por parte de los Estados miembros con fundamento en aspectos característicos tales como:

Tabla 12.

Característica del modelo de protección de datos personales en la Unión Europea

Modelo Centralizado de Protección de Datos Personales Unión Europea
El tratamiento de datos personales como un derecho fundamental
La gestión de los Estados para prevenir riesgos de seguridad
Basado en el enfoque social de los derechos humanos
Acatamiento de instrumentos legales, principios y estándares de protección
Transferencia de datos con un nivel adecuado de protección
Vigilancia y control autónoma con autoridades especializadas y responsabilidad proactiva
Protección para todos los residentes en los territorios de la unión europea
Privacidad desde el diseño y por defecto
Autorregulación y veracidad del consentimiento consentimiento

Fuente: Creación basada en la normatividad de PDP - Europea

La adecuación se evalúa a la luz de todas las circunstancias que rodean una operación de transferencia de datos y debe tenerse en cuenta la calidad, procedencia, circulación y destinación de acuerdo con la vida útil del dato, según las leyes de los diferentes países. Las transferencias de datos personales deben ser asumidas con responsabilidad respecto a la protección de la vida privada, mediante instrumentos de contratación adecuada entre los diferentes operadores y actores del tratamiento de la información personal tanto dentro como fuera de la UE.

El reglamento establece controles y contrapesos en forma de cooperación y supervisión, de modo que las discrepancias entre estas interpretaciones sean menos significativas o sean menos numerosas que las que actualmente se encuentran entre las leyes de protección de datos de los Estados miembros, sin embargo, sería muy arriesgado actuar como si hubiera total uniformidad.

Los objetivos básicos que se persiguen con la nueva normativa europea en protección de datos son básicamente:

1. El reforzamiento de los derechos de las personas (por ej., incidiendo en el concepto de dato personal o en las categorías de datos sensibles; aumentando la transferencia; potenciando los derechos del titular e incluyendo nuevos derechos- como el derecho al olvido o a la portabilidad de los datos-; reforzando el consentimiento y las vías de recurso, etc.);
2. el establecimiento de un marco global en materia de protección de datos (que se aplique en otros ámbitos hasta ahora excluidos, como la cooperación policial y judicial en materia penal);
3. desde el punto de vista de la globalización, la clarificación de la normativa sobre transferencias internacionales de datos y la promoción de unos principios universales en la materia;
4. el reforzamiento de las instituciones (autoridades nacionales y europeas en materia de protección de datos);
5. y, en relación con los responsables de tratamientos y desde la dimensión del mercado interior, una reducción de las cargas administrativas (por ej., en cuanto a la notificación de ficheros), acompañado de un aumento de su responsabilidad (por ej., introduciendo los principios de privacidad desde e diseño y por defecto, la rendición de cuentas o las

notificaciones de violaciones de datos), así como el fomento de la autorregulación y de regímenes europeos de certificación[20]. (Reglamento EU 2016/679).

Las distintas instancias implicadas en el proceso de reforma han señalado que con la modificación de la Directiva se trata de reforzar y adaptar la normativa en protección de datos personales a los nuevos desafíos ya señalados, así como los principios adoptados siguen siendo válidos en las nuevas circunstancias, con las necesarias adaptaciones y complementos.

La Comisión Europea ha elegido el Reglamento EU 2016/679 como el instrumento jurídico más adecuado para la nueva regulación de la protección de datos personales. Con ello, se pretende reducir la fragmentación a la que han dado lugar las distintas legislaciones nacionales y ofrecer una mayor seguridad jurídica, con el fin de mejorar la protección de los derechos de las personas. La base jurídica utilizada ha sido la regulación del TFUE, que permite legislar sobre la protección de los datos personales y su circulación "en el ejercicio de actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de éstos" (Artículo 16.2).

El Reglamento se centra sobre todo el consentimiento respecto de ciertas actividades realizadas en el entorno digital "además de mencionar el tema a propósito de otras cuestiones, como la información, el derecho al olvido, etc.; y el cumplimiento de los principios en materia de protección de datos establecidos en la propia propuesta de Reglamento". Esto permite una legislación nacional en cuestiones no reguladas en el Reglamento[21], al margen de otros temas sobre los que la UE no tienen competencia (piénsese, por ej., en la contratación con menores o en el tratamiento de datos en el ámbito escolar o sanitario).

El consentimiento de los menores para el tratamiento de sus datos personales

[20] La propuesta de Reglamento también prevé establecer modelos normalizados a nivel europeo para la información a los interesados, ejercicio de los derechos en materia de protección de datos, obtención del consentimiento verificable de los representantes legales, etc

[21] Se trata de una competencia compartida (cfr. arts. 2.2 y 4 del TFUE)

La legalidad del consentimiento de los menores, es una de los mayores desafíos jurídicos en el tratamiento de la información personal de estos, dada la trascendencia de los servicios de la sociedad de la información. La licitud de la administración de los datos del menor de 13 años es lícita siempre y cuando exista el consentimiento o autorización del padre o tutor. Y así mismo, el responsable del tratamiento está en la obligación implementar medidas tecnológicas pertinentes y eficaces para verificar el consentimiento de un sujeto de especial protección como son los niños, siendo transparente en los eventos de relación contractual. El Reglamento, otorga la facultad de aplicar métodos de obtención del consentimiento verificable (e incluso la adopción de medidas específicas de acuerdo al tipo de organización); así como la capacidad para establecer formularios normalizados para la obtención de dicho consentimiento (artículo 8.3 y 4).

Pues bien, a pesar del título tan genérico que acompaña el artículo 8 “tratamiento de los datos personales relativo a los niños”, en realidad él regula únicamente una cuestión muy puntual, como es la validez del consentimiento de los menores en relación con el tratamiento de sus datos personales en los servicios de la sociedad de la información específicamente dirigidos a éstos (y ello sin perjuicio de la legislación nacional sobre contratación con menores). No se establece, por tanto, una edad a partir de la cual un menor puede consentir con carácter general el tratamiento de sus datos personales o por debajo de la cual debería contarse con la intervención de los representantes legales. Esta regla general podría haberse acompañado igualmente de la correspondiente salvedad respecto del derecho contractual de cada Estado, y sobre el que a UE no tiene una competencia genérica.

El concepto de servicio de la sociedad de la información, engloba las actividades típicas de los prestadores de servicios y de contenidos en línea, incluidas las redes sociales (De Miguel Asensio,

2011)[22]. Las leyes de los servicios de la sociedad de la información (LSSI) como las mencionadas directivas excluyen expresamente determinadas actividades: así, los servicios telefónicos, fax o télex (ej. Marketing en medicina realizada por estos medios en forma directa); el uso del correo electrónico con un propósito distinto al originalmente recaudado y con fines económicos de quienes lo utilizan (incluso aunque o usen para celebrar contratos); la radiodifusión sonora o televisiva o el teletexto televiso u otros servicios equivalentes; y la utilización de medios electrónicos (ej. Consulta médica con utilización de equipos electrónicos, consulta en tienda del catálogo electrónico…)[23].

La expresión relativa a la oferta directa de estos servicios a menores, utilizada en el artículo 8 del Reglamento general de la protección de datos. Ante la falta de una definición en la propuesta de Reglamento, podría interpretarse como la "oferta directa de servicios de la sociedad de la información a los niños" (COPPA, 1998) o como aquellos servicios específicamente dirigidos a los menores que la norma pretende proteger, esto es, menores por debajo de 13 años. Esto, desde luego, supone limitar su ámbito de aplicación y podría interpretarse en el sentido de que sitios web dirigidos a un público adolescentes no tendrían que realizar un control de edad de sus usuarios[24].

[22] Indica también este auto que la práctica de los tribunales españoles ha considerado como prestadores de servicios de la sociedad de la información a quienes proporcionan servicios de acceso, correo electrónico, alojamiento de páginas web, alojamiento de mensajes en chat, herramientas de búsqueda de información de Internet o servicios del tipo wikis. Igualmente, analiza este autor en qué casos el suministro de contenidos en Internet no constituye una actividad económica y, en consecuencia, no pueden ser considerados como un servicio de la sociedad de la información (por ej., en el caso de páginas de Internet de carácter personal, si bien se tiene cada vez más hacia un modelo menos centralizado que facilita la generación de ingresos por arte de este tipo de páginas).

[23] Sobre el tema, vid. entre otros, De Miguel Asensio (2011), pp.118 y ss.; Peguera Poch, M. Y Tarrés vives, M. (2010), pp. 319 y ss

[24] No hay que olvidar que en la normativa Estadounidense esta regla se complementa con ciertos requerimientos a las webs ‹‹genéricas›› cuando tengan conocimiento efectivo de que están tratando datos de menores, cosa que no ocurre en el Reglamento europeo, como inmediatamente se pondrá de relieve. Por otra parte, tras la modificación de las normas de desarrollo de la COPPA, se distingue, dentro de los sitios web dirigidos a menores, entre aquéllos cuyo publico principal lo constituyen precisamente los menores protegidos por la Ley, y aquellos otros para los que este sector de la población es sólo un público secundario (pudiendo estos últimos utilizar pantallas de verificación de edad)

La protección de los datos de los menores es tratada en el Reglamento y en concreto en el artículo 8 trata de los siguientes aspectos:

Figura 16. Medidas de protección de datos personales plasmadas en el reglamento europeo
Fuente: Creación propia basada en EU2016/679.

a) *Licitud en el tratamiento de datos*: En aras de la especial protección que merece los derechos y libertades fundamentales de los niños, la ponderación que debe llevarse a cabo con la consiguiente determinación de cuándo debe prevalecer el interés legítimo del responsable y cuándo los derechos y libertades del interesado, debe ser especialmente cuidadosa cuando se trate de datos de menores. (EU 2016/679, Considerando 38, 6).

Ello puede hacer que en estos casos normalmente se decante la balanza a favor de la protección del menor; debiendo, en consecuencia, ampararse el tratamiento de sus datos para que sea lícito en alguno de los otros previstos en el artículo 6.1 de la propuesta de Reglamento (consentimiento, protección del interés vital del interesado, etc.). (EU 2016/679, 6).

b) *Transparencia:* conforme al artículo 11, La información dirigida a menores, que deberá facilitarse en un lenguaje adaptado a sus posibilidades de comprensión (EU 2016/679, 11.2).

c) *El derecho al olvido y a la supresión*: El Reglamento acoge el derecho a la supresión de los datos y a que el responsable se abstenga de darles más difusión especialmente en el caso de los datos proporcionados siendo el interesado un niño (artículo 17.1). Indica el considerando 53 de la propuesta, que se trata de datos que se otorgaron cuando el titular no estaba seguro de los riesgos relacionado con el tratamiento. Por tanto, aunque al menor se le pudiera considerar capacitado para prestar consentimiento por sí mismo, ello no impide que se adopten otras medidas de protección respecto de actuaciones realizadas antes de alcanzar la mayoría de edad. Además, como ya se supo de relieve al principio de este trabajo, esta medida contribuye también a evitar la generación de perfiles desde edades tempranas. (EU 2016/679, 8.1).

d) *Medidas basadas en la elaboración de perfiles*: Toda persona a no debe ser objeto de elaboración de perfiles a través de tratamientos automatizados de datos. Si bien este precepto no hace referencia expresa a los menores, el considerando 58 de la propuesta de Reglamento señala, para los supuestos excepcionales en que pueden admitir estas medidas, que en ningún caso deben referirse a un niño. (EU 2016/679, 20).

e) *Evaluación de impacto*: dentro del objetivo perseguido por el Reglamento de simplificar las cargas administrativas de los responsables de tratamientos, pero asegurando un estricto cumplimiento de la normativa de protección de datos, se prevé como nueva obligación de los responsables de tratamientos la de realizar evaluaciones de impacto en materia de protección de datos en ciertos casos, e incluye como operación que conlleva este tipo de riesgos el tratamiento de datos personales en bases de datos automatizadas relativas a niños. En este supuesto se podrían considerar por ejemplo, los ficheros de Colegios o los que recaben datos personales de menores a través de sitios web específicamente dirigidos a éstos. (EU 2016/679, 33.2.d).

f) *Códigos de conducta*: El fomento de la autorregulación constituye también uno de los objetivos del Reglamento. La elaboración de estos Códigos de conducta, que deberán tener en cuenta las características de los distintos sectores de tratamientos de datos, entre ellos, el relativo a la información y protección de los niños. (EU 2016/679, 38).

g) *Campañas de sensibilización por las autoridades de control*: Por último, el Reglamento incide también en las funciones de los entes de control dentro del accionar encaminado a la protección de los menores, así como la sensibilización de la ciudadanía para proteger el derecho de los niños frente al tratamiento de sus datos personales, en particular, con actividades específicas dirigidas a los niños. Se trata, en realidad, de una medida que las autoridades de control españolas (y, en general, las nacionales de distintos países miembros) vienen realizando en los últimos años, sobre todo desde el auge de las redes sociales, con el fin de conseguir una mayor educación y sensibilización de los riesgos en el entorno online[25].

h) *Consolidación de Estándares Internacionales* para facilitar la cooperación en materia del tratamiento adecuado de los datos personales en concordancia con la protección de diversos derechos entre los distintos Estados.

Muchos otros países fuera de la UE también adoptaron leyes de protección de datos debido a la influencia de la Organización para la Cooperación y el Desarrollo OCDE, y sus directrices sobre protección de datos, influenciaron las negociaciones del Consejo de Europa con la UE para declarar que sus regímenes proporcionan una protección adecuada de los datos y suponen un respeto por los estándares de protección generales, que son aplicables tanto al sector público como

[25] Tanto la AEPD como las Agencias que existen en algunas Comunidades Autónomas, han creado diverso material de carácter formativo y orientador sobre la protección de si intimidad y datos personales, dirigido a los propios menores, padres, profesores, etc. Así, por ejemplo, a AEPD) ha elaborado quías para el tratamiento de datos de los datos de los menores de edad y para los usuarios de Internet (incluido menores). También la Agencias autonómicas, junto con la Comisión de Libertadores e Informática han creado guías para el uso de las TIC por edades (hasta los 11 años, de 12 a 14 y de 15 a 17 años). Pueden consultarse en las webs de las distintas Agencias: http://www.agpd.es, http://www.apdcat.net, http://www.avpd.euskadi.net

al privado. Es un llamado a salvaguardar los derechos de los niños por encima del interés económico de los diferentes operadores de la información.

2.2. Modelo sectorial de protección de datos personales: Estados Unidos de Norteamérica

La tutela de los datos personales en Estados Unidos se analiza en un contexto propio de un país que se caracteriza por tener privilegios en seguridad pública y defensa nacional y que por lo tanto, necesita considerar regulaciones y criterios de retención y acceso de datos a través de normas específicas, es decir su principal atención se encuentra en el acceso de los datos personales por parte de los entes de control y vigilancia (Privacy Act) en aras de prevenir posibles vulneraciones y riesgos externos o propios del poder del Estado.

Tabla 13.

Normativa del derecho a la privacidad en Estados Unidos (a nivel federal)

Título	Title V of the Gramm- Leach-Bliley Act (GLBA)
Referencia legal	15 U.S.C. §6801,et seq
Objeto de la norma	"Establece condiciones para la cesión por entidades financieras de información financiera de consumidores a terceras entidades no filiadas. A tal fin tienen que informar a los consumidores sobre sus prácticas de recogida y cesión de datos. También están obligadas a proporcionar a los consumidores la posibilidad de oponerse (opt-out) a la cesión de sus datos."
Sanciones	"Dependerá de cada caso atendiendo a quién sea la autoridad competente"
Autoridad competente	Federal Trade Commission Agencia independiente del gobierno de los Estados Unidos, establecida en 1914. "Su misión principal es promover los derechos de los consumidores y la eliminación y prevención de prácticas que atentan contra la libre competencia."
Título	The Children's Online Privacy Protection Act (COPPA)
Referencia legal	15 U.S.C. §6501,et seq
Objeto de la norma	"Protege la recogida de datos personales de menores de 13 años por medios electrónicos. Se aplica a los operadores de sitios web comerciales que estén dirigidos a menores de 13 años o si el operador conoce que obteniendo

	información de menores de 13 años. El tratamiento de datos de menores de 13 años requiere informar a los padres y obtener su consentimiento.”
Sanciones	“15 U.S.C.41 et seq”
Autoridad competente	Federal Trade Commission
Título	Identity Theft and Assumption Deterrence Act of 1998 (Identity Theft Act)
Referencia legal	18 U.S.C. § 1028, 1028(a) (7)
Objeto de la norma	“Tipifica como crimen federal la transmisión o uso intencionado, sin autoridad legal, de los datos de identificación de otras personas con la finalidad de cometer, ayudar o auxiliar en, una actividad ilícita que constituya la violación de una ley federal o que constituya delito conforme a cualquier ley estatal o local aplicable. La FTC establecerá una base de datos primaria que tiene por objeto recoger datos de víctimas del delito de suplantación de identidad con la finalidad de asistirles y referirlos a las autoridades competentes en cada caso.”
Sanciones	“1 de cárcel cuando lo obtenido tenga un valor acumulado igual o superior a 1,000 dólares”
Autoridad competente	Autoridad competente en cada caso
Título	The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
Referencia legal	42 U.S.C. §1320d,et seq
Objeto de la norma	Establece “los estándares para proteger la privacidad de los datos de salud de los individuos. La regulación aplica a planes de salud, centros de salud, y proveedores de servicios médicos que transmitan información por medios electrónicos. Aunque hay excepciones, las entidades sujetas a la regulación tienen que informar a los interesados obre los usos y cesiones de sus datos de salud, obtener el consentimiento para poderlos tratar y ceder, y proporcionar acceso a los datos que son objeto de tratamiento”
Sanciones	“Sanciones civiles y penales que variarán en función de la infracción y que pueden llegar hasta 1.500.000 dólares.”
Autoridad competente	Oficina de Derechos Civiles del Ministerio de Salud y Servicios Humanos (Office of Civil Rights, U.S. Department of Health&HumanService)3
Título	The Cable Communications Policy Act of 1984
Referencia legal	47 U.S.C. § 551
Objeto de la norma	Limita la recogida, tratamiento y comunicación de información de los abonados. En concreto, “impone a los operadores de cable la obligación de informar y obtener el conocimiento, electrónicamente o por escrito, de los consumidores para poder tratar sus datos. Igualmente, el consentimiento es exigible para poder comunicar los datos a terceros, salvo requerimientos de autoridades basados en una orden judicial o para el cumplimiento de los servicios contratados. Los abonados tienen el derecho de acceso y rectificación de sus datos.”
Sanciones	El Tribunal puede otorgar: “1. Daño emergente que no sea inferior al daño asegurado a razón de 100 dólares por cada día de infracción o 1.000 dólares. Cualquier que sea la cantidad superior.

	2. Lucro cesante. 3. Costas de abogado y otras costas de litigio razonables.”
Autoridad competente	“Acción civil ante los Tribunales de Distrito de los Estados Unidos.”
Título	The Fair Credit Reporting Act (FCRA)
Referencia legal	“15 U.S.C. § 1681,et seq”
Objeto de la norma	“Aplica a los burós de créditos y permite la cesión de información crediticia únicamente a entidades que tengan finalidades adecuadas. Establece el derecho de los consumidores a acceder y rectificar la información en los informes de crédito.”
Autoridad competente	FTC. Limitada a algunas entidades financieras.
Título	The Federal Videotape Privacy Protection Act
Referencia legal	18 U.S.C. § 2710
Objeto de la norma	“Obliga a las entidades que se dedican a la venta o alquiler de vídeos a obtener el consentimiento de los clientes para poder ceder sus datos personales. Sólo podrán facilitar listas de consumidores que incluyan nombres y direcciones si se les ha ofrecido previamente la opción de ser excluidos (opt-out) de dicho listado”
Sanciones	El Tribunal puede otorgar: “1. Daño emergente que no sea inferior al daño asegurado a razón de 2.500 dólares. 2. Lucro cesante 3. Costas de abogados y otros costes de litigio razonables. 4. Otra compensación que el tribunal estime adecuado para reparar el daño”
Autoridad competente	Acción civil ante los Tribunales de Distrito de los Estados Unidos.

Fuente: Creación propia basada en la normativa de EE.UU.

Se han identificado una serie de instrumentos de regulación especial de acuerdo a los sectores sociales, económicos y políticos de relevancia para Estados Unidos por ser una sociedad que se caracteriza por el consumo y donde la importancia de la privacidad se pondera por intereses superiores como la “seguridad y la supremacía nacional”. Por lo tanto, el tratamiento a la información de las personas se protege con el derecho a la privacidad, el cual está llamado a su desaparición con la muerte del sujeto de derecho. El derecho a la privacidad de los niños en la sociedad de la información online, es uno de los temas regulados de manera sectorial y de especial cuidado por la Legislación de Estados Unidos.

2.2.1. Ley de Protección de la Privacidad en Línea de Los Niños: "The Children's Online Privacy Protection Act" (COPPA, 1998):

En el ordenamiento jurídico de Estados Unidos se han identificado una serie de instrumentos de regulación especial para cada tipo de dato personal, para el caso sub-examine de los NNA, dependiendo de igual manera de su relación con la privacidad y con la protección de intereses propios de la soberanía estatal, como se identifica a continuación:

Tabla 14.

Marco normativo de la privacidad y la protección de datos personales de niños en los Estados Unidos

Organización internacional o entidad	Norma	Tema que regula	Año de expedición
Bill of rights (Carta de Derechos de los Estados Unidos)	IV Enmienda	"El derecho de los habitantes de que sus personas, domicilios, papeles y efectos se hallen a salvo de pesquisas y aprehensiones arbitrarias, será inviolable, y no se expedirán al efecto mandamientos que no se apoyen en un motivo verosímil, estén corroborados mediante juramento o protesta y describan con particularidad el lugar que deba ser registrado y las personas o cosas que han de ser detenidas o embargadas." (IV Enmienda)	1787
"Comisión Interamericana de Derechos Humanos y la Corte Interamericana de Derechos Humanos"	Convención Americana sobre derechos humanos	Base "del sistema interamericano de promoción y protección de los derechos humanos" "Artículo 11. Protección de la Honra y de la Dignidad 1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad. 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación. 3. Toda persona tiene derecho a la protección de la ley contra esas	1969 (entró en vigor en 1978)

Organización internacional o entidad	Norma	Tema que regula	Año de expedición
		injerencias o esos ataques." ("Convención Americana sobre derechos humanos")	
Ley federal	"Privacy Act" (Ley de privacidad)	Buscaba "proteger a la persona frente a datos de índole personal, que se ponen en conocimiento del público o de terceros sin el consentimiento del afectado." Alcance limitado al Gobierno federal y no al gobierno estatal o al sector público. (Ley de carácter general de la protección de datos tiene base en la "Privacy Act")	1974
Federal Trade Commision FTC	"Children's Online Privacy Protection Act" (COPPA)	"Se aplica únicamente a los datos personales recabados online de los menores por debajo de los 13 años de edad." La Ley como "sus normas de desarrollo contienen una definición de ‹‹personal information›› o datos personales a los efectos de su aplicación, principios para su tratamiento, la autorregulación, el control y la revisión normativ"a ("Ley de protección de la privacidad de los niños en línea", COPPA, 1998)	1998 (entra en vigor en el 2000)

Fuente: Creación propia basada en la normatividad de EE.UU.

De acuerdo con lo anterior, los Estados Unidos de Norteamérica desde finales del siglo XVIII da los primeros pasos a la garantía de un perfil de intimidad familiar relacionado con la inviolabilidad del domicilio y establece ciertos límites de su acceso de forma arbitraria. Ya en el siglo XX el reconocimiento de la protección de datos de carácter general es una realidad legislativa con la Privacy Act que fundamenta en 1998 la promulgación de la Ley de Protección de la Privacidad en Línea de Los Niños: Children's Online Privacy Protection Act (en adelante COPPA). Primera norma de carácter sectorial dedicada a la protección de la privacidad de la información personal de los niños, y referente normativo para muchos países que han regulado su tratamiento[26].

[26] En Canadá, al igual que ocurre en el ámbito europeo, la normativa en materia de protección de datos (en particular, la Ley de protección de datos personales y documentos electrónicos de 2000 – PIPEDA, en inglés -; y, en el caso de la provincia de Quebec, la Ley sobre protección de datos personales en el sector privado, de 1993) no contienen normas específicas para menores. No obstante, en la práctica muchos sitios web para menores en Canadá han adoptado las previsiones de la COPPA, convirtiéndose así en un modelo para Norteamérica. Vid., al respecto, Steeves, v. y Webster,

3.2.1.1. Ámbito de aplicación

La aplicación de la COPPA se dirige al tratamiento de datos personales online de los niños "menores de 13 años de edad" y establece una definición de "personal information" o datos personales el cual se refiere a aquella información que identifique o permita contactar a una persona y de acuerdo con su aplicación[27]: "el nombre; dirección; correo electrónico; teléfono; número de la seguridad social; información que el menor revele sobre sí mismo o su familia y que se asocie a los anteriores datos" (COPPA, 1998, 1302(8)); un ‹‹identificador permanente›› (ej., número de cliente contenido en una cookie) que se asocie a datos de una persona identificable; o la combinación de nombre o fotografía con otra información que permita contactar con la persona presencial virtualmente.

La recolección tratamiento y comunicación de datos personales se definen en las normas de desarrollo de la COPPA. La recolección de datos hace referencia, no necesariamente requerir los datos personales a un menor, sino también el posibilitar que el niño pueda hacer públicos sus datos (ej., a través de cookies). Y la comunicación o revelación de datos (‹‹disclosure››), incluye tanto la cesión de datos (compartir, vender, alquilar, etc. Los datos personales), como poner a disposición públicamente dichos datos (ej., a través de un chat, tablones de anuncios, etc.).

c., ‹‹closingthe barn door: the effect of parental supervisión on canadian children's online privacy››, en bulletin of science, technology & society, vol. 28, núm. 1, febrero 2008, pp. 4 y ss.; benyekhlef, k., Couture – Ménard, p. a. y Paquette-Bélanger, e., ‹‹menores, redes sociales y el derecho al olvido››, en Piñar Mañas, j. l., Redes sociales y privacidad del menor, Reus, Madrid, 2011, pp.194 y ss.

[27] Sec. 1302 (8) COPPA y §312.2 COPPA Rule

Los operadores y responsables de los sitios web o servicios en línea, son requeridos frente al ‹‹conocimiento efectivo›› de manera particular para el tratamiento de los datos personales de niños, sin obligarlos a comprobar su edad.

3.2.1.2. Principios

Los principios que fundamentan la protección de la privacidad y seguridad de la información de NNA, se identifican en:

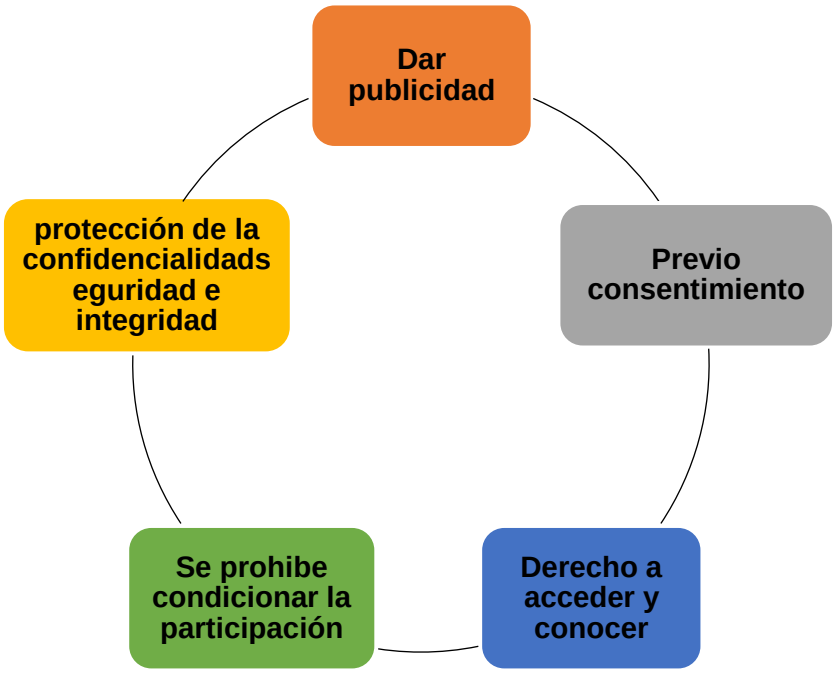


Figura 17. Principios de la ley COPPA.
Fuente: Creación propia (2017).

La dimensión publicitaria, legalidad del consentimiento parental, derecho de accesibilidad y conocimiento de la información personal tratada del menor, el ejercicio de los derecho de

cancelación del dato y rechazo del tratamiento, confidencialidad, seguridad e integridad de los datos personales, así como, limitar la participación del niño en actividades de comunicación (Andreu Martinez, 2014).

Y sobresale las "Políticas de privacidad sobre el tratamiento de datos de los menores"[28] publicadas, adecuadas y transparentes para su comprensión y conocimiento de su finalidad.

Mecanismos de recolección y verificación legal del consentimiento por parte de los representantes legales y condiciones del tratamiento[29], por parte de los distintos operadores de sitios web: el consentimiento del progenitor por medio del correo electrónico para asegurar su veracidad si es interno, pero si es para circulación de los datos (identificación del rostro y la voz entre otros).

La autorregulación: "puerto seguro" (safe harbor), por parte de la industria.

Demostrar la implementación de código autorregulatorios para la protección de los niños aprobados la Federal Trade Commission (en adelante FTC) Como por ejemplo código de buenas prácticas promovido por la industria de la publicidad y el marketing destinado a los niños[30].

La Unidad de Revisión de Publicidad Infantil: "Children's Advertising Review Unit" (en adelante CARU), cumple una función de control y evaluación de las webs cuyo destino de información son los niños, para aseguramiento y cumplimiento de la normativa COPPA.

> "Por ejemplo el caso de la empresa UMG Inc., demandada por la CARU porque como discográfica disponía de diversas webs de promoción de sus productos y alguna de ellas estaba dirigida a menores (por las estrellas del pop y las actividades que contenía), y las webs genéricas recaban el dato de fecha de nacimiento, por lo que tenían un ‹‹conocimiento efectivo›› de que

[28] Vid. § 312.4 COPPA Rule
[29] § 312.4 (c) COPPA Rule.
[30] El código se denomina ‹‹ Self-RegulatoryProgramforChildren'sAdvertising›› y puede consultarse en http://www.caru.org/guidelines/.

trataban datos de menores, sin consentimiento previo de sus representantes legales, por lo que fue sancionada por $400.000 por incumpliendo de la COPPA". (Federal Trade Comisión, 2017).

2.2.2. Inspección y propuesta de modificación de las normas de desarrollo de la COPPA

La revisión de las normas de desarrollo de la COPPA por parte de la FTC se contempló cada cinco años, con el objeto de actualizar los conceptos y su implementación efectiva. La revolución de la sociedad de la información que ha traido consido cambios tecnológicos es cada vez más rápida con el acceso a plataformas líquidas y algoritmos de inteligencia artificial que va más allá de las redes sociales y la utilización de dispositivos móviles de ultima generación digitalizada que invita a todos los Estados y entidades como la FTC a incorporar una regulación más pertinentes a dichos cambios como la COPPA, con el fin de responder a dichos paradigmas iustecnológicos [31] sin olvidar la protección de la privacidad, el panóptico digital de la familia, la autorregulación de la industria de marketing dirigida a los niños, niñas y adolescentes en razón de su capacidad legal. La COPPA realizó un proceso de consulta en el año 2011 y 2012[32] que luego fueron aprobadas en 2012 y entró en vigencia en 2013, con algunas precisiones tales como:

[31] En febrero de 2012, la FTC llevó a cabo un estudio sobre las aplicaciones para móviles dirigidas a menores (denominado ‹‹ Mobile apps forkids: current privacy disclosures are disap-pointing ››, accesible en: http//ftc.gov/os/2012/02/120216mobile_apps_kids.pdf), en donde se pone de relieve la deficiente información en cuanto a las practicas relacionadas con la protección de datos, de manera que los padres, antes de la descarga de la aplicación, no pueden conocer qué datos se recaban, el uso que se les da y quién tendrá acceso a los datos de los menores. De ahí que la FTC anunciara una enérgica aplicación de la COPPA en este ámbito.

[32] Puede consultarse en: http://ftc.gov/os/2011/09/110915coppa.pdf y http://www .ftc.gov/os /2012/ 08/120801copparule.pdf

- “Expandir la definición de dato personal para que incluya la información de localización geográfica y también los archivos de fotos, video y audio que contengan la imagen o voz de un niño tales como en sitio web.
- Redefinir las pautas de recolección de información: por un lado, simplificando y haciendo más visible la contenida en las políticas de privacidad; y por otra, respecto de la notificación que reciban los padres, haciendo que se muestre la información principal en un aviso sencillo y de conocimiento inmediato (succinct ‹‹ just-in-time ›› notice). Asi como permitir el acceso a los adolescentes de participar en comunidades interactivas de manera responsable.
- Actualizar los mecanismos de consentimiento parental verificable por parte de los operadores que incluyan en las notificaciones paternas la información necesaria y clara para su comprensión previa.
- Fortalecer los requisitos de confidencialidad y seguridad, de manera que se asegure que no sólo el proveedor de servicios en online, sino también los terceros a los que éstos faciliten datos de menores, han implementado medidas razonables de protección de los datos.
- Añadir disposiciones en materia de retención y supresión de datos (por ej., que no se podrán guardar los datos más allá del tiempo razonablemente necesario para cumplir la finalidad para la que fueron recabados, o que se adopten medidas de seguridad a la hora de suprimir la información, con el fin de evitar accesos no autorizados).
- Reforzar los requisitos exigidos a los códigos de autorregulación, requiriendo, entre otros, una auditoria anual a los miembros y un informe a la FTC de los resultados globales de dichas auditorias.” (COPPA, 2013, Recuperado: http://www.ftc.gov/opa/2012/12/coppa.shtm.).

Sobresale los retos de conceptualizar los datos de contacto online,[33]referentes a la geolocalización o big data, inteligencia artificial requieren ser revisados a la luz de su marco teórico y jurídico por los actores protagonista de su tratamiento como el Estado de derecho y la industria informática desde la privacidad desde el diseño.

Al igual el concepto de "operador y hosting de datos de menores de edad" en la web[34] requiere de un "estándar de responsabilidad superior" como generadores de contenidos, juegos, imágenes dirigidas a NNA como sujetos de derecho de especial protección.

En cuanto al significado de sitio web o servicio en línea dirigido a menores, requiere de precisiones en cuanto al funcionamiento y estructura de códigos binarios y algoritmos que permitan entender el funcionamiento para el tratamiento de información dirigida a menores de edad.

Frente a los mecanismos de verificación del consentimiento parental sigue siendo limitado su abordaje en cuanto, es necesario regular el tratamiento de la información en nuevas plataformas tecnológicas online con códigos de verificación mas segura.[35]. Es preciso hacer distinciones entre usos internos y externos de la información personal y más aún cuando se trata de NNA, y exigir

[33] Para la FTC, esta definición identifica a forma de contacto directo, privado y usuario a usuario que se pretende cubrir con dicha norma, ya que el contacto en línea puede ser alcanzado actualmente a través de diferentes mecanismos, más allá del correo electrónico. La FTC no comparte algunas de las observaciones realizadas durante el proceso de reforma, como por ej., las que pretendían considerar que actividades como los chats moderados no suponen ‹‹un contacto directo›› online con un menor y, en consecuencia, no era necesario que el operador que utilizara nombres de usuario anónimos, informara y requiriera el previo consentimiento parental.

[34] Señala la FTC que, más allá de los casos en que el sitio web o servicio puede no ser dueño, controlar o tener acceso a la información personal recolectada, cabe que dicha información sea recabada en su nombre, debido a los beneficios que recibe agregando contenidos más atractivos, funcionalidades o ingresos publicitarios.

[35] Reconoce la FTC que la mayor parte de los comentarios recibidos sobre la propuesta de reforma de este punto solicitaban de forma enérgica mantener este sistema. Señalaban, así, que se trata de un método fácil de usar para las compañías y los padres, fácil de entender, efectivo y asequible; que la implementación de otros mecanismos supondría importantes costes para los operadores y los padres; se cuestionaba la fiabilidad de otros sistemas de obtención del consentimiento o que la eliminación del sistema e-mail plus implicara una mayor innovación en esta materia.

de la industria mecanismos mas confiables de verificación del consentimiento informado y voluntario del titular del derecho protegido.

Estados Unidos acepta el reto de continuar en la adecuación de su normativa a los intereses de protección colectiva de menores, distinguiendo que la edad de acceso a la tecnología es cada vez menor y los adolescentes buscan su reconocimiento mediante la autodeterminación informativa sin mayores controles[36]. Se requiere de vías mas adecuadas a la autopoiesis de la protección de datos personales de una generación que busca obtener mayor y más acelerada información del mundo[37]. Es necesario repensar el alcance de la COPPA frente a la efectividad del tratamiento de datos de NNA, en el contexto real de una sociedad de la transparencia y modernidad líquida.

2.2.3. Logro: Puerto seguro de la privacidad EU – EE. UU

En la actualidad, entre los países de América que han sido reconocidos con un nivel adecuado de protección de datos se destaca Estados Unidos (2016):

Tabla 15.

Comparativo del nivel adecuado de terceros países frente a la reglamentación - Comunidad Europea de protección de datos personales

País	Norma constitucional	Norma General	Principios básicos legales	Normas sectoriales	Convenio 108/81	Fuentes

[36] Los adolescentes tienen más facilidad para acceder a internet (bibliotecas, casas de amigos, dispositivos móviles, etc.); que es menos probable que un adolescente facilite los datos de contacto de sus padres y mucho más que falsifique esta información o mienta sobre su edad. Además, los tribunales han reconocido que, conforme aumenta la edad, aumenta también su derecho constitucional a acceder a la información y expresarse públicamente por sí solos. Vid. Proposed Rules September 2011.

[37] Vid. La declaración presentada por la FTC ante el Senado sobre el tema (‹‹ProtectingYoouths in an online wordl››), disponible en: http:// www.ftc.gov/os/testimony/100715toopatestimony.pdf

Canadá	Sí	Sí	Sí	Sí	Sí	Decisión 2002/2/CE
Argentina	Sí	Sí	Sí	Sí	Sí	Decisión 2003/490 CE
Uruguay	Sí	Sí	Sí	Sí	Sí	Decisión 2012/484/CE
Estados Unidos	No	Si	Sí	Sí	No	Decisión 2016/1250/CE

Fuente: Creación actualizada, basada en Remolina, N. (2010) https://www.privacyshield.gov/list

Estados Unidos, a la fecha es el último país americano en recibir la Decisión de Ejecución (UE) de nivel adecuado de tratamiento de Protección de Datos de acuerdo a la Directiva 95/46 del Parlamento Europeo y del Consejo, y el otorgamiento del Escudo de la privacidad UE. EE. UU, que hace relación a "los principios de privacidad" así como los compromisos de las autoridades Estadounidenses referidas en la Directiva 95/46/CE, artículo 25, apartado 1 la cual dispone lo siguiente:

> «Los Estados miembros dispondrán que la transmisión a terceros países de datos personales que se encuentren en tratamiento o estén destinados a ser transformados tras la transferencia sólo podrá tener lugar si, el tercer país en cuestión garantiza un nivel de protección adecuado. Sin perjuicio del cumplimiento de las disposiciones nacionales adoptadas de conformidad con las demás disposiciones de la presente Directiva."

La Comisión valoró la regulación y las prácticas de privacidad de los Estados Unidos, los compromisos de los operadores y responsables del tratamiento como de los órganos oficiales que permitan asegurar un nivel adecuado de administración de los datos personales en el referente del Escudo de la privacidad UE-EE. UU y es así que éste fue otorgado gracias a un "sistema de autocertificación" en el que los operadores de la información a nivel estatal se comprometen a

respetar “los principios de protección de la vida privada” sin que con ello se afecte el tratamiento jurídico de la Unión Europea.

Tabla 16.

Estados Unidos reconoce los principios de protección de datos personales

Principios en el marco del Escudo de privacidad	Principio complementario
Principio de notificación	Sobre “datos de recursos humanos”
Principio de integridad de los datos y de limitación de la finalidad	
Principio de opción	
Principio de integridad de los datos y de limitación de la finalidad	
Principio de seguridad	
Principio de acceso	
Principio de recurso, aplicación y responsabilidad	
Principio de la responsabilidad de la transferencia ulterior	

Fuente: Creación propia, fundamento Decisión 1250/CE 2016

Es importante resaltar de acuerdo a la Decisión (1250/CE 2016), que la Comisión considera los principios de privacidad determinados por el Departamento de Comercio de los Estados Unidos de manera global y sustancialmente garantista de conformidad con la Directiva 95/46/CE: “el acceso a los datos personales transferidos en el marco del escudo de la privacidad UE EE.UU. y utilización de los mismos por los poderes públicos Estadounidenses”, la Tutela Judicial efectiva, transparente de la privacidad en los diferentes ámbitos, así como los mecanismos de control[38] y

[38] Decisión (1250/CE 2016) […] Las declaraciones y compromisos prestados por el Gobierno Estadounidense, la Comisión opina que las injerencias de los poderes públicos de los Estados Unidos en los derechos fundamentales de las personas cuyos datos se transfieran desde la Unión a dicho país en el marco del Escudo de la privacidad a efectos de seguridad nacional, aplicación de la ley u otros fines de interés público, y las consiguientes restricciones impuestas

supervisión frente al incumplimiento de la protección cuyo propósito se encamina a rectificar y suprimir las contingencias identificadas (Decisión 1250/CE 2016).

Finalmente frente a la cooperación internacional para proteger la privacidad infantil, la "Federal Trade Commission" (FTC) y la "Red Global de Vigilancia de la Privacidad: Global Privacy Enforcement Network" (GPEN), conformada por: "autoridades de Protección de datos de Canadá, Francia, Nueva Zelanda, Israel, Australia, Irlanda, España, Reino Unido, Italia, Países Bajos, Alemania y Victoria (Australia)", y Estados Unidos (FTC) entre otras agencias de protección de datos personales se está avanzando para proteger en todo el mundo la privacidad de los niños en internet. Proteger la privacidad infantil y ayudar a los negocios a comprender sus responsabilidades de cumplimiento de los estándares de privacidad en el mundo globalizado. (Feredal Trade Commission, 2017).

2.3. Modelo híbrido de protección de datos personales: Colombia

El modelo centralizado de la protección de datos personales propio de la Unión Europea en consonancia con el modelo sectorial propio de los Estados Unidos, han facilitado la construcción y consolidación de instrumentos jurídicos que responden a la confianza en las instituciones estatales o en la confianza al sector empresarial en juego; y ha sido acogido el modelo europeo en un alto porcentaje en el mundo, como es el caso de Colombia con la expedición de la Ley Estatutaria 1581 de 2012.

La Corte Constitucional colombiana, señaló la importancia de acoger en el ordenamiento jurídico un modelo híbrido de protección de datos personales que se caracteriza en gran medida

a las entidades autocertificadas con respecto a su adhesión a los principios de privacidad, se limitarán a lo estrictamente necesario.

por los lineamientos propios del modelo centralizado y el modelo sectorial (Corte Constitucional, Sala Plena, Sentencia C-748, 2011). Modelos que como se puede observar a continuación en el cuadro comparativo se identifican por el enfoque basado en la prevención o la protección del derecho de carácter fundamental por parte de las entidades de vigilancia del Estado.

Tabla 17.

Análisis comparativo de modelos de protección de datos personales

Modelo Híbrido de Protección de Datos Personales Colombia
Enfoque reactivo y de gestión de riesgos
Enfoque mixto Derecho autónomo de carácter fundamental
Confianza en el gobierno y en Mercado
Los datos se recaban cuando es necesario
Los derechos y las excepciones se prevén en Ley
Existen autoridades públicas especializadas Ej. Delegatura para la protección de datos personales de la Superintendencia de Industria y Comercio
Se protege a todo individuo que esté en territorio colombiano en virtud de las normas y tratados internacionales

Fuente: Creación propia

Aunque los Estados Unidos por regla general son reacios a regular la industria de la información, existe un acuerdo de puerto seguro con la UE, para garantizar que el libre flujo de información personal entre Europa y los Estados Unidos con el fin de que no fuera restringido por la UE debido a la inadecuada protección de datos personales en los Estados Unidos.

En comparación con el modelo sectorial hay entidades de control y vigilancia sectoriales dependiente del Estado, con diversas categorías de datos personales, así como diversidad normativa donde se evidencia la falta de sumisión a una regulación específica, se acogen legislaciones especiales y diferentes de acuerdo a cada clase de categoría de personal, de acuerdo con la proximidad a los derechos a la intimidad o privacidad, la seguridad y defensa nacional; intereses de especial protección para el Estado y frente al cual se concluye que la ponderación

genera diferenciación en el tratamiento jurídico como la intervención de las autoridades según el tipo de dato.

De igual manera, se caracteriza la protección de datos personales por la autorregulación[39] de los mercados y el Estado regula la protección "de ciertos datos en ámbitos en los que se presenta un alto riesgo de lesión de la intimidad, como la esfera financiera, la salud y los derechos de los niños" (Corte Constitucional, Sala Plena, Sentencia C-748, 2011).

El modelo híbrido de protección de datos personales propio del tratamiento jurídico en Colombia, partió de:

> "…. la Ley 1266 de 2008 buscaba convertirse en una ley de principios generales aplicable a todas las categorías de datos personales aplicable a todas las categorías de datos personales. Sin embargo, como observó esta Corporación en la Sentencia C-1011 de 2008 [49], peses a su pretensión de generalidad, el proyecto de ley en realidad solamente establecía estándares básicos de protección para el dato financiero y comercial destinado a calcular el nivel de riesgo crediticio de las personas." (Corte constitucional, Sala Plena, Sentencia C-748, 2011).

Por lo tanto, la Ley 1266 se le dio la categoría de una regulación sectorial del habeas data. Que luego con la Ley 1581 de 2012 se incluyen estándares mínimos de tratamiento de datos personales, cuyo objeto radica en: "… disposiciones generales para la protección de datos personales". Y es así que el modelo de regulación del tratamiento de datos personales en Colombia obedece a un sistema híbrido de protección en el que confluye "una ley de principios generales con otras regulaciones sectoriales que deben ser estudiados en concordancia con la ley general, pero que

[39] Dos conceptos de autorregulación en el contexto de la protección de datos personales para resaltar es el de la Red Iberoamericana de Protección de Datos: "(…) las reglas adoptadas por las entidades para definir sus políticas y compromisos relativos al tratamiento de los datos personales.". Ver documento elaborado por el Grupo de Trabajo reunido en Santa Cruz de la Sierra – Bolivia. Los días 3 a 5 de mayo de 2006 www.redipd.org. Y la Comisión Europea se ha referido a la autorregulación como códigos de conducta "el conjunto de normas que se aplican a una pluralidad de responsables del tratamiento que pertenezcan a la misma actividad profesional o al mismo sector industrial, cuyo contenido haya sido determinado fundamentalmente por miembros del sector industrial o profesión en cuestión".

introduce reglas específicas que atienden a la complejidad del tratamiento de cada tipo de dato" (financiero, publicidad, tecnológicos entre otros). (Corte Constitucional, Sala Plena, Sentencia C-748, 2011).

A continuación, se describe los documentos internacionales que han inspirado el ordenamiento normativo del tratamiento de datos personales como un derecho desarrollado por Europa, Norteamérica, Latinoamérica cada uno con un enfoque jurídico propio de su cultura y tradición socioeconómica y política local con una mirada de armonización o de adecuación de referentes mínimos de tratamiento global, para una mayor comprensión de su injerencia dogmática en el modelo híbrido colombiano.

2.4. Armonización y estándares internacionales de protección de datos personales y la privacidad de los niños

Las autoridades estatales realizan esfuerzos por medio de estándares internacionales de protección de datos personales para contrarrestar los riesgos de los NNA, en un entorno pluridimensional inimaginable que se generan con ocasión del desarrollo de los tratados de libre comercio, donde surge la necesidad de circular internacionalmente datos personales, con países que ofrezcan un nivel adecuado de protección frente a los estándares internacionales, en particular Europa, que ha sido pionera en desarrollar la reglamentación de cara a las nuevas tendencias de la era digital.

Tabla 18.

Principales organizaciones internacionales que han emitido documentos sobre tratamiento de datos personales

Organización	Principales documentos
Red Iberoamericana de Protección de Datos (RIPD)	Estándares de Protección de Datos Personales para los Estados Iberoamericanos (2017)
Unión Europea (UE)	(1) Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo del 27 de abril de 2016, relativo a la protección de personas físicas en lo que respecta al 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). **Hace mención específica a la protección de datos personales de los niños** (2) Protocolos adicionales al Convenio 108 del Consejo para la protección de personas respecto al tratamiento automatizado de datos de carácter personal y relativo a la transferencia de datos (2001 y 2018); (3) Carta de los Derechos Fundamentales de la Unión Europea (2000); (4) Convenio 108 del Consejo para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal (1981)
Organización de los Estados Americanos (OEA)	Principios de la OEA sobre la privacidad y la protección de datos personales con anotaciones (2015)
Organización para la Cooperación y el Desarrollo Económico (OCDE)	Directrices relativas a la protección de la intimidad y de la circulación transfronteriza de datos personales (2013, 1980)
Conferencia Internacional de Autoridades de Protección de Datos y Privacidad (CIAPDP)	Estándares internacionales para la protección de la privacidad en relación con el tratamiento de datos de carácter personal – Resolución de Madrid – (2009)
Foro de Cooperación Económica Asia Pacífico (APEC)	Marco de privacidad APEC (2004) APEC Cross Border Privacy Rules (CBPR) APEC Cross Border Privacy Enforcement Arrangement (CPEA)
Organización de las Naciones Unidas (ONU)	Resolución 45/95 de 14 de diciembre de 1990. Principios rectores para la reglamentación de los ficheros computarizados de datos personales

Fuente: Elaboración Nelson Remolina Angarita© (2018)

En procura del proceso de armonización de los temas relevantes del tratamiento de datos personales se fue consolidando su reconocimiento en instrumentos normativos de carácter general que recogen los referentes jurídicos que surgen de las equivalencias respecto a los diversos mitos y tradiciones jurídicas de cada país frente a la tendencia internacional de ciencia, tecnología e innovación como lo refiere Remolina:

> “a) muestran que la protección de datos personales no es nueva y que no son creación original del legislador local sino fruto de una tendencia internacional para tratar de conciliar las necesidades de las empresas, de los Estados y el respeto de los derechos humanos; b) permiten determinar el origen y el alcance de muchos términos, definiciones e instituciones utilizados en las regulaciones locales; c) proporcionan una idea de las tendencias de ciertos aspectos afines al tratamiento de datos personales y permiten tener una aproximación general a los principios e instituciones existentes en otras partes del mundo.” (2018, p. 50-51).

Aunque la novedad de estandarizar el tratamiento moldea el sistema jurídico con cada avance tecnológico que incorpora la gobernanza de los datos a nivel empresarial, gubernamental bajo el enfoque de protección de los derechos humanos, el valor comercial del dato sigue estando presente en las relaciones de consumo, que impiden armonizar de manera global su tratamiento. Se evidencia un amplio desarrollo normativo del tratamiento de los datos personales con el propósito de proteger la privacidad de las personas físicas y a la libre circulación de esta información en línea, entre las que se destaca desde 1980 directrices de la OCDE, que han servido de guía para la regulación del procesamiento automatizado de datos que identifican a las personas como sujetos de derecho, frente al desarrollo del internet en una sociedad global de la información, cuyos principios se resaltan: “democracia pluralista, respecto de los derechos humanos y economías de mercados abiertas” (Directrices OCDE, 2002).

Como por ejemplo de manera particular, las “Reglas de Heredia” destacan las recomendaciones a los poderes judiciales para la divulgación de la jurisprudencia en los países de América Latina, las cuales surgen del Seminario internet y sistema judicial realizado en la ciudad de Heredia, en el cual se aprobaron las “reglas mínimas para la difusión de información judicial en Internet”, (Reglas de Heredia, 2003), las cuales fueron inspiradas en la Directiva europea 95/46/CE 8.1.

Las Reglas de Heredia, con relación a la protección de la privacidad de los menores de edad, establece la anonimización de los datos personales de NNA en las providencias judiciales publicadas en internet de manera explícita en su numeral 5:

> "Regla 5. Prevalecen los derechos de privacidad e intimidad, cuando se traten datos personales que se refieran a niños, niñas, adolescentes (menores)… o cuando se trate de datos sensibles o de publicación restringida según cada legislación nacional aplicable[40] o hayan sido así considerados en la jurisprudencia emanada de los órganos encargados de la tutela jurisdiccional de los derechos fundamentales". (Directiva 95/46/CE 8.1).

Es fundamental que los jueces cuando redacten sus sentencias u otras resoluciones y actuaciones, traten al máximo no invadir la esfera íntima de los sujetos en litigio, como lo expresa las recomendaciones de Heredia para la divulgación de jurisprudencia en América Latina, donde apremia un mayor tratamiento de anonimización[41]: Las Reglas de Heredia tienen ya una vigencia alrededor de 16 años, con trascendencia normativa nacional e internacional en especial para los países latinoamericanos.

A continuación se identifica los "Estándares Internacionales para la Protección de la Privacidad en relación con el Tratamiento de Datos de Carácter Personal" – Resolución de Madrid – (2009), la cual se visibiliza las primeras directrices de armonización a nivel global.

[40] La protección de los niños y adolescentes es unánime en todas las legislaciones de América Latina. Muchos países de la región tienen sus propias categorías de datos sensibles, otros las están desarrollando en nuevos proyectos de ley. En algunos casos la enumeración es más amplia como las "actitudes personales" en Panamá, o los "antecedentes penales" en el proyecto de Costa Rica También en algunos países es muy rica la jurisprudencia constitucional. Recuperado: http://www.iijusticia.org/heredia/Reglas_de_Heredia.htm

[41] Sin perjuicio del principio de máxima publicación que hace referencia la Comisión Interamericana de Derecho Humanos: "el principio de máxima divulgación, la ley debe garantizar que el acceso a la información pública sea efectivo y lo más amplio posible; y en caso de contemplar excepciones, éstas no deben convertirse en la práctica en la regla general.

2.4.1. Estándares de protección de la privacidad en el tratamiento de datos personales a nivel europeo

La Agencia Española de Protección de Datos (AEPD) ha gestionado la "Propuesta Conjunta de Estándares Internacionales de Protección de la Privacidad en relación con el Tratamiento de Datos Personales", buscando la armonización de esa pluralidad de regímenes, labor encomendada a un Grupo de Trabajo de autoridades para que la redactara de forma conjunta para su redacción, la cual fue aprobada en la 31 Conferencia de autoridades de protección de datos y privacidad. (Resolución de Madrid sobre Estándares Internacionales de Privacidad, 2009).

La Resolución de Madríd sobre Estándares Internacionales de Privacidad, no es un acuerdo internacional ni tampoco una normativa jurídicamente vinculante, sin embargo, su valor y relevancia como texto de referencia se derivan de que su elaboración ha contado con una amplia participación de la comunidad internacional de protección de datos y privacidad en aras de garantizar un alto nivel de seguridad y tomando como base instrumentos internacionales en la materia tales como:

- "Directrices de la Organización para la Cooperación y el Desarrollo Económicos - OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales" (1980).
- "Convenio No. 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal" (1981).
- "Directrices de la ONU para la regulación de los archivos de datos personales informatizados, adoptados mediante Resolución 45/90 de la Asamblea General" (1990).

- “Directiva 95/46/CE del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.” (1995).
- Recomendaciones sobre privacidad del Foro de Cooperación Económica de Asia Pacífico - APEC que en su contenido incluye:
    - Principios básicos de protección de datos y privacidad.
    - Derechos de los interesados, incluida la posibilidad de resarcimiento por los daños sufridos.
    - Obligaciones de los implicados en el tratamiento de datos.
    - Previsiones sobre la existencia y características de mecanismos de control.
    - Regulación de las condiciones para la realización de transferencias internacionales
    - Criterios para el diseño y aplicación de medidas de seguridad y medidas preventivas. (2004).

Resalta la necesidad de cooperación entre los distintos Estados para regular el ámbito de aplicación, definiciones, mecanismos de protección, principios básicos, legitimación para el tratamiento, derechos del interesado, seguridad, supervisión que de manera integral y armonizada se coordine a través de estándares internacionales, con el objeto de:

- “a. Definir un conjunto de principios y derechos que garantice la efectiva y uniforme protección de la privacidad a nivel internacional, en relación con el tratamiento de datos de carácter personal;
- b. Facilitar los flujos internacionales de datos de carácter personal, necesarios en un mundo globalizado” (Resolución de Madrid sobre Estándares Internacionales de Privacidad, Disposición general No. 1, 2009).

Desde hace alrededor de 10 años, se enfatiza en los principios y derechos con una perspectiva de facilitar el intercambio de información a gran escala entre los Estados y por lo tanto, es necesario establecer estándares globales que aporten elementos claves para el adecuado tratamiento de datos personales con un enfoque internacional y cuyas regulaciones locales armonicen su desarrollo en diversos ámbitos tales como el espacial, económico y legal; como se reflejó en los acuerdos de: Alemania, Austria, Bélgica, Burkina-Fasso, Canadá, Canadá, Eslovenia, España, Francia, Hong Kong, Irlanda, Italia, Nueva Zelanda, Países Bajos, Portugal, Reino Unido, República Checa y Suiza.

2.4.2. Estándares de protección de datos personales de los Estados Iberoamericanos

Méjico, Ecuador, Argentina, Colombia, Brasil, Perú y Uruguay, Canadá y España, de manera particular, presentan en el año 2009 la necesidad de realizar recomendaciones en materia del tratamiento de la privacidad de la información personal de los niños en la era digital con el Memorándum de Montevideo suscrito como un instrumento consultivo para el sector público y privado (empresas, instituciones educativas, padres y comunidad en general) de relevancia para la protección del interés superior de NNA; acogido especialmente por Colombia de acuerdo al pronunciamiento de la Corte Constitucional. (Corte Constitucional, Sala Plena, Sentencia C-748, 2011).

La propuesta del "Memorándum de Montevideo y la Protección De Datos Personales Y La Vida Privada en las Redes Sociales en Internet de niños" (2009) incorpora las siguientes recomendaciones:

1. "Normativa nacional aplicable al sector público y privado.

2. Derechos y principios básicos reconocidos internacionalmente.

3. Mecanismos para la aplicación efectiva de la normativa (autoridad independiente).

4. Prohibición de tratamiento de datos personales del niño en la industria.

5. Tratamiento de datos personales de adolescentes con mecanismos de controles parentales.

6. Proteger la vida privada es la característica general en todos los sistemas de comunicación.

7. El cambio en el grado de privacidad del perfil de usuario debe ser sencillo y sin costo alguno.

8. Reglas de privacidad de las páginas web, servicios, aplicaciones, entre otros, deben ser explícitas, sencillas y claras, en un lenguaje adecuado para los niños y adolescentes.

9. Se debe proveer información sobre los pronósticos y finalidades para los cuales se utilizarán los datos personales, así como las transmisiones que se realicen a terceros.

10. Se debe proveer información de las transmisiones que se realicen a terceros.

11. Se debe proveer información sobre la persona o personas responsables del tratamiento de la información.

12. Ofrecer un enlace a los parámetros de publicidad.

13. Aviso de que la red social ha preseleccionado los parámetros, si es así que pueden ser cambiados en todo momento según las preferencias de los NNA.

14. Cambio de los parámetros por defecto de los contenidos personales que puedan ser accesibles por los amigos y las redes que el usuario determine.

15. Publicidad de los perfiles de los usuarios según cada perfil debe estar contenida en la política de privacidad.

16. Evitar publicidad no adecuada para NNA.

17. Toda red social digital debe indicar de manera clara la razón que motiva el exigir ciertos datos personales y en particular, la fecha de nacimiento en el momento de inscripción y la creación de una cuenta.

18. Implementar mecanismos para la verificación fehaciente de la edad del niño para abrir una cuenta o acceder a determinado contenido.

19. Toda red social digital, sistema de comunicación o base de datos debería contar con formas de acceso a la información, rectificación y eliminación de datos personales, para usuarios o no usuarios, tomando en consideración las limitantes de la ley.

20. Política accesible a los usuarios en materia de conservación de la información.

21. Obligaciones de privacidad frente a terceros debe ser explicita, clara y visible.

22. La indexación de información de NNA está prohibido en todas sus formas. Las cuentas de menores de edad deben ser "privadas por defectos inaccesibles" a través de buscadores de la red (Comisaria Europea para la Sociedad de la Información.

23. En caso de los adolescentes estos deben autorizar de forma expresa la indexación de sus datos mínimos.

24. Prohibición de instalar aplicaciones sin ser autorizadas expresamente por el usuario.

25. Medidas de índole técnica y operativa para garantizar la seguridad de la información en particular la integridad, disponibilidad y confidencialidad” (Ornelas, 2010 p.p. pp. 171 – 173).

Este instrumento consultivo es una proclama global orientada a la juridificación y gestión de los riesgos de seguridad de las tecnologías de la información digital de NNA que han involucrado un sistema técnico e informático y un sistema jurídico que debe incorporar elementos conceptuales, mecanismos de protección basado en un enfoque humanizante de la industria frente

a los múltiples riesgos de los menores de edad en la era digital; quienes han incursionado en el uso de las tecnología de la información y las comunicaciones a más temprana edad y por lo tanto, requiere ser educado desde la técnica de la privacidad desde el diseño mismo de los sistemas de información para proteger sus derechos como lo refiere la Corte Constitucional en Colombia: "los niños, niñas y adolescentes son titulares de todos los derechos, y por tanto pueden ejercerlos en función de su edad y madurez, además que sus opiniones deben ser consideradas en función de su edad y madurez" (Corte Constitucional, Sala Plena, Sentencia C-748, 2011).

De igual manera, como uno de los referentes destacados de cooperación de los Estados entorno al tratamiento de datos personales basado en estándares globales, surge la Red Iberoamericana de Protección de Datos Personales[42] a partir del Encuentro Iberoamericano de Protección de Datos (EIPD) en el año 2003, iniciativa que contó con el respaldo político en la Declaración final de la XIII cumbre de jefes de Estado y de gobierno de países iberoamericanos cuya misión es:

> "Fomentar, mantener y fortalecer un estrecho y permanente intercambio de información, experiencias y conocimientos entre ellos, así como promover los desarrollos normativos necesarios para garantizar una regulación avanzada del derecho a la protección de datos personales en un contexto democrático, tomando en consideración la necesidad del continuo flujo de datos entre países que tienen diversos lazos en común y una preocupación por este derecho." (Red Iberoamericana de Protección de Datos Personales, 2009).

Colombia, hace parte de la Red Iberoamericana de Protección de Datos Personales con la participación de la Superintendencia de Industria y Comercio – Delegación de la Protección de Datos Personales y en la actualidad (junio, 2017), acoge y aprueba públicamente los estándares de

[42] Ver Red Iberoamericana de Protección de Datos Personales los Estados miembros: Unión Europea, Andorra, Argentina, Colombia, Perú, Ecuador, Argentina, México, Panamá, Venezuela, Portugal, Bolivia, Brasil, Chile, Costa Rica, El Salvador, España, Guatemala, Honduras, Nicaragua, Paraguay, República Dominicana, Uruguay.

protección de datos personales de los Estados Iberoamericanos como un instrumento que contiene las lineamientos orientadores que contribuyen a la construcción de normas de protección de datos en los países de la región iberoamericana, así como facilitar la modernización y pertinencia de las regulaciones existentes frente a los cambios de la sociedad de la información tecnológica.

Los instrumentos jurídicos de orden internacional que soportan la elaboración de los Estándares de protección de datos personales y que han sido referentes en su consolidación se identifican con: "las Directrices de privacidad y de la circulación transfronteriza de datos personales de la Organización para la Cooperación y Desarrollo Económicos (OCDE); el Convenio número 108 del Consejo de Europa y su Protocolo; el Marco de Privacidad del Foro de Cooperación Económica Asia Pacífico y el Reglamento del Parlamento Europeo y del Consejo, relativo a la protección de las personas en lo relacionado con el tratamiento de datos personales y la libre circulación de estos datos, entre otros**."** (Red Iberoamericana de Protección de Datos Personales, 2009).

Los estándares iberoamericanos tienen como objeto:

- "Establecer un conjunto de principios y derechos comunes de protección de datos personales que los Estados Iberoamericanos puedan adoptar y desarrollar en su legislación nacional, con la finalidad de contar con reglas homogéneas en la región.
- Garantizar el efectivo ejercicio y tutela del derecho a la protección de datos personales de cualquier persona física en los Estados Iberoamericanos, mediante el establecimiento de reglas comunes que aseguren el debido tratamiento de sus datos personales.
- Facilitar el flujo de los datos personales entre los Estados Iberoamericanos y más allá de sus fronteras, con la finalidad de coadyuvar al crecimiento económico y social de la región.
- Favorecer la cooperación internacional entre las autoridades de control de los Estados Iberoamericanos, con otras autoridades de control no pertenecientes a la región y

> autoridades y organismos internacionales en la materia**.”** (Red Iberoamericana de Protección de Datos Personales, 2017).

El desarrollo de una regulación en materia de protección de datos personales de NNA no se limita solo a los estándares internacionales, igual la regulación dada por la Unión Europea y los Estados Unidos, se destacan por ser las de mayor relevancia a nivel internacional y no se puede dejar de lado otros preceptos establecidos, como es el caso de los señalados por los Estados Iberoamericanos. Por tal motivo se realizará un análisis sucinto de los aspectos más relevantes de su regulación para establecer un comparativo con lo anteriormente mencionado en las otras regulaciones.

Como se ilustró con anterioridad los estándares de protección de datos personales de los Estados Iberoamericanos resalta en sus consideraciones:

> “Estando conscientes acerca de los riesgos potenciales que pueden derivarse en la esfera de las personas físicas con motivo del tratamiento de sus datos personales a gran escala efectuado por parte de organismos públicos y derivados y, en particular, teniendo en cuenta la especial vulnerabilidad de las niñas, niños y adolescentes, quienes demandan de garantías adecuadas y suficientes de protección frente a usos indebidos o arbitrarios de su información personal, preservando de esta manera su interés superior, el libre desarrollo de su personalidad, su seguridad y otros valores que son objeto de máxima protección por parte de los Estados Iberoamericanos.” (Red Iberoamericana de Protección de Datos Personales, 2017).

Se resalta cuatros aspectos que hacen referencia al tratamiento de la privacidad y los datos personales de los niños, con el fin de que los Estados adecuen su regulación en aras de garantizar su efectiva protección.

Tabla 19

Estándares Iberoamericanos para el tratamiento de datos personales de NNA

Aspecto	Estándar
Interés superior de los NNA	"El privilegio por la protección del interés superior de los NNA, conforme a la Convención sobre los Derechos del Niño y demás instrumentos internacionales que busquen su bienestar y protección integral."
Formación académica de los NNA	"La promoción en la formación académica de los NNA, el uso responsable, adecuado y seguro de las tecnologías de la información y comunicación y los eventuales riesgos a los que se enfrentan en ambientes digitales respecto del tratamiento indebido de sus datos personales, así como el respeto de sus derechos y libertades"
Legalidad en la obtención del consentimiento	"El responsable obtendrá la autorización del titular de la patria potestad o tutela, conforme a lo dispuesto en las reglas de representación previstas en el derecho interno de los Estados Iberoamericanos, o en su caso, solicitará directamente la autorización del menor de edad si el derecho interno de cada Estado Iberoamericano ha establecido una edad mínima para que lo pueda otorgar directamente y sin representación alguna del titular de la patria potestad o tutela. (Capítulo I)."
Principio de transparencia	"Reconocimiento especial del principio de transparencia en cuanto a la información proporcionada dada a los NNA como titulares de la información debe ser suficiente y fácilmente accesible, así como redactarse y estructurarse en un lenguaje claro, sencillo y de fácil comprensión para los titulares a quienes va dirigida, especialmente si se trata de niñas, niños y adolescentes." (Capítulo II).

Fuente: Creación propia basada en los estándares iberoamericanos de PDP

La razón de ser de los estándares aprobados es contribuir a la regulación guiada de las tendencias innovadoras en la materia, con niveles adecuados de protección de la información personal, que garantice el ejercicio efectivo de los derechos y propicie condiciones de competitividad y desarrollo económico de los países, facilitando marcos conceptuales, marcos de aplicación y directrices con el fin de adecuar el tratamiento jurídico de datos de los menores, en torno al interés superior, la formación académica, la legalidad del consentimiento y el principio de transparencia. A nivel internacional de manera conjunta, se proyecta elaborar una propuesta de estándares universal sobre protección de datos y privacidad de las autoridades de protección de datos con el propósito de invitar a los Estados, a buscar alianzas para proteger los derechos

fundamentales basado en el enfoque de garantía de los derechos humanos en todos los Estados producto de las recomendaciones de la APEC, la OCDE y encuentros internacionales.

Como lo refiere Remolina, los instrumentos normativos y estandarizados a nivel internacional responden a los intereses locales de regulación y gestión de cada país, y es así como, se evidencia que en la mayoría de los Estados no existe una regulación sectorial para el tratamiento de la información personal de los niños en la era digital. En materia de la legalidad del consentimiento y el principio de la transparencia hace falta mayor claridad sobre su concepto e implementación en el ambiente digital y empresarial. La teoría de protección de los derechos humanos es reconocida por todas las organizaciones interesadas en el tema, sin embargo, la visión global de los Estados es la de facilitar el bienestar económico y social de acuerdo con los postulados APEC y OCDE. (2018).

Capítulo III: Tratamiento Jurídico de Datos Personales de los Niños en Colombia y su Adecuación a los Estándares De Protección

En la actualidad, es acertado afirmar que el patrimonio de la humanidad se encuentra en la sociedad del conocimiento en donde el epicentro de la creación de nueva información se ha multiplicado en los últimos años, por lo que para Larrinaga esto implica que a mayor información circulando por el mundo globalizado en que se hallan inmersos los ciudadanos digitales, se deben proteger velozmente los datos personales. (2002).

Colombia, es un país que se encuentra en proceso de consolidación de instrumentos normativos para un adecuado tratamiento de la información de las personas. En este capítulo se realiza el análisis el marco constitucional y legal del derecho a la protección de datos personales, el alcance jurisprudencial, la relación con otros derechos, principios, estructura legal del tratamiento, el interés superior del niño frente a las tecnologías, los retos de protección relacionados con el consentimiento, la autorregulación, responsabilidad de los operadores del tratamiento y los mecanismos de vigilancia para comprender los retos y desafíos en materia de protección de la información personal de NNA.

La Ley Estatutaria de Protección de Datos Personales 1581 de 2012 resulta de vital importancia en el escenario del derecho de las nuevas tecnologías y paradigmas relacionados con la instrumentación y materialización de la protección del derecho a la privacidad en diversidad de sistemas de información de carácter general tanto en entidades de carácter público como de carácter privado y recoge las iniciativas frente a la responsabilidad de los operadores del

tratamiento de información en el uso que se haga de ella por intereses de tipo económico, político o social en una órbita que se caracteriza por la ciber-evolución.

3.1. Naturaleza constitucional del derecho a privacidad de datos personales de los niños

Los primeros cimientos normativos del derecho a la protección de datos personales en Colombia se fundamentan desde el siglo XIX (1810 y 1886) con el reconocimiento jurídico del derecho a la vida privada, intimidad personal y familiar y al buen nombre conforme a su regulación relacionada con la primera manifestación doctrinal del derecho a la intimidad como el de nos ser molestado en su persona y propiedad como se observa en las siguientes constituciones de 1810 y 1886:

Tabla 20.

Postulado normativo del derecho a la vida privada en Colombia antes de 1991

Normativa	Disposición
Constitución Del Estado Libre e Independiente del Socorro, de 1810 (15 agosto)	**Derecho a la vida privada personal y en relación con la propiedad** "Nadie será molestado en su persona o en su propiedad sino por la ley" (Artículo 2)
Constitución Política de Colombia de 1886	**Derecho a la vida privada personal, familiar y en su domicilio** "Nadie podrá ser molestado en su persona o familia, ni reducido a prisión o arresto, ni detenido, ni su domicilio registrado, sino a virtud de mandamiento escrito de autoridad competente, con las formalidades legales y por motivo previamente definido en las leyes". (Artículo 23) **Derecho a la vida privada con relación a la correspondencia** "La correspondencia confiada a los telégrafos y correos es inviolable. Las cartas y papeles privados no podrán ser interceptados ni registrados, sino por la autoridad, mediante orden de funcionario competente, en los casos y con las formalidades que establezca la ley y con el único objeto de buscar pruebas judiciales". (Artículo 43)

Fuente: Creación propia basada en la normatividad de Colombia.

Se establece el reconocimiento jurídico del derecho a no ser molestada la persona en su individualidad, así como en su relación con la propiedad, como una forma de proclama de libertad que se traduce con más amplitud en el Estado de derecho como el derecho a la vida privada personal, familiar, protección a su domicilio y correspondencia, en un escenario centralista de intervención y protección del Estado por autoridad de la ley.

Ahora bien, en su trayectoria normativa el reconocimiento del derecho a la intimidad del niño, se incorpora al ordenamiento jurídico colombiano, los postulados internacionales de protección a la vida privada en el marco de la dignidad humana, antes de 1991 en su orden:

Tabla 21.

Primeros instrumentos de protección de los derechos del niño y el derecho a la vida privada antes de la Constitución Política de 1991

Norma	Disposición
Ley 74 de 1968 Aprobó el Pacto de los Derechos Civiles y Políticos, adoptado por la Asamblea General en 1966 (16 de diciembre)	**En general** "Nadie será objeto de injerencias arbitrarias e ilegales en su **vida privada**, su familia, su domicilio o su correspondencia ni de ataques ilegales a su honra y reputación. (…)". (artículo 17 Pacto de derechos civiles y políticos) **Reconoce los derechos y mecanismos de protección de los niños** "Adopción de medidas especiales de protección y asistencia a favor de todos los niños y adolescentes sin discriminación alguno por razón de filiación o cualquier otra condición. Debe protegerse a los niños y adolescentes contra la explotación económica, social o cualquier forma de trabajo". (artículo 10) Reconocimiento del derecho a la igualdad, identidad y nacionalidad así como medidas de protección del niño, tanto por parte de su familia como de la sociedad y del Estado. (artículo 24 Pacto de Derechos Civiles y Políticos)
Ley 16 de 1972 Aprobó la Convención Americana sobre los derechos humanos (Pacto San José de Costa Rica - 1969)	**Protección de la Honra y de la Dignidad en general** **1.** "Toda persona tiene derecho al respecto de su honra y al reconocimiento de su dignidad **2.** Nadie puede ser objeto de injerencias arbitrarias en **su vida privada**, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación. **3.** Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques" (artículo 11)

Norma	Disposición
Decreto 2737 de 1989 (noviembre 27) Se expide el Código del Menor	**Derechos del niño** "Todo niño tiene derecho a las medidas de protección que su condición de menor requiere por parte de su familia, de la sociedad y el Estado". (artículo 19) **Reconoce expresamente los convenios y tratados internacionales** Manifiesta que los mismos servirán de guía de interpretación y aplicación (Artículo 9) Así mismo hace referencia a que en cualquier actuación de las autoridades relacionadas con menores sobre cualquier otra consideración se tendrá en cuenta el interés superior del menor. (Artículo 20) **En cuanto a la vida privada del menor:** "Los medios de comunicación social respetarán el ámbito personal del menor, y por lo tanto, no podrán efectuar publicaciones, entrevistas o informes que constituyan injerencia arbitraria en la **vida privada**, la familia, el domicilio, las relaciones o las circunstancias personales del menor, ni podrán afectar su honra o reputación. "A los medios masivos de comunicación les está prohibida la difusión de cualquier programa o mensaje que atente contra la moral o la salud física o mental de los menores." (Artículo 25) **En cuanto a los datos del menor:** "La sentencia que decrete la adopción producirá todos los derechos y obligaciones propios de la relación paterno-filial y **deberá contener los datos necesarios** para que su inscripción en el registro civil constituya al acta de nacimiento y reemplace la de origen, la cual se anulará. En la sentencia se omitirá el nombre de los padres de sangre si fueren conocidos…" (Artículo 112) "En la transmisión o publicación de los hechos delictivos en los que aparezca involucrado un menor como autor, partícipe o testigo de los mismos, no se le podrá entrevistar, ni dar su nombre, **ni divulgar datos que lo identifiquen o puedan conducir a su identificación** …" (Artículo 301)

Fuente: Creación propia basada en la normatividad de Colombia.

La regulación internacional sobre la protección de los derechos del niño, constituye el faro para adoptar medidas especiales de salvaguarda del menor por parte de su familia, la sociedad y el Estado Colombiano contra la explotación económica, social o cualquier forma de trabajo y se

reconocen algunos instrumentos internacionales que sirvieron de inspiración a la estructuración del Código del Menor de 1989 con el objeto de establecer un marco de protección específico del menor, en cuanto, a derechos fundamentales, principios rectores, armonización de los convenios y tratados internacionales relativos al tema, medidas de protección, competencia y procedimientos. Y así mismo, se identifica el interés superior del menor y el derecho a la vida privada dentro de un contexto relacionado con los medios de comunicación social por primera vez se refiere al principio de necesidad de los datos del menor en el ámbito de la adopción frente a la publicidad de las decisiones judiciales.

Con el fin de ratificar el reconocimiento jurídico de los derechos del niño, Colombia expide la Ley 12 de 1991," por medio de la cual se aprueba la Convención sobre los Derechos del Niño, adoptada por la Asamblea General de las Naciones Unidas el 20 de noviembre de 1989" y que permite inspirar la construcción de instrumentos jurídicos de protección en todos los ámbitos relacionados con la vida de los NNA:

Tabla 22.

Normativa de reconocimiento de la Convención de los Derechos del Niño y su derecho a la vida privada en Colombia

Norma	Disposición
Ley 12 de 1991 (22 de enero) Aprueba la Declaración de los Derechos del Niño - DDA Adoptada por la Asamblea de la ONU 1989. (20 de noviembre)	**Armoniza el principio que establece el interés superior del menor** Fundado en sus derechos prevalentes (Artículo 3). Interés superior del menor desde una perspectiva humanista de protección especial para quien se encuentra en condiciones de indefensión o desde una perspectiva "ética que sostiene que sólo una adecuada protección del menor garantiza la formación de un adulto sano, libre y autónomo" (Carta de las Naciones Unidas, artículo 55). **En cuanto a la vida privada del niño**

Norma	Disposición
	"1. Ningún niño será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia ni de ataques ilegales a su honra y a su reputación. 2. El niño tiene derecho a la protección de la ley contra esas injerencias o ataques." (Artículo 16) **En el procedimiento penal donde esté involucrado un niño** vii) "Que se respetará plenamente su vida privada en todas las fases del procedimiento" (Artículo 40)

Fuente: Creación propia basada en la normativa nacional

Esta regulación, incorpora postulados de la Declaración de Ginebra de 1924 "sobre los Derechos del Niño, la Declaración de los Derechos del Niño adoptada por la Asamblea General el 20 de noviembre de 1959, y reconocida en la Declaración Universal de Derechos Humanos, en el Pacto Internacional de Derechos Civiles y Políticos, en el Pacto Internacional de Derechos Económicos, Sociales y Culturales", en los cuales se resalta la importancia de la familia en el sistema social, la formación integral de los niños, la salvaguarda de sus derechos y sus deberes como miembro de una comunidad que amerita la protección de su derecho a la vida privada desde una perspectiva humanista en los diferentes ámbitos.

Ahora bien, desde 1948 a 1969, como se analizó en el capítulo primero, a nivel internacional se da respuesta a la pregunta ¿en que consiste el derecho a la intimidad? Bajo el enfoque de la figura de la persona y a su protección de vida privada, familiar, domicilio o correspondencia contra cualquier arbitrariedad que la afecte e incluso a su honra como lo establece la Declaración Universal de los Derechos Humanos (DUDH, 1948, art. 12) que a su vez, fue ratificada por el Pacto Internacional de Derecho Civiles y Políticos (ONU, Resolución 2200 A (XXI), 1966) y la Convención Americana de Derechos Humanos (CADH, 1969, art. 11).

Para el caso colombiano y en el marco del Estado social de derecho se establece el derecho a la intimidad en concordancia con el derecho a la protección de datos personales en el artículo 15 de la Constitución de Política de 1991como se lee a continuación:

> "Todas las personas tienen *derecho a su intimidad personal y familiar* y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tiene derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos de entidades públicas y privadas [...] (Cursivas propias) (Const.1991, artículo 15 y 20),

Normativa que acoge el postulado internacional de proteger la vida privada de las personas en dimensiones individuales y familiares de libertad que fueron fundamentando la protección de datos personales; partiendo de la figura de derecho al habeas data, el cual surge como un instrumento garantista del derecho a proteger la información personal en un ámbito sectorial del derecho a la intimidad y buen nombre, como lo refiere López Medina cuando presenta una línea de interpretación de la sentencia T-414 de 1992:

> "..los deudores están protegidos, no solamente por la garantía de intimidad, la cual impide la formación de "perfiles virtuales" que los excluyan de las redes financieras, sino que incluso "el ciudadano no puede ser privado *de su derecho de acceso al crédito sin justa causa y observando la garantía del debido proceso*". (2009, p. 186)

Radio de protección constitucional que fue ampliando el giro de la privacidad y autodeterminación de la información en otros ámbitos de protección tales como: el penal, el tecnológico, la economía digital, Egoverment, marketing, internet de las cosas entre otros ambitos privados a un nivel general y público respecto al procesamiento de los datos personales como se observa en las siguientes normativas que se fundamentan en la Declaracion de los Derechos Humanos, y que tiene por objeto desarrollar dos dimensiones relacionadas con la

autodeterminación informativa que involucra: el derecho constitucional de la privacidad y el derecho a la información a que se refiere los artículos 15 y 20 de la Constitución Política de Colombia de 1991.

Tabla 23.

Protección constitucional de la intimidad e información personal de los NNA

Norma	Disposición
Constitución Política de Colombia 1991 (7 de Julio)	**Derecho a la intimidad, buen nombre y protección de datos personales** Por primera vez incorpora la recolección, tratamiento y circulación de datos como derecho fundamental de todos los ciudadanos en Colombia de acuerdo a las exigencias de la sociedad de la información: (artículo 15 y 20): "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. *De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.* *En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.* : (Const, artículo 15): Y "*Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial y la de fundar medios masivos de comunicación. Estos son libres y tienen la responsabilidad social*. Se garantiza el derecho a la rectificación en condiciones de equidad. No habrá censura" (Const. artículo 20): **Derechos fundamentales de los niños** *Reconoce los derechos fundamentales de los NNA, su protección integral, la co-responsabilidad de la familia sociedad y Estado, así como el principio de prevalencia de sus derechos*. Reconoce "los demás derechos consagrados en la Constitución, en las leyes y en los tratados internacionales ratificados por Colombia." (Const. artículo 44) **Protección y formación integral del adolescente por parte del Estado**

Establece la responsabilidad del Estado y los particulares de garantizar el *derecho a la educación, a la protección y a la formación integral de la juventud* (Const. artículo 45)
Derecho a la libertad de iniciativa privada Tiene una responsabilidad social: "*La actividad económica y la iniciativa privada son libres, dentro de los límites del bien común." (*Const. artículo 333)

Fuente: Creación basada en la norma constitucional, (1991) cursiva propia)

La dogmática jurídica del artículo 15 y 20 de la Constitución política se concibe como primera aproximación teórica a la protección de datos personales con la acción del habeas data, el cual es concebido en el ordenamiento jurídico como un derecho fundamental, que en razón a su naturaleza se desprenden diversas posturas:

En primer lugar, se conoce común derecho fundamental que permite conocer, actualizar y rectificar informaciones almacenadas sobre las personas en bancos de datos y en archivos de entidades públicas y privadas.

En segundo lugar, el habeas data más que un derecho fundamental sustantivo, es un instrumento, mecanismo o garantía esencial para afianzar la protección efectiva de otros derechos fundamentales como la intimidad, buen nombre entre otros.

Y en tercer lugar una interpretación de habeas data como un derecho autónomo y técnico (1995), compuesto por: la autodeterminación informática y la libertad individual y la libertad económica, cuyo desarrollo, control y vigilancia se da en el marco del derecho público y privado, mediante políticas de protección de datos efectivas.

En este sentido, la finalidad jurídica de la protección de los datos personales se fundamenta en redimir el derecho fundamental a la privacidad y protección de la información en una dimensión tecnológica así como los procedimientos y recursos para su tutela jurídica que tienen todas las

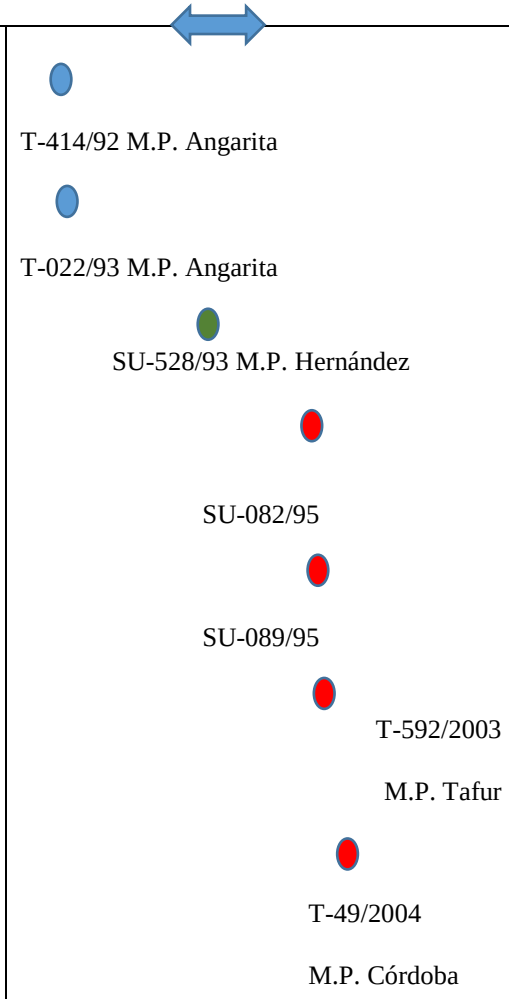
personas respecto a los verbos rectores de*: "conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales" y de expresar y difundir su pensamiento, la de informar y recibir información veraz"* (Const. 1991, artículo 15) (cursiva propia), que involucra el derecho fundamental al hábeas data como una garantía del derecho a la vida privada.

Es decir, desde 1992, la Corte Constitucional ha ilustrado las tendencias de la interpretación dada a la protección de la privacidad de la información personal contenida en bases de datos y el alcance que ha tenido el derecho en el sistema jurídico colombiano de acuerdo con tres líneas jurisprudenciales que inicia con la identidad de protección fuerte con el derecho a la intimidad, luego con el derecho a la libertad y se consolida con un derecho autónomo de protección de la privacidad y la autodeterminación informativa contenida en la protección de datos personales.

En su momento López Medina se hace la siguiente pregunta como línea de interpretación inicial del derecho al tratamiento de la información personal en bases de datos con una visión de protección al derecho a la intimidad: "¿Bajo qué condiciones específicas puede una base de datos financieros poseer y divulgar información sobre un deudor sin violar las garantías constitucionales de intimidad y buen nombre?" (2009, p.186).

Tabla 24.

Transición Línea jurisprudencial de la Corte Constitucional: Derecho fundamental de la protección a la privacidad e información personal

Prevalencia de los intereses propios de la garantía del derecho a la intimidad		Prevalencia de los intereses a información por parte del sector financiero; el deudor es protegido no por la garantía de intimidad, sino por la construcción de "buen nombre.".

Fuente: López, 2009

Se detiene a recoger las características de la línea jurisprudencial destacando como fundadora la sentencia T-414 de 1992 que reconoce: El concepto de habeas data, entendido como el derecho que protege el tratamiento adecuado de la intimidad de las personas en escenarios individuales y familiares propios de la sociedad de la información y el correlativo derecho de exigir su protección por parte del Estado. Y frente al desarrollo tecnológico T-022 de 1993 incorpora la protección no

sólo de la intimidad sino otros escenarios como la formación de “perfiles virtuales” que se excluya al ciudadano deudor del sistema financiero; Y con la Sentencia SU-528/93 se equilibra la balanza a la protección de prescripción de las obligaciones crediticias en virtud del derecho a la información veraz y oportuna.

Se presenta la primera línea de interpretación constitucional con base en el enfoque: *“Derecho fundamental de protección a los datos personales como un derecho fuertemente relacionado al derecho fundamental a la intimidad”,* en cuanto desarrolla el proyecto de vida desde la individualidad propia del ser humano, evitando toda arbitrariedad:

> “El artículo 15 de la Constitución relativo al derecho a la intimidad, contiene una zona de reserva para la propia persona, de la que quedan excluidos los demás, a menos que la persona protegida decida voluntariamente compartir dicho ámbito. Contiene dicho artículo, entre otros, los derechos a la intimidad personal y familiar, al buen nombre, al habeas data y a la inviolabilidad de la correspondencia y demás formas de comunicación privada. Todos estos derechos están unidos por su finalidad, cuál es la de aislar a la persona de las injerencias de terceros, así como proteger su imagen”. (Corte Constitucional, Sala primera de revisión, sentencia T-412, 1992).

Así como el derecho al anonimato en los siguientes términos:

> “El derecho a la intimidad -que abarca también la inviolabilidad del domicilio, el habeas data, la inviolabilidad de la correspondencia y la reserva de los libros de contabilidad y demás documentos particulares-, se encamina a proteger la vida privada del individuo y la de su familia, de todas aquellas perturbaciones ajenas que, de manera indebida, buscan penetrar o desvelar los sucesos personales o familiares. La divulgación de eventos relativos a las personas, con propósitos comerciales o particulares, cuando debían permanecer en el anonimato, siendo

tan sólo cuestionables por las vías jurídicas que previamente se han establecido, contraría en consecuencia el especial deber de respeto que debe mantenerse sobre estos acontecimientos, a fin de garantizar el ejercicio indiscriminado del derecho fundamental". (Corte Constitucional, Sala primera de revisión, sentencia T-340, 1993).

Al igual establece el concepto de habeas data, entendido como el derecho que protege el tratamiento adecuado de la intimidad de las personas en escenarios individuales y familiares propios de la sociedad de la información y el correlativo derecho de exigir su protección por parte del Estado.

Como segunda línea de interpretación constitucional se destaca el: *"Derecho fundamental de protección a los datos personales como un derecho fuertemente relacionado al derecho fundamental a la libertad."*

La Corte invita a mantener el equilibro entre el derecho a la intimidad (art. 15 CP.) y el derecho a la información (art. 20 C.P.), aunque cuando estos derechos fundamentales entren en conflicto, será la intimidad y la protección de los datos personales los que prevalecen para la aplicación del operador jurídico por cuanto: "Caracteriza a la intimidad como un derecho de carácter general, absoluto, extrapatrimonial, inalienable e imprescriptible y que se pueda hacer valer "erga omnes", tanto frente al Estado como a los particulares". (Corte Constitucional, Sala primera de revisión, sentencia T-414, 1992).

Se reconoce el derecho a la intimidad como una de las manifestaciones más directas de la dignidad humana como el valor primordial del Estado Social de Derecho, y ante la falta de equilibrio o coexistencia, la intimidad deberá prevalecer frente el aseguramiento de la paz.

De igual manera presenta un concepto de dato personal en los siguientes términos:

> “El dato es un elemento material susceptible de ser convertido en información cuando se inserta en un modelo que lo relaciona con otros datos y hace posible que dicho dato adquiera sentido. El dato que constituye un elemento de la identidad de la persona, que en conjunto con otros datos sirve para identificarla a ella y solo a ella, y por lo tanto sería susceptible de usarse para coartarla, es de su propiedad, en el sentido de que tendría ciertos derechos sobre su uso.
>
> Consiste la libertad informática en la facultad de disponer de la información, de preservar la propia identidad informática, es decir, de permitir, controlar o rectificar los datos concernientes a la personalidad del titular de los mismos y que, como tales, lo identifican e individualizan ante los demás”. (Corte Constitucional, Sala primera de revisión, sentencia T-414, 1992).

Y otro concepto de intimidad: “El derecho a la intimidad comprende una temática amplia que cobija muchos aspectos de la vida pública y privada de las personas, entendiendo ésta última como aquel espacio personalísimo que por su naturaleza no le atañe a terceros. La realización personal y el libre desarrollo de la personalidad exigen de parte de los particulares y del Estado, el reconocimiento y el respeto de las conductas que la persona realiza, para vivir de manera sana y equilibrada, física y emocionalmente.” (Corte Constitucional, Sala primera de revisión, sentencia

Así mismo, la Corte Constitucional por medio de sus pronunciamientos estableció el concepto de la autodeterminación informativa como: “… la facultad de la persona a la cual se refieren los datos, para autorizar su conservación, uso y circulación, de conformidad con las regulaciones legales."(Corte Constitucional, Sala Plena, sentencia SU-082, 1995).

Y como tercera línea de interpretación constitucional se enfoca *‘‘el derecho fundamental de protección a los datos personales como un derecho autónomo e independiente*.”que surge y prevalece desde 1995; a partir de múltiples pronunciamientos del alto tribunal en los que establece:

> “En relación con el derecho a la información y la legitimidad de la conducta de las entidades que solicitan información de sus eventuales clientes, a las centrales de información que para el efecto se han creado, así como la facultad de reportar a quienes incumplan las obligaciones con ellos contraídas, tiene como base fundamental y punto de equilibrio, la autorización que el interesado les otorgue para disponer de esa información, pues al fin y al cabo, los datos que se van a suministrar conciernen a él, y por tanto, le asiste el derecho, no sólo a autorizar su circulación, sino a rectificarlos o actualizarlos, cuando a ello hubiere lugar. Autorización que debe ser expresa y voluntaria por parte del interesado, para que sea realmente eficaz, pues de lo contrario no podría hablarse de que el titular de la información hizo uso efectivo de su derecho”. (Corte Constitucional, Sala Plena, sentencia SU-082, 1995).

Es decir desarrolla el tratamiento de datos personales en un dimensión plurifacétia que requiere del determinismo y autoreferenciación de los derechos del titular de la información personal. Así mismo, la gestión de los datos personales:

> “El ámbito de acción o de operatividad del derecho al habeas data o derecho a la autodeterminación informática, está dado por el entorno en el cual se desarrollan los procesos de administración de bases de datos personales. De tal forma que integran el contexto material: el objeto o la actividad de las entidades administradoras de bases de datos, las regulaciones internas, los mecanismos técnicos para la recopilación, procesamiento, almacenamiento, seguridad y divulgación de los datos personales y la reglamentación sobre usuarios de los servicios de las administradoras de las bases de datos”. (Corte Constitucional, Sala Plena, sentencia T-729, 2002).

Identifica las características del derecho autónomo: El objeto de protección del derecho fundamental al hábeas data es el dato personal que tiene como características:

"i) estar referido a aspectos exclusivos y propios de una persona natural, ii) permitir identificar a la persona, en mayor o menor medida, gracias a la visión de conjunto que se logre con el mismo y con otros datos; iii) su propiedad reside exclusivamente en el titular del mismo, situación que no se altera por su obtención por parte de un tercero de manera lícita o ilícita, y iv) su tratamiento está sometido a reglas especiales (principios) en lo relativo a su captación, administración y divulgación". (Corte Constitucional, Sala Plena, sentencia C-1011, 2008).

Identifica el núcleo del derecho al tratamiento de datos personales y su autonomía en los siguientes términos:

> "El núcleo del derecho al habeas data compuesto por la autodeterminación informática y la libertad incluida la libertad económica. Este derecho como fundamental autónomo, requiere para su efectiva protección de mecanismos que lo garanticen, los cuales no sólo deben pender de los jueces, sino de una institucionalidad administrativa que además del control y vigilancia tanto para los sujetos de derecho público como privado, aseguren la observancia efectiva de la protección de datos y, en razón de su carácter técnico, tenga la capacidad de fijar política pública en la materia, sin injerencias políticas para el cumplimiento de esas decisiones." (Corte Constitucional, Sala Plena, sentencia C-748, 2011)

Finalmente es importante resaltar los aspectos que requieren ser regulados en consideración de la Corte Constitucional:

"Dentro de las prerrogativas o contenidos mínimos que se desprenden del derecho al habeas data encontramos por lo menos las siguientes: (i) el derecho de las personas a conocer –acceso- la información que sobre ellas están recogidas en bases de datos, lo que conlleva el acceso a las bases de datos donde se encuentra dicha información; (ii) el derecho a incluir nuevos datos con el fin de que se provea una imagen completa del titular; (iii) el derecho a actualizar la

información, es decir, a poner al día el contenido de dichas bases de datos; (iv) el derecho a que la información contenida en bases de datos sea rectificada o corregida, de tal manera que concuerde con la realidad; (v) el derecho a excluir información de una base de datos, bien porque se está haciendo un uso indebido de ella, o por simple voluntad del titular –salvo las excepciones previstas en la normativa" Corte Constitucional, Sala Plena, sentencia T-058. 2013).

El surgimiento de la autonomía del derecho a la protección de datos personales se da gracias a los precedentes jurisprudenciales que perfilan su importancia en el ordenamiento jurídico de acuerdo con la Corte:

"Para la Corte, el habeas data es un derecho de doble naturaleza. Por una parte, goza del reconocimiento constitucional de derecho autónomo, consagrado en el artículo 15 de la Constitución y, por otra, ha sido considerado como una garantía de otros derechos. Como derecho autónomo, tiene el habeas data un objeto protegido concreto: el poder de control que el titular de la información puede ejercer sobre quién (y cómo) administra la información que le concierne y el poder de su titular de conocer, actualizar, rectificar, autorizar, incluir y excluir información personal cuando ésta sea objeto de administración en una base de datos". (Corte Constitucional, Sala Plena, Sentencia T-058, 2013).

Sin lugar a dudas la línea jurisprudencial del derecho a la protección de datos personales muestra la importancia de la libertad y la igualdad para el ejercicio eficaz del derecho desde la naturaleza y razón de ser de su existencia, enfoque que lo hace dependiente; sin embargo, desde el análisis de su autonomía se fundamenta en su contenido que se caracteriza por su carácter único y diferencial frente a los demás derechos.

La línea jurisprudencial del derecho a la protección de datos personales en la era tecnológica, concluye que es un derecho autónomo e independiente para el modelo de Estado Social de Derecho Colombiano, democrático y pluralista, por cuanto la tendencia de su tratamiento jurídico es la reducir la arbitrariedad, los riegos y aumentar la discrecionalidad y seguridad argumentada desde la juridicidad.

La teoría general del derecho a la protección de datos personales permite identificar cuáles son sus "escenarios constitucionales" como ya lo había referido López Medina (2009), en el análisis de los escenarios constitucionales respecto al derecho a la intimidad, y las líneas jurisprudenciales denominada "autónomas" en el cual presenta los contextos de su tratamiento para la época como se lee en los siguientes términos:

> "(i)contextos donde la información que afecta al particular ha sido divulgada por medios de prensa", (ii) contextos donde la información que afecte al particular tiene contenido crediticio y ha sido divulgada mediante informes provenientes de bancos de datos; (iii) contextos donde se discute la posibilidad de que el Estado intercepte comunicaciones por dentro de marcos institucionales específicos (a través de organismos de seguridad o dentro de cárceles), suspendiendo por tanto las garantías de intimidad e inviolabilidad de comunicaciones; y (iv) si se trata de algunos casos en que se ha presentado conflicto entorno a la reserva que cobija a las historias médicas."[43] (2009 p. 149).

[43] Ver Sentencias T-161/93, T-413/93, C-411/93, T158/94, T650/99 y T-1563/2000

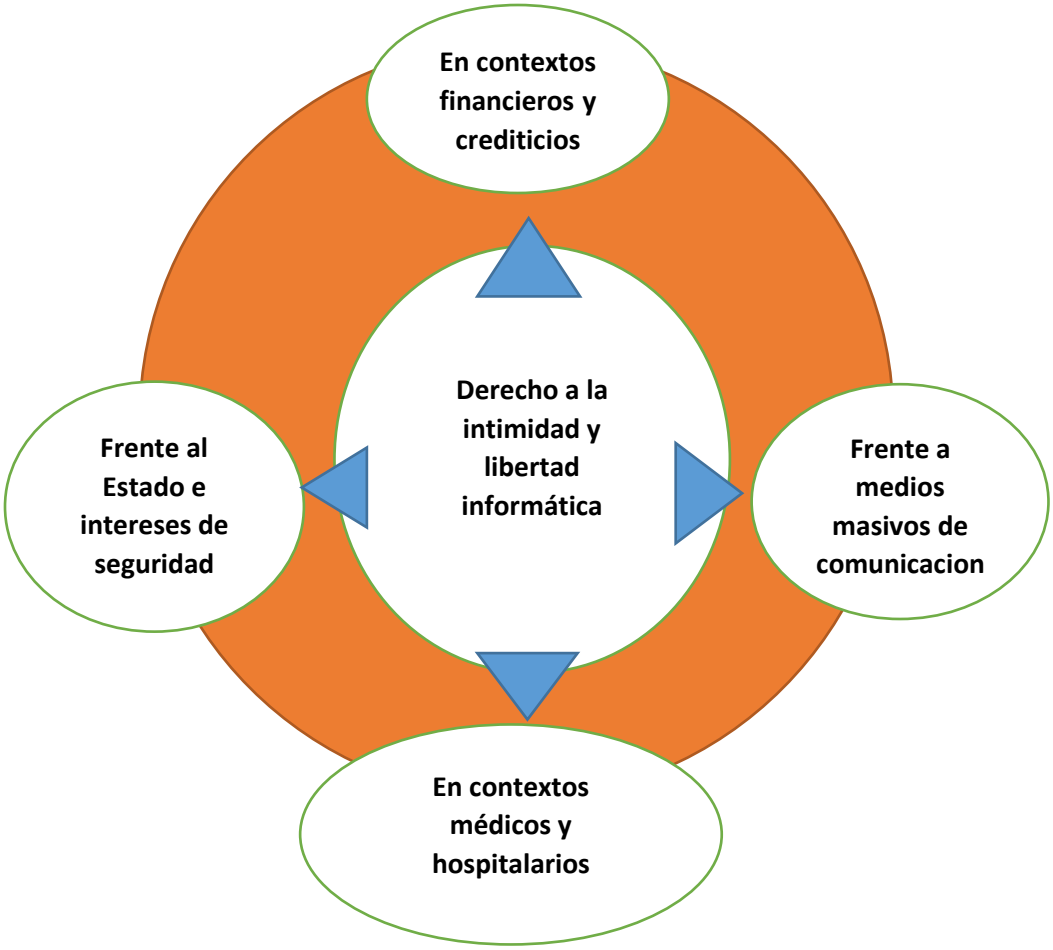


Figura 18. Escenarios constitucionales del derecho a la intimidad
Fuente: López (2009 p. 150)

Ahora bien, frente a estos diferentes escenarios constitucionales del derecho a la intimidad y la libertad informática se incorpora la autonomía de un derecho cuyo interés es proteger la privacidad y la autodeterminación informativa con el desarrollo dogmático del derecho a la protección de datos personales de carácter general que se encuentra consagrado en la Ley Estatutaria 1581 de 2012, tanto en el ámbito público como privado, y cuyo estudio se encuentra en la sentencia C-784 de 2011, que permitió fundamentar la declaratoria de constitucionalidad del proyecto de Ley Estatutaria de protección de datos personales en Colombia.

En el marco de la sociedad de la información y de cara a las nuevas tecnologías de la información y las comunicaciones de manera particular la protección integral de los derechos de los niños se logra materializar en el marco jurídico constitucional y legal; en su orden constatando un avance legislativo significativo de protección del derecho fundamental a la intimidad y del derecho a la información, así como la prevalencia de los derechos de los NNA con ocasión de los cambios sociales, económico y el desarrollo tecnológico que trasciende y sustenta el origen de la protección de datos personales como un derecho de carácter autónomo de la sociedad de la transparencia del siglo XXI y la salvaguarda de los derechos del niño, con la Constitución Política de 1991.

Y teniendo en cuenta la efectiva protección de los datos privados de los niños: "*como una esfera individual impenetrable en la que cada cual puede realizar su proyecto de vida y en la que ni el Estado ni otros particulares pueden interferir*." (Corte Constitucional, Sala Plena, sentencia C-748, 2011). (Cursiva fuera de texto)

Figura 19. Escenarios constitucionales del derecho a la privacidad y protección de datos personales de los niños, niñas y adolescentes:
Fuente: Creación con base en la sentencia C-748 (2011)

En cuanto a la interpretación constitucional del tratamiento de los datos personales de los niños se enfoca en postulados tales como:

1. Los niños por su naturaleza son sujetos de especial protección constitucional.
2. La capacidad limitada para otorgar su consentimiento, aunque se exija la autorización de los padres o tutores.
3. Y la utilización de los sistemas de información digital de acuerdo a su autodeterminación informativa sin límites.

Dicha regulación se inspira en una alto porcentaje en el modelo europeo de protección de datos personales así como en el modelo de la Privacy Act, según lo analiza la Corte Constitucional y el abordaje normativo que se describe en el constructo legal, jurisprudencial y doctrinal a la luz de las directrices y estándares internacionales de protección de datos personales que han incidido en la mayoría del ordenamiento jurídico de los Estados latinoamericanos, como es el caso colombiano. (Corte Constitucional, Sala Plena, Sentencia C-748, 2011).

3.2. Tratamiento legal de datos personales de los niños a nivel general y sectorial

El Estado Colombiano presenta el tratamiento jurídico de datos personales desde 1981 bajo un perspectiva proteccionista de la “reserva” de los datos personales con herramientas jurídicas desarrolladas a la par con los cambios y adelantos tecnológicos, en aras de garantizar el derecho a la privacidad e información personal en materia de ética médica, identificación personal,

publicidad y acceso a documentos públicos en procura de la seguridad y defensa nacional, sin embargo, no se individualizó la protección a los niños como se observa en las siguientes disposiciones legislativas:

Tabla 25.

Instrumentos legales de protección de los datos personales antes de 1991

Normativa	Disposición
Ley 23 de 18 de febrero de 1981	**Derecho a la reserva de los datos en materia de ética médica** Define la historia clínica como el registro obligatorio de las condiciones de salud del paciente. Y como documento privado queda sometido a reserva el cual puede darse a conocer a "terceros previa autorización del paciente" en las condiciones previstas por la ley (artículo 34) (comillas fuera de texto) No se especifica en el texto normativo los NNA.
Ley 57 de 5 de junio de 1985	**Límites de publicidad de los actos y documentos oficiales en materia de acceso a la información** Limita el acceso de los ciudadanos a los documentos oficiales de acuerdo con el carácter reservado conforme a la Constitución o la ley, o no hagan relación a la defensa o seguridad nacional. (Artículo 12 y 20) No se especifica en el texto normativo los NNA.
Ley 96 de 21 de noviembre de 1985 Por la cual se modifican las Leyes 28 de 1979 y 85 de 1981, el Código Contencioso Administrativo, se otorgan unas facultades extraordinarias y se dictan otras disposiciones	**Derecho a la Información de identificación personal y derecho a la reserva** "Toda persona tiene derecho a que la Registraduría le informe sobre el número, lugar y fecha de expedición de documentos de identidad pertenecientes a terceros. Tienen carácter reservado las informaciones que reposen en los archivos de la Registraduría, referentes a la identidad de las personas, cómo son sus datos biográficos, su filiación y fórmula dactiloscópica. De la información reservada sólo podrá hacerse uso por orden de autoridad competente. Con fines investigativos, los jueces y los funcionarios de policía y de seguridad tendrán acceso a los archivos de la Registraduría. Cualquier persona podrá inspeccionar en todo tiempo los censos electorales, pero en ningún caso se podrá expedir copia de los mismos." (Artículo 51)

Normativa	Disposición
No se especifica en el texto normativo los NNA.	

Fuente: Creación propia

Se evidencia los primeros inicios de la protección sectorial de los datos personales con un enfoque más de protección al derecho a la reserva y a la información que al derecho a la privacidad, reflejo de la visión centralista de la Constitución Política de 1886 y la limitada garantía de los derechos del menor.

Para dar inicio al tratamiento jurídico de la privacidad de la información de los menores de edad en particular, es importante hacer referencia al significado de un niño, niña y adolescente en el ordenamiento jurídico colombiano, pues en su desarrollo el Código de la Infancia y la Adolescencia, Ley 1098 de 2006, establece en su artículo 3º un concepto jurídico de interpretación como se lee: "(…) se entiende por niño o niña las personas entre los 0 y 12 años, y por adolescente las personas entre 12 y 18 años de edad", (Ley 1098, 2006, artículo 3), definición acorde con la noción establecida en la Convención sobre los derechos del niño: "(…) todo ser humano menor de dieciocho años de edad." (Naciones Unidas Derechos Humanos, 1989, artículo 1).

Significa que hablar de niño por su condición y capacidad y ante la protección de la privacidad de sus datos personales, su alcance debe ser considerado de manera especial y prevalente por parte de la legilación y herramientas de protección integral y no sólo incoporar su prohibición con determinadas excepciones en cuanto a la naturaleza del tratamiento de la información ya sea de niños y niñas, así como para la categoría de adolescentes sin existir claridad respecto del alcance, la responsabilidad o los límites en el uso de las TIC; no solo frente a la edad, sino respecto a la adecuación de un sistema de gestión de datos personales de niños de acuerdo a los estándares internacionales y las tendencias en el tratamiento digital, con el propósito de prevenir los innumerables riesgos (ejemplo ciberniñera: persona idónea que identifica y clasifica la categoría

de riesgo de las páginas web para niños) y salvaguardar de manera integral sus derechos fundamentales. (Corte Constitucional, Sala Plena, sentencia C-748, 2011).

En cuanto a las leyes de protección de datos personales, han sido estructuradas de acuerdo al progresivo desarrollo de la ciencia, la tecnología y la innovación en diferentes sectores del ámbito público y privado propio de la gobernanza digital, como se muestra en el siguiente esquema:

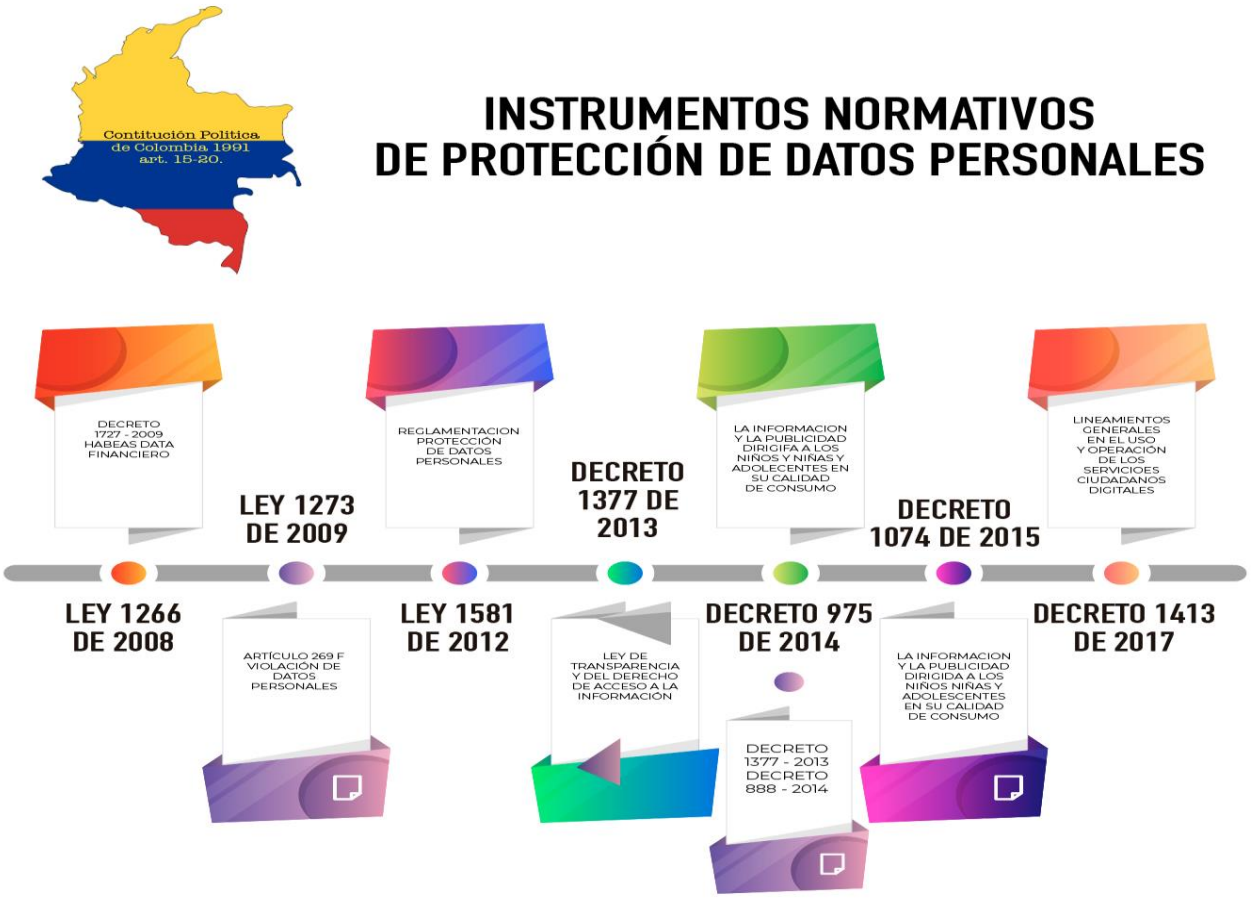


Figura 20. Regulación de la protección de datos personales en Colombia.
Fuente: Creación propia (2017) basada en la regulación de PDP 1991-2017

El régimen de tratamiento de datos personales en Colombia, inicia su regulación en el sector financiero y crediticio con la Ley 1266 de 2008 y ha venido consolidando su gestión de tratamiento

demostrable en el sector empresarial y la incursión paulatino en el ámbito penal con la Ley 1273 de 2009 en cuanto establece el bien jurídico tutelado de privacidad de la información por el delito de violación de datos personales; y así mismo, su trascendencia en el ámbito escolar, tecnológico y sector público con fundamento en la política de privacidad y transparencia de la información de los ciudadanos digitales con el Decreto 1413 de 2017.

La estructura de la Ley Estatutaria de Protección de Datos Personales 1581 de 2012, que se compone de IX Titulos, muestra el alcance del tratamiento en su orden de aplicación, conceptual, orgánico y administrativo:

"Titulo I. Objeto, ámbito de aplicación y definiciones"

"Titulo II. Principios rectores"

"Titulo III. Categorías especiales de datos"

"Titulo IV. Derechos y condiciones de legalidad para el tratamiento de datos"

"Titulo V. Procedimientos"

"Titulo VI. Deberes de los Responsables del tratamiento"

"Titulo VII. Mecanismos de vigilancia y control : Capitulo I. De la autoridad de protección de datos Capítulo II. Procedimientos y sanciones Capitulo III. Del Registro Nacional de Bases de Datos"

"Titulo VII. Transferencia de datos a terceros países"

"Titulo IX. Otras disposiciones" (Congreso de la República, LEPDP 1581, 2012) (Cursiva y negrilla fuera de texto)

La normativa abarca en la categoría de datos especiales los: *"Derechos de los niños, niñas y adolescentes. En el tratamiento se asegurará el respeto a los derechos prevalentes de los niños, niñas y adolescentes"*(Congreso de la República, LEPDP 1581, 2012 art. 7), y a su vez el

tratamiento de toda clase de datos que contenga información personal pertinente para su procesamiento por parte de entidades de orden público o privado, en cuanto, a los derechos ARCO[44] cuyo objeto corresponde al control de la calidad, volumen y uso de datos personales : "*conocer, actualizar y rectificar* las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma." (Congreso de la República, LEPDP 1581, 2012, art. 1) (Cursiva fuera de texto).

Y a su vez exceptúa de su alcance:

"a) A las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico…

"b) a las bases de datos y archivos que tengan por finalidad la seguridad y defensa nacional, así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo;

c) a las bases de datos que tengan como fin y contengan información de inteligencia y contrainteligencia;

d) a las bases de datos y archivos de información periodística y otros contenidos editoriales;

e) a las bases de datos y archivos regulados por la Ley 1266 de 2008" (Congreso de la República, LEPDP 1581, 2012, art. 2).

En tal sentido, el derecho referenciado abarca un mayor ámbito de aplicación de la privacidad en diferentes escenarios de la vida de los ciudadanos digitales, incluyendo los niños, niñas y

[44] Derechos del titular del dato, como sujeto activo de la información consultar Remolina Angarita "Los derechos de acceso, rectificación, cancelación y oposición en la Ley de datos personales y su reglamento" Protección de datos personales en México, Mexico Tirant Lo Blanch, 2013, p.p. 181-205"

adolescentes que a diario utilizan los servicios que ofrece el ecosistema informativo y tecnológico, sin embargo, por motivos de seguridad y defensa nacional, información de inteligencia, periodística, financiera y crediticia no se establece límites en el tratamiento que involucra información de menores de edad, cuando debe ser más exigente procesamiento desde la privacidad por diseño y por defecto y veracidad en el consentimiento del titular o representante legal.

Como segundo referente conceptual es preciso identificar las siguientes definiciones que da la ley de manera expresa para entender el alcance del derecho a la protección de datos personales:

> "a) Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales;
>
> b) Base de Datos: Conjunto organizado de datos personales que sea objeto de Tratamiento;
>
> c) Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables;
>
> d) Encargado del tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento;
>
> e) Responsable del tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos;
>
> f) Titular: Persona natural cuyos datos personales sean objeto de tratamiento;
>
> g) Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión." (Congreso de la República de Colombia, LEPDP 1581, 2012, art. 3).

Los conceptos del tratamiento de datos personales, como lo refiere Remolina, responden a referentes teóricos locales e internacionales “gaseosos” que dificultan su interpretación acertada de los casos de vulneración de los derechos (2018, p. 51).

Sin embargo, facilita un acercamiento conceptual que se va perfeccionando como el caso de: Un dato personal es toda información que identifica o permite identificar a una persona física. Las imágenes se enmarcan dentro del concepto de dato personal y, en consecuencia, les resulta aplicable el régimen de protección de datos personales. Cuando se trate de datos personales de NNA la autorización previa para el tratamiento debe ser dada por el representante legal, contando, en lo posible, con la opinión del menor, y a su vez con su respectiva verificación en el marco de la responsabilidad demostrada.

Por lo tanto, el derecho al tratamiento de datos personales consiste en la “facultad que tenemos todos los ciudadanos de conocer, actualizar, rectificar y eliminar la información que se haya recogido sobre nosotros en archivos y bases de datos. “ (Superintendencia de industria y comercio, 2018) como se evidencia en la siguiente clasificación:

*Figura 21***.** Tipos de datos personales

Fuente: Ley 1581, 2012, Artículo 5

Frente a un contexto de principios y derechos fundamentales del niño, se establece los postulados se destaca la juridificación en relación con los principios y de los derechos de los menores, como es el caso de la protección de la intimidad, el reconocimiento del interés superior del menor y el derecho a la representación la cual está implícita en todos.

Los principios que rigen el tratamiento de datos personales de manera armónica con la regulación internacional, y de acuerdo con los precedentes jurisprudenciales de la Corte Constitucional en Colombia, muestran un desarrollo significativo, aunque como se analiza hay vacíos normativos en su conceptualización:

Tabla 26.

Principios que rigen el tratamiento de datos personales en Colombia

Principios	Concepto
Legalidad	”El Tratamiento a que se refiere la presente ley es una actividad reglada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen”
Finalidad	“El Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular;”
Libertad	“El Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento;”
Veracidad o calidad	“La información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error;”
Transparencia	“En el Tratamiento debe garantizarse el derecho del Titular a obtener del Responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan;”
Acceso y circulación restringida	“El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la presente ley. Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la presente ley”
Seguridad	“La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente

Principios	Concepto
	ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;"
Confidencialidad	"… garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma."

Fuente: Creación basada en el artículo 4 de LEPDP (2012)

La Corte Constitucional al evaluar la constitucionalidad del proyecto de ley que pasaría a ser la LEPDP, determinó el alcance de interpretación de los principios en función de la garantía de los derechos fundamentales en su orden armónico y sistémico como es el habeas data:

> "Además de las obligaciones derivadas de los principios rectores del proceso de administración de bases de datos personales, existen otros que tienen su origen directo en normas constitucionales, específicamente: (i) la prohibición de discriminación por las informaciones recaudadas en las bases de datos, (ii) el principio de interpretación integral de los derechos constitucionales y (ii) la obligación de indemnizar los perjuicios causados por las posibles fallas en el proceso de administración de datos." (Corte Constitucional, Sala Plena, sentencia C-748, 2011).

Finalmente, de acuerdo con la Corte Constitucional, los siguientes principios derivan del núcleo temático de la LEPDP:

> "*Principio de la proporcionalidad del establecimiento de excepciones*: La Ley consagra materias exceptuadas, más no excluidas, del régimen general de la administración de datos, tal y como se explicó en el análisis del ámbito de aplicación de la norma. Sin embargo, tal

tratamiento especial debe estar justificado en términos de proporcionalidad y responder a los estándares internacionales de protección.

Principio de autoridad independiente: la adopción de una normatividad sólo es efectiva si se garantiza que dentro de la estructura del Estado exista un órgano encargado de garantizar el respeto de los principios anteriormente desarrollados. Esta autoridad debe garantizar imparcialidad e independencia.

Principio de exigencia de estándares de protección equivalentes para la transferencia internacional de datos: Tal y como se deduce del artículo 26 del Proyecto de Ley Estatutaria, existe una prohibición de transferencia internacional a cualquier tipo de países que no proporcionen niveles adecuados de protección de datos." (Corte Constitucional, Sala Plena, sentencia C-748, 2011) (Cursiva fuera de texto).

El alcance del régimen de privacidad y de datos personales de NNA se enmarca en las categorías especiales de datos y responde a los siguientes interrogantes que muestran el nivel de *prohibición y de tratamiento* de datos personales de los NNA (cursiva fuera de texto):

a. ¿Se permite el tratamiento de datos personales de NNA en Colombia?

En su orden la legislación colombiana reconoce el derecho a la vida privada y el derecho a la información de los niños, niñas y adolescentes en el Código de la Infancia y la Adolescencia (Ley 1098 de 2006) y la ley de protección integral de la familia (Ley 1361 de 2009) con una perspectiva más innovadora de protección integral e incluyente de todos los miembros del núcleo familiar, propia de las exigencias del siglo XXI, aunque con algunas limitaciones en el tema iusinformático, como se evidencia a continuación con el reconocimiento del derecho a la protección de datos personales como un derecho fundamental autónomo:

Tabla 27.

Instrumentos legales de protección del derecho a la privacidad y protección legal de NNA en Colombia

Normativa	Disposición
Ley 1098 de 2006 Aprobó el Código de la Infancia y la Adolescencia.	**Protección integral de NNA** Avance significativo respecto al reconocimiento de "las reglas de interpretación y aplicación, protección integral e interés superior del niño" (Artículo 6, 7 y 8) **En cuanto a la intimidad de NNA** "Los niños, las niñas y los adolescentes tienen derecho a la intimidad personal, mediante la protección contra toda injerencia arbitraria o ilegal en su vida privada, la de su familia, domicilio y correspondencia. Así mismo, serán protegidos contra toda conducta, acción o circunstancia que afecte su dignidad." (Artículo 33) **En cuanto a la información de NNA** "Sujeto a las restricciones necesarias para asegurar el respeto de sus derechos y el de los demás y para proteger la seguridad, la salud y la moral, los niños, las niñas y los adolescentes tienen derecho a buscar, recibir y difundir información e ideas a través de los distintos medios de comunicación de que dispongan." (artículo 34)
Ley 1361 de 2009 Ley de protección integral de la familia	"El Estado y la sociedad deben garantizar a la familia el ejercicio del derecho a la honra, dignidad e intimidad" (Artículo 4)
Ley 1581 de 2012 Ley de Protección de datos personales	"Derechos de los niños, niñas y adolescentes. En el Tratamiento se asegurará el respeto a *los derechos prevalentes de los niños, niñas y adolescentes.* *Queda proscrito* el tratamiento de datos personales de niños, niñas y adolescentes, salvo aquellos datos que sean de naturaleza pública. *Es tarea del Estado y las entidades educativas de todo tipo proveer información y capacitar a los representantes legales y tutores sobre los eventuales riesgos a los que se enfrentan los niños, niñas y adolescentes respecto del Tratamiento indebido de sus datos personales*, y proveer de conocimiento acerca del uso responsable y seguro por parte de niños, niñas y adolescentes de sus datos personales, su derecho a la privacidad y protección de su información personal y la de los demás. El Gobierno Nacional reglamentará la materia, dentro de los seis (6) meses siguientes a la promulgación de esta ley." (Artículo 7) (negrilla por fuera de texto)
Decreto 1377 de 2013 Por el cual se reglamenta parcialmente la Ley 1581 de 2012	*"El Tratamiento de datos personales de niños, niñas y adolescentes está prohibido***,** excepto cuando se trate de datos de naturaleza pública, de conformidad con lo establecido en el artículo 7° de la Ley 1581 de 2012 y

Normativa	Disposición
	cuando dicho Tratamiento cumpla con los siguientes parámetros y requisitos: 1. Que responda y respete el interés superior de los niños, niñas y adolescentes. 2. Que se asegure el respeto de sus derechos fundamentales. Cumplidos los anteriores requisitos, *el representante legal del niño, niña o adolescente otorgará la autorización* previo ejercicio del menor de su derecho a ser escuchado, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto. Todo responsable y encargado involucrado en *el tratamiento de los datos personales de niños, niñas y adolescentes*, deberá velar por el uso adecuado de los mismos. Para este fin deberán aplicarse los principios y obligaciones establecidos en la Ley 1581 de 2012 y el presente decreto. La familia y la sociedad deben velar porque los responsables y encargados del *tratamiento de los datos personales de los menores* de edad cumplan las obligaciones establecidas en la Ley 1581 de 2012 y el presente decreto." (Artículo 12).

Fuente: Creación propia basada en la regulación colombiana de tratamiento jurídico de la vida privada, y la protección de datos personales de NNA - 2006 a 2017. (Cursiva fuera de texto)

Se evidencia en el ordenamiento jurídico colombiano el transito del derecho a la intimidad al tratamiento de la privacidad e información personal del niño en el marco del aseguramiento y respeto de los derechos del niño y a su vez en un plano de *"prohibición"* en primera instancia y de manera general en el año 2012. Con posterioridad de acuerdo con los parámetros de la Sentencia C-748 de 2011 de la Corte Constitucional, se reglamenta mediante el Decreto 1733 de 2013, el cual incorpora requisitos, responsabilidad de los operadores del tratamiento de la información y del Estado, así como la familia y la sociedad en general de manera progresiva.

De conformidad con la Ley Estatutaria de Protección de Datos Personales 1581 de 2012 se establece por primera vez y de manera particular la prohibición y a su vez el tratamiento de los datos personales de los niños en el artículo 7, de acuerdo con los siguientes aspectos:

- La prevalencia de los derechos del niño.
- La prohibición del tratamiento de los datos personales del niño, salvo los datos de naturaleza pública.
- Corresponsabilidad en el ámbito preventivo frente a los múltiples riesgos de los NNA.

b. ¿Cuál es el alcance de la prohibición del tratamiento de datos personales de NNA?

Como primera medida la Corte Constitucional señala:

> "Que la interpretación del inciso segundo, no debe entenderse en el sentido de que existe una prohibición casi absoluta del tratamiento de los datos de los menores de 18 años, exceptuando los de naturaleza pública, pues ello, daría lugar a la negación de otros derechos superiores de esta población como el de la seguridad social en salud, interpretación ésta que no se encuentra conforme con la Constitución. De lo que se trata entonces, es de reconocer y asegurar la plena vigencia de todos los derechos fundamentales de esta población, incluido el habeas data. En este mismo sentido, debe interpretarse la expresión naturaleza pública." (Corte Constitucional, Sala Plena, sentencia C-748, 2011).

En este sentido, de acuerdo a la jurisprudencia anteriormente citada se ha de tener en cuenta que: "el tratamiento de los datos personales de los menores de 18 años, al margen de su naturaleza, pueden ser objeto de tratamiento siempre y cuando el fin que se persiga con dicho tratamiento responda al interés superior de los niños, las niñas y adolescentes y se asegure sin

excepción alguna el respeto de sus derechos prevalentes". (Corte Constitucional, Sala Plena, sentencia C-748, 2011).

Es decir, la Corte Constitucional conminó al legislador en su sentencia C -748 de 2011, en el sentido de incorporar nuevos elementos de salvaguarda de otros derechos fundamentales que podrían verse vulnerados con ocasión de la prohibición del tratamiento de los datos personales de los NNA, como, por ejemplo: el derecho a la educación, salud, integridad, libre de expresión.

Y es así que, el Decreto 1377 de 2013 recoge en su artículo 12 los postulados de la Corte Constitucional respecto a dos requisitos para el adecuado tratamiento de los datos personales de NNA de acuerdo a su condición y naturaleza del sujeto de derecho, con criterios hermenéuticos de segundo grado que fundamentan un avance normativo de cara a los principios de gestión del riesgo frente a las tendencias de la sociedad de la información, en los siguientes términos:

"1. Que responda y respete el interés superior de los niños, niñas y adolescentes.

2. Que se asegure el respeto de sus derechos fundamentales.

Cumplidos los anteriores requisitos, el representante legal del niño, niña o adolescente otorgará la autorización previo ejercicio del menor de su derecho a ser escuchado, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto.

Todo Responsable y Encargado involucrado en el Tratamiento de los datos personales de niños, niñas y adolescentes, deberá velar por el uso adecuado de los mismos. Para este fin deberán aplicarse los principios y obligaciones establecidos en la Ley 1581 de 2012 y el presente Decreto.

La familia y la sociedad deben velar porque los Responsables y Encargados del Tratamiento de los datos personales de los menores de edad cumplan las obligaciones establecidas en la Ley 1581 de 2012 y el presente decreto." (Decreto 1377, 2013 art. 12).

En conclusión, de manera excepcional es posible el tratamiento de datos personales de los NNA, cuando se cumplan los siguientes criterios:

- La finalidad del tratamiento responda al interés superior de los NNA.
- Se asegure el respeto de sus derechos fundamentales de los NNA.
- De acuerdo con la madurez del niño, niña o adolescente se tenga en cuenta su opinión.
- Se cumpla con los principios previstos en la LEPDP para el tratamiento de datos personales.

c. ¿Qué significa el principio del interés superior del niño frente a la protección de datos personales?

La Corte Constitucional reafirma la protección especial de los NNA:

> "En definitiva, (i) el principio del interés superior de los niños, las niñas y adolescentes se realiza en el estudio de cada caso en particular y tiene por fin asegurar su desarrollo integral; (ii) este principio, además, persigue la realización efectiva de los derechos fundamentales de los menores de 18 años y también resguardarlos de los riesgos prohibidos que amenacen su desarrollo armónico. Estos riesgos no se agotan en los que enuncia la ley, sino que también deben analizarse en el estudio de cada caso particular; (iii) debe propenderse por encontrar un equilibrio entre los derechos de los padres o sus representantes legales y los de los niños, las niñas y adolescentes. Sin embargo, cuando dicha armonización no sea posible, deberán prevalecer las garantías superiores de los menores de 18 años. En otras palabras, siempre que prevalezcan los derechos de los padres, es porque se ha entendido que ésta es la mejor manera de darle aplicación al principio del interés superior de los niños, las niñas y adolescentes." (Corte Constitucional, Sala Plena, sentencia C-900, 2011).

d. ¿Por qué los NNA son sujetos de especial o protección constitucional reforzada?

Los niños son sujetos de especial tratamiento jurídico dado su desarrollo físico, mental y emocional que requiere ser atendido de acuerdo a los primeros años de madurez de manera proactiva por parte de los padres, el Estado y la sociedad en general, dadas las condiciones de vulnerabilidad respecto a la falta de autonomía privada y los riesgos a los que se expone por su inexperiencia, ingenuidad y excesiva confianza.

Y con mayor énfasis se debe reglamentar la protección constitucional reforzada en la medida en que la revolución tecnológica expone a un mundo digital a seres inocentes (niños), ávidos de conocimiento e innovación donde se desconoce por parte de la industria de la web el principio de la dignidad humana y la garantía efectiva de sus derechos fundamentales.

e. ¿Cuáles ámbitos refiere la corresponsabilidad para la protección de los derechos de los NNA?

La Corte señala la responsabilidad compartida en su orden:

"En cuanto al inciso 3° del artículo 7° del proyecto debe también resaltarse que no sólo el Estado y las entidades educativas deben desarrollar acciones para evitar el uso inadecuado de los datos personales de los menores de 18 años, sino que también son responsables en el aseguramiento de dicha garantía:

(i) Los progenitores u otras personas que se encuentren a cargo de su cuidado y los educadores;

(ii) El legislador, quien debe asegurarse que, en cumplimiento de sus funciones legislativas, específicamente, en lo referente al tratamiento de los datos personales de los menores de 18 años, dicha normativa no deje de contener las medidas adecuadas de protección para garantizar su desarrollo armónico e integral, y la efectividad de sus derechos fundamentales

contenidos en la Constitución Política y en los estándares internacionales que existen sobre la materia;

(iii) El sistema judicial; específicamente los servidores públicos deben proteger los derechos derivados del uso de los datos personales de los menores de 18 años observando los estándares internacionales o documentos especializados sobre la materia;

(iv) Los medios de comunicación;

(v) Las empresas que proveen los servicios de acceso a la Internet, desarrollan las aplicaciones o las redes sociales digitales, a quienes se advierte que deben comprometerse en la defensa de los derechos fundamentales de los niños, niñas y adolescentes". (Corte Constitucional, Sala Plena, sentencia C-748, 2011).

f. ¿Frente a los datos personales de NNA de naturaleza pública es posible su tratamiento?

Finalmente, la Corte Constitucional concluye que en ciertos casos sí es posible el tratamiento de datos personales de NNA:

"Esta Sala observa que la interpretación del inciso segundo, no debe entenderse en el sentido de que existe una prohibición casi absoluta del tratamiento de los datos de los menores de 18 años, exceptuando los de naturaleza pública, pues ello, daría lugar a la negación de otros derechos superiores de esta población como el de la seguridad social en salud, interpretación ésta que no se encuentra conforme con la Constitución. De lo que se trata entonces, es de reconocer y asegurar la plena vigencia de todos los derechos fundamentales de esta población, incluido el habeas data." (Corte Constitucional, Sala Plena, sentencia C-748, 2011).

g. ¿En el ámbito preventivo que acciones se deben realizar para el adecuado tratamiento de los datos personales?

En el ámbito preventivo se establece la necesidad de implementar acciones educativas para niños, padres de familia, directivos, administrativos y comunidad en general respecto al adecuado uso de las tecnologías de la información y comunicación y tratamiento responsable de la información personal.

> "El Estado y las entidades educativas de todo tipo deben proveer información y capacitar a los representantes legales y tutores sobre los eventuales riesgos a los que se enfrentan los niños, niñas y adolescentes respecto del tratamiento indebido de sus datos personales, y proveer de conocimiento acerca del uso responsable y seguro por parte de niños, niñas y adolescentes de sus datos personales, su derecho a la privacidad y protección de su información personal y la de los demás". (Congreso de la República, LEPDP 1581, 2012, art 7).

h. ¿Cuáles son los derechos de los niños como titulares de la información personal y su correspondiente deber de los operadores de los datos personales?

Los derechos de los titulares de los datos se enmarcan en el calificativo ARCO siendo estos: Acceso, Rectificación, Cancelación y Oposición, que se encuentran en el Artículo 8° de la LEPDP enunciando que:

> "El Titular de los datos personales tendrá los siguientes derechos:
>
> a) Conocer, actualizar y rectificar sus datos personales frente a los Responsables del Tratamiento o Encargados del Tratamiento. Este derecho se podrá ejercer, entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado;
>
> b) Solicitar prueba de la autorización otorgada al Responsable del Tratamiento salvo cuando expresamente se exceptúe como requisito para el Tratamiento, de conformidad con lo previsto en el artículo 10 de la presente ley;

c) Ser informado por el Responsable del Tratamiento o el Encargado del Tratamiento, previa solicitud, respecto del uso que le ha dado a sus datos personales;

d) Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la presente ley y las demás normas que la modifiquen, adicionen o complementen;

e) Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el Responsable o Encargado han incurrido en conductas contrarias a esta ley y a la Constitución;

f) Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento."

Para hablar de deberes en Responsables y Encargados del tratamiento de datos personales se debe tener en claro la conceptualización de los mismos, los cuales están consignados en los literales d y e del artículo 3 de la LEPDP:

"d) Encargado del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento;

e) Responsable del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos;"

En su artículo 17 la LEPDP consagra los deberes de los responsables del tratamiento de datos personales de este modo:

"Los Responsables del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:

a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data;

b) Solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular;

c) Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada;

d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;

e) Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible;

f) Actualizar la información, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada;

g) Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento;

h) Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la presente ley;

i) Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular;

j) Tramitar las consultas y reclamos formulados en los términos señalados en la presente ley;

k) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y en especial, para la atención de consultas y reclamos;

l) Informar al Encargado del Tratamiento cuando determinada información se encuentra en discusión por parte del Titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo;

m) Informar a solicitud del Titular sobre el uso dado a sus datos;

n) Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.

o) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio. Revocar la autorización dada para el tratamiento de datos personales o solicitar la supresión del dato cuando en su tratamiento no se hayan respetado los principios y garantías constitucionales y legales. Esto procede cuando la Superintendencia de Industria y Comercio haya determinado que el Responsable del tratamiento o el Encargado del tratamiento ha incurrido en conductas contrarias a la Constitución o a la Ley 1581 de 2012." (Congreso de la República, LEPDP 1581, 2012).

Así, se ha de tener especial observancia en las sanciones que se dan ante la ausencia de cumplimiento de las funciones de los responsables del tratamiento de datos personales lo que se ha constituido como una *"infracción que podrá ser sancionada por la Superintendencia de Industria y Comercio, previa investigación por parte de la Delegatura de Protección de Datos Personales".*

En relación con los responsables del tratamiento de los datos personales la Corte Constitucional manifestó:

"Los responsables del tratamiento tienen mayores compromisos y deberes frente al titular del dato, pues son los llamados a garantizar en primer lugar el derecho fundamental al habeas data, así como las condiciones de seguridad para impedir cualquier tratamiento ilícito del dato. La calidad de responsable igualmente impone un haz de responsabilidades, específicamente en lo que se refiere a la seguridad y a la confidencialidad de los datos sujetos a tratamiento." (Corte Constitucional, Sala Plena, sentencia C-748, 2011)

Por su parte la LEDPDP consagra los deberes de los encargados del tratamiento de datos personales:

"Los Encargados del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:

a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data;

b) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;

c) Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de la presente ley;

d) Actualizar la información reportada por los Responsables del Tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo;

e) Tramitar las consultas y los reclamos formulados por los Titulares en los términos señalados en la presente ley;

f) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y, en especial, para la atención de consultas y reclamos por parte de los Titulares;

g) Registrar en la base de datos la leyenda reclamo en trámite en la forma en que se regula en la presente ley;

h) Insertar en la base de datos la leyenda información en discusión judicial una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal;

i) Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio;

j) Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella;

k) Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares;

l) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

Parágrafo. En el evento en que concurran las calidades de Responsable del Tratamiento y Encargado del Tratamiento en la misma persona, le será exigible el cumplimiento de los deberes previstos para cada uno." (LEPDP, 2012, artículo 18)

3.2.1. Tratamiento de datos personales de niños en el ámbito empresarial

El desarrollo normativo de la protección de los datos en el comercio electrónico, las estrategias de información y la publicidad dirigida a los NNA en su calidad de consumidores y la exigencia de la Superintendencia de Industria y Comercio a través de la Delegatura para la Protección de Datos Personales a las empresas de su ingreso en el Registro Nacional de Bases de Datos incluyendo los datos de los niños, resulta un avance paulatino de normatividades referentes al tema dentro de un contexto empresarial enfocándose en los aspectos propios de este campo.

Tabla 28.

Desarrollo normativo de la protección de los NNA en el ámbito empresarial

Norma	Disposición	NNA
Ley 527 de 18 de agosto de 1999	"Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones." (Arts. 2 y 32).	Sobresale la definición normativa del mensaje de datos como la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax.
Ley 1480 de 2011	"Por medio de la cual se expide el Estatuto del Consumidor y se dictan otras disposiciones"	Artículo 1°." Principios generales. Esta ley tiene como objetivos proteger, promover y garantizar la efectividad y el libre ejercicio de los derechos de los consumidores, así como amparar el respeto a su dignidad y a sus intereses económicos, en especial, lo referente a: La protección especial a los NNA, en su calidad de consumidores, de acuerdo con lo establecido en el Código de la Infancia y la Adolescencia." (Artículo 1) "Derecho a la información de los NNA. El Gobierno Nacional reglamentará, en el término de un año a partir de la entrada en vigencia de la presente ley, los casos, el contenido y la forma en que deba ser presentada la información que se suministre a los NNA en su calidad de consumidores, en desarrollo del derecho de información consagrado en el artículo 34 de la Ley 1098 de 2006." (Artículo 28)
Decreto 886 de 2014	"Se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos"	"Reglamentar la información mínima que debe contener el Registro Nacional de Bases de Datos, creado por la Ley 1581 de 2012, así como los términos y condiciones bajo las cuales se deben inscribir en este los Responsables del Tratamiento
Decreto 975 de 2014	"Por el cual se reglamentan los casos, el contenido y la forma en que se debe presentar la información y la publicidad dirigida a los niños, niñas y	"Estrategias de información y la publicidad dirigida a los NNA en su calidad de consumidores"

Norma	Disposición	NNA
	adolescentes en su calidad de consumidores"	
Decreto No. 1074 de 2015	"Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. La información y la publicidad dirigida a los niños, niñas y adolescentes en su calidad de consumidores" Reglamenta Parcialmente la Ley 1581 de 2012	Requisitos especiales para "el tratamiento de datos personales de NNA Ejercicio de los derechos de los titulares y legitimación para el ejercicio de los derechos del titular (Capítulo 25) Regula los casos, contenido y forma en que se deben presentar la información y la publicidad dirigida a los NNA en su calidad de consumidores" (Capítulo 33)

Fuente: Creación basada en la normatividad de PDP

Mediante el Decreto Único Reglamentario del Sector Comercio 1074 de 2015 por el medio del cual se reglamenta parcialmente la Ley Estatutaria de Protección de Datos Personales y se establece los requisitos para el tratamiento de datos personales de NNA en el ámbito empresarial:

"Artículo 2.2.2.25.2.9. Requisitos especiales para el tratamiento de datos personales de niños. Está prohibido, excepto cuando se trate de datos de naturaleza pública, de conformidad con lo establecido en el artículo 7 de la Ley 1581 de 2012 y cuando dicho tratamiento cumpla con los siguientes parámetros y requisitos:

1. Que responda y respete el superior de los niños.

2. Que se asegure el respeto de sus derechos fundamentales.

Cumplidos los anteriores requisitos, el representante legal del niño, niña o adolescente la autorización previo ejercicio del menor de su derecho a ser escuchado, opinión que valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto." (Decreto 1074, 2015).

Por lo tanto, todo operador de la información personal de los niños ya sea responsable o encargado, debe administrar el uso adecuado de los datos que identifican las personas de

conformidad con los principios establecidos por la Ley 1581 de 2012. Así como la familia y la sociedad están llamados a exigir a dichos operadores de la información personal el responsable tratamiento los datos personales de los menores de edad. (Decreto 1074, 2015).

3.2.2. Tratamiento de datos personales de los menores de edad en el ámbito penal

Otra de las implicaciones jurídicas que se dan a partir de la vulneración de los datos personales son, por una parte, el sancionar penalmente la conducta que genero dicha vulneración y por la otra parte tenemos aquella consecuencia jurídica que implica el reconocimiento de un perjuicio al individuo titular de los estos datos personales, debiendo aquella persona que generó este perjuicio la reparación del daño.

Los actos ilícitos generan consecuencias jurídicas, desde la reparación de un daño hasta sancionar penalmente la conducta, a partir de esto los actos ilícitos se clasifican en faltas civiles y faltas penales, siendo las faltas civiles a partir de las cuales se genera la responsabilidad civil imponiendo la obligación de reparar el daño causado, como lo expresa Tamayo:

Como se ve, el hecho ilícito consiste siempre en el incumplimiento de obligaciones contractuales, cuasicontractuales, legales o simplemente en el incumplimiento del deber general de prudencia. De allí que podamos afirmar que la responsabilidad civil encuentra su fundamento jurídico en los hechos ilícitos. (2007, p.7).

En el campo del derecho penal todos aquellos actos ilícitos que generen la violación de datos personales son susceptibles de ser sancionados penalmente, debido a que la violación de datos personales se configura como un delito.

El delito informático como lo señala Gil Osorio, Juan Fernando y Silva Ossa (2005) es toda aquella conducta, típica, antijurídica y culpable que tiene por finalidad la destrucción o el daño de ordenadores, información personal, medios electrónicos, así como la obtención ilegal de información personal que se encuentra contenida en diversos medios como; datos, redes de internet, aparatos electrónicos, con el propósito de sacar provecho para sí o para un tercero.

En este sentido, un delito informático dentro de la modalidad de violación de datos personales, hace referencia a todos aquellos actos ilícitos que el ser humano realiza y son susceptibles de ser sancionados penalmente por el derecho penal, como lo describe el artículo 269F del código penal colombiano.

El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes. (Congreso de la República de Colombia, 2012).

Este tipo penal se desarrolló con el fin de proteger el bien jurídico del derecho a la privacidad de información personal, sancionando penalmente aquellas conductas que generan la violación de los datos personales, señalando cuales acciones generan dicha afectación, todo ello teniendo en cuenta, la actual era de las tecnologías y las comunicaciones.

La interpretación de la violación de datos debe ser amplia, en razón del gran número de medios por los cuales actualmente se puede generar una mayor vulneración de los registros de información personal en diversas tecnologías que existen en la actualidad y el deseo de las personas de estar cada vez más conectadas con el mundo digital; como se observa en la siguiente tabla:

Tabla 29.

Instrumentos de protección de datos personales en el ámbito penal

Normativa	Disposición
Ley 599 de 2000 (Código Penal Colombiano)	Tipifica como delito la violación de datos personales enmarcado en la vulneración de los principios relacionados con la confidencialidad, la integridad y la utilización de los sistemas informáticos (artículo 269F) Bien jurídico tutelado
Ley 906 de 2004	Las disposiciones de la establecen los principios rectores y garantías procesales con respecto a los derechos de carácter fundamental tales como: "la intimidad, la igualdad, la libertad de los tratados internacionales… la defensa de la intimidad de toda persona tal como lo estipula la norma" (Código de Procedimiento Penal, 2004 Art. 14). Así mismo, el artículo 244 de la reglamenta el control de legalidad sobre la búsqueda en bases de datos y examen de ADN, de conformidad con el principio de la dignidad humana. (Código de Procedimiento Penal, 2004).
Ley 1273 de 2009	Tipifica las conductas relacionadas con: "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos" y los delitos como el acceso abusivo a un sistema informático, que consiste en sancionar la conducta de la persona cuando sin autorización o por fuera de lo acordado acceda a un sistema informático protegido ya sea que este esté protegido o no con una medida de seguridad, o por que se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, esta conducta le acarrearía pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Fuente: Creación basada en el ordenamiento penal (2017)

Los instrumentos normativos de protección de datos personales en el ámbito penal especifican una protección especial para proteger el bien jurídico tutelado de la privacidad, confidencialidad, integridad y utilización de los sistemas de información personal a nivel general y no diferenciada para los menores de edad de acuerdo con la clasificación dada por el Sistema de Responsabilidad Penal para Adolescentes y la Ley de Infancia y Adolescencia:

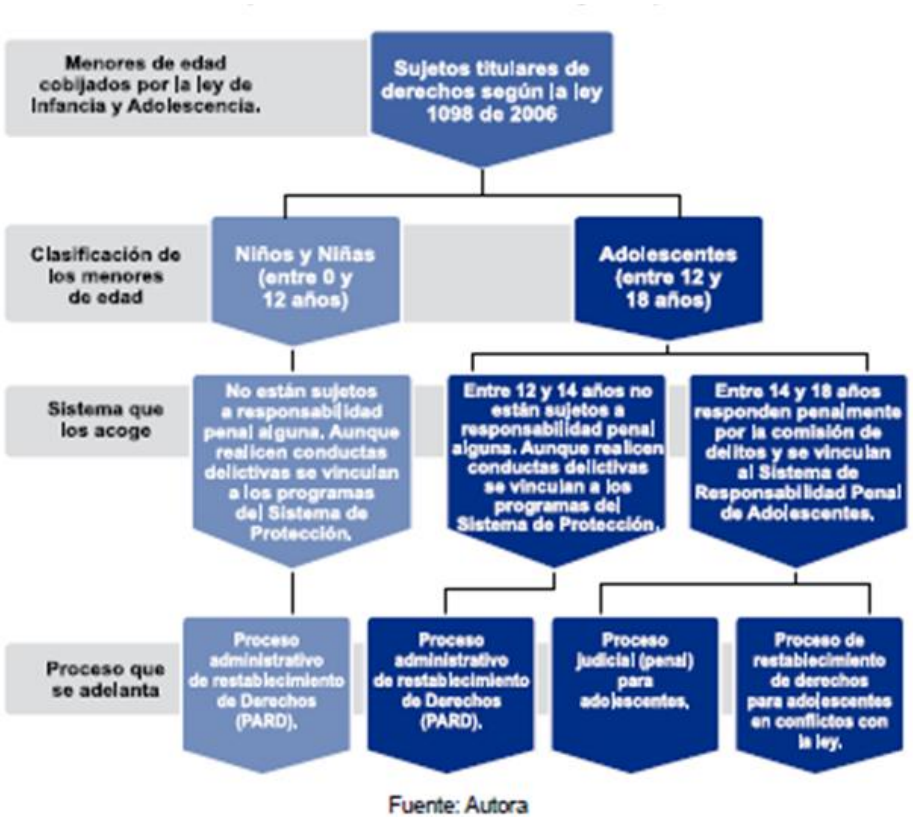


*Figura 21***.** Sujetos titulares de derecho según la Ley 1098 de 2006
Fuente: MINJUSTICIA (2015)

Sistema de responsabilidad penal para adolescentes, que acoge la teoría sistémica de acuerdo a la capacidad de comprensión y de accionar de los menores de edad como sujetos de derecho de especial protección bajo su nivel de responsabilidad y protección según la edad, niños y niñas*:* (entre 0 a 12 años) y adolescentes (entre 12 y 18 años) de acuerdo con el interés superior del niño y el fin de restablecimiento de sus derechos.

Es así que la Policía Nacional, la Fiscalía General de la Nacional y el Ministerio de las Tecnologías de la Información y las Comunicaciones están haciendo grandes esfuerzos reactivos y preventivos por combatir los delitos informáticos en sus diferentes modalidades a partir de la

Ley 1273 de 2009 y el Decreto 1413 de 2017. Aunque las brechas de seguridad relacionadas con la fuga de información e interceptación ilegal de llamadas, correos electrónicos, WhatsApp, pueden facilitarles a los cibercriminales vectores de ataque para lograr fines maliciosos, con los conocidos daños a la imagen de las instituciones, públicas o privadas.

Tabla 30.

Estudios estadísticos de las denuncias en materia de delitos informáticos en Colombia a 2017

Delito Denuncia	2014	2015	2016	2017	Total
Artículo 269A "Acceso abusivo a sistema informático"	398	1170	1776	780	**4124**
Artículo 269B "Obstaculización ilegítima de sistema informático o red de telecomunicaciones"	0	12	28	8	**48**
Artículo 269C "Interceptación de datos informáticos"	14	33	56	19	**122**
Artículo 269D "Daño informático"	8	47	113	34	**202**
Artículo 269E "Uso de software malicioso"	2	20	40	19	**81**
Artículo 269F "Violación de datos personales"	261	1050	1794	821	**3926**
Artículo 269G "Suplantación de sitios web para capturar datos"	41	36	170	82	**429**
Artículo 269I "Hurto por medios informáticos y semejantes"	3108	4977	6941	2902	**17928**
Artículo 269J "Transferencia no consentida de activos"	173	293	293	200	**959**
Total	**4005**	**7738**	**11211**	**4865**	**23814**

Fuente: SIEDCO desde el 2014 hasta el 01 de agosto del año 2017

Las referidas estadísticas muestran un alto nivel de denuncias y capturas por el delito de violación de datos personales, frente a lo cual exige por parte de las autoridades mejores estrategias reactivas y preventivas que permitan una adecuada intervención de las autoridades de control y vigilancia en procura de garantizar el derecho fundamental a la protección de datos personales, así como los derechos directamente o indirectamente vulnerados.

Al igual, se han llevado a cabo estudios por parte de la Policía Nacional sobre delitos informáticos en los cuales NNA en Colombia son víctimas de su ilegal uso, con ocasión de otros dos tipos delictuales: Artículo 218 C.P.: Pornografía con "persona menor de 18 años" y Artículo 219ª C.P.: "Utilización o facilitación de medios de comunicación para ofrecer actividades sexuales con persona menor de 18 años". Los siguientes datos que se registran a corte de 30 de agosto de 2017 son:

Tabla 31

Denuncias y capturas Colombia 2014-2017

Delito Denuncia	**2014**	**2015**	**2016**	**2017**	**Total**
"Pornografía con personas menores de 18 años" (C.P., 2000, Artículo 218)	165	474	84	366	**1789**
"Utilización o facilitación de medios de comunicación para ofrecer actividades sexuales con personas menores de 18 años" (C.P., 2000, Artículo 219ª)	2	42	50	28	**122**
Total	**167**	**516**	**834**	**394**	**1911**
Delito Capturas	2014	2015	2016	2017	Total
"Pornografía con personas menores de 18 años" (C.P., 2000, Artículo 218)	14	25	0	19	**98**
Utilización o facilitación de medios de comunicación para ofrecer actividades sexuales con personas menores de 18 años(C.P., 2000, Artículo 219ª)	2	3	4	9	**18**
Total	**16**	**28**	**44**	**28**	**116**

Fuente: SIEDCO desde el 2014 hasta el 01 de agosto del año 2017

Como parte de la atención oportuna de víctimas de delitos informáticos, el Centro Cibernético Policial Colombiano cuenta con la primera iniciativa a nivel iberoamericano, consistente en la atención policial en línea denominada CAI VIRTUAL, siendo oportuna en la atención de incidentes informáticos así como la recepción de solicitudes de personas víctimas de delitos

informáticos perpetrados en el territorio nacional, y en este mismo sentido se recepcionan solicitudes e inquietudes a nivel internacional, teniendo en cuenta que existen colombianos residentes en el exterior que se contactan a través de esta herramienta para reportar novedades y solicitar asesoría, a continuación se muestra la estadística:

Tabla 32.

Usuarios impactados en el periodo 2014-2017

Modalidad	**2014**	**2015**	**2016**	**2017**	**TOTAL**
Alertas preventivas en redes sociales @CaiVirtual	7086	2788	2825	1338	**14037**
Seguidores en Twitter	20000	5050	6558	3243	**34851**
Chats a través de nuestro portal de servicios 24/7	19097	13795	21239	16360	**70391**
Visitantes a nuestro portal web https://caivirtual.policia.gov.co/	321681	109915	132687	114390	**678673**
Correos electrónicos atendidos	14429	3192	5624	5823	**29068**
Total usuarios impactados	**375207**	**131952**	**166008**	**141154**	**827020**

Fuente: SIEDCO desde el 2014 hasta el 01 de agosto del año 2017

La estadística de las alertas, amenazas o riesgos de los servicios de ciudadanos digitales propios de las redes sociales, chat, correos electrónicos entre otros representa un significativo número de víctimas informáticos que acuden al sistema de vigilancia digital para salvaguardar sus derechos entre los que se encuentran niños, niñas y adolescentes que en ocasiones no acuden por miedo a sus padres, sociedad o falta de confianza en las instituciones del Estado.

3.2.3. Tratamiento de datos personales de niños en el ámbito educativo

La protección de datos personales de NNA también presente avances en el ámbito educativo concretamente con la Ley 1620 de 2013 entre los aspectos más sobresalientes de esta normatividad se resalta la "creación del sistema de información unificado de convivencia escolar en el marco del sistema nacional de convivencia escolar" entorno a aspectos propios de la formación integral de niño, así como el garantizar el derecho a la intimidad y la confidencialidad de las personas físicas.

Tabla 33.

La protección de datos personales de NNA en el sector educativo

Disposición normativa	**NNA**
"Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones - tic-, se crea la agencia nacional de espectro y se dictan otras" (Ley 1341, 2009)	Establece: "Articulación del plan de TIC: El Ministerio de Tecnologías de la Información y las Comunicaciones coordinará la articulación del Plan de TIC, con el Plan de Educación y los demás planes sectoriales, para facilitar la concatenación de las acciones, eficiencia en la utilización de los recursos y avanzar hacia los mismos objetivos. Apoyará al Ministerio de Educación Nacional para: 1. Fomentar el emprendimiento en TIC, desde los establecimientos educativos, con alto contenido en innovación 2. Poner en marcha un Sistema Nacional de alfabetización digital. 3. Capacitar en TIC a docentes de todos los niveles. 4. Incluir la cátedra de TIC en todo el sistema educativo, desde la infancia. 5. Ejercer mayor control en los cafés Internet para seguridad de los niños" (Artículo 39)
"Se crea el Sistema Nacional de Convivencia Escolar y Formación para el Ejercicio de los Derechos Humanos, la Educación para la Sexualidad y la Prevención y	Regula "la Participación de varias entidades que hacen parte sistema nacional de convivencia escolar y formación para los derechos humanos, la educación para la sexualidad y la prevención y mitigación de la violencia escolar" (Capítulo IV): "3. Las IPS, EPS y las IE., garantizarán el derecho a la intimidad y la confidencialidad de las personas involucradas." Establece las herramientas del "Sistema Nacional de Convivencia Escolar y Formación para el Ejercicio de los Derechos Humanos, la

Disposición normativa	NNA
Mitigación de la Violencia Escolar" (Ley 1620 de 2013)	Educación para la Sexualidad y la Prevención y Mitigación de la Violencia Escolar. (Capítulo V) Se crea el Sistema de información unificado de Convivencia Escolar en el marco del Sistema Nacional de Convivencia Escolar y formación para los derechos humanos, la educación para la sexualidad y la prevención y mitigación de la violencia escolar, para la identificación, registro y seguimiento de los casos de acoso, violencia escolar y de vulneración de derechos sexuales y reproductivos que afecten a los NNA de los establecimientos educativos. Este Sistema garantizará el derecho a la intimidad y la confidencialidad de las personas involucradas, de acuerdo con los parámetros de protección fijados en la Ley Estatutaria 1266 de 2008." (Artículo 28) (subrayado por fuera del texto)

Fuente: Creación propia

La normativa muestra el enfoque proteccionista y de responsabilidad del sistema educativo entorno a la formación de los NNA en diversos temas relacionados con las TICs, aunque su implementación ha sido pausada y poco exigente como por ejemplo la accesibilidad a los escenarios de los coffee internet sin ningún control y seguimiento por parte del Estado.

Dentro del Plan Decenal del Sistema de Justicia 2017 – 2027 se refiere la importancia de fortalecer el uso adecuado de las tecnologías de las información y las comunicaciones mediante la promoción e implementación de "programas de formación de educación superior, capacitación, socialización, sensibilización y desarrollo integral de competencias y habilidades a los operadores de justicia, policía judicial, abogados litigantes y demás servidores públicos del sistema de justicia para fortalecer sus aptitudes y actitudes según su cargo, especialidad, región, grupo de interés, conflictividad y problema social. Dichos programas tendrán en cuenta las destrezas y conocimientos de los actores del sistema de justicia para actuar con base en los nuevos modelos procesales adoptados por el país" (Bases del Plan Nacional de Desarrollo 2014-2018, DNP, 2014).

3.2.4. Tratamiento de datos personales de los niños en el sector público y de las Tecnologías de la información y las comunicaciones

Finalmente se puede observar que la protección de datos personales de NNA presenta avances en el ámbito de las tecnologías de la información y las comunicaciones, teniendo en cuanto el actual avance de estas tecnologías dentro de la vida cotidiana de las personales especialmente de los niños, establecer una normatividad frente a este ámbito resulta necesario, ahora las regulaciones en este ámbito se centran en la obligación de suministrar información, así como su correspondiente rectificación, regular la figura del responsable y del encargado del tratamiento de los datos personales así como evaluar el impacto de los mismos.

Tabla 34.

La protección de datos personales en el sector de las Tecnologías de la información y las comunicaciones

Norma	Disposición
"Plan Nacional de Desarrollo 2014 - 2018 "Todos por un nuevo país"" (Ley 1753 de 2015)	Contenidos digitales, obligatoriedad de suministro de información: "El uso y reutilización de esta información deberá garantizar la observancia de los principios y normas de protección de datos personales, de conformidad con lo dispuesto en las Leyes 1581 de 2012 y 1712 de 2014, así como las demás normas que regulan la materia" (Artículo 159)
"Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones" (Decreto 1078 de 2015)	Establece el objeto de la "Comisión Nacional Digital y de Información Estatal" el cual es la coordinación y orientación superior de la ejecución de funciones y servicios públicos relacionados con el manejo de la información pública, el uso de infraestructura tecnológica de la información para la interacción con los ciudadanos y el uso efectivo de la información en el Estado Colombiano"

“Lineamientos Generales en el Uso y Operación de los Servicios Ciudadanos Digitales" (Decreto 1413 de 2017)	Regula el tratamiento de datos personales, seguridad y privacidad de la información en temas novedosos tales como: Responsable y encargado del tratamiento, evaluación del impacto de tratamiento de datos personales, responsabilidad demostrada y programa integral de gestión de datos, privacidad por diseño y por defecto, seguridad de la información y limitación al uso de la información (Capítulo 6)

Fuente: Creación propia

Las disposiciones contenidas en el decreto 1413 del 2017, guardan una relación frente los usos tecnológicos y digitales, pero no hacen referencia a los derechos de los niños de manera particular. A diferencia con los estándares internacionales en materia de protección de datos personales, particularmente a través del modelo europeo, haciendo énfasis en el reglamento (UE) 2016/679 del Parlamento y del Consejo Europeo, se presenta la siguiente relación de los aspectos más destacados:

Frente al objeto de su regulación la Ley 1581 de 2012 comparte algunos aspectos normativos el decreto 1413 de 2017 así como también abarca otros temas de relevancia, tales como:

1. Establecer lineamientos para la gestión de servicios ciudadanos digitales y permitir a la ciudadanía el acceso a la administración pública a través del correo electrónico.
2. La figura jurídica del responsable y del encargado acorde con los postulados establecidos en el modelo europeo, atribuyéndose a estas personas la responsabilidad en el tratamiento de los datos personales.
3. El Reglamento (UE) 2016/679, parte de un reconocimiento a la protección personal de datos como un derecho fundamental, el cual no es absoluto, por lo que debe guardar un equilibrio con los demás derechos, en virtud del principio de proporcionalidad.

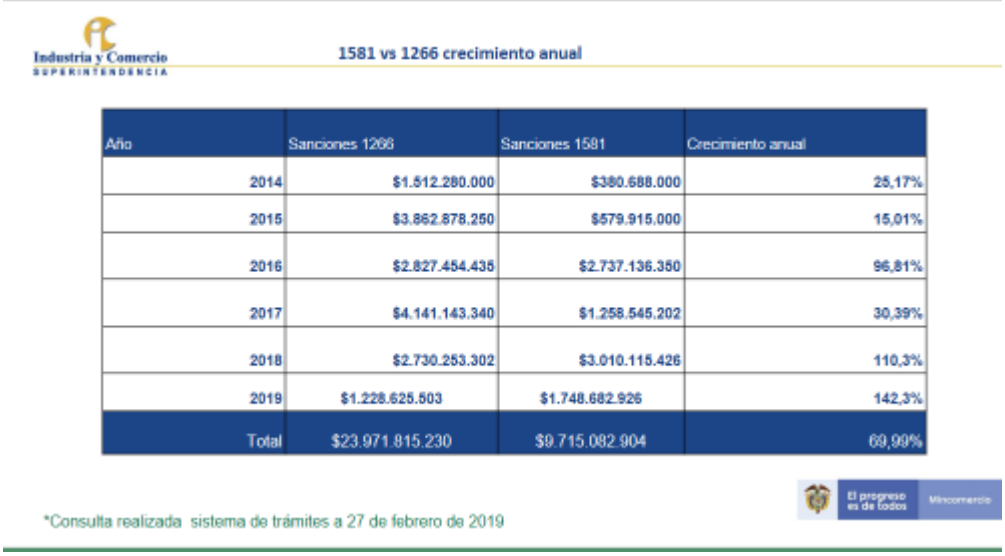
4. La regulación se orienta por los principios de accesibilidad exclusiva, escalabilidad, gratuidad, libertad de entrada en el mercado, libre elección, portabilidad, privacidad por diseño y efecto, seguridad, privacidad, circulación restringida de información y usabilidad.
5. Está en consonancia con postulados plasmados en el modelo europeo de protección de datos, a través de inclusión de determinadas figuras, mecanismos, evaluaciones, entre otros.
6. Los operadores de servicios ciudadanos digitales están en el deber de realizar evaluación de impacto respecto a la administración de los datos personales.
7. Acoge el modelo europeo respecto al deber de evaluar el nivel de seguimiento y vigilancia a las personas físicas por parte de los operadores en internet, respecto a las técnicas de caracterización de su perfil para que de manera preventiva y proactiva se actué respecto a las predicciones de comportamiento. (2017).

3.3. Control del tratamiento de datos personales por parte de la Superintendencia de Industria y Comercio

A más de 10 años de implementación de la ley de habeas data o primera ley de protección de datos personales para el sector financiero y crediticio se siguen presentando diversos casos a nivel empresarial donde no existen políticas de privacidad ni de protección de datos personales construidas y adecuadas de acuerdo con las disposiciones de administración o gestión integral de información personal.

De las sanciones impuestas por violación de la Ley 1266 de 2008 y a Ley 1581 de 2012 ha aumentado de 2014 a 2019, en un porcentaje de 69.99% ha sido por no solicitar o conservar copia

de la autorización para el tratamiento de datos personales 9% por no tramitar las consultas y reclamos formulados.



Año	Sanciones 1266	Sanciones 1581	Crecimiento anual
2014	$1.512.280.000	$380.688.000	25,17%
2015	$3.862.878.250	$579.915.000	15,01%
2016	$2.827.454.435	$2.737.136.350	96,81%
2017	$4.141.143.340	$1.258.545.202	30,39%
2018	$2.730.253.302	$3.010.115.426	110,3%
2019	$1.228.625.503	$1.748.682.926	142,3%
Total	$23.971.815.230	$9.715.082.904	69,99%

Figura 23. 1581 vs 1266 crecimiento anual
Fuente: SIC, 2019

Algunas de las sanciones relevantes que ha impuesto la Superintendencia de Industria y Comercio por violación del derecho a la privacidad y protección de datos personales son:

1. La omisión de procedimientos y políticas de privacidad adecuadas, la falta de información sobre la finalidad del tratamiento del dato y el mayor porcentaje en la falta de autorización del titular de la información y niveles de seguridad como se presenta en el siguiente reporte:

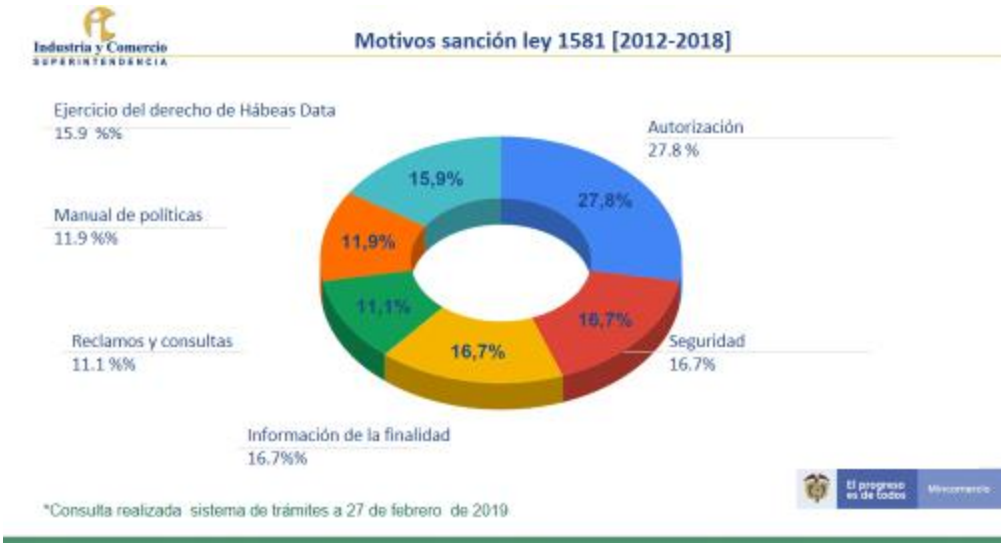


Figura 24. Motivos sanción Ley 1581 (2012-2018)

2. La falta de autorización del reporte o del consentimiento del titular del dato para realizar el tratamiento que se requiere, frente a lo cual se requiere capacitar a las empresas en la implementación de la política de privacidad.

Figura 2522. Motivos sanción 1266 año 2019

Fuente: SIC, 2019

3. Ausencia de la autorización para el tratamiento y la falta de atención oportuna por reclamos de los afectados se presentan en el mayor índice, por lo que se requiere de mayores controles por parte de los operadores.

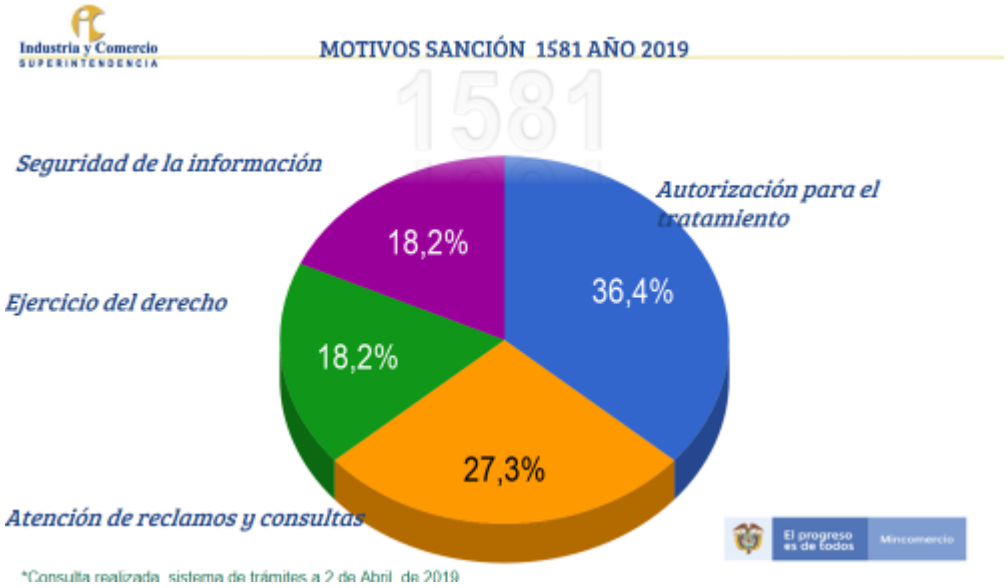


Figura 26. Motivos sanción 1581 año 2019

Fuente: SIC, 2019

Y con relación al sector financiero y crediticio se evidencia la necesidad de mayor calidad de los datos y comunicación previa al consumidor sobre sus derechos en el marco del tratamiento informado de sus datos.

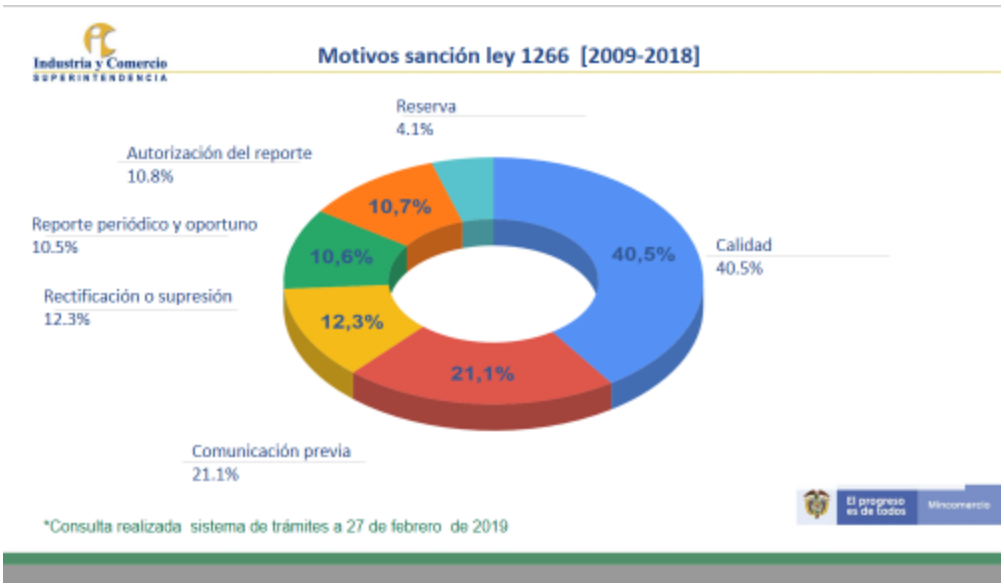


Figura 27. Motivos sanción Ley 1266 (2009-2018)

Fuente: SIC, 2019

En comparación con otros sectores empresariales se identifica la falta de autorización por parte del titular, mayor seguridad y la falta de comunicación de la finalidad del tratamiento de datos al cliente o usuario.

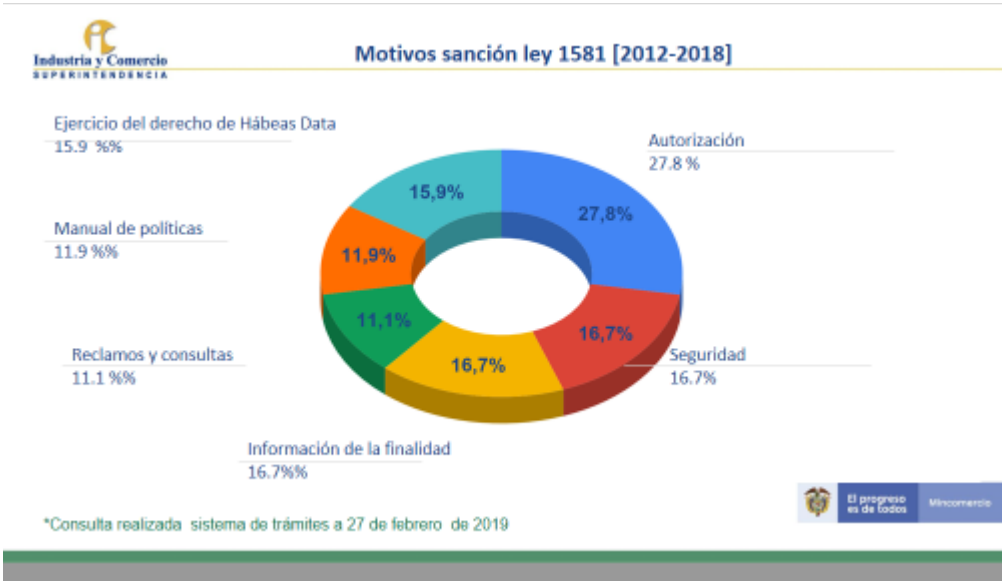


Figura 28. Motivos sanción Ley 1581 (2012-2018)

Fuente: SIC, 2019

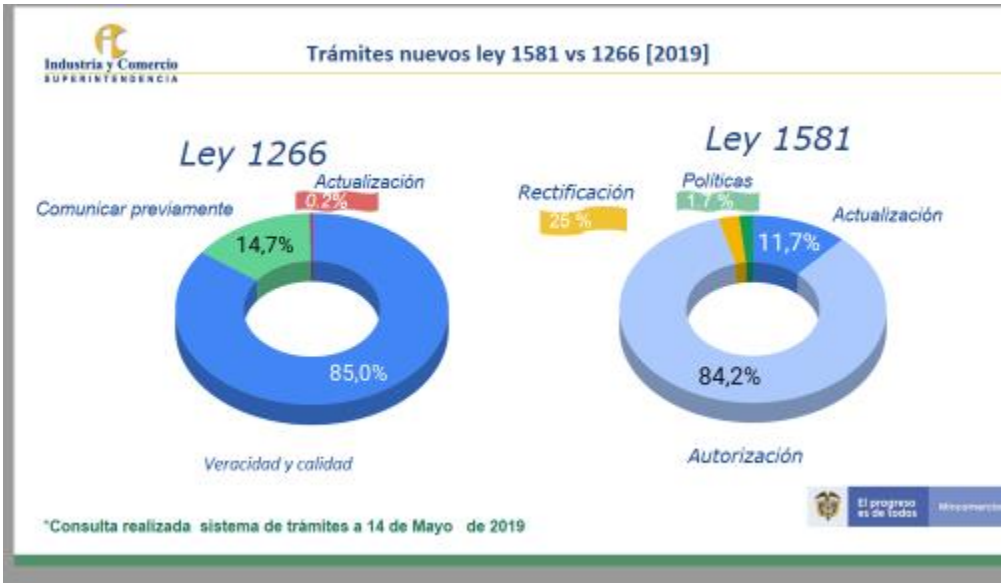


Figura 29. Trámites nuevos Ley 1581 vs 1266 (2019)
Fuente: SIC, 2019

En términos generales los resultados estadísticos evidencian la falta de conocimiento de la regulación de la protección de datos personales, la implementación de políticas de privacidad, normas corporativas vinculantes y códigos de buenas prácticas desde la privacidad por diseño para garantizar la calidad del dato, la obtención así como verificación de la autorización legal.

En materia del tratamiento de datos personales de NNA en Colombia se presenta algunos casos ilustrativos en los cuales la Superintendencia de Industria y Comercio ha impuesto sanciones en virtud del incumpliento del régimen jurídico de protección:

1. *Recolección, circulación y seguridad de los datos personales de menores de edad sin solicitar la autorización de los padres de familia para el tratamiento. - Centro Comercial Cosmocentro de Cali - Sanción: $30.800.000.*

Hechos relevantes

La SIC, recibió el 6 de septiembre del 2013, una denuncia contra la persona jurídica: Cosmocentro Ciudadela comercial de Cali, en virtud de una actividad infantil denominada “taller de cometas” del “club cosmitos” desarrollada por Cosmocentro en la cual se recolecta información personal relacionada con 21 niños que participan en esa actividad, incluyendo el hijo de 5 años de edad de la denunciante, datos relacionados con el nombre, edad, dirección, teléfono, fecha de nacimiento, nombre del acudiente, numero del celular y correo electrónico.

El 28 de agosto del 2013, la denunciante recibió un correo electrónico por parte de la persona jurídica Cosmocentro, en la cual solicitaba completar la información que faltaba en el formulario de la inscripción para la base datos del “club cosmitos” del centro comercial. Este correo electrónico incluía los formularios con la información personal de cada uno de los 21 niños que participaron en la actividad antes mencionada.

Pronunciamiento de la SIC

Teniendo en cuenta que Cosmocentro, es la entidad que procedió a recoger, decidir y hacer tratamiento sobre los datos personales de los menores, se constituyó en el responsable del tratamiento de los datos personales, en los términos que lo establece el literal e) del artículo 3 de la Ley 1581 del 2012, por lo que le son imputables los deberes que se derivan de su actividad.

Se observa que el texto que presenta la investigada como prueba de que informo al titular sobre los usos que pretendían dar a los datos recogidos, es insuficiente ya que no brindo toda la información requerida, por lo que dicho texto no es ni constituye el otorgamiento de una autorización para el tratamiento de los datos personales.

Ahora bien, es relevante resaltar que en este caso en particular donde el análisis de la conducta de la investigada se centra en la recolección y uso de información de menores de edad, la

valoración de dicho tratamiento se debe realizar atendiendo las normas especiales que regulan el uso de esta categoría de datos.

Así debe recordarse que el tratamiento de datos personales de menores esta permito siempre y cuando se acuda a una interpretación restringida, según la cual ese uso de la información se debe sujetar a la interpretación esbozada de la corte constitucional cuando analizo la exequibilidad del artículo 7 de la Ley 1581 del 2012. Aun cuando el texto original de la norma estableció en principio que quedaba "proscrito el tratamiento de datos personales de niños, niñas y adolescentes, salvo aquellos datos que sean de naturaleza pública".

La Corte aclaro que dicha disposición "no debe entenderse en el sentido de que existe una prohibición absoluta del tratamiento de datos de menores de 18 años, exceptuando los de naturaleza pública, pues ello, daría lugar a la negación de otros derechos superiores a esta población". (Corte Constitucional, Sala Plena, sentencia C-748, 2011).

Siguiendo esa línea de interpretación, esa corporación concluyo que "el tratamiento de los datos personales de menores de 18 años, al margen de su naturaleza, pueden ser objeto de tratamiento siempre y cuando el fin que se persiga con dicho tratamiento responda al interés superior de los niños, niñas y adolescentes y se asegure sin excepción alguna el respeto de sus derechos prevalentes" (Corte Constitucional, Sala Plena, sentencia C-748, 2011).

Es importante recalcar que de acuerdo con la Ley 1581 del 2012, los datos personales públicos son aquellos que no son semiprivados, privados o sensibles. Así mismo la norma plantea de manera no taxativa que datos como los relativos a la condición civil de las personas, su profesión u oficio, la calidad de comerciante y servidor público pueden ser considerados datos personales de carácter público, por lo anterior, la información relativa a la dirección y teléfono de su domicilio y el correspondiente a su número celular, así como el correo electrónico personal, son datos que

pertenecen al ámbito privado del titular, por lo que su tratamiento debe adelantarse previa autorización expresa e informada y para el uso o tratamiento que se haya autorizado.

Es claro que la falta de diligencia por parte de Cosmocentro, vulnero el derecho a la protección de datos de los titulares al no conservar bajo las condiciones de seguridad requerida la información de estos, situación que es de mayor trascendencia al tratarse de información relativa a menores de edad, máxime cuando se trata de datos privados como quera que hacen referencia a la información de contacto y ubicación, datos que no son públicos,

Se resalta que no se observa, en la documentación de la entidad investigada, ni en su portal de internet, así como dentro de su política de tratamiento que cuente con protocolos de seguridad para el tratamiento de datos personales que pueda prevenir o minimizar el riesgo en el tratamiento de estos datos, mucho menos cuando se trata del envió de información personal a través de comunicaciones electrónicas. Por lo anterior, con la divulgación masiva de datos personales, este despacho considera que son más el resultado de una falta de protocolos de seguridad y capacitación en el tratamiento de datos personales, que considerarlo como un error humano.

En este orden de ideas este despacho encuentra que con su actuar el responsable realizo tratamiento de datos personales de menores de edad, sin contar con la autorización de los representantes legales de los mismos. Igualmente encuentra probado que con su conducta la investigada no garantizo la seguridad en el tratamiento de datos personales, facilitando, mediante la divulgación a terceros no autorizados, el acceso y el uso no autorizado de los mismos.

2. *Información de treinta usuarios (tres casos menores de edad) que habían realizado consultas médicas por la página web de la empresa - COLMÉDICA MEDICINA PREPAGADA S.A. (SIC,* Resolución 39298, 2016)

Hechos relevantes

1. En el proceso de investigación se pudo establecer que Colmédica dejó en evidencia información de treinta usuarios que habían realizado consultas médicas por la página web de la empresa (atención en línea), la entidad no había tomado las medidas de seguridad adecuadas, toda vez que, una de las pacientes digitó su nombre en un motor de búsqueda www.colmedica.com – consulta best doctors cuando le arrojó como resultado, la información que había suministrado en dicho portal para su consulta médica, en dicha búsqueda aparecían datos como: 1) nombre y apellido, 2) documento de identificación, 3)dirección de correspondencia y ciudad ,4) correo electrónico, 5) fecha de nacimiento, 6) género, 7) una descripción de la consulta formulada por el usuario del servicio en la que hace relación a su condición de salud actual indicando las patologías que padece; 8) diagnósticos y reportes de exámenes médicos en general y 9) Y la trazabilidad de la solicitud. Adicionalmente, en tres casos analizados de forma aleatoria, se hacía relación a información personal de salud de menores. *(SIC,* Resolución 39298, 2016).

Pronunciamiento de la SIC

Mediante Resolución 39298 del pasado 21 de junio de 2016, la Dirección de investigaciones de protección de datos personales de la Superintendencia de Industria y Comercio formulo cargos contra COLMÉDICA MEDICINA PREPAGADA S.A., en la medida en que se determinó que efectivamente ostenta la calidad de responsable del tratamiento de los datos personales de sus usuarios, ya que es quien establece los fines y medios esenciales para el tratamiento.

Se incumple los *deberes por el responsable de tratamiento de los datos personales,* consagrados en los art 9 y 17 de la Ley 1581:

- Deber de obtener autorización previa para el tratamiento.
- Deber de gestionar la seguridad de la información en forma eficiente.

- Deber de informar sobre la ocurrencia de incidentes de seguridad: en este punto se advierte que no se admite excepción alguna a este deber de informar a la SIC cualquier violación a las medidas de seguridad que originen riesgos en la administración de los datos personales que realicen los responsables de tratamiento.

Se desconoce *la clasificación de los datos personales*: Datos sensibles: Generan una vinculación a la esfera personalísima del titular, siendo así una materialización del art 15 de la C.P, conforme a esto los responsables y encargados, deben ser más diligentes cualquier operación que involucre datos sensibles. Datos de niñas, niños y adolescentes: salvaguardar teniendo en cuenta que se trata de sujetos de especial protección (Artículo 44 C.P), deben prevalecer sus derechos y el interés superior de este tipo de sujetos de especial protección constitucional.

La divulgación indebida de datos personales, semiprivados y privados, de carácter sensible, y algunos relativos a niños, niñas y adolescentes, obedeció a un incidente de seguridad que comprometió los datos personales de los titulares poniendo en riesgo los mismos, información que debió ser informada en su momento por COLMÉDICA a la Superintendencia.

Cargos imputados:

1. Omisión del deber de gestionar la seguridad de la información por parte de COLMÉDICA bajo las condiciones de calidad.
2. Falta del deber de COLMÉDICA de informar a la SIC los incidentes de seguridad de la información.
3. Incumple el artículo 2.2.2 .25.3.7 del decreto único reglamentario 1074 de 2015 y su integración con la circular externa No 002 del 03 de nov de 2015.

4. Disposiciones relacionadas con la seguridad de la información y la interpretación del deber de contenido en el literal n) del artículo 17 de la Ley 1581 del 2012, en específico, el concepto de violaciones a los códigos de seguridad.

Sanción económica

Multa de $827.346.000 que equivalen a 1200 SMMLV por incumplimiento de lo dispuesto en el literal d) art 17 y literales f y g del art 4 de la Ley 1581 del 2012 y otra multa por el valor de $ 206.836.500 que equivalen a 300 SMMLV por la infracción del literal n) art 17 de la Ley 1581, relacionado con el deber de reportar los incidentes de seguridad a la autoridad de control en los eventos de riesgos y afectación a la administración integral de la información.

Es sin duda la tipología de información (Datos médicos) y los riesgos en su administración la que llevan a la Superintendencia a la imposición de una multa en esta cuantía. Es claro que lo que se castiga es la falta de diligencia y la inobservancia del deber de informar al ente supervisor sobre la ocurrencia de una brecha de seguridad que expuso información sensible por internet.

Es deber de las entidades de salud tomar las medidas necesarias de seguridad, partiendo que se tratan de entidades que por su naturaleza manejan un nivel de información muy sensible; es mayor el deber de cuidado que se requiere dando aplicación a los postulados del Art. 26 y 27 del Decreto 1377 de 2013 (Decreto Único Reglamentario 1074 de 2015 cap. 25).

Una vez la superintendencia recibe la queja e inicia investigación, comprobó que este hecho no solo se había presentado con la quejosa, si no con 30 personas más la privacidad y la protección de los datos, son derechos que van unidos y hoy en día los usuarios son cada vez más conocedores y celosos de entregar su información personal a un tercero; así mismo, exigen un adecuado uso de sus datos por parte de las empresas (SIC, Resolución 39298, 2016).

Hay que implementar controles adecuados de tratamiento de datos personales y reducir el impacto de la materialización de los riesgos que conlleva la práctica de la privacidad desde la entrada de cada proceso administrativo.

3. *Colegio Religioso desconoce la autorización para administrar los datos personales y datos personales sensibles (SIC, 2018, Resolución No. 94719).*

Hechos relevantes

Infracción de la protección de datos personales por la recolección de los datos sin autorización del titular por excepción de la actividad sin ánimo de lucro y de origen canónico que cumple las obligaciones contractuales propias del servicio de educativo, no contar con el Manual de Política de privacidad de datos personales, no acoger el principio de libertad y proporcionalidad, de conformidad con la Ley 1581 (2012 art. 9), Decreto 1377 (2013, art.5 y 6) y Decreto 1074, 2015).

Pronunciamiento de la SIC

De conformidad con la Ley 1581 la entidad recurrente (el colegio) incumple la normativa sin estar incurso en las excepciones relacionadas con obtener autorización para el tratamiento de los datos personales, que establece:

"La autorización del titular no será necesaria cuando se trate de:

a) Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial:
b) Datos de naturaleza pública;
c) Casos de urgencia médica o sanitaria;
d) Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos;

e) Datos relacionados con el Registro Civil de las personas" (Ley Estatutaria PDP, 2012, artículo 10).

Por lo anterior, la naturaleza de la entidad recurrente no se adecua a los anteriores casos de excepción y así mismo, no cumple con el principio de libertad que se caracteriza por vía jurisprudencial como: "pilar fundamental de la administración de los datos" y con ello "permite al ciudadano elegir voluntariamente si su información personal puede ser utilizada o no en bases de datos" (Corte Constitucional, sentencia, 2011, C-748 numeral 2.6.5.2.3).

Y además ha generado: "…altos riesgos en términos de vulneración del habeas data, la intimidad e incluso la dignidad de los titulares de los datos, los agentes que realizan en estos casos el tratamiento tienen una responsabilidad reforzada que se traduce en una exigencia mayor en términos de cumplimiento de los principios del artículo 4 y los deberes del título VI. Esa mayor carga de diligencia se deberá también traducir en materia sancionatoria administrativa y penal." (…)" (Corte Constitucional, sentencia, 2011, C-748) (subrayado fuera de texto).

Lo anterior, conlleva a la falta de legitimidad en todas las etapas de recolección y procesamiento de los datos que faculta al titular en dar su consentimiento y autorización libre, previa y veras a quienes desee que gestionen su información. (Corte Constitucional, sentencia, 2008, C-1011) tales como:

"…

a) Padres de familia y estudiantes matriculados
b) Padres de familia y estudiantes interesados a ingreso.
c) Empleados del Colegio; docentes, directivos docentes, administrativos y personal de servicios generales.
d) Datos personales de exalumnas del Colegio

e) Datos personales de proveedores de productos y servicios que requiere el Colegio.

f) Visitantes del Colegio" (SIC, 2018, Resolución No. 94719 hoja 7).

Todos los anteriores datos recolectados ameritan autorización del titular, y en el marco de la responsabilidad demostrada de verificación de la autorización del tratamiento de datos personales, las entidades públicas y privadas deben cumplir:

> "a) El tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo; b) El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobe datos sensibles o sobre los datos de las niñas, niños y adolescentes; c) Los derechos que le asisten como Titular; d) La identificación, dirección física o electrónica y teléfono del Responsable del Tratamiento" (Ley Estatutaria PDP, 2012, 1581 art. 12).

Y tal virtud normativa, se debe garantizar el cumplimiento de los fines esenciales del Estado Social de Derecho tales como: "garantizar la efectividad de los principios, derechos y deberes consagrados en la Constitución" (Colombia, Constitución Política, 1991, artículo 2) y a su vez, la efectiva protección de los derechos humanos y el desarrollo de la actividad e iniciativa privada y empresarial en el marco del bien común de las personas considerados como sujetos y no como cosas de derecho, que se soportan en el postulado: libre competencia económica es un derecho de todos que supone responsabilidades" y por lo tanto "la empresa, como base del desarrollo, tiene una función social que implica obligaciones" (Colombia, Constitución Política, 1991, artículo 333).

Para efectos prácticos las empresas están llamadas a cumplir con el principio de la responsabilidad demostrada (accountability) y "compliance", el cual se define como: "los responsables del tratamiento de datos personales deben ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, que han implementado medidas apropiadas y efectivas

para cumplir con las obligaciones establecidas en la Ley 1581 de 2012. (Ley Estatutaria PDP, 2013, 1377, art. 26).

Medidas de tratamiento de datos personales de manera adecuada tales como:

"(1) Diseñar y poner en marcha un programa integral de gestión de datos (en adelante PIGDP), lo cual exige compromisos y acciones concretas de los directivos de la organización, así como la implementación de controles de diversa naturaleza que se enuncian en el texto de la guía;

(2) Desarrollar un plan de revisión, supervisión, evaluación y control del PIGDP, y

(3) Demostrar el debido cumplimiento de la regulación sobre tratamiento de datos personales.

Las empresas requieren de un decidido y proactivo compromiso de protección de los derechos fundamentales y programas integrales de datos personales de sus consumidores y usuarios más allá del valor de uso comercial desde su diseño, revisión, actualización, indexación y evaluación en procura de modelos de gestión de seguridad de datos online y offline que garanticen los derechos y libertades humanas en procura del principio de la dignidad humana.

La noción de "compliance" hace relación a: "conjunto de procedimientos y buenas práctica adoptadas por las organizaciones para identificar y clasificar los riesgos operativos y legales a los que se enfrentan y establecer mecanismos internos de prevención, gestión, control y reacción frente a los mismos" (Cfr. World Compliance Association (WCA). http://www.worldcomplianceassociation.com).

Se incorpora identificar y clasificar los riesgos como una tarea conjunta de las empresas para su mitigación del compliance y accountability que involucran la revisión de un "sistema de administración de riesgos asociados al tratamiento de datos personales" (SIC, 2015, Guía para implementación del principio de responsabilidad demostrada, accountability, p. 16-18).

Dentro de las sanciones se establece el cumplimiento de obligaciones legales y estatutarias sobre tratamiento de datos personales, cumplir el principio de demostración ante entes de control y vigilancia e imponer sanción pecuniaria.

3.4. Nivel de adecuación del tratamiento de la privacidad de datos personales de los niños a los estándares de protección

Colombia, hoy tiene un "nivel adecuado" de protección de datos personales? La respuesta es no, a pesar de los esfuerzos de avanzar en su tratamiento jurídico a la luz del estándar europeo e iberoamericano, en aras de facilitar la transferencia internacional de información, garantizar los derechos de las personas a la luz de la Constitución Nacional y de generar ventajas competitivas con nuevos y novedosos negocios de cara a la libertad de iniciativa privada, en una democracia participativa e incluyente; la respuesta en ese momento es que al igual como la mayoría de los países latinoamericanos, no ha sido considerado por la Comisión Europea como un Estado que garanticen un nivel adecuado de protección como ya en su momento lo mencionó Remolina (2012).

En la medida en que un Estado tenga un nivel adecuado de tratamiento de datos personales, garantiza la protección de los derechos de las personas en general y se crea un escenario competitivo frente a las nuevas oportunidades de negocios internacionales y las condiciones jurídicas lícitas, justas y equitativas en el contexto ciber-evolutivo de los servicios de la sociedad de la información; en razón a que efectivamente la protección de datos personales es considerado un elemento consustancial de las sociedades democráticas.

3.4.1. Primeros estándares Internacionales de Protección de la privacidad de los niños en el tratamiento de datos de carácter personal

De acuerdo con la exigencia internacional en materia del tratamiento de datos personales los estándares europeos desde el 2009 cimentaron su desarrollo e importancia a nivel internacional, destacando los siguientes lineamientos en general y es especial los relacionados con los niños:

Tabla 35.

Exigencia internacional de protección de los datos personales de NNA

Estándar Europeo
"Es imperativo expedir una Ley acorde a la materia"
"Caracterizada por ser general, integral, armónica y sistemática de los aspectos medulares del habeas data y la protección de toda clase de dato personal"
"Con altísimos estándares y acorde a fenómenos diferentes a la transferencia internacional de datos como la captura o recolección de información personal de ciudadanos de cualquier parte del mundo por internet"
"Reglas particulares para la niñez y la adolescencia de manera que se conviertan en sujetos especialmente protegidos por las regulaciones de protección de datos personales, con el fin de mitigar los riesgos y peligros a que se ven expuestos en internet, particularmente en las redes sociales"

Fuente: Creación basada en los estándares de privacidad de datos personales (2009)

Al comparar el régimen de protección de los datos personales de los NNA, de la Unión Europea, Estados Unidos y Colombia, se evidencia en cada una de estas regulaciones aspectos innovadores y diversos enfoques de derechos, unos acordes y otros apartados del interés superior del niño. Por lo tanto, establecer las diferencias y similitudes, así como estrategias de mejoramiento y mecanismos idóneos de protección integral y de prevención de riesgos en Colombia, contribuye a construir adecuados escenarios de privacidad de los datos personales.

Tabla 36.

Leyes y lineamientos de protección de datos personales de niños EE. UU – UE y Colombia

Aspectos Relevantes	Estados Unidos (FTC)	Unión Europea (Grupo de Trabajo del Artículo 29)	Colombia
Legislación	"COPPA Children's Online Privacy Protection Act of 1998 modificación aprobada en 2013"	"Documento de trabajo 1/08 sobre la protección de datos personales de los niños"	Ley 1581 de 2012 Ley Estatutaria de Protección de Datos Personales (Decreto reglamentario 1377 de 2013)
Ámbito de aplicación	"Se aplica únicamente a los datos personales recabados online de menores de 13 años. Padres y Tutores legales, operadores de páginas web, mensajes en línea, salas de chat y correo electrónicos. En particular, la ley está dirigido a operadores de sitios web que están dirigidas a niños o que tienen conocimiento que los niños están visitando el sitio"	"Dirigido a menores de 18 años dentro del ambiente escolar. El documento ofrece directrices específicas dirigidas a los colegios, específicamente a profesores y autoridades escolares".	"Por regla general esta proscrito el tratamiento de datos personales de niños, niñas y adolescentes, salvo aquellos que sean de naturaleza pública y cuando se cumpla los requisitos: • Que responsa y respete el interés superior de los niños, niñas y adolescentes • Que se asegure el respeto a sus derechos fundamentales"
Objetivo	"Regular la recogida, tratamiento, información y comunicación en línea recabada por personas físicas o morales dentro del territorio de los	"Establecer los principios generales para la protección de los datos de los niños y de manera particular el tratamiento de esta información que se	"Conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos y los demás derechos, libertades y

Aspectos Relevantes	Estados Unidos (FTC)	Unión Europea (Grupo de Trabajo del Artículo 29)	Colombia
	Estados Unidos de América que contengan datos de niños menores de 13 años".	realiza en los colegios – área crítica especifica que recaba un sin número de información de sus alumnos".	garantías constitucionales relacionadas con el derecho a la intimidad y el derecho a la información
La información	"La información sujeta al ámbito de esta ley, será aquella que contenga los datos que se en listan a continuación. • Nombre. • Domicilio. • Correo electrónico. • Número telefónico. • Número de seguridad social. •Cualquier medio de identificación que permita el contacto físico o en línea con un individuo especifico. • Información del menor o de sus padres recolectada por un sitio web"	"Publicidad de menores Geolocalización de menores en aparatos inteligentes Redes sociales"	"Reglamenta los casos, la forma y el contenido en que se deberá presentar la información y la publicidad dirigida a los niños, niñas y adolescentes en su calidad de consumidores por cualquier medio, sea impreso, electrónico, audiovisual, auditivo, entre otros en el ámbito privado. En el ámbito público: se debe fomentar las prácticas democráticas, la inclusión de información sobre el derecho de acceso a la información con sus principios y reglas básicas"
Principios y Derechos	"Publicidad de las políticas o aviso de privacidad sobre el	"Reconoce como derechos	"Principio de legalidad Principio de finalidad Principio de libertad

Aspectos Relevantes	Estados Unidos (FTC)	Unión Europea (Grupo de Trabajo del Artículo 29)	Colombia
fundamentales del niños	tratamiento de datos de los menores Información y obtención del previo consentimiento de los padres o representantes legales del menor para el tratamiento de sus datos personales Se reconoce a los padres el derecho a acceder y conocer los datos personales recabados del menor. Se prohíbe condicionar la participación de un menor en un juego para obtener información. Es necesario adoptar mecanismos de protección de la confidencialidad, seguridad e integridad de los datos personales de los menores".	fundamentales del niño: El principio de interés superior por el niño; La protección y cuidado necesario para el bienestar de los niños; El derecho a la intimidad; El derecho a la de representación; La adaptación al grado de madurez del niño; El derecho a ser consultados; entre otros"	Principio de veracidad o calidad Principio de transparencia Principio de acceso y circulación restringida Principio de seguridad Principio de confidencialidad Reconoce como derechos fundamentales de los niños: El principio de interés superior del niño La protección y cuidado necesario para el bienestar del niño El derecho a la intimidad El derecho a la representación La adaptación al grado de madurez del niño El derecho a ser consultados entre otros"
Autorregulación	Recoge normas de puerto seguro "safe harbor" es decir se da importancia la autorregulación por parte de la industria (las	Tecnologías que mejoren la protección de la intimidad (parámetros por defecto respetuosos con la intimidad,	La autorregulación es voluntaria. Responsabilidad demostrada Accountability. En el sector privado se habla

Aspectos Relevantes	Estados Unidos (FTC)	Unión Europea (Grupo de Trabajo del Artículo 29)	Colombia
	empresas presentan ante la FTC códigos autorregulatorios, en los que se concreten criterios para el tratamiento de datos personales de menores) como por ejemplo los códigos de buenas prácticas de la industria de la publicidad.	programas informáticos de verificación de edad), autorregulación por la propia industria a través de códigos de buenas prácticas que incluyan medidas de ejecución eficaces y sanciones disciplinarios y medidas legislativas ad hoc	del código colombiano de autorregulación publicitaria (2013), el cual dedica un capítulo completo a los mensajes comerciales dirigidos a NNA, en primer lugar, con el fin de adecuar sus disposiciones a la Ley 1098 de 2006
Privacidad por diseño y por defecto	"Informar de forma clara en la web sobre los datos que se van a tratar y los mecanismos que se van a utilizar para ello, las finalidades del tratamiento por ejemplo instalar pantallas de verificación de edad"	"El artículo 25 del Reglamento aborda la privacidad desde el diseño y por defecto. (Reglamento (UE) 2016/679). Es relevante en la medida que el diseño de una aplicación, un sitio o servicio web se desarrolle cumpliendo con la protección adecuada y segura de la información y privacidad de las personas identificando y superando los defectos a que haya lugar en el proceso del	"Es un tema regulado por el Decreto 1413 de 2017 como medida preventiva de tratamiento adecuada de los datos personales de manera general".

Aspectos Relevantes	Estados Unidos (FTC)	Unión Europea (Grupo de Trabajo del Artículo 29)	Colombia
		sistema de información".	
Autoridad de revisión y control	"Federal Trade Comission"	"Agencia Nacional de Protección de Datos"	"Superintendencia de Industria y Comercio SIC"
Revisión y control de la norma	"Cada 5 años se realiza la revisión de la norma para evaluar su implementación y efectividad en la práctica"	"Se sujeta los cambios normativos al estudio técnico del grupo de trabajo del Reglamento Europeo de Protección de Datos Personales"	"Es un tema novedoso por regular"
Recomendaciones	Modificar definiciones tales como datos personales, operador, y sitio web o servicio online dirigido a menores Clarificar la información contenida en las políticas de privacidad Actualizar los mecanismos de consentimiento parental verificable Añadir disposiciones en materia de retención y supresión de datos	Reconocimiento en el ámbito escolar representación y protección por parte de Padres y Tutores legales. • Expedientes de alumnos. • No discriminación. •Protección en la comunicación de datos. • Solicitud de consentimiento para publicar resultados escolares confidenciales. • Consideraciones sobre la utilización de	Herramientas seguras de verificación de la edad y control parental Actualizar los mecanismos de consentimiento parental verificable Información clara y trasparente en el tratamiento de la información de menores Regular el modelo de privacidad de NNA desde el diseño y por defecto

Aspectos Relevantes	Estados Unidos (FTC)	Unión Europea (Grupo de Trabajo del Artículo 29)	Colombia
	Reforzar los requisitos exigidos a los códigos de autorregulación	datos biométricos para acceso al colegio. • Círculo cerrado de televisión CCTV. • Condiciones de salud. • Sitios web de los colegios. • Consideraciones sobre las fotografías y credenciales. • Grabaciones de audios y video con teléfonos celulares.	

Fuente: Creación basada en Ornelas, L., la legislación COPPA, GT29 Europa, Ley 1581 de 2012 y sus reglamentarios

Cada uno de estas regulaciones refleja un ámbito de aplicación distinto, a pesar de estar dirigidos a la protección de los datos personales de los NNA, atiendo de la edad de los menores; la normatividad de Estados Unidos frente a la protección de datos personales se aplica únicamente a los datos personales recabados online de menores de 13 años, la normatividad europea se dirige a los menores de 18 años y la normatividad colombiana señala que prohíbe el tratamiento de NNA salvo las excepciones legales.

Los objetivos de cada una de estas regulaciones se centran en los derechos ARCO que corresponden a la recolección, tratamiento, información y comunicación en línea que es recabada

por personas físicas o morales, y con la prevalencia a nivel europeo del establecimiento de los principios generales para la protección de los datos de los niños.

Ahora bien, frente a la información, se presentan distintos aspectos, como el reconocimiento de las nuevas tecnologías, aparatos inteligentes y nuevas tecnologías como un factor a tener en cuenta para una protección efectiva de los datos personales. Y a partir del comparativo se puede evidenciar el reconocimiento en menor o mayor medida de la inclusión de las nuevas tecnologías dentro de la vida cotidiana de las personas, por tal motivo todos estos modelos hacen mención de información en sitios web, aparatos inteligentes, redes sociales y medios electrónicos, el reconocimiento de la era tecnológica y su impacto en la sociedad es fundamental para la protección de datos personales.

La autorregulación es un aspecto destacado dentro de un adecuado modelo de protección de datos personales, por tal motivo es necesario precisar las similitudes, diferencias, enfoque, implementación propia de cada modelo frente a una perspectiva con los demás.

Se requiere técnicas de autocontrol o sistemas de autorregulación publicitaria, a través de las cuales se establezcan normas éticas y morales o códigos deontológicos que rijan la misma.[45]

En Estados Unidos se da importancia a la autorregulación por parte de la industria, esto se da a través de las buenas prácticas, en Europa se implementa de manera similar donde además de lo anterior se incluyen sanciones y medidas de ejecución, en el caso Colombia se adopta una postura similar todo ello a partir del enfoque de la responsabilidad demostrada.

[45] Algunas normas deontológicas que afectan la relación de la infancia y la publicidad prestando especial atención a la aparición del menor en mensajes comerciales en España serían las siguientes: convenio de autorregulación de las cadenas de televisión en relación con determinados contenidos referidos a la protección de la infancia y la juventud; código deontológico para la publicidad infantil en el sector juguetero. Méndiz A, Medina H. A. (2012) La representación de la infancia en la publicidad: panorama por el marco deontológico español. Revista Internacional de investigaciones de publicitarias. Universidad Complutense de Madrid. Madrid. Vol. 6,1.

Otro aspecto novedoso a destacar es la privacidad por diseño y por defecto, que es acogido por la protección de datos personales de NNA, es un aspecto propio de cada Estado, partiendo de la cultura de su nación, su avance tecnológico y normativo así como las necesidades que persigue, es decir, el avance normativo frente a un determinado asunto está dado por muchos aspectos, un Estado avanzado tecnológicamente tiene la necesidad de establecer diversos, medios, controles, entes de vigilancia y normatividad en torno ello, caso contrario, un Estado tecnológicamente poco avanzado, aquí su avance en esta materia no sería muy amplio ya que no tendría la necesidad de establecer una amplia regulación frente a ello.

La privacidad por diseño y por defecto surge en Colombia con la implementación del decreto 1413 del 2017, sin embargo, frente a los otras regulaciones este ha sido un tema de amplio recorrido y por lo que se persigue es el mejoramiento de la misma regulación mediante su revisión, por ejemplo en Estados Unidos donde cada 5 años se realiza la revisión de la norma para evaluar su implementación y efectividad en la práctica finalmente en Europa la revisión de la norma está sujeta al estudio técnico del grupo de trabajo del reglamento Europeo de protección de datos personales.

En el campo de la protección de los datos personales, la responsabilidad por parte de los operadores privados y público, está presente en la medida en que una afectación a los datos personales puede generar diversas repercusiones negativas a una persona dependiendo si afecta o no aspectos patrimoniales o derechos fundamentales; de esta manera el tratamiento abarca tiene por objetivo proteger los intereses de las personas, en cuanto a su honra, dignidad e intimidad que puedan ser vulnerados a través del acceso no autorizado a sus datos personales, divulgación no autorizada de los mismos, entre otros.

Figura 30. Las redes sociales.

Fuente: Imágenes Recuperado:https://www.google.com/search?q=proteccion+de+datos+personales+de+ni%C3%B1os&source=lnms&tbm=isch&sa=X&ved=0ahUKEwipvoP4ivPbAhWwt1kKHRcKARAQ_AUICigB&biw=1366&bih=635

El control y vigilancia está enmarcada en la responsabilidad demostrada o accountability que tiene su origen desde 1980 gracias a la Organización para la Cooperación y el Desarrollo Económico OCDE[46], por medio de las directrices relativas a la protección de la privacidad y los flujos transfronterizos de datos personales, introdujeron el concepto accountability, como primer instrumento en el ámbito supranacional que analiza en profundidad el derecho a la protección de datos de carácter personal y donde se recalcaba el rol del responsable del tratamiento como el llamado a implementar medidas dentro de la organización que permitieran cumplir con el resto de principios consagrados por dicho instrumento, “la obligación de un individuo o de una organización de rendir cuentas sobre sus actividades, aceptar responsabilidad sobre ellas y divulgar los resultados de manera transparente” (Superintendencia de Industria y Comercio, 2017).

[46] Guía para la implementación del principio de Responsabilidad Demostrada (Accountability), cuya elaboración se basó en OECD. Guidelines on the protection and transborder flows of Personal Data, 1980 y la Oficina de Privacidad de Canadá Y LA la Oficina de Privacidad e información de Columbia Británica

Para el caso colombiano el principio de responsabilidad demostrada, consiste en que una entidad que recoge y trata datos personales debe ser responsable por el cumplimiento efectivo de las medidas que se implementan en los principios de privacidad y protección de datos.

En el Decreto 1377 de 2013, introdujo en el sistema colombiano de protección de datos el criterio de la responsabilidad demostrada como una obligación en cabeza de los responsables del tratamiento. De igual manera se dispuso, "que los responsables deben ser capaces de demostrar, a petición de la superintendencia de industria y comercio, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2011" (2013).

Uno de los aspectos que destaca de esta norma, es aquella disposición por medio de la cual la Superintendencia de Industria y Comercio, en su calidad de autoridad nacional de protección de datos, tiene que tener en cuenta la existencia de políticas y medidas adecuadas en el momento de evaluar la imposición de una sanción.

Estas medidas deben ser adoptadas teniendo en cuenta los factores propios de la organización como su tamaño, su naturaleza jurídica, la naturaleza de los datos tratados, el tratamiento al cual son sometidos, así como su ocultamiento.

El artículo 27 del decreto 1377 de 2013, establece las políticas internas que se deben implementar a fin de garantizar el efectivo cumplimiento del derecho:

- En la organización debe existir una estructura administrativa que sea proporcional a la estructura del responsable para implementarlas.
- Se deben adoptar mecanismos internos que permitan desarrollar políticas que incluyan herramientas de implementación, entrenamiento y programas de educación.

- Implementación de procesos que permitan la atención de consultas y reclamos de los titulares.

La Superintendencia de Industria y Comercio (en adelante SIC) en su calidad de autoridad de protección de datos tiene como función la inspección, vigilancia y control del tratamiento de datos personales a nivel general con mayor énfasis en el sector empresarial, con el fin de grantizar el cumplimiento de la regulación en materia de los principios, derechos, garantías, medidas de seguridad y demás disposiones previstas en la Ley 1581 de 2012 a través de la Delegatura para la Protección de Datos Personales según la LEPDP y en virtud de la responsabilidad demostrada en el tratamiento de datos personales por parte de los responsables deben ser capaces de demostrar, a petición de la SIC que: “han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y el decreto 1377 de 2013, de una manera que sea proporcional a lo siguiente:

- La naturaleza jurídica del responsable y, cuando sea del caso, su tamaño empresarial, teniendo en cuenta si se trata de una micro, pequeña, mediana o gran empresa, de acuerdo con la normativa vigente.
- La naturaleza de los datos personales objeto del tratamiento.
- El tipo de tratamiento.
- Los riesgos potenciales que el referido tratamiento podrían causar sobre los derechos de los titulares (LEPDP, 2012, artículo 19)

Dentro de las funciones de la SIC descritas en la Ley 1581 de 2012 en materia de protección de datos personales se destaca:

“Velar por el cumplimiento de la legislación en materia de protección de datos personales.

Adelantar las investigaciones del caso, de oficio o a petición de parte y, como resultado de ellas, ordenar las medidas que sean necesarias para hacer efectivo el derecho de hábeas data.

Disponer el bloqueo temporal de los datos cuando, de la solicitud y de las pruebas aportadas por el Titular, se identifique un riesgo cierto de vulneración de sus derechos fundamentales, y dicho bloqueo sea necesario para protegerlos mientras se adopta una decisión definitiva.

Promover y divulgar los derechos de las personas en relación con el Tratamiento de datos personales e implementar campañas pedagógicas para capacitar e informar a los ciudadanos acerca del ejercicio y garantía del derecho fundamental a la protección de datos.

Impartir instrucciones sobre las medidas y procedimientos necesarios para la adecuación de las operaciones de los Responsables del Tratamiento y Encargados del Tratamiento a las disposiciones previstas en la presente ley.

Solicitar a los Responsables del Tratamiento y Encargados del Tratamiento la información que sea necesaria para el ejercicio efectivo de sus funciones". (Ley 1581, 2012, artículo 12).

La Superintendencia a través de la Dirección de Investigación de Protección de Datos Personales, ejercerá la vigilancia de los operadores, fuentes y usuarios de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países de la misma naturaleza, en cuanto se refiere a la actividad de administración de datos personales. Además, podrá ordenar la corrección, actualización o retiro de datos personales de una base de datos, cuando así se determine dentro de la investigación y, administrará el Registro Nacional Público de Bases de Datos.

La nueva legislación establece una serie de mecanismos preventivos en cabeza de los encargados o responsables del tratamiento de la información, para evitar el manejo inadecuado e indiscriminado de la información, entre ellos:

> “el aviso de privacidad, el procedimiento para obtener la autorización del titular previo al inicio del tratamiento, herramientas que garanticen condiciones de seguridad adecuadas para evitar la adulteración, pérdida, consulta, uso o acceso fraudulento sobre la información, medidas tecnológicas para proteger los datos personales y sensibles, manual interno de políticas y procedimientos para cumplir con la ley sobre protección de datos, elaborar las políticas del tratamiento de la información y suministrarlas al registro nacional de bases de datos, el cual está a cargo de la superintendencia de industria y comercio” (Pardo, 2012 pp. 18-20).

Finalmente se resalta las recomendaciones que cada uno de estas regulaciones de protección de datos personales de NNA presenta como reforzar la autorregulación, la presentación de información más clara y transparente, así como la creación de herramientas de verificación de la edad acompañadas de un control por parte de los padres.

Colombia, en materia de protección de los datos personales de carácter general cuenta con la Ley Estatutaria 1581 de 2012, y otros instrumentos normativos que regulan la materia de manera general, sin embargo, requiere de un marco legal que le permita ser considerado como un país con nivel adecuado de protección de datos personales respecto a las exigencias establecidas por estándares internacionales con respecto a seguridad de la información personal en las transferencias, transmisión internacional y la protección de los datos personales de NNA, en particular en redes sociales. Está en proceso de regulación las reglas mínimas para la difusión de información judicial en Internet, la transparencia de la información por parte de las entidades públicas en lo atinente a los datos sensibles y las decisiones individuales automatizadas de acuerdo a las Reglas de Heredia.

La adecuación del tratamiento de datos personales entorno a la privacidad de la información personal de NNA a los estándares internacionales ha sido progresiva de acuerdo a los principios

de protección y a las exigencias que implican la implementación de las TIC y el equilibrio con la garantía de los derechos de interés superior y protección integral.

Tabla 37.

Comparativo de los principios regulados en instrumentos internacionales de protección de datos personales y la normativa en Colombia

OCDE	**Convenio 108 CE-1981**	**Resolución 45/95 ONU**	**Resolución 95/46 CE**	**Colombia**
Limitación de recogida	Tratamiento leal y legítimo	Legalidad y lealtad	Leal y lícita	Legalidad
Calidad de datos	Calidad	Exactitud	Exactos	Veracidad o Calidad
Especificación de la finalidad	Finalidad	Especificación de la finalidad	Fin determinado explícito y legítimo	Finalidad
Limitación de uso	Proporcionalidad	No discriminación	Adecuados, pertinentes y no excesivos	Acceso y circulación restringida
Apertura	Conservación de datos	Acceso de la Persona interesada	Conservados en forma adecuada	Transparencia
Salvaguarda de seguridad		Seguridad	Seguridad	Seguridad
Participación individual		Autoridad garante	Autoridad garante	Libertad
Responsabilidad		Transferencias internacionales	Transferencias internacionales	Confidencialidad
Libre circulación y restricciones legítimas				Responsabilidad demostrada

Fuente: Creación propia basada en la normatividad de PDP.

El sistema jurídico colombiano acoge los principios del tratamiento de datos personales, regulados por los diferentes instrumentos normativos internacionales, destacando la concordancia

y armonización en su estructura por la dogmática jurídica y por ser pionero en materia de protección de datos personales como se evidencia en el capítulo segundo.

Respecto al Memorándum de Montevideo referente de protección de datos personales y la vida privada en las redes sociales en internet de NNA (2009) para orientar la construcción del marco legal sobre la protección de datos personales y la vida privada en las redes sociales en internet, en particular de NNA de los diferentes Estados Iberoamericanos; Colombia presenta avances frente a la normatividad en general. Al respecto se observa el panorama general sobre su cumplimiento:

Tabla 38.

Cumplimiento del Memorándum de Montevideo para el marco legal sobre la protección de datos personales y la vida privada en las redes sociales en internet de NNA en Colombia

Recomendaciones	Colombia
"Normativa nacional aplicable al sector público y privado"	Ley 1581 de 2012 – Dto 1377 de 2013
"Derechos y principios básicos reconocidos internacionalmente"	Ley 1581 de 2012 a nivel Nacional
"Mecanismos para la aplicación efectiva de la normativa (autoridad independiente)"	SIC – entidad adscrita el Ministerio de Comercio, Industria y Turismo
"Prohibición de tratamiento de datos personales del niño en la industria"	Ley 1581 de 2012
"Tratamiento de datos personales de adolescentes con mecanismos de controles parentales"	En proceso
"Proteger la vida privada es la característica general en todos los sistemas de comunicación"	En proceso
"Los cambios en el grado de privacidad del perfil de usuario debe ser sencillo y sin costo alguno"	En proceso
"Reglas de privacidad de las páginas web, servicios, aplicaciones, entre otros, deben ser explícitas, sencillas y claras, en un lenguaje adecuado para los niños y adolescentes	En proceso

Recomendaciones	Colombia
“Se debe proveer información sobre los pronósticos y finalidades para los cuales se utilizarán los datos personales, así como las transmisiones que se realicen a tercero”	Se requiere establecer los protocolos
“Se debe proveer información de las transmisiones que se realicen a terceros”	Decreto 1413 de 2017
“Se debe proveer información sobre la persona o personas responsables del tratamiento de la información”	Establecer el alcance
“Ofrecer un enlace a los parámetros de publicidad”	Decreto No. 1074 de 2015
“Aviso de que la red social ha preseleccionado los parámetros, si es así que pueden ser cambiados en todo momento según las preferencias de los NNA”	Establecer el alcance
“Cambio de los parámetros por defecto de los contenidos personales que puedan ser accesibles por los amigos y las redes que el usuario determine”	Establecer el alcance
“Publicidad de los perfiles de los usuarios según cada perfil debe estar contenida en la política de privacidad”	Decreto No. 1074 de 2015
“Evitar publicidad no adecuada para NNA”	Decreto No. 1074 de 2015
“Toda red social digital debe indicar de manera clara la razón que motiva el exigir ciertos datos personales y en particular, la fecha de nacimiento en el momento de inscripción y la creación de una cuenta”	Establecer el alcance
“Implementar mecanismos para la verificación fehaciente de la edad del niño para abrir una cuenta o acceder a determinado contenido”	Establecer el alcance
“Toda red social digital, sistema de comunicación o base de datos debería contar con formas de acceso a la información, rectificación y eliminación de datos personales, para usuarios o no usuarios, tomando en consideración las limitantes de la ley”	Decreto 1413 de 2017
“Política accesible a los usuarios en materia de conservación de la información”	Decreto 1413 de 2017
“Obligaciones de privacidad frente a terceros debe ser explicita, clara y visible”	Decreto 1413 de 2017
“La indexación de información de NNA está prohibido en todas sus formas. Las cuentas de menores de edad deben ser "privadas por defectos inaccesibles" a través de buscadores de la red (Comisaria Europea para la Sociedad de la Información)”	Establecer los límites

Recomendaciones	Colombia
"En caso de los adolescentes estos deben autorizar de forma expresa la indexación de sus datos mínimos"	Establecer el alcance
"Prohibición de instalar aplicaciones sin ser autorizadas expresamente por el usuario"	Establecer el alcance
"Medidas de índole técnica y operativa para garantizar la seguridad de la información en particular la integridad, disponibilidad y confidencialidad"	Establecer el alcance

Cumple (regulado)
En proceso de cumplimiento
No cumple (vacío normativo)

Fuente: Creación propia con base en el Memorándum de Montevideo[47]

Para Colombia, las directrices y recomendaciones internacionales se fueron materializando primero con la norma estatutaria Ley 1581 de 2012 en su artículo 7 en cuanto proscribe el tratamiento de los datos de los NNA, de manera restrictiva y ya con el Decreto reglamentario que reconoce un mayor grado de autonomía y habilitación en consideración a la jurisprudencia de la Corte Constitucional[48] en cuanto a la privacidad y seguridad de su información personal. (Decreto 1377 , 2013).

Sin embargo requiere de mecanismos de protección necesarios para garantizar un nivel adecuado de tratamiento de la información personal de los niños en la era digital relacionados con la legalidad y verificación del consentimiento, códigos de conducta, fortalecimiento de la autorregulación, programas de gestión integral de datos, estrategias pedagógicas enfocadas a

[47] Basado en Ornelas, L. (2010), "El derecho de las niñas, niños y adolescentes a la protección de sus datos personales: Evolución de derechos y su exigencia frente a las redes sociales." Protección de datos personales. Compendio de lecturas y legislación Alonso Editores (pp. 171 – 173).

[48] Corte Constitucional Sentencia C-748 de 06 de octubre de 2011, por medio de la cual se hace control de constitucionalidad del proyecto de "Ley Estatutaria No. 184 de 2010 del Senado y 046 de 2010 de la Cámara por medio del cual se dictan disposiciones generales para la protección de datos personales".

promover la prevención de riesgos y adecuadas a la edad de los niños, responsabilidad proactiva de los operadores y responsables del tratamiento respecto al diseño por privacidad y por defecto enfocados a la protección del interés superior del niño.

Hoy, apremia mayores esfuerzos normativos y administrativos la protección del interés superior del niño en la sociedad de la información y la tecnología; y por lo tanto, se debe avanzar en estudios investigativos de índole jurídico por parte de la academia dada su especificidad así como por parte de los entes gubernamentales como el Ministerio de las Tecnologías de la Información y las Comunicaciones, el Ministerio de Educación, el Instituto Colombiano de Bienestar Familiar y la Policía Nacional para destacar; así como las iniciativas de seguimiento y control de laboratorios de observación tales como: el observatorio de investigación en Colombia: "Observatorio Habeas Data" Ciro Angarita de la Universidad de los Andes, el cual tiene como objetivo el estudio e intercambio de teorías relacionados con el papel del derecho en la sociedad de la información y conocimiento, incluyendo Internet, protección de datos personales y las redes sociales digitales, la prevención de riesgos con ocasión de las inadecuadas prácticas que afectan la garantía de los derechos fundamentales y los impactos negativos que las mismas conllevan en la vida futura. (Corte Constitucional, Sala Plena, Sentencia C-748, 2011).

Para la Corte Constitucional de Colombia y el Memorándum de Montevideo, los Estados debe intervenir en el acceso adecuado a las redes sociales por parte de los NNA teniendo en cuenta dos recomendaciones las cuales son:

La primera recomendación que se establece es el reconocimiento por parte del Estado y las entidades educativas frente al tutor o progenitor del menor y su responsabilidad en el uso de los datos personales del niño, niña o adolecente.

La segunda recomendación, la cual es prohibir la publicación, la recopilación y el tratamiento de los datos personales sin la autorización del titular de esos datos, “no permitir la recopilación, tratamiento, difusión, publicación o transmisión a terceros de datos personales, sin el consentimiento explícito de la persona concernida. Se debe restringir el uso de la información recogida con cualquier otra finalidad diferente a la que motivo su tratamiento, y en especial a la creación de perfiles de comportamiento”. (Corte Constitucional, Sala Octava de Revisión, Sentencia T-260, 2012).

Así mismo, se establece la necesidad de regular mecanismos de control parental para los datos personales en donde el titular sea un niño, niña o adolecente:

“En el caso de niñas y niños se debe considerar la prohibición de tratamiento de datos personales. En el caso de adolescentes se deberá tener en cuenta los mecanismos de controles parentales de acuerdo a la legislación de cada país.” (Corte Constitucional, Sala Octava de Revisión, Sentencia T-260, 2012).

De igual forma, en esta misma sentencia se establece que las redes sociales deben ponderar el lenguaje sencillo para facilitar el entendimiento de los menores de edad; por lo que “toda red social digital debe indicar explícitamente en la parte relativa a la publicidad contenida en su política de privacidad, sobre los anuncios publicitarios e informar claramente, en especial a los menores, sobre el hecho de que las informaciones personales de los perfiles personales de los usuarios se emplean para enviar publicidad según cada perfil”. Así mismo se propone, que toda red social debe establecer la razón de solicitar datos privados.

“Toda red social digital debe indicar de manera clara la razón que motiva el exigir ciertos datos personales, como la fecha de nacimiento y la fecha de creación de la cuenta (..) Por su parte y para garantizar el derecho del habeas data, se constituye que Toda red social digital, sistema de

comunicación o base de datos deberá contar con formas de acceso a la información, rectificación y eliminación de datos personales para usuarios o no usuarios, tomando en consideración las limitantes de la ley.” (Corte Constitucional, Sala Octava de Revisión, Sentencia T-260, 2012).

La Corte advierte, que aunque no es constitucional impedir el acceso al internet por parte de menores de edad, en especial a las denominadas redes sociales, este acceso si se puede limitar teniendo en cuenta dos factores relacionadas con el menor los cuales son; la edad y la madurez y estos se pueden definir de la siguiente manera:

“La edad y madurez del menor van a determinar el cumplimiento de uno de los principios rectores en materia de protección de datos personales, como es el referente a la libertad, el cual es entendido de la siguiente manera:

Principio de libertad: el tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.” (Corte Constitucional, Sala Octava de Revisión, Sentencia T-260, 2012).

Ahora bien, con la entrada en vigencia de la Constitución Política de 1991, al ser la Constitución norma de normas (Constitución Política de 1991, Consejo Superior de la Judicatura Art. 4) y al estar jerárquicamente en un nivel superior a las normas tipo ley, la vigencia de todas las normas preexistentes en el ordenamiento jurídico, quedan supeditadas al respeto de los principios y postulados constitucionales, de tal suerte que por vía de acciones constitucionales de ciudadanos que consideran violatorio del derecho a la igualdad algunas normas de protección de datos personales, entre ellas las relativas al derecho a la seguridad jurídica de los padres en el cuidado de sus hijos en la etapa de niñez, la Corte Constitucional colombiana se ha pronunciado (Corte

Constitucional, Sala Plena, Sentencia C-283, 2011) para afianzar el cumplimiento de los estándares internacionales que garanticen la prevalencia de los derechos de los niños, niñas y niñas en virtud del interés superior.

Seguidamente, la Corte establece un nuevo momento de posible riesgo para los derechos fundamentales tales como:

> "los derechos de los usuarios pueden verse afectados además con la publicación de contenidos e información en la plataforma –fotos, videos, mensaje, comentarios a publicaciones de amigos"… "Pues los alcances sobre la privacidad de los mismos pueden tener un alcance mayor al que consideró el usuario en un primer momento, ya que estas plataformas disponen de potentes herramientas de intercambio de información, de capacidad de procesamiento y de análisis de la información facilitada por los usuarios." (Corte Constitucional, Sala Octava de Revisión, Sentencia T-260, 2012).

Posteriormente, se menciona la potencial vulneración de los derechos fundamentales, en cuanto *las redes sociales* pueden autorizar a los motores de búsqueda de mostrar el perfil con datos personales.

> "Otro de los riesgos señalados en el texto mencionado hace referencia a que en ocasiones las redes sociales permiten a los motores de búsqueda de internet indexar en sus búsquedas los perfiles de los usuarios, junto con información de contactos y perfiles de amigos, lo que puede llegar a afectar la privacidad del usuario, la protección de sus datos y dificultará el proceso de eliminación de los mismos del internet". (Corte Constitucional, Sala Octava de Revisión, Sentencia T-260, 2012).

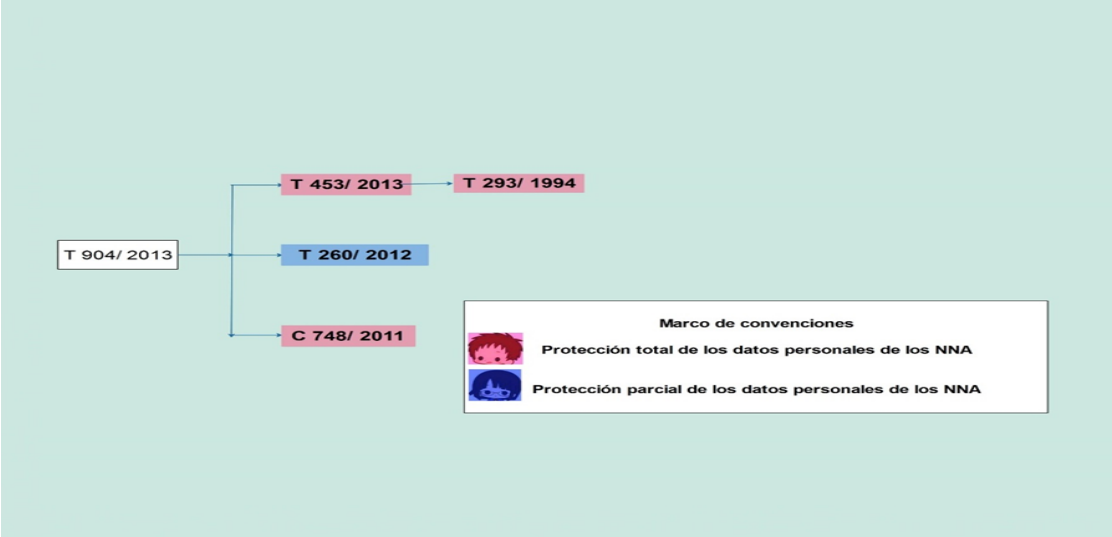


Figura 31. Telaraña jurisprudencial sobre la protección de datos personales de NNA en el ámbito digital

Fuente: Creación propia

Finalmente la Corte dentro de esta misma sentencia señala:

> "el peligro inminente que sufre los derechos a la intimidad y el habeas data, en cuanto las redes sociales almacenan la información intima de la persona aun cuando esta ha cancelado la cuenta en dicha red social, a pesar de la cancelación de la cuenta, en ocasiones, la información intima del usuario puede continuar publicada y ser accesible desde los perfiles de otros usuarios, además de indexada y almacenada en la caché de los distintos buscadores existentes en internet". (Corte Constitucional, Sala Octava de Revisión, Sentencia T-260, 2012)

En caso de los menores de edad, la Corte señala diversos motivos que pueden ocasionar la vulneración de sus derechos entre ellos, la corte advierte la vulneración que pueden sufrir los menores frente a la protección de sus datos personales pues estos son vulnerables:

> “la proliferación de la información personal gráfica de los menores, ya sea publicada por ellos mismos o por terceros con desconocimiento de los riesgos a los cuales pueden ser expuestos.” (Corte Constitucional, Sala Octava de Revisión, Sentencia T-260, 2012).

La Corte Constitucional, advierte que la única forma de evitar estas vulneraciones contra los derechos de los menores de edad en especial los niños y niñas, es la constante vigilancia de los padres y que estos mismos aprendan el funcionamiento y el reglamento de los sitios en línea en especial las redes sociales.

Otro de los primeros acercamientos a un estándar de protección de datos personales que tiene en consideración Colombia son las “Reglas de Heredia”: Recomendaciones para los poderes judiciales para la divulgación de la jurisprudencia en los países de América Latina que corresponden a reglas mínimas para la difusión de información judicial en Internet, la cual ha sido estudiada por el Centro de Documentación Judicial – CENDOJ – del Consejo Superior de la Judicatura, e ilustra el alcance de la publicación de información “jurisprudencia” en internet en atención al balance entre la trasparencia y la privacidad.

El “Estudio técnico jurídico para determinar la aplicación de las normas de protección de datos de carácter personal en las bases de datos administradas por el centro de documentación judicial CENDOJ” (2013), puntualiza su transformación frente a los nuevos desarrollos tecnológicos y los desafíos del derecho con una mirada de prevención y gestión del riesgo, con el fin de lograr un equilibrio entre transparencia, acceso a la información pública y derechos de privacidad e intimidad, de acuerdo con los estándares europeos más exigente y riguroso con modernas tecnologías de la información propias del internet de las cosas en la era digital.

Al respecto, se promulga de manera general la Ley 1712 de 2014 que regula el derecho de transparencia y accesibilidad a la información pública nacional, así como precedentes

jurisprudenciales[49] que desarrollan la interpretación de la controversia entre el derecho a la intimidad, buen nombre y habeas data frente a los derechos de libertad, acceso y la transparencia en la publicación de la información. (2013 p.1).

El alcance de la accesibilidad de la información de los menores de edad en el marco de la responsabilidad penal para adolescentes, se muestra respecto a la publicidad de las sentencias que no constituyen un antecedente judicial y como lo refiere la Regla de Heredia No. 5:

> "Regla 5. Prevalecen los derechos de privacidad e intimidad, cuando se traten datos personales que se refieran a niños, niñas, adolescentes (menores)… o cuando se trate de datos sensibles o de publicación restringida según cada legislación nacional aplicable o hayan sido así considerados en la jurisprudencia emanada de los órganos encargados de la tutela jurisdiccional de los derechos fundamentales" (2013, R. 5).

Los registros de investigación y juicio penal están amparados por la reserva, salvo en aquello eventos que sean requeridos por las autoridades judiciales competentes como mecanismo de investigación y de restablecimiento de los derechos de manera proporcional y eficiente (Minjusticia, 2015).

La Superintendencia de Industria y Comercio ha emitido resoluciones en materia administrativa e investigativa con el fin de adelantar los procedimientos necesarios para garantizar la protección del derecho a la protección de datos personales en este ámbito, como es la Resolución 47.868 de 26 de julio de 2016, respecto al derecho a la rectificación de antecedentes judiciales que integra el sistema de información de la Policía Nacional, en virtud del principio de veracidad consagrado en el artículo 4 b) de la Ley l581 de 2012 por la cual ordenó actualizar los registros: "se actualice la información que se encontraba registrada en la base de datos del sistema de información sobre

[49] Corte Constitucional Sentencia C-274 de 2013, Sentencia T-020/14, Sentencia T-277/15.

antecedentes y anotaciones (SIAN) de la policía nacional de Colombia.” (Agencia Española de Protección de Datos, 2017, p.52).

3.4.2. Estándares Iberoamericanos para el tratamiento de datos personales de los niños

Los Estándares Iberoamericanos de protección de datos personales responden a una proclama internacional de los Estados por reglamentar el esfuerzo comunitario que permita salvaguardar los derechos de las personas en el marco de la privacidad frente al uso inadecuado de las TIC; por lo tanto considera:

> “Estando conscientes acerca de los riesgos potenciales que pueden derivarse en la esfera de las personas físicas con motivo del tratamiento de sus datos personales a gran escala efectuado por parte de organismos públicos y derivados y, en particular, teniendo en cuenta la especial vulnerabilidad de las niñas, niños y adolescentes, quienes demandan de garantías adecuadas y suficientes de protección frente a usos indebidos o arbitrarios de su información personal, preservando de esta manera su interés superior, el libre desarrollo de su personalidad, su seguridad y otros valores que son objeto de máxima protección por parte de los Estados Iberoamericanos”. (Red Iberoamericana de Protección de Datos Personales, 2017).

Los principios contenidos en las disposiciones en materia de protección de datos personales de NNA establecidas por los Estados Iberoamericanos/2017 en contexto con las disposiciones del Reglamento Europeo 679/2016 y en la Ley Estatutaria Colombiana 1581 de 2012, guardan armonía a pesar de los diversos enfoques. Con relación a los Estándares Iberoamericanos hay concordancia frente a algunos principios, aunque, se debe incorporar mayor claridad respecto a los

principios de: *legitimación, lealtad, transparencia, finalidad, proporcionalidad, calidad, responsabilidad, integridad, seguridad y confidencialidad*.

Tabla 39.

Comparativo de los principios de la protección de los datos personales UE, Iberoamérica y Colombia

REGLAMENTO 679/2016	***Estándares Iberoamericanos (2017)***	***COLOMBIA (2012)***
Licitud, ***lealtad*** *y transparencia*	***Lealtad,*** *Ilicitud*	*Legalidad*
Exactitud	*Calidad*	*Veracidad o Calidad*
Limitación de la finalidad	*Finalidad*	*Finalidad*
Minimización de datos	***Proporcionalidad***	*Acceso y circulación restringida*
Limitación del plazo de conservación	*Transparencia*	*Transparencia*
Integridad *y confidencialidad*	*Seguridad y Confidencialidad*	*Seguridad y Confidencialidad*
Responsabilidad proactiva	***Legitimación***	*Libertad*
	Responsabilidad	*Responsabilidad demostrada*

Fuente: Creación propia

Los alcances y el contexto de cada principio, concretamente se señala frente al principio de transparencia, el cual se centra en la obligación que tiene el responsable del tratamiento de los datos personales de informar al titular de los mismos la gestión que se le dará a estos datos con el propósito que pueda tomar decisiones informadas, el principio de finalidad señala que el responsable del tratamiento no podrá tratar los datos personales para una finalidad distinta de la que motivo el tratamiento original, el principio de responsabilidad señala que el responsable del tratamiento mantendrá todas las medidas, físicas, administrativas y técnicas para garantizar la integridad, confidencialidad y disponibilidad de los datos personales, finalmente el principio de

confidencialidad establece que el responsable tiene la obligación de implementar medidas y controles frente a los terceros que intervienen en el tratamiento de datos personales para que se respete la confidencialidad de los mismos.

De otra parte, se requiere establecer mayores límites respecto a la adecuación a los principios de legalidad, exactitud, limitación de la finalidad, minimización de datos, limitación del plazo de conservación, integridad y confidencialidad y responsabilidad proactiva cuya regulación innovadora parte del Reglamento General de Protección de Datos de la Unión Europea 679/2016 (en vigor 2018) y que destaca una especie de mayoría de edad digital fijada en los 13 años, considerando lícito la utilización de datos de menores únicamente si el menor tiene una edad superior y requiriéndose la autorización de los padres o tutores tanto para darse de alta en la red como para poder operar en la misma cuando el niño es menor a esa edad, lo que parece conforme con el grado de madurez de los menores de edad en el entorno digital. Junto a ello el nacimiento del "derecho al olvido" en internet surgido de la ST-JUE de 13 de mayo de 2014 permite la eliminación de contenidos de los menores independientemente de su edad por parte de los padres durante su minoría de edad considerando responsables no solo a los creadores de contenidos sino también a los buscadores, con el tratamiento jurídico de responsabilidad demostrada en forma solidaria. Se requiere normas globales de protección de datos personales que armonicen los principios y estándares internacionales en el tratamiento.

De otra parte, la regulación colombiana sobre los principios de protección de datos personales requiere del desarrollo de los principios de lealtad, proporcionalidad, legitimación y responsabilidad proactiva. Dado que el principio de la responsabilidad proactiva se traduce en la obligación de las empresas de implementar una serie medidas organizativas y técnicas que

garanticen el tratamiento de los datos personales de forma diligente y dando cumplimiento a los lineamientos contenidos en el Reglamento General de Protección de Datos (RGPD).

Ahora en razón de este principio las organizaciones deben:

- Realizar una identificación de los datos de carácter personal que son tratados durante el normal desarrollo de sus actividades.
- Identificar el uso que hace de estos datos personales.
- Identificar el tipo de tratamiento al que son sometidos los datos personales.

Es síntesis, este principio se basa en atribuir a los agentes que realizan el tratamiento de datos personales una responsabilidad proactiva, en vez de una reactiva, es decir, se debe incrementar la diligencia con carácter previo con el propósito de evitar resultados negativos dentro del tratamiento de los datos personales, ahora este actuar se debe poder acreditar, por lo cual, una mera actuación formal no será aceptable. De esta manera, se busca el actuar diligente del responsable del tratamiento de los datos personales, evitando los riesgos derivados de ello y disponiendo de la capacidad de acreditar su diligencia.

Los Estándares Iberoamericanos de Protección de Datos Personales recogen la proclama internacional de proteger el interés superior del niño, la pedagogía jurídica de los NNA en diversos ámbitos del derecho y las nuevas tecnologías, legalidad en la obtención del consentimiento y principio de transparencia frente a lo cual Colombia cumple parcialmente.

Tabla 40.

Estándares Iberoamericanos del tratamiento de datos personales de NNA en Colombia

Aspecto	Estándar	Colombia
Interés superior de los NNA	El privilegio por la protección del interés superior de los NNA, conforme a la Convención sobre los Derechos del Niño y demás instrumentos internacionales que busquen su bienestar y protección integral.	Ha identificado mayores sectores de regulación para la protección integral y el interés superior de NNA. Aunque existe ausencia de un sistema integral de privacidad de la información personal niños.
Formación académica de los NNA	La promoción en la formación académica de los NNA, el uso responsable, adecuado y seguro de las tecnologías de la información y comunicación y los eventuales riesgos a los que se enfrentan en ambientes digitales respecto del tratamiento indebido de sus datos personales, así como el respeto de sus derechos y libertades	En proceso de desarrollo: fase inicial de formación por parte de la Superintendencia de Industria y Comercio, el Ministerio de las TIC y el Ministerio de Educación
Legalidad en la obtención del consentimiento	El responsable obtendrá la autorización del titular de la patria potestad o tutela, conforme a lo dispuesto en las reglas de representación previstas en el derecho interno de los Estados Iberoamericanos, o en su caso, solicitará directamente la autorización del menor de edad si el derecho interno de cada Estado Iberoamericano ha establecido una edad mínima para que lo pueda otorgar directamente y sin representación alguna del titular de la patria potestad o tutela. (Capítulo I).	Falta desarrollo normativo sobre la veracidad de la legalidad del consentimiento en internet y por parte de los intermediarios de la información
Principio de transparencia	Reconocimiento especial del principio de transparencia en cuanto a la información proporcionada dada a los NNA como titulares de la información debe ser suficiente y fácilmente accesible, así como redactarse y estructurarse en un lenguaje claro,	Se requiere mayor exigencia del principio de Transparencia respecto a la información de NNA

Aspecto	Estándar	Colombia
	sencillo y de fácil comprensión para los titulares a quienes va dirigida, especialmente si se trata de niñas, niños y adolescentes. (Capítulo II).	

Fuente: Creación propia

Colombia ha avanzado en la construcción de una normativa de carácter general y sectorial, aunque se requiere mayor esfuerzo de regulación en aspectos tales como: formación académica de los NNA, legalidad en la obtención del consentimiento y el principio de transparencia, limitación de la finalidad, lealtad y licitud en el tratamiento de sus datos personales.

Atendiendo las consideraciones del reglamento modelo de protección de datos Europeo, la legislación COPPA de Estados Unidos, la Convención de los Derechos del niño, el Código de Infancia y la Adolescencia de Colombia, las recomendaciones del Memorándum de Montevideo y los Estándares Iberoamericanos de protección de datos personales, es importante la juridificación y prevención de los riesgos propios de la era digital respecto al derecho a la protección de datos personales de la generación interactiva más joven: Los niños. Para tal efecto se requiere:

- Sistema de autorregulación y marco normativo que se traduzcan en códigos deontológicos elaborados de manera responsable por cada operador del tratamiento de datos, con el control de la entidad de vigilancia.
- Diseñar normas teniendo en cuenta la opinión de las niñas, niños y adolescentes, en lo que se refiere el tratamiento de su información personal en internet de tal manera que su libre expresión y participación pueda ser escuchada y valorada.
- Madurez suficiente para tratar sus datos determinar la edad (13 años Reglamento Europeo)
- Imposibilidad de obtener datos de los integrantes de la unidad familiar no utilizar internet para afectar la privacidad de terceros.

- Verificación de edad: Problema aplicabilidad de los operadores de la información de servicios para determinar la capacidad de verificar que efectivamente un menor es menor, el menor tiene esa edad.
- Faltan mayores herramientas tecnológicas seguras. En principio hay herramientas para verificar que son mayores porque tienen una firma electrónica o porque respecto a la autorización para el juego y la compra de licor en Estados unidos y Canadá hay terceros de confianza en los cuales uno se registra para mostrar que es mayor de edad pero no sucede lo mismo en el caso de menores en este caso el Estado plantea un tipo de base de datos que pueda establecer respuestas que da el niño de sí o no, fecha tal que puedan identificar la identidad del menor como por ejemplo un número de identificación único, para así los operadores de los datos puedan tener control sobre el registro.
- Información clara, las políticas de privacidad de los entornos de internet una red social o de un servicio donde medie un contrato y las políticas de privacidad son difíciles de entender como el caso de una hipoteca y para de los menores más aún de acuerdo a su edad y capacidad de comprensión, que permita la transparencia en el tratamiento de sus datos. Los expertos en privacidad lo que esperan es que se reivindican las normas y su operatividad se cumpla en todos los ámbitos como por ejemplo la geolocalización.
- Seguimiento y acompañamiento de la responsabilidad parental, es decir el control por medio de herramientas que cumplen una función en determinadas edades, por ejemplo, nos preguntamos: ¿existe un control para manejar moto por parte de los menores? Es decir, hay controles parentales sin educación en valores, ¿más aún los padres están educados en valores? ¿Le dedica tiempo a su hijo para acompañarlo en internet?.

- Compromiso de los poderes públicos: Se requiere de recursos y capacidad para la formación de docentes especialistas en el tema, modificación de planes de estudio, elaborar manuales para la formación de los menores en materia de privacidad con el fin de formarlos integralmente.
- La infancia en red sin riesgos mediante la privacidad por diseño y por defecto.
- Gobernanza de la protección de datos personales del niño: informes de evaluación y rendición de cuentas.
- Estrategias pedagógicas y jurídicas del sistema de educativo frente a la accesibilidad adecuada de las TICs, la autorregulación y la protección de los datos personales y la privacidad de NNA en el marco de la prevención integral y la garantía del interes superior.

Capítulo IV: Medidas Proactivas de Gestión Integral de Datos Personales de Niños, Niñas y Adolescentes

Este capítulo presenta medidas proactivas de seguridad del tratamiento de los datos personales frente al nivel de adecuación del régimen jurídico de protección de datos personales de NNA a los estándares internacionales, así como la propuesta de creación de un modelo integral de protección de datos personales dirigido a garantizar los derechos de los niños en Colombia, con base en la Convención de los derechos del niño, los "Estándares de Protección de Datos Personales de los Estados Iberoamericanos", las tendencias del Reglamento (EU) 2016/679 del Parlamento Europeo y del Consejo y demás instrumentos de regulación acordes con la protección de la dignidad humana de los derechos de los NNA, tanto en el ámbito preventivo y reactivo.

Una vez analizado el marco jurídico para la protección de datos en Colombia, se identifica la necesidad de avanzar en el ejercicio efectivo de la privacidad en aspectos tales como la veracidad de la legalidad del consentimiento del titular, el principio de accountability y programas integrales de gestión de datos (PIGDP) en las entidades públicas y privadas, el derecho de desindexación, el uso de tecnologías de vigilancia, los desafíos del internet de las cosas y el uso de big data, escenarios todos que ameritan mayor intervención del Estado en gran medida cuando estamos frente al interés superior del niño.

Colombia, es uno de los países que acogió de manera progresiva en su ordenamiento jurídico la protección de datos personales de NNA como se analizó en el capítulo anterior, sin embargo, la adecuación a los estándares internacionales evidencia la urgente intervención del Estado para estructurar e implementar un modelo integral de protección de datos personales de NNA, en

equilibrio a los requerimientos de la digitalización y la garantía de los derechos humanos. El modelo integral de protección de datos personales de NNA, incluye la identificación de las variables, su dinámica sistémica, las causas y consecuencias que inciden y se derivan de la vulneración de la información personal de los NNA, así como las recomendaciones frente a las medidas preventivas y de protección acordes con los principios de protección integral, interés superior, corresponsabilidad y perspectiva de género.

4.1. Fundamento teórico

Frente a las múltiples situaciones de bullying en las redes sociales, vulneración del derecho a la intimidad, honor, libertad de expresión, perfilación de los datos con fines comerciales sin el consentimiento de los niños o sus representantes legales, los menores al momento de navegar por internet, requieren de la apropiación del conocimiento tecnológico, de acuerdo a su grado de maduréz, capacidad y autonomía para comprender y darle significado a la información apropiada para su edad. Y facilitar el empoderamiento del conocimiento tecnológico para comprender el mundo del internet como un espacio que además de ser sistémico, se constituye en un espacio privado y público de protección de los derechos humanos.

Figura 32. Menores y protección de datos en redes sociales
Fuente: CONACYT, Centro de investigación e innovación en tecnologías de la información y la comunicación Recuperado: https://centrosconacyt.mx/objeto/menoresyredes/ (2018)

Este panorama de universalidad y digitalización del conocimiento genera grandes preocupaciones en torno a la juridificación de la protección y seguridad de la información personal en las redes sociales de niños, niñas y adolescentes; que expresa la necesidad de crear e implementar las políticas de tratamiento de los responsables y encargados, las transferencias de datos personales, las normas corporativas vinculantes y la responsabilidad demostrada, entre otros (Ley Estaturaria 1581, 2012).

Igualmente, se han definido los lineamientos y términos para garantizar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones, con el fin de contribuir con la construcción de un Estado más eficiente y transparente y una sociedad cada vez más incluyente.

Es así que, el sistema informático, está conformado por un conjunto de partes en las que se establece una forma de relación que las articula en la unidad que es precisamente el sistema" (Aracil y Gordillo, 1995, p. 11). Es decir, las plataformas electrónicas requieren la interacción con los usuarios, a través de la información o datos personales, la cual posibilita el acceso a las diversas plataformas electrónicas a las que acceden los menores, las cuales cuentan con una regulación o normatividad para proteger la privacidad y la información personal como bien jurídico tutelado por la Ley 1273 de 2009, la cual se ha denominado "de la protección de la información y de los datos" de carácter individual o colectivo y la seguridad en los medios informáticos, que con posterioridad es superada por la regulación de la Ley 1581 de 2012, en un radio de protección más amplio.

A través, de este modelo de gestión datos se busca analizar la protección de datos personales en el ordenamiento jurídico colombiano, con el objeto de comprender su dinámica sistémica y de esta manera evaluar cuáles son las causas y consecuencias que inciden y se derivan del ejercicio o de la concreción del derecho.

En el tratamiento jurídico de los datos personales online de NNA, se definen cuatros variables que pueden ser determinantes en el tratamiento preventivo. La primera es la protección de la información, la segunda es la seguridad de su información personal de la tercera es la probabilidad de afectación de la información personal de NNA, y la última es la implementación de modelo de gestión integral de datos online para NNA. Cuando comienza a decrecer algunas de estas variables o cuando las oportunidades aumentan, ignorar la ley se vuelve mucho más atractivo para el posible infractor (Ensayos Sobre Política Económica, Vol. 27, Núm. 60, Edición diciembre 2009, p. 85).

Esto se puede evidenciar de manera causal en la **figura 17.**

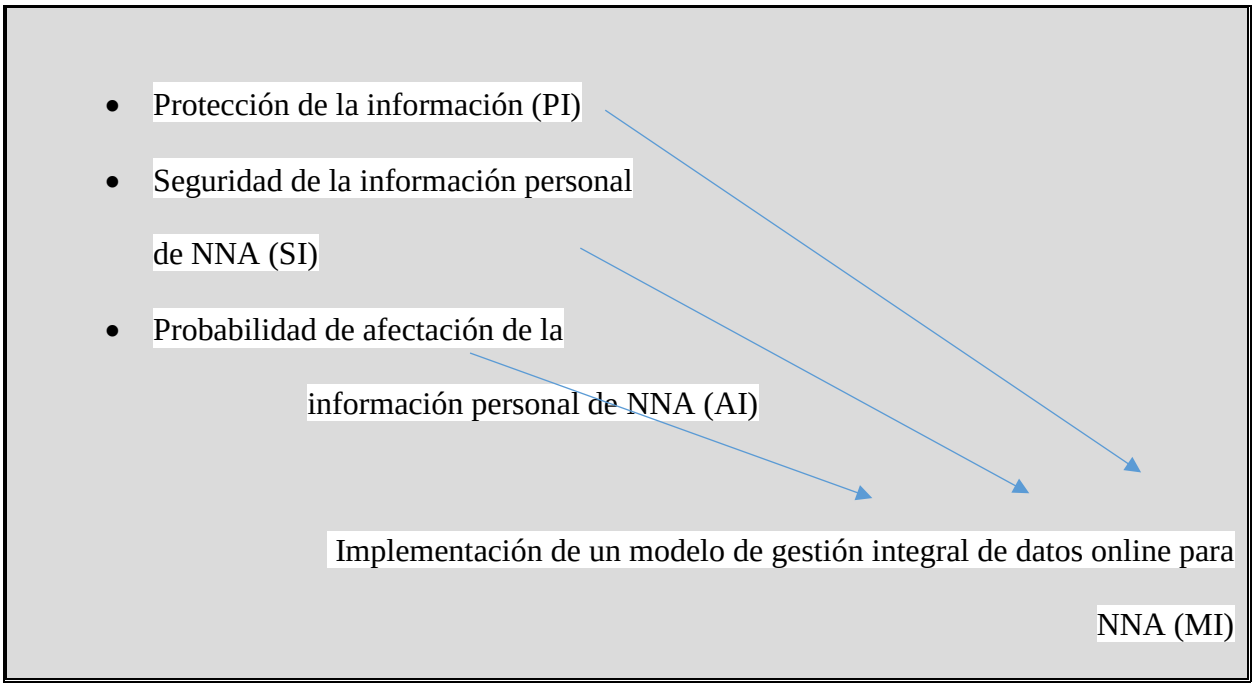


Figura 33. Variables de la protección de datos personales de NNA

Fuente: Creación propia

Es así que, el sujeto activo al violar los datos personales o realizar la suplantación de sitios web para capturar datos personales, reconoce tanto el beneficio como las consecuencias de su accionar delictivo. Así como la necesidad de capacitarse para capturar datos personales con la idea de no dejar rastro alguno en la Web, para no ser descubierto.

De otra parte, existe la necesidad de implementar medidas de seguridad en equilibrio con la privacidad desde su diseño y arquitectura mediante las cuales se reduzca la consumación de actos delictivos por el inadecuado uso de los datos personales y suplantación de sitios web para capturar datos personales, y es así que esta se convierte en una de las causas y consecuencias que inciden y se derivan de la realización o de la concreción de un delito informático.

4.2. Política para la ciberseguridad y ciberdefensa de datos personales de los niños

El Consejo Nacional para la Política Económica y Social estableció los lineamientos de política en ciberseguridad entendido como la “capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética” y ciberdefensa entendida como la “capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la soberanía nacional” lineamientos orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país. (CONPES, 3701, 2011).

Se requiere hacer una estrategia nacional segura basada en la normatividad de la seguridad digital y un diagnóstico que recoja “la problemática central y la capacidad actual del Estado para enfrentar las amenazas cibernéticas, las debilidades y al respecto no existe una estrategia nacional

segura. A partir de ello, se establecen los lineamientos que permitirán desarrollar políticas de prevención y control, ante el incremento de amenazas informáticas".

Colombia, no es ajena en la implementación de acciones relacionadas con la protección de datos personales en el marco de la Política Nacional de Seguridad Digital, aunado a la política de ciberseguridad y ciberdefensa, la cual la ha venido reconociendo el Consejo Nacional de Política Económica y Social y el Departamento Nacional de Planeación a partir del CONPES 3854 del 11 de Abril de 2016, con el fin de administrar el riesgo, como uno de los pilares de la seguridad digital que permita fortalecer las capacidades para identificar, gestionar, tratar y mitigar los riesgos de ciberseguridad que se presenten en las diferentes actividades socioeconómicas en el entorno digital.

Así mismo, el CONPES 3854 de 2016 establece la Política Nacional de Seguridad Digital[50] que se proyecta implementar durante los años 2016 a 2019 para que en el 2020, la economía del país mejore ostensiblemente (307.000 nuevos empleos y crecimiento del 0.1% del PIB) basado en:

> "fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el País". (CONPES 3854, 2016 – No. 5.1).

De acuerdo con la naturaleza y el sector económico desarrolla un modelo de gestión de riesgos de seguridad digital (en adelante MGRSD) encaminado a:

[50] El Consejo Nacional de Política Económica y Social de la República de Colombia, Ministerio de tecnologías de la información y las comunicaciones, Ministerio de Defensa Nacional, Dirección de Inteligencia y Departamento Nacional de Planeación. Recuperado de: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

> “alcanzar beneficios sociales y económicos, proveer servicios esenciales, operar infraestructuras críticas, preservar los derechos humanos y los valores fundamentales y proteger a las personas frente a las amenazas de seguridad digital”. (CONPES 3854, 2016. p. 4).

Así como, las recomendaciones y las mejores prácticas de uso seguro y gestión de riesgos de seguridad digital promovida por la Organización para la Cooperación y el Desarrollo Económico OCDE.

En los niveles de seguridad digital, como primera medida se proyecta establecer “un marco institucional en torno a la seguridad digital, en segundo lugar crear las condiciones para gestionar el riesgo mediante mecanismos de participación activa y adecuación del marco legal y regulatorio de la materia y capacitación para comportamientos responsables en el entorno digital. Como tercera medida, se fortalecerá la defensa y seguridad nacional en el entorno digital, a nivel nacional y trasnacional, con un enfoque de gestión de riesgos. Por último, se generarán mecanismos permanentes para impulsar la cooperación, colaboración y asistencia en materia de seguridad digital, a nivel nacional e internacional, con un enfoque estratégico” (CONPES 3854 de 2016, p. 3).

Uno de los paradigmas de la protección de datos es la gestión de las relaciones con los stakeholders (partes interesadas) de una organización que requiere el uso sistemático de los datos personales básicos de un ciudadano. Por esto y con el fin de que estas relaciones se construyan de forma sólida y desde un punto de vista de la confianza mutua, es necesario incluir todos aquellos aspectos que garanticen el máximo respeto por su información (Herrera & Corujo, 2013).

Para ello, la tecnología pone a disposición plataformas que ayudan a llevar a cabo las interacciones de forma segura y eficiente. Conjuntamente, en un escenario de avances tecnológicos vertiginosos, se hace imprescindible el desarrollo de una estrategia de protección de la privacidad

y de los datos personales mucho más complejo e integral; es decir de 360º. Todo ello contribuye no solo a reforzar las citadas relaciones, sino también a detectar todas las posibilidades de nuevos negocios que surjan con ocasión del mejor tratamiento de los datos (Herrera & Corujo, 2013).

De otra parte, el Ministerio de Justicia en coordinación con diversas entidades del Estado presenta el Plan Decenal del Sistema de Justicia 2017 – 2027 en el cual se analiza la necesidad de mayores niveles de exigencia frente a los mecanismos de seguridad respecto a la protección de datos personales de conformidad con la Ley Estatutaria 1581 de 2012 entorno a:

> "… i) Principios rectores para el tratamiento de datos personales ii) las categorías especiales tales como el tratamiento datos personales de niños, niñas y adolescentes que aseguren el respeto a sus derechos iii) Los derechos de los titulares y las condiciones de legalidad para el tratamiento de los mismos iv) Procedimientos de consulta de información del titular y reclamos sobre la información contenida en la base de datos, v) Deberes de los responsables del tratamiento y encargados del tratamiento, así como los mecanismos de vigilancia y sanción los cuales están en cabeza de la Superintendencia de Industria y Comercio." (MINJUSTICIA, 2017, p. 72).

De igual manera, identifica la importancia del Registro Nacional de Bases de Datos cuya reglamentación contenida en el Decreto 886 de 2014 que debido a las condiciones complejas de la gestión de datos personales por parte de las entidades se rehúsan a la mayor accesibilidad de la información o no adecuan los procesos para facilitar el intercambio directo de la información entre los diversos entes u operadores. (MINJUSTICIA, 2017).

Otro aspecto de mayor exigencia para la protección eficaz de la protección de los datos personales de NNA, es la reducción de la brecha digital entendida como:

"En el sistema de Justicia, las brechas hacen referencia a las diferencias que existen entre los diversos usuarios, según su capacidad para utilizar las TIC de forma eficaz y efectiva, debido a los distintos niveles de alfabetización, de motivación para acceder a la información, de las competencias y habilidades en la apropiación de las tecnologías, así como problemas de accesibilidad y conectividad a la misma tecnología" (MINJUSTICIA, 2017, P. 73).

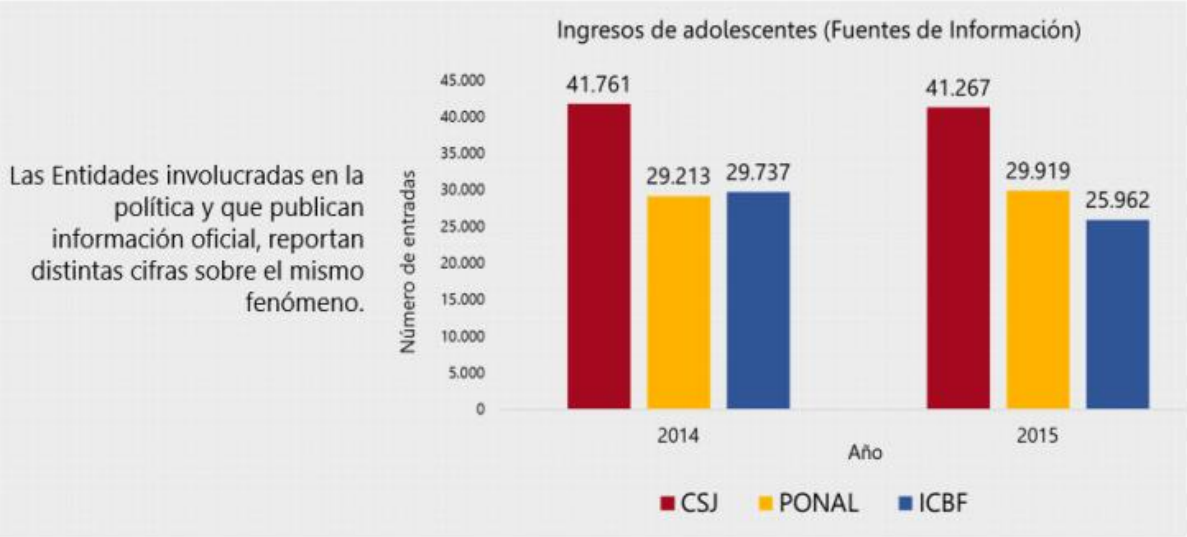


*Figura 34***.** Estado actual de los Sistemas de Información de Justicia. Ejemplo: Sistema de Responsabilidad Penal Adolescente Modelo de Gestión Pública Eficiente al Servicio del Ciudadano.
Fuente: Presentación Resultados de la Encuesta de Calidad de Vida, DNP, 2016.

De igual manera, destaca la disparidad en la información que maneja las diferentes entidades (Policía Nacional, Consejo Superior de la Judicatura y el Instituto Colombiano de Bienestar Familiar), lo cual, refleja falta seguridad en la gestión de los sistemas de información de carácter público que puede llegar a afectar derechos fundamentales con decisiones basadas en datos no reales, por lo tanto, la necesidad de generar información de calidad, confiable para garantizar la

protección de los derechos fundamentales como lo señala el Departamento Nacional de Planeación:

> "Es por ello que los datos e información generados por las diferentes fuentes en materia de justicia deben ser confiables, de calidad y con cumplimiento de estándares internacionales, como lo pretende el Departamento Administrativo Nacional de Estadística, aprovechando los registros administrativos y la certificación de operaciones estadísticas para evaluar la eficacia, pertinencia, calidad, publicación y divulgación de la información a nivel nacional y territorial desde la perspectiva integral del sistema de justicia en beneficio de los ciudadanos." (MINJUSTICIA, 2017, p. 71).

Sin lugar a dudas se visibiliza la necesidad de mejorar la conectividad en todo el país contribuye como lo manifiesta el plan decenal:

> "Si bien la cultura digital ciudadana ha presentado notorios avances, el principal foco de uso a internet sigue siendo la búsqueda de información y el acceso a redes sociales (MinTIC, 2015). De acuerdo al último Estudio de Cultura de Uso de TIC en los Colombianos para relacionarse con el Estado- 2015, 26% de los ciudadanos dicen haber visitado o utilizado páginas de internet de entidades públicas durante el año 2015, siendo que las empresas grandes son las que "van adelante en el desarrollo de una cultura digital y de interacción con el Estado a través de medios electrónicos (M.E.). Son estas las que más visitan y usan los sitios web de las entidades públicas". En segundo lugar, existen limitaciones de acceso y conectividad por parte de las entidades y operadores de sistema de justicia. Si bien se reconocen los valiosos avances en el cumplimiento del Plan Vive Digital y la ampliación de la cobertura nacional de internet, aún persisten las limitaciones de acceso y conectividad a las TIC, entendida esta última como la capacidad de un dispositivo (computador, PDA, móvil, etc.) para conectarse en cualquier lugar

geográfico generalmente a otro ordenador personal u otro dispositivo.” (MINJUSTICIA, 2017, p. 74 y 75).

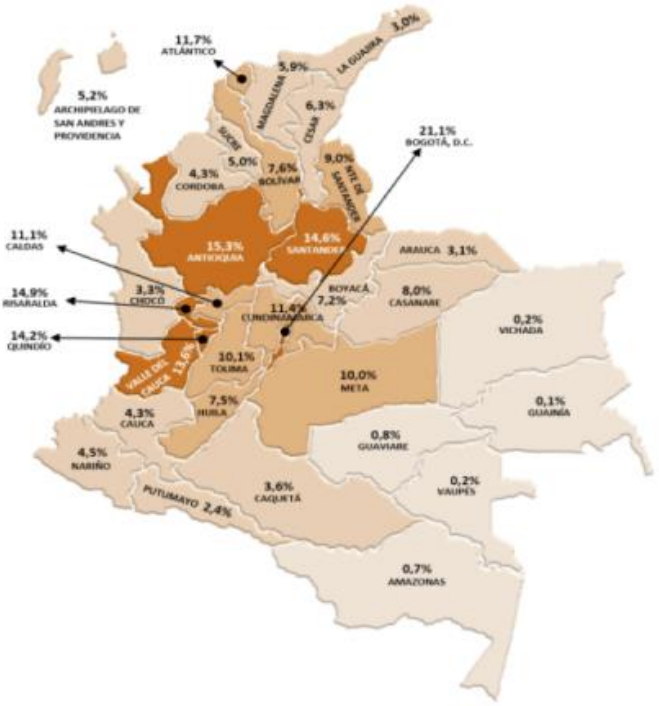


*Figura 23***.** Índice de Penetración de Internet dedicado por Departamento
Fuente: Proyección de población DANE 2016 y datos reportados por los proveedores de redes y servicios al SIUSTColombia TIC. Sept. 2016.

De igual forma, persisten barreras cognitivas por no tener en cuenta el enfoque diferencial de cada comunidad, ya que la falta de contenidos adecuados por parte de las instituciones se da en gran medida por la ausencia de caracterización de los usuarios, ciudadanos y grupos de interés del sistema de justicia, lo cual dificulta aún más una adecuada atención, provisión y desarrollo de los servicios de justicia bajo plataformas tecnológicas, así como la vinculación de programas y acciones desarrolladas por parte del Ministerio de Tecnologías de la Información y las Comunicaciones-Mintic bajo su nuevo enfoque de economía digital.

*Figura 246***.** Modelo de Gestión Pública Eficiente al Servicio del Ciudadano
Fuente: Metodología para la implementación del Modelo Integrado de Planeación y Gestión, DAFP, Secretaria de Trasparencia, Presidencia de la Republica, 2012.

Este modelo también debe contar con la finalidad de aunar esfuerzos en pro de la información de uso compartido no sólo por el Ministerio de Justicia y del Derecho sino de las demás entidades que conforman el sistema de justicia, comenzando por los mecanismos de captura, registro y recopilación de la información de manera eficiente y confiable a nivel nacional y territorial con el fin de asegurar los datos e información de tipo estadístico necesarios para su posterior uso y análisis por temática o dimensión de justicia, incluyendo un tratamiento especial y protegido de la información cuando sea el caso (ver acción política de protección de datos personales o sensibles). Para mayor ilustración se incluye la propuesta presentada por la Oficina de Información en Justicia del Ministerio de Justicia y del Derecho para un modelo eficiente e integrado para la gestión de información.

> “El modelo integrado de gestión de información no solo deberá tener en cuenta las necesidades básicas de los ciudadanos en cuanto a trámites y servicios, sino además deberá facilitar la gestión de manera estandarizada los requerimientos de información de tipo estadístico (aseguramiento de la información, conceptualización y modelaje de datos) respetando la independencia misional de las instituciones.” (MINJUSTICIA, 2017).

En el Plan Nacional de Desarrollo de Colombia se refleja el compromiso del Estado en la regulación del tratamiento de la información personal con base en estándares reconocidos:

> “…El uso y reutilización de esta información deberá garantizar la observancia de los principios y normas de protección de datos personales, de conformidad con lo dispuesto en las Leyes 1581 de 2012 y 1712 de 2014, así como las demás normas que regulan la materia. El suministro de la información será gratuito, deberá solicitarse y realizarse respaldado en estándares que faciliten el proceso de intercambio y no en tecnologías específicas que impidan el acceso, no estará sujeto al pago de tributo, tarifa o precio alguno y las entidades públicas solo podrán cobrar los costos asociados a su reproducción o los derivados de la aplicación de procesamientos o filtros especiales. Las entidades públicas propenderán por la integración de los sistemas de información para el ejercicio eficiente y adecuado de la función pública.” (Ley 1753, 2015, artìculo 159).

La comunidad dedicada a la protección de la información personal hace énfasis en un modelo que privilegia le gestión del riesgo y la asignación de responsabilidades en cabeza del responsable del tratamiento. Por tanto, la creación de un Programa Integral de Gestión de Datos Personales se fundamenta en tres (3) ejes temáticos: (i) el gobierno corporativo; (ii) los controles del sistema de gestión integral de datos personales y; (iii) la sostenibilidad del programa integral para la gestión de datos personales.

Debido al actual desarrollo tecnológico en los sistemas informáticos, se han generado nuevas formas y maneras de relacionarse, nuevas tendencias de conectividad en la sociedad y así mismo, nuevas alternativas de comunicación. Un ejemplo de ello, son las transacciones monetarias, así como la compra de bienes o servicios, las cuales se pueden realizar en forma efectiva a través de plataformas tecnológicas, las cuales facilitan el acceso a contenidos informáticos a la distancia de un clic.

Figura 37. Comienza una nueva era en el tratamiento y protección de los datos personales
Fuente: UniRrevista, Recuperado, https://www.unir.net/derecho/revista/noticias/comienza-una-nueva-era-en-el-tratamiento-y-la-proteccion-de-datos-personales/549201788758/.

Uno de los valores más significativos para los usuarios de estas plataformas informáticas es el ahorro de tiempo y costos en desplazamiento, teniendo en cuenta que en la actualidad esto se convierte en una necesidad dada las circunstancias de productividad empresarial, las jornadas laborales y los compromisos familiares.

4.3. Juridificación del tratamiento de datos personales y el sistema informático

Se evidencia que la información relacionada con la identificación de las personas y los niños, que se ha materializado en múltiples datos personales, se ha convertido en un baluarte importantísimo para los negocios y la delincuencia, un bien comercializado en diferentes mercados nacionales e internacionales y en un insumo constante de los sistemas de información privados y públicos, como refiere Remolina:

> "(i) Se nutren de datos personales, (ii) Ofrecen innumerables posibilidades para recolectar, almacenar y circular esa información en poco tiempo y de manera imperceptible para las personas a que se refieren los datos. (iii) No son absolutamente seguros. (iv) Evolucionan rápidamente y Traspasan las fronteras físicas, lo cual facilita el flujo internacional de la información en comento." (Remolina, 2010, p. 492).

Aunado a las palabras de Schwartz: "el valor monetario de esta clase de información es grande y sigue creciendo. Las empresas a nivel global rápidamente están reorientando sus esfuerzos para aprovechar y obtener utilidades de esta tendencia" (2004). Información a gran escala, comúnmente hoy denominada "Big data": hiper-información personal correlacionada para crear, analizar y predecir perfiles en una sociedad posmoderna que requiere de fórmulas, estrategias, mecanismos y herramientas de protección y prevención frente a los diferentes escenarios de vulnerabilidad e inseguridad jurídica.

4.3.1. Fases y variables de regulación de datos personales en el sistema informático

Cabe destacar que “un sistema se percibe como algo que posee una entidad que lo distingue de su entorno, aunque mantiene interacción con él”, (Javier y Franco, 1995, p.12). Es así que la regulación jurídica del sistema informático es la consecuencia de una normatividad armonizada con los estándares internacionales que protegen la privacidad de los menores de edad en ambientes online. Las redes sociales, internet, las empresas, la familia, las entidades públicas y privadas entre otras organizaciones del orden nacional e internacional están llamadas a implementar mecanismos de protección efectivos frente a la garantía de los derechos en el sistema informático pluridimensional.

Figura 38. Protección del derecho a la privacidad de los niños en la era digital

Fuente: Creación propia del código QR e imágenes de redes sociales, organizaciones y entidades públicas publicadas en internet

La estructura de realimentación realiza un estudio del comportamiento del sistema, el cual está conformado por las partes del sistema; es así que en nuestro caso la "Regulación jurídica del sistema informático" es el macro sistema que, a su vez, involucra el sub sistema informático y el sub sistema jurídico, los cuales están conformados así; sub sistema informático, incluye: bases de datos, ficheros, archivos, datos electrónicos o semejantes, software, hardware y transferencia consentida y no consentida de activos; y el sub sistema jurídico, incluye: el legislador, victima sujeto pasivo, activos patrimoniales, victimario sujeto activo, normas, modalidades delictivas, bien jurídico tutelado., hurto y jaqueo de cuentas bancarias.

En consecuencia, surge "un diagrama en el que de forma esquemática se indican las influencias implícitas de las partes del sistema en la descripción del proceso" (Aracil y Gordillo, 1995, p 14) que aquí, cabe mencionar:

> "Las partes de un sistema no representan un comportamiento autónomo e independiente unas de otras, sino que los vínculos que las articulan en la unidad del sistema se manifiestan en que los comportamientos de cada una de ellas presentan formas de dependencia o correlación con los de las otras." (Aracil y Gordillo, 1995, p 25).

La dinámica de sistemas analiza la forma en que las relaciones en un sistema permiten explicar su comportamiento; causas y consecuencias que inciden y se derivan de la realización o de la concreción de la violación de datos personales en el sistema de "Regulación jurídica del sistema informático", es así que, al interior de la sociedad inciden algunos aspectos en su concreción, es decir, factores determinantes para identificar las variables que inciden en el incremento o descenso del mismo.

Un ejemplo del anterior escenario equivale a la sanción (duración de la sentencia: severa o leve) que debe asumir quien incurre en la vulneración de datos personales, esto podría incidir en el incremento o descenso de los delitos informáticos, así mismo, surge una nueva variable; la población susceptible, la cual puede variar según preferencias para realizar las transacciones digitales o físicas o según la percepción social frente a la seguridad y alfabetización informática, también otra de las variables podría ser el número de delincuentes capacitados tecnológicamente para cometer los delitos informáticos y sustraer las información o bases de datos personales.

Adicionalmente, entre las variables podríamos mencionar el nivel de seguridad informática con las que cuentan las plataformas digitales para realizar las transacciones monetarias y finalmente, el número de delincuentes que son reinsertados a la sociedad.

Los elementos que integran el sistema informático manifiestan unos vínculos, “cómo se manifiestan los vínculos entre las partes del sistema; respecto a cómo variaciones de determinados atributos Xk, afectan las manifestaciones del otro Xj; es decir, sobre cómo se producen las interacciones en el seno del sistema” (Aracil y Gordillo, 1995, p 26). Es así que, la realimentación entre las partes del sistema puede ser positiva o negativa. Un ejemplo de ello, podría ser la falta de normas sancionatorias severas para con los delincuentes y su vínculo directo con el incremento o descenso de datos personales.

Fase de Modelado Cualitativo, o Causal, del sistema

1. Identificación de Variables, Relaciones Causales y Polaridades

Variables

Caso de estudio

Pregunta de investigación:

¿Existe en Colombia la necesidad de implementación de un modelo integral de datos online para los NNA?

Identificación de las Variables:

- Protección de la información (PI).
- Seguridad de la información personal de NNA (SI).
- Probabilidad de afectación de la información personal de NNA (AI).
- Implementación de un modelo de gestión integral de datos online para NNA (MI).

Definición de variables

Tabla 41. *Sistema teórico*

Variable	Definición
Protección de la información (PI)	Se fundamenta en el grado de amparo con el que cuenta la información suministrada por las bases de datos informáticos.
Seguridad de la información personal de NNA (SI)	Corresponde a las mediante medidas de seguridad de infraestructura, de autenticación y de autorización.
Probabilidad de afectación de la información personal de NNA (AI)	Es el índice de vulneración de seguridad de la información personal.
Implementación de un modelo de gestión integral de datos online para NNA (MI)	Es una propuesta derivada de la praxis del estudio teórico recolectado con anterioridad.

Fuente: Creación propia

Operacionalización de las variables

Tabla 42.

Variable Nº 01: Protección de la información

Dimensiones	Indicadores
Derecho de protección del dato personal	• Evolución histórica en el ordenamiento jurídico • Objeto de protección constitucional del derecho de

	Protección de datos personales • Sujetos titulares del derecho de protección • Derechos del titular del dato personal • Encargados y responsables del tratamiento de datos personales
Mecanismos para protección	▪ Mecanismos jurídicos ▪ Mecanismos técnicos o tecnológicos

Fuente: Puello, C. (2016)

Figura 43.

Variable Nº 02: Seguridad de la información personal de NNA

Dimensiones	Indicadores
Derechos fundamentales	• Derechos de los niños • Información • Intimidad • Libre desarrollo de la personalidad
Tutela jurisdiccional	• Acción de tutela • Acción penal • Acción de responsabilidad civil • Habeas Data
Autoridades nacionales competentes	• Corte Constitucional de Colombia • Superintendencia de Industria y Comercio • Instituto Colombiano de Bienestar Familiar • Ministerio de las Tecnologías de la Información y las Comunicaciones • Ministerio de Educación
Organismos internacionales cooperantes	• ONU • UNICEF • OCDE • Red Iberoamericana de Protección de Datos Personales

Fuente: Puello, C. (2016) & Autora

Tabla 44.

Variable Nº 03: Probabilidad de afectación de la información personal de NNA

Dimensiones	Indicadores
Justificación de su protección	• Instrumentos internacionales de protección a los derechos de los niños.

	• Constitution Política de 1991. • Código de Infancia y adolescencia. • Jurisprudencia Constitucional.
Factores económicos, sociales y culturales	• Ausencia de pedagogía en la familia. • Ausencia de pedagogía en la escuela.
Ausencia de parámetros jurídicos de seguridad de información de NNA	• Falta de una regulación jurídica estatutaria para la protección de datos personales de los NNA en Colombia.

Fuente: Puello, C. (2016) & Autora

Tabla 45.

Variable Nº 04: Implementación de un modelo de gestión integral de datos online para NNA en Colombia.

Dimensiones	Indicadores
Necesidad	• Análisis y valoración socio-juridico de la ausencia de un modelo integral de gestión de datos online para NNA en Colombia.
Análisis jurídico previo	• Revisión normativa nacional e internacional de los instrumentos de protección de datos de NNA
Propuesta	• Propuesta de un proyecto de Ley Estatutaria de protección de datos de NNA en Colombia.

Fuente: Puello, C. (2016) & Autora

Relaciones causales

Si (PI) aumentan, (SI) aumenta PI + SI

Si (SI) aumentan, (AI) disminuye SI - AI

Si (AI) disminuye, (MI) aumenta AI + MI

Si (MI) aumenta, (PI) aumenta PI + SI

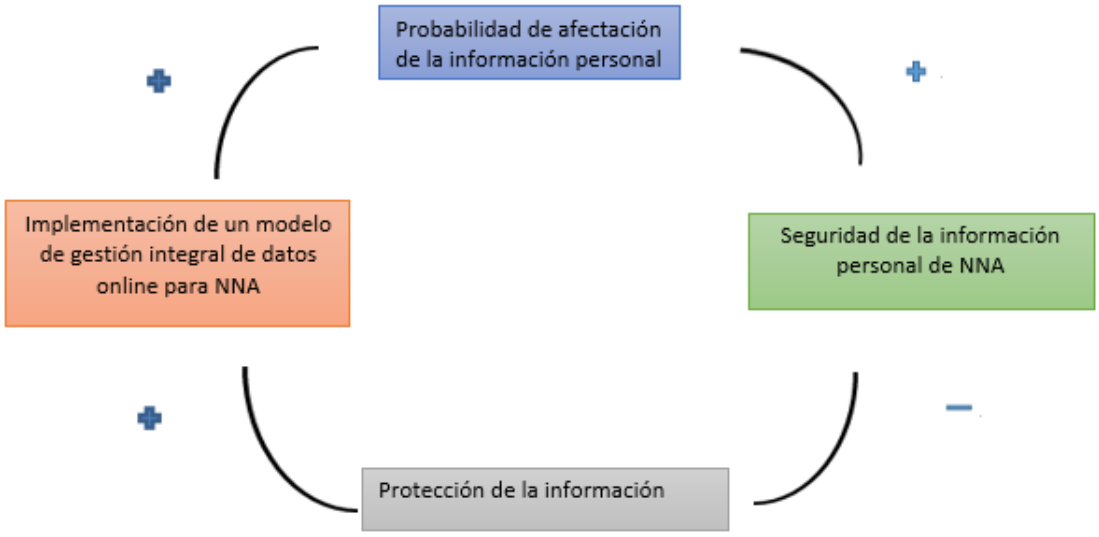


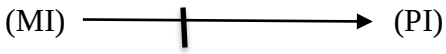
Figura 39. Diagrama causal

Fuente: Creación propia

En este sentido, es importante tener en cuenta que el presente diagrama causal corresponde a un tipo de balance (B-), toda vez que parte positivamente de la variable de origen (PI) y se regresa a ella de forma negativa (-) con posterioridad al recorrido de la totalidad del ciclo.

Retardos (II)

En el presente diagrama causal es posible identificar la existencia de un retardo respecto al tiempo transcurrido entre la implementación de un modelo de gestión integral de datos online para NNA y la protección de la información.



Elementos clave y limitantes

Elementos clave: Dentro de los elementos clave es importante destacar las políticas de seguridad de la información, el fortalecimiento de las bases digitales de la información y la implementación de un modelo de gestión integral de datos online para NNA.

Elementos limitantes: Los elementos limitante del presente diagrama causal se fundamentan en la deficiencia tecnológica de los sistemas de información respecto a las políticas de seguridad, la ausencia normativa de una de Ley Estatutaria para la Protección de Datos Online de los NNA que garantice los siguientes principios: consentimiento, autorregulación, privacidad por diseño y por defecto o responsabilidad proactiva de los co-garantes (Estado, sociedad y familia) en aras de proteger el interés superior del niño.

En este orden de ideas, desde un enfoque finalista es importante traer a colación algunos aportes de Becker (1968) teniendo en cuenta la Teoría Económica del Crimen (TEC) en donde el individuo que infringe la ley lo hace como producto de un proceso cognitivo con interés económico que le ofrece el crimen, de lo cual para el caso en estudio podría derivarse la consumación de los hurtos y la transferencia no consentida de datos como un verdadero activo.

Por consiguiente, es posible plantear un modelo de protección integral en la vía preventiva y en la vía punitiva, de acuerdo al aporte realizado por Kliksberg (2002) por medio del cual por la vía preventiva se deben fortalecer políticas públicas de seguridad de la información y por la vía

punitiva se hace necesario fortalecer las sanciones impuestas a las personas que busquen vulnerar el bien jurídico tutelado denominado "de la protección de la información y de los datos".

En este sentido, la ciencia, tecnología e innovación fundamenta el análisis jurídico realizado en el presente estudio investigativo, toda vez, que recae sobre la fundamentación y caracterización normativa de la protección de la información personal con fundamento en los derechos humanos y el cumplimiento del principio de la dignidad humana de su titular.

Con relación a la tutela de la protección de datos del niño se resalta los aspectos más relevantes en la preocupación de los Estados y comunidades por avanzar en la garantías de todos los derechos que en conexidad pudieran resultar afectados, por ellos se busca crear modelos que sustenten el pensamiento constitucional que dé respuesta a un pensamiento paradigmático del derecho frente a las tecnologías de la información desde el concepto de problema y no de concepto, para afinar mejor las herramientas de trabajo integral. La Constitución establece un vínculo especial entre legitimidad y legalidad en el Estado Social de Derecho para consolidar la garantía del interés superior del niño y los derechos que lo fundamentan.

4.3.2. Propuesta de tratamiento jurídico de datos personales online de los niños, niñas y adolescentes

La redimensión de los derechos humanos, su conexidad con el internet y en especial la educación global de los más jóvenes en la era digital son los pilares de la regulación en dimensiones divergentes que deben ser abordadas en el marco de la protección de datos personales: La ONU[51] reconoce el derecho de acceso a internet como un “derecho humano”, para todas las

[51] Ver la ilustración de la II Conferencia Mundial de Derechos Humanos Viena (1993), la cual señala: “(d)eben reforzarse los mecanismos y programas nacionales e internacionales de defensa y protección de

personas sin distinción (incluye al niño[52]) y en concordancia con el derecho a la libertad de expresión reconoce de manera vinculante el contexto offline y online a la luz de la Declaración de los derechos humanos:

> "Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión." (1948, artículo 19)

Figura 40: La ONU declara el acceso a Internet como un derecho humano.
Fuente: Carballo, J (2016) Recuperado de: https://computerhoy.com/noticias/internet/onu-declara-acceso-internet-como-derecho-humano-47674.

En este escenario, el derecho de acceso a internet de los menores es considerado un derecho humano que trae consigo oportunidades para su conocimiento y educación, sin embargo, existe una fragmentación jurídica en el abordaje proteccionista frente a los múltiples riesgos que trae el

los niños, en particular las niñas, los niños abandonados, los niños de la calle y los niños explotados económica y sexualmente, incluidos los utilizados en la pornografía y la prostitución infantil o la venta de órganos, los niños víctimas de enfermedades, en particular el SIDA, los niños refugiados y desplazados, los niños detenidos, los niños en situaciones de conflicto armado y los niños víctimas del hambre y la sequía o de otras calamidades". Recuperado de http://www.ohchr.org/SP/NewsEvents/OHCHR20/Pages/WCHR.aspx

[52] Incluye a niños, niñas y adolescentes de acuerdo con la Convención de los derechos del niño. (1959)

inadecuado uso de esta herramienta tecnológica, donde sencillamente y en muchas ocasiones sin ningún control parental, se vulneran los derechos de niñas, niños y adolescentes, en condiciones inimaginables por parte de desconocidos en la red. Como lo refiere Pérez respecto al tratamiento de datos personales en internet:

> "Su potencialidad en la difusión ilimitada de imágenes e informaciones la hace un vehículo especialmente poderoso para perpetrar atentados criminales contra bienes jurídicos básicos: la intimidad, la imagen, la dignidad, el honor y la libertad sexual de las personas, en particular, de los menores" (Pérez, 1990 p. 155).

La responsabilidad de los operadores de la información, en cuanto, a las exposiciones a los riesgos en internet que afectan al desarrollo del niño, debe ser analizada en pluridimensiones reales al interior de los actores que tienen un acercamiento o contacto con él, tales como la familia, las organizaciones privadas y públicas, así como la sociedad en general (Fernández, A. 2015).

El Estado Colombiano esta llamado al cumplimiento de los estándares iberoamericanos de protección de datos personales con fundamento en el interés superior del niño, la garantía de los derechos fundamentales, actualización de los principios y elementos técnicos y conceptuales reconocidos a nivel global tales como: el principio de la dignidad humana y la transparencia de conformidad con los tratados de derecho internacional.

De acuerdo con los Estándares Iberoamericanos de Protección de Datos se propone la revisión de la normatividad existente en el tratamiento de datos personales de niños en el entorno digital que incluya los siguientes componentes:

La estructuración de un modelo de gestión de riesgos en materia de protección de datos personales para menores de edad debe involucrar dos etapas: una primera etapa que corresponde a la planeación e identificación de los riesgos de probabilidad y la otra etapa hace alusión a la

evaluación y seguimiento respecto al impacto o nivel de responsabilidad proactiva de los operadores del tratamiento de la información personal, ya sea a nivel público o privado, con el fin de garantizar la protección de los derechos de todos los ciudadanos en general y con mayor énfasis y prevalencia el interés superior de los niños, niñas y adolescentes.

El cumplimiento normativo de los elementos más importantes relacionados con las amenazas y riesgos probables a los que se expone la actividad propia del sistema de tratamiento de datos personales, fortalece la labor proteccionista y preventiva de los riesgos que con mayor énfasis requiere los datos que identifican a los titulares de especial protección del derecho, como son los niños. El fin de dicha gestión de datos, consiste en disminuir el riesgo e impacto a todo nivel en aras de garantizar el efectivo cumplimiento pluridimensional de los requisitos regulatorios, principios, derechos y libertades de todas los titulares de información.

En el marco de la juridificación del tratamiento de datos personales de niños, niñas y adolescentes en la era digital se establece como propuesta en la esfera offline y online, la conceptualización, alcance, límites, requisitos y responsabilidad proactiva con una regulación especial y garantista de los derechos humanos que contenga disposiciones generales sobre el derecho fundamental a la privacidad de datos personales de ” niños, niñas y adolescentes” en la era digital:

a. Cuyo ***objeto*** busque desarrollar el derecho constitucional a la privacidad y protección de datos personales de los niños, niñas y adolescentes como sujetos titulares de protección integral en la era digital, de acuerdo con el derecho de los niños a la intimidad e información contemplado en los artículos 15, 20 y 44 de la Constitución Política, los artículos 33 y 34 del Código de la Infancia y la Adolescencia, los derechos contemplados en el artículo 7 de la Ley 1581 de 2012 y demás normas reglamentarias y concordantes.

b. **Ambito de aplicación** corresponda a sujetos de especial protección de la presente ley los niños, niñas y adolescentes menores de 14 años. El derecho a la autodeterminación informativa y la autorregulación de los menores de edad en materia del tratamiento de datos personales online obedece a la protección de su interés superior y la protección de los derechos fundamentales.

Se limita el alcance de los datos de niños de naturaleza pública, los datos sensibles de los menores de edad en los diferentes escenarios públicos y privados

c. **Su conceptualización.** Defina elementos determinantes de estandarización en virtud del interés superior del titular:

Autorización: Corresponde a una aprobación previa y expresa del titular del tratamiento de los datos personales.

Base de datos: Compendio organizado y sistemático contentivo de datos personales en disponibilidad de tratamiento.

Dato personal: Es la información pública o privada de índole descriptiva correspondiente a una persona natural.

Administrador del tratamiento de datos personales: Es la persona natural o jurídica de tipo privado o publica que realiza el tratamiento de los datos personales y que se encuentra representado por el responsable del tratamiento.

Responsable del tratamiento: Es la persona natural o jurídica de tipo privado o publica quien toma las decisiones concernientes al tratamiento de los datos personales en las fuentes de información.

Titular: Corresponde a la persona natural niño, niña o adolescente, quien tiene a su disposición los datos personales que serán tratados con posterioridad.

Tratamiento de datos personales: Es el proceso de operaciones mediante el cual se recolecta, almacena y utilizan los datos privados o públicos de una persona natural.

d. Los principios que fundamentan la "interpretación y aplicación de la ley de tratamiento de datos personales para NNA en el ámbito online", acoge la teoría armónica e integral de acuerdo con los establecidos en la normativa 1581 de 2012:

Legalidad: El proceso del tratamiento de los datos personales se fundamentará en el estricto cumplimiento de la presente Ley Estatutaria, con lealtad y licitud en el marco del interés superior del niño.

Principio de finalidad: La finalidad del tratamiento debe ser determinada, explicita, legítima, exacta, (fines públicos, científicos**,** históricos, estadísticos, su circulación y trazabilidad) y delimitada

Veracidad y calidad: Los datos personales deben ser veraces y actualizados, se prohíbe de manera expresa la utilización de información errónea e incompleta.

Acceso y circulación de los datos: Se ha de tener en cuenta la privacidad de los datos personales en cumplimiento del derecho fundamental a la intimidad del titular de los datos personales.

Autorregulación: Exigencia de empoderar al titular de la información en el conocimiento del ejercicio de sus derechos y los deberes.

Privacidad por diseño y por defecto: Acoge la definición dada respecto a la "privacidad por diseño: Es la protección de la información que exige la incorporación en las especificaciones de diseño de tecnologías, procesos, prácticas de negocio e infraestructuras físicas que aseguren la protección de la privacidad de la información." (Decreto 1413, 2017, artículo 2.2.17.1.3) e

incorpora el interés superior del niño y la garantía de sus derechos fundamentales de forma prevalente en la operación del tratamiento de su información personal.

Seguridad: Corresponde a un circuito de responsabilidad técnica y administrativa en el proceso de recolección, tratamiento y utilización de los datos personales a fin de evitar la vulneración de los datos y de los derechos fundamentales de su titular.

Confidencialidad: Se debe garantizar la reserva de la información recolectada por parte de todas las personas naturales y jurídicas que intervienen en el tratamiento de los datos personales.

Los principios de protección de datos personales regulados por la Ley 1581 de 2012**,** forman parte de la protección integral del derecho a la privacidad del niño, niñas y adolescente con mayores niveles seguridad y de prevención del riesgo en materia de transparencia, acceso y circulación restringida.

e. **Prevalencia de los derechos fundamentales de los niños, niñas y adolescentes:** En el proceso de tratamiento de los datos personales bajo la titularidad de los "niños, niñas y adolescentes" se observará el artículo 44 constitucional y de los tratados y convenios internacionales ratificados por Colombia.

f. Derechos de los niños, niñas y adolescentes. El acceso a la tecnología, e internet conlleva el ejercicio de los derechos de autodeterminación informativa, educación, libertad de expresión con responsabilidad por lo tanto se exige mayor nivel de verificación y seguridad informática legítima en el tratamiento de los datos personales que asegure el respeto a los derechos prevalentes de los "niños, niñas y adolescentes" de acuerdo a los estándares de protección de la privacidad y los datos personales.

g. Limitación de los sitios web o servicio en línea dirigido a niños: Un sitio web comercial o servicio en línea, o parte de un sitio web comercial o servicio en línea, no se considerará dirigido

a los niños únicamente para referirse o vincularse a un sitio web comercial o servicio en línea dirigido a niños utilizando herramientas de localización de información, índice, referencia, puntero o enlace de hipertexto.

Se limita el uso desproporcionado de dispositivos móviles, acceso a redes sociales y plataformas no aptas para la edad de los niños. Se debe fortalecer en el ámbito familiar, educativo y social el adecuado uso de las tecnologías de la información y las comunicaciones por parte de los niños, niñas y adolescentes mediante estrategias y didácticas apropiadas al nivel educativo.

h. Consentimiento verificable de los representantes legalmente y tutores: El término "consentimiento paterno verificable" significa cualquier esfuerzo razonable (teniendo en cuenta la tecnología disponible), incluyendo una solicitud de autorización para la futura recolección, uso y divulgación descrita en el aviso, para asegurar que un padre de un niño reciba aviso del operador las prácticas de recolección, uso y divulgación de información personal, y autoriza la recopilación, uso y divulgación, según proceda, de información personal y el uso posterior de esa información antes de que se recopile la información del niño.

i. Prueba expresa de la autorización. Los responsables del tratamiento de los datos personales deberán contar con una autorización previa y expresa de la autorización del manejo de los datos personales de los niños, niñas y adolescentes por parte de los representantes legales de los mismos. El operador o responsable del tratamiento debe demostrar los medios de legalidad y seguridad utilizados para obtener dicho consentimiento libre y espontáneo del titular, el padre o tutor legalmente autorizado.

j. Deber especial de informar al titular. Deberá existir un carácter facultativo, con lenguaje claro y sencillo en el proceso de información acerca del tratamiento de datos de los niños, niñas y adolescentes de acuerdo a la edad, con especial cuidado cuando se trate de datos sensibles.

k. Estandares de privacidad y protección de datos personales online de niños, niñas y adolescentes. El tratamiento jurídico de protección de datos personales acoge los estándares iberoamericanos y europeos de protección de datos personales y los pertinentes en consideración al interés superior de los "niños, niñas y adolescentes," el principio de transparencia, la legalidad del consentimiento, la educación y formación en el uso de los servicios digitales tanto en el ámbito privado como público.

l. Programa integral de protección de datos personales online de niños, niñas y adolescentes: Se deberá crear un programa integral para la protección de los datos personales online de los niños, niñas y adolescentes en Colombia, a fin de documentar todos los procedimientos realizados por las personas encargadas del tratamiento de los datos personales y verificar el cumplimiento de los parámetros legales en su utilización, en donde le corresponderá su instrucción y supervisión a la Superintendencia de Industria y Comercio.

La Superintendencia de Industria y Comercio, capacitará y orientará a los responsables y encargados del tratamiento sobre un programa integral de protección de datos personales de "niños, niñas y adolescentes" y gestión de riesgos online de conformidad con el principio de la dignidad humana y los estándares de privacidad y protección de datos personales.

m. Responsabilidad proactiva de los operadores públicos y privados: Le corresponderá al Estado por medio de sus representantes capacitar a los responsables del tratamiento de la información de los "niños, niñas y adolescentes". De igual manera, deberá brindar un apoyo pedagógico a los representantes legales acerca del uso responsable de los datos personales, dispositivos de comunicaciones online, la connotación del respeto al derecho a la privacidad y los riesgos a los que se expone por su inadecuada utilización.

La responsabilidad administrativa de proteccion de datos personales de niños, niñas y adolescentes**:** Las entidades públicas y privadas debe incorporar en sus procesos administrativos la formación de sus trabajadores en la política de privacidad de datos personales en todos los procesos empresariales. La Superintendencia de Industria y Comercio contará con una delegatura especial para la protección de los datos personales cuya función sea la de vigilar, inspeccionar y controlar la garantía por el respeto de los derechos fundamentales, garantías y procedimientos en el correcto tratamiento de los datos personales de los "niños, niñas y adolescentes" en Colombia.

n. Responsabilidad de los representantes legales del menor. Los representantes legales del menor están llamados a responder por el abandono y arbitrariedad en el uso de internet y las redes sociales que afecte los derechos del niño y los derechos de los terceros. El ICBF está autorizado a declarar el maltrato de los niños cuando se encuentren situaciones que afectan la educación de los niños.

O. Protección integral de datos personales. Se debe coordinar acciones por parte de la Superintendencia de Industria y Comercio, el Ministerio de las Tecnologías de la Información y las Comunicaciones, el Instituto Colombiano de Bienestar Familiar, la Policía de Infancia y Adolescencia y el Centro Cibernético de la Policía Nacional con el fin de garantizar la adecuada gestión integral de datos personales de n"iños, niñas y adolescentes" por parte de operadores y responsables del tratamiento por medio de acciones preventivas y de promoción registradas en bases de datos nacionales donde se identifique las sanciones impuestas con ocasión de las conductas reprochables de violación de los datos personales de niños.

Así mismo, se creará un Observatorio y Registro Único de Bases de Datos de Menores de Edad, con el fin de identificar, evaluar el nivel de cumplimiento normativo en cuanto a los principios, derechos, garantías y procedimientos previstos en la Ley.

p. Cooperacion internacional de protección de datos personales. con la cooperación de UNICEF, la ONU, la Red Iberoamericana de protección de datos personales, entre otras organizaciones y entidades públicas y privadas de reconocida trayectoria en materia de protección de datos personales de “niños, niñas y adolescentes” a nivel internacional se sucribirán convenios para apoyar la lucha contra los ciberdelitos en materia de violación de datos personales (creación de observatorios), la prevención de riesgos y el fortalecimiento de alianzas de cooperación internacional para sistemas de información de niños, niñas y adolescentes armonizados y conectados en la era digital.

q. Vigencia de la ley: Tiene vigencia de 5 años, en los cuales se realiza estudios técnicos de impacto para su respectiva modificación. Rige a partir de la fecha de su promulgación y deroga las disposiciones que le sean contrarias.

La regulación es el reflejo del gobierno y la gestión de los datos, el cual es complejo por la intervención de los seres humanos, es decir, por naturaleza es complejo y si no se facilita el proceso de información se vuelve aún más complicado, por lo tanto, el gobierno de los datos debe gestionar en un ámbito independiente pero interoperable los diferentes sistemas o aplicativos. Cada programa debe traer la facilidad de extraer datos individuales y datos masivos para la toma de decisiones que estén relacionados con los menores de edad, con el fin de reducir la variabilidad y minimizar los riesgos de forma proactiva. Se sugiere por lo tanto, el sistema de protección y gestión integral de la privacidad y datos personales de niños, niñas y adolescentes con la metodología de estandarización internacional e innovación de las TIC y soluciones inventivas de protección integral que garantice el derecho a su privacidad y sus datos personales en la era digital como un derecho humano.

4.4. Gestión de riesgos de seguridad digital y privacidad de datos personales de los niños

En el marco de la política nacional de seguridad digital en Colombia, la lucha contra ciberdelincuencia, cibercriminalidad a nivel mundial, se requiere de la eficiente gobernanza de datos a nivel global que involucre al Estado como garante de los derechos humanos, la comunidad y los diferentes actores de la revolución industrial 4.0, contando con un sistema de protección de datos personales de la infancia y adolescencia y un programa integral de gestión de datos personales de los niños (PIGD) en las entidades públicas y privadas.

4.4.1 Sistema de protección de datos personales de la infancia y adolescencia

Como referente de un sistema de especial protección para los NNA se encuentra en el Código de Infancia y Adolescencia (Ley 1098 de 2006) y la regulación del Sistema de Responsabilidad Penal para Adolescentes, en los siguientes términos:

> “El sistema de responsabilidad penal para adolescentes es el conjunto de principios, normas, procedimientos, autoridades judiciales especializadas y entes administrativos que rigen o intervienen en la investigación y juzgamiento de delitos cometidos por personas que tengan entre catorce (14) y dieciocho (18) años al momento de cometer el hecho punible. " (L.1098, 2006, Art. 139.) (Subrayado fuera de texto).

Por lo tanto, la garantía del interés superior del niño y su protección integral, en torno a su derecho a la privacidad y protección de la información personal por parte del Estado Colombiano amerita con prevalencia estructurar e implementar un Sistema de protección de datos personales de la infancia y la adolescencia que incluya todas las dimensiones (física y online) del programa

integral de protección de datos personales de NNA en relación con los servicios de la sociedad de la información.

Figura 41. Sistema de protección de datos personales de NNA
Fuente: Creación propia basada en la articulación de los componentes del sistema digital y jurídico (2018)

Un Sistema de protección de datos personales de la infancia y adolescencia, adecuado a los estándares internacionales de protección de la privacidad y protección de datos personales, tanto en el ámbito preventivo como proteccionista que incluya un conjunto de principios, normas, procedimientos, autoridades (administrativas y judiciales) especializadas y lideradas por un ente rector como el Instituto Colombiano de Bienestar Familiar, Ministerio de Educación, el Ministerio de la Tecnologías de la Información y las Comunicaciones, con el apoyo de la Superintendencia de Industria y Comercio que garantice la protección de la información relativa a los menores de edad, imponiendo consigo diferentes sanciones y obligaciones a los diversos entes involucrados en el tratamiento de sus datos personales.

Un sistema dentro del cual se encuentra consagrado un Registro Nacional de Bases de Datos relacionado con información de los menores de edad, armonizada a nivel nacional e internacional, y cuyas entidades de carácter público o privado encargadas del tratamiento de datos personales y

la prestación de servicios para los niños como sistemas de salud, colegios, transporte entre otros, se establezcan los protocolos que delimitan el alcance del deber de cuidado y adecuada protección de su privacidad de acuerdo con los estándares internacionales y la Convención de los Derechos del Niño.

Tabla 46.

Componentes del Sistema de protección de datos personales de la infancia y adolescencia

Ámbito	Estrategia	Composición	Actores
Preventivo	Programa integral de gestión de datos personales de niños (PIGD) Registro Nacional de Bases de Datos	Autorregulación Campañas de sensibilización en procura de una cultura de respeto por la privacidad y protección de datos personales. Programas educativos dirigidos a estudiantes y docentes Códigos de buenas prácticas, normas vinculantes, Políticas de privacidad con protocolos de aseguramiento más exigentes	Estado Empresa Padres Sociedad civil
Reactivo – Protección	Proyecto de Ley Estatutaria para la Protección de Datos Personales Online de los NNA	Principios: Interés superior del niño, Lealtad, licitud, confidencialidad, seguridad e integridad y limitación de la finalidad Legalidad y veracidad del consentimiento Privacidad por diseño y por defecto Responsabilidad proactiva Normas vinculantes	

	Derecho al olvido Derecho a la memoria Prohibiciones en publicidad y la industria
N.	**Aspectos por regulación e implementación**
1	Aplicación de nuevos Principios: Rendición de cuentas o Accountability, mejores mecanismos de protección y métodos de validación (privacidad desde el diseño y por defecto)
2	Concientización y responsabilidad en materia del tratamiento de datos personales: Responsabilidad proactiva Implementación de la política de privacidad y transparencia y método de control en multinacionales. Es aplicable a todo tipo de empresas tanto micro, mediana como grandes de las cuales resulta fácil desarrollar la política de privacidad y transparencia
3	Tratamiento de los datos de menores (establecimiento de la edad). Legalidad y veracidad del consentimiento del menor
4	Derecho al olvido: El derecho de oponerse a la creación de perfiles
5	Portabilidad de los datos: Copia de la base de datos
6	Mayor claridad regulatoria respecto a la transferencia y cooperación internacional de datos personales
7	Fortalecer la inspección, vigilancia y control mediante un sistema de supervisión interactivo de identificación de riesgos
8	Fomento de la autorregulación, normas vinculantes y programas integrales de gestión de datos personales, sellos de confianza, códigos de buenas prácticas de privacidad en los diferentes ámbitos.

Fuente: Creación basada en los Estándares Iberoamericanos de protección de datos (2017) y el Reglamento EU 2016/679.

Los actores y operadores del Estado llamados a responder directamente por la protección de datos personales de los menores de edad a nivel nacional son la Superintendencia de Industria y Turismo, la Presidencia de la República (la Secretaría de Transparencia), la Procuraduría General de la Nación, el Ministerio de Tecnologías de la Información y las Comunicaciones, el Ministerio de Educación, el Ministerio de Comercio Industria y Turismo, el Departamento Administrativo de la Función Pública, El Instituto Colombiano de Bienestar Familiar, el Centro de Documentación Judicial de la Rama Judicial, la Registraduría Nacional del Estado Civil, la Fiscalía General de la Nación, la Policía Nacional, la Unidad para la Atención y Reparación de Víctimas del Conflicto

Armado, Policía Nacional, Medicina legal, Ministerios de Educación y TIC, el Departamento Nacional de Planeación, Defensoría del Pueblo, órganos judiciales).

De igual manera, debe reglamentarse la responsabilidad proactiva de todas las empresas (offline y online), los padres y la sociedad civil en general como actores y operadores de la privacidad y los datos de los niños, por medio de las normas vinculantes y las buenas prácticas de privacidad empresarial.

4.4.2. Programa integral de gestión de datos personales de los niños (PIGD) en las entidades públicas y privadas

Las entidades que realizan tratamiento de datos personales están llamadas a la creación de un proyecto global interactivo con recursos educativos, de sensibilización y prevención, de habilidades para la vida digital, de inclusión digital, redes sociales, identidad digital, ciberconvivencia, ciberciudadanía, e-derechos infancia, videojuegos online, denuncia oline, ayuda a padres y madres, apoyo a centros escolares en dichas temáticas:

a) Tratamiento adecuado de los datos personales

La protección de datos personales, implica de igual modo la prevención personal de la información que el individuo circula por cualquier medio de comunicación offline - online. Exige el conocimiento de los riesgos y las buenas prácticas de privacidad que hacen de la cultura un escenario de confianza y seguridad global con adecuados procedimientos y directrices de reconocimiento internacional.

b) Privacidad inferida y autorregulada

El respeto de la privacidad en las redes sociales o ambientes virtuales empieza por el individuo que luego se traslada a la colectividad que al igual debe responder por su tratamiento de forma autorregulada y colaborativa en escenarios y operadores online proactivos para la infancia y la adolescencia, porque la privacidad de los niños es responsabilidad de todos los actores del sistema jurídico y digital.

Ahora bien, la tendencia en materia de protección de datos personales de niños es la de fortalecer la autorregulación a todo nivel como lo enfatiza la comunidad europea, por cuanto, estos sujetos de derecho adquieren mayor conocimiento y agilidad en el manejo de las tecnologías de la información y las comunicaciones, por lo tanto, considera lícito el tratamiento de datos personales de un menores de edad cuanto tenga como mínimo 16 año como lo establece el Reglamento Europeo. Colombia limita el tratamiento de datos personales de menores de edad de manera general con la Ley 1581 de 2012, sin embargo su alcance en el entorno digital, como se evidencia en el Código de la Infancia y el Código Civil identifica el concepto de niño entendido como: “las personas entre los 0 y 12 años y por adolescentes las personas entre 12 y 18 años”, solo para ambientes físicos (Código civil artículo 34) y su regulación debe estar encaminada a la protección integral del niño incluso en un escenario con el cual interactúa toda su vida de manera sistemática a más temprana edad.

5. Conclusiones

Existe un mundo líquido lleno de realidades y falacias en algoritmos que se escapan al entendimiento del sistema sociojurídico como, por ejemplo, la traducción del título de la tesis: “Adecuación del tratamiento de datos personales de niños, niñas y adolescentes en el marco de la juridificación y la prevención de los riesgos digitales” al código binario:

01000001 01100100 01100101 01100011 01110101 01100001 01100011 01101001 11000011 10110011 01101110 00100000 01100100 01100101 01101100 00100000 01110100 01110010 01100001 01110100 01100001 01101101 01101001 01100101 01101110 01110100 01101111 00100000 01100100 01100101 00100000 01100100 01100001 01110100 01101111 01110011 00100000 01110000 01100101 01110010 01110011 01101111 01101110 01100001 01101100 01100101 01110011 00100000 01100100 01100101 00100000 01101110 01101001 11000011 10110001 01101111 01110011 00101100 00100000 01101110 01101001 11000011 10110001 01100001 01110011 00100000 01111001 00100000 01100001 01100100 01101111 01101100 01100101 01110011 01100011 01100101 01101110 01110100 01100101 01110011 00100000 01100101 01101110 00100000 01100101 01101100 00100000 01101101 01100001 01110010 01100011 01101111 00100000 01100100 01100101 00100000 01101100 01100001 00100000 01101010 01110101 01110010 01101001 01100100 01101001 01100110 01101001 01100011 01100001 01100011 01101001 11000011 10110011 01101110 00100000 01111001 00100000 01101100 01100001 00100000 01110000 01110010 01100101 01110110 01100101 01101110 01100011 01101001 11000011 10110011 01101110 00100000 01100100 01100101 00100000 01101100 01101111 01110011 00100000 01110010 01101001 01100101 01110011 01100111 01101111 01110011 00100000 01100100 01101001 01100111 01101001 01110100 01100001 01101100 01100101 01110011

Figura. 42. Código binario del título de la Tesis Doctoral: Protección de datos personales de niños, niñas y adolescentes en el marco de la juridificación y la prevención de los riesgos digitales en Colombia.

Fuente:. Creación basada en el sistema binario.

Da cuenta, del acoplamiento del sistema jurídico a la conceptualización y contextualización propia de la sociedad de la transparencia y de la información líquida, que facilita la interacción y generación de oportunidades entre todos los seres humanos de diferentes edades pero a la vez

genera riesgos propios del cristal de la soledad, la imagen, el secreto oculto de quien es realmente el hombre desde la infancia en el ecosistema digital.

El ejercicio de derechos por parte de los niños, niñas y adolescentes como usuarios de las redes sociales y la falta de mecanismos efectivos de tutela ARCO, es decir de "acceso, rectificación, cancelación y oposición", de datos personales de los menores de edad, en el ámbito digital requiere de la implementación de un *"Sistema global de Protección de la Privacidad e Información de niños, niñas y adolescentes en la era digital*" adecuado a los estándares internacionales de privacidad y tratamiento de datos personales a nivel proteccionista y preventivo, es por ello, relevante concluir que Colombia requiere incorporar a su ordenamiento jurídico, los Estándares de Protección de Datos Personales de los Estados Iberoamericanos, mediante una Ley Estatutaria de Protección de la Privacidad e Información de los niños, niñas y adolescentes en la era digital y un modelo de gestión de riesgos de seguridad digital para NNA con base en los siguientes postulados:

1**) En relación al cumplimiento del derecho:**

a. Protección integral, dignidad humana e "interés superior del niño": Deber de protección por parte de los operadores y responsables de su información personal con programas de gestión integral adecuados a la calidad del sujeto de derecho y de acuerdo con la "Convención sobre los Derechos del Niño, los Estándares Iberoamericanos de Protección de Datos Personales", sistema de autorregulación y marco normativo que se traduzcan en códigos deontológicos con base en la opinión de las niñas, niños y adolescentes en lo que se refiere el tratamiento de su información personal en internet de tal manera que su libre expresión y participación pueda ser escuchada y valorada, determinar la madurez suficiente para tratar sus datos determinar la edad y exigir

mecanismos o herramientas de verificación de edad, implementar herramientas tecnológicas seguras.

b. Mecanismos de verificación de la legalidad del consentimiento y autorización por parte de los titulares de la información facultados por la ley para cualquier servicio de los ciudadanos digitales con especial relevancia para identificar a los infantes, adolescentes de cualquier nacionalidad.

c. Consentimiento válido y legal, información clara, las políticas de privacidad de los entornos de internet una red social o de un servicio por ejemplo la geolocalización, observación en el control parental, es decir el control por medio de herramientas que cumplen una función en determinadas edades, compromiso de los poderes públicos.

d. Principio de transparencia: Deber del reconocimiento especial del principio de transparencia en cuanto a la información proporcionada dada a los menores de edad, como sujetos protagónicos de la información debe ser adecuada para su edad cumpliendo: que se suficiente y fácilmente accesible.

e. En relación con la capacidad: El menor de edad es persona, y como tal está dotado de personalidad civil (o capacidad jurídica) desde el momento de su nacimiento. Por lo que respecta a su capacidad cuando se trate del derecho a protección de datos, derecho a la intimidad, el honor y la imagen el criterio de “capacidad de obrar evolutiva o progresiva del menor” podrá realizar actos de disposición siempre que sus condiciones de madurez o capacidad de autodeterminarse se lo permitan.

f. Sistema de autorregulación y políticas de privacidad y normas vinculantes que se traduzcan en códigos deontológicos elaborados de manera responsable por cada operador del tratamiento de datos, con el control de la entidad de vigilancia.

g. Revisar el concepto de dato personal para adecuarlo a las exigencias de referenciación internacional, así como las diversas formas de tratamiento de la información en actividades personales o exclusivamente domésticas, en redes sociales digitales que involucra datos de niños, niñas y adolescentes o datos de carácter personal de terceros que ampliaría la responsabilidad relacionada con el tratamiento y la aplicabilidad de los principios de la protección de datos de carácter personal, incidentes digitales, rendición de cuentas, análisis de impacto, privacidad desde el diseño y por defecto y analítica de datos.

h. Regular la exigencia y grado de responsabilidad (responsabilidad reforzada y proactiva) de los intermediarios de la información en internet frente al inadecuado tratamiento de datos personales de “niños, niñas y adolescentes” en todos los escenarios de los servicios digitales incluyendo las redes sociales.

i. Regular el alcance de la privacidad o la información en el caso de las redes sociales, cuando fallece el titular de los datos que es un menor de edad y se considera relevante su información para el ejercicio de otros derechos tales como el derecho de cancelación, el derecho de acceso, el derecho al olvido entre otros.

j. Incorporar el alcance y los límites del derecho al olvido y el derecho al recuerdo en materia de protección de la privacidad y datos personales propios del internet, como, por ejemplo, las redes sociales, cuando fallece el titular de los datos que es un menor de edad y se considera relevante su información para el ejercicio de otros derechos.

k. Regular los periodos de adecuación de la normativa nacional con el apoyo de órganos especializados en el entorno de digital y la dimensión internacional dado los avances de la inteligencia artificial, big data e internet de las cosas entre otras novedades de cada generación tecnológica.

2) **En relación con los mecanismos de prevención de riesgos en la era digital:**

a. Fortalecer el diseño e implementación de programas integrales de gestión de seguridad de las tecnologías de la información digital para niños.

b. Fortalecer la formación académica de los “niños, niñas y adolescentes”, padres de familia, operadores y responsables del tratamiento de la información en la promoción del uso responsable y seguro del internet y las tecnologías de la información digital.

c. Establecer mayores estrategias pedagógicas y jurídicas en entidades públicas y privadas que acojan en su actividad empresarial y pública, practicas responsables de privacidad y protección de la información personal de los menores de edad; conciencia sobre la privacidad: un cambio de cultura empresarial y autorregulación para la protección de datos del niño.

d. Se requiere de recursos para la formación de docentes especialistas en el tema, modificación de planes de estudio, elaborar manuales para la formación de los menores en materia de privacidad con el fin de formarlos integralmente, autorregulación para la protección de datos del niño. Regular el tratamiento específico de la privacidad desde el diseño y por defecto respecto a los datos del niño, gobernanza de la protección de datos personales del niño: informes de evaluación y rendición de cuentas de los entes privados y públicos, estrategias pedagógicas y jurídicas que permitan un nivel adecuado de protección de los datos del niño para generar conciencia sobre el derecho fundamental; un derecho humano de connotación internacional y tecnológico cada vez más visible y de significancia.

3) En relación al sector público:

a) Información clara, sobre geolocalización, políticas de privacidad de los entornos de internet una red social o de un servicio donde medie un contrato y las políticas de privacidad son difíciles de entender como el caso de una hipoteca y para de los menores más aún de acuerdo a su edad y capacidad de comprensión, que permita la transparencia en el tratamiento de sus datos con el compromiso de los poderes públicos, es fundamental para proteger una infancia en red sin riesgos mediante la gobernanza de la protección integral de datos personales en todas sus dimensiones.

b) Mayor exigencia de responsabilidad de los actores del sistema social y el sistema de internet respecto a la formación y el conocimiento de los derechos y deberes relacionados con la privacidad y protección de datos de "niños, niñas y adolescentes", las oportunidades, riesgos, amenazas de la utilización de las redes sociales o medios de interacción offline y online tanto a los titulares como a los representantes legales del menor.

c) A pesar de haber regulado el sector de la publicidad en el comercio, industria y turismo respecto al control de distribución o circulación de la información personal de niños, niñas y adolescentes (Decreto 1377, 2013) se presenta vacíos respecto a los operadores de las redes sociales y la información que circula en internet. Se requiere claridad respecto a los contratos que celebran los niños, niñas y adolescentes de acuerdo a su capacidad en los casos de mora o retrasos.

d) La Superintendencia de Industria y Turismo, está llamada a limitar el uso de dispositivos de geolocalización (ejemplo drones), utilización de datos o perfiles de niños con fines publicitarios y de marketing, con medidas sancionatorias de multa a los operadores, intermediarios y responsables de servicios de internet, o bloqueos a los sitios web que permitan prácticas restrictivas o violatorias de los derechos humanos. Así como en el proceso de inspección, control y vigilancia en cuanto a:

- Las prácticas de validación de la autorización de los padres o representantes legales de los menores, e incluso el consentimiento mismo de los menores.

- Expresar claramente la finalidad de la recolección de los datos con un lenguaje claro y proporcionado para la edad de los niños.
- Establecer niveles de gestión de seguridad de los riesgos digitales frente a los menores de edad.
- Limitar y sancionar el valor de uso comercial de datos relacionados con información personal de los niños sin los requisitos de ley, desde la privacidad por diseño y por defecto.
- Formular programas de apropiación, autorregulación y gestión de la información personal de niños, niñas y adolescentes en Internet en cabeza del Ministerio de las Tecnologías de la Información y las Comunicaciones como por ejemplo el denominado: "Teprotejo" facilitando el conocimiento del "uso sano, seguro y constructivo de las tecnologías de la información", entre otros programas integrales de gestión del riesgo digital dirigido a niños, niñas y adolescentes con el apoyo del Ministerio de Eduación, los Defensores de Familia, las Comisarías de Familia, los entes territoriales y otras entidades estatales que faciliten la garantía de sus derechos en el marco de la Constitución Política de 1991, la Ley 1098 de 2006, la Ley 1755 de 2015 y los tratados internacionales de protección .

4) En relación a la tutela internacional del derecho a la protección de datos personales de NNA

a) Fortalecer la participación en la Red Iberoamericana de Protección de Datos Personales con el fin de crear mecanismos de cooperación internacional que permitan la protección del interés superior de niños, niñas y adolescentes frente al tratamiento de su información personal.

b) Implementar mecanismos de resolución de incidentes digitales cuando se trate de datos personales de "niños, niñas y adolescentes" de manera más expedita y prevalente.

c) Generar redes de cooperación global que facilite la transferencia internacional de datos personales y la creación de la legislación acorde a los cambios tecnológicos por cuestiones técnicas, y la protección desde el diseño tanto de normas como del sistema de información, teniendo en cuenta la opinión de las niñas, niños y adolescentes, en lo que se refiere el tratamiento de su información personal en internet de tal manera que su libre expresión y participación pueda ser escuchada y valorada, formación integral para tratar sus datos, determinar la edad, restricciones frente a obtener datos de los integrantes de la unidad familiar, autorregulación para no utilizar internet para afectar la privacidad de terceros.

Para finalizar los Estados están llamados a realizar buenas practicas de gobierno y gestión de datos de todos los ciudadanos y en especial de niños, niñas y adolescentes en aras de garantizar el interés superior, los derechos fundamentales y la dignidad humana en todas sus dimensiones ya sea física o virtual.

Los operadores y responsables de datos personales están llamadas en el ambito operacional a incorporar reglas de calidad de datos en todos los procesos del ciclo de vida de los datos y reducir los errores sistemáticos operacionales por el diseño o el procesamiento de información en el ámbito de la ingeniería de datos, así como en el ámbito directivo o también denominado gobierno de datos estructurar los niveles de decisión estratégica.

Los datos deben generar o manejarse con su propia identidad y personalidad haciendo abstracción de todos los elementos de una organización tales como tecnología, procesos u otros conceptos. En toda organización debe existir un plan estratégico de negocios, un plan estratégico de tecnología e información y entre los dos un plan estratégico de datos e información. Y el plan estratégico tecnología e información soporta el plan estratégico de datos e información.

Se hace necesario la verdadera privacidad por diseño y por defecto respecto a los paquetes de información que deben funcionar con protocolos de privacidad estandarizados tanto desde su

arquitectura como en su procesamiento que facilite la toma de decisiones que de por si son complejas por la naturaleza del big data, así como el acoplamiento del principio de accountability al principio de responsabilidad proactiva con programas integrales de gestión de datos (PIGDP) tanto en las entidades públicas y privadas, el derecho de desindexación, el uso de tecnologías de vigilancia, los desafíos del internet de las cosas, la privacidad en la la inteligencia artificial que requieren mayor intervención del Estado frente a la protección integral del niño bajo el enfoque basado en los derechos humanos.

Es imperativo la exigencia de la responsabilidad reforzada y proactiva de las empresas de la revolución industrial y tecnológico respecto a sus plataformas de información tales como Google y redes sociales considerados escenarios de “dialectica de libertad”, y a su vez vías panópticas de la libertad del individuo que voluntariamente entrega o expone su información a la “mirada” constante del vigilante digital cuyo interés es su posición dominante en el mercado como lo refiere Byun Chul Han y no la educación sistémica del hombre en procura de garantizar sus derechos fundamentales desde su infancia en la era digital.

Referencias Bibliográficas

Aba Catoira, A. (2011). La protección de los derechos de los menores ante las nuevas tecnologías, internet y redes sociales. En L. Cotino Hueso, Libertades de expresión e información en internet las redes sociales; ejercicio, amenazas y garantías (pág. p. 491). Valencia: PUV (Publicaciones de la Universidad de Valencia).

Adame, Tenorio, M. (2012) La protección de datos personales desde el derecho al acceso a la información y como derecho fundamental autónomo, el caso mexicano. Revista Internacional de Protección de Datos Personales, Universidad de los Andes, Bogotá

Agamben, Giorgio. (2005). "Elogio de la profanación" (En profanaciones, Adriana Hidalgo Editora) Buenos Aires

(1996). La comunidad que viene, Pretextos, Valencia, España.

Agencia Española de Protección de Datos. (2017). Red Iberoamericana de Protección de Datos RIPD. Informe 2016 La protección de datos de los menores de edad. Trama Editorial. Madrid. Recuperado de http://www.redipd.es/documentacion/otrosdocumentos/common/Primer_informe_Red_Iberoamericana_de_Proteccion_de_Datos.pdf

Alexy, Robert. (2005). "Los derechos fundamentales en el Estado Constitucional Democrático", en CARBONELL, Miguel (ed), Neoconstitucionalismo (s), 2ª. Ed. Madrid Trotta.

(1993). Derecho y razón práctica. Recuperado de http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1900-65862014000200015

(1993). Teoría de los derechos fundamentales. Recuperado de https://es.scribd.com/doc/7764613/ALEXY-Robert-Teoria-de-Los-Derechos-Fund-Amen-Tales

Álvarez-Cienfuegos Fidalgo, J. (2007). Un Apunte Sobre los Derechoshumanos y sus Generaciones. En T. Da Cunha Lopes, R. Luviano González, B. Revuelta Vaquero, & R. Sánchez Benítez, Globalización Derechos Humanos y Sociedad de la Información. México: Universidad Michoacana de San Nicolás de Hidalgo.

Amaya, N. S, (2016). La protección de la intimidad y vida privada en internet: la integridad contextual y los flujos de información en las redes sociales (2004 – 2014) Agencia Española de Protección de Datos. Madrid. España

Andreu Martínez, M. B. (2014). La Protrección de Datos Personales de los Menores de Edad. recuperado de https://www.casadellibro.com/libro-la-proteccion-de-datos-personales-de-los-menores-de-edad/9788490149928/2269810

(2009). Diez años de aplicación de la Chidren's Online privacy Protection Act Estadounidense. Reflexiones para el derecho español. Revista española de Protección de Datos (Núm.7), Recuperado de: https://dialnet.unirioja.es/servlet/articulo?codigo=3402031.

APEC Cancillería. (s.f.). Foro de Cooperacion Asia Pacificio (APEC), recuperado de http://www.cancilleria.gov.co/foro-cooperacion-asia-pacifico-apec

Banisar, D. (28 de November de 2016). National Comprehensive Data Protection/Privacy Laws and Bills 2016. recuperado de SSRN: https://ssrn.com/abstract=1951416 or http://dx.doi.org/10.2139/ssrn.1951416

Barba Martínez, G. P. (1982). Tránsito a la modernidad y derechos fundamentales. recuperado de https://e-archivo.uc3m.es/handle/10016/10004

Barberis, M. (2013). Los derechos humanos como adquisición evolutiva. DOXA Cuadernos de Filosofía del Derecho (36) Universidad de Alicante España, 25-40.

Barlow, J.P.,(1996) " Declaración de Independencia del Ciberespacio" Cibernautas por la Tolerancia, Recuperado de: http://www.ctv.es/ USERS/mrb/tolerancia/

Baudrillard, Jean. (1978). Agonie des Realen, Berlín

(1991). La guerra del golfo no ha tenido lugar. Barcelon Anagrama.

(2009). La sociedad de consumo, Sus mitos, sus estructuras. Original: La societé de consommation. –Ses mythes, ses structure, 1970 Trad. Alcira Bixio, Madrid, Siglo XXI, España.

Baudrillard & E. Morin, (2011) La violencia del mundo, Buenos Aires, Editorial Capital Intelectual.

Barthes, R. (2010). La cámara lúcida. Paidós, Barcelona.

Bauman, Zygmunt (2004). Modernidad líquida. Trad. Mirta Rosenberg. Recuperado de https://catedraepistemologia.files.wordpress.com/2009/05/modernidad-liquida.pdf

Bazán, V. (2005). El Habeas Data y el Derecho de Autodeterminación informativa en perspectiva de Derecho Comparado. Centro de Estudios Constitucionales de Chile, p. 85-139.

Béjar, H. (1988): «Privacidad», en Terminología científico social. Aproximación científica. Barcelona: Antrophos, pp. 785-787. El ámbito íntimo: privacidad, individualismo y modernidad, Madrid: Alianza.

Bejar Merino, H. (1989). La Cultura del Individualismo. Recuperado de http://www.reis.cis.es/REIS/PDF/REIS_046_05.pdf

Bentham Jeremy, (1979 [1791]), El panóptico. Madrid: Ediciones de la piqueta.

Benyekhlef, K., Couture Ménard, P. A., & Paquette Bélanger, E. (2011). Menores, redes sociales y el derecho al olvido. En J. L. Piñar Mañas, Redes sociales y privacidad del menor (pág. 194 y ss). Madrid, España: Reus.

Berlin, I. (1988). «Dos conceptos sobre la libertad», en Cuatro ensayos sobre la libertad. (J. Bayón, Trad.) Madrid: Alianza Editorial.

Bill of Rights. (1689). Inglaterra. Recuperado de: https://archivos.juridicas.unam.mx/www/bjv/libros/6/2698/20.pdf

Bobbio, N. (1991). El tiempo de los derechos. recuperado de http://ijdh.unla.edu.ar/advf/documentos/2017/02/589352927c58c.pdf

Böckenförde, E. (1996). Escritos sobre Derechos Fundamentales. recuperado de https://es.scribd.com/doc/191539042/Ernst-Wolfgang-Bockenforde-Escritos sobre derechos fundamentales

Bourdie, P. & Teubner, G. (2000) La fuerza del derecho. Estudio preliminar y traducción Carlos Morales de Setién Ravina. Siglo del hombre Editores, Ediciones Uniandes Instituto Pensar, Bogotá

Boza, Beatriz, (2004) Acceso a la información del Estado: marco legal y buenas prácticas, Konrad Adenauer Stiftung, Lima.

Byun-Chul Han, (2013) La sociedad de la transparencia Traducción Gábas, Herder Bogotá

(2012) La Sociedad Del Cansancio. Barcelona, Herder Editorial

(2014) La Agonía Del Eros. Barcelona, Herder Editorial

(2014) Psicopolítica: Neoliberalismo Y Nuevas Técnicas De Poder, Barcelona, Herder Editorial.

(2014) En El Enjambre. Barcelona, Herder Editorial

Buttarelli, G. (2011). Los menores y las nuevas tecnologías. En J. L. Piñar Mañas, Redes sociales y privacidad del menor (pág. pp.144 y ss.). Madrid: Reus.

Camps Mirabet, N. (2007). El principio del interés superior del menor; marco normativo internacional y aplicación e el derecho interno. En A. M. Padial Albäs, & M. D. Toldrá Roga, Estudios jurídicos sobre la protección de la infancia y a adolescencia (pág. 23 y ss.). Valencia: Tirant lo Blanch.

Carreras Serra, L. (1996). Régimen jurídico de la información. Periodistas y medios de comunicación. Barcelona, España: Ariel Barcelona.

Carta de los Derechos Fundamentales de la Unión Europea. (2000). Obtenido de Parlamento Europeo: Recuperado en: http://www.europarl.europa.eu/charter/pdf/text_es.pdf.

Carta Magna. (1215). Londres. Recuperado de: https://archivos.juridicas.unam.mx/www/bjv/libros/6/2698/17.pdf

Castilla del Pino, C. (1996). Teoría de la intimidad. Revista de Occidente, 15-31.

(2007). Protección del derecho a la Intimidad y uso de las nuevas tecnologías de la información (Vol. 1). Huelva, España: Universidad de Huelva.

CE. European Court of Human Rights (1950). Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales.: Recuperado de: http://www.echr.coe.int/Documents/Convention_SPA.pdf

Chinchilla, T. (1999). ¿Que son y cuáles son los Derechos fundamentales? recuperado de https://es.scribd.com/document/312697713/Lectura-6-Chinchilla-Herrera-T-Que-Son-y-Cuales-Son-Los-Derechos-Fundamentales

Cifuentes, E. (1997). El Habeas Data en Colombia. Ius et Praxis (1), 66-83.

Cóngreso de Colombia (26 de mayo de 1873). Código Civil de los Estados Unidos de Colombia [Ley 84 de 1873], DO 2.867 [Imprenta nacional] Recuperado de: http://www.secretariasenado.gov.co/senado/basedoc/codigo_civil.html

Cóngreso de Colombia (26 de mayo de 1887). Código Civil, DO [Ley 57 de 1887] [Imprenta nacional] Recuperado de: https://www.alcaldiabogota.gov.co/sisjurMantenimiento/normas/Norma1.jsp?i=39535

Congreso de Colombia, (8 de noviembre de 2006). Código de la Infancia y la Adolescencia. [Ley 1098 de 2006]. DO: 46.446 [Imprenta Nacional] Recuperado de: https://www.icbf.gov.co/cargues/avance/docs/ley_1098_2006.htm

Congreso de Colombia, (31 de diciembre de 2008). Ley Estatutaria de Hábeas Data crediticia, financiera, comercial, de servicios y provenientes de terceros países. [Ley 1266 de 2008] DO: 47.219 [Imprenta Nacional] Recuperado de http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

Congreso de Colombia (2016). Código Nacional de Polícia y Convivencia. [Ley 1801 de 2016], DO 49.949 [Imprenta Nacional] Recuperado de: https://www.policia.gov.co/sites/default/files/ley-1801-codigo-nacional-policia-convivencia.pdf

Congreso de Colombia (17 de octubre de 2012). Ley Estatutaria de Protección de Datos Personales. [Ley 1581 de 2012] DO: 48584 [Imprenta Nacional] Recuperado de: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Congreso de Colombia (5 de enero de 2009). Código Penal, nuevo bien jurídico: de la protección de la información y de los datos" y las TIC, [ley 1273 de 2009] DO 47223 [Imprenta

Nacional] Recuperado de: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Congreso de Colombia (6 de marzo de 2014). Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional [ley 1712 de 2014] DO 49.084 [Imprenta Nacional] Recuperado de: http://www.secretariasenado.gov.co/senado/basedoc/ley_1712_2014.html

Congreso de Colombia (9 de junio de 2015). Plan Nacional de Desarrollo 2014-2018 [ley 1753 de 2015] DO 49.538 [Imprenta Nacional] Recuperado de: http://www.secretariasenado.gov.co/senado/basedoc/ley_1753_2015.html

Conde Ortiz, C. (2005). La protección de datos personales: un derecho autónomo con base en los conceptos de intimidad y privacidad. Cádiz, España: Dykison.

Coletti& J. Linares (1997) La intervención sistémica en los servicios sociales ante la familia multiproblemática: La experiencia de Ciutat Vella (pp. 45- 82). Barcelona: Paidós Terapia Familiar.

Congreso de Colombia, (26 mayo de 1873). Código Civil DO: 2.867. Ley 57 de 1887, art. 4o. Con arreglo al artículo 52 de la Constitución de la República Recuperado de: http://www.secretariasenado.gov.co/senado/basedoc/codigo_civil.html.

Congreso de Colombia, (24 de julio de 2000) Código Penal Ley 599. DO: 44.097. Recuperado de: http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html

Congreso de Colombia, (2006). Ley 1098, Código de la infancia y la adolescencia, Bogotá Colombia, Imprenta Nacional, publicada en el DO 46446.

Congreso de Colombia, (2008). Ley 1266 Habeas Data Financiero y Crediticio. Recuperado de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488

Congreso de Colombia, (2012). Ley 1581 Ley Estaturaria ara la Protección de Datos Personales. Bogotá, Colombia: Imprenta Nacional, publicada en el Diario Oficial 48584 del 18 de octubre de 2012.

Congreso de Colombia, (2014). Ley 1712 Ley de la transparencia y del acceso a la información pública nacional y otras disposiciones Recuperado de: https://www.mintic.gov.co/portal/604/articles-7147_documento.pdf

Consejo Nacional de Política Económica y Social, Colombia, 3701 (2011) Lineamiento de política para ciberseguridad y ciberdefensa. Bogotá Recuperado de: https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

Consejo Nacional de Política Económica y Social, Colombia, 3854, (2016) Política Nacional de Seguridad Digital. Bogotá Recuperado de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Consejo de Europa. (1981). Convenio No. 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

Consejo de Europa. (1995) Directiva 95/46/CE. Recuperado de http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:31995L0046&from=EN

Consejo de Europa. (2000). Carta de los derechos fundamentales Recuperado de: http://www.europarl.europa.eu/charter/pdf/text_es.pdf

Constan, Benjamín (1988), Sobre el espíritu de conquista, Madrid, Alianza Editorial.

Constant, Benjamin (1997 [1819]) “De la liberté des anciens comparée à celle des modernes”, Écrits politiques, Gallimard: Paris. Traducción al español (1989) en Escritos políticos. Madrid: Centro de Estudios Constitucionales.

Constitución Española. (1978). Constitución del Reino de España. Boletín Oficial del Estado Num. 311 del 29 de diciembre de 1978. Madrid, España.

Constitución De Los Estados Unidos De América. (1787). Recuperado: https://www.constitutionfacts.com/content/constitution/files/usconstitution_spanish.pdf

Constitución Política de los Estados Unidos Mexicanos. (1917). Cámara de Diputados México, Recuperado en: http://www.diputados.gob.mx/LeyesBiblio/htm/1.htm

Constitución Política de Colombia. (1991). Alcaldía de Bogotá: Recuperado en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4125

Contreras, S. (2012). Ferrajoli y los Derechos Fundamentales. Obtenido de Revista de la Inquisición (Intolerancia y Derechos Humanos) Volumen 16.

Convención sobre los Derechos del Niño. (1989). Obtenido de Naciones unidas: http://www.oehchr.org

Corte Suprema de Justicia de los Estados Unidos, (1973) Roe Vs Wade Recuperado de: https://jurisprudencia.mpd.gov.ar/Jurisprudencia/Forms/DispForm.aspx?ID=1935&source=https://jurisprudencia.mpd.gov.ar/Jurisprudencia/Forms/voces.aspx?voces=AUTONOM%C3%8DA%20PERSONAL

Corte Constitucional de Colombia, Sala Tercera de Revision, (13 de noviembre del 2012) Sentencia T-937 (M.P. Luis Ernesto Vargas Silva)

Corte Constitucional de Colombia, Sala Plena, (12 de mayo del 2010) Sentencia C-334 (M.P. Juan Carlos Henao Perez)

Corte Constitucional de Colombia, Sala Plena, (8 de febrero de 1993) Sentencia C-033 (M.P. Alejandro Martínez Caballero).

Corte Constitucional de Colombia, Sala Plena, (17 de febrero de 1994) Sentencia C-063 (M.P. Alejandro Martínez Caballero).

Corte Constitucional de Colombia, Sala Plena, (16 de octubre del 2008) Sentencia C-1011 (M.P. Jaime Córdoba Triviño).

Corte Constitucional de Colombia, Sala Plena, (12 de Julio del 2012) Sentencia C-540 (M.P. Jorge Iván Palacio Palacio).

Corte Constitucional de Colombia, Sala Plena, (6 de octubre del 2011) Sentencia C-748 (M.P. Jorge Ignacio Pretelt Chaljub)

Corte Constitucional de Colombia, Sala Plena, (12 de febrero del 2015) Sentencia SU-053 (M.P. Gloria Stella Ortiz Delgado)

Corte Constitucional de Colombia, Sala Plena, (1 de marzo de 1995) Sentencia SU-082 (M.P. Jorge Arango Mejía)

Corte Constitucional de Colombia, Sala Plena, (21 de junio del 2012) Sentencia SU-458 (M.P. Adriana maría Guillén Arango)

Corte Constitucional de Colombia, Sala Octava de Revision, (27 de junio del 2013) Sentencia T-366 (M.P. Alberto Rojas Ríos).

Corte Constitucional de Colombia, Sala Tercera de Revision, (27 de enero del 2014) Sentencia T-020 (M.P. Luis Guillermo Guerrero Pérez).

Corte Constitucional de Colombia, Sala Primera de Revision, (29 de enero de 1993) Sentencia T-022 (M.P. Ciro Angarita Barón).

Corte Constitucional de Colombia, Sala Quinta de Revision, (8 de febrero del 2016) Sentencia T-036 (M.P. Gloria Stella Ortiz Delgado).

Corte Constitucional de Colombia, Sala Octava de Revision, (7 de febrero del 2013) Sentencia T-058 (M.P. Alexei Julio Estrada)

Corte Constitucional de Colombia, sala sexta de revsion, (12 de octubre del 200) Sentencia T-1390 (M.P. Alejandro Martínez Caballero)

Corte Constitucional de Colombia, sala octava de revision, (29 de marzo del 2012) Sentencia T-260 (M.P. Humberto Antonio Sierra Porto).

Corte Constitucional de Colombia, Sala septima de revision, (23 de julio de 1996) sentencia T-322 (M.P. Alejandro Martínez Caballero)

Corte Constitucional de Colombia, sala septima de revision, (13 de septiembre de 1995) sentencia T-411 (M.P. Alejandro Martínez Caballero)

Corte Constitucional de Colombia, sala primera de revision, (16 de junio de 1992) sentencia T-414 (M.P. Ciro Angarita Baron).

Corte Constitucional de Colombia, sala septima de revision, (13 de junio del 2002) sentencia T-467 (M.P. Eduardo Montealegre Lynett)

Corte Constitucional de Colombia, sala novena de revision, (30 de octubre de 1997) sentencia T-552 (M.P. Vladimiro Naranjo Mesa)

Corte Constitucional de Colombia, sala septima de revision, (23 de julio del 2012) sentencia T-585 (MP. Jorge Ignacio Pretelt Chaljub).

Corte Constitucional de Colombia, sala de revision de tutelas, (9 de diciembre de 1992) sentencia T-598 (M.P. Simón Rodríguez Rodríguez & Jaime Sanín Greiff).

Corte Constitucional de Colombia, sala tercera de revision, (7 de septiembre del 2007) sentencia T-705 (M.P. Jaime Córdoba Triviño)

Corte Constitucional de Colombia, sala septima de revision, (5 de septiembre del 2002) sentencia T-729 (M.P. Eduardo Montealegre Lynett)

Corte Constitucional de Colombia, (7 de febrero del 2014) sentencia T-76, (M.P. Luis Guillermo Guerrero Pérez).

Corte Suprema de los Estados Unidos (22 de enero de 1973). Sentencia Roe vs. Wade, 410 US 113.

Cotino, Hueso L. (2007) Derecho constitucional II. Derechos fundamentales. Materiales docentes de innovación educativa, Publicaciones de la Universidad de Valencia, Col·lecio Laboratori de Materials, 2007, 525 páginas. Recuperado de http://goo.gl/e05HZ

(2009) “El derecho de acceso a las nuevas tecnologías y su recepción constitucional y en el Estatuto de la Comunidad Valenciana”, en RAMÓN FERNÁNDEZ, Francisca (coord.), La influencia del Derecho valenciano en las disciplinas tecnológicas, Universidad Politécnica de Valencia-Tirant lo Blanch, Valencia, 2009. págs. 181-198.

(2011 a) “Internet y derechos humanos” en AA. VV., Diccionario iberoamericano de derechos humanos y fundamentales, (Guillermo Escobar, ed.), Federación Iberoamericana de Ombudsmen. Recuperado de: www.portalfio.org

(2012) El derecho a la educación como derecho fundamental. Especial atención a su dimensión social prestacional, Madrid España, Centro de Estudios Políticos y Constitucionales.

H. L., Sauhuquillo O., & Corredoira A, Loreto (eds.), (2015). El paradigma del Gobierno Abierto. Retos y oportunidades de la participación, transparencia y colaboración, Universidad Complutense, Madrid, Recuperado de: https://paradigmagobiernoabierto.org/2016/02/07/libro_completo/.

Davara Fernandez. (2011). hacia la estandarización de la protección de los datos personales. Madrid, España.

Dávara, Rodríguez, M. (1998), La protección de datos en Europa: principios, derechos y procedimiento, Madrid, Grupo Asnef Equifax-Universidad Pontificia de Comillas.

Dávila, P., & Naya, L. (2006). La evolución de los Derechos de la Infancia: Una visión internacional (Vol. 7). Madrid: Encounters on Education.

De Miguel Asensio, P. A. (2011). Derecho Privado de Internet. Cizur Menor, Navarra: Civitas-Thomson Reuters.

Declaración Universal de los Derechos Humanos. (1948). Obtenido de Naciones Unidas: Recuperado en: http://www.un.org/es/documents/udhr/.

Departamento de Derecho Internacional Washington D.C. (2010). Ley Modelo Interamericana sobre acceso a la información pública y su guía de implementación. Washington D.C.

Departamento Nacional de Planeación de Colombia (2017), Boletín técnico Indicadores básicos de TIC en Hogares 2017 Recuperado: https://www.dane.gov.co/files/investigaciones/boletines/tic/bol_tic_hogares_2017.pdf

Dermizaky Peredo, P. (2000). El Derecho a la Intimidad. Ius et Praxis, vol. 6(núm. 1), pp. 177-193.

Desantes, Guanter, J.M.: (1977). Fundamentos del Derecho de la Información. RAYCAR. S.A. IMPRESORES. Madrid.

(1992).: El futuro de los profesionales de la información, Concepción de Chile.

(1994) Estudios públicos. Ensayo sobre la condición legal del informador. [acceso 3 de enero de 2011]. Documento en PDF.

(1998): Ética y Derecho, promotores de la técnica informativa. Universidad de Piura. Perú.

(2004): Derecho a la información. Meteriales para un sistema de la comunicación. Fundación COSO. España.

Directiva 95/46/CE. (24 de octubre de 1985). Obtenido de http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:31995L0046&from=EN.

Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales. (16 de diciembre de 2014). Obtenido de www.oecd.org/sti/ieconomy/15590267.pdf

Domínguez, A. G. (2008). Tratamiento de Datos Personales y Derechos Fundamentales (2 ed.). Madrid, España: Dykinson.

Constitucion De Los Estados Unidos De America. (1787). Recuperado: https://www.constitutionfacts.com/content/constitution/files/usconstitution_spanish.pdf

European Unión, European Union Agency for Fundamental Rights, y Council of Europe, Handbook on European data protection law, Publications Office of the European Union, Belgium. (2014). Obtenido de http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf

Fappiano, A. (s.f.). Habeas data: una aproximación a su protección. En H. F. Zamudio, Protección de datos de carácter personal (págs. 647-648). Buenos Aires: Astrea.

Fariñas Matoni, L. M. (1993). El Derecho a la Intimidad. Madrid, España: Trivium S.A.

Fernández, E. (1984). Teoría de la justicia y derechos humanos. Madrid, recuperado de https://www.casadellibro.com/libro-teoria-de-la-justicia-y-derechos-humanos/9788474441512/463859

Fioravanti, Maurizio (2007). Los derechos fundamentales. recuperado de https://es.scribd.com/document/325084902/Fioravanti-Los-Derechos-Fundamentales

Fiscalia General de la Nación, (2019) Datos abiertos de la Fiscalía General de la Nación Recuperado de: https://www.fiscalia.gov.co/colombia/gestion/estadisticas/

Flórez R. (2011). La protección de la intimidad económica con relación al dato financiero en la jurisprudencia constitucional colombiana [1992-2008]. Medellín, Colombia: Unaula.

Foucault, Michel. (2013). Las palabras y las cosas. En A. Pons, citada en el "Desorden Digital". Madrid, España: Siglo XXI.

(2007) Nacimiento De La Biopolítica, Curso En El Collège De France. (1978-1979). Fondo De Cultura Económica. Buenos Aires.

F. Hondius, (1983) A decade of international data protection, "Netherlands of international Law Review, vol. 30. No. 2

Foro de Cooperación Asia Pacifico (2004), Marco de privacidad APEC. Recuperado de http://www.cancilleria.gov.co/foro-cooperacion-asia-pacifico-apec

Frosini, V. (1982). Cibernética, derecho y sociedad, trad. cast. de C. Salguero Talvera. . Madrid, España: Temis.

Garcia Fernandez, F. (2010). Las redes sociales en la vida de tus hijos Como conseguir que se relacionen on-line de forma segura y responsable. Madrid: Abertis - Foro generaciones interactivas.

Garriga, Dominguez, A. (2010). Tratamiento de Datos personales y Derechos fundamentales. Madrid, Esp1aña: Dykinson.

Garzón Valdés (2003) selección de los participantes depende de la libre decisión de cada individuo

Godina, H. (2006). El panóptico moderno. A Parte Reí.

Gómez-Juárez S, I. (2008). La protección de los datos del menor como e-consumidor. En L. Cotino Hueso, Consumidores y usuarios ante las nuevas tecnologías (pág. 729 y ss). Valencia: Tirant lo Blanch.

Gómez Jara, D. C., Teoría de sistemas y derecho penal: Fundamentos y posibilidades del aplicación. Recuperado de: https://dialnet.unirioja.es/servlet/libro?codigo=8706

Gómez-Juárez S, I. (2008). La protección de los datos del menor como e-consumidor. En L. Cotino Hueso, Consumidores y usuarios ante las nuevas tecnologías (pág. 729 y ss). Valencia: Tirant lo Blanch.

González, A. D. (2009). Derecho a la intimidad en las actividades preventivas y en los actos de investigación en el nuevo proceso penal colombiano. Bogotá, Colombia: Universidad Libre de Colombia.

González, R. (s.f). Aproximaciones a los Derechos Humanos de Cuarta Generación. Perú.

Grun, E. (1995). Una Visión sistémica y Cibernética del Derecho, Buenos Aires Abeledo Perrot. Obtenido de Inter-mediacion: http://www.inter-mediacion.com/cibernetica.htm

Gutiérrez, B. J. D. (2001). Los límites entre la intimidad y la información. Bogotá, Colombia: Universidad Externado de Colombia.

Guzmán, G, M. (2013). El Derecho Fundamental A La Protección De Datos Personales En México: Análisis Desde La Influencia Del Ordenamiento Jurídico Español.(Tesis doctoral, Universidad Complutense De Madrid). Obtenido de http://eprints.ucm.es/228

Hassemeer, W., & Chirino, S. A. (1997). El derecho a la Autodeterminación informativa. Buenos Aires: Del puerto.

Henderson, S. (2010). Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search. Catholic University Law Review.

Hegel, G. (1966). Femenología del espíritu, México FCE

Heidegger, (1987) Unterwegs zur Sprache, Stuttgart, Barcelona

Herrera, C., & Corujo, A. (2013). Privacidad By Desubgb: Hacia un nuevo paradigma de gestión inteligente de la información y los datos personales. iberia de Llorente & Cuenca, Versión Virtual. Obtenido de http://www.desarrollando-ideas.com/2013/11/privacidad-por-diseno-hacia-un-nuevo-paradigma-de-la-proteccion-de-datos/.

Heredero Higueras, (1983-1984) Documentación administrativa No. 198, Traducción Manuel Daranas)

Hootsuite (2018) Tendencias en redes sociales para el 2018. Informe anual de Hootsuite con las últimas tendencias globales en redes sociales. Recuperado de: file:///C:/Users/LENOVO/Downloads/gd-SocialTrends-es_03%20(1).pdf

Humanium. (2016). Evolución histórica de los Derechos del niño. Recuperado de http://www.humanium.org/es/historia/

ICONTEC, (2013). Norma NTC: ISO/IEC 27001. Colombia Recuperado de: https://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf

Información, I. F. (2010). Protección de Datos Personales. (Alonso, Ed.) México D.F., México.

Informe de Investigación de la Comisionada de Protección de Datos Personales de Canadá, Chantal Benier, sobre Facebook. (2009). Recuperado de http://www.utm.mx/edi_anteriores/temas56/T56_5Resena1_ProteccDatos.pdf

Instituto Colombiano de Bienestar Familiar, (2019) “Programa en TIC confio” Recuperado de: https://www.enticconfio.gov.co/

Jasper, M. C. (2009). Privacy and the Internet: Your expectations and rights under the law. New York: Oxford University Press.

Jiménez Ben, W. G. (2007). El Enfoque de los Derehcos Humanos y las Políticas Públicas. Civilizar, ciencias sociales y humanas, Universidad Segio Arboleda, Vol. 7(Num 12), 31-46.

Jacopo DAlonzo, (2013) El origen de la nuda vida: Política y lenguaje en el pensamiento de Giorgio Agamben, Revista Pléyade 12 Universidad Di Roma La Sapienza.

Kant, I. (1983). Fundamentación de la metafísica de las costumbres. (E. Morente García, Trad.) Madrid: Espasa-Calpe.

Kelsen, H. (1982). Teoría Pura del Derecho. México: Universidad Nacional Autónoma de México.

Kuhn, Thomas. S. (2004). Las estructuras de las revoluciones científicas. México: Fondo de Cultura Económica.

Kuneva, M. (2009). Comisario Europeo del Consumidor. Mesa Redonda de Keynote. Bruselas, Belgica, Comision Europea del Consumidor.

Laguado, R. (2011). Intimidad personal e interoperabiliad: el reto de proteger al individuo. Bogotá: UniAndes.

Larenz, K.(1979), Metodología de la Ciencia del Derecho Barcelona, Ariel, España

Ley Federal de Datos Personales en posesión de los particulares. (2010). México.

Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. (2002). México.

Ley Orgánica 0015. (1999). Ley Orgánica 0015 de 1999, 13 de diciembre, de protección de Datos de Carácter personal. Madrid, España: Boletin Oficial de España (298) del 14 de diciembre de 1999, BOE-A-1999-23750.

Ley orgánica 15. (1999). Protección de datos de carácter personal. España.

Lopez Diaz, E. (1996). El derecho al honor y el derecho a la intimidad: jurisprudencia y doctrina. Madrid: Dykinson.

López, Medina, D. (2010). Derechos y libertades. Revista de filosofía del derecho y derechos humanos.

Lorente López, M. C. (2015). Los Derechos al Honor a la Intimidad Personal y Familiar de la Propia Imagen del Menor. Pamplona, España: Aranzadi.

Lucena, I. (2012). La protección de la intimidad en la era tecnológica: hacia una reconceptualización. Recuperado el 13 de agosto de 2014, de Revista Internacional del Pensamiento Político. Recuperado de http://www.pensamientopolitico.org/Descargas/RIPP07117144.pdf

Luquin, B. (2012). La Protección juríodico Civil del Menor Usuario de Telelefonía móvil en la Sociedad de la Tecnología. Pamplona, España: Aranzadi.

Madrid, Conesa. F. (1984). Derecho a la intimidad, informática y Estado de Derecho. Valencia, España: Universidad de Valencia.

Marecos, G. A. R. (2013). Configuración jurídica del derecho a la autodeterminación informativa. Legíslación y Publicaciones de la Corte Suprema de Justicia de Asunción, Paraguay, 41.

Martinez De Pison, J. (1997). Derechos humanos: historia, fundamento, realidad. Zaragoza, España: Egido.

Martínez, Martínez R. (2004). Una aproximación crítica a la autodeterminación informativa. Madrid: Civitas Ediciones.

(2004). El derecho fundamental a la protección de datos personales: perspectivas Revista Internet, derecho y política. Univesitat Oberta de Catalunya, Barcelona, España.

Maturana Humberto, (1999). Transformación en la convivencia, Dolmen Ediciones, Caracas, Montevideo, Santigao de Chile.

Ministerio de Justicia del Perú. (2013). El derecho fundamental a la protección de datos personales. Obtenido de Ministerio de Justicia del Perú: Recuperado de: https://www.minjus.gob.pe/wp-content/uploads/2014/02/Cartilla-Derecho-Fundamentalok.pdf

Ministerio de Comercio, Industria y Turismo (26 de Mayo de 2015). Decreto Único Reglamentario del Sector Comercio. [ley 1074 de 2015] DO: Recuperado de http://wp.presidencia.gov.co/sitios/normativa/decretos/2015/Decretos2015/DECRETO%201074%20DEL%2026%20DE%20MAYO%20DE%202015.pdf

Ministerio de Comercio, Industria y Turismo (27 junio de 2013) Reglamentación de la Ley 1581 de 2012. [Decreto 1377 de 2013] DO 48834. Recuperado de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646

Ministerio de Tecnologías de la Información y las Comunicaciones TIC de Colombia, (2018), Modelo de getión de riesgos de seguridad digital. Recuperado de: https://www.funcionpublica.gov.co/documents/418548/34316316/Anexo+4+Lineamientos+para+la+Gestion+del+Riesgo+de++Seguridad+Digital+en+Entidades+P%C3%BAblicas+-+Gu%C3%ADa+riesgos+2018.pdf/1ce5099d-c5e5-8ba2-00bc-58f801d3657b

Ministerio de Tecnologías de la Información y las Comunicaciones TIC de Colombia, (2017), Decreto 1413, Se establece lineamientos generales en el uso y operación de los servicios de los ciudadanos digitales. Recuperado de: https://www.mintic.gov.co/portal/604/w3-article-59399.html

MinTIC (2016) Seguridad y privacidad de la información: controles de seguridad y privacidad de la información (Guía No. 8) Versión 3.0.1 de 6 de marzo de 2016. En: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

MinTIC, (2016) Guía No. 7 Seguridad y privacidad de la información Recuperado de: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

MinTIC, (2016) Guía Modelo de seguridad y privacidad de la información Recuperado de: http://estrategia.gobiernoenlinea.gov.co/623/articles-8258_recurso_1.pdf

Ministerio de Comerio, Industria y Turismo, Colombia (2014) Decreto 886, Reglamento del Registro Nacional de Bases de Datos. Recuperado de: http://wsp.presidencia.gov.co/Normativa/Decretos/2014/Documents/MAYO/13/DECRETO%20886%20DEL%2013%20DE%20MAYO%20DE%202014.pdf

Ministerio de Comerio, Industria y Turismo, Colombia (28 de mayo de 2014) "Reglamentan los casos, el contenido y la forma en que se debe presentar la información y la publicidad dirigida a los niños, niñas y adolescentes en su calidad de consumidores" [Decreto 975 de 2014] Recuperado de: http://wsp.presidencia.gov.co/Normativa/Decretos/2014/Documents/MAYO/28/DECRETO%20975%20DEL%2028%20DE%20MAYO%20DE%202014.pdf

Ministerio de Comerio, Industria y Turismo, Colombia (2018) Decreto 090, Nueva regulación del Registro Nacional de Bases de Datos.

Moncada Flórez, J. P., (2010) La responsabilidad de los prestadores de servicios de intermediación en la sociedad de la información (Tesis de Doctorado, Universidad de Granada) Granada, España.

Molina, Q. (1999). Tutela de la autodeterminación informativa, ponencia Congreso Internacional Derechos y Garantias en el Siglo XXI. Buenos Aires, Argentina: Asociación de Abogados de Buenos Aires.

Morales, P. F. (1984). La Tutela penal de la intimidad: privacy e informática. Barcelona, España: Barcelona.

Murillo de la Cueva, P. L. (1990). El Derecho a la autodeterminación informativa. Madrid, España: Tecnos.

(1993). Informática y protección de datos personales (estudios sobre la Ley Orgánica 5/1992 de Regulación del Tratamiento automatizado de los datos de carácter personal). Madrid: Centro de estudios constitucionales.

Nietzsche, F. (1947). La voluntad del poder, Aguilar, Tomo IX Buenos Aires.

(1972). Más allá del bien y del mal, Alianza, Madrid.

Novoa, M. E. (1981). Derecho a la vida privada y libertad de información, un conflicto de derechos. México: Siglo XXI Editores.

Office the Australian Information Commissioner (1988): "Australian Privacy Principles Guidelines". Privacy Act.

Office of the Privacy Commissioner of Canada: "Getting Accountability Right with a Privacy Management Program"

Organization of American States OAS (1948). Declaración Americana de los Derechos y Deberes del Hombre. Conferencia Internacional Americana Bogotá Colombia, Recuperado de: http://www.oas.org/es/cidh/mandato/Basicos/declaracion.asp.

Organization form Economic Cooperation and Development - OCDE. (1980). Guidelines on the Protection of Privacy and Transborder Flows of Personal Data Recuperado de: https://www.oecd-ilibrary.org/science-and-technology/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_9789264196391-en

Organización para la Cooperación y el Desarrollo Económico - OCDE. (2002). Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales. Recuperado de: https://www.oecd.org/sti/ieconomy/15590267.pdf

Organización para la Cooperación y el Desarrollo Económico - OCDE. (2013, 1980). Directrices relativas a la protección de la intimidad y de la circulación transfronteriza de datos personales

Organización para la Cooperación y el Desarrollo Económico - OCDE. (2016) Políticas de banda ancha para América Latina y el Caribe: un manual para la economía digital. Recuperado de: http://www.oecd.org/internet/broadband-policies-for-latin-america-and-the-caribbean-9789264251823-en.htm

Organización de los Estados Americanos OEA. (1969). Convención Americana sobre Derechos Humanos o Pacto de San José. Conferencia Especializada Interamericana Sobre Derechos Humanos (B-32). San José de Costa Rica.

Organización de las Naciones Unidas - ONU (1948) Declaración Universal de los Derechos Humanos. Recuperado de: http://www.un.org/es/documents/udhr/.

(1989) Convención sobre los Derechos del Niño. Recuperado de: https://www.un.org/es/events/childrenday/pdf/derechos.pdf

(1990) Principios rectores para la reglamentación de los ficheros computarizados de datos personales. Asamblea General de la ONU Resolución 45/95 de 1990.

(1966). Pacto Internacional de Derechos Civiles y Políticos. Recuperado de: https://www.ohchr.org/SP/ProfessionalInterest/Pages/CCPR.aspx

(2009), Resolución 12/16**,** Recuperado de: https://www.un.org/es/sections/documents/general-assembly-resolutions/

(2012), Resolución 20/8**,** Recuperado de: https://www.un.org/es/sections/documents/general-assembly-resolutions/

(2014), Resolución 26/13**,** Recuperado de: https://www.un.org/es/sections/documents/general-assembly-resolutions/

(2015), Resolución 69/166**,** Recuperado de: https://www.un.org/es/sections/documents/general-assembly-resolutions/

(2015), Resolución 28/16**,** Recuperado de: https://www.un.org/es/sections/documents/general-assembly-resolutions/

(2015), Resolución 70/184**,** Recuperado de: https://www.un.org/es/sections/documents/general-assembly-resolutions/

(2016), Resolución 32/16**,** Recuperado de: https://www.un.org/es/sections/documents/general-assembly-resolutions/

Ornelas, Núñez L. (2010). Compendio de lecturas y legislación (2ª ed.). (A. Editores, Ed.) México.

(2010). La Protección de menores en internet. Recuperado de http://libros.metabiblioteca.org/bitstream/001/307/9/978-968-5954-59-4.pdf

(2007). "El derecho de las niñas, niños y adolescentes a la protección de sus datos personales. Evolución de derechos y su exigencia frentes a las redes sociales", Marcial Pons, España.

Ortiz, R. (2001). Habeas Data, derecho fundamental y garantia de la protección de los Derechos de la Personalidad. Caracas, Venezuela: Frónesis.

Parejo, A. L. (1994). El derecho fundamental a la intimidad. En J. M. a Sauca, Problemas actuales de los derechos fundamentales (págs. 293-310). Madrid, España: Universidad Carlos III y BOE.

Peguera, M., & Tarrés Vives, M. (2010). Marco jurídico de los servicios de las sociedades de la información y del comercio electrónico. En M. Peguera Poch, Principios de derecho de la sociedad de la información (pág. 319 y ss). Cizur Menor (Navarra): Aranzadi-Thomson Reuters.

Pérez, Luño A. E (1987). Nuevas, tecnologías, sociedad y derecho. El impacto socio-jurídico de las N.T. de la información. Madrid: 154.

(2006). La tercera generación de derechos humanos. Cizur Menor (Navarra): Thomson-Aranzadi.

(1986). La Defensa del Ciudadano y la protección de sus datos. Oñati, España: Instituto Vasco de Administración Pública.

(1989). Libertad informática y derecho a la autodeterminación informativa, Congreso sobre Derecho Informático, Universidad de Zaragoza.

(2004). Los derechos fundamentales. 8ª ed. Madrid, Tecnos.

(1994). Dilemas actuales de la protección de la intimidad. Edición de José María Sauca, Universidad Carlos III de Madrid, Boletín Oficial del Estado, Madrid, España. p. 313 y ss.

(1997). Internet navegaciones y abordaje en “La Ley” (Revista Jurídica Española de Doctrina, Jurisprudencia y Bibliografía) No. 4258.

(1999). Aproximación a la Escuela Histórica del Derecho. Boletín de la Facultad de Derecho, p. 15-43.

(2005). Derechos Humanos, Estado de Derecho y Constitución. Noveno Edición, Madrid, España: Tecnos.

(2004) ¿Ciberciudadanía o ciudadanía.com?. Recuperado de http://ebookbit.com/book?k=%C2%BFCiberciudadania+O+Ciudadania.Com%3F&charset=utf-8&lang=es&isbn=9788497840187&source=sites.google.com

(2007). Trayectorias contemporáneas de la Filosofía y Teoría del Derecho (5ª ed ed.). Madrid España: Tebar S.L.

(2008). La protección de los datos personales del menor en Internet. Revista Española de Protección de Datos, pp. 44 y ss.

(2009). La protección de los datos personales del menor en internet. Recuperado de: https://ebuah.uah.es/dspace/bitstream/handle/10017/6441/proteccion_perez_AFDUA_2009.pdf?sequence=1

(2009). Internet y los Derechos Humanos, Revista Derecho y conocimiento vol.2 Universidad de Huelva, España. Recuperado de http://rabida.uhu.es/dspace/bitstream/handle/10272/2550/b15616630.pdf?sequence=1

Pierre, B. (2000). La Fuerza del Derecho. Bogotá, recuperado de https://existenciaintempestiva.files.wordpress.com/2014/03/bourdieu-teubner-la-fuerza-del-derecho.pdf

Pierre, P. (2018) Los códigos de la inteligencia. Dasnyapp Inc, Primera Edición V. I. Recuperado de:https://books.google.com.co/books?id=0zVsDwAAQBAJ&dq=en+fecha+Einstein+dijo:+Todos+somos+muy+ignorantes.+Lo+que+ocurre+es+no+todos+ignoramos+las+mismas+cosas.&hl=es&source=gbs_navlinks_s

Piñar Mañas, J. L. & Recio Gayo M. (2018). El derecho a la protección de datos en la jurisprudencia del Tribunal de Justicia de la Unión Europea España: Reus S.A.

(2016). Reglamento General de Protección de Datos -Hacia un nuevo modelo europeo de privacidad-. Madrid, España: Reus S.A.

(2014). Transparencia, acceso a la información y protección de datos, Editorial Reus. España.

(2008). ¿Existe privacidad?, Lección magistral impartida en la Universidad San Pablo-CEU Madrid, España.

(2005). El derecho fundamental a la protección de datos personales, Protección de datos de carácter personal en Iberoamérica. II Encuentro Iberoamericano de Protección de Datos (pág. 20). Valencia, España: La antigua Guatemala

Policía Nacional de Colombia. (2017). Informe Balance Cibercrimen en Colombia. Recuperado de: https://caivirtual.policia.gov.co/sites/default/files/informe_cibercrimen_2017.pdf

Policía Nacional de Colombia, (2019) Centro Cibernético de la Policia Nacional, Protectio Recuperado de: https://caivirtual.policia.gov.co/

Post, J., Preston, L., & Sachs, S. (2002). Gestión de la empresa extendida: la nueva visión de las partes interesadas. Management Review, 45: 06-28.

Platón, (1987) La República Libro VII, Madrid

Prosser, W. (1960). Privacy. California Law Review (Nº 383).

Puccinelli Oscar., R. (2004). Evolución Histórica y análisis de las distintas especies, subespecies, tipos y subtipos de Habeas Data en América Latina. Universitas, Universidad Javeriana (N° 107), 04-73.

(2013). Acerca de la Evolución y actual autonomía de los derechos "de" y "a" la protección de datos personales, Universidad Nacional de Rosario. Recuperado de: https://es.scribd.com/document/164204062/Acerca-de-la-evolucion-y-actual-autonomia-de-los-derechos-de-y-a-la-proteccion-de-datos

Puente de la Mora, X. (agosto de 2006). Privacidad de la Información Personal y su protección Legal en Estados Unidos. Recuperado el 13 de agosto de 2014, de Alfa- Redi: http://www.alfa-redi.org/node/9027

Ramonet, I. (octubre de 2003). Le Monde Diplomatique. Recuperado el 26 de agosto de 2017, de El quinto poder: Recuperado en: http://www.lemondediplomatique.cl/El-quinto-poder.html

Rawls, J. (1979). Teoría de la Justicia. (D. González, Trad.) Madrid: FCE.

Red Iberoamericana de Protección de Datos RIPD. (s.f.). (2017) Recuperado de http://www.redipd.es/la_red/Historia/index-ides-idphp.php

Rheinhold, H., (1996): La comunidad virtual, trad. cast. de J.A. Álvarez, Gedisa, Barcelona.

Rebollo Delgado, L. (2005) El derecho fundamental a la intimidad, 2ª. Ed. Madrid, Dkyinson.

Red Iberoamericana de Protección de Datos Personales. (2017). (s.f.). Mi "ciberamigo" me chantajeaba. Ingresa en prisión un joven que acosó desde Cádiz a más de 250 mujeres,

muchas de ellas menores, a través de la red. Recuperado de http://www.redipd.es/la_red/Miembros/index-ides-idphp.php El País España: http://www.elpais.com/articulo/sociedad/ciberamigo/chantajea/elpepisoc/20090615elpepisoc_5/Tes

Reglamento 679 (UE) . (27 de 04 de 2016). Reglamento relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales. Bruselas, Bélgica: Diario Oficial de la Unión Europea del 27 de abril de 2016.

Reglas de Heredia. (2003). Reglas mínimas para la difusión de información judicial en internet. Heredia, Costa Rica.

Remolina Angarita, N. (2018). La responsabilidad demostrada en las funciones misionales de la Registraduría Nacional del Estado Civil. Editorial Temis.|

(2015). "Recolección internacional de datos: Un reto del mundo postinternet", en BOE – Boletín Oficial del Estado, Madrid.

(2015). "Accountability y compromiso gerencial en el tratamiento de datos personales, 24-III-2015", En: https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/Accountability-Nelson-Remolina-abril-de-2015.pdf

(2015). "El principio de "Accountability" en el gobierno Obama y en el contexto Iberoamericano 03-II-2015" En: https://habeasdatacolombia.uniandes.edu.co/?p=1804

(2013). Tratamiento de datos personales, aproximación internacional y comentarios a la Ley 1581 de 2012. Legis Editores, Bogotá.

(2012). "Aproximación constitucional de la protección de datos personales en Latinoamérica" Revista internacional de protección de datos personales, No. 1.

(2002). Centrales de información, habeas data y protección de datos personales. Legis Editores, Bogotá.

(2003). Data protection: panorama nacional e internacional. Editorial Legis, Bogotá, Colombia:

(2009). Comisario Europeo del Consumidor: La protección de los menores. Memorias I Seminario Euro-Iberoamericano de protección de datos. Cartagena: Kuneva Meglena.

(2010) ¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo? Revista Colombiana de Derecho Internacional, pp. 489-524.

Riascos G. (2010). Los delitos informaticos, relativos a la intimidad, los datos personales y el Habeas Data. Bogotá, Colombia: Akane, Univesidad de Nariño.

Rincon, R. (2018). Derecho en la era de las TIC, Bogotá, Ecoe Ediciones, Colombia

Rivero H. (2000). El interés del menor. recuperado de https://www.dykinson.com/libros/el-interes-del-menor/9788498490145/

Rodríguez P. (2010). La nueva generación de derechos humanos: origen y justificación. recuperado de https://www.dykinson.com/libros/la-nueva-generacion-de-derechos-humanos-origen-y-justificacion/9788497723015/

Roig, A. (2010). Derechos Fundamentales y Tecnologías de la Información y de las Comunicaciones (TICs). (Bosch, Ed.) Barcelona, España.

Rubenfeld, J. (1989). The right of Privacy. Harvard Law Review, vol. 102(núm. 4), págs. 737-807.

Ruíz, Miguel, C. (1995). La Configuracion Constitucional del Derecho a la Intimidad. (Universidad Complutense de Madrid, Ed.) Madrid, España: Tecnos.

San Agustín (1956) Confesiones, Libro X

Salmón, E., & Blanco, C. (2012). El Derecho al debido proceso en la jurisprudencia de la Corte Interamericana de Derechos Humanos. Bogotá DC: Universidad del Rosario.

Sánchez, M. (2011). Reseña de "El cerebro digital. Cómo las nuevas tecnologías están cambiando nuestra mente" de Small, G & Vorgan, G. Teoría de la Educación. Educación y Cultura en la Sociedad de la Información, vol.12(núm. 1), pp. 417-418.

Sánchez, R. (2016). Extimidad: Exhibir lo íntimo . La Jornada, 6-7.

Sarmiento, M. B. (1997). Constitución política de Colombia comentada por la comisión colombiana de juristas. Bogotá: Impreandes-Precencia.

Schmitt, C. (1982). Teoría de la Constitución, traducción de Francisco Ayala. Madrid, España: Alianza.

Schwartz, P. M. (2004). Property, Privacy and Personal Data, . Harvard LawReview. recuperado de http://paulschwartz.net/pdf/Schwartz-harvard-pdf.pdf

Sennett, Richard (2000), La Corrosión Del Carácter; Las Consecuencias Personales Del Trabajo En El Nuevo Capitalismo, Editorial Anagrama, Colección Argumentos, Barcelona.

Sloterdijk, Peter, Skoza, B., & Thierer, A. (2009). COPPA 2.0: The New Battle over Privacy,Age Verification, Online Safety § Free Speech. The Progress & Freedm Foundation.

Small, G. (2009). El cerebro digital. Barcelona, recuperado de http://www.redalyc.org/pdf/2010/201021400020.pdf

Solove, D. J. (2005). The New Vulnerability: Data Security and Personal Information, en Securing Privacy in the Internet Age. California, Estados Unidos: Stanford Universitu Press.

Steeves, V., & Webster, C. (2008). Closing the barn door: The effect of parental supervision on Canadian Children's online privacy. Bulletin of Science, Technology & Society, pp. 4 y ss.

Stuart Mill, J. (2004), Sobre la libertad, 6a ed. Trad. De Pablo de Azcárate, Madrid, Alianza Editorial.

Suñé, E. (2009). Los Derechos Humanos en el Ciberespacio: La Declaración de Derechos del Ciberespacio. Convención Internacional de Derecho Infórmatico, Electrónico y de las Comunicaciones, (págs. 39-64). Oviedo, España.}

Superintendencia de Industria y Comercio (2017) Guía para la implementación del principio de responsabilidad demostrada (accountability) Recuperado de: http://www.sic.gov.co/noticias/guia-para-la-implementacion-del-principio-de-responsabilidad-demostrada

Superintendencia de Industria y Comercio SIC (2019), Registro de quejas y sanciones de la SIC por violación de datos personales, BPGP Bogotá Recuperado de: http://www.sic.gov.co/sanciones-proteccion-datos-personales-2019

Téllez Aguilera, A. (2002) La protección de datos en la Unión Europea, Madrid, Edisofer

Tenorio, Adame M. (2012). "La protección de datos personales desde el derecho al acceso a la información y como derecho fundamental autónomo. El caso mexicano, Bogotá Universidad de los Andes, Facultad de Derecho No. 1.

Toledo, A. (2013). Conferencia internacional "Derechos Humanos en la Era Digital". Obtenido de Boletín N° 25. Versión Virtual: https://karisma.org.co/2008-2014/?cat=1&paged=9: Digital Rights LAC.

Torres, Ávila, J. (2014). Los paradigmas del control de poder y el principio de división de poderes. Justicia Juris, p. 87-101.

(2015). La fundamentación del derecho a la inclusión digital. Revista Prolegómenos Derechos y Valores, 47-64.

(2016). La transparencia y el buen gobierno: Una perspectiva desde los derechos humanos y las obligaciones de los gobiernos locales. Colombia: Universidad Católica de Colombia.

(2017). La teoría del garantismo: poder y constitución en el Estado contemporáneo. Revista de Derecho (núm. 47), pp. 138-166.

(2012). Del Cloud Computing al Big Data. Barcelona, España: Universitat Oberta de Catalunya (Universidad Abierta de Cataluña).

Torres, J., Becerra Ortíz, J. A., Sánchez Acevedo, M. E., & Díaz García, C. V. (2015). La responsabilidad del Estado por la utilización de tecnologías de la información y comunicación. (TIC). Colombia: Universidad Católica de Colombia.

(2015). El derecho a la inclusión digital. En G. D. Flórez Acero, El Derecho Y Las Tecnologías De La Información Y La Comunicación. (Tic) (págs. p.10 - 37). Colombia: Universidad Católica.

Toscano M., L., Prudente T., M., & Aguilar, T. (2012). Leyes de Protección de datos personales en el mundo y la protección de datos biométricos. Seguridad, defensa Digital UNAM, 68-94.

Tratado de Lisboa, (2008), por el que se modifican el tratado de la Unión Europea y el tratado constitutivo de la Comunidad Europea, firmado en Lisboa el 13 de diciembre de 2007 (2007/c 306/01). Revista de Estudios Regionales, Malaga, España. Recuperado de http://www.redalyc.org/pdf/755/75511138013.pdf

Travieso, J. A. (2014). Régimen Jurídico de los Datos Personales. Buenos Aires, Argentina: AbeledoPerrot S.A.

(2012) –Derecho Internacional 2.0. Revista jurídica de Buenos Aires. AbeledoPerrot S.A. Buenos Aires

(1995). Derechos humanos y derecho internacional (2 ed.). Buenos Aires: Heliasta.

Troncoso, R. A. (2006), La protección de datos personales en busca del equilibrio. Valencia, Tirant lo Blanch. España

Urabayen, M. (1977), Vida privada e información, un conflicto permanente, Pamplona, Eunsa.

UNICEF & The Guardian. (2016). Los derechos de la Infancia y el Internet. Fondo de la Naciones Unidad para la Infancia. Recuperado de: https://www.unicef.org/csr/files/Spanish_UNICEF_GUARDIAN_publication.pdf

Unión Europea. (2000). Carta de los Derechos Fundamentales de la Unión Europea Obtenido de Parlamento Europeo: Recuperado en: http://www.europarl.europa.eu/charter/pdf/text_es.pdf.

Unión Europea, (2016) Reglamento 679 (UE) del Parlamento Europeo y del Consejo, Reglamento relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales. Bruselas, Bélgica: Diario Oficial de la Unión Europea del 27 de abril de 2016.

United States Congress, COPPA (2000) Children's Online Privacy Protection Act. Recuperado de: https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

Valero, J. (2013). La Protección de los Datos Personales en Internet ante la Innovación Tecnológica. Pamplona, España: Aranzadi.

Vazán, V. (2014) Control de las omisiones Inconstitucionales e Inconvenientes Recorrido por el derecho y la jurisprudencia americanos y europeos. Fundación Konrad Adenauer, Bogotá

Vasquez Rocca (2017), Byung-Chul Han: la sociedad de la transparencia, autoexplotación neoliberal y psicopolítica. De lo viral-inmunológico a lo neuronal-estresante, Nómadas. Critical Journal of Social and Juridical Vol. 52 Núm. 4 (2017): Número especial: Settimana Bologna.

Vigo, R. L. (2007). Ética y responsabilidad judicial (1 ed.). Santa Fe: Rubinzal Culzoni.

Villabella Armengol (2015), Los métodos en la investigación jurídica. Algunas precisiones. Universidad Nacional Autónoma de México, Instituto de Investigaciones Jurídicas

Villagrasa, G. (2011). El interés superior del menor. En I. Ravellat Ballesté, Derecho de la persona (pág. 25 y ss). Barcelona: Bosch.

Warmund, J. (2000). Can COPPA work? An analysis of the parental consent measures in the Children's Online Privacy Protection Act. Media and Entertainment Law Journal.

Warren, Samuel and Brandeis, Louis (1890). “The Right to Privacy”. The Harvard Law Review, Vol. 4(Nº 5).Traducción al español (1995) El derecho a la intimidad. Edición a cargo de Benigno Pendás y Pilar Baselga. Ed. Civitas S.A. Madrid.

Apéndices

Apéndice A. Derechos de petición

Tabla 52.

Derechos de Petición - Reglamentación de la Ley de Protección de Datos Personales de NNA en Colombia

Anexo	Nombre
1	Presidencia de la República
2	Ministerio de Industria y Comercio
3	Ministerio de Tecnologías de la Información y las Comunicaciones –MIN-TIC
4	Superintendencia de Industria y Turismo y Comercio
5	Instituto Colombiano de Bienestar Familiar ICBF
6	Policia Nacional
7	Fiscalía General de la Nación

Fuente: Creación propia

Con el fin de escuchar las voces institucionales encargadas de la protección de datos personales en Colombia, se presentó solicitud de información por medio del Derecho de Petición, en virtud de los vacíos jurídicos en la reglamentación del Artículo 7 de la Ley Estatutaria de Protección de Datos Personales Ley 1581 de 2012, relacionada con los derechos de los NNA en materia del adecuado tratamiento de "….sus datos personales, el derecho a su privacidad y protección de su información personal y la de los demás", el cual en forma literal establece:

Es tarea del Estado y las entidades educativas de todo tipo proveer información y capacitar a los representantes legales y tutores sobre los eventuales riesgos a los que se enfrentan los niños,

niñas y adolescentes respecto del Tratamiento indebido de sus datos personales, y proveer de conocimiento acerca del uso responsable y seguro por parte de niños, niñas y adolescentes de sus datos personales, su derecho a la privacidad y protección de su información personal y la de los demás. El Gobierno Nacional reglamentará la materia, dentro de los seis (6) meses siguientes a la promulgación de esta ley. (Artículo 7 de la Ley Estatutaria de Protección de Datos Personales Ley 1581 de 2012)

El 25 de enero de 2017 se presenta la referida petición a la Presidencia de la República de Colombia y a su vez por intermedio de la secretaría jurídica y la Consejería Presidencial para la Primera Infancia, se remite la solicitud por competencia al Instituto Colombiano de Bienestar Familiar, el Ministerio de Tecnologías de la Información y las Comunicaciones –MINTIC y al Departamento Administrativo para la Prosperidad Social. El Departamento Administrativo para la Prosperidad Social remite a la petición al Ministerio de Justicia y del Derecho, el Ministerio de Tecnologías de la Información y las Comunicaciones –MINTIC, Ministerio de Hacienda y Crédito Público, y al Ministerio de Comercio, Industria y Turismo.

El Ministerio de Tecnologías de la Información y las Comunicaciones –MINTIC traslada la petición de solicitud de información a la Superintendente Delegada para la protección de datos personales de la Superintendencia de Industria y Comercio de conformidad con la Ley 1581 de 2012. Entidad encargada de la vigilancia, control e inspección del tratamiento adecuado de datos personales por parte de las entidades públicas y privadas.

El Ministerio de Industria y Turismo, manifiesta respecto al pedimento que ya está reglamentado el tratamiento de datos personales de los niños, niñas y adolescente que contempla la ley 1581 de 2012 mediante el artículo 12 del Decreto 1377 de 2013

El Ministerio de Hacienda y Crédito Público, resalta la importancia de las funciones de la Superintendencia de Industria y Comercio según el artículo 21 de la Ley 1581 de 2012 entre las principales:

"…a) Velar por el cumplimiento de la legislación en materia de protección de datos personales;

d) Promover y divulgar los derechos de las personas en relación con el Tratamiento de datos personales e implementará campañas pedagógicas para capacitar e informar a los ciudadanos acerca del ejercicio y garantía del derecho fundamental a la protección de datos;

i) Sugerir o recomendar los ajustes, correctivos o adecuaciones a la normatividad que resulten acordes con la evolución tecnológica, informática o comunicacional…"(Ley 1581, 2012, art. 21)

Apéndice B. Resumen de entrevistas estructuradas

Tema: Paradigmas, avances y retos entorno a la protección de datos personales de NNA en Colombia

Entrevistas realizadas por: Lucero Galvis Cano, Doctor © en Derecho, Magister en Administración de Empresas, Especialista en Derecho Administrativo, Especialista en Derecho Penal y Abogada (Se anexa los audios):

1. Entrevistado: Nelson Remolina Angarita - Universidad De Los Andes (Actual Superintendente Delegado para la Protección de Datos Personales - 2019)

Fecha: 14 diciembre de 2016

Lugar: Universidad de los Andes – Bogotá

En el desarrollo de la entrevista realizada al Director del Observatorio Ciro Angarita Barón sobre la protección de datos personales en Colombia de la Universidad de los Andes y del Grupo de Estudios en Internet, Comercio Electrónico, Telecomunicaciones e informática, Doctor en Derecho, experto académico y precursor de la normativa en Colombia en materia de Protección de Datos Personales se analizaron los siguientes temas:

¿Desde un contexto histórico cual es el hecho que da inicio a la protección de datos personales? Hay un libro IBM del holocausto y lo cito en el libro está documentado la historia y lo de Roosvelt son hechos pero no son los únicos es como que citan mucho insisto lo de Alemania, insisto como de protección de datos otra cosa es privacidad, privacidad es lo que tienes es que marcar la

protección de datos de los niños que son públicos, privados semiprivados es decir son todos, no solo datos referidos a la privacidad del niño; por eso cuando me mencionas protección de datos es diferente, en algunos casos, son conexos pero hoy son derechos autónomos e independientes. Para que lo tengas presente internacionalmente, en Colombia hecho histórico la Constitución Política de 1991 artículo 15 esos dos párrafos del derecho a conocer: “En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.

La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley.”

En el mundo hay referencias dos razones a la protección de datos una la necesidad de que circulen de un país a otro datos de la gente para efectos de negocios internacionales y eso uno lo puede derivar de los mismo documentos por ejemplo de la OECD donde la exposición de motivos está previsto eso la necesidad de circulación transfronteriza de la información de un país a otro, en los año 70 incluso antes no había regulación entonces se empezó a mirar cual debería hacer para la información de un país a otro sin desconocer las normas locales eso es una razón negocios internacionales. Y la otra razón fue derechos humanos particularmente se ha hecho alusión al caso que está documentado en un libro que se llama IBM del Holocausto y fue como en tiempos de guerra un señor Watson de IBM va a Alemania ofrece un servicio, cuando eso IBM no hacía computadores ni nada sino censos de población y entonces le dice ustedes quieren ubicar gente hagan un censo pidan la información y luego la ubican con esa información ese ha sido como un hecho que infortunadamente implicó como con los datos de la gente fueron determinantes para ubicar una persona y luego llevarlas a campos de concentración y muchos de ellos pues fallecieron. En Colombia el hecho histórico es la Constitución de 1991 esa constitución como parte de los

grandes aportes y novedades en derechos y uno de estos es este derecho de protección de datos que habla el artículo 15 respecto a que las personas no solo tienen derecho a conocer y actualizar su información sino también algo muy importante para tenerlo presente el deber constitucional de administrar correctamente bases de datos eso lo ha dicho la Corte Constitucional pero en la Constitución dice que la recolección, circulación y tratamiento se respetaran los derecho y garantías prevista en la constitución, o sea el hecho histórico que marcó la protección de datos en Colombia fue la Constitución de 1991.

¿Podría determinarse que existe un interés filosófico en proteger este nuevo derecho de protección de datos personales o sólo es proteger un nuevo mercado que surge con el valor económico de nuestros datos? Derechos humanos y negocios no son incompatibles, pero a veces la realidad lo que muestra es que se da más preferencia al negocio que a los seres humanos. Nosotros filosóficamente siempre hemos querido reivindicar la dignidad humana eso dicen los derechos para garantizarla, pero ya a la hora de hacer muchas actividades la prevalencia, casi el gran poder la tienen las empresas, se sugiere mirar el libro de la autoría de Remolina que escribió sobre internet de las empresas. Y vale el dato, si se preguntan cuál es la ley más importante del mundo de protección de datos, es la política de Facebook, en donde se vinculan a más de 1.7 billones de personas en el mundo, a través de un contrato que todos lo aceptan todos los usuarios de Facebook, no hay ninguna ley en el mundo de un país que tenga tanta ámbito de aplicación e injerencia en el mundo que Facebook, una política, si se mira hoy el tema de los datos es como el insumo y el motor de la economía del siglo XXI. Pero es el gran activo de muchas empresas y eso es legítimo desde luego como Facebook, google, pero estas empresas fueron las que primero llegaron a internet antes que los Estados y ellas empezaron a regular, contractualmente, es un instrumento regulador por excelencia en internet y pionero ha sido el contrato y sigue siendo eso,

su relación con Facebook no está vinculada por ninguna ley del mundo, si no por un contrato que aceptas en la relación con Facebook. Eso no es ilegal per se pero a lo que voy es que quienes tienen hoy más información de ciudadanos y fijan las reglas de eso en el mundo son las empresas y no los Estados, eso es una realidad y las empresas tienen su objetivo, que desde luego es legítimo el ánimo de lucro, tienen otros propósitos o finalidades como por ejemplo la protección de los derechos de las personas, por tanto no son incompatibles los derechos humanos ni negocios, pero si es importante un poco ponerle freno en algunas cosas al ambiente empresarial cuando ponen en riesgo los derechos de las personas y de los niños por ejemplo.

¿Cuáles son los principios constitucionales que se amparan por medio de la protección de datos personales en Colombia?

La corte constitucional a través de varias sentencias, hoy un poco más de doscientas ha desarrollado los principios a través de los cuales se deben observar para tratar adecuadamente los datos personales, esto viene desde la sentencia T- 4141 de 1992 hasta este año 2016, cada año hay una sentencias que hable sobre el tema. Los principios que ha desarrollado la corte parte de lo siguiente, primero el principio de libertad que significa que la persona es la titular y propietaria de su información por lo tanto la persona por regla general es la que va a definir a quien le va a dar sus datos, para que fines a quien puede circularlo, a quien puede permitirle acceso a su información. Aquí se parte de algo que es la libertad informática, en donde es la misma persona la que define qué pasa con sus datos, es como cuando usted define quien entra a su casa. Lo mismo lo que pasa es que hoy se entra al ámbito de la gente, no solo en ámbitos físicos, si no con la información de la gente, entonces históricamente siempre se ha planteado que es un principio y como principio tiene excepciones no es absoluto, pero ese es el primer presupuesto que la persona sea la que defina si autoriza o no si alguien recolecta sus datos, para que propósito pueden circular

eso lo primero, segundo son los fines, también la corte ha dicho que el tratamiento de datos es cualquier actividad recolección almacenamiento, circulación, no es para cualquier propósito, pues el que tenga los datos no puede hacer lo que quiera con la información, sino para los fines o que autorice el titular o que fije la ley, entonces también es eso el uso de los datos por ende es limitado otro principio muy importante es la calidad, veracidad de la información y eso va de la mano con el artículo 20 de la constitución le está diciendo hoy en día buena parte de las decisiones de la gente se toma con fundamento en información hoy estamos en el mundo de la información y la información es la clave casi de todo, entonces si esa información no es correcta o no está actualizada puede tomarse decisiones equivocadas sobre las personas, esto es lo que se llama los perfiles virtuales entonces la corte ha dicho que la información debe ser veraz imparcial comprobable, comprensible, actualizada, ha venido poco a poco definiendo que esa información que la gente que la tenga debe ser de calidad y eso es muy importante porque si la información no es de calidad puede afectar los derechos de la gente, voy a darle un ejemplo piense una historia clínica, hospitalizado dos días y le hacen pruebas y en esas pruebas hay varios turnos y todos se anotan en la hoja de la historia clínica, en un primer turno le hicieron exámenes para mirar esa persona que medicamentos no tolera, y encuentran que no tolera la penicilina y no hacen el respectivo reporte en el registro , al siguiente turno no encuentran esa anotación y le aplica penicilina, aquí hay cosas tan inmediatos como ese que afectan directamente la vida de las personas por la calidad de la información, o hay otras cosas que ya son otros efectos , por ejemplo que afecta el buen nombre de las personas, por ejemplo hay gente que ha sido detenidos en cárceles por que reportan el motor de un carro que fue hurtado, el motor fue registrado mal, a nombre de otra persona y mientras se soluciona el problema la persona está detenida, entonces si hay muchas casos reales de la corte constitucional que muestran como los derechos de las personas se ven afectados

por el mal tratamiento de sus datos y uno de esos problemas es que la información no es de calidad entonces eso es otro principio importante, otro tema que ha desarrollado la corte es el derecho al olvido, y eso tiene que ver muy bien con los niños porque? porque hoy en día todo lo que se pone en internet queda en la red y básicamente se pierde el control sobre esa información. Lo que hacen hoy los niños que entran a las redes sociales digitales y las utilizan como ellos consideran, eso va a afectar el futuro de los niños cuando ese niño ya sea adulto va a mirar toda su información que dejo en internet ya sea positiva o negativa va a ser tomada en cuenta para muchas decisiones, y se insiste en lo que se hace cada día mas es la publicidad comportamental, a partir de lo que se hace en internet pues se toman decisiones , pero también lo hace el Estado, cuando vas a solicitar una visa pues también miran el perfil en Facebook previamente, antes de hacer la entrevista. Cada vez los seres humanos son más predecibles por lo que hacemos en internet y por la información que tenemos, y gran parte de los usuarios en internet son los menores de edad, los niños son más impulsivos casi a utilizar la tecnología, porque desde niños contrario a los adultos , tienen la tecnología y la están utilizando y crean fotos, imágenes, datos de ellos, videos de todo tipo, hay un caso en Cundinamarca en donde los niños se hacían videos sexuales y pues los publicaban en internet y a ellos les parecía que eso estaba bien, un niño de esos de pronto cuando ya se adulto esa información es muy posible que le afecte, si un niño de pequeño fue mal estudiante, indisciplinado, sancionado en el colegio, eso va quedando en su historia y entonces lo que ha dicho la corte es que la información negativa, no es algo absoluto y no tiene vocación de ser perenne, porque la gente cambia y no hay que condenar a la gente totalmente por la historia o información negativa de su pasado, hoy en día se está ejercitando el derecho al olvido por ejemplo de los niños y de otras personas, entonces el punto es si tiene derecho una persona a cambiar su vida, a pesar de la información negativa de su pasado y eso tiene que ver con tratamiento de datos, llama mucho

la atención que los niños de hoy pagaran mucho tiempo y dinero tratando de borrar la información de su pasado en internet eso lo dijo el vicepresidente de google su momento alguien, es una frase muy disiente, entonces el derecho de olvido es muy importante porque el niño puede estar haciendo muchas cosas buenas o malas, pero esas cosas van a incidir en su futuro, entonces eso hay que mirarlo también en la limitación de tratamiento de dato personales en el tiempo, no es por siempre y sobre todo la información negativa. Otro principio es la confidencialidad los datos que no sean públicos, quien tiene acceso a ellos deben mantener la reserva y confidencialidad y no estar difundiéndolo a terceros, esa es otro principio que ha desarrollado la corte constitucional, entonces autorización o libertad, veracidad, temporalidad, confidencialidad, calidad y hay otros como proporcionalidad, es decir si usted entrega sus datos para unos fines, solo deben ser los datos estrictamente necesarios para cumplir esa finalidad. Entonces pensemos en un niño que entrega sus datos para jugar en internet, hay que mirar que datos está entregando, si son estrictamente necesarios o si hay algo más, se tiene que mirar porque ya hubo un estudio sobre un barrido de privacidad de niños que mostraba como se recogen datos que van ya desde por ejemplo fotos de niños, y se dice bueno para jugar porque una foto de un niño, bueno cosas así que probablemente en algunos casos puede haber una razón sensata para sustentar por qué que nosotros de pronto no, pero sobre eso ya hicieron un estudio las autoridades de protección de datos, para que se tenga presente, para documentarse, hay unos estudios recientemente que hizo un estudiante de tesis de pregrado, solamente sobre eso, porque que es lo que le gusta a los niños, pues jugar, entonces se puso a investigar sobre empresas que recolectan datos de niños y si lo estaban haciendo de acuerdo a la ley y ninguna lo está haciendo. Hay algo más que ha mencionado la corte que es fundamental en este tema y es el deber constitucional de administrar correctamente los datos personales y ahí los datos de los menores de edad.

Qué tipo de responsabilidad tiene el Estado Colombiano en relación con los datos personales de cada uno de sus asociados, es decir hasta donde podría decirse si se están entregando esos datos. La responsabilidad del Estado está definida en la constitución, tiene unas finalidades estipuladas en la constitución y entre otras es para garantizar los derechos de las personas, por ejemplo expide normas, crea una autoridad, lo que pasa es que eso no solo depende solo del Estado, también depende de los papas, de los centros de educación, de las empresas, de todos, todos tienen que ver con el tema concreto de niños, entonces la responsabilidad del Estado va hasta donde fija la constitución y ahí están las finalidades y para qué están las autoridades si están básicamente para proteger a las personas en su vida, honra, bienes y sus derechos, y garantizar la dignidad humana, como lo hace el Estado? vía regulatoria, vía administrativa con autoridades, pero hay otro tema muy importante requiere de atención es la educación del contexto socio tecnológico actual que es totalmente diferente y ese es un tema que hay que mirarlo como política de Estado, el tema de la educación de los niños para vivir una sociedad digital, y eso falta, desde luego no es de un día para otro, pero hay que empezar a sacar documentos, por ejemplo el artículo 6 de la Ley 1581 dice que el Estado debe reglamentar la materia sobre la protección de datos personales de niños, y hasta donde sabemos no lo ha hecho, es importante investigar porque no lo ha hecho, que ha pasado, hay que reglamentarlo y porque no lo ha reglamentado ya que es su responsabilidad. Pero se insiste este no es un tema solo de responsabilidad del Estado, sino de todos, de toda la sociedad.

¿Desde un contexto mundial los Estados han avanzado en el tratamiento y responsabilidad de los operadores de la protección de datos personales como derecho humano de protección global? Si, internacionalmente las entidades gubernamentales y no gubernamentales han establecido principios la OECD, APEC, ONU, OEA, la red iberoamericana de la protección de datos, las autoridades internacionales de protección de datos han emitido principios, bueno esos principios

no son vinculantes, pero ya a nivel del mundo más o menos se puede decir que el 40% de la población mundial tienen leyes de protección de datos generales porque en el resto de los países hay pero sectoriales, entonces sí ha venido creciendo el tema y esas leyes le imponen unos deberes a los responsables de tratamientos de datos, entonces si se ha avanzado regulatoriamente y en esas regulaciones si se le imponen a los operadores unas obligaciones, en algunos casos generales para el tratamiento de datos de cualquier personas y en otra que son muy escasa específicamente para tratamiento de datos de niños, ósea hay que mirara que regulaciones expresamente lo dice y otras básicamente lo hacen y otras que expresamente lo dicen, la autoridad de protección de datos colombiana si lo hace como hay otras que no, ahora el reglamente Europeo 679 del 20016 por fin se incluyó el tema expresamente de los menores, es importante el reglamento, aunque empieza a regir dentro de tres años, porque será una norma vinculante de aplicación inmediata para todos los países Europeos, pero si las normas que existen, si imponen obligaciones a los operadores en tratamiento de datos como derecho humano, actualmente si lo hay, lo que pasa es que no es en todo el mundo, pero si lo hay.

¿Cuál es el modelo a nivel internacional que más garantiza el derecho a la autodeterminación informativa de los niños en la era digital?

Hay enfoques internacionales de protección de datos, normalmente que habla del enfoque Norte Americano y el enfoque Europeo, siempre se parte de lo siguiente, el que más garantiza, quiere decir que unas cosas es lo que digan las normas y otra cosa es la realidad, entonces en ambas partes del mundo si se protege el derecho de protección de datos, lo que pasa es que de manera diferente, en Europa es un derecho constitucional ósea está en la carta Europea del año 2000 artículo octavo, en la constitución de Estados Unidos no está el tema de protección de datos, no está el tema de intimidad solo esta como en 10 o 12 constituciones pero estatales no la federal, pero allá hace

relación a la intimidad en la acepción clásica, es decir la violación de las comunicaciones, del domicilio y correspondencia, esas cosas la clásica, no de protección de datos, entonces estamos planteando que en una parte del mundo tiene un enfoque parte que este es un tema de naturaleza constitucional ósea del más alto nivel, mientras en otra parte del mundo no se menciona como eso, en una parte del mundo Europa para que se garantice efectivamente dice es necesario que este una autoridad autónoma e independiente, técnica que cumpla esta función, de que la ley efectivamente sea una realidad ese es el enfoque Europeo, mientras que el enfoque Norteamericano no es necesario la autoridad especializada en este tema, en el enfoque Europeo propende más porque haya regulación y autorregulación, mientras el enfoque Americano pretende que haya más autorregulación que regulación, no son excluyentes, Estados Unidos es nacido, no por falta de iniciativa, pero aún no hay una ley de privacidad general, hay una ley del año 1974 law privacy, pero es del sector público, pero ha habido muchas iniciativas para que salga esa ley de privacidad pero normalmente no sale, normalmente hay mucho lobby para que no salga, se recomienda leer dos documentales para que se den cuenta del lobby en este tema, uno busquen un documental que se llama "el costo de lo gratuito" , documental de la BBC y hay una profesora Norte Americana muestra que si hay iniciativas pero que no han pasado por el lobby, porque el interés de eso?, porque el tema de datos ya lo tienen regulado las empresas y no quieren las empresas que se metan los Estados porque puede afectar el modelo de negocio, eso es entendible, pero el tema hay que mirarlo si es sensato o no , hay una película que sacaron , lo que pasa es que esta en alemán, titulada "democracy", muestra como gastan cuatro año para sacar una norma y lo que más resalta es el lobby, más de cuatro mil observaciones sobre eso, este tema es representativo económicamente, si no o hubiese lobby, ósea si no afecta a nadie pues dejan así, el lobby normalmente es cuando afecta

o altera de alguna manera, no solo en los negocios si no el mundo, entonces hay esos enfoques. Cuál es el mejor? eso lo dirá una persona de ese país.

¿Nuestro modelo se ajusta a los estándares y principios internacionales? Sí, Colombia tiene incluso un 90% del modelo Europeo y un 10 % de modelo Norte Americano, y Colombia si sigue básicamente el tema de que hay una norma general, aquí en Colombia esto es un derecho constitucional fundamental, tenemos dos leyes estatutarias, tenemos mucha jurisprudencia, tenemos una autoridad de protección de datos que ha sido muy eficiente, la gestión que ha hecho la SIC en este tema comparada con otras entidades en el mundo, incluso con latino América, le sobra, es una gestión para destacar, pues ahí va, lo que pasa es que como todo no va a ser suficiente la capacidad del Estado, pensemos en seguridad, este no va a tener para poner un policía a cada ciudadano detrás para proteger su seguridad, cosas así tradicionales, ahora pensemos en esto de datos, entonces seguramente habría que hacer más esfuerzos para que la autoridad tenga más capacidad de acción , pero con lo que ha hecho se cree que es muy destacable muy positivo, entonces si Colombia ha hecho ese esfuerzo, tiene unas normas sobre el tema, pero obviamente falta mucho por hacer.

¿Cuál es el reto que tenemos nosotros en materia de transferencia internacional de datos personales? Bueno una cosa es protección de datos en el país y otra es cuando salen del país, entonces aquí pueden salir por transferencias internacionales, transmisión internacional, o recolección internacional, hoy en día lo que está pasando es que los datos de los colombianos los están recolectando desde afuera, ósea transferencia y transmisión es que alguien desde acá los envié, ejemplo que usted desde Bucaramanga envié una base de datos para Miami, transferencia o transmisión, pero otra cosa es que usted desde Miami recolecte datos de los niños en Colombia, por ejemplo, Facebook el 85% de datos que tiene ósea de más de 1.5 billones de personas es de

personas fuera de Estados Unidos y Canadá es un acto de recolección desde afuera, por muchos años , más de cuarenta años se empezó a mirar, el tema de cuando alguien desde acá envía datos a Miami, transferencia o transmisión, bien porque era que pensaban eso, ahora con internet se da más desde afuera que recolecten datos de acá y eso no se está borrando, por ejemplo hay un proyecto de ley de protección de datos, que se está trabajando sobre la recolección de datos de niños, por ejemplo datos que se recolectan con fines de explotación sexual, lo que no es nuevo , siempre ha existido, lo que pasa es que si se mira desde el punto de vista de datos, se están recolectando datos que circulan por todo lado, eso que pasa con niños no es nuevo , lo que pasa es que hay que dar una lectura desde los datos, imágenes, datos sensibles, obtenidos ilegalmente obviamente, solo si se va por ahí, otra cosa es los datos de los niños para jugar en internet, un juego, bueno ahí ya cambia, pero es que hay datos de datos que se pueden recolectar de niños y adultos desde luego, pero pensando en eso, entonces mucha de esta información sale del país, para dar un ejemplo del tema, en Brasil hace unos años se detectaron que a través de una red social digital, la explotación sexual de muchos niños y contacto con redes sociales digitales se hacía desde Estados Unidos, entonces a lo que voy es que hoy estamos en una sociedad transfronteriza, global hiperconectada, entonces los retos de protección de esto con el contexto hoy en día son muchísimo mayores, porque si antes eran locales, en escenarios locales y no se podía hacer todo, entonces piense ahora esto frente al mundo, entonces es enorme el tema, todo lo internacional cada día es cada vez más cotidiano, pero también los retos son también de una dimensión sustancialmente diferente al tema local que antes veíamos eso es un cambio importante del mundo antes y después de internet, eso sí es como un gran reto.

Considera que a pesar de que los Estados utilicen herramientas para proteger el derecho a la intimidad es una utopía la protección frente a Alemania, como las cárceles en la época de la guerra

Nazi se utilizaban para vigilar los presos y estos a su vez vigilaban a los vigilantes Hoy en día el tema de nuestra intimidad hay que mirarlo desde varias enfoques, uno lo que hagan terceros respecto a nuestra información, pero también lo que nosotros hagamos con nuestra información y hasta donde estamos aún nosotros abrimos o cerramos puertas respecto a eso, entonces hoy es claro que estamos en una sociedad hipervigilada, y un ejemplo mire su perfil en Facebook y mire los videos que hace Facebook sobre su información, en donde se replica información relacionada, con los amigos, los gustos, momentos, recuerdos, todos los likes que da la persona , que le gusto que no le gusto, entonces ahí estamos vigilados con la autorización de uno, entonces hasta donde el tema de responsabilidad también donde de uno y no solo de terceros, la empresa entonces obtiene la autorización y maneja los datos, pero no solo vigilados por las empresas si no por los Estados, por las empresas grandes como google, Facebook. El caso es que ahí hay mucha vigilancia, muchas de las cosas son intimas y muchas es con nuestra autorización, hay que otras que no es con nuestra autorización, cuando alguien ya se mete a un sistema de información nuestra y saca datos de nuestra información, que pasa si esto de la protección es una utopía, podemos lograrlo por varias coas, primeros si nosotros facilitamos la información o dos cuando alguien lo hace sin nuestra autorización también lo hace muchas veces sin dejar rastro, entonces es difícil identificar eso, pero el tema de la intimidad es algo que no es de ahora, ósea es un tema de siglos, lo que pasa es que ahora en este contexto de internet es mucho más sencillo acceder a la información de la gente que antes no se podía hacer, por qué? porque la misma gente es la que la está compartiendo, hoy en día somos mucho más predecibles por todas las cosas que hacemos en internet, y mucha de esa información es privada, pero que uno la difunde eso es importante, y es que nosotros somos también responsables de lo que está pasando acá, pues los Estados poco a poco van haciendo cosas

pero no son perfectas ni suficientes siempre, pero el tema es que se están haciendo cosas, pero la verdad falta bastante.

¿En su experiencia profesional conoce casos paradigmáticos sobre el tema en estudio de menores de edad? En Colombia hay que mirarlo con la autoridad de datos que ha llegado, recientemente salió una sanción por ejemplo de los colegios, muchos ni siquiera cumplen la ley, o ni saben que existe, nosotros de hecho hace un tiempo revisamos páginas web de colegios y encontramos básicamente que muy pocos tenían la política para empezar por ahí, pero muchísimas usted podría ver todas las páginas de los colegios en Bucaramanga y ver cuales tenían colgada en la página web y ninguna, seguramente va a encontrar más de cuando lo hicimos en Bogota, que fue hace más de dos años y más del 90% de los colegios no tenían nada, pero este año una investigación, un colegio "Rosher" en donde los padres de familia se quejaban sobre que estaba pasando con las datos de sus hijos y no tenían nada en la visita, entonces ese ya es un tema ahí, porque hay muchas cosas que pueden estar sucediendo, pero no se hacen públicos entonces no se tiene como documentarlos, datos también, si se mira el tema de explotación sexual de menores de edad , esos son datos, en última son datos, imágenes , se tendrían que mirar cifras con la policía nacional quejas que se han dado sobre eso, porque son datos que se pueden poner como ejemplos de lo que está pasando, y de lo que se puede documentar, porque en la tesis doctoral uno tiene que documentar, entonces con cifras de la policía nacional, pueden ser quejas, ahí se puede hacer una idea de lo que se sabe, porque a veces es mucho más lo que no se sabe que lo que se sabe, entonces se tiene que mirar como esas fuentes oficiales con las cifras y quejas se podría hacer un derecho de petición para solicitar información sobre si ha habido quejas, en caso de que se hayan dado las fechas, cuantas, porque lo que se ha sabido es que cada día mas la gente se queja, según cifras de la SIC, vienen aumentando, aunque estas no relacionan datos de menores, pero si han venido

aumentando cada vez más , dos que investigaciones se han dado y tres cuales son los resultados de esas investigaciones, entonces eso ya permite en Colombia aterrizar información, que está pasando de lo que se sabe, pero bueno se puede demostrar.

¿Qué autores y doctrinantes conoce usted que haya estudiado el tema de protección de datos personales a nivel general? De doctrina en Latino América los doctrinantes pioneros y que más han trabajado están en Argentina, Oscar Pucinelli, Pablo Palacio, en Brasil, Danilo Doneda, en México, Lina Ornella. Sin embargo, hay muchas más, incluso en México sacaron en su momento un libro sobre protección de datos menores de edad con ocasión del memorándum en Montevideo, era una compilación de documentos, con ocasión del memorándum en Montevideo, o precedentes dándole fuerza.

El principal protector de los datos debe ser la persona, entonces un modelo ideal es que las personas sean conscientes sobre esto, cuando se está haciendo una investigación y el profesor va desarrollando esto, porque lee y lee, pero ve que muchas veces la gente no es consciente de esto, uno le da más relevancia e importancia al tema de lo que le da la gente a la situación en particular, entonces un modelo ideal partiría de la concientización ciudadana, de la importancia del tema, para que el ciudadano tome decisiones informadas, eso es muy importante, eso entonces se debería hacer con el tema de niños que sea primero la persona, y creo que todos los modelos están partiendo de un punto más allá de este que debería ser el primaria como tal. y lo otro pues si efectivamente que haya normas que digan que se puede hacer y que no se puede hacer, sino autoridades que garanticen que cuando hay una irregularidad, se corrija ese error se sancione, pero no hay que pensarlo todo desde la perspectiva sancionatoria, sino ante todo preventiva. Se debería trabajar mucho el tema de la privacidad en el diseño, hoy en día la sociedad gira en torno a la sistematización de todo, hoy en día casi todos los procesos están sistematizados prácticamente todo

está definido por códigos, y todo lo define el creador de ese código, quien hace el software tiene mucho poder, si usted mira cuanto tiempo gastan en equipos, buscando en internet y todo, ahí finalmente están tomando datos suyos, entonces la privacidad por diseño el primer principio que hay es preventivo, es decir, que lo que se busca es evitar más que reparar, entonces como evitarlo, quien va a crear una página web, una APP piense también en la privacidad y el tratamiento de datos de la gente y adopte medidas para, es inevitable recolectar datos de la gente, sin duda, y esto no está hecho para que no se recolecten, pero que se recolecten los datos estrictamente necesarios, no que se abran puertas para dar usos indebidos con la seguridad puntual que se quiera, fíjese ahorita lo que paso en el caso Colmédica, que ha sido público, entonces casos de pacientes dando historias clínicas, en ese caso también se dieron casos de menores de edad, consultas online que hace el medico con niños y los padres de niños y esa información quedo libre en internet entonces falta de seguridad y esa es la multa en mil cuarenta millones de pesos , es un tema de seguridad. A raíz de este tema ICONTEC está facilitando diplomados sobre autoría de la seguridad de la información, a lo que voy es a una falla en seguridad como se difunde información personal, entonces hay que pensar todo desde del diseño, entonces hay que pensar en la privacidad desde el diseño, eso es muy importante, si la tecnología ha abierto esas puertas, los diseñadores de tecnología y procesos deberían pensar también en la intimidad desde el principio, normalmente no lo hacen , quien crea un software al final el tema no está siendo importante ahí, la protección de datos lo que busca es que sea un tema más, ese el principio que sea preventivo y no reparativo, ese es un buen modelo de protección de dato, porque la idea de la protección no es actuar cuando alguien viola mis derechos si no actuar para que nadie viole tus derechos.

2. Andrés Guzmán Caballero - Director ADALID Security, Legal & Forensic Corporation

Fecha: 11 enero de 2017

Lugar: ADALID Security, Legal & Forensic Corporation– Bogotá

La entrevista realizada a Andrés Guzmán Director ADALID Security, Legal & Forensic Corporation experto académico y profesional en Colombia en materia de seguridad y protección de la información digital se desarrolla de acuerdo a los siguientes temas:

Información judicial en Internet.

Existe información judicial en internet de fallos en los que pueden existir nombres de menores de edad o información de menores de edad, entonces cuando tu vienes y me cuentas tu cuento yo lo que te digo es que tu cuento está muy grande, y que tu cuento es muy amplio, que deberías enfocarte un poco más, yo obviamente sé que vas en la mitad de tu tesis doctoral, pero si te vas para todos lados no le vas a dar absolutamente nada, tienes que enfocarte porque yo sé que este tema de protección de datos es demasiado grande, yo te cuento solamente en las reglas de ley ya hay libros escritos, ahí el tipo que más escribe es una gran amigo mío, es argentino, puedes buscar a Carlos Gregorio o buscarme a mí, hay una consultoría que yo le hice al CENDOJ que es sobre las reglas de protección de la información judicial de los menores en procesos judiciales, como testigos, como víctimas, como lo que sea, ¿qué tratamiento de protección le da la ley? y eso es un problema de reglamentación, ¿por qué no está reglamentada si el niño es un testigo? ¿Por qué no se lleva a otro sitio?, si le hace preguntas por teléfono, por televisión, si le hace la entrevista un abogado, un psicólogo, un pedagogo… eso no está reglamentado y eso debe tener una reglamentación. Lo otro es el tratamiento de los menores.

Las reglas nacen de una reunión de todos los países empezaron a reglamentarlo internamente, por ejemplo: Costa rica lo tiene muy bien reglamentado, tú haces un derecho de petición al

CENDOJ para solicitar el resultado de una consultoría sobre las reglas de Heredia en Colombia, se la va a entregar porque es un documento público y en ella se encuentra como funciona en otros países en USA, México y tengo un acuerdo de confidencialidad de 5 años. Reglas mínimas para la difusión de información judicial en internet Reglas de Heredia (Costa Rica 9 de Julio de 2003), Esta toda la información normativa y jurisprudencial de cada País y como está la publicación judicial en web de cada país, por ejemplo: en Perú encontramos la cara de los depredadores sexuales en internet, aparecen todos y a los señores que deben alimentos, si usted no le da de comer a sus hijos, no lo meten a la cárcel… pero si lo boletean por internet. Por ejemplo en el Salvador aparecen alimentos morosos, así funciona en cada país y la base normativa de todos los países. Nosotros no podemos traer el sistema de Canadá porque nosotros importamos un sistema europeo que es todo lo contrario, aún así nosotros poseemos un sistema americano anglosajón en su gran parte de protección, nosotros importamos el accountability que es un modelo super gringo, no es un modelo coercitivo, importamos un modelo conservador traído por el Superintendente José Alejandro Bermudez que sabe mucho del tema, montó desde su punto de vista personal y no desde el organismo nacional más que desde el punto de vista normativo, porque tú ves la norma la responsabilidad demostrada es para no cumplir la norma y llegar al punto de la seguridad informática de cuidar las bases de datos que ya debería haberse reglamentado el tema técnico y esa norma técnica no la ha sacado porque si no esto de la responsabilidad demostrada se vuelve una locura y el que tiene una cámara en la tienda tiene que cumplir un montonón de normas que no puede cumplir y le toca a ellos hablar es responsabilidad demostrada donde se dice que cumpla esto, pero tranquilo cuando usted la embarre no te voy apretar, es más una situación fáctica más que normativa porque jurídicamente no funciona, ellos quieren crear un hibrido para hacer la norma masa laxa.

El tema de protección de datos no es adaptable de forma muy sencilla a la vida real, es un modelo obligado, decir que Colombia ha adoptado un modelo de protección de datos es una mentira. En España y acá, los empresarios tienen que tener unas bases de datos terribles que no todos pueden cumplir. No solo es acá es en todos lados. Traer la norma europea es una locura, tenemos un sistema americano casi en todo. Le hemos dado más valor al dato que al valor económico. Lo estamos viendo desde el punto de vista filosófico no mercantil.

Al ámbito de protección de niños es exagerado, porque proscribimos el tratamiento de datos, hoy en día pedirle a un menor que no use redes es sacarlo del mundo, de la sociedad… es mejor como funciona la venta de equipos en Inglaterra, que vienen los equipos por defecto con control parental para niños menores de dos años, es decir… tú compras un iPhone, el equipo viene bloqueado, el padre debe desbloquearlo y cuadrar el control de acorde a la edad de su hijo o buscar a alguien que le enseñe, es algo súper bien, cuando le venden a todo el mundo el equipo viene bloqueado, pues a los papás les toca ser un poco avanzados en el tema.

Hay que ayudarles a los papás, hoy en día tienen que aprender a las malas. Y más porque todo esto va muy rápido, así uno como papá quiera estar actualizado es muy complejo.

Bases de datos e intimidad

El sistema de bases de datos no sirve para nada, en el mundo no ha servido para nada; acá en Colombia no sé qué tanto funcione. Me parece que el modelo como está tiene su lógica y está bien estructurado, pero hay que enseñarle a las personas como funciona, el problema es las personas, ellas no saben quién las va a revisar o cómo funciona y nadie lo sabe. Faltan sistemas donde se enseñen a las personas a hacer las cosas bien antes de que las sancionen.

La intimidad es un derecho a que las demás personas no sepan lo que no queremos que sepan, es un derecho propio, salvaguardado jurídicamente y tiene mecanismos de protección, la intimidad

es una figura incomprendida, las personas no tienen ni idea que tienen ese derecho. El problema es que el Estado no nos hace consientes del derecho.

Se deben crear procesos inteligentes, procesos que puedan ser reales.

3. Claudia García Vargas – Asesora Jurídica Superintendencia De Industria Y Comercio

Fecha: 12 enero de 2017

Lugar: Superintendencia de Industria y Comercio – Bogotá

En el desarrollo de la entrevista realizada a la asesora jurídica de la Superintendencia de Industria y Comercio Claudia García Vargas se trataron los siguientes temas:

Frente al tratamiento de los datos personales de los adolescentes que desean ingresar a la universidad se refirió a la consulta de la Universidad del Rosario a la Superintendencia de Industria y Comercio (SIC en adelante), la oficina jurídica emite el concepto respecto a la protección de datos personales que deben tener las universidades cuando hacen propaganda para ofrecer los programas académicos, vinculando a estudiantes que están finalizando su etapa escolar, para lo que se hacen ferias escolares, visitas a colegios, y se recogen datos de asistencia de los menores; se debe ponderar los derechos de los menores, cual era la obligación del Estado en protegerlos, porque la sentencia estaba un poco enfocada a que estaba proscrito el tratamiento de datos personales de menores la sentencia C-748 del 2011, pero como ante la ponderación de derechos fundamentales había que ponderar el derecho a la educación y el derecho a la protección de datos personales, entonces la ley de protección de datos personales dice siempre y cuando con su tratamiento se garantice un bien superior de los menores, se permite el tratamiento de datos, que en este ejemplo es la educación sobre el discernimiento de los menores en edades ya cercanas a la

mayoría de edad, es decir como esa información si les permite a ellos optar por acceder a una universidad y dar sus datos para que sean vinculados y sin la necesidad de la autorización de sus papas, por ejemplo, o de sus representantes legales, se pueden recolectar datos de los menores con los fines únicos de acceder a planes y proyectos académicos para que estos puedan decidir sobre su futuro en la educación sin que necesiten la autorización de los padres, pero lo restringe obviamente a la madurez de los muchachos en última etapa de formación que van y se acercan a la universidad . Por ejemplo ese fue un concepto que va asumiendo la postura frente al tratamiento de datos de menores en esa etapa, que ha dicho la Superintendencia de Industria y Comercio en ese sentido, ahorita mismo ya salió la sanción contra el colegio Clerman, que es la primera entidad educativa sancionada sobre tratamiento de datos de menores o por ejemplo contra un centro comercial Cosmocentro. En el año 2015 se hizo un proyecto de auditoria a colegios y universidades en el país, entonces se visitaron como ocho colegios, dos universidades en general y se pudo establecer que las universidades están trabajando en el tema, pero no han ajustado todos los procedimientos tan grandes que tienen las universidades, por ejempló recolección de datos en proyectos de investigación, todo lo de las encuestas que hacen ya en la parte académica, en la parte administrativa se puede ir estructurando los procesos, hay universidades que tienen un muy buen trabajo, en Barranquilla por ejemplo hay un buen trabajo en seguridad de la información, protocolos de atención y manejan datos de menores de edad, los muchachos que recién ingresan a la universidad, suele pasar ahí el tema de menores de edad, como datos biométricos, de encuestas, se hizo esa inspección y verificación a colegios en donde se encontró que ellos tenían implementado unas prácticas que por naturaleza misma de la función que prestan ellos han adelantado, la psicóloga recibe la hoja de vida del menor, bueno el formulario y muy celosamente lo guardan hacen su proceso de selección, lo conoce digamos las personas que deciden ,

seleccionan y matriculan a unos, pero los colegios normalmente no se habían visualizado que el resto de la información de las personas no seleccionadas que hacían con esos datos y cuando se fue a verificar la mayoría de esos colegios que visitamos, si bien habían incluido autorización dentro del contrato de prestación de servicios, para el tratamiento de datos no habían incluido políticas de tratamiento de la información, entonces si se quiere hacer el ejercicio con colegios particulares de Colombia que ya tengan políticas de tratamiento de datos eso ha sido un poco lo que se hizo este año a raíz de las visitas que se hizo el año pasado, entonces la SIC además de hacer esas visitas de inspección también este año encontró que era absolutamente necesario informar a los colegios, entonces ha participado en cuanto evento y actividad la han invitado con respecto a charlas de menores, tenemos un convenio con red papas, con el cual la idea es a través de ellos iremos nosotros difundiendo este conocimiento, hicimos un proyecto piloto para el Quindío, Armenia, donde a través de las secretarias de educación departamental y municipal, en las reuniones con los rectores se les hablo, luego se fue a los colegios que abrieron sus puertas y a partir de ahí hicimos un perito entre niños, adolescentes y profesores, se hizo un plan piloto para sensibilizar a los colegios y que se formaran en eso, hay un gran desconocimiento, así como en el país hay un gran desconocimiento del tema, aunque hay unas prácticas sanas que ese sector tiene es un muy normal que nadie conozca la historia la menor, pero eso no quiere decir que estén cumpliendo con la ley de protección de datos personales.

Con el tema de transparencia, la secretaria de transparencia de presidencia de la república está estructurando unas directrices generales para poder medir la transparencia en Colombia, es decir las entidades oficiales tenemos unos procesos de que los derechos de petición se tienen que manejar, entonces si se está dando que se da a conocer la información a través de peticiones entonces la plataforma de administración electrónica facilita de una vez la norma, que las entidades

muestran que contratan, es decir la información general de las entidades está a disposición del ciudadano por esa norma, pero no se estaba midiendo, entonces la secretaria de transparencia de la presidencia junto con las entidades digamos el DNP el DANE, el archivo nacional están sacando como unos grandes indicadores que permitan ya medirla y hablar de los niveles de transparencia en Colombia, que pasa con el tema de los datos sexuales, obviamente esa información, datos personales de connotación sensible, ya sea adultos o menores es sensible, y siempre y cuando el DANE por ejemplo todo el régimen de estadísticas está excluido del régimen de protección de datos personales porque la misma ley lo dice, pero toda la información que tanto entidades educativas como de salud reportan ellos lo hacen a nivel estadístico, es decir, por ejemplo yo lo digo porque en los colegios y universidad pasaron , les obliga a reportar al ministerio de educación cuantas mujeres, cuántos hombres, cuantos pertenecientes al grupo raciales, cuantos afros, cuantos indígenas, de estratos bajos están accediendo, pero toda esa información todas las entidades las reportan de manera genérica, es decir que no hay violación, es decir por ejemplo si el colegio recibe tantos alumnos en el año de los cuales tantos pertenecen a tal situación , pero netamente estadístico, es decir ellos no tienen , salvo que sean por los ministerios para certificar por ejemplo como que el muchacho curso en tal colegio, pero eso es parte de un deber legal, entonces es ahí cuando la ley de protección de datos se mete con estas leyes, pero si existe deber legal para tener esa información, obviamente las entidades tienen que reportar, entonces las empresas tienen que reportar, los empleados tienen que reportar los hijos en el sistema, para que los ampare la seguridad social, entonces obviamente cuando uno estudia esta materia tiene que partir del escenario de que la regla general es autorización, política de tratamiento, pero cuando hay unas entidades del sector público que en virtud de sus facultades y funciones recogen cierta información, entonces muchos, DANE es netamente estadístico, colegios frente a ministerios y secretarias de educación son

también temas anonimizados. Pero podríamos decir que si es responsabilidad del Estado cuando digamos x estudiante o el colegio x la mayoría dijeron que somos sexuales, es decir, igual seguimos esa tendencia. Lo que pasa es que ahí ya se junta con otro derecho , que es el derecho a la intimidad , entonces obviamente el género es un dato que se pregunta en todas partes, el género y en Colombia obviamente todavía existe y se sigue diciendo femenino o masculino, pero esa es una información que se solicita, porque todas las entidades educativas deben informar cuantos hombres cuantas mujeres, y si hay una condición digamos una preferencia sexual o un problema derivado ahí , entonces se maneja mirando la norma de historia clínica en donde se tiene una confidencialidad en la información

Tenemos un desarrollo jurisprudencial con las sentencias de unificación…

En Colombia hay dos grandes vertientes, toda la década de los ochenta y finalmente toda la realización de datos personales fue a raíz de todo lo que surgía con lo que hoy llamamos el habeas data financiero y esa información la persona en mora que nunca los bancos la sacaban y había una muerte financiera de las personas, el maestro Ciro Angarita, desarrolla una de las dos tendencias, la que siguió en Colombia, uno que lo ligaba netamente con el derecho a la intimidad y el otro si empezó a hablar de la autodeterminación informativa, eje central la sentencia Alemana del año 1983, porque, el maestro se va a estudiar a Italia y para la época en la que el regresa había salido el pronunciamiento de la sentencia Alemana sobre censo electoral, habla de la autodeterminación informativa, entonces el maestro Ciro viene a Colombiae e introduce el termino, empieza las dos la autodeterminación informática y la autodeterminación informativa, que termina siendo autodeterminación informativa, entonces hay esa línea jurisprudencial que se despega ya de la intimidad y habla ya de la autodeterminación informativa y desarrolla efectivamente que cada persona es quien tiene la facultad de determinar qué tanta información se divulga y cual no, es

fundamentalmente la autodeterminación informativa, ahí hay dos, la sentencia 748 de 2011 en la primera fase, lo más importante es un derecho autónomo e independiente al derecho a la intimidad, si bien pueden juntarse es un derecho totalmente autónomo, pero aquí lo que tiene Colombia en el avance es que desde la década de los ochenta precisamente el desarrollo jurisprudencial habla de ese derecho autónomo que tiene el derecho a la protección de datos, como derecho totalmente autónomo. La sentencia SU 89 no recuerda bien, lo bonito de ver el desarrollo jurisprudencial, en el desarrollo jurisprudencial hay un libro del ex superintendente De La Calle que hace una compilación de todo el desarrollo jurisprudencial aquí en Colombia, este puede servir como guía. Las sentencias de unificación SU 082 del 95 y la SU 089 del 95, que reúnen todo lo que se ha discutido en Colombia en la década de los ochenta que fue donde más pronunciamientos hubo y finalmente ahí permiten conocer maso menos eso, una que va muy ligada a la intimidad y otra que va más ligada a la autodeterminación informativa que es la segunda y es lo que finalmente se termina desarrollando en Colombia, que se cree que es lo más, es el bien jurídico tutelado es la posibilidad de autodeterminar la información, en España la constitución que es muy reciente, en el artículo 18. 1 0 18.2, ellos hablan también de la posibilidad de controlar la información de medios automatizados, porque en las dos partes es eso , el tema de medios automatizados que son los que permiten que la información viaje, ósea el chisme y la publicidad de la información, está también la sentencia que propone el maestro Remolina, quien saca las dos tendencias, Colombia es un modelo hibrido porque toma el derecho a la protección de datos, como un derecho fundamental, que es la línea europea y un poco de la línea Estadounidense en donde existen normas sectoriales que regulan el tema y como un derecho del consumo, entonces en Estados Unidos es un derecho que viene pegado de los consumidores, como un derecho fundamental, a raíz de la segunda guerra mundial y el manejo de la información Nazi y la

declaración de derechos humanos, y todo el manejo de la información que se viene después, pero en Estados Unidos desde 1890 Brandéis habla sobre el derecho a no ser molestado, entonces empieza a desarrollarse un poco la teoría privacy que en Estados Unidos la teoría es privacy que no es la relación para Colombia, porque en Colombia seria la protección de datos personales entonces se suele confundir el privacy con la protección de datos personales, entonces es súper importante en todo el desarrollo marcar la diferencia no es privacidad o intimidad por así decirlo, si no es un tema y el derecho a la protección de datos personales es otro tema completamente diferente e independiente, que pueden estar anclados pero son derechos totalmente autónomos, es recomendada la primera parte de la sentencia 748, porque ellos hablan precisamente de la connotación de un modelo hibrido colombiano, que toma de las dos tendencias, en Colombia porque, en Estados Unidos pues ya se sabe la regulación the privacity act que es la norma 74 de privacidad que es con la que empieza, por ejemplo se habla es de derecho de consumo del operador, de los usuarios de telefonía celular, entonces se habla de toda la reglamentación de telefonía celular y meten eso de la protección de los datos en ese tema, comercio electrónico, entonces sacan la norma que regula todo lo de comercio electrónico y dentro de ella una parte que habla sobre protección de datos personales, en el comercio electrónico, entonces ellos tienen normas por sectores diferentes, los estadunidenses y dentro de cada norma tienen un tema relativo a la protección de los datos personales, ese es el modelo estadunidense, porque Colombia es un sistema hibrido, porque toma dos regímenes el general que da la 1581 y el especial que es el habeas data financiero que la da la Ley 1266 del 2008 entonces es como coger el mundo y organizarlo un poco a la realidad colombiana y la realidad colombiana ha venido caminando con el mundo, no lo copiamos, Colombia ha tenido un desarrollo jurisprudencial sobre el manejo de la información, obviamente ya materializados en una ley que sigue los lineamientos Europeos.

¿Respecto a la preocupación que se tiene digamos al modelo garantista del derecho que pareciera ser que es un utopía al derecho a la intimidad, porque cada vez la conectividad juegan un papel preponderante en la toma de decisiones? Luego del 2001 con el tema de que el terrorismo la seguridad es el bien que hay que proteger del mundo, entonces restringe un poco el tema de la intimidad, se vuelve un poco más pequeño ese núcleo , por eso es siempre una yuxtaposición de valores ahí, el derecho a la comunicación, el derecho a la seguridad, versus el derecho a la protección de la información, a la reserva de las comunicaciones, entonces son unos derechos que en este mundo moderno están así, no solo por el tema tecnológico, sino también por los conflictos políticos hoy en día .

¿En la búsqueda de estar a la par con los principios internacionales considera que nuestro modelo de protección de datos se ajusta a los modelos y estándares internacionales Europeos, estadunidenses o canadienses? Bueno yo creo que Colombia está más dado a proteger el derecho fundamental, es que como en Colombia es un derecho fundamental, si fuera un derecho de consumo se vería netamente como una parte para garantizar, llevar a buen término la transacción, pero en Colombia si es un derecho fundamental, obviamente si me preguntan cuál de las dos tendencias en Colombia es la que más rige, es la tendencia en razón a que es un derecho estrictamente constitucional establecido en el artículo 15 como fundamental , es una tendencia de protección internacional, está muy ligada a la estrategia Europea por que en Europa también es un derecho fundamental, entonces en esa medida como el nacimiento del derecho como tal, está muy pegado a las normas internacionales, de hecho Colombia ha buscado caminar en dos sentidos, uno, mirando cómo funciona el tema de aval ante la comunidad Europea obviamente con el cambio de reglamente Europeo esto se va a cambiar, pero en Latinoamérica solo hay dos países que certificamos como países seguros, Argentina hace 12 o 15 años por la unión Europea y el año

pasado Dubái, es un proceso, lento, demorado, obsoleto en muchos temas pero que Colombia cuando se planteó este tema en el año 2008 , si empezó a caminar en el proceso en que Europa lo certificara como un país seguro en esa medida los principios que trae la ley no son exactos pero si están muy de la mano con el tema Europeo, Colombia tiene una autoridad de protección de datos personales , recuerda el requisito fundamental para todo el continente Europeo, pues para toda Europa, tener ley, tener autoridad y nosotros tenemos eso, países por ejemplo de Iberoamérica como Chile, no tienen una autoridad pero si trabajan sobre el tema de protección de datos personales, entonces si nos ponemos a compararnos con muchos países en Iberoamérica, Colombia está mucho más avanzada a medida que ya tiene autoridad, tiene ley, ha aplicado sanciones, tenemos un desarrollo permanente es decir estamos refiriendo a Perú por ejemplo tiene autoridad también se está trabajando en este tema México no tiene tantos pronunciamientos, entonces si uno se da cuenta, Colombia si busca amparar el derecho, entonces lo que pasa, tenemos registro nacional de base de datos que es el tercer elemento, tenemos ley, autoridad y registro que son las bases de datos, eran tres requisitos que la ley Europea exigía, en su proceso de certificación los hemos trabajado , hoy que es lo pasa, hay una realidad que entre Colombia Estados Unidos y Europa han tenido que renegociar un poco su reglamento para poder intercambiar información entre ellos The right to privacy, que es la nueva norma de certificación para que ellos entreguen y operen y Colombia en este punto es estratégico porque cumple un poco lo de Europa y ahora le está apuntando no solamente a protección de datos, pero si en todos los temas económicos, para ser incluida en la OECD, entonces si ustedes miran la guía de responsabilidad demostrada que tiene Colombia sobre los manejos de seguridad de la información es una tendencia muy Canadá, tienen esa tendencia, porque la misma cartilla lo dic , no es como Europa era o España era estática, ósea si tienes un dato público, lo manejas relajado, pero datos semiprivados ya con más cuidado y

un dato sensible es súper delicado, ese es el modelo de seguridad europeo el modelo de seguridad de manejo de datos colombiano está muy a lo que avanzo el reglamento Europeo, pero estamos muy al manejo de que usted sea responsable de lo suyo, modelo de auto regulación, entonces el mundo está girando hoy hasta ahora según el reglamento Europeo, está girando a la autorregulación, Colombia tiene la guía de responsabilidad demostrado hace más de un año, si donde le dice a las entidades autorregulen en el manejo de la información, usted miso dependiendo de la capacidad administrativa, financiera, su volumen de información establezca procesos y procedimiento que le permitan contar con un programa integral de gestión del dato que es lo que habla la guía y que tenga su oficial de protección de datos, en el mundo el programa oficial de datos hasta ahora lo trae el régimen Europeo y nosotros lo tenemos desde la Ley 1581 del 2012 y con los decretos que lo desarrollan y la guía de responsabilidad demostrado, entonces yo sí creo que Colombia está muy adelante en manera de regulación de estos temas, ha trabajado intensamente estos años para estar a la vanguardia del tema, lo que pasa es una cosa, si uno va a mirar en Facebook solamente tienen dos políticas de protección de datos personales, uno para el mundo y otra para Alemania, Alemania hasta hace unos años fue el único país que tenía una política diferente de Facebook, porque se lo exigía la autoridad Alemana por la necesidad de la protección de su información , entonces si nos damos cuenta esas sociedades han caminado hacia la reserva, nosotros hemos sido un poco líticos y nos cogido la tecnología de la información y la gente todavía se pregunta qué porque tengo que hacer esto, entonces se deben mirar cuales son las realidades sociales totalmente diferentes las que mueven el contexto en Europa o en algunos países de Europa y la realidad en nuestro país entonces nosotros estamos haciendo un proceso de sensibilización frente a la necesidad de que las personas regulen la información y que ahí si ejerza su derecho de autodeterminación informativa, se ha venido trabajando con el ministerio de

educación y la idea es seguir trabajando con las diferentes entidades , por ejemplo el tema del régimen de menores está un poco con el misterio también de salud, seguridad social, esta con el ICBF. Debe haber obviamente una mayor reglamentación, no digo que este hecho todo, faltan pero muchísimas cosas, pero más puntuales, salió una norma sobre video vigilancia, entonces se ha trabajado con diferentes sectores en ese sentido.

¿Qué es lo que más le preocupa respecto al tema de la protección de datos en Colombia? La displicencia de los titulares de la información, y la falta de conciencia de los padres, con el menor, sobretodo la falta de conciencia de los padres. Las universidades deben abrir cursos de protección de datos personales como una manera de sensibilización a la sociedad en general, dentro de las cátedras de derecho dan mucho programación y tecnología pero en general, la nacional abrió hace dos años la cátedra de protección de datos personales fue un reto para los sistemas y servicios de información a los estudiantes de pregrado de las facultades de derecho administración y economía, ingeniería de sistemas entonces tengo alumnos y en los semestres son maso menos treinta abogados y diez ingenieros, es un reto dictarle a los ingenieros norma, pero ha sido muy interesante, ya en el externado en la maestría de derecho y tecnología está la de Sergio Arboleda con la maestría de derecho y doctorado en la Universidad de los Andes una de las electivas fue derecho y tecnología

4. Ricard Martínez Martínez - Universidad De Valencia - España

Fecha: 19 de mayo de 2017

Lugar: Universidad de Valencia

En el desarrollo de la entrevista realizada a Ricard Martínez Martínez, Presidente de la Asociación Profesional Española de Privacidad, Director de la Cátedra de Privacidad y

Transformación Digital de la Universidad de Valencia, Técnico en control de base de datos, Miembro del grupo de trabajo sobre derechos digitales de los ciudadanos del Ministerio de Energía, Turismo y Agenda digital.

¿Cómo valora en general el tratamiento de la información personal de niños y niñas en Europa?

En el marco de la Unión Europea digamos que las aproximaciones han sido más materiales que jurídicas, en el segundo lustro de este siglo (2006-2007) se diseña al menos un par de programas de actuación (Seicer Internet y You Kids Online) donde se producen distintos materiales que analizan nuestros riesgos y las distintas políticas preventivas, además con la emergencia de las redes sociales, se produce una serie de contactos entre Viviane Reding -entonces vicepresidenta de la Comisión- que se reúne con los principales responsables de las redes sociales de la unión europea, para plantear los problemas vinculables al tratamiento de datos personales de menores en el contexto de estas redes.

Existe un reglamento General de protección de datos aprobado en el 2016, que contiene un precepto específico destinado a los menores, definiendo una edad teórica de 16 años para el tratamiento de los datos de carácter personal, edad que está por encima de los mínimos de muchos Estados miembros, por ejemplo España son 14 años, sin perjuicio de que sus legislaciones pueden establecer una distinta; a su vez establece que se adoptarán medidas de protección de datos para esos menores, pero las vincula de algún modo a las disponibilidades de la técnica, se preocuparan de proteger a los menores pero deben tener en cuenta las circunstancias concretas y las posibilidades de actuación. Estaría muy bien si hubiese un elemento adicional, por ejemplo: el contexto norteamericano, en la children's online privacy protection, existe un mandato en el que bianualmente la Federal Trade Commission revisa con unas condiciones materiales y técnicas de aplicación, las medidas de protección de los menores, no se condiciona al Estado de acuerdo a la

técnica de las capacidades de acción, pero se busca que los sectores concernidos identifiquen claramente cuáles son sus prácticas y políticas a la hora de proteger a los menores.

¿Cómo valora en general el tratamiento de la información personal de niños y niñas en España?

En España conozco entre otras cosas porque fui asesor del ministerio de justicia que redactó esta norma y parte del grupo de trabajo que redactó el real decreto 1707 de 2007, el artículo 13 es una norma bastante más acabada que la europea, que establece cuatro principios incompletos, insatisfactorios e insuficientes pero al menos muy precisos:

Establece la no posibilidad de utilizar los menores instrumentalmente para obtener datos de terceras personas, con una excepción cuando los datos que el menor facilite posean un consentimiento o autorización de su padre o madre.

Informar al menor en términos que pueda entender, cuando el menor le pueda prestar el consentimiento y por tanto ya esté informado.

Tercera gran regla ¿quién puede consentir? Pueden consentir los mayores de 14 años, existiendo el consentimiento del tutor legal en caso en el que el menor tenga menos de 14 años.

La última regla es una regla de diligencia en la verificación, y deben establecerse mecanismos para la verificación de la edad del menor para la autentificación de la veracidad del consentimiento de la madre padre o tutor legal.

¿Existen estudios estadísticos del nivel de denuncias que se han venido presentando con ocasión de los niños como víctimas de la afectación a la protección de datos?

Es muy complicado, en relación con la protección de datos tendría que ir a las memorias de la agencia española de protección de datos, el problema es que en las memorias de la agencia de protección de datos normalmente hay referencias puntuales, tendría que buscar allí para ver las infracciones del artículo 6 de la ley de protección de datos cuando estén relacionados con el artículo

13 del reglamento, yo intuyo que son muy escasas las denuncias que se presenta en esta materia y el seguimiento que se hace.

Le voy a contar una verdad que a mí me resulta sorprendente, al parecer en España por ejemplo a diferencia de lo que sucede en Alemania no se abierto ninguna diligencia de investigación en relación con la muñeca Cayla mientras que en Alemania se ha prohibido su venta y se ha ordenado la destrucción de la misma.

¿Considera que la directiva 95/46 ha sido un instrumento jurídico importante para la defensa de los derechos del honor, la intimidad personal y familiar y la imagen de los menores?

Sí, es decir la directiva no, el marco conjunto de protección de datos ha sido una cuestión interesante, la directiva proporciona el contexto (El caldo de cultivo), es decir, ya sabíamos que teníamos que proteger los datos, en el momento que se hace, la directiva la protección de datos de los menores hay que decir que está asegurada, ¿por qué? porque en el año 96 el uso del Internet por parte de los menores es residual, en ese momento en España justo en el 96 además, tenemos dos leyes, una vigente desde el 82 (la Ley orgánica 182) y después la Ley Orgánica del 96 que sigue vigente y que regula los derechos del menor, que una y otra, parten del consentimiento para tratar datos e imágenes sobre todo, porque están pensadas para la imagen y la intimidad del menor. Especialmente el artículo 4 de la ley orgánica 96 que establece condiciones para el consentimiento.

Pero en ese momento empiezan una etapa “pre-internet”, las normas son funcionales, pero esto comienza a entrar en crisis a partir del periodo en torno al 2007, cuando nacen dos fenómenos que ya está impactando a los menores al corto plazo, esos son por una parte las redes sociales y por otra los Smartphones.

¿Por qué el Smartphone? Porque hasta el momento de que existiese el Smartphone, uno podía aplicar ciertas políticas de protección de los menores, consistentes por ejemplo, en que el uso de

internet fuese controlado en un entorno doméstico bajo la supervisión de los padres, es decir una buena política era no prohibirle entrar al menor, pero si acompañarle en el aprendizaje en espacios controlados, en el momento en el que tienes un Smartphone que se conecte a internet, es irrelevante que tú no contrates conexión para ese Smartphone, porque ese Smartphone cuando encuentre una red WIFI se puede conectar, el menor ya desarrolla su vida en el mundo de internet sin ningún tipo de control parental, es imposible. Esos dos momentos son cruciales y son los que dejan anticuada la legislación. Y en ese momento ya no sirven ni las leyes españolas, ni la directiva.

¿Considera que el nuevo reglamento general de protección de datos recoge las necesidades más apremiantes en materia de protección de datos de menores?

No.

¿Cómo valora el reglamento en general?

No le puedo valorar, primero porque no sé cuál va a ser su resultado, segundo porque hace una llamada a la legislación estatal y tercero porque a mi juicio ocurre algo muy divertido con las normas de la Unión Europea y que uno aprende a base de ver jurisprudencia y a base de ver algunas resoluciones sancionadoras de las autoridades de protección de datos. Puede ocurrir que de repente una norma comunitaria se mas importante en la exposición de motivos que el artículo, por poner un ejemplo: si usted ve la guía de la agencia española de protección de datos sobre anonimización o el documento del grupo de trabajo del artículo 29 sobre anonimización, verá que ambas recomendaciones invocan curiosamente sobre el considerando 26 de la directiva, lo importante no está estrictamente en la definición de anonimización de la norma, sino en lo que dice el considerando 26 de la directiva. Esto es una práctica muy usada en el Derecho de la unión europea, debo confesarle que a mí me repugna bastante, que yo siempre pensé que las exposiciones de

motivos aclaraban la intención del legislador, no legislaban, lo cierto es que se está utilizando casi como si fuese el derecho positivo, en el sentido fuerte, es lo que hay.

Bueno tal vez podamos encontrar en la exposición de motivos de ese reglamento una llamada fundamental a la importancia de los datos de los menores, que después se utilizara por los reguladores para su interpretación o aplicación del derecho, lo cierto es que sobre los menores solo tenemos ese artículo.

Respecto de la publicidad desde el diseño y por defecto

Un ejemplo claro de esto lo tenemos dentro de la red social, tenemos la posibilidad de establecer patrones de perfilado adicionales, puesto que el sujeto sabe que está en una red social y viene información sobre sí mismo, además se relaciona con unos determinados sujetos con determinadas características y usa unos determinados likes en un determinado contexto, por tanto, tenemos la posibilidad de establecer una mirada muy precisa sobre ese sujeto, menores en uso ¿Qué podemos hacer? ¿Qué es un menor? Menor es una persona en formación; es capaz de distinguir un menor entre ¿publicidad e información? ¿Tiene la suficiente madurez para identificar cuando se le está manipulando la información contextual para inducir sus preferencias? pues ese menor y no sé si acabar con esto pero… recientemente hemos leído que las redes sociales, por ejemplo, se habían planteado, alguna red como Facebook, ante la abundante información a la que uno puede acceder, definir la información que ve como primera opción al usuario en función de su propio perfil, enseñarle en primer lugar las cosas que potencialmente más le van a interesar, eso significa ¿qué esa red social oriente la conversación para incitar al consumo a un menor?, es decir es posible que si un producto determinado ha pagado las conversaciones primeras que vea el menor de sus contactos se refiera a comentarios sobre ese producto y en tal caso el menor ante una incentivación

del efecto moda: “todos mis amigos están hablando de este juguete”. Claro pero esto no está regulado, pero el reglamento no dice nada de esto.

Respecto a privacidad por defecto lo que hacemos es que las fotografías susceptibles de ser difundidas con carácter general en noticias, tiene unas reglas de captación, tiene que ser fotos generales, no se tiene que identificar al menor o procurar no hacerlo, en todo caso si el padre no ha consentido en que su hijo no salga en una foto de esa clase, su hijo no aparecerá, se hace lo posible para que no aparezca y no aparecerá, y hay corto estadio en el que si la foto de su hijo es fantástica y podría ser utilizable, para por ejemplo una promoción o publicidad, se requiere un consentimiento expreso para de ese tipo de usos, es un modelo de privacidad por defecto extremo, hemos procurado identificar todos los supuestos, además lo llevamos haciendo años, no existe la obligación de tener privacidad por defecto en ese momento, la privacidad por defecto podría diseñarse de otra manera, por qué, porque yo puedo, digámoslo así, no dejar de hacer publicidad por defecto, en el que yo aplicase una regla de carácter más general siempre que cumpliese con los requisitos de información y consentimiento, y siempre que minimizase el impacto de los datos de modo coherente, estrictamente con las finalidades que persigo, mientras yo no me vaya del margen que me permite la norma, yo voy a estar cumpliéndola, lo que digo es que la privacidad por defecto en el caso de los menores debería de tener complementado una regulación, debería tener exigencias claramente definidas.

¿Considera que existen algunos vacíos frente al tema del consentimiento?

Algunos sujetos como Paul Rads, pero también otros en el mundo de la sociología (Alexandra Ocuiste), han demostrado desde una perspectiva jurídica y material, que puede hablarse de lo que podríamos definir como una falacia del consentimiento, en nuestro país y he visto una tesis por Monica Bilazao que abordaba en parte esa materia, la idea básica es que incluso con el

consentimiento explícito que prevé el reglamento general de protección de datos, en el mundo de internet, se produce una relación asimétrica, desde una perspectiva material, un sujeto (ha demostrado a Alexandra Ocuiste entre otros) que la mayor parte de sujetos acepta las políticas de privacidad solo por la existencia de un enlace en las políticas de privacidad, es decir, el mero hecho de la existencia de un texto aparentemente legal, suscita la confianza suficiente, como para que el usuario ni siquiera se moleste en leer las condiciones concretas, es más la secuencia de diseño en este tipo de entornos, hace que la lectura o no de las políticas de privacidad no sean obligatorias, si no opcional, por tanto tú podrías estar concediendo los enteros derechos de tu vida, todos tus bienes y no te estarías dando cuenta, le recuerdo por tanto, eso apunta desde una perspectiva material lo que se llama falacia del consentimiento, por otra parte y materialmente hablando también es cierto y se ha demostrado, que el volumen de información que contienen las políticas de privacidad es de tal intensidad, que uno debería dedicar prácticamente la mitad del año en solo leer políticas de privacidad.

Segunda cuestión, pero no solo es eso, incluso en el caso de que el ciudadano, la persona, estuviese dispuesta a leer esa política de privacidad y a aceptarla o no libremente, se enfrentaría a lo que jurídicamente abordó Paul Rads y es que la mayor parte de las ocasiones se enfrenta a cláusulas y que en España traduciríamos por condiciones generales de la contravención que es algo que se entiende menos, es decir, es un conjunto de condiciones cerradas, que uno toma o deja, pero no tiene la opción de negociar, se produce una asimetría jurídica, es decir, no es un contrato sin el magnate, no es un contrato bilateral, la mayor parte de servicios gratuitos de internet se produce lo que yo llamo una apariencia de donación, es decir, parece que alguien nos está haciendo una buena opción puesto que no pagamos aparentemente por el servicio, y en el marco de esa donación nosotros agradecemos que se nos ofrezca gratuitamente el servicio, y por tanto aceptamos lo que

ahí se pone, eso produce una grande crisis en la concepción material del derecho a la protección de datos y a quien hace el contenido.

Esto tiene con modelos de autorregulación, evidentemente, hay que generar un impulso de comunidad, ¿por qué? y esta es la segunda dimensión, claro que hay que regular la protección de datos, claro que hay que imponer sanciones, claro que hay que regular los delitos, esa es la otra parte de la ecuación, esto es el balanceo, yo promuevo una ciudadanía empoderada, yo promuevo unas empresas comprometidas, y a todo el que se vaya de ese marco, a ese sí, a ese le damos el estacazo, pero en ese juego no puedo pensar que voy a obtener ningún resultado medianamente práctico sólo con el derecho sancionador, eso es imposible, porque cualquier experto que venga de otro sector como el de la medicina, nos dirá que lo que mejores resultados produce en el ámbito médico es la prevención, y que cuando un señor le tienen que poner un antibiótico de última generación que vale miles de euros, mal vamos, lo mejor habría sido que no hubiese contraído la infección, entonces esa es la cuestión.

¿Qué tipo de acción del modelo de autorregulación de protección de datos ha funcionado para garantizar los derechos de los niños y niñas en la era digital?

Bastaría con que, primero el reglamento permita a la industria digital que trate datos de menores, a probar códigos de conductas sectoriales, en el desarrollo de un código de conducta a la luz de los principios de privacidad desde el diseño y por defecto, y guiado por un principio que está en nuestras normas internacionales de derechos del niño y en la ley española, al menos en la Ley Orgánica 196 que es el principio de interés superior del menor, debían ser guía suficiente para que las entidades que tratan datos de menores como objetivo principal, adoptasen políticas respetuosas con los derechos de los menores e incluso tratasen de ir más allá, de lo que la norma permite.

5. Lorenzo Cotino Hueso - Universidad De Valencia - España

Fecha: 30 de mayo de 2017

Lugar: Universidad de Valencia

En el desarrollo de la entrevista realizada a Lorenzo Cotino Hueso, profesor titular de Derecho Constitucional de la Universidad de Valencia España, Coordinador de la Red de especialistas en Derecho de las Tecnologías de la información y las telecomunicaciones, se platearon los siguientes temas:

Respecto a la protección de los datos de las niñas y niñas específicamente en Europa ¿cómo valora esta normativa o este desarrollo normativo?

En general es muy difícil de responder, eso no se puede responder ni en general. La problemática de los datos de menores, es una problemática que afecta muchos ámbitos bastante diversos y entonces lo que hay que ver en general es la atención que ha prestado la regulación legal o en su caso reglamentaria de la problemática específica que presentan los menores, entonces los menores presentan realmente una problemática más que especifica, sino que tienen ámbitos generales que son problemáticos para menores o mayores, se hacen más sensibles cuando son menores, entonces desde mi punto de vista legislativo sí que es cierto que se ha apreciado y hablo sobre todo en España en su caso de la directiva de la unión europea, que regulación específica sobre el menor hay poca expresamente, se ha sentado sobre todo en la cuestión del consentimiento del menor y en la normativa que hasta ahora ha regido hasta el año 2018 en medidas de seguridad, hay algunas referencias concretas de especiales garantías de seguridad cuando hay menores, pero visto desde este punto de vista, sería muy escasa la atención que se ha prestado al menor expresamente en la legislación.

Pero si es cierto los agentes reguladores y las autoridades han tenido especial cautela en las problemáticas relativas a los menores, es decir, no se ve tanto a nivel legislativo, pero si una mayor atención de los órganos de garantía relativa a los menores, por cuando a la respuesta a esta pregunta en general, a la respuesta que se ha dado a las problemáticas del menor, si ha sido suficiente, en su caso si habría que mantenerla en términos de suficiencia, pues hecha la premisa anterior, a la vista no hay mucha regulación, parecería que no hay mucha atención, pero a lo que hay que prestarle atención sobre todo es a si se ha vigilado específicamente cuando hay tratamientos de datos de menores o cuando hay ámbitos sensibles que especialmente afecten a los menores, ahí ya vemos un nivel de análisis legislativos si no de más de práctica y se puede decir que en general, al menos a nivel institucional, hay una atención y de hecho el reglamento europeo, posteriormente también los menores y sobre todo en políticas que insisten que hay que tener mucho cuidado con los datos en menores, mi valoración es que en la práctica los peligros se están dando, que es posible que las instituciones no tengan medios para hacer regir plenamente toda normativa de protección de datos que es bastante garantista, pero para la problemática real y actual que cada día se suscita con los menores pues falta mucho más.

En tema de medidas preventivas, Europa o España también, han toma en consideración algunas acciones que son importantes para avanzar en el tema, frente a todo este avance tecnológico y teniendo en cuenta que los niños hoy en día son niños digitales o nativos digitales que requieren cada vez mayor atención…

Aquí es llamativo tener en cuenta por ejemplo para buscar algunos datos de observatorios de uso de las nuevas tecnologías, pero por ejemplo tiene interés entre otros por la agencia española de protección de datos y su memoria anal, pues se evidencia que es estratégico para el futuro la protección de los menores y lo evidencia en la misma memoria anal que tiene, pone por relevancia

como tanto a nivel europeo, como a nivel español pues que los peligros que asechan en internet a los menores, muchos de ellos vinculados a la privacidad y a la protección de datos, aunque no solo son muchos más a los menores, no solo es protección de datos, es que España precisamente, es que es uno de los países de Europa e incluso del mundo en que más acceso a internet tienen los menores, estamos hablando de datos recientes de menores de 10 a 15 años están accediendo a un entorno al 95% a internet, hablamos de menores 10-15 años y que 9 de cada 10 datos que aunque nos puedan sorprender y aunque ya percibamos esto, los vemos en estudios, 9 de cada 10 menores entre 6 y 14 años navegan por internet, pues claro esos usos de internet acompañados de los peligros que se producen en internet, más allá de la protección real de datos que es aquí lo que nos interesa, pues hacen que haya un especial atención al fenómeno.

Entonces ¿qué medidas específicas están haciendo? pues son muchas medidas que son necesarias de evangelización, campañas preventivas de sensibilización que los padres y menores intenten ser conscientes de que si nos trasladáramos dos décadas atrás estamos dejando ir a nuestros hijos solos a un burdel y por la noche, y que no somos conscientes de ello y que simplemente es que lo están haciendo en el comedor de casa, entonces esas medidas de sensibilización son necesarias y es que no haya un colegio en toda España que no haya recibido charlas de sensibilización sobre los delitos típicos que se comenten sobre menores. tanto a los menores según la edad que tienen, como a sus padres, y es que básicamente las medidas están, han sido impulsadas de alguna manera por la unión europea en el año 2012, básicamente no han parado de hacer campañas de sensibilización, no obstante este es un tema que pues es necesario, la educación, la prevención, los valores es importante sensibilizar, pero al jurista no le interesa, la medidas específicas que se han adoptado como lo había especificado no son tanto normativas, sino como medidas de campañas institucionales y de perseguir focos, sobre todo a lo que más interesa

sobre privacidad y protección de datos en los menores, entonces ahí hay una estrategia de inspección de la agencia española de protección de datos que intentan seguir sobre ellos, sobretodo como grandes prestadores de servicios de internet que traten datos, más allá de que no se guían de los casos más pequeños de delitos y faltas, si no de problemas administrativos para cumplir la normativa de protección de datos, entonces la valoración es difícil, esas son las campañas europeas de sensibilización.

¿Hablar de responsabilidad proactiva en protección de datos de menores es un avance?

El significado sí, es un avance importante, la directiva del 95 que rige hasta el 2018 tuvo muchísimas ventajas, muchísimas virtudes, pero es increíble que desde el año 95 siga rigiendo y el ejemplo que han tomado los países latinoamericanos tomando de modelo, pero ya mas no se le puede pedir, en su época fue un avance y esos principios siguen totalmente vivos, son un avance igual, y en aquel entorno girar en torno al paradigma del consentimiento y los principios de seguridad de protección de datos era algo novedoso, el consentimiento es algo que ya no está tan vivo, tiene muchos problemas, sigue siendo una garantía básica y un derecho fundamental, y además se articulas como derecho subjetivo a través del derecho al consentimiento, pero el consentimiento no es una garantía efectiva, se está demostrando y mucho menos en el caso de los menores, entonces sí que el modelo regulatorio que va mucho más allá de estos clásicos principios y que usa las garantías de principios nacidos de publicidad desde el diseño y por defecto, y garantías efectivas y proactivas de la protección de datos desde las garantías preventivas, la idea básica del reglamento es que la privacidad debe existir desde el nacimiento del tratamiento de datos, este cambio es un auténtico cambio de paradigma y ha de ser ejemplarizante.