



universidad  
de león



*FACULTAD DE DERECHO*

*UNIVERSIDAD DE LEÓN*

*CURSO 2019/2020*

*ANÁLISIS COMPARADO DE LA PROTECCIÓN DE  
DATOS PERSONALES A CARGO DE LAS EMPRESAS DE  
TELECOMUNICACIONES EN CUBA Y ESPAÑA: UNA  
VISIÓN TÉCNICO- JURÍDICA*

COMPARATIVE ANALYSIS OF THE PROTECTION OF PERSONAL DATA IN  
CHARGE OF TELECOMMUNICATION COMPANIES IN CUBA AND SPAIN:  
A LEGAL-TECHNICAL VISION

MÁSTER EN DERECHO DE LA CIBERSEGURIDAD Y ENTORNO DIGITAL

AUTORA: ING. ANNIE ABREU CÍVICO

TUTOR: DR. LUIS ÁNGEL BALLESTEROS MOFFA



universidad  
de león



### *Dedicatoria*

*Dedico este trabajo a mi familia, amigos, compañeros y profesores que me han apoyado para cumplir esta meta y que han aportado su granito de arena en mi crecimiento profesional.*



universidad  
de león



### *Agradecimientos*

*A la Fundación Carolina, a la Universidad de León y al Instituto Nacional de Ciberseguridad, todos de España, por la oportunidad de formar parte de este máster y por los conocimientos adquiridos.*

*A todos los profesores que han sido parte de este programa especialmente a los profesores coordinadores del máster: Dra. Isabel Durán Seco y Dr. Salvador Tarodo Soria, así como a mi tutor Dr. Luis Ángel Ballesteros Moffa, por su apoyo y sus observaciones certeras, por su disposición y ayuda.*

*A todos los compañeros del máster que con nuestras diversas nacionalidades y profesiones creamos una gran familia.*



## ÍNDICE

<b>ABREVIATURAS Y ACRÓNIMOS.....</b>	<b>6</b>
<b>Resumen .....</b>	<b>8</b>
<b>Palabras Clave .....</b>	<b>8</b>
<b>Abstract .....</b>	<b>8</b>
<b>Key Word.....</b>	<b>9</b>
<b>OBJETO Y OBJETIVOS DEL TRABAJO.....</b>	<b>10</b>
<b>METODOLOGÍA .....</b>	<b>11</b>
<b>INTRODUCCIÓN.....</b>	<b>13</b>
<b>CAPÍTULO I: DERECHO GENERAL COMPARADO DE LA PROTECCIÓN DE DATOS EN ESPAÑA Y CUBA. ....</b>	<b>15</b>
<b>I.1 Régimen Jurídico consolidado en la Unión Europea y España. ....</b>	<b>15</b>
I.1.1 Derecho común a la privacidad en la Unión Europea: El RGPD.....	15
I.1.1.1 Antecedentes legales .....	15
I.1.1.2 Aspectos relevantes.....	16
I.1.1.3 Ámbito de aplicación .....	18
I.1.1.4 Competencias .....	19
I.1.2 Adaptación de España al RGPD: la LOPDPGDD.....	20
I.1.2.1 Antecedentes legales .....	20
I.1.2.2 Aspectos relevantes de la LOPDPDG.....	21
I.1.2.3 Ámbito de aplicación .....	23
I.1.2.4 Agencia Española de Protección de datos y otras autoridades de control .....	24
<b>I.2 Modelo cubano en desarrollo. ....</b>	<b>26</b>
I.2.1 El reconocimiento de la protección de datos personales en la Constitución Cubana como un derecho Fundamental. ....	26
I.2.2 Primeros pasos en la implantación de un Reglamento de Protección de datos. ....	28
I.2.3 Regulaciones Administrativas que regulan de manera dispersa la protección de datos personales. ....	30
<b>CAPÍTULO II: DERECHO ESPECIAL COMPARADO DE LA PROTECCIÓN DE DATOS EN LAS COMUNICACIONES ELECTRÓNICAS.....</b>	<b>32</b>



<b>II.1 Sistema Jurídico Europeo y español.....</b>	<b>32</b>
II.1.1 Derecho especial de privacidad en las comunicaciones electrónicas: Directiva 2002/58/CE .....	32
II.1.1.1 Antecedentes.....	32
II.1.1.2 Novedades .....	33
II.1.1.3 Adaptación al ordenamiento español.....	35
II.1.1.4 .....	35
Modificaciones a la Directiva 2002/58/CE .....	35
II.1.2 Propuesta de Reglamento ePrivacy de 2017 .....	38
II.1.2.1 Aspectos Generales del Reglamento ePrivacy .....	39
II.1.2.2 Reacciones a lo establecido en el Reglamento ePrivacy. ....	42
II.1.3 Riesgos específicos regulados a tener en cuenta por las empresas de Comunicaciones electrónicas.....	43
II.1.3.1 Secreto o confidencialidad de las comunicaciones electrónicas.....	43
II.1.3.2 Datos de tráfico (metadatos) y localización de las comunicaciones electrónicas .....	44
II.1.3.3 Cookies .....	45
<b>II.2 La prestación de servicios públicos de Telecomunicaciones en Cuba. ....</b>	<b>47</b>
II.2.1 La protección de datos personales en las nuevas normas jurídicas del proceso de informatización de la sociedad.....	47
II.2.1.1 El Decreto-Ley No. 370 y la protección de datos.....	48
II.2.1.2 Decreto 360 y la privacidad.....	49
II.2.1.3 Resolución 127 .....	51
II.2.2 La privacidad en la prestación de servicios públicos de telecomunicaciones: ETECSA .....	51
II.2.2.1 Disposiciones Administrativas de ETECSA para la protección de los datos personales.....	52
II.2.2.2 Ejemplo de vulneraciones a la privacidad de ETECSA. ....	53
<b>Conclusiones.....</b>	<b>54</b>
<b>Bibliografía .....</b>	<b>57</b>



universidad  
de león



<b>Anexos .....</b>	<b>62</b>
<b>Anexo A. Resumen de la Política de privacidad de Movistar.....</b>	<b>62</b>
<b>Anexo B. Resumen de la Política de privacidad de Telefónica.....</b>	<b>64</b>
<b>Anexo C. Resumen de la Política de privacidad de ETECSA .....</b>	<b>69</b>



## ABREVIATURAS Y ACRÓNIMOS

AEPD	Agencia Española de Protección de Datos
CP	Código Penal
DPO	Delegado de Protección de Datos
ETECSA	Empresa de Telecomunicaciones de Cuba
GT29/CEPD	Grupo de trabajo del Artículo 29 actual Comité Europeo de Protección de Datos
LCD	Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.
LGT	Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
LOPD	Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
LOPDGDD	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
LOTARD	Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal.
LSSI	Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.



universidad  
de león



MINCOM	Ministerio de las Comunicaciones
RGPD	Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales
STJUE	Sentencia del Tribunal de Justicia de la Unión Europea
TC	Tribunal Constitucional
TFUE	Tratado de Funcionamiento de la Unión Europea
TIC	Tecnologías de Información y las Comunicaciones
TS	Tribunal Supremo





universidad  
de león



## Resumen

El presente trabajo de investigación aborda la regulación que protege los datos personales en la utilización de las nuevas tecnologías, y en particular Internet, en los países de España y Cuba. Por un lado, profundiza en el marco general de salvaguardia y cómo ha evolucionado en ambos países. para adentrarse más adelante en los riesgos específicos asociados al funcionamiento de las empresas de telecomunicaciones, las normas que rigen este sector y cómo los avances tecnológicos han creado nuevos tipos de datos que son necesarios proteger para preservar la privacidad de los usuarios y crear confianza en el uso de estos servicios. En el caso de España se analizan tanto las normas de la UE, como SU trasposición al Derecho español y los cambios que traería para las comunicaciones electrónicas la aplicación del nuevo Reglamento *ePrivacy*. Mientras que, en el caso de Cuba, se analizan las normas establecidas por MINCOM y ETECSA que hacen mención a los datos personales y su tratamiento, a la espera de un nuevo Reglamento de Protección de Datos que profundice en el tema.

## Palabras Clave

Tecnologías, Internet, protección de datos, comunicaciones electrónicas, normas jurídicas, reglamento, privacidad, usuarios.

## Abstract

This research work addresses the regulation that protects personal data in the use of new technologies, and in particular the Internet, in the countries of Spain and Cuba. On the one hand, it delves into the general framework of safeguarding and how it has evolved in both countries. to delve further into the specific risks associated with the operation of telecommunications companies, the regulations that govern this sector and how technological advances have created new types of data that need to be protected to preserve the privacy of users and create confidence in the use of these services. In the case of Spain, both the EU



universidad  
de león



rules and its transposition into Spanish law and the changes that the application of the new ePrivacy Regulation would bring for electronic communications. While, in the case of Cuba, the norms established by MINCOM and ETECSA that make mention of personal data and their treatment are analyzed, pending a new Data Protection Regulation that deepens the subject.

### **Key Word**

Technologies, Internet, data protection, electronic communications, legal norms, regulations, privacy, users



## OBJETO Y OBJETIVOS DEL TRABAJO

El objeto del presente estudio es:

*Estudiar y analizar las legislaciones existentes en los países de España y Cuba en materia de protección de datos personales, haciendo especial énfasis en las normas establecidas en el sector de las comunicaciones electrónicas.*

Para lograr el objeto general se trazan los siguientes objetivos específicos:

- 1) *Sintetizar el régimen europeo de protección de datos, describiendo con especial detalle los principales aspectos del RGPD.*
- 2) *Estudiar la trasposición de la normativa española al derecho europeo analizando los aspectos generales de la LOPDGDD.*
- 3) *Conocer el proceso evolutivo del régimen de protección de datos en Cuba, hasta llegar a su inclusión como derecho fundamental en la Constitución de 24 de febrero de 2019.*
- 4) *Profundizar en la protección de datos personales en las comunicaciones electrónicas, con énfasis en los nuevos retos que surgen del uso de Internet.*
- 5) *Caracterizar la actividad del Ministerio de Comunicaciones y ETECSA en la regulación de la privacidad de sus clientes.*



universidad  
de león



## **METODOLOGÍA**

El desarrollo de las tecnologías, el uso de Internet y la automatización de muchos procesos se han estudiado desde la perspectiva ingenieril para lograr avances que beneficien a la sociedad. Sin embargo, estos adelantos se han empleado también para causar perjuicios a las personas y sus derechos fundamentales. Por lo que ciencias como el Derecho pasan a proponer soluciones que sirvan de base para resolver los problemas que surgen en la sociedad. Motivo por el cual se decide abordar desde la perspectiva jurídica el tema seleccionado y utilizar una metodología de investigación que corresponda con la naturaleza propia de las ciencias del derecho.

### **a) Planteamiento del problema y la hipótesis de la investigación**

A través del estudio de la información seleccionada sobre el tema a abordar, para enmarcar el marco teórico y práctico, teniendo en cuenta el objeto y los objetivos previamente determinados, se establece el siguiente problema de investigación.

*Cómo se adaptan los principios y reglas generales de protección de datos personales a los riesgos específicos que en esta materia representan las comunicaciones electrónicas, especialmente Internet y las nuevas tecnologías disruptivas.*

### **b) Fundamentación teórica y planificación de la investigación**

Al ser una investigación que abarca dos países distintos con realidades tecnológicas y políticas diferentes y tratarse de un tema de gran actualidad, para elaborar el marco teórico y estructurar el estudio se llevó a cabo una revisión de bibliografía con soporte en diferentes formatos. A través del acceso a bibliotecas físicas y virtuales, medios digitales y el acceso a normas públicas de ambos países que profundizaban en la materia.

### **c) Métodos de Investigación para el desarrollo del trabajo**



universidad  
de león



Teórico-Jurídico: Este método sentó las bases para identificar los conceptos y la doctrina en materia de protección de datos, partiendo desde una filosofía general para acercarnos al objeto de la investigación hasta llegar a las teorías y doctrinas más concretas en el ámbito de las comunicaciones electrónicas, trazando el diseño y la orientación de la investigación.

Método Exegético-Analítico-Histórico: Con la ayuda de este método se realizaron las interpretaciones a los textos legales que hacían mención a la temática. Realizando su análisis dentro de los períodos históricos en los que se enmarcan cada uno.

Método de Derecho Comparado: La comparación de las normas legales y las realidades sociales de los países vinculados a esta investigación permitieron determinar similitudes y diferencias entre sus normas técnicas y jurídicas. Determinando los objetivos perseguidos por cada Estado en el establecimiento de sus regulaciones, encontrando ventajas y desventajas que pueden ser analizadas en ambos sistemas jurídicos.

#### **d) Resultados, conclusiones y recomendaciones**

El objeto desarrollado en este trabajo se ve reflejado en los resultados obtenidos y las conclusiones presentadas sobre el tema tratado.



universidad  
de león



## INTRODUCCIÓN

El desarrollo de la informática y la aplicación de nuevas tecnologías, como Internet, ha permitido que mejoren de forma exponencial los trámites cotidianos y el modo de vida de los ciudadanos. El incremento en la automatización de estos procesos ha traído consigo un aumento en el tratamiento de los datos que, aunque representan un progreso para las sociedades modernas, se convierte también en todo un desafío para la tutela de los derechos de las personas. Precisamente cuando se le reconoce a los ciudadanos la facultad para controlar estos datos y la capacidad de decidir sobre ellos se le está concediendo el derecho fundamental de protección de sus datos personales.

Como se evidencia anteriormente el surgimiento de la protección de datos como un derecho fundamental tiene una vinculación estrecha con el avance tecnológico que trae consigo la automatización del tratamiento de los datos. Por lo que la brecha tecnológica que existe en cuanto a países desarrollados y subdesarrollados, podría crear también una diferenciación en las normas jurídicas en cuanto a la privacidad. En el caso de España por ejemplo en el año 2004 el acceso a Internet en los hogares se situaba en un 33 por ciento, para el año 2010 se apaga la televisión analógica y en el año 2015 el acceso a Internet desde el móvil superaba el 80 por ciento.<sup>1</sup> Mientras que en Cuba las cifras reflejan un panorama menos alentador; el uso de Internet en puntos de acceso colectivo mediante wifi comenzó en 2013 y el acceso a Internet por datos móviles se prueba por primera vez en diciembre de 2018.

En la comparación entre ambos países España no solo lidera en el aspecto tecnológico, sino que desde el ámbito jurídico es pionera al reconocer como un derecho fundamental la protección de datos en el artículo 18.4 de la Constitución española de 1978. Además, al

---

<sup>1</sup> PÉREZ MARTÍNEZ, J., FRÍAS BARROSO, Z., & UREÑA LÓPEZ, A. (2018). “*La evolución de Internet en España: del Tesis a la economía digital*”. Red.es. <https://www.bcg.com/documents/file100409.pdf>



universidad  
de león



formar parte de la Unión Europea está sujeta a las normas del Derecho Comunitario, que en el tema de privacidad es bastante abarcador, sin estar exentos de debates que apoyan o critican fuertemente algunas regulaciones. En cambio, en Cuba comienza lentamente a interiorizarse la necesidad de la protección de datos en las normas del país, como parte fundamental del proceso de informatización de la sociedad en la que se acerca cada vez más el ciudadano a las tecnologías.

La necesidad de normas específicas que regulen la protección de datos en Cuba se ve especialmente justificado en el sector de las telecomunicaciones, donde se han evidenciado las principales vulneraciones a la privacidad de los cubanos. Debido a esta situación se ha decidido abordar en el presente trabajo de investigación los enfoques que en materia de reglamentación con respecto a este tema se abordan en Cuba. Tomando como referencia la comparación con la experiencia reglamentaria de la UE y en especial España, que en el ámbito específico de las comunicaciones electrónicas se encuentran en deliberación con respecto a nuevas medidas para proteger la privacidad de los usuarios en la era de Internet.



universidad  
de león



## CAPÍTULO I: DERECHO GENERAL COMPARADO DE LA PROTECCIÓN DE DATOS EN ESPAÑA Y CUBA.

### I.1 Régimen Jurídico consolidado en la Unión Europea y España.

#### *I.1.1 Derecho común a la privacidad en la Unión Europea: El RGPD*

##### *I.1.1.1 Antecedentes legales*

La clasificación de la protección de datos como un derecho fundamental en Europa ha sido parte de un proceso evolutivo que tiene sus orígenes en los primeros textos al respecto en la década de los 70. El primer documento reconocido como instrumento internacional vinculante que regula de forma expresa la protección de datos es el Convenio 108 del Consejo de Europa de 1981.<sup>2</sup> El objeto fundamental de este documento era garantizar que cualquier persona ubicada en un Estado firmante se le respetara su derecho a la vida privada, atendiendo al tratamiento automatizado de sus datos de carácter personal.<sup>3</sup>

Mientras que a nivel de la UE el primer documento comunitario armonizador fue la Directiva 95/46 CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, con dos objetivos claramente marcados, por un lado, la protección de los datos personales y por el otro la circulación de estos datos entre los Estados miembros de la UE. Es precisamente esta directiva la que ha sido derogada por el Reglamento General de Protección de Datos 2016/679 RGPD.<sup>4</sup>

Otro fundamento que marcó un hito en el espacio comunitario fue la Carta de Derechos Fundamentales de la Unión Europea del año 2000, que eleva el derecho a la protección de

---

<sup>2</sup> PALMA ORTIGOSA, A. (2018). “Contexto normativo de la protección de datos personales”. En *Protección de datos, responsabilidad activa y técnicas de garantía* (1ra Edición, pp. 9-16). Editorial Reus, S. A.

<sup>3</sup> PAVÓN PÉREZ, J. (2001). “La protección de datos personales en el consejo de Europa: el protocolo adicional al convenio 108 relativo a las autoridades de control y a los flujos transfronterizos de datos personales.” *Anuario de La Facultad de Derecho*, 19, 235–252.

<sup>4</sup> CORRIPIO GIL-DELGADO, M. D. L. R., & MARROIG POL, L. (2002). “El ordenamiento español y la protección de datos personales en el sector de las telecomunicaciones” - Dialnet. *Boletín Del Ministerio de Justicia*, No 1930, págs. 3565-3583. <https://dialnet.unirioja.es/servlet/articulo?codigo=286299>





datos como un derecho fundamental, plasmado en el artículo 8, distinguiéndolo además del derecho a la intimidad.<sup>5</sup> Sin embargo, no es hasta el año 2009, después del tratado de Lisboa, que se le otorga a la Carta el mismo valor que los Tratados originarios.<sup>6</sup>

Además de las normas anteriormente citadas, destaca la importancia del Tratado de Funcionamiento de la UE, más conocido como TFUE, que en su Artículo 16 reconoce el derecho a la protección de datos personales e introduce una base jurídica específica para la adopción de normas relativas a la protección de datos de carácter personal.<sup>7</sup> Precisamente, y atendiendo a lo planteado en el Considerando 1 del RGPD, el Artículo 16 apartado 1 del TFUE y el Artículo 8.1 de la Carta, son los fundamentos legales habilitantes en los que se ha basado el legislador europeo como base para el nuevo Reglamento General de Protección de Datos.

#### *1.1.1.2 Aspectos relevantes*

El RGPD entró en vigor en los países de la UE el 25 de mayo de 2018, persiguiendo dos objetivos fundamentales regular el derecho a la protección de los datos y garantizar la libre circulación de los mismos, aportando un conjunto de novedades con respecto a la Directiva 95/46. Entre las primeras a analizar están las relacionadas con la actualización de los principios rectores para el tratamiento de los datos, recogidos en artículo 5. Resaltando el principio de tratamiento lícito y leal de los datos personales y unido a estos, la inclusión del principio de transparencia, esta modificación con respecto a la regulación previa aumenta el deber de información del responsable del fichero, así como el resguardo de la documentación

---

<sup>5</sup> DE FARAMIÑAN GILBERT, J. M. (2001). “La carta de los derechos fundamentales de la Unión Europea.” *Revista de Estudios Regionales*, 01, 237–264. <https://econpapers.repec.org/RePEc:rer:articu:v:01:y:2001:p:237-264>

<sup>6</sup> El parlamento europeo para garantizar la conformidad de la legislación y las políticas relativas a los derechos fundamentales necesitaba de la existencia de una declaración de derechos específica de la Unión. En el año 2000 el Parlamento, el Consejo y la Comisión proclamaron solemnemente la Carta en Niza. Tras ser revisada, fue proclamada de nuevo en 2007. Sin embargo, la Carta solo tuvo efecto directo tras la adopción del Tratado de Lisboa el 1 de diciembre de 2009, como establece el artículo 6, apartado 1, del TUE, convirtiéndose así en una fuente vinculante de Derecho primario.

<sup>7</sup> ZABALLOS PULIDO, E. (2013). “La protección de datos personales en España: Evolución Normativa y Criterios de Aplicación” [Universidad Complutense de Madrid]. <http://eprints.ucm.es/21927/1/T34576.pdf>



sobre el tratamiento de los datos de forma tal que sea apliquen mecanismos sencillos de ejercer el derecho a la información.<sup>8</sup>

Mientras que para proteger dicha información del alcance de terceros, se establecen las bases sobre las que se otorga el consentimiento, considerado la columna legal del tratamiento de los datos personales, más allá de los términos anteriormente utilizados como consentimiento inequívoco, o explícito, se define el consentimiento del interesado como una acción afirmativa o declaración, por lo que no se permitirá el consentimiento tácito y basado en la inacción.<sup>9</sup> El artículo 7 establece como deber la capacidad del responsable de demostrar que obtuvo el consentimiento necesario del titular de los datos.

En cuanto a los menores el Artículo 8 del RGPD propone su regulación, estableciendo como edad límite para otorgar el consentimiento los 16 años, en caso de ser menor bastaría con la autorización del titular de la patria potestad o tutela, permitiendo a los Estados Miembros establecer edades diferentes en sus normas nacionales, sin que esta sea menor de 13 años.

El RGPD parte del principio de responsabilidad activa, que se basa en que la actuación por parte de los encargados o responsables de los datos no es eficiente cuando ya se ha cometido la infracción. Por lo que se establecen medidas a adoptar, que rigen desde sus obligaciones hasta la exigencia de designar un DPO en determinados supuestos recogidos en el artículo 37. Es precisamente esta figura del DPO una de las novedades que aporta el reglamento, regulando sus funciones mínimas destinadas principalmente al asesoramiento y supervisión.<sup>10</sup> Las funciones exclusivas otorgadas al DPO realzan su importancia con respecto al

---

<sup>8</sup> MEJÍA CAMBAR, O. (2019). “Análisis al reglamento General de Protección de Datos en la Unión Europea: Un Vistazo a la Actualidad de la Era Digital.” *La Revista de Derecho*, 40(1), 93–104. <https://doi.org/10.5377/lrd.v40i1.8909>

<sup>9</sup> ORTEGA GIMÉNEZ, A., & GONZALO DOMENECH, J. J. (2018). “Nuevo marco jurídico en materia de protección de datos de carácter personal en la Unión Europea.” *Revista de La Facultad de Derecho*, 44, 01–35. <https://doi.org/10.22187/rfd2018n44a2>

<sup>10</sup> GARCÍA MAHAMUT, R. (2019). “Del reglamento general de protección de datos a la lo 3/2018 de protección de datos personales y garantías de los derechos digitales.” In Rosario García Mahamut & iBeatriz T. Mallén (Eds.), *El reglamento general de protección de datos un enfoque nacional y comparado. Especial referencia a la lo 3/2018 de protección de datos y garantía de los derechos digitales* (TIRANT LO, pp. 95–103).



universidad  
de león



Responsable de Seguridad, fomentando la cultura del *compliance* en materia de protección de datos.<sup>11</sup>

En cuanto a los derechos que poseen los titulares de los datos, se regula de forma explícita el derecho al olvido, que no se encontraba expresamente en la Directiva comunitaria, aunque sí se podía desarrollar a través de principios como el de calidad y finalidad de los datos. Este derecho se recoge en el artículo 17 como derecho a la supresión de los datos y a pesar de tener su origen en derechos ya existentes, toma forma en el ordenamiento jurídico, pudiendo ser ejercido y solicitarse bajo ciertas condiciones la supresión de los datos a cualquier responsable del tratamiento.<sup>12</sup>

#### *1.1.1.3 Ámbito de aplicación*

El ámbito de aplicación aparece regulado en los artículos 2 y 3 del RGPD, que los divide en ámbito material y territorial. El ámbito material coincide en contenido con el de la Directiva 95/46, en cuanto a su aplicación al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales, aunque cada vez es más escaso el método manual para tratar los datos, no deja ventanas abiertas al tratamiento que no sea cubierto por el RGPD.

Quedan excluidos los tratamientos en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión, como puede ser el tratamiento de datos de Seguridad Nacional. Se excluyen además los llevados a cabo por los Estados miembros, cuando estén relacionados con la Política Exterior y de Seguridad Común de la UE. No entran en el ámbito los datos tratados por personas físicas en actividades personales o

---

<sup>11</sup> ORTEGA GIMÉNEZ, A., & GONZALO DOMENECH, J. J. (2018). “Nuevo marco jurídico en materia de protección de datos de carácter personal en la Unión Europea.” *Revista de La Facultad de Derecho*, 44, 01–35. <https://doi.org/10.22187/rfd2018n44a2> Podemos entender como *compliance* los procedimientos adoptados 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.

<sup>12</sup> COBACHO LÓPEZ, Á. (2019). “Reflexiones en torno a la última actualización del derecho al olvido digital.”. *Revista de Derecho Político*, 1(104), 197-227. <https://doi.org/10.5944/rdp.104.2019.24313>



domésticas, ni los que son por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención.

En el ámbito territorial, el RGPD conserva al igual que en la Directiva el criterio de establecimiento en la UE. Según el artículo 3.1 será aplicable al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no. Lo que significa que el RGPD es aplicable siempre que exista un establecimiento en la Unión, con independencia del país en que esté localizado.<sup>13</sup>

#### *1.1.1.4 Competencias*

El RGPD establece la competencia a las autoridades de control de cada Estado miembro, dotándolas de funciones y poderes, convirtiéndolas en el principal mecanismo del derecho nacional para hacer cumplir la legislación de la UE en cuanto a la protección de datos personales. La petición ante la afectación de datos personales puede hacerse a través de una reclamación ante la autoridad de control, y a través de la vía judicial contra el encargado o el responsable del tratamiento. De conformidad con lo recogido en el artículo 55 del RGPD cada autoridad desempeña sus funciones en el territorio de su Estado, o cuando el tratamiento sea llevado a cabo por las autoridades públicas de su Estado miembro.<sup>14</sup>

Atendiendo a lo planteado anteriormente cada autoridad es competente para llevar a cabo investigaciones e intervenir en su territorio, pero como puede suceder, sobre todo en el ámbito de Internet, el encargado y el responsable pueden tener sus establecimientos en más de un Estado Miembro, o por el contrario, el tratamiento de los datos puede afectar a interesados en

---

<sup>13</sup> GONZALO DOMENECH, J. J. (2017). "La aplicación del nuevo RGPD en el contexto del tratamiento de datos en la UE." *REVISTA LEX MERCATORIA Doctrina, Para xis, Jurisprudencia y Legislación*, 4(1), 37. <https://doi.org/10.21134/lex.v4i1.1303>

<sup>14</sup> DE MIGUEL ASENSIO, P. A. (2017). "Competencia y Derecho aplicable en el reglamento general sobre protección de datos de la Unión Europea.". *Revista Española de Derecho Internacional*, 69(1), 75-108. <https://doi.org/10.17103/redi.69.1.2017.1.03>



universidad  
de león



diferentes Estados, por lo que para el control del tratamiento transfronterizo el RGPD establece el mecanismo de “Ventanilla única”. Este mecanismo consiste en asignar una autoridad de control principal, que será la del principal establecimiento o único establecimiento del responsable o encargado del tratamiento. En las actividades transfronterizas la autoridad de control principal será el único interlocutor con el responsable o del encargado del tratamiento y de la cooperación con otras autoridades de control, la cual comprende intercambio de información y asistencia mutua.<sup>15</sup>

### *1.1.2 Adaptación de España al RGPD: la LOPDPGDD.*

#### *1.1.2.1 Antecedentes legales*

El principal fundamento legal en hacer mención a la protección de datos personales en España es la propia Constitución Española de 1978. En el artículo 18 se presenta a la privacidad desde un ámbito más amplio que la mera protección a la intimidad de las personas. Se hace alusión expresa a la informática, ofreciendo no solo garantía frente a su uso indebido a todos los derechos, sino que amplía también la cobertura a todos los procedimientos o medios técnicos que pudieran afectar al ejercicio de la libertad.<sup>16</sup> Para el desarrollo de este artículo se dicta el 29 de octubre la Ley Orgánica 5/1992, de Regulación del Tratamiento Automatizado de Datos de Carácter Personal. La LOTARD contenía como objetivo principal limitar del uso de la informática y otros medios de tratamiento automatizados, para hacer cumplir la protección del derecho al honor, la intimidad y la propia imagen, lo que delimitaba su ámbito de aplicación a los ficheros automatizados.<sup>17</sup>

---

<sup>15</sup> AGENCIA de los Derechos Fundamentales de la Unión Europea., & Consejo de Europa (Estrasburgo). (2018). *Manual de legislación europea en materia de protección de datos*. <https://doi.org/10.2811/60145>

<sup>16</sup> PÉREZ LUÑO, A. (1981). “Informática y libertad: Comentario al artículo 18.4 de la Constitución.” *Revista de Estudios Políticos*, 24, 31–54.

<sup>17</sup> ZABALLOS PULIDO, E. (2013). “La protección de datos personales en España: Evolución Normativa y Criterios de Aplicación” [Universidad Complutense de Madrid]. <http://eprints.ucm.es/21927/1/T34576.pdf>



universidad  
de león



El 24 de octubre de 1995 la Unión Europea publica la 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. Con este antecedente para adaptar el ordenamiento jurídico español a las normas de la UE, el 13 de diciembre de 1999 se aprueba la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD), que deroga a la antigua LOTARD. El ámbito de aplicación de la LOPD incluía no solo a los datos situados en ficheros automatizados, sino además los datos personales recogidos en soporte físico que pudieran ser sometidos a tratamientos automatizados.<sup>18</sup>

A partir de la aplicabilidad directa del Reglamento Europeo 2016/679 surge la necesidad de aprobar una norma interna que sirva de complemento para la aplicación de la legislación europea, que ya no podía ser cubierta por la LOPD. La adaptación del derecho español al RGPD se ve efectuada con la entrada en vigor el 7 de diciembre de 2018, de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD), que deroga a la anterior LOPD y asimismo derogó el más reciente Real Decreto Ley 5/2018, de 27 de julio.<sup>19</sup> Esta derogación permite que las lagunas jurídicas que existían entre la normativa nacional previa y el RGPD, encontraran un panorama normativo más claro sobre la protección de los datos personales en España.<sup>20</sup>

### *1.1.2.2 Aspectos relevantes de la LOPDPDG*

La LOPDGDD no es en sí misma una norma de trasposición o transformación, sino que se crea como complemento al Reglamento 2016/679, para desarrollar el Derecho de la Unión Europea sobre la protección de datos, sin embargo, eso no la ha desprovisto de un conjunto de novedades. Primeramente, cabe destacar la regulación referente a la tutela de los datos de

---

<sup>18</sup> CORRIPIO GIL-DELGADO, M., & MARROIG POL, L. (2002). “El ordenamiento español y la protección de datos personales en el sector de las telecomunicaciones” - Dialnet. *Boletín Del Ministerio de Justicia*, No 1930, págs. 3565-3583. <https://dialnet.unirioja.es/servlet/articulo?codigo=286299>

<sup>19</sup> SALMANTICENSIS, A. I. (2019). Personales y garantía de los derechos digitales. *Crónica de Legislación*, 7, 254–259.

<sup>20</sup> JEFATURA DEL ESTADO. (2018). Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales. *Boletín Oficial Del Estado*, 294(6 de Diciembre de 2018), 5–68.



universidad  
de león



personas fallecidas recogidas en el artículo 3. A pesar de no incluir el tratamiento de estos datos en su ámbito de aplicación, el referido artículo la Ley permite que las personas vinculadas con el fallecido puedan solicitar el acceso, rectificación o supresión de estos datos, siempre y cuando el propio fallecido no haya solicitado una prohibición expresa.<sup>21</sup>

Con respecto a la edad mínima para prestar el consentimiento el RGPD como se ha mencionado, ha establecido como límite 16 años, pero dejando a disposición de los Estados Miembros la potestad de fijar una edad menor. La LOPDPDG en su artículo 7 estableció esta edad hasta los 14 años, mientras que el artículo 12.6 de la norma, expresa que “en cualquier caso los titulares de la patria potestad podrán ejercitar en nombre y representación de los menores de 14 años, los derechos de acceso, rectificación, cancelación, oposición o cualesquiera otros que pudieran corresponderles”.

Se considera la figura del DPO como representativa entre las novedades que establece el RGPD y la norma española mantiene esta destacada importancia. En la LOPDPGDD se hace obligatoria la asignación del DPO en determinados supuestos y entidades recogidos en los artículos 37.1 y 34 respectivamente. Las entidades que nombren un DPO deberán notificar a la AEPD en un plazo no mayor a los 10 días. Precisamente entre los más recientes procedimientos sancionadores de la AEPD se encuentra la multa de 25.000 euros a la empresa tecnológica GLOVO, por no contar con un delegado de protección de datos, siendo la primera de este tipo en España.<sup>22</sup>

Otra novedad que aporta esta nueva Ley es la inclusión del Título X *Garantía de los Derechos Digitales*. A pesar de ser creada como complemento al Reglamento, la Ley Orgánica no se limitó solo a contemplar los derechos incorporados en la normativa

---

<sup>21</sup> MINERO ALEJANDRE, G. (2019). “Nuevas tendencias en materia de protección de datos personales. La nueva Ley Orgánica y la jurisprudencia más reciente.” *Anuario Jurídico y Económico Escorialense*, 52, 125–148.

<sup>22</sup> PS: N°: PS/00417/2019 de la AEPD Se considera que la falta de designación de DPO, al realizar la empresa un tratamiento de datos personales a gran escala, da lugar a la vulneración del artículo 37.1b) del RGPD en relación con el artículo 34 de la LOPDGDD.



universidad  
de león



comunitaria, sino que a través de los 19 artículos que componen el Título X adiciona un segundo conjunto de normas destinadas a garantizar los derechos digitales.<sup>23</sup> La garantía de este tipo de derechos se respalda en artículo 18.4 de la Constitución Española, no sin resaltar la necesidad de que los nuevos derechos de la era digital alcancen el rango constitucional.<sup>24</sup>

Una serie de estos derechos digitales están destinados a regular el uso de las tecnologías en el ámbito laboral, que hasta el momento estaba protegida solamente por doctrinas jurisprudenciales del TC y el TS. La LOPDGDD establece normas específicas para el tratamiento de dispositivos digitales, aparatos de videovigilancia, grabación de sonidos y geolocalización en el ámbito laboral. Se incluye un nuevo derecho referente a la desconexión digital para velar que se cumplan los horarios de descanso, vacaciones e intimidad personal. Mientras que el artículo 91 dota a los convenios colectivos de la capacidad de ampliar estas garantías y libertades relacionadas con la protección de datos personales y de derechos digitales en la esfera laboral.<sup>25</sup>

### *1.1.2.3 Ámbito de aplicación*

Teniendo en cuenta lo expresado en el artículo 2 relativo al ámbito de aplicación de la LO 3/2018, será aplicado lo dispuesto en los Título I al IX y en los artículos 89 a 94, establecido para cualquier tratamiento de datos personales contenidos o destinados a ser incluidos en un fichero, sujeto tanto para tratamientos total o parcialmente automatizados y los que no sean automatizados, de manera que se cubran todas las posibles variantes en el tratamiento de los datos personales.

---

<sup>23</sup> Estado, A. E. B. O. del. (2018). Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. *Boletín Oficial Del Estado (BOE)*, 294, 1–68.

<sup>24</sup> SALMACENTIS, A. I. (2019). "Protección de datos y derechos digitales". *Crónica de Legislación*, 7, 254-259.

<sup>25</sup> SERRANO OLIVARES, R (2018). "Los derechos digitales en el ámbito laboral: comentario de urgencia a la ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales." *IUSLabor*, 3/2018, 216–229.





universidad  
de león



Quedan exentos de su aplicación los tratamientos que hayan sido excluidos del ámbito de aplicación del Reglamento, así como tratamientos sometidos a normativa sobre protección en materias clasificadas. Además se excluyen de aplicación los datos de las personas fallecidas, sin perjuicio de lo contenido en el Artículo 3, que posibilita que las personas vinculadas al fallecido por razones familiares o sus herederos puedan solicitar el acceso, rectificación o supresión de los datos del fallecido.<sup>26</sup>

Al mismo tiempo, se contienen previsiones respecto de los tratamientos a los que no sea directamente aplicable el Reglamento (UE) 2016/679 que pueden afectar a actividades no comprendidas en el ámbito de aplicación del Derecho de la Unión Europea, y el tratamiento de datos llevado a cabo con ocasión de la tramitación por los órganos judiciales de los procesos de los que sean competente.<sup>27</sup>

#### *1.1.2.4 Agencia Española de Protección de datos y otras autoridades de control*

El RGPD establece que los Estados miembros han de disponer de una o más autoridades independientes de control de protección de datos, en España se crea desde el año 1994 y bajo amparo de la ya mencionada LOTARD la Agencia Española de Protección de Datos, con el objetivo de velar que se cumplieran y aplicaran las normas relativas a la protección de datos. La AEPD estuvo presente por tanto en el proceso evolutivo de las diferentes normas tanto a nivel europeo como las españolas, con el establecimiento del RGPD asume un rol más concienciador en cuanto a la relevancia e importancia del reglamento para la protección de datos, llegando a ser un ejemplo de transparencia y comunicación.<sup>28</sup>

---

<sup>26</sup> JEFATURA DEL ESTADO. (2018). Proyecto de Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales. *Boletín Oficial Del Estado*, 294(6 de Diciembre de 2018), 5–68.

<sup>27</sup> AA.VV. (2018). “ La ley orgánica de protección de datos personales y garantía de los derechos digitales: proceso de elaboración, estructura, objeto, ámbito de aplicación, y principios de la norma proceso de elaboración.”. *Revista Del Gabinete Jurídico De Castilla-La Mancha*, 16.

<sup>28</sup> RODERO, Á. B. (s. f.). *Agencia de Protección de Datos: la AEPD y la ley de protección de datos*. Recuperado 9 de junio de 2020, de <https://www.angelbenitorodero.es/proteccion-de-datos/agencia-de-proteccion-de-datos-la-aepd-y-la-ley-de-proteccion-de-datos/>



universidad  
de león



La LOPDGDD dedica el Título VII Capítulo 1 a la AEPD, aunque hace referencia a la misma a lo largo de diferentes artículos, en el referido título se le mantiene como autoridad independiente que se relaciona con el gobierno a través del Ministerio de Justicia. El régimen jurídico por el que se regula la Agencia se establece por lo dispuesto en el RGPD, en la LOPDGDD y en las disposiciones de desarrollo de dicha ley de protección de datos.

Entre las funciones que prevé la LOPDGDD para la AEPD están: emitir autorizaciones, la publicación de circulares y directrices, atender peticiones y reclamaciones formuladas por las personas afectadas, requerir a los responsables y los encargados de los tratamientos la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones del Reglamento (UE) 2016/679 y la LOPDGDD, y en su caso, ordenar la cesación de los tratamientos e incluso la suspensión de transferencias internacionales de datos.<sup>29</sup>

Además de la Agencia Española en la actualidad existen en España tres autoridades autonómicas de protección de datos. La Autoridad Catalana de Protección de Datos, ente de derecho público y un organismo oficial de la Generalidad de Cataluña que responde directamente ante el Parlamento de Cataluña. La Agencia Vasca de Protección de datos entidad del sector público, con personalidad jurídica propia y plena capacidad pública y privada, por lo que se refiere al tratamiento de los datos de carácter personal contenidos en ficheros de titularidad pública creados y mantenidos por los organismos autonómicos, forales y locales de la Comunidad Autónoma del País Vasco. El Consejo de Transparencia y Protección de Datos de Andalucía, creado por el artículo 43 de la Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía, es la autoridad

---

<sup>29</sup> KLUWER, W. G. J. (n.d.). *Agencia Española de Protección de Datos*. Retrieved June 9, 2020, from [https://guiasjuridicas.wolterskluwer.es/Content/Documento.aspx?params=H4sIAAAAAAAAAEAMtMSbF1jTAAAUNDU0NLtbLUouLM\\_DxbIwMDCwNzAwuQQGZapUt-ckhlQaptWmJOcSoArv0c4zUAAAA=WKE](https://guiasjuridicas.wolterskluwer.es/Content/Documento.aspx?params=H4sIAAAAAAAAAEAMtMSbF1jTAAAUNDU0NLtbLUouLM_DxbIwMDCwNzAwuQQGZapUt-ckhlQaptWmJOcSoArv0c4zUAAAA=WKE)



universidad  
de león



independiente de control en materia de transparencia y protección de datos en la Comunidad Autónoma de Andalucía.<sup>30</sup>

Respecto a las autoridades autonómicas el artículo 57 de la LOPDGDD establece que podrán ejercer las funciones establecidas en los artículos 57 y 58 del Reglamento 2016/679/UE, cuando se refieran a tratamientos de los que sean responsables las entidades integrantes del sector público de la correspondiente Comunidad Autónoma o quienes presten servicios a través de cualquier forma de gestión directa o indirecta. Así como los tratamientos llevados a cabo por personas físicas o jurídicas para el ejercicio de las funciones públicas correspondientes a la Administración Autónoma o Local y los que se encuentren expresamente previstos, en su caso, en los respectivos Estatutos de Autonomía.

Mientras que en general el artículo 56.2 de la LOPDGDD establece que la AEPD informará a las autoridades autonómicas de protección de datos acerca de las decisiones adoptadas en el Comité Europeo de Protección de Datos y recabará su parecer cuando se trate de materias de su competencia.<sup>31</sup>

## **I.2 Modelo cubano en desarrollo.**

### *1.2.1 El reconocimiento de la protección de datos personales en la Constitución Cubana como un derecho Fundamental.*

El modelo económico cubano ha establecido entre sus prioridades el desarrollo de las nuevas tecnologías y su alcance en todas las esferas de la sociedad, avance que se ha visto reflejado en su infraestructura de redes y en las medidas adoptadas para permitir que un espectro más amplio de la población tenga acceso a Internet, propiciando que cada vez más cubanos estén

---

<sup>30</sup> *Autoridades autonómicas en materia de protección de datos en la LOPDGDD y en el RGPD.* (n.d.). Iberley. El Valor de La Confianza. Retrieved June 9, 2020, from <https://www.iberley.es/temas/autoridades-autonomicas-materia-proteccion-datos-lopdgdd-rgpd-62848>

<sup>31</sup> PALOMAR, A., & FUERTES, J. (n.d.). *Autoridades autonómicas de Protección de Datos.* Retrieved June 9, 2020, from <https://practico-proteccion-datos-personales.es/vid/autoridades-autonomicas-proteccion-datos-716170265>



universidad  
de león



presentes en las nuevas plataformas digitales de carácter nacional e internacional, y como consecuencia que estén sujetos a las cláusulas y condiciones que se establecen para el tratamiento de los datos en ellas expuestos. Se han creado nuevos y modernos desafíos que requieren de un respaldo jurídico que permita proteger los derechos de las personas.<sup>32</sup>

La Constitución cubana puesta en vigor el 24 de febrero de 2019, refleja por primera vez en la ley fundamental del país un apartado que recoge de manera específica la protección de datos, atendiendo a la necesidad de darle reconocimiento como un derecho con rango constitucional.<sup>33</sup> Este documento comienza por reconocer en el Capítulo II relativo a los Derechos, en el Artículo 48, el derecho a la intimidad personal y familiar, a la propia imagen y voz, honor e identidad personal y en los artículos 49 y 50 los derechos referentes a la inviolabilidad del domicilio y la inviolabilidad de la correspondencia y demás formas de comunicación, respectivamente, salvo por orden expresa de la autoridad competente, con las formalidades legales y por motivo previamente definido en la ley.

El Capítulo VI de la Constitución sobre Garantía de los derechos es donde se recoge el derecho a la protección de datos, quedando plasmado en el Artículo 97 de la siguiente forma: “Se reconoce el derecho de toda persona de acceder a sus datos personales en registros, archivos u otras bases de datos e información de carácter público, así como a interesar su no divulgación y obtener su debida corrección, rectificación, modificación, actualización o cancelación. El uso y tratamiento de estos datos se realiza de conformidad con lo establecido en la ley. ”

---

<sup>32</sup> AMOROSO FERNÁNDEZ, Y., & VALENZUELA, L. (2019). “La nueva Constitución: punto de partida para regular la protección de datos en Cuba” – *Observatorio Iberoamericano de Protección de Datos*. <http://oiprodat.com/2019/09/25/la-nueva-constitucion-punto-de-partida-para-regular-la-proteccion-de-datos-en-cuba/>

<sup>33</sup> OJEDA BELLO, Z., & AMOROSO FERNÁNDEZ, Y. (2016). “La protección de los datos personales en Cuba desde la legislación vigente”. *Justicia Juris*, 12, 87-94.



universidad  
de león



Probablemente el mayor problema de este artículo sea que solo hace mención de los datos recogidos desde bases de información públicas, lo que no garantiza a nivel constitucional la protección de los datos recogidos en registros privados, que pueden usar esta información con varios fines, como los comerciales. Dejando esta especificación a que sea desarrollada en futuras normas.

Precisamente la incorporación de estos nuevos bienes jurídicos en la constitución abre las puertas a la creación de futuras leyes y procedimientos que sean garante de la tutela de los mismos. Normas que deben ir encaminadas tanto a definir un tratamiento legítimo de los datos, como a establecer un sistema específico para el control de los datos que permitan en un futuro cercano interponer el recurso de habeas data.

### *1.2.2 Primeros pasos en la implantación de un Reglamento de Protección de datos.*

La apertura y acceso a las tecnologías es una fuente de progresos para el país, pero viene aparejado con los riesgos inminentes del uso de las mismas, lo que comienza a llamar la atención de especialistas y expertos, haciendo énfasis en la protección de datos. Las primeras acciones en Cuba estuvieron más bien encaminadas a la protección de los datos almacenados en sistemas automatizados ante la ocurrencia de virus informáticos. Pero la atención frente a los virus de computadora no abarcaba todos los problemas de destrucción, manipulación, adulteración o divulgación no autorizada de datos, por lo que se crea un Grupo de Expertos de protección de datos para trabajar en la adecuación de un régimen legal de protección de los datos.<sup>34</sup>

Es con estos antecedentes que el 4 de marzo de 1992, el presidente del Instituto Nacional de Sistemas Automatizados y Técnicas de Computación (INSAC), aprobó el Reglamento para la

---

<sup>34</sup> AMOROSO FERNÁNDEZ, Y. (1994). "Breve exposición de la informática en Cuba: la protección y comercialización del software . El régimen de protección de los datos". *Revista General de Información y Documentación*, 4, 195-205.



universidad  
de león



Protección de Datos y Programas Informáticos. Este reglamento fue promulgado por el INSAC atendiendo a lo establecido en el artículo 86 del Decreto Ley N.º 67, de 19 de abril de 1983, de la Organización de la Administración Central del Estado, en el que se establecía que el “Instituto de Sistemas Automatizados y Técnicas de Computación es el encargado de dirigir, ejecutar y controlar la aplicación de la política del estado y el Gobierno en la actividad relativa a los sistemas automatizados de dirección y las técnicas de computación.”

El Reglamento constituyó una unificación de las disposiciones administrativas para regular la protección de los datos y programas de computación. Entre sus elementos más relevantes se encontraban las medidas obligatorias para las personas que intervinieran en el proceso de explotación de los medios de computación, para evitar la aparición de virus informáticos. El capítulo II hacía referencia a los responsables de Protección de Datos, definiendo sus funciones. Sin embargo, el alcance de este Reglamento no iba encaminado a proteger los datos personales, sino que más bien se refería de manera más amplia a los datos recogidos en unidades físicas que pudieran afectarse por virus tecnológicos, teniendo en cuenta que las inversiones que hacía el país en medios informáticos eran de carácter social.<sup>35</sup>

El Reglamento 3 de 1992 del INSAC quedó derogado por la Resolución 6 de 1996 del Ministerio del Interior (MININT), Reglamento sobre la Seguridad Informática, que fue evolucionando durante la década de los 90, con el trabajo de diferentes entidades por separado que buscaban unificar todas estas tareas y funciones. Hasta que se aprueba la Resolución 127 del 2007, aprobada por el Ministerio de las Comunicaciones (MINCOM), Reglamento de Seguridad para las Tecnologías de la Información. Los reglamentos promulgados desde 1992 hasta el aún vigente Reglamento de Seguridad, se basan fundamentalmente en la protección de los bienes informáticos, tanto de ataques físicos, como los producidos a través de la red.

---

<sup>35</sup> AMOROSO FERNÁNDEZ, Y. (1994). “Breve exposición de la informática en Cuba: la protección y comercialización del software . El régimen de protección de los datos”. *Revista General de Información y Documentación*, 4, 195-205



### *1.2.3 Regulaciones Administrativas que regulan de manera dispersa la protección de datos personales.*

Durante años la antigua Constitución de la República de Cuba de 24 de febrero de 1976, que fuera reformada en julio de 1992 y junio de 2002, no hacía mención a la protección de los datos personales, ni directamente reflejaba el derecho a la intimidad, sino que más bien quedaba asumido por lo preceptuado en artículo 9 a) que exponía: “El Estado garantiza la libertad y la dignidad plena del hombre, el disfrute de sus derechos, el ejercicio y cumplimiento de sus deberes y el desarrollo integral de su personalidad”, la protección frente al uso de la informática quedaba a una interpretación indeterminada, que vulneraba el uso indiscriminado de la información personal al no tener un respaldo legal que lo sustentara.<sup>36</sup>

A pesar de no existir ninguna ley que hiciera referencia o una mención directa a la protección de los datos personales como derecho autónomo, en la esfera administrativa, diferentes Ministerios a través de sus regulaciones hacían mención a esta protección, aunque no persiguieran como objetivo la protección de la información personal como un derecho. El propio MINCOM, en el ya mencionado Reglamento de Seguridad para las Tecnologías de la Información en el artículo 79 expresa la prohibición de difundir información que afecte al interés social, la moral, las buenas costumbres y la integridad de las personas, por cualquier persona natural o jurídica, medida que evita que se vulneren los derechos de los ciudadanos. Mientras que el artículo 84 impide el uso las redes públicas de transmisión de datos para explorar o monitorear información sobre los usuarios legales de las mismas.<sup>37</sup>

Al encontrarse los datos referentes a la salud entre los de máxima prioridad, cabe mencionar la Resolución Ministerial 1/2007, del Ministerio de Salud Pública, sobre el Reglamento General de Hospitales, con respecto al tratamiento de los datos obtenidos para la conformación del expediente médico, en el artículo 122 especifica el uso de los mismos solo

---

<sup>36</sup> SOARES CRUZ, A. P. (2013). “Algunas consideraciones sobre la protección de datos personales en la legislación cubana” 53(9), 1689-1699. <https://doi.org/10.1017/CBO9781107415324.004>

<sup>37</sup> Ídem



universidad  
de león



para fines médicos, científicos, docentes y legales. No se define un responsable del tratamiento, ya que expresa que todo el personal del hospital velará por la reserva del contenido y que será sancionable el incumplimiento o falta de discreción. Esta resolución no otorga a los pacientes ningún derecho sobre los datos recogidos en el expediente médico, ni le otorga garantías ante la posible mala utilización de sus datos.<sup>38</sup>

En sentido general existen un conjunto de normas que de forma dispersa protegen la información, sin hacer especial énfasis en que tipo de datos se está tutelando. Mediante estos reglamentos se definen las formas de actuar que preserven la confidencialidad y el acceso a la información general que se procesa en estos ministerios, por lo que el incumplimiento de las mismas queda sujeto a medidas administrativas o cautelares. Con la inclusión de la protección de datos como un derecho en la Constitución, queda establecido en el cronograma legislativo cubano, la propuesta de ley sobre Protección de Datos Personales, para febrero del año 2021, norma jurídica que tendrá como ponente al Ministerio de Justicia, para regular e integrar aspectos que permitan un tratamiento más integral en cuanto a la protección de datos personales.<sup>39</sup>

---

<sup>38</sup>OJEDA BELLO, Z., & AMOROSO FERNÁNDEZ, Y. (2016). "La protección de los datos personales en Cuba desde la legislación vigente". *Justicia Juris*, 12, 87-94.

<sup>39</sup> Ídem





## CAPÍTULO II: DERECHO ESPECIAL COMPARADO DE LA PROTECCIÓN DE DATOS EN LAS COMUNICACIONES ELECTRÓNICAS.

### II.1 Sistema Jurídico Europeo y español.

#### *II.1.1 Derecho especial de privacidad en las comunicaciones electrónicas: Directiva 2002/58/CE*

##### *II.1.1.1 Antecedentes*

El uso masivo de los ordenadores, aparejado a todos los avances tecnológicos que forman parte de la Revolución Informática ha representado un reto directo para la protección de los datos personales, haciendo necesario que surjan legislaciones que salvaguarden la información personal. Precisamente la unión de las tecnologías informáticas y las comunicaciones electrónicas fomentó que las empresas de telecomunicaciones hicieran uso de la digitalización, aumentando su potencial con evidentes ventajas para los usuarios y a su vez representando un riesgo para los derechos fundamentales de los mismos.<sup>40</sup>

Para lograr con éxito todos estos avances en Europa, resaltaba la necesidad de establecer un marco de regulación adecuado para el tratamiento de los datos personales y la protección de la intimidad dentro del sector de las telecomunicaciones. Es entonces cuando se publica la Directiva 97/66/CE del Parlamento y del Consejo de 15 de diciembre 1997, que en su artículo 1 establecía que las disposiciones de esta directiva especificaban y complementaban a la Directiva general de protección de datos 95/46/CE. Su ámbito de aplicación no se limitaba solo al derecho a la intimidad en el tratamiento de los datos, sino que además incluía la libre circulación de los mismos y de los servicios de telecomunicaciones.<sup>41</sup>

---

<sup>40</sup> BALLESTEROS MOFFA, L. Á. (2005). *La privacidad electrónica . Internet en el centro de protección.* Tirant lo Blanch, Valencia, 348 pags.

<sup>41</sup> MANTECA VALDELANDE, V. (2000). "La protección de datos personales en las telecomunicaciones : regulación comunitaria europea y española. ". 43-73. <https://doi.org/10.33426/rcg/2000/51/629>



universidad  
de león



La trasposición de la Directiva 97/66/CE al ordenamiento jurídico español se hace mediante antigua Ley 11/1998, de 24 de abril, General de Telecomunicaciones y Real Decreto 1736/1998, conocido como Reglamento del Servicio Universal, de 31 de julio por el que se aprobó el Reglamento de desarrollo del Título III de la Ley General de Telecomunicaciones, en lo relativo al servicio universal de telecomunicaciones. Sin embargo, mientras se determinaban estas normas jurídicas, la innovación tecnológica que representó el paso de lo analógico a lo digital evolucionó también las infraestructuras y redes de comunicación, sobre todo en el ámbito de Internet. Se comienzan a utilizar las tecnologías de sistemas de fibra óptica basadas en luz para transmitir información, ya que proveía ventajas como incluir mayor seguridad en la transmisión de la señal y disponibilidad de un gran ancho de banda, permitiendo grandes velocidades de transmisión de la información.<sup>42</sup>

El profundo cambio que comenzó a evidenciarse en el mercado y en los servicios ofertados a través de Internet, ponía en evidencia la necesidad de una nueva norma que se adaptase a las nuevas posibilidades que se habrían a los usuarios por el uso de la red, que además incluía nuevos riesgos para los datos personales. Por lo que el 31 de julio de 2002 se publicó en el Diario Oficial de las Comunidades Europeas, la Directiva 2002/58/CE, del Parlamento y del Consejo, de 12 Julio, sobre la privacidad y las comunicaciones electrónicas. Como su propio texto lo expresa, llega para sustituir a la Directiva 97/66/CE que tuvo un corto período de vigencia, al igual que el Real Decreto 1736/1998, que pasa a ser modificado.<sup>43</sup>

### II.1.1.2 Novedades

La Directiva 2002/58/CE se publica por la necesidad de adaptar las normas a los avances que ya se evidenciaban y los que se preveían en los servicios y las tecnologías de las empresas de telecomunicaciones. La primera novedad de esta norma radica precisamente en establecer una

---

<sup>42</sup> ORTIZ LIMA, C. M. (2010). *Transmisión vía fibra óptica de señales analógicas utilizando subportadora modulada en frecuencia de pulsos : aplicación potencial en instrumentación y control*. Instituto Nacional de Astrofísica, Óptica y Electrónica.

<sup>43</sup> DAVARA RODRIGUEZ, MIGUEL ANGEL. 2003. "La Protección de Datos Personales En El Sector de Las Comunicaciones Electrónicas." *Universidad Pontificia Comillas* 1ra: 183.



universidad  
de león



neutralidad tecnológica con respecto a la regulación de diferentes servicios, por lo que sustituyó el término telecomunicaciones por el de Comunicaciones Electrónicas. De esta manera se incluyen todos los diferentes tipos de servicios de transmisión de comunicaciones electrónicas, con independencia y sin discriminación de la tecnología que se utilice. Factor que permite se proteja por igual a usuarios y consumidores sin que afecte la tecnología por la que acceden al servicio.<sup>44</sup>

Con la Directiva 2002/58/CE se intenta impulsar el desarrollo transfronterizo de los nuevos servicios de comunicaciones electrónicas, así como establecer una norma que proteja los derechos y libertades fundamentales de las personas físicas y los intereses de las personas jurídicas ante la inminente capacidad de almacenar y tratar automáticamente los datos de abonados y usuarios. Por este motivo es considerada una Directiva sectorial, que abarca los datos gestionados tradicionalmente en las telecomunicaciones como datos de tráfico y guías y los que se generan con las nuevas formas de tratamiento como la identificación de las líneas de llamadas, desvíos de llamadas, etc. Además, se regulan las nuevas categorías de datos, asociadas a las conexiones de red que producen otras formas de anotaciones como las cookies o archivos de incidencias como los logs.<sup>45</sup>

Al ser una directiva sectorial se completa y especifica con lo establecido en la Directiva general de protección de datos 95/46/CE, regulando riesgos propios que no fueron contemplados en su predecesora la Directiva 97/66/CE. Amplía su ámbito de aplicación desde la tradicional telefonía hasta la transmisión de datos por Internet, contemplando de modo específico los servicios de contenido en línea y los relativos a la sociedad de la información. La norma no se condiciona ante los requisitos conceptuales de estas categorías y se muestra abierta para la regulación desde una perspectiva integral. Ejemplo de ello son las

---

<sup>44</sup> CORRIPIO GIL-DELGADO, MARÍA DE LOS REYES, and Lorenzo MARROIG POL. 2002. "El Ordenamiento Español y La Protección de Datos Personales En El Sector de Las Telecomunicaciones - Dialnet." *Boletín del Ministerio de Justicia* No 1930: págs. 3565-3583.  
<https://dialnet.unirioja.es/servlet/articulo?codigo=286299> (March 9, 2020).

<sup>45</sup> CORRIPIO, M. R. (2002). "Novedades Legislativas sobre protección de datos. La Directiva 2002/58/CE" *Revista de Contratación Electrónica*. Número. 32. Noviembre de 2002



universidad  
de león



comunicaciones no solicitadas con fines de venta directa, sin que necesariamente el spam recibido en el correo electrónico se encuentre amparado por una actividad económica, por lo que este problema no tiene que ceñirse estrictamente al ámbito de los servicios de la sociedad de la información.<sup>46</sup>

### *II.1.1.3 Adaptación al ordenamiento español*

Para trasponer la Directiva 2002/58/CE en España se estableció la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, que fue derogada por la LGT. Además se traspuso a través de la LSSI (modificada por la Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información) y el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, aprobado por Real Decreto 424/2005, de 15 de abril, al cual se remite el art. 31 del Real Decreto 899/2009, de 22 de mayo, por el que se aprueba la carta de derechos del usuario de los servicios de comunicaciones electrónicas.<sup>47</sup>

### *II.1.1.4 Modificaciones a la Directiva 2002/58/CE*

La Directiva 2002/58/CE ha sido modificada en dos ocasiones, la primera por la promulgación por parte de la Unión Europea de la Directiva 2006/24/CE sobre la conservación de datos de tráfico de las comunicaciones electrónicas. Esta directiva es creada para otorgarle poderes a los Estados en la lucha contra el terrorismo. Sin embargo, desde su publicación tuvo muchos detractores, pues representaba una vulneración de derechos fundamentales y en especial el derecho a la intimidad y secreto de las comunicaciones como se refleja en el artículo 12 de la Declaración Universal de Derechos Humanos y el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea.<sup>48</sup>

---

<sup>46</sup>BALLESTEROS MOFFA, L. Á. (2005). *La privacidad electrónica . Internet en el centro de protección*. Tirant lo Blanch, Valencia, 348 pags..

<sup>47</sup> BALLESTEROS MOFFA, L. Á. (2018). “La revisión del régimen jurídico de la privacidad en la Unión Europea”. *Revista del posgrado en derecho de la UNAM*, Num 8(April 2016), 38-64.

<sup>48</sup> RODRIGUEZ DELGADO, J. P. (2008). «La Ley 25/2007 sobre conservación de comunicaciones electrónicas a la luz de la Directiva europea 2006/24/CE». *RCE*, 92, 3-45.



universidad  
de león



Mientras que los operadores de telecomunicaciones mostraban su apoyo ante las nuevas obligaciones que se les exigían, las autoridades de protección de datos expresaban que la conservación de los datos debía ser por períodos lo más breves posibles al ser una intervención en la vida de los ciudadanos. La Directiva tenía una tendencia totalitaria en cuanto a la conservación de todos los datos relativos a las comunicaciones electrónicas. Además, estableció una permanencia de los datos de 6 meses a dos años, pudiendo los Estados miembros superar estos plazos, mientras que admitía la disponibilidad total ante delitos graves, faltando especificaciones en cada caso.<sup>49</sup> La Directiva 2006/24/CE fue anulada por incumplir el principio de proporcionalidad por la STJUE de 8 de abril de 2014.

España transpuso esta Directiva mediante la Ley 25/2007 de conservación de datos relativos a las comunicaciones electrónicas, en la misma se respeta la doctrina emitida por el Tribunal Constitucional sobre la necesidad de una doble garantía, por un parte, que los datos conservados sean datos de tráfico, no contenido de las comunicaciones, y por otro lado, que los datos de dicha comunicación solo puedan ser exigidos por vía judicial. Como bien establece el Artículo 1 sobre el objetivo de la LCD, los operadores de telecomunicaciones están obligados a conservar los datos, pero el fin de los mismo sería la detección, investigación y enjuiciamiento de delitos graves contemplados en las leyes penales. Sin embargo, debe analizarse si la Ley al incluir todos los delitos graves del CP no excede en cierta medida aquellos para los que se pensó la directiva, en especial delitos de terrorismo, tráfico de armas y explosivos, y posiblemente, delitos informáticos., teniendo en cuenta que los futuros autores verán violados su derecho al secreto de las comunicaciones y el de intimidad<sup>52</sup>

---

<sup>49</sup> RODOTÀ, S. (2006). “La conservación de los datos de tráfico en las comunicaciones electrónicas.” *IDP: Revista de Internet, Derecho y Política*. Num 3, 53-60.

<sup>52</sup> RODRIGUEZ DELGADO, J. P. (2008). «La Ley 25/2007 sobre conservación de comunicaciones electrónicas a la luz de la Directiva europea 2006/24/CE». *RCE*, 92, 3-45.



La anulación de la Directiva 2006/24/CE no implicó la derogación de la LCD que según el Informe de la AEPD 0343/2013, se mantiene apoyada en la previsión genérica de conservación de datos de la Directiva 2002/58/CE. Por lo que mantiene su vigencia, y en consecuencia sigue siendo aplicable para todas aquellas empresas y entidades que entren dentro de su ámbito de aplicación en tanto no sea modificada por parte del legislador comunitario. Sin embargo, será posible la interposición de un incidente procesal de nulidad, solicitando su inaplicación por el principio de primacía del Derecho Europeo. Abriendo el abanico de situaciones que deben ser consideradas por parte de los prestadores de servicios de comunicaciones electrónicas incluidos en el ámbito de aplicación de la LCD.

La Directiva 2002/58/CE fue modificada por segunda vez por la Directiva 2009/136/CE<sup>53</sup> que resaltó por una regulación más explícita del uso de las cookies. Mientras que la Directiva 2002/58/CE se limitaba a exigir que se le otorgara al usuario información suficiente con respecto al uso de las cookies por el servidor, la nueva Directiva en el artículo 5.3 modificado hace alusión al consentimiento explícito cuando requiere que el interesado “haya dado” su consentimiento y, además, establece como única excepción a esta regla la configuración del navegador para aceptar las cookies.<sup>54</sup>

La aplicación de esta Directiva creó debates entre los comerciantes europeos que operan en Internet pues consideraban que los ponía en desventaja con respecto a los comerciantes extracomunitarios. Sin embargo, en la práctica la Directiva 2009/136/CE busca regular diferentes intereses, por un lado, el derecho a la protección de la intimidad de los usuarios y,

---

<sup>53</sup> Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009 por la que se modifican la Directiva 2002/22/CE Relativa al Servicio Universal y los Derechos de los Usuarios en Relación con las Redes y los Servicios de Comunicaciones Electrónicas, la Directiva 2002/58/CE Relativa al Tratamiento de los Datos Personales y a la Protección de la Intimidad en el Sector de las Comunicaciones Electrónicas y el Reglamento (CE) no 2006/2004 Sobre la Cooperación en Materia de Protección de los Consumidores. Diario Oficial n° L 337, de 18 de diciembre de 2009, páginas 11 a 36.

<sup>54</sup> APRICIO SALOM, J., & SANFULGENCIO TOMÉ, S. S. (2014). “El régimen jurídico de las cookies y su aplicación por la Agencia Española de Protección de Datos.” *Revista Aranzadi Doctrinal*, 11, 1–21.



universidad  
de león



por otro, la libertad en los negocios, pues si no se establecen límites a esta última puede vulnerar muchos de los principios básicos de la protección de datos.<sup>55</sup>

En España, el Real Decreto-ley 13/2012 implementó en el artículo 22.2 de la Ley de Servicios de la Sociedad de la Información<sup>56</sup> los cambios establecidos en la Directiva 2009/136/CE, mediante la transcripción casi literal del texto establecido en esa Directiva. Esta modificación entró en vigor el 1 de abril de 2012. En apartados posteriores de este capítulo se aborda con más profundidad la regulación de las cookies en el régimen jurídico español.

### *II.1.2 Propuesta de Reglamento ePrivacy de 2017*

La propuesta de aplicación del RGPD vaticinaba un cambio en toda regulación existente en materia de protección de datos, incluyendo el sector de las comunicaciones electrónicas. En este sentido en junio del 2015 la Comisión Europea presenta un estudio sobre la efectividad de la Directiva 2002/58/CE y su incompatibilidad con el RGPD, en el que se indicaban los principales fallos para su transposición dentro de la ley nacional de los Estados Miembros.<sup>58</sup> El estudio impulsó a una consulta pública y revisión de la Directiva 2002/58/CE en 2016,<sup>59</sup> que resultó en la propuesta del Reglamento sobre el respeto a la vida privada y a la protección de los datos personales en el ámbito de las comunicaciones electrónicas (en lo adelante ePrivacy), que forma parte de la estrategia de Mercado Único Digital de la Comisión Europea.

---

<sup>55</sup> ZAMORA, P. L. (2012). “La incorporación de la Directiva 2009/136/CE del Parlamento Europeo y del Consejo de 25 de noviembre de 2009 al ordenamiento jurídico español.” *Nueva Época num 14*, 225–228. <https://doi.org/10.5209/FORO.39002>

<sup>56</sup> Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. Boletín Oficial del Estado nº 166, de 12 de julio de 2002, páginas 25.388 a 25.403.

15

<sup>58</sup> ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation, Jan. 31, 2015, <https://ec.europa.eu/digital-single-market/en/news/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data>.

<sup>59</sup> European Commission, Public Consultation on the Evaluation and Review of the ePrivacy Directive, Apr. 11, 2016, <https://ec.europa.eu/digital-single-market/en/news/public-consultation-evaluation-and-review-eprivacy-directive>.



universidad  
de león



Esta figura normativa es obligatoria en todos sus elementos y directamente aplicable en cada Estado miembro, logrando así una regulación homogénea de esta materia. Sin embargo, la entrada en vigor del ePrivacy que se esperaba en 2018, coincidiendo con la aplicación del RGPD, no se ha podido lograr al no llegar hasta la fecha a un acuerdo. Teniendo en cuenta que el ePrivacy es considerado *lex specialis* con respecto al RGPD, su no aprobación y la falta de actualización de la Directiva vigente con respecto a los avances actuales hace que surjan ciertos conflictos que la Comisión Europea ha tratado de mitigar.<sup>60</sup> Tanto las autoridades de protección de datos nacionales como el TJUE han intentado dar una respuesta a la actual inseguridad jurídica.<sup>61</sup> Este último en su sentencia de 1 de octubre de 2019, *Bundesverband der Verbraucherzentralen und Verbraucherverbände*<sup>62</sup> interpreta la Directiva 2002/58/CE y simultáneamente el RGPD para llegar a una conclusión sobre el consentimiento.<sup>63</sup>

### *II.1.2.1 Aspectos Generales del Reglamento ePrivacy*

Los principales puntos sobre los que gira el debate de la propuesta de reglamento e Privacy, son precisamente aquellos que afectan los intereses de otros actores que van más allá de las tradicionales compañías de telecomunicaciones. Los aspectos más importantes son el ámbito

---

<sup>60</sup> El Comité Europeo de Protección de Datos ha intentado dar respuesta a ciertas cuestiones con la publicación de su Opinión 5/2019 “on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities.”

<sup>61</sup> Sentencia de 29 de julio de 2019, Fashion ID GmbH & Co.KG c. Verbraucherzentrale NRW eV, Asunto C-40/17, ECLI:EU:C:2019:629 sobre el uso de las cookies. Sentencia del TJUE de 13 de junio de 2019, Google LLC y Bundesrepublik Deutschland, Asunto C-193/18, ECLI:EU:C:2019:498 sobre el servicio de correo electrónico en Internet. Sentencia de 5 de junio de 2019 Skype Communications Sàrl e Institut belge des services postaux et des télécommunications (IBPT), Asunto C-142/18, ECLI:EU:C:2019:460 sobre el protocolo de voz por Internet (VoIP).

<sup>62</sup> 1 de octubre de 2019, Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V. c. Planet49 GmbH, Asunto C-673/17, ECLI:EU:C:2019:801. el TJUE interpreta la Directiva 2002/58/CE conjuntamente con el RGPD y llega a la conclusión de que el consentimiento al que se hace referencia en estas disposiciones no se presta de manera válida cuando el almacenamiento de información o el acceso a la información ya almacenada en el equipo terminal del usuario de un sitio de Internet a través de cookies se autoriza mediante una casilla marcada por defecto de la que el usuario debe retirar la marca en caso de que no desee prestar su consentimiento.

<sup>63</sup> GASCÓN MARCÉN, A. (2020). “El Reglamento sobre la privacidad y las comunicaciones electrónicas , la asignatura pendiente del Mercado Único Digital”, 93/2020; CEU Ediciones, *Serie Unión Europea y Relaciones Internacionales*.





universidad  
de león



territorial y material, la interrelación entre la propuesta de ePrivacy con el RGPD, las medidas de aplicación y los riesgos más específicos a ser regulados por las empresas de comunicaciones electrónicas que se abordan en posteriores apartados como son las disposiciones sobre las cookies, la aplicación de consentimiento y la confidencialidad de las comunicaciones.

El ámbito territorial del ePrivacy establece que será aplicado a los servicios de comunicación electrónica que son proporcionados a usuarios finales en la UE, así como la protección de la información relativa a los equipos terminales de los usuarios finales situados en la Unión, aunque el proveedor del servicio no esté establecido en la UE. Por lo que al igual que el RGPD el ámbito territorial es aplicable a nivel mundial, con lo que se pretende solventar la falta de protección del consumidor frente a las empresas ubicadas fuera de la UE, hasta el momento no sujetas a su normativa de aplicación. Esto supondrá que servicios no pensados para ser utilizados en Europa, deberán en principio cumplir con el Reglamento si son utilizados por usuarios europeos, estando obligados a nombrar un representante en un Estado miembro.<sup>64</sup>

Mientras que el ámbito de aplicación amplía su alcance, abriendo el abanico de opciones que se incluyen en el concepto de comunicaciones electrónicas. Con esta definición se pretende incluir dentro del alcance del reglamento y sus requisitos con respecto a la confidencialidad servicios de voz sobre IP como Skype, servicios de mensajería instantánea y de correos electrónicos basados en la web como WhatsApp y Gmail respectivamente, comúnmente referidos como servicios de transmisión libre, del término en inglés *over the top* (OTT) e incluye además las comunicaciones de máquina a máquina en Internet de las cosas (IoT) tendencia que se verá incrementada con la implantación del 5G . La extensión de la aplicación del reglamento a nuevos sectores como OTT, posibilita que los proveedores de estos servicios que compiten con los tradicionales de telecomunicaciones se rijan por la misma ley o similar,

---

<sup>64</sup> Principales novedades de la Propuesta de Reglamento Europeo e-Privacy. (2017). <https://periscopiofiscalylegal.pwc.es/propuesta-de-reglamento-europeo-e-privacy-principales-novedades/>



universidad  
de león



lo cual forma parte de las políticas de estrategia del Mercado Único Digital, ya que hasta el momento actúan sin tener que respetar las mismas reglas.<sup>65</sup>(Traducción propia)

Un aspecto importante del reglamento es cómo regula la privacidad teniendo en cuenta su vínculo directo con la protección de datos; muchos esperaban que se integrara la privacidad como un principio desde el diseño y por defecto, pero no fue así. El artículo 10 establece que los programas informáticos comercializados que posibilitan las comunicaciones electrónicas, como los navegadores web, al iniciarse su instalación deben informar a los usuarios acerca de las opciones de configuración de confidencialidad antes de proceder a completar la instalación, solicitando el consentimiento del usuario final para una configuración determinada. Estableciendo por tanto una privacidad por opción y no por defecto, alejándose de los criterios del RGPD. Probablemente se regule de esta forma por lo negativo que resultaría para determinados modelos de negocios que operan desde Internet, pero permitiría propiciar desde la UE modelos de negocios más respetuosos con los usuarios.<sup>66</sup>

El reglamento ePrivacy atribuye las funciones de control a las autoridades responsables de la aplicación del RGPD, para lo que será necesario dotar a las autoridades de protección de datos de los recursos suficientes. Otro punto en el que la propuesta se alinea con el RGPD es el de las sanciones con multas administrativas, que pueden ser de hasta un 4% del volumen de negocios anual a nivel mundial o hasta un máximo de 20 millones de euros, pudiendo imponerse por incumplimiento de obligaciones o por incumplimiento del principio de

---

<sup>65</sup> GREGORY VOSS, W. (2017). «First the GDPR, Now the Proposed ePrivacy Regulation». *Journal of Internet Law*, 21(1), 3-11. <https://search-proquest-com.ezproxy.is.ed.ac.uk/docview/1918794232/fulltextPDF/39570841F54048ADPQ/1?accountid=10673%0Ahttps://ssrn.com/abstract=3008765>

<sup>66</sup> GASCÓN MARCÉN, A. (2020). «El Reglamento sobre la privacidad y las comunicaciones electrónicas, la asignatura pendiente del Mercado Único Digital» (93/2020; CEU Edición, Serie Unión Europea y Relaciones Internacionales).



universidad  
de león



confidencialidad. Al igual que el RGPD, el principio de confidencialidad cobra especial protagonismo, en este caso en la transmisión de las comunicaciones electrónicas.<sup>67</sup>

### *II.1.2.2 Reacciones a lo establecido en el Reglamento ePrivacy.*

La propuesta de reglamento debe adoptarse por procedimiento legislativo ordinario, lo que requiere que el Parlamento Europeo y el Consejo de la UE lleguen a un acuerdo para su aprobación. El pasado 22 de noviembre de 2019, el Comité de Representantes Permanentes de los Gobiernos de los Estados miembros en el Consejo de la Unión Europea, rechazó el último borrador del Reglamento ePrivacy. Desde que se elaborara el primer borrador de la Comisión hecho público en enero de 2017 y hasta la fecha, se han elaborado fatigosamente borradores tanto del parlamento como del consejo, sin que se concreten acuerdos en las negociaciones.<sup>68</sup>

La posición asumida por España ha sido de apoyo a la Comisión Europea para la revisión de la Directiva 2002/58/CE para generar la confianza y seguridad que necesita el nuevo escenario digital. Pero considera que con la aprobación del RGPD, es innecesario regular tan detalladamente el procesado de la información sobre todo de los metadatos. Además, plantea que se podría aceptar el tratamiento de procesamiento posterior compatible existente en el RGPD. Con respecto a las “cookies” considera que debería ser más flexible el régimen, al menos en lo referente a la petición de consentimiento por las webs.<sup>69</sup>

Se ha expuesto que varios Estados han intentado retrasar de manera consiente la aplicación del ePrivacy para mantener en el poder a las empresas que monetizan con los datos en línea de los usuarios, los medios de comunicación digital, redes sociales y las empresas de telecomunicaciones. En este sentido la Asociación Europea de Operadores de Redes de Telecomunicaciones que representa a empresas como Telefónica en España y Orange en Francia,

---

<sup>67</sup> MORALES, A. (2018). *Análisis de la propuesta de Reglamento E-Privacy*. <https://www.cysae.com/analisis-de-la-propuesta-de-reglamento-e-privacy/>

<sup>68</sup> BENALAL QUINTANA, A. (2019). “Ser o no ser en la era digital: el futuro reglamento de ePrivacy.” *Prisacom*, 1–3.

<sup>69</sup> REPRESENTACIÓN PERMANENTE DE ESPAÑA ANTE LA UNIÓN EUROPEA (2019). *Propuesta de Reglamento sobre e-privacidad en las comunicaciones electrónicas*. <https://es-ue.org/documentation/transportes-telecomunicaciones-y-energia/>



universidad  
de león



declaró que "Las medidas excesivamente restrictivas sobre la privacidad electrónica no agregarían una protección significativa a las personas, pero obstaculizarían la capacidad de las empresas de telecomunicaciones para ofrecer una mayor elección al consumidor, al ingresar al espacio de servicio digital con nuevas ofertas ".<sup>70</sup>

### *II.1.3 Riesgos específicos regulados a tener en cuenta por las empresas de Comunicaciones electrónicas.*

#### *II.1.3.1 Secreto o confidencialidad de las comunicaciones electrónicas.*

El artículo 39 de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones establece que los operadores que presten servicio o exploten redes públicas de comunicaciones electrónicas deberán garantizar el secreto de las comunicaciones acorde a lo establecido en los artículos 18.3 y 55.2 de la Constitución Española. En concordancia con el artículo 5.1 de la Directiva 2002/58/CE que establece que los Estados miembro mediante legislación nacional asegurarán la confidencialidad de las comunicaciones y los datos de tráfico asociados a ellas. Mientras que el Reglamento UE 611/2013, de 23 de junio de 2013 relativo a las medidas aplicables a la notificación de casos de violación de datos personales en el marco de la Directiva 2002/58/CE, especifica la obligación de notificar a las autoridades nacionales competentes y a los usuarios afectados de las violaciones ocurridas.<sup>71</sup>

Existen limitaciones para la transmisión y la obligación de notificar a afectados de brechas de seguridad. El propio régimen constitucional del secreto de las comunicaciones prevé la posibilidad de interceptación e intervención de las comunicaciones, por las denominadas interceptaciones legales. Entre ellas se encuentran en sus distintas modalidades, por medidas

---

<sup>70</sup> OBSERVATORY, C. E. (2018). "Shutting down ePrivacy: lobby bandwagon targets Council Retrieved ". <https://corporateeurope.org/en/power-lobbies/2018/06/shutting-down-eprivacy-lobby-bandwagon-targets-council?hash=keZ3nidpfZbeVQAaYUYoSTDAvjXndSjmZurmIQLAQeY>

<sup>71</sup> RIVERO SÁNCHEZ-COVISA, F. J. (2017). "Revisión del concepto constitucional del secreto de las comunicaciones" Dykinson.



de investigación tecnológica de la LECrim. y la Ley Orgánica 2/2002, de 6 de mayo, reguladora del Control Judicial Previo del Centro Nacional de Inteligencia. Unido a estas, la LGT regula en su artículo 40 las interceptaciones realizadas por los servicios técnicos. Al no tener el rango, ni la función para formular límites al derecho fundamental del secreto de las comunicaciones siempre que la intervención pueda afectar al ámbito constitucionalmente deberá contarse con autorización judicial que legalice la intervención.<sup>72</sup>

### *II.1.3.2 Datos de tráfico (metadatos) y localización de las comunicaciones electrónicas*

Los metadatos son un tipo de información que a nivel técnico sirven para organizar, clasificar y estructurar un conjunto de datos más numerosos y complejos. En el acceso a Internet serán metadatos, tanto para el origen como para el destino de la comunicación, la identificación de usuario asignada, el nombre y la dirección del abonado o usuario al que se le ha atribuido una dirección de protocolo internet (IP); la fecha y hora de conexión y desconexión del servicio de acceso a internet; el servicio de internet utilizado; o la línea digital de abonado (DSL). Además, se incluyen los datos de localización en los datos de tráfico, ya que forman parte del tratamiento en la conducción de una comunicación.<sup>73</sup>

Sin este tipo de datos sería técnicamente imposible la transmisión de la información, es posible diferenciar tres categorías principales de datos vinculados a las comunicaciones electrónicas. Primeramente, los datos de tráfico cuya definición en el marco comunitario vigente se establece en el artículo 2 b) de la Directiva 2002/58/CE como, “cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efecto de facturación de las mismas”. Los datos de localización<sup>74</sup> que según considerando 17 del Reglamento ePrivacy los datos de localización que se generen en un contexto distinto al de la prestación de servicios de comunicaciones

---

<sup>72</sup> DE ASÍS ROIG, A. (2017). “Secreto, protección de datos y seguridad e integridad en las telecomunicaciones.” In *Los retos del Estado y la Administración en el siglo XXI* (pp. 2129–2154). Tirant lo Blanch.

<sup>73</sup> PÉREZ RIVAS, D. A. (2017). *Metadatos vs privacidad: la insoportable levedad de la red.* (pp. 233-250).

<sup>74</sup> Definidos en el art. 2 c) de la Directiva 2002/58/CE como cualquier dato tratado en una red de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible al público.



electrónicas no han de considerarse metadatos. Finalmente, los datos de suscripción o datos de abonado, que constituyen la información personal recabada del abonado a la hora de suscribir el contrato de prestación de servicios de comunicación. Puesto que tales datos son previos a la comunicación y se hallan desligados no forman parte de este régimen.<sup>75</sup>

El tratamiento de los datos de tráficos está limitado a efectos de facturación o pago y solo dentro del tiempo preciso. Acorde con el artículo 6 de la Directiva 2002/58/CE una vez no sean necesarios para la transmisión de la comunicación es obligatorio eliminarlos o volverlos anónimos. Las empresas de telecomunicaciones tienen permitido el tratamiento de estos datos con un límite del tiempo necesario para hacer promoción del servicio, previa información y consentimiento del usuario. Mientras que los datos de localización podrán tratarse si se hacen anónimos o con consentimiento previo del usuario. El proveedor debe informar al interesado el tipo de dato, finalidad, plazo, etc., y concederle el derecho a revocar el consentimiento otorgado.<sup>76</sup>

### *II.1.3.3 Cookies*

Las cookies son una especie de dispositivo que se descarga en el equipo de un usuario con la finalidad de almacenar datos, que irán siendo actualizados cuando se acceda a diferentes sitios webs y finalmente podrán ser recuperados por la entidad responsable. Los prestadores de servicios web alegan que su uso tiene como fin principal mejorar la experiencia del usuario. Por lo general conservan datos de la navegación que pueden mantenerse incluso una vez apagado el navegador. Están reguladas en la LSSI, el artículo 22 de esta ley permite a los prestadores de servicios el uso de cookies siempre que se haya obtenido el consentimiento de los usuarios de forma clara y completa.<sup>77</sup>

---

<sup>75</sup> GONZÁLEZ LÓPEZ, J. J. (2017). "La retención de datos de tráfico de las comunicaciones en la Unión Europea : una aproximación crítica". *Diario La Ley*, No 6456, 1-19.

<sup>76</sup> CAMACHO CLAVIJO, S. (2005). *Parte intervinientes, formación y prueba del contrato electrónico*. Editorial Reus, S. A.

<sup>77</sup>. GARCÍA TERCERO, D. Á. (2016). "Los datos personales en las comunicaciones electrónicas". Universitat Rovira I Virgili.



El Comité Europeo de Protección de Datos, hace referencia diversos grupos de cookies en su mayoría en función de su uso como cookies de entrada, de autenticación, de seguridad, de sesión de reproductor multimedia, de complemento para intercambiar contenidos sociales, etc. En correspondencia con el tipo y uso de la cookie, la Directiva 2002/58/CE en su artículo 5.3 establece excepciones a la obligación de obtener el consentimiento, con una redacción un tanto difusa que no especifica la obligación de informar en los casos que se regulan. Por lo que el GT29 precisa en su Dictamen 4/2012 que, una cookie es necesaria siempre que la transmisión de la comunicación electrónica no sea posible sin el uso de la misma. En resumen, de ser posible la transmisión sin instalar una cookie, la excepción no operaría y sería necesario obtener el consentimiento para su instalación.<sup>78</sup>

El legislador comunitario reconoció que la aplicación de la Directiva 2002/58/CE no ha resultado eficaz para la protección efectiva de la privacidad de los equipos terminales de los usuarios. En este sentido la Propuesta de Reglamento ePrivacy regula el uso de las cookies en sus artículos 8, 10 y 11. El artículo 8 amplía el número de excepciones a la necesaria obtención de consentimiento, añadiendo la instalación cuando sea necesario para medir la audiencia de un sitio web en cuestión. La principal novedad que presenta esta Propuesta en materia de consentimiento del interesado es que establece que, “cuando sea técnicamente posible y factible”, podrá obtenerse por medio de “la configuración técnica adecuada de una aplicación informática que permita acceder a internet”. Incorpora, en su artículo 10, las condiciones en las que debe desarrollarse esta manifestación del consentimiento.<sup>79</sup>

---

<sup>78</sup> SALOM, J. A., & TOMÉ, S. S. (2014). “El régimen jurídico de las cookies y su aplicación por la Agencia Española de Protección de Datos”. *Revista Aranzadi Doctrinal*, 11, 1–21.

<sup>79</sup> FLAQUER RIUTORT, J. (2018). “Nuevas tendencias y propuestas en el tratamiento legal del uso de cookies : especial referencia a la propuesta de reglamento comunitario sobre la privacidad y las comunicaciones electrónicas (ePrivacy).”. *Revista Aranzadi de Derecho y Nuevas Tecnologías*, num 47.



universidad  
de león



El artículo 10 impondría la obligación a los fabricantes de programas informáticos, como los navegadores, de ofrecer a sus usuarios la posibilidad de impedir a terceros el almacenamiento de información sobre sus equipos terminales. Tendrían que informar al usuario, en el momento de la instalación, las distintas opciones de configuración de confidencialidad, sin que pueda proseguirse y completarse el proceso, sin haberse solicitado el consentimiento respecto de una configuración determinada. Esta propuesta de la Comisión Europea evita la práctica actual de avisos constantes y repetidos. Siendo necesario tomar las medidas técnicas necesarias que ofrezcan “opciones mucho más sencillas y garantistas de la privacidad del usuario, perfectamente desarrollables a partir de la configuración del navegador, en el que se puede elegir el grado de rastreo que se está dispuesto a tolerar y sin verse expuesto, de manera continua, a los avisos sobre este particular.”

## II.2 La prestación de servicios públicos de Telecomunicaciones en Cuba.

### *II.2.1 La protección de datos personales en las nuevas normas jurídicas del proceso de informatización de la sociedad*

Acercar a los ciudadanos a las tecnologías de la información y las comunicaciones constituye uno de los sectores estratégicos del país, acorde con lo establecido en la Conceptualización del Modelo Económico y Social Cubano y en las Bases del Plan Nacional de Desarrollo Económico y Social hasta 2030. El principal objetivo es fomentar y desarrollar la informatización de la sociedad, para lo que se aprueba en el año 2015 la instrumentalización de la “Política Integral para el Perfeccionamiento de la Informatización de la Sociedad”. Se realiza bajo la premisa de avanzar en la Informatización en la misma medida que se avance en la Ciberseguridad del país, para evolucionar en la seguridad del desarrollo y uso de las tecnologías.<sup>80</sup>

---

<sup>80</sup> PUIG MENESES. Y. *Informatización de la sociedad en Cuba | Presidencia de la República de Cuba*. (2019). <https://www.presidencia.gob.cu/es/gobierno/programas-priorizados/informatizacion-de-la-sociedad-en-cuba/>





universidad  
de león



Para el cumplimiento de estos objetivos se realiza el Resumen de las Prioridades de la Informatización de la Sociedad Cubana, fechado igualmente en 2015, en el que no se contempla expresamente la protección de datos de los usuarios, sin embargo, existen ciertos acápites que ya comenzaban arribar en esa dirección. Se puede apreciar en los Ejes Estratégicos como el referido al Gobierno y comercio electrónico que establece se deben fomentar los servicios en línea y crear las bases legales, técnicas y organizativas que garanticen condiciones de seguridad. Mientras que el eje referido al Marco Legal insta a actualizar la legislación vigente; conformar el marco regulatorio que garantice impulsar, promover y desarrollar el uso de las TIC.<sup>81</sup>

Sin embargo, no es hasta el año 2019 donde por primera vez se emitieron normas jurídicas de rango superior que ordenan todo el proceso de informatización, que fueron publicadas en la Gaceta Oficial de la República, en su edición ordinaria número 45 de 2019. Entre ellas las que a finales del mes de mayo del mismo año el Ministerio de Comunicaciones diera a conocer que regulan el uso de las Redes Privadas de Datos y el empleo de Sistemas Inalámbricos de Alta Velocidad.<sup>82</sup>

### *II.2.1.1 El Decreto-Ley No. 370 y la protección de datos*

Anteriormente, existían 39 documentos relacionados con el proceso de informatización de la sociedad, los cuales al entrar en vigor las nuevas normas jurídicas quedaron reorganizados quedando como norma jurídica de rango superior del país en materia de informatización el Decreto-Ley No. 370 del 17 de diciembre de 2018 sobre Informatización de la Sociedad Cubana. Su objetivo es elevar la soberanía tecnológica en beneficio de la sociedad, la economía, la seguridad y la defensa nacional, así como contrarrestar las agresiones

---

<sup>81</sup>GUERRA, E. (2016). *El caso ETECSA: Un problema de privacidad*.  
<http://www.postdata.club/issues/201609/el-caso-etecsa.html>

<sup>82</sup> PAZ, C. Y. (2019). *Informatización de la sociedad en Cuba: ordenar el proceso*.  
<http://citmatel.cu/noticias/informatizacion-de-la-sociedad-en-cuba-ordenar-el-proceso>



universidad  
de león



cibernéticas, salvaguardar los principios de seguridad de las redes y servicios, y defender los logros alcanzados por el Estado socialista.<sup>83</sup>

En el Decreto 370 el Estado incorpora por primera vez el Gobierno Electrónico en la prestación de sus servicios y trámites, la difusión de información e interacción con la población. En la Administración Pública en Cuba los estudios sobre gobierno electrónico se evidencian desde las ciencias jurídicas señalando que primeramente se debe entender en profundidad la realidad del contenido de este modelo de negocio. La estrategia cubana tiene al ciudadano en el centro de sus objetivos, buscando elevar su calidad de vida a través del uso de las TIC. Por lo que los usuarios necesitan saber que sus comunicaciones con el Gobierno son seguras, y que sus documentos y transacciones electrónicas están reconocidos y protegidos por la ley.<sup>84</sup>

En este sentido el artículo 33 del mencionado decreto establece que “los datos de carácter personal en soporte electrónico solo se pueden revelar a terceros que posean interés legítimo debidamente acreditado ante autoridad competente o que estén autorizados por el titular de estos datos; ante el incumplimiento de lo dispuesto, se procede conforme a lo establecido en la legislación vigente.” Declara además que son responsables del uso de las plataformas tecnológicas que protejan los datos del usuario y garanticen la veracidad y autenticidad de la información, los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular.

### *II.2.1.2 Decreto 360 y la privacidad*

---

<sup>83</sup> ÁVILA, Y. (2019). *Gaceta Oficial pública nuevas normas jurídicas para la Informatización*. <https://www.cubaperiodistas.cu/index.php/2019/07/gaceta-de-cuba-publica-nuevas-normas-juridicas-para-la-informatizacion/>

<sup>84</sup> ANTÚNEZ SÁNCHEZ, A., MATOS GUERRA, I., & ZAMORA RODRÍGUEZ, A. (2020). *La ventanilla única de certificación ambiental. Un análisis en el derecho ambiental en cuba.* “. [https://huespedes.cica.es/gimadus/34/34-04\\_ventanilla\\_unica\\_certificacion.html](https://huespedes.cica.es/gimadus/34/34-04_ventanilla_unica_certificacion.html)



universidad  
de león



La segunda regulación en hacer mención directa a los datos personales es el Decreto No. 360 sobre la Seguridad de las Tecnologías de la Información y la Comunicación y la Defensa del Ciberespacio Nacional que se adopta el 5 de junio de 2019, formando parte de las nuevas normas jurídicas para el reordenamiento de la informatización. La norma complementa el Decreto-Ley No. 370 regulando el empleo seguro de las TIC para la informatización de la sociedad, la defensa del ciberespacio nacional y establece la seguridad de las TIC y de los servicios y las aplicaciones que soportan, así como de las infraestructuras críticas de las TIC, con la finalidad de contar con una estrategia de fortalecimiento y sostenibilidad.<sup>85</sup>

Además, y en palabras de Miguel Gutiérrez Rodríguez, director general de Informática del MINCON se contempla igualmente, de manera habilitante, la protección de los datos personales en el entorno digital.<sup>86</sup> Este decreto en su Sección Tercera relativa al empleo seguro de las Tecnologías de la Información y la Comunicación establece que los Ministerios de Interior y de Justicia serán los encargados en base a sus funciones de velar por la protección de la información de personas físicas y jurídicas y la privacidad de los datos personales.

Mientras que les otorga a las entidades total responsabilidad por la información personal que manejen y los documentos que gestionen en el desempeño de sus funciones, pudiendo solo facilitárselo a las autoridades competentes y en correspondencia con la legislación vigente. El tratamiento de la información debe llevarse a cabo bajo los principios de legalidad, propiedad y necesidad, indicando de forma explícita los objetivos y alcances de dicho tratamiento. Con respecto al consentimiento no es del todo claro cuando es necesario o no que sea otorgado,

---

<sup>85</sup> GARCÍA SANTOS, N. (2019). "Modernizan Sistema de Enseñanza Personalizada a Distancia". Artículo publicado en Juventud Rebelde. In R. Polanco Fuentes, P. Terry, & M. Céspedes (Eds.), *Juventud Rebelde* (Sábado, 18).

<sup>86</sup> PUIG MENESES, Y. (2020). "Informatización de la sociedad cubana, un proceso impostergable" › *Cuba* › *Granma - Órgano oficial del PCC*. <http://www.granma.cu/cuba/2020-05-21/informatizacion-de-la-sociedad-cubana-un-proceso-impostergable-21-05-2020-11-05-21>



universidad  
de león



pues el término que se utiliza es ser solicitado cuando “se requiera”, dejando un margen abierto al indicar cuando existe el deber de otorgar el consentimiento.<sup>87</sup>

### *II.2.1.3 Resolución 127*

La Resolución 127 del 24 de junio de 2019 del Ministro de Comunicaciones que aprueba el Reglamento sobre proveedores de servicios de hospedaje y alojamiento está destinada a las personas jurídicas, la norma regula la organización, el funcionamiento y la expedición de licencias de operación del proveedor de servicios públicos de alojamiento y hospedaje en el entorno de Internet en el territorio nacional. En su Artículo 21 establece obligaciones a cumplir por los proveedores, en el apartado u) especifica que deben cumplir con la protección y tratamiento de los datos personales de sus clientes.

### *II.2.2 La privacidad en la prestación de servicios públicos de telecomunicaciones: ETECSA*

Los servicios de telecomunicaciones en Cuba sentaron sus bases de crecimiento en los servicios a través de la Red Nacional de Transmisión de Microondas, el cable de fibra óptica nacional, la Red Nacional de Transmisión de Datos, centrales telefónicas, los transmisores de radio y televisión y la aplicación de una nueva política de atención a los clientes más inclusiva. Como muestra de ello se comienza a comercializar el servicio de telefonía celular a personas naturales desde el 14 de abril de 2008. Este servicio es ofrecido por el único operador que desarrolla la telefonía fija, celular y los datos en Cuba, la Empresa de Telecomunicaciones de Cuba S.A., a efectos legales ETECSA, encargada de la prestación de servicios públicos de telecomunicaciones en todo el territorio nacional.<sup>88</sup>

ETECSA, en la prestación de los servicios públicos de telecomunicaciones y la instalación, operación, explotación y comercialización de redes públicas de telecomunicaciones se rige

---

<sup>88</sup> PÉREZ SALOMÓN, O. (2019). *Las telecomunicaciones en Cuba: 1959-2019* | *Cubadebate*. <http://www.cubadebate.cu/especiales/2019/05/09/las-telecomunicaciones-en-cuba-1959-2019/#.Xvm1envtBIU>



universidad  
de león



primeramente por la Constitución de la República de Cuba que ya cuenta entre sus derechos el referido a la protección de datos personales y por las disposiciones relativas a la contratación económica y al contrato de servicio previstas en el Código Civil. Debe cumplir además con lo establecido en la Ley de Protección de los Derechos de los Consumidores, que en sus principios contempla la protección a la privacidad y seguridad de los datos de los consumidores, aunque este derecho no aparece reflejado entre los derechos de los consumidores listados en el sitio oficial de ETECSA.<sup>89</sup>

Al ser la única empresa encargada de brindar los servicios la telefonía e Internet en Cuba está supeditada también a las normas jurídicas que se emiten desde el MINCOM y a cumplir con las funciones que le son asignadas a este. Entre las que se encuentran la aplicación de las normas relativas a la integridad y privacidad de la información que circula por las redes de telecomunicaciones e informáticas, asegurando su seguridad e invulnerabilidad. Para lo que debe disponer de políticas y estrategias para el desarrollo, evolución, producción, comercialización y utilización de las telecomunicaciones.<sup>90</sup>

#### *II.2.2.1 Disposiciones Administrativas de ETECSA para la protección de los datos personales.*

La información que circula por las redes no debe ser la única a la que se asegure protección pues la empresa obtiene y registra información personal de todos los usuarios que tiene. Al no existir una regulación específica en Cuba que proteja estos datos, y no estar del todo cubierta aún por las nuevas normas establecidas, Etecsa cuenta con políticas de privacidad que le permite cumplir con su deber administrativo en la salvaguarda de la información.

Las Páginas Amarillas de ETECSA, directorio telefónico donde se puede encontrar información comercial, tanto de personas naturales como jurídicas, establece reglas para el

---

<sup>89</sup> Generales, D. (2013). No. 321/2013 *Concesión administrativa a la Empresa de Telecomunicaciones de Cuba S.A.* 321.



universidad  
de león



tratamiento a la información y los datos personales. Respetando principios que no están definidos por normas jurídicas cubanas, como el de finalidad de los datos, “Los datos personales de los Usuarios serán utilizados para el cumplimiento de los fines indicados y siempre dentro de la competencia y atribuciones de ETECSA”, además asegura la confidencialidad de los mismos.

El 8 de enero de 2019 ETECSA implanta la Resolución 176, nueva norma jurídica que modifica las hasta el momento existentes condiciones contractuales vinculadas al servicio de telefonía básica fija en la vivienda. Mantiene los preceptos que se comienzan a manejar en las normas del país e incluye la protección de datos entre los Principios Generales a tener en cuenta en la elaboración de los contratos correspondientes al servicio telefónico básico que se presta a personas naturales. Debe garantizar el reconocimiento y aplicación del principio de respeto a la privacidad de los datos personales del usuario y la inviolabilidad de sus comunicaciones salvo los casos previstos en la legislación vigente.

Mientras que la regulación en el ámbito de Internet se rige por lo establecido en el Decreto No. 321/2013, Concesión Administrativa a la Empresa de Telecomunicaciones de Cuba, S.A. para la prestación de servicios públicos de telecomunicaciones. En el mismo se le establece a ETECSA la obligación de cuidar del secreto de la información proporcionada por los usuarios o transmitida o generada por las redes públicas al prestar sus servicios y no divulgarla si no existe consentimiento previo de éstos, tomando todas las medidas conducentes a este fin.

#### *II.2.2.2 Ejemplo de vulneraciones a la privacidad de ETECSA.*

Un ejemplo claro de la vulneración al derecho de los datos personales para millones de cubanos lo constituyó la filtración por cuatro años consecutivos de la base de datos de la compañía ETECSA. A partir de la cual se crearon aplicaciones de ordenador y para móviles en las cuales se podía acceder a los teléfonos fijos y móviles de las personas, su dirección particular, su número de DNI y a través del mismo su fecha de nacimiento. Información personal de carácter sensible que pone aún hoy en situación de indefensión a millones de



universidad  
de león



personas, que pueden ver sus datos utilizados para acceder a esferas íntimas de su vida como es el hogar o para mensajes comerciales no deseados.

En Cuba, el hecho más notorio en el ámbito de mensajes no deseados fue el relativo a la plataforma Zunzuneo, una red social patrocinada por la Agencia Internacional de Estados Unidos para la Ayuda al Desarrollo (USAID). El 10 de abril de 2014 mediante nota de prensa en el periódico, Daniel Ramos Fernández, Jefe de Seguridad de ETECSA, señaló la detección de tráfico de mensajería proveniente de ZunZuneo, que realizaba envíos masivos de mensajes a clientes de la empresa. Por otra parte aseguró que la misma no había entregado la base de datos de sus usuarios a ningún operador ni entidad extranjera, por lo que desconocía la vía y forma empleada para que un proyecto como ZunZuneo haya podido acceder a esa información.<sup>91</sup>

Sin embargo, esta base de datos clandestina proveniente del interior de la empresa continuó filtrándose hasta el año 2016, lo que refleja que no basta con que desde el ámbito administrativo y por los respectivos Ministerios, se creen regulaciones que en alguna medida se refieren a la protección de los datos personales. Es necesario que se defina una ley que profundice en el análisis de este tema y que permita que se le dé seguimiento de forma sistémica. Solo así se evitará la eventual indefensión de los ciudadanos ante las nuevas tecnologías en la esfera personal, teniendo en cuenta que la profusa legislación administrativa del Ministerio de la Informática y las Comunicaciones, no garantiza una tutela efectiva.

## Conclusiones

---

<sup>91</sup> GUERRA, E. (2016). *El caso ETECSA: Un problema de privacidad*. <http://www.postdata.club/issues/201609/el-caso-etecsa.html>



universidad  
de león



Primera: Para reconocer la protección de datos como un derecho fundamental, un elemento esencial es incluirlo en la norma primera del país, la Constitución. Colocando la privacidad ante cualquier interés político, social o económico. En el caso de España fue previsora de los riesgos que podría tener el uso de la informática y su repercusión en la privacidad de las personas, lo que ha servido de base jurídica para las normas siguientes en este ámbito. Sin embargo, en Cuba los avances tecnológicos carecían de una visión certera en cuanto a los efectos que la desprotección de los datos podría tener en las personas. Esto ha cambiado radicalmente con la inclusión de este derecho en la nueva Constitución de la República, lo que permitirá la configuración de un recurso procesal que sirva de garantía a este derecho, más conocido como hábeas data.

Segundo: Debido al impacto transversal que tiene la protección de datos, normalizar su regulación es esencial para evitar la fragmentación, de forma que todas las Administraciones se rijan por la misma norma en el tratamiento de los datos. La UE estableció el RGPD, que tuvo su trasposición al derecho español con la LOPDGDD, normas que han contribuido a fortalecer este derecho y su aplicación en el mercado único digital. En el caso de Cuba al no existir aún un Reglamento que regule de forma específica la protección de datos personales, deja en manos de las diferentes administraciones las medidas que garanticen la privacidad de la información. No se especifican criterios homogéneos para todos los Ministerios que puedan ser utilizados a nivel nacional, sin embargo, se espera el establecimiento de un reglamento que proteja los datos para febrero del año 2021, que debe unificar y simplificar el tratamiento que deben seguir las empresas. Además, teniendo en cuenta la apertura a los negocios por cuenta propia, este Reglamento puede esclarecer la regulación de los datos recogidos en las bases de datos privadas, que carecen del amparo constitucional.

Tercera: El ámbito de los derechos fundamentales adquiere todo un nuevo escenario cuando se refiere a su protección en las comunicaciones electrónicas; por esta razón en la UE se ha establecido una Directiva que regula de forma específica la protección de los datos en esta esfera. Estableciendo las obligaciones que tienen los proveedores de estos servicios para ofrecer condiciones adecuadas y de calidad. La redacción de las normas que regulan la





universidad  
de león



protección de datos en las telecomunicaciones debe basarse en el principio de neutralidad tecnológica que expanda su campo de acción y perdure en el tiempo. En este sentido en Cuba es necesaria la inclusión de una regulación específica que incluya tanto al MINCOM como a ETECSA, que asegure a los usuarios que sus datos tendrán el tratamiento correcto para preservar su privacidad. En la actualidad esta seguridad se encuentra desparramada en un conjunto de normas que no especifican de forma clara los procedimientos, ni el tratamiento por el tipo de dato que obtienen en el ejercicios de sus funciones.

Cuarta: El uso de Internet ha creado nuevas categorías de datos que necesitan de una regulación especial que proteja los derechos de los usuarios. La Comisión Europea ha planteado la propuesta de Reglamento ePrivacy, que regula de forma más estricta los datos personales directos, o los datos indirectos que permiten localizarnos como individuos a través de la navegación web u otras herramientas que traten datos en la red. Generando diferentes posiciones en los Estados miembros, evidenciando la dificultad de regular la privacidad de los usuarios en Internet, más cuando los datos se han convertido en elementos de mercado para muchas empresas. Cuba se encuentra jurídicamente muy alejada de llegar a regular estos datos, pero debe existir una disposición política que avizore la necesidad de normar su tratamiento, para que se lleven a cabo las inversiones y las medidas técnicas necesarias.

Quinto: El Estado cubano ha establecido entre sus estrategias de desarrollo la informatización del país para lograr una sociedad más avanzada que esté en concordancia con los tiempos que corren a nivel mundial, sin embargo, han centrado sus objetivos en la seguridad de las aplicaciones y la información que se genera de estas, no en la protección de los datos de las personas. Precisamente cada día más cubanos se hacen usuarios de las diferentes plataformas de Internet, sin estar educados en la necesidad de tener cautela con la información personal que entregan al mundo. Siendo la empresa por la que acceden a la red, la que por más de 4 años permitió la filtración de los datos de millones de cubanos, por lo que el sector de las telecomunicaciones en Cuba debe hacer conciencia de la importancia de preservar la privacidad de sus clientes, de generar normas más específicas y educar a los usuarios desde la



universidad  
de león



acción en la importancia de otorgar sus datos personales, exigiendo el consentimiento en cada caso y explicando las consecuencias de su otorgamiento.

## Recomendaciones

Primera: Dar seguimiento al proceso de aprobación del Reglamento de ePrivacy, haciendo énfasis en las medidas referentes a los nuevos datos que surgen del uso de Internet, como los metadatos y las cookies y analizar su efecto en la protección de los datos personales y la confianza de los usuarios.

Segunda: Aprobación de un Reglamento cubano de Protección de Datos, a la luz de las fortalezas y problemas que han estado presentes en los modelos más avanzados de Europa y España.

## Bibliografía

- AA.VV. (2018). " La ley orgánica de protección de datos personales y garantía de los derechos digitales: proceso de elaboración, estructura, objeto, ámbito de aplicación, y principios de la norma proceso de elaboración". *Revista Del Gabinete Jurídico De Castilla-La Mancha*, 16.
- AGENCIA de los Derechos Fundamentales de la Unión Europea., & Consejo de Europa (Estrasburgo). (2018). *Manual de legislación europea en materia de protección de datos*. <https://doi.org/10.2811/60145>
- AMOROSO FERNÁNDEZ, Y. (1994). "Breve exposición de la informática en Cuba : la protección y comercialización del software . El régimen de protección de los datos". *Revista General de Información y Documentación*, 4, 195-205.
- APARICIO SALOM, J., & SANFULGENCIO TOMÉ, S. (2014). «El régimen jurídico de las cookies y su aplicación por la Agencia Española de Protección de Datos». *Revista Aranzadi Doctrinal*, 11, 1-21.
- ÁVILA, Y. (2019). *Gaceta Oficial pública nuevas normas jurídicas para la Informatización*. <https://www.cubaperiodistas.cu/index.php/2019/07/gaceta-de-cuba-publica-nuevas-normas-juridicas-para-la-informatizacion/>



universidad  
de león



- BALLESTEROS MOFFA, L. Á. (2005). *La privacidad electrónica . Internet en el centro de protección*. Tirant lo Blanch.
- \_ «La revisión del régimen jurídico de la privacidad en la Unión Europea». (2018) *Revista del posgrado en derecho de la UNAM*, Num 8(April 2016), 38-64.
- BENALAL QUINTANA, A. (2019). "Ser o no ser en la era digital : el futuro reglamento de ePrivacy". *Prisacom*, 1-3.
- CAMACHO CLAVIJO, S. (2005). *Parte intervinientes, formación y prueba del contrato electrónico*. Editorial Reus, S. A.
- CORRIPIO GIL-DELGADO, M. D. L. R., & MARROIG POL, L. (2002). "El ordenamiento español y la protección de datos personales en el sector de las telecomunicaciones". *Boletín del Ministerio de Justicia*, No 1930, págs. 3565-3583.  
<https://dialnet.unirioja.es/servlet/articulo?codigo=286299>
- DAVARA RODRIGUEZ, M. A. (2003). "La Protección de Datos personales en el sector de las Comunicaciones Electrónicas". *Universidad Pontificia Comillas, Ira*, 183.
- DE ASÍS ROIG, A. (2017). "SECRETO, PROTECCIÓN DE DATOS Y SEGURIDAD E INTEGRIDAD EN LAS TELECOMUNICACIONES". En *Los retos del Estado y la Administración en el siglo XXI* (pp. 2129-2154). Tirant lo Blanch.
- DE FARAMIÑAN GILBERT, J. M. (2001). "La carta de los derechos fundamentales de la Unión Europea". *Revista de Estudios Regionales*, 01, 237-264.  
<https://econpapers.repec.org/RePEc:rer:articu:v:01:y:2001:p:237-264>
- DE MIGUEL ASENSIO, P. A. (2017). "Competencia y Derecho aplicable en el reglamento general sobre protección de datos de la Unión Europea.". *Revista Española de Derecho Internacional*, 69(1), 75-108. <https://doi.org/10.17103/redi.69.1.2017.1.03>
- EUROPEA, R. P. D. E. A. L. U. (2019). "Propuesta de Reglamento sobre e-privacidad en las comunicaciones electrónicas.". <https://es-ue.org/documentation/transportes-telecomunicaciones-y-energia/> [Consulta: 01 junio 2020]
- FLAQUER RIUTORT, J. (2018). "Nuevas tendencias y propuestas en el tratamiento legal del uso de cookies : especial referencia a la propuesta de reglamento comunitario sobre la privacidad y las comunicaciones electrónicas (ePrivacy)". *Revista Aranzadi de Derecho y Nuevas Tecnologías*, num 47.
- GARCÍA MAHAMUT, R. (2019). "Del reglamento general de protección de datos a la lo 3/2018 de protección de datos personales y garantías de los derechos digitales". En Rosario García Mahamu & tBeatriz T. Mallén (Eds.), *El reglamento general de*



universidad  
de león



*protección de datos un enfoque nacional y comparado especial referencia a la lo 3/2018 de protección de datos y garantía de los derechos digitales* (TIRANT LO, pp. 95-103).

GARCÍA SANTOS, N. (2019). Modernizan Sistema de Enseñanza Personalizada a Distancia. Artículo publicado en *Juventud Rebelde*. En R. Polanco Fuentes, P. Terry, & M. Céspedes (Eds.), *Juventud Rebelde* (Sábado, 18).

GARCÍA TERCERO, D. Á. (2016). "Los datos personales en las comunicaciones electrónicas". Universitat Rovira I Virgili.

GASCÓN MARCÉN, A. (2020). «El Reglamento sobre la privacidad y las comunicaciones electrónicas, la asignatura pendiente del Mercado Único Digital» (93/2020; CEU Edicio, Serie Unión Europea y Relaciones Internacionales).

Generales, D. (2013). No. 321/2013 *Concesión administrativa a la Empresa de Telecomunicaciones de Cuba S.A. 321*.

GONZÁLEZ LÓPEZ, J. J. (2017). "La retención de datos de tráfico de las comunicaciones en la Unión Europea : una aproximación crítica". *Diario La Ley*, No 6456, 1-19.

GREGORY VOSS, W. (2017). «First the GDPR, Now the Proposed ePrivacy Regulation». *Journal of Internet Law*, 21(1), 3-11. <https://search-proquest-com.ezproxy.is.ed.ac.uk/docview/1918794232/fulltextPDF/39570841F54048ADPQ/1?accountid=10673%0Ahttps://ssrn.com/abstract=3008765>

GUERRA, E. (2016). *El caso ETECSA: Un problema de privacidad*. <http://www.postdata.club/issues/201609/el-caso-etecsa.html> [Consulta: 04 junio 2020]

PUIG MENESES, Y. *Informatización de la sociedad en Cuba | Presidencia de la República de Cuba*. (2019). <https://www.presidencia.gob.cu/es/gobierno/programas-priorizados/informatizacion-de-la-sociedad-en-cuba/> [Consulta: 04 junio 2020]

Jefatura del Estado. (2018). "Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales.". *Boletín Oficial del Estado*, 294(6 de Diciembre de 2018), 5-68.

MANTECA VALDELANDE, V. (2000). "La protección de datos personales en las telecomunicaciones : regulación comunitaria europea y española.". 43-73. <https://doi.org/10.33426/rcg/2000/51/629>

MEJÍA CAMBAR, O. (2019). "Análisis al reglamento General de Protección de Datos en la Unión Europea: Un Vistazo a la Actualidad de la Era Digital". *La Revista de Derecho*, 40(1), 93-104. <https://doi.org/10.5377/lrd.v40i1.8909>



universidad  
de león



- MINERO ALEJANDRE, G. (2019). Nuevas tendencias en materia de protección de datos personales. La nueva Ley Orgánica y la jurisprudencia más reciente. *Anuario jurídico y económico escorialense*, 52, 125-148.
- MORALES, A. (2018). *Análisis de la propuesta de Reglamento E-Privacy*. <https://www.cysae.com/analisis-de-la-propuesta-de-reglamento-e-privacy/> [Consulta: 10 marzo 2020]
- OBSERVATORY, C. E. (2018). "Shutting down ePrivacy: lobby bandwagon targets Council Retrieved". <https://corporateurope.org/en/power-lobbies/2018/06/shutting-down-eprivacy-lobby-bandwagon-targets-council?hash=keZ3nidpfZbeVQAaYUYoSTDAvjXndSjmZurmIQLAQeY> [Consulta: 14 mayo 2020]
- OJEDA BELLO, Z., & AMOROSO FERNÁNDEZ, Y. (2016). "La protección de los datos personales en Cuba desde la legislación vigente". *Justicia Juris*, 12, 87-94.
- ORTEGA GIMÉNEZ, A., & GONZALO DOMENECH, J. J. (2018). Nuevo marco jurídico en materia de protección de datos de carácter personal en la Unión Europea. *Revista de la Facultad de Derecho*, 44, 01-35. <https://doi.org/10.22187/rfd2018n44a2>
- ORTIZ LIMA, C. M. (2010). "Transmisión vía fibra óptica de señales analógicas utilizando subportadora modulada en frecuencia de pulsos : aplicación potencial en instrumentación y control". Instituto Nacional de Astrofísica, Óptica y Electrónica.
- PALMA ORTIGOSA, A. (2018). «Contexto normativo de la protección de datos personales». En *Protección de datos, responsabilidad activa y técnicas de garantía* (1ra Edición, pp. 9-16). Editorial Reus, S. A.
- PALOMAR, A., & FUERTES, J. (s. f.). *Autoridades autonómicas de Protección de Datos*. Recuperado 9 de junio de 2020, de <https://practico-proteccion-datos-personales.es/vid/autoridades-autonomicas-proteccion-datos-716170265>
- PAVÓN PÉREZ, J. (2001). "La protección de datos personales en el consejo de Europa: el protocolo adicional al convenio 108 relativo a las autoridades de control y a los flujos transfronterizos de datos personales". *Anuario de la Facultad de Derecho*, 19, 235-252.
- PAZ, C. Y. (2019). *Informatización de la sociedad en Cuba: ordenar el proceso*. <http://citmatel.cu/noticias/informatizacion-de-la-sociedad-en-cuba-ordenar-el-proceso> [Consulta: 04 junio 2020]
- PÉREZ LUÑO, A. (1981). "Informática y libertad: Comentario al artículo 18.4 de la Constitución". *Revista de estudios políticos*, 24, 31-54.



universidad  
de león



- PÉREZ MARTÍNEZ, J., FRÍAS BARROSO, Z., & UREÑA LÓPEZ, A. (2018). «*La evolución de Internet en España: del Tesis a la economía digital*». Red.es. <https://www.bcg.com/documents/file100409.pdf>
- PÉREZ RIVAS, D. A. (2017). «*Metadatos vs privacidad: la insoportable levedad de la red.*» (pp. 233-250).
- RODERO, Á. B. (s. f.). «*Agencia de Protección de Datos: la AEPD y la ley de protección de datos*». Recuperado 9 de junio de 2020, de <https://www.angelbenitorodero.es/proteccion-de-datos/agencia-de-proteccion-de-datos-la-aepd-y-la-ley-de-proteccion-de-datos/>
- RODRIGUEZ DELGADO, J. P. (2008). «La Ley 25/2007 sobre conservación de comunicaciones electrónicas a la luz de la Directiva europea 2006/24/CE». *RCE*, 92, 3-45.
- SALMACENTIS, A. I. (2019). «Protección de datos y derechos digitales». *Crónica de Legislación*, 7, 254-259.
- SALOMÓN, O. P. (2019). *Las telecomunicaciones en Cuba: 1959-2019 | Cubadebate*. <http://www.cubadebate.cu/especiales/2019/05/09/las-telecomunicaciones-en-cuba-1959-2019/#.Xvm1envtbIU> [Consulta: 04 junio 2020]
- SERRANO OLIVARES, R. (2018). «Los derechos digitales en el ámbito laboral: comentario de urgencia a la ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales». *IUSLabor*, 3/2018, 216-229.
- SOARES CRUZ, A. P. (2013). «*Algunas consideraciones sobre la protección de datos personales en la legislación cubana*». 53(9), 1689-1699. <https://doi.org/10.1017/CBO9781107415324.004>
- ZABALLOS PULIDO, E. (2013). «*La protección de datos personales en España: Evolución Normativa y Criterios de Aplicación*» [Universidad Complutense De Madrid]. <http://eprints.ucm.es/21927/1/T34576.pdf>
- ZAMORA, P. L. (2012). «La incorporación de la Directiva 2009/136/CE del Parlamento Europeo y del Consejo de 25 de noviembre de 2009 al ordenamiento jurídico español». *Nueva época*, 14, 225-228. <https://doi.org/10.5209/FORO.39002>



universidad  
de león



## Anexos

Anexo A. Resumen de la Política de privacidad de Movistar

Fecha de publicación: Julio 2020

A través de la presente Política se informa que los datos personales de los clientes Movistar serán tratados de conformidad con los principios de transparencia, limitación de la finalidad, minimización de datos, exactitud, integridad y confidencialidad, así como respetando el resto de obligaciones y garantías establecidas en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, como en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.

Para ello hemos actualizado nuestra Política de Privacidad, que afecta a personas físicas y a los interlocutores de empresas, y que sustituye a la que anteriormente regulaba el tratamiento de los datos de clientes Movistar, con el objetivo de renovar la confianza del cliente y brindarle una experiencia diferencial.

A los efectos de cumplir con la mencionada normativa y ayudar al Cliente o usuario de cualquier Producto o Servicio Movistar a entender cómo se recopilan, emplean, tratan y protegen sus datos personales, Movistar le informa de los siguientes aspectos relacionados con su derecho a la protección de datos personales.

### 1. **Glosario de términos**

Definición de los conceptos utilizados por la Política de privacidad para su mejor comprensión.

### 2. **¿Quién trata tus datos?**

Indicación de quiénes son los responsables del tratamiento y el contacto de nuestra oficina del Delegado de Protección de datos (DPO).



3. **¿Qué es un dato personal y qué datos tratamos?**

Explicación de las categorías de datos tratadas por Movistar.

4. **¿Cómo tratamos tus datos?**

Explicación de los distintos roles que puede asumir el cliente y el usuario, así como las diferencias que implica a la hora de definir la forma en que tratamos sus datos.

5. **¿Para qué tratamos tus datos?**

Relación de las bases legitimadoras y finalidades para las cuales Movistar podrá realizar el tratamiento de datos de carácter personal (ejecución del contrato, interés legítimo y consentimiento).

6. **Plazos de conservación de la información**

Indicación de los periodos de conservación relacionados con cada uno de los tratamientos de datos de carácter personal según la finalidad del mismo.

7. **Ejercicio de derechos**

Detalle de toda información necesaria sobre los derechos que asisten al cliente o usuario así como los medios por los cuales puede solicitar a Movistar su ejercicio.

8. **Información que compartimos: destinatarios o categorías destinatarios**

Detalle de la información que compartimos con destinatarios y las finalidades de la comunicación.

9. **Transferencias internacionales de datos**

Concreción de las transferencias internacionales de datos que llevamos a cabo fuera del Espacio Económico Europeo.

10. **Seguridad y confidencialidad en el tratamiento de tu información**

Medidas de confidencialidad y seguridad de la información utilizadas por Movistar para la protección de los datos de carácter personal.

11. **Decisiones automatizadas**

Información sobre la existencia, en su caso, de decisiones automatizadas que produzcan efectos para el cliente.

12. **Tratamiento ulterior**

Alcance del tratamiento ulterior de los datos de carácter personal para nuevas finalidades.





### 13. Tratamiento de datos de menores

Información sobre el tratamiento de datos realizado por Movistar en caso de que el cliente o usuario sea menor de edad.

### 14. ¿Cómo y para qué anonimizamos tus datos?

Información acerca del proceso de anonimización de los datos personales del cliente o usuario.

### 15. Cookies

Detalle de la Política de cookies.

### 16. Cambios de la política

Regulación del procedimiento de modificación de la Política de privacidad.

### 17. Miscelánea

Aplicabilidad y contexto de la Política de privacidad.

La explicación detallada de cada acápite puede consultarse en <https://www.movistar.es/particulares/centro-de-privacidad/>.

Anexo B. Resumen de la Política de privacidad de Telefónica

## **Información adicional y detallada sobre el uso de sus datos de carácter personal:**

### 1. RESPONSABLES DE TRATAMIENTO

#### *1.1. ¿Quiénes son los responsables de tratamiento?*

Es responsable del tratamiento Telefónica, S.A. (con CIF A28015865 y dirección postal en Gran Vía 28, 28013, Madrid).

#### *1.2. ¿Existe un Delegado de Protección de Datos al que pueda contactar?*

Sí; los interesados podrán ponerse en contacto con el Delegado de Protección de Datos (DPO) a través de la siguiente dirección de correo electrónico [DPO\\_telefonicasa@telefonica.com](mailto:DPO_telefonicasa@telefonica.com).



universidad  
de león



## 2. FINALIDAD DEL TRATAMIENTO Y LEGITIMACIÓN

### 2.1. *¿Con qué finalidad trataremos sus datos y cuál es la base que nos legitima?*

La finalidad principal es la resolución en segunda instancia de las reclamaciones de los usuarios finales con relación a los productos y servicios de las empresas del Grupo Telefónica Adheridas al Reglamento del SDC, que actúa como marco de referencia.

Como segunda finalidad, y tal y como señala el Reglamento del SDC, la elaboración de informes, estadísticas y estudios que identifiquen las oportunidades de mejora respecto al grado de orientación al cliente de los procesos y practicas internas del Grupo Telefónica con el objeto de canalizar las mismas a las Áreas de Negocio correspondientes y fomentar su puesta en práctica en pro de los derechos de los usuarios finales.

La licitud para el tratamiento viene determinada por su consentimiento, el cual ha sido prestado y recabado a través del formulario online de reclamaciones del SDC y al marcar la casilla aceptando este aviso legal de protección de datos; y/o mediante el envío directo de sus datos personales al enviar su reclamación al SDC a través de correo postal ordinario.

Del mismo modo, el SDC tiene un interés legítimo para la elaboración de informes y estadísticas, conforme a su función de identificación de oportunidades de mejora, hasta que no sea revocado el consentimiento.

El interesado será el único responsable en el supuesto de haber facilitado datos falsos, inexactos, incompletos o no actualizados.

### 2.2. *¿Será necesario que nos facilite todos sus datos? ¿Qué sucederá si no nos los facilita?*

Será necesario que nos facilite ciertos datos personales (según lo dispuesto en el artículo 9º del reglamento del SDC). Una vez se esté tramitando la reclamación puede que nos dirijamos



universidad  
de león



a Ud. para requerirle información adicional. En caso de que no nos facilite los datos solicitados, ello podría impedir la resolución de su reclamación por el SDC.

2.3. *¿Realizaremos decisiones individualizadas automatizadas y/o elaboración de perfiles, que produzcan efectos jurídicos o le afecten significativamente de modo similar?*

No.

2.4. *¿Durante cuánto tiempo trataremos sus datos?*

Los datos personales proporcionados serán conservados mientras subsista la finalidad para la cual fueron recabados y hasta el vencimiento de los plazos de prescripción de las obligaciones legales en base a normativa vigente, siendo bloqueados cuando hayan dejado de ser pertinentes para el cumplimiento de dicha finalidad.

### 3. DESTINATARIOS DE CESIONES:

3.1. *¿Cederemos sus datos a otras empresas?*

No.

### 4. DESTINATARIOS DE TRANSFERENCIAS INTERNACIONALES:

4.1. *¿Sus datos de carácter personal serán transferidos a terceros países u organizaciones internacionales?*

No.

### 5. DERECHOS DEL INTERESADO:

5.1. *¿Qué derechos le amparan en relación al tratamiento de sus datos?*

Como prevé el Reglamento General de Protección de Datos, le informamos que usted tiene los siguientes derechos:



- Derecho de acceso:  
A través del ejercicio de este derecho Ud. puede conocer qué datos de carácter personal están siendo tratados por parte del responsable, la finalidad de este tratamiento, el origen de los citados datos y si se han comunicado o se van comunicar a un tercero.
- Derecho de rectificación:  
A través del ejercicio de este derecho Ud. puede modificar aquellos datos que sean inexactos o incompletos.
- Derecho de cancelación y supresión:  
A través del ejercicio de este derecho Ud. puede solicitar la cancelación y/o supresión cuando, entre otros motivos, los datos ya no fueran necesarios para los fines que fueron recogidos.
- Derecho de oposición:  
A través del ejercicio de este derecho Ud. puede, por motivos relacionados con su situación particular, oponerse al tratamiento de sus datos en cuyo caso se dejarán de tratar, salvo que se acredite un interés legítimo o sea necesario para el ejercicio o la defensa de posibles reclamaciones.
- Derecho a la limitación del tratamiento:  
A través del ejercicio de este derecho Ud. puede solicitar la limitación del tratamiento de sus datos, en cuyo caso le informamos que únicamente los conservaremos para el ejercicio o defensa de reclamaciones tal y como prevé el Reglamento General de Protección de Datos.
- A la portabilidad de sus datos  
A través del ejercicio de este derecho Ud. puede recibir los datos personales que le incumban, y que haya facilitado, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento.

## 5.2. ¿Cuándo responderemos a su solicitud?

Responderemos a sus peticiones a la mayor brevedad posible y, en todo caso, en el plazo de un mes desde la recepción de su solicitud. Dicho plazo podrá prorrogarse otros dos meses en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes. El responsable informará al interesado de la prórroga dentro del primer mes desde la solicitud.



universidad  
de león



### 5.3. ¿Dónde debe dirigirse para el ejercicio sus derechos?

Para ejercitar estos derechos, usted puede dirigirse a C/Gran Vía 28, 4ª planta, Servicio de Defensa del Cliente (ref. LOPD) o enviar un correo electrónico [SDC.datos@telefonica.com](mailto:SDC.datos@telefonica.com) (indicando en el asunto: LOPD seguido del derecho que sea ejercitar). En ambos casos, se deberá remitir una fotocopia del Documento Nacional de Identidad. De no cumplir estos requisitos, no será gestionada la petición.

### 5.4. ¿Usted tiene derecho a reclamar?

Sí. Usted, especialmente cuando no haya obtenido satisfacción en el ejercicio de sus derechos, tiene derecho a presentar reclamación ante la autoridad nacional de control, a estos efectos debe dirigirse ante la Agencia Española de Protección de Datos

Con carácter previo a la presentación de dicha reclamación contra la Agencia Española de Protección de datos, usted puede dirigirse al Delegado de Protección de Datos (DPO) a través de la siguiente dirección de correo electrónico [DPO\\_telefonicasa@telefonica.com](mailto:DPO_telefonicasa@telefonica.com).

\*\*\*\*\*

*ESTE AVISO LEGAL DE PROTECCIÓN DE DATOS PREVALECE FRENTE A CUALQUIER OTRO AVISO LEGAL/CLÁUSULA DE PROTECCIÓN DE DATOS QUE CONTenga CUALQUIER CONDICIÓN QUE CONTRADIGA LO AQUÍ ESTABLECIDO*

Obtenido de [https://www.telefonica.es/es/acerca\\_de\\_telefonica/servicio-defensa-cliente/politica-de-privacidad](https://www.telefonica.es/es/acerca_de_telefonica/servicio-defensa-cliente/politica-de-privacidad)



universidad  
de león



Anexo C. Resumen de la Política de privacidad de ETECSA

## Protección al consumidor

### Derechos del consumidor

- Recibir un trato amable y ser escuchado con respeto
- Tener las condiciones adecuadas para la seguridad, protección de la vida, la salud y conservación del medio ambiente
- Recibir información veraz, oportuna y educativa sobre los servicios, productos y cualquier modificación que la empresa realice
- Que sean protegidos nuestros intereses económicos mediante transacciones contractuales y de compraventa, justas y equitativas; divisar el precio de los productos y las tarifas de los servicios; presenciar la prueba del artículo que lo requiera, así como recibir el comprobante de pago
- Tener la posibilidad de escoger, en consonancia con nuestras expectativas como consumidores y condiciones de la economía nacional
- Obtener servicio postventa y de reparación de acuerdo a los compromisos establecidos
- Acceder a los órganos correspondientes para la protección de nuestros derechos, donde podamos exponer nuestras opiniones y reclamaciones

Obtenido de [http://www.etcscu.com/proteccion\\_al\\_consumidor/](http://www.etcscu.com/proteccion_al_consumidor/)

### Política de privacidad de Páginas Amarillas

Esta Política de Privacidad establece los términos en que se utiliza y protege la información y los datos personales que son proporcionados por los usuarios, al momento de su publicación en el sitio web de Páginas Amarillas.

A los efectos de la presente "Política", se entiende por Usuario a la persona que voluntariamente se registre en este sitio web, mediante los formularios establecidos por la



universidad  
de león



Empresa de Telecomunicaciones de Cuba S.A. ETECSA, en tanto Visitante es aquella persona que accede libremente a la información disponible en este sitio Web sin necesidad de registrarse previamente.

ETECSA y el Usuario asumen la obligación de mantener el principio de confidencialidad de dicha información, así como de utilizar ésta exclusivamente en los términos pactados en el correspondiente contrato, reservándose el derecho mutuo de establecer la acción por indemnización de daños y perjuicios que sea procedente en caso de su incumplimiento.

El tratamiento a la información y los datos personales que se realiza en el sitio [www.pamarillas.cu](http://www.pamarillas.cu) de ETECSA, se rige por las siguientes reglas:

- Los datos personales de los Usuarios serán utilizados para el cumplimiento de los fines indicados en el formulario correspondiente y siempre dentro de la competencia y atribuciones de ETECSA.
- ETECSA asegurará la confidencialidad de los datos personales de los usuarios, requeridos para su registro en el sitio web de Páginas Amarillas.
- ETECSA publicará el contenido de la información suministrada y el sitio de enlace, respetando la integridad de los contenidos que se suministran, siempre y cuando estos no comprendan algún elemento que atente contra la dignidad de personas, ideas, religiones o símbolos de cualquier país o de una entidad nacional o internacional; sean contrarios a la ley, a la moral, a las buenas costumbres, a las normas de conducta generalmente aceptadas o atenten contra el orden público.
- ETECSA realizará el filtrado y tratamiento de datos mediante mecanismos automatizados, con el objetivo de generar registros de la actividad de los visitantes y registros de audiencia y sólo utilizará dicha información para la elaboración de informes que cumplan con los objetivos de evaluación del comportamiento del servicio en cuestión. En ningún caso realizará operaciones que impliquen asociar dicha información a algún usuario identificado o identificable o relacionar a este con otro sitio web sin su consentimiento.



universidad  
de león



- Ambas partes respetarán las disposiciones vigentes sobre derechos de Propiedad Intelectual.
- El Usuario garantiza y declara que es legítimo titular de los derechos de Propiedad Intelectual asociados a los contenidos, informaciones y datos objeto de publicidad en el sitio web Páginas Amarillas o que en su defecto cuenta con la debida autorización del titular de tales derechos. Los derechos antes mencionados comprenden sin limitación: las marcas, nombres comerciales, lemas comerciales, emblemas empresariales, rótulos de establecimientos, indicaciones de procedencia; nombres de dominio; dibujos industriales y diseños industriales; derechos de autor que comprenden cualquier manifestación de las artes sin que se limiten: a las obras escritas y orales, las obras musicales, con letra o sin ella; las obras audiovisuales; las obras radiofónicas; las obras de dibujo, pintura, grabado, diseño y otras similares; las obras fotográficas y otras de carácter similar; las obras de artes plásticas; los mapas, planos, croquis y otras obras similares; las traducciones, versiones, adaptaciones, arreglos musicales y demás transformaciones de carácter creativo de una obra científica, literaria, artística o educacional; las antologías, enciclopedias y otras compilaciones.
- El Usuario garantiza que las informaciones, contenidos y datos proporcionados para su publicación en el sitio web, no violan los derechos de Propiedad Intelectual de terceros, ni atentan contra la dignidad de las personas. El Usuario será responsable ante posibles reclamaciones, corriendo a su cuenta y riesgo de los daños y perjuicios que se generen por tales motivos.

Obtenido de <http://pamarillas.cu/generales/index/politica-de-privacidad>