



universidad  
de león



**FACULTAD DE DERECHO  
UNIVERSIDAD DE LEÓN  
CURSO 2018/2019**

**EL ASISTENTE DE VOZ DE GOOGLE Y  
LA AUSENCIA DEL CONSENTIMIENTO  
EXPLÍCITO DE TERCEROS PARA EL  
TRATAMIENTO DE DATOS  
GOOGLE'S VOICE ASSISTANT AND  
THE ABSENCE OF THIRD PARTY'S  
EXPLICIT CONSENT FOR DATA  
PROCESSING**

**MÁSTER EN DERECHO DE LA CIBERSEGURIDAD  
Y ENTORNO DIGITAL**

AUTOR: D. CÉSAR AUGUSTO MEJÍA OSORIO

TUTOR: D. SALVADOR TARODO SORIA

# ÍNDICE

ABREVIATURAS

RESUMEN

PALABRAS CLAVES

ABSTRACT

KEY WORDS

INTRODUCCIÓN 1

HIPÓTESIS PLANTEADA 2

OBJETIVOS GENERALES 2

METODOLOGÍA 3

1. HISTORIA Y EVOLUCIÓN DE LOS SISTEMAS DE 4

RECONOCIMIENTO DE VOZ Y ANÁLISIS DEL ASISTENTE DE VOZ DE *GOOGLE* 4

1.1 BREVE HISTORIA DE LOS SISTEMAS DE RECONOCIMIENTO DE VOZ 4

1.1.2 *Cómo operan los sistemas ASR* 5

1.1.3 *Lista de asistentes de voz más usados* 7

1.2 ANÁLISIS DE LA POLÍTICA DE PRIVACIDAD DE *GOOGLE* 8

1.2.1 *Criterios de la política de privacidad de Google* 10

1.2.2 *Objetivo* 10

1.2.3 *Finalidad* 10

1.2.4 *Información que recoge Google* 10

1.2.5 *¿Por qué y para qué recoge Google estos datos?* 12

1.2.6 *Controles de privacidad* 12

1.2.7 *Compartir información* 13

1.2.8	<i>Proteger información</i>	13
1.2.9	<i>Exportar y eliminar tu información</i>	14
1.2.10	<i>Cumplimiento y cooperación con autoridades reguladoras</i>	14
1.3	MI ACTIVIDAD DE <i>GOOGLE</i> .	15
1.3.1	<i>Módulo de actividad de voz y audio de Google</i>	16
1.3.2	<i>Cómo opera el asistente de voz de Google</i>	17
2.	DERECHO A LA INTIMIDAD, PROPIA IMAGEN, SECRETO DE LAS COMUNICACIONES, Y PROTECCIÓN DE DATOS, EN EL ÁMBITO DE GRABACIONES DE VOZ	19
2.1	DERECHO A LA INTIMIDAD	19
2.2	DERECHO A LA PROPIA IMAGEN	21
2.3	DERECHO AL SECRETO EN LAS COMUNICACIONES	23
2.4	DERECHO DE PROTECCIÓN DE DATOS	25
2.5	DATOS BIOMÉTRICOS ESPECIALMENTE PROTEGIDOS	28
2.5.1	<i>Que es un dato biométrico</i>	28
2.5.2	<i>La voz como dato biométrico</i>	29
2.5.3	<i>Biometría y clonación de voz</i>	30
2.6	TRATAMIENTO AUTOMATIZADO DE DATOS	30
3.	CONTRATO, POLÍTICA DE PRIVACIDAD, TÉRMINOS Y CONDICIONES.	31
3.1	EL CONTRATO A LA LUZ DE LA LEGISLACIÓN DE ESPAÑA	31
3.1.1	<i>Contrato electrónico</i>	32
3.1.2	<i>Contrato por adhesión</i>	33
3.2	LA CALIFICACIÓN JURÍDICA DE LA POLÍTICA DE PRIVACIDAD Y LOS TÉRMINOS Y CONDICIONES DE <i>GOOGLE</i>	34
4.	EL CONSENTIMIENTO	35
4.1	EL CONSENTIMIENTO EN EL <i>RGPD</i>	36

4.1.1 <i>El consentimiento explícito</i>	37
4.1.2 <i>La manifestación de voluntad informada</i>	38
4.1.3 <i>Manifestación de voluntad inequívoca</i>	39
4.2 EL CONSENTIMIENTO EN EL MÓDULO DE ACTIVIDAD DE VOZ Y AUDIO DE GOOGLE.	39
4.3 CONSENTIMIENTO EN LAS GRABACIONES DE VOZ	40
5. RESULTADOS OBTENIDOS QUE RESUELVEN LA HIPÓTESIS	42
5.1 PRUEBAS TÉCNICAS AL MÓDULO DE ACTIVIDAD DE VOZ Y AUDIO DE GOOGLE EN DISPOSITIVOS ANDROID	42
5.2 ANÁLISIS DE LA ENCUESTA ELECTRÓNICA: ASISTENTES VIRTUALES ACTIVADOS POR VOZ EN EL HOGAR Y SMARTPHONES (TELÉFONOS INTELIGENTES)	46
REFLEXIÓN	49
CONCLUSIONES	50
TABLAS	1
GRÁFICOS	2
BIBLIOGRAFÍA	1
FUENTES NORMATIVAS	3
FUENTES JURISPRUDENCIALES	5
OTRAS FUENTES	6
ANEXOS	8

## **AGRADECIMIENTO**

Como Becario del Máster Universitario en Derecho de la Ciberseguridad y Entorno Digital en la Universidad de León España 2018/2019, agradezco la beca otorgada por parte de la Fundación Carolina, el INCIBE, y Unileón, que me han permitido esta grata experiencia para mi crecimiento personal y profesional.

Espero que sigan con la labor de apoyar a muchos estudiantes que sueñan con esta valiosa oportunidad.

Gracias.

Cesar Mejía.

## ABREVIATURAS

<i>AEPD</i>	Agencia Española de Protección de Datos
<i>AIMC</i>	Asociación para la Investigación de Medios de Comunicación
<i>APDC</i>	Asociación de Profesores de Derecho Civil
<i>Android</i>	Sistema operativo de <i>Google</i> para teléfonos móviles
<i>AVH</i>	Asistente Virtual de Hogar
<i>AVG</i>	Asistente de Voz de <i>Google</i>
<i>ASR</i>	Automatic Speech Recognition
<i>AVA</i>	Actividad de Voz y Audio
<i>AVV</i>	Asistente Virtual de Voz
<i>BOE</i>	Boletín Oficial del Estado
<i>CENDOJ</i>	Centro de Documentación Judicial
<i>DOCE</i>	Diario Oficial de las Comunidades Europeas
<i>DOUE</i>	Diario Oficial de la Unión Europea
<i>GAFAM</i>	Google-Alphabet, Amazon, Facebook, Apple y Microsoft
<i>GPS</i>	Global Positioning System
<i>GT29</i>	Grupo de Trabajo del artículo 29
<i>HMM</i>	Hidden Markov Models
<i>IA</i>	Inteligencia Artificial
<i>IDC</i>	International Data Corporation
<i>IVR</i>	Interactive Voice Response
<i>IMEI</i>	International Mobile Equipment Identity
<i>IOS</i>	Sistema operativo móvil de Apple
<i>IP</i>	Internet Protocol
<i>LOPDGDD</i>	Ley Orgánica de Protección de Datos Personales y Garantías de los Derechos Digitales.
<i>LORTAD</i>	Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de carácter Personal.
<i>OS</i>	Operating System

<i>PT</i>	Propietario del Terminal
<i>LCEUR</i>	Legislación de las Comunidades Europeas
<i>LOPD</i>	Ley Orgánica de Protección de Datos de carácter personal
<i>LVCRS</i>	Large Vocabulary Continuous Speech Recognition System
<i>RGPD</i>	Reglamento General de Protección de Datos
<i>RCA</i>	Radio Corporation of America
<i>STC</i>	Sentencia del Tribunal Constitucional
<i>STS</i>	Sentencia del Tribunal Supremo
<i>TEDH</i>	Tribunal Europeo de Derechos Humanos
<i>TFM</i>	Trabajo Final de Máster
<i>TIC</i>	Tecnologías de la Información y la Comunicación
<i>Usuario</i>	Operador del sistema
<i>WIFI</i>	Tecnología que permite la interconexión inalámbrica de dispositivos electrónicos

## RESUMEN

Los asistentes virtuales de voz están cada vez más presentes en el campo del uso de los asistentes de hogar y Smartphones, están inmersos en nuestra privacidad e intimidad, sin que podamos percibir su verdadero funcionamiento; más allá de solo facilitarnos ciertas actividades, se esconden riesgos que muchos desconocemos. El presente *TFM* realizó un estudio a nivel jurídico y técnico, comprobando cómo el asistente de voz de *Google* vulnera el consentimiento explícito, la intimidad y privacidad de terceros, al capturar la voz, la cual es un dato biométrico de carácter especial, que permite la identificación plena e inequívoca de cualquier persona.

Mediante pruebas técnicas se determinó cómo el asistente de voz de *Google* graba en diferentes circunstancias a terceros, para luego someter la captura a un tratamiento automatizado no consentido. Si bien, el ámbito jurisprudencial en España parte de la base de que no se requiere consentimiento para grabar a los que intervienen dentro de la misma conversación; se deja claro en esta investigación, que se requiere el consentimiento explícito para el procesamiento automatizado que *Google Inc.* aplica a cada captura de voz de terceros. Por lo anterior estaríamos ante una ilicitud de tratamiento de datos personales.

**PALABRAS CLAVES:** asistente de voz de *Google*, asistente virtual de voz, consentimiento explícito, dato, datos biométricos, intimidad, privacidad.



## **ABSTRACT**

Virtual voice assistants are increasingly present in the field of the use of home helpers and Smartphones, they are immersed in our privacy and intimacy, without us being able to perceive their true functioning; beyond just facilitating certain activities, there are hidden risks that many of us do not know. The present TFM carried out a study at a legal and technical level, verifying how Google's voice assistant violates the explicit consent, privacy and privacy of third parties by capturing the voice, which is a special biometric data that allows the full and unequivocal identification of any person.

Through technical tests, it was determined how Google's voice assistant records third parties in different circumstances, and then subjects the capture to an automated treatment without consent. While the jurisprudential environment in Spain is based on the assumption that no consent is required to record those involved in the same conversation, it is made clear in this investigation that explicit consent is required for automated processing that Google Inc. applies to each third party voice capture. Therefore, we would be faced with an unlawful processing of personal data.

**KEY WORDS:** Google voice assistant, virtual voice assistant, explicit consent, data, biometric data, privacy, privacy.

## INTRODUCCIÓN

Un asistente virtual de voz es un agente de software inteligente, que puede estar presente en *chatbot*, *chatterbot*, *bot* o *robot de charla*<sup>1</sup> que facilita ciertas tareas cotidianas a usuarios que se comunican por medio de la voz, y de esta manera el AVV procesa, interpreta y responde las consultas al interesado. Los AVV han evolucionado al punto de tener conversaciones continuas y fluidas con los usuarios, gracias a la Inteligencia Artificial, y al aprendizaje automático, aplicado a la interacción entre asistente virtual y usuario, por medio del procesamiento del lenguaje natural.<sup>2</sup>

La innovación y practicidad que nos ofrecen los AVV, también conlleva riesgos, debido al uso de la voz como dato elemental para la operación de este tipo de tecnología. Entre los AVV más conocidos, tenemos a: *Alexa*, *Siri*, *M*, *Cortana*, y *Google Assistant*.<sup>3</sup> El presente TFM estudia el AVV *Google Assistant*, y su objetivo es determinar si este puede grabar la voz de terceros, que no han dado el consentimiento explícito para el uso y tratamiento de este dato biométrico de carácter especial; y aun así, la voz puede ser procesada, almacenada y usada para posibles fines de publicidad dirigida al usuario operador del dispositivo.

Esta investigación inicialmente refiere las generalidades de los sistemas de reconocimiento de voz; y asimismo, da a entender cómo opera el AVG Asistente de Voz de *Google*, analizándolo desde el contexto técnico y normativo. Además, explica las nociones del contrato correspondientes a este estudio, detallando lo referente al consentimiento.

---

<sup>1</sup> COBOS TORRES, Juan Carlos. *Integración de un Chatbot como habilidad de un robot social con gestor de diálogos*. Tesis de maestría, Universidad Carlos III de Madrid, Leganés, Madrid, 2013. Agentes Conversacionales o Chatbots. Un agente conversacional es un programa de software que interpreta y responde a las declaraciones realizadas por los usuarios en lenguaje natural corriente. Se integra técnicas de lingüística computacional y la comunicación se puede establecer a través de Internet, mensajes instantáneos, e-mail, foros, etc.

<sup>2</sup> GRONDONA, N.; MAZZA, M.; DORFMAN, P. Asistentes virtuales de clase en la Educación Universitaria. *Una visió crítica: III Congrés Europeu de Tecnologies de la Informació en l'Educació i en la Societat*. 2012. p. 294-296.

<sup>3</sup> ALBERTO GARCÍA. *Google Assistant, Alexa o Siri: ¿cuál es el mejor asistente de voz para tu hogar?* [en línea] [Fecha de consulta: 08 03 2019]. [<https://www.adslzone.net/reportajes/domotica/google-assistant-alexa-siri>]

Este *TFM* se basa en la obtención de resultados por medio de la realización de pruebas técnicas al *AVG*, que comprueben la hipótesis planteada

## **HIPÓTESIS PLANTEADA**

¿Puede el *AVG* grabar y procesar la voz de terceros sin el consentimiento explícito requerido para el tratamiento de datos de especial protección?

## **OBJETIVOS GENERALES**

Determinar si el *AVG* graba y procesa la voz de terceros sin el consentimiento explícito requerido para el tratamiento de datos de especial protección.

Determinar en qué medida esa ausencia de consentimiento vulnera derechos fundamentales, en relación con la recogida y el procesamiento de datos a través del *AVG*.

### **Objetivos específicos**

1. Referir las generalidades de los sistemas de reconocimiento de voz, al igual que el Asistente de voz de *Google* desde el contexto técnico y normativo.
2. Explicar el contrato correspondiente al Asistente de voz de *Google*, detallando lo referente al consentimiento.
3. Demostrar si el Asistente de voz de *Google* graba y procesa la voz de terceros, sin consentimiento para el tratamiento de datos especiales.

## METODOLOGÍA

La metodología empleada para la realización de este trabajo es mixta.

Primero se utilizó la investigación cualitativa, conforme a la técnica de recolección de datos, usando fuentes primarias y secundarias, acorde a la revisión documental, doctrinal, y jurídica, instituida en la observación subjetiva, para describir los componentes de la hipótesis planteada, estableciendo así un análisis perceptivo e interpretativo de la comprensión del presente estudio desde la parte teórica y normativa.

En segundo lugar, se manejó la investigación cuantitativa, al apoyarse en el razonamiento deductivo, ya que el posicionamiento frente al conocimiento de la realidad va conforme al descubrimiento de los fenómenos.

Esta investigación es explicativa, ya que permitió dar a comprender un fenómeno, por qué ocurre y en qué condiciones se da este; teniendo en cuenta la verificación de hipótesis causales; es decir, se fue más allá de la descripción de conceptos, con el fin de dirigirse a responder las causas de los eventos físicos o sociales que componen el estudio.

El diseño es de tipo experimental, ya que se tomó una acción y después se observó las consecuencias de esta, dada la naturaleza de los datos registrados, se concreta en el estudio de los fenómenos basados en una construcción de los hechos, a partir de un modelo de análisis prefijado en la hipótesis a investigar.

El experimento se llevó a cabo por medio de pruebas técnicas, utilizando dispositivos móviles y muestra de personas elegidas de forma aleatoria, involucrando la intencionalidad de la acción para analizar los posibles efectos y resultados, que dieron una respuesta objetiva a la pregunta investigativa, integrando los criterios de fiabilidad, validez y credibilidad.

De igual manera, se obtuvo información directa sobre la percepción medible del público, relativo al planteamiento objeto de estudio, es por esto que se empleó la encuesta como otra técnica de recolección de información, conocida como una de las más difundidas en el campo de las ciencias humanas y sociales, utilizando el instrumento privilegiado del cuestionario

electrónico para este caso, buscando alcanzar la traducción de las variables empíricas por la forma directa de obtención de datos.

## **1. HISTORIA Y EVOLUCIÓN DE LOS SISTEMAS DE RECONOCIMIENTO DE VOZ Y ANÁLISIS DEL ASISTENTE DE VOZ DE GOOGLE**

### **1.1 BREVE HISTORIA DE LOS SISTEMAS DE RECONOCIMIENTO DE VOZ**

Los primeros avances de la tecnología *ASR Automatic Speech Recognition*, fueron en la década de los años 50, “*el reconocimiento de un vocabulario reducido, del orden de 10 palabras, emitidas por un único locutor [...]*”<sup>4</sup> Igualmente, luego de diferentes pruebas, dio pie a que la industria *RCA* ayudara en el campo de la normalización de la voz, en el desarrollo de la técnica *LVCSR Large Vocabulary Continuous Speech Recognition System*, la cual se refiere a la capacidad del reconocimiento continuo de palabras, pudiendo esta técnica reconocer dictados de párrafos completos<sup>5</sup>.

---

<sup>4</sup> RUFINER, Hugo L.; MILONE, Diego H. Sistema de reconocimiento automático del habla. *Ciencia, Docencia y Tecnología*. 2004, vol. 15, no 28, p. 151-177. Breve reseña histórica, Los primeros intentos de desarrollo de sistemas de *ASR* datan de los años 50. Estos primeros trabajos abordaban el reconocimiento de un vocabulario reducido, del orden de 10 palabras, emitidas por un único locutor. La década de los 60 marca el inicio de tres proyectos que han tenido gran repercusión en el área. Estos proyectos fueron desarrollados por Martin (RCA Labs.),

<sup>5</sup> ANTÓN MARTÍN, Javier. *Desarrollo de un sistema de reconocimiento de habla natural independiente del locutor*. Tesis de Licenciatura, Universidad Autónoma de Madrid escuela politécnica superior, Madrid, 2015. Sistema *LVCSR*: Para *LVCSR*, normalmente el vocabulario es elegido con el objetivo de maximizar la cobertura para un tamaño de diccionario dado, pudiendo contener palabras iguales con más de una pronunciación. Además, la generación del diccionario se puede ver influida por aspectos como el tipo de habla, leída o espontánea [7], siendo recomendable tratar esta variabilidad de las pronunciaciones, y así obtener el mayor rendimiento posible al sistema.

El análisis de voz se da a mediados de los años sesenta, considerando el habla como uno de los sistemas biométricos más eficaces, debido a su naturalidad, donde es comprobable que el patrón de voz de una persona es único<sup>6</sup>.

*“El reconocimiento de voz funciona mediante la digitalización de diferentes palabras de una persona. Cada palabra se descompone en segmentos, de los cuales se obtienen 3 o 4 tonos dominantes que son capturados en forma digital y almacenados en una tabla o espectro, que se conoce con el nombre de plantilla de la voz (voice print) [...]”<sup>7</sup>*

### **1.1.2 Cómo operan los sistemas ASR**

Las tres etapas de reconocimiento de voz del sistema ASR, se componen de:

1. *“Procesamiento o análisis del habla (en inglés se conoce como frontend): en esta etapa se realiza algún tipo de análisis de la señal de voz en términos de la evolución temporal de parámetros espectrales (previa conversión analógica/digital de la señal). Esto tiene por función hacer más evidentes las características necesarias para la etapa siguiente y a veces también limpiar y reducir la dimensión de los patrones para facilitar su clasificación [...]”<sup>8</sup>.*
2. *“Clasificación de unidades fonéticas o modelo acústico: esta etapa clasifica o identifica los segmentos de voz ya procesados con símbolos fonéticos (fonemas, dífonos o sílabas). A veces se puede asociar una probabilidad con este símbolo fonético, lo que permite ampliar la información presentada al siguiente módulo [...]”<sup>9</sup>.*
3. *“Análisis en función de reglas del lenguaje o modelo del lenguaje: en esta última etapa se pueden aprovechar las reglas utilizadas en la codificación del mensaje contenido en la señal para mejorar el desempeño del sistema y producir una*

---

<sup>6</sup> CORTÉS OSORIO, JIMY ALEXANDER, MEDINA AGUIRRE, FRANCISCO ALEJANDRO, MURIEL ESCOBAR, JOSÉ A. *Sistemas de seguridad basados en biometría*. [en línea]. Pereira Colombia: vol. XVII, núm. 46, 2010 [Fecha de consulta 8 junio de 2019] Disponible en: <http://www.redalyc.org/articulo.oa?id=84920977016>.

<sup>7</sup> Ibidem

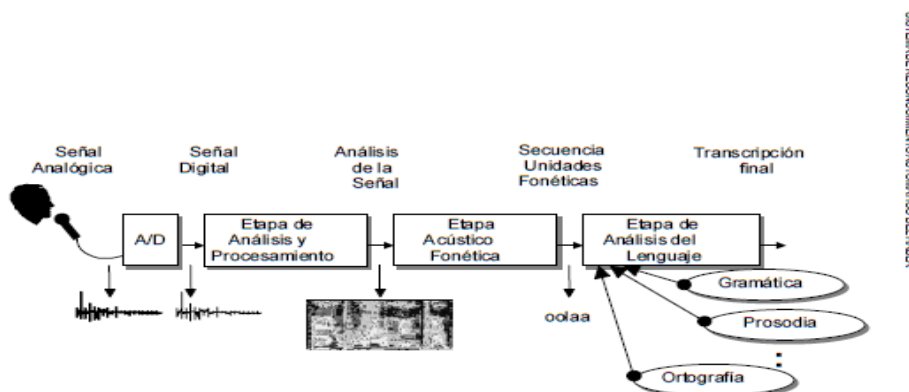
<sup>8</sup> Ibidem

<sup>9</sup> Ibidem.

transcripción adecuada. Aquí se utilizan otras fuentes de conocimiento como la ortográfica, la sintáctica, la prosódica, la semántica o la pragmática [...]”<sup>10</sup>.

Lo anterior puede apreciarse en la siguiente gráfica la cual pertenece al citado autor:

Gráfico 1: Componentes de un sistema de ASR típico.



Fuente: RUFINER Hugo / MILONE Diego, Sistema de reconocimiento automático del habla. 028. Argentina: Ciencia, Docencia y Tecnología, 2004.

En la década de los 60, se dio inicio al campo de la normalización de la voz, mediante proyectos desarrollados por Martin (*RCA Labs.*), en el; Vintsyuck (*URSS*), en métodos de programación dinámica, y Reddy , formalizando los primeros trabajos en reconocimiento de voz continua<sup>11</sup>.

Uno de los avances que ayudó a dar evolución al reconocimiento de voz, fue la técnica denominada *HMM Hidden Markov Models*, a partir de un análisis detallado de la voz, sin importar su interlocutor; es decir, que se apoya en distinguir estadísticamente el

<sup>10</sup>Ibidem.

<sup>11</sup> RUFINER, Hugo L.; MILONE, Diego H. Sistema de reconocimiento automático del habla. *Ciencia, Docencia y Tecnología*. 2004, vol. 15, no 28, p. 151-177.

comportamiento de la voz gracias a factores temporales, permitiendo la reconstrucción de palabras que bajo probabilidad tengan ciertas similitudes.

Definiendo de manera concreta cómo opera el mecanismo de *HMM*, se puede ver que “*Se utilizan secuencias de voz para el entrenamiento y, posteriormente durante reconocimiento, se obtiene la probabilidad de cada modelo (palabra o fonema), seleccionando la de mayor probabilidad[...]*”<sup>12</sup>.

Es importante saber que un *AVV* es un software apoyado por un dispositivo, que ayuda a que la interacción y contacto físico entre hombre y máquina se vea reducida, siendo el asistente de voz el ente incorpóreo digital que facilita ciertas actividades bajo la captura de sonido ambiente, el cual contiene la voz del o los interlocutores, el procesamiento de los datos capturados, el auto aprendizaje de las palabras más usadas por el propietario del terminal *PT*, y con esto pueda generar respuestas a las consultas u órdenes que se le imparten<sup>13</sup>.

Los *AVV* vienen instalados en diferentes dispositivos como: Tablet, teléfonos móviles inteligentes, Smart TV, asistentes de hogar o personales, y en muchos dispositivos que tienen la capacidad de que su sistema operativo y micrófono integrado al dispositivo, puedan incorporar un programa de asistente de voz<sup>14</sup>.

### **1.1.3 Lista de asistentes de voz más usados**

Los asistentes de voz más conocidos se relacionan en la siguiente tabla<sup>15</sup>:

---

<sup>12</sup> SUCAR, Luis Enrique. *Probabilistic graphical models. Advances in Computer Vision and Pattern Recognition*. London: Springer London. 2015, vol. 10, p. 978-1.

<sup>13</sup> GRONDONA, N.; MAZZA, M.; DORFMAN, P. Asistentes virtuales de clase en la Educación Universitaria. *Una visió crítica: III Congrés Europeu de Tecnologies de la Informació i en la Societat*. 2012. p. 294-296.

<sup>14</sup> MEDINA, Javier; CABEZA, Eduardo; PEÑA, Juan Luis Castro. Asistentes virtuales en plataformas 3.0. *IE Comunicaciones: Revista Iberoamericana de Informática Educativa*. 2013, no 18, p. 41-49.

<sup>15</sup> ALBERTO GARCÍA. *Google Assistant, Alexa o Siri: ¿cuál es el mejor asistente de voz para tu hogar?* [en línea] [Fecha de consulta: 08 03 2019]. [<https://www.adslzone.net/reportajes/domotica/google-assistant-alexasiri>]. *Google Assistant* fue uno de los primeros asistentes virtuales, y está presente en todos los móviles *Android* de los últimos dos años y posteriores. Además, contamos con que ya hay más de 10.000 dispositivos que se pueden controlar a través de Google Assistant.



Tabla 1: Lista Asistentes de voz.

FABRICANTE	ASISTENTE DE VOZ
Apple	Siri.
Amazon	Alexa.
Facebook	M.
Google	Google Assistant
Microsoft	Cortana.

Fuente: Elaboración propia a partir de datos de <https://www.adslzone.net/reportajes/domotica/google-assistant-alexa-siri>

Se debe tener en cuenta, que no solo los asistentes de voz se presentan en dispositivos electrónicos, sino que también interactúan en llamadas telefónicas, donde la voz es capturada por medio de preguntas claves que realiza el asistente, con el fin de poder brindar soluciones acordes a las necesidades o consultas generadas.

El asistente de voz en cuestión de análisis en el presente *TFM* es el del fabricante *Google Inc*, donde se encuentra enmarcado los controles de actividad de *Google*, denominado como actividad de voz y audio <sup>16</sup>.

## 1.2 ANÁLISIS DE LA POLÍTICA DE PRIVACIDAD DE *GOOGLE*

Para este análisis se usa la política de privacidad de *Google* del 22 de enero de 2019, la cual para el momento del desarrollo del presente trabajo se encuentra vigente, aclarando que

---

<sup>16</sup> GOOGLE INC, *Gestionar la actividad de voz y audio de Google*. [en línea] [Fecha de consulta: 09 Junio 2019]. [<https://support.google.com/websearch/answer/6030020?co=GENIE.Platform%3DAndroid&hl=es>].

*Google* maneja una política de privacidad general para la mayoría de sus productos; en el caso de políticas de privacidad específicas es de aclarar que no se aplican para la AVA<sup>17</sup>.

Es importante para poder comprender el funcionamiento del AVG, tener presente la política de privacidad que rige este módulo de *Google* de análisis y procesamiento de voz.

Dentro de la política, *Google* es enfático en afirmar que se toma muy en serio el tratamiento, recolección, uso y procesamiento de datos, donde se esfuerzan al máximo para cumplir sus siete principios de privacidad los cuales son<sup>18</sup>:

1. *“Respetar a nuestros usuarios y su privacidad.*
2. *Especificar claramente qué datos recogemos y por qué.*
3. *No vender nunca la información personal de nuestros usuarios.*
4. *Permitir que los usuarios puedan controlar su privacidad con facilidad.*
5. *Dar a los usuarios los medios para que consulten, trasladen o eliminen sus datos.*
6. *Integrar las tecnologías de seguridad más sólidas en nuestros productos.*
7. *Actuar con ejemplaridad para mejorar la seguridad online de todos[...]*<sup>19</sup>.

En el análisis de la política, se busca si existe claridad y legitimidad frente al uso de la voz, en el entendido que esta se considera un dato biométrico, especialmente protegido por el *Reglamento General De Protección De Datos 2016/679*.

---

<sup>17</sup> GOOGLE INC, *POLÍTICA DE PRIVACIDAD DE GOOGLE*. [en línea] [Fecha de consulta: 11 Enero 2019]. [<https://policies.google.com/privacy?hl=es>].

<sup>18</sup> GOOGLE INC. *Centro de Seguridad* [en línea] [Fecha de consulta: 11 Enero 2019]. [<https://safety.google/intl/es/principles/>]. Protegemos la privacidad de cada persona. Es una responsabilidad que adquirimos como creadores de productos y servicios de productos accesibles para todo el mundo. Esto es especialmente importante porque, a medida que avanza la tecnología, la seguridad también debe evolucionar. Tanto nuestro equipo como nuestros procesos y productos se rigen por estos principios para garantizar la privacidad y la seguridad de los datos de nuestros usuarios.

<sup>19</sup> *Ibidem*.

### ***1.2.1 Criterios de la política de privacidad de Google***

Dentro de la política de privacidad de *Google*, encontramos los siguientes criterios<sup>20</sup>:

### ***1.2.2 Objetivo***

Advierte la forma de como recogen los datos, la gestión que le dan y en caso de requerir su exportación o eliminación expone el procedimiento que se debe ejecutar.

### ***1.2.3 Finalidad***

*Google* desarrolla un amplia variedad de productos y servicios, aplicado a diferentes tipos de dispositivos, aclarando que para el acceso de estos, puede hacerse en ciertos productos de modo invitado, es decir no requiere el uso de una cuenta de *Google*, en este caso la información recolectada servirá para sus métricas y análisis sin que se pueda identificar y perfilar el usuario que está haciendo uso de sus servicios o productos, caso contrario cuando el usuario accede bajo una cuenta debidamente registrada en *Google*.

### ***1.2.4 Información que recoge Google***

Se recolecta información básica, sin especificar claramente qué es para *Google* esto, solo dando el ejemplo de que idioma se habla, pero si da el detalle que recolecta información compleja para facilitar “*los anuncios que te resultarán más útiles, las personas que más te interesan online o los vídeos de YouTube que te pueden gustar*”.

Existe otra categoría llamada *identificadores únicos*, donde recogen los siguientes datos: tipo de navegador, tipo de dispositivos de acceso, sistema operativo, tipo de operador de internet,

---

<sup>20</sup> GOOGLE INC. *Política de privacidad de Google* [en línea] [Fecha de consulta: 11 Enero 2019]. [<https://policies.google.com/privacy?hl=es>].

número de teléfono móvil, versión de la aplicación, dirección IP, fecha, hora y las páginas web visitadas.

La actividad es otra categoría, donde *Google* enumera de donde obtiene toda la información que usan para su respectivo análisis:

- *“Los términos que buscas.*
- *Los vídeos que ves.*
- *Las visualizaciones y las interacciones con el contenido y los anuncios.*
- *Información sobre voz y audio cuando utilizas funciones de audio.*
- *Actividad de compra.*
- *Usuarios con los que te comunicas o compartes contenido.*
- *Actividad en sitios web y aplicaciones de terceros que utilizan nuestros servicios.*
- *Historial de navegación de Chrome que has sincronizado con tu cuenta de Google[...]*”<sup>21</sup>

Otra categoría es “La información de tu ubicación”, donde el uso que se da es para indicar destinos, promociones cercanas u horarios de películas de cines aledaños entre otros.

*Google* enumera las diferentes fuentes de donde obtiene todos los elementos que ayuda a precisar los niveles de ubicación de sus usuarios:

- *“GPS*
- *Dirección IP*
- *Datos del sensor de tu dispositivo*
- *Información sobre elementos cercanos a tu dispositivo como, por ejemplo, puntos de acceso Wi-Fi, antenas de servicio de telefonía móvil y dispositivos con el Bluetooth activado[...]*”<sup>22</sup>.

---

<sup>21</sup> Ibidem.

<sup>22</sup> Ibidem.

### **1.2.5 ¿Por qué y para qué recoge Google estos datos?**

Debido que la mayoría de los servicios son gratuitos, especifica que requiere los datos recolectados para poder financiarse a través de venta de servicios dirigidos a compañías o público en general, aclarando que no comparte información sensible con el ánimo que se ofrezca publicidad dirigida a “*la raza, la orientación sexual o la salud*”. Igualmente, los datos recolectados ayudan a *Google* a mejorar sus servicios y productos, optimizando su productividad, rendimiento y acceso. Los nuevos productos y servicios de *Google* se basan en el análisis y comportamiento de sus usuarios, pudiendo así generar aplicaciones que suplen necesidades específicas en el mercado.

### **1.2.6 Controles de privacidad**

*Google* da la posibilidad de gestionar, revisar y actualizar la información sobre la privacidad de sus productos, teniendo en cuenta que muchos de estos servicios están activos por defecto.

Se enumeran los controles a los cuales el usuario tiene acceso:

- “*Controles de actividad.*”
- *Configuración de anuncios.*
- *Sobre ti.*
- *Recomendaciones compartidas.*
- *Datos compartidos por ti[...]*<sup>23</sup>.

Igualmente se da la forma de actualizar información personal mediante los siguientes controles:

- “*Mi actividad.*”
- *Panel de control de Google.*

---

<sup>23</sup> Ibidem.

- *Tu información personal[...]*”.

### **1.2.7 Compartir información**

El primer evento es cuando el usuario comparte información por medio de cualquier producto o servicio de *Google*, sea que comparta en modo oculto, privado o público.

El segundo evento es cuando *Google* considera que debe entregar información que posee sobre sus usuarios en los siguientes eventos:

- Cuando se usa la cuenta de *Google* corporativas o académicas, se tiene acceso por el administrador de dominio a los datos almacenados en cualquier cuenta.
- Por motivos legales.

### **1.2.8 Proteger información**

Cuenta *Google* con herramientas y técnicas que incluye:

- *“Cifrado de datos.*
- *Navegación segura.*
- *Verificación en dos pasos.*
- *Restricción de acceso a usuarios no autorizados.*
- *Revisión de la práctica de recogida de datos, con el fin de garantizar un acceso no autorizado físico o lógico a los datos[...]*”<sup>24</sup>.

---

<sup>24</sup> Ibidem.

### **1.2.9 Exportar y eliminar tu información**

Se tiene la opción de exportar, retirar y eliminar la información que *Google* ha recolectado de los usuarios.

### **1.2.10 Cumplimiento y cooperación con autoridades reguladoras**

*Google* hace una revisión periódica de la política de privacidad en aras de actualizarla en los siguientes temas:

- Transferencia de datos bajo los marcos de Privacy Shield UE - EE. UU., Suiza - EE. UU y Protección de Datos EU.
- Requisitos exigidos por Europa para poder operar en el territorio.

Dentro del análisis de los términos y condiciones de *Google*, puede inferirse el reconocimiento de “*información sobre voz y audio cuando utilizas funciones de audio[...]*”<sup>25</sup> la cual es recolectada para su respectiva analítica, con el fin de que “*los anuncios que te resultarán más útiles, las personas que más te interesan online o los vídeos de YouTube que te pueden gustar[...]*”<sup>26</sup>. Sumado a identificadores únicos como la *IP*, el dispositivo móvil, S.O usado y anudado a las preferencias específicas de este dispositivo como *IMEI*, numero móvil y otros datos como: Datos de tráfico, navegación, la ubicación brindada por el *GPS* y toda la información generada por cada uno de los sensores de nuestros teléfonos inteligentes. Se puede colegir que cada conversación capturada, procesada, guardada y perfilada por el *AVG* para ser llevada al *AVV*, se reviste de características que perfilan cada audio en un auténtico metadato<sup>27</sup> enriquecido de información personal e inequívoca de cada *PT*.

---

<sup>25</sup> Ibidem.

<sup>26</sup> Ibidem.

<sup>27</sup> SENSO, José A.; DE LA ROSA PIÑERO, Antonio. El concepto de metadato. Algo más que descripción de recursos electrónicos. *Ciência da Informação*. 2003, vol. 32, no 2. La primera acepción que se le dio (y actualmente la más extendida) fue la de dato sobre el dato, ya que proporcionaban la información mínima necesaria para identificar un recurso. En este mismo trabajo se afirma que puede incluir información descriptiva

En el presente trabajo de investigación se estudiará por medio de pruebas técnicas, la frecuencia y facilidad con que el AVG puede grabar voces de terceros ajenos a los terminales de prueba que se usaran en cada uno de los experimentos.

### **1.3 MI ACTIVIDAD DE GOOGLE.**

Es el espacio donde *Google Inc*, registra todos los datos que el *PT* genera, para luego ser registrados, procesados, perfilados y almacenados. Estos se centralizan en los servidores de *Google*, los cuales se encargan de ofrecer el contenido referente a la actividad, dirigido únicamente al *PT* debidamente registrado<sup>28</sup>.

Como se pudo evidenciar en la política de privacidad de *Google*, cada uno de los datos son usados para ofrecer mejores servicios, además de publicidad dirigida, basada en el perfilamiento de los datos entregados.

Dentro de *Mi Actividad de Google* podemos ver las siguientes opciones:

- *“Controles de actividad de Google*
- *Controlar qué actividad se guarda en la cuenta*
- *Gestionar el ajuste Información del dispositivo*
- *Ver y controlar la actividad de la cuenta*
- *Eliminar la actividad*
- *Gestionar la actividad de voz y audio de Google*
- *Controlar lo que otros usuarios ven sobre ti en los servicios de Google*
- *Compartir información de uso y diagnósticos con Google*
- *Ver y controlar los datos de Actividad en la Web y en Aplicaciones[...]*<sup>29</sup>

---

sobre el contexto, calidad y condición o características del dato. La evolución del término desde esta fecha hasta 1997 ha sido descrita por Lange y Winkler (1997) revelando que no existen demasiadas novedades.

<sup>28</sup> GOOGLE INC, *Ver y controlar la actividad de la cuenta*. [en línea] [Fecha de consulta: 09 Mayo 2019]. [<https://support.google.com/accounts/answer/7028918?co=GENIE.Platform%3DDesktop&hl=es>]

<sup>29</sup> Ibidem.



Es por ello que dentro del análisis del presente *TFM*, nos enfocaremos en el control de actividad de audio y voz *AVV* de *Google*.

### ***1.3.1 Módulo de actividad de voz y audio de Google***

Según *Google*, el módulo de actividad de voz o en siglas *AVA* está orientado a que registra las entradas de voz y audio en los servicios de *Google*, para mejorar el reconocimiento de voz; por ejemplo, cuando se dice "Ok *Google*" para hablarle y activar el *AVV*.

Asimismo, el *AVA* se activa de forma predeterminada, cuando utilizamos el *AVG*, este asistente viene instalado de fábrica en todos los dispositivos bajo el sistema operativo *Android*<sup>30</sup>, al iniciar el reconocimiento de voz del *PT*, se debe realizar una fase de aprendizaje donde solicita que se repita seis veces la palabra *Ok Google*, hasta que el asistente reconozca la voz de quien indicará las órdenes. La función *Voice Match*<sup>31</sup> desde ese momento queda activa, generando un vínculo entre el *AVG* y el *PT*, implementando como identificador único el reconocimiento de voz.

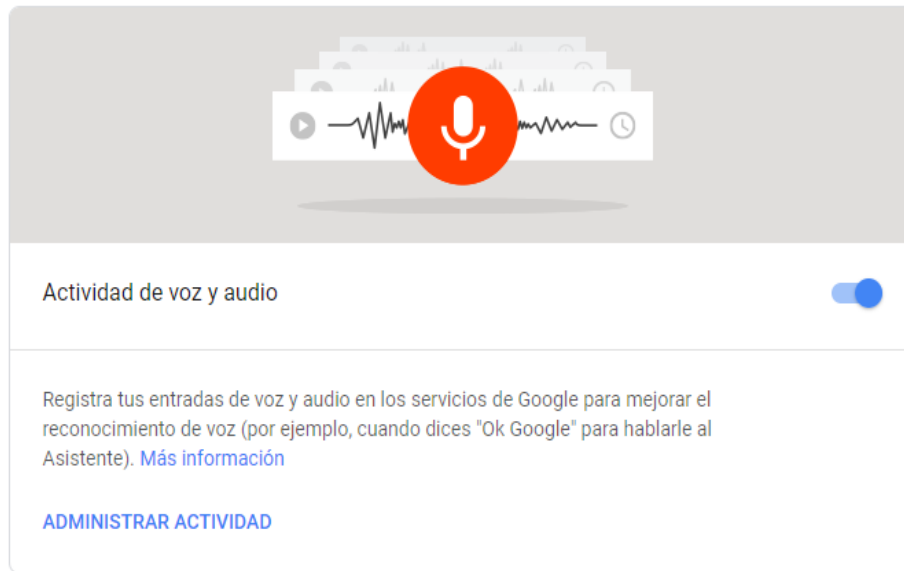
---

<sup>30</sup> BASTERRA, BERTEA, BORELLO, CASTILLO Y VENTURI. *Android OS Documentation Release 0.1* [en línea] [Fecha de consulta: 09 Mayo 2019]. [<https://buildmedia.readthedocs.org/media/pdf/androidos/latest/androidos.pdf#page=7&zoom=100,0,432>].

*Android* es un sistema operativo móvil desarrollado por Google; es uno de los más conocidos junto con iOS de Apple. Está basado en Linux, que junto con aplicaciones middleware está enfocado para ser utilizado en dispositivos móviles como teléfonos inteligentes, tablets, Google TV y otros dispositivos.

<sup>31</sup> *GOOGLE INC*, *Configuración de Voice Match*, [en línea] [Fecha de consulta: 09 Mayo 2019]. [<https://myactivity.google.com/>]. *Voice Match* permite que tu Asistente te distinga de otras personas. Para ello, crea modelos únicos de tu voz que se almacenan sólo en los dispositivos que habilites. Inicialmente, los modelos se crean con la información de inscripción que brindaste al activar *Voice Match*.

Gráfico 2: Actividad de voz y audio, captura de pantalla de Google.



Fuente: copiada de:

<https://support.google.com/websearch/answer/6030020?co=GENIE.Platform%3DDesktop&hl=es>

### 1.3.2 Cómo opera el asistente de voz de Google

Tabla 2: Cómo opera el asistente de voz de Google

<b>ASISTENTE DE VOZ GOOGLE</b>
<b>FUNCIONAMIENTO</b>
Mediante la captura de sonido ambiente de forma continua, realiza el envío de estas capturas a Internet, donde <i>Google</i> ejecuta el análisis y procesamiento bajo inteligencia artificial “IA” <sup>32</sup> que permite identificar la voz del interlocutor y cuando este diga de “OK <i>Google</i> ” proceda el asistente de voz a operar.

<sup>32</sup> HARDY, Thomas. IA (Inteligencia Artificial). Polís: Revista Latinoamericana. 2001, no 2, p. 18. La inteligencia artificial (IA) tiene por objetivo el estudio y el análisis del comportamiento humano en los ámbitos de la comprensión, de la percepción, de la resolución de problemas y de la toma de decisiones con el fin de poder reproducirlos con la ayuda de un computador. De esta manera, las aplicaciones de la IA se sitúan principalmente en la simulación de actividades intelectuales del hombre. Es decir, imitar por medio de máquinas, normalmente electrónicas, tantas actividades mentales como sea posible, y quizás llegar a mejorar las capacidades humanas en estos aspectos.

<b>MODO DE FUNCIONAMIENTO</b>	
<b>ACTIVO</b>	<b>PASIVO</b>
En ciertos modelos de dispositivos, es posible la operación del AVG así el teléfono esté bloqueado, con el comando de voz "Ok Google", procede a desbloquear el dispositivo, y en este caso el asistente de voz inicia su ejecución.	En el momento que el dispositivo no está bloqueado, entra en modo de escucha de sonido ambiente, a la espera de que por medio del comando de voz "Ok Google" se active el AVG.
<b>REQUERIMIENTOS</b>	
<ul style="list-style-type: none"> <li>● Se debe tener una cuenta de <i>Google</i>, en caso de que sea una cuenta de <i>Google</i> corporativa, académica o de investigación, debe contar con permiso del administrador para usar los servicios AVA de <i>Google</i>.</li> <li>● Conexión continua a internet con el fin de que <i>Google</i> en sus servidores pueda procesar y almacenar todas las consultas realizadas a su asistente. Sin internet no operan las consultas realizadas al AVG.</li> </ul>	
<b>FINALIDAD</b>	
El sonido ambiente es procesado de manera continua sea de modo pasivo o activo y enviado a internet, al momento de decir por medio de voz "OK Google" el asistente se activa esperando que orden recibir. Todas y cada una de las búsquedas realizadas por el AVG quedan almacenadas en la actividad de voz de <i>Google</i> . Tal como se menciona en la política de privacidad, los datos recolectados serán usados con fines de publicidad dirigida <sup>33</sup> .	

Fuente: Propia

*Google* indica dentro de las ayudas de AVA que el asistente de voz opera o se activa al momento de decir "Ok Google" o presionar el icono del micrófono, pero indica qué contenido guarda en sus servidores "Google graba tu voz y otros audios, además de algunos segundos anteriores, cuando usas activaciones de audio [...]"<sup>34</sup>.

<sup>33</sup> SENDPULSE. *Que es Publicidad dirigida* [en línea] [Fecha de consulta: 09 Mayo 2019]. [https://sendpulse.com/latam/support/glossary/targeting]. La Publicidad dirigida es un mecanismo de publicidad que permite separar a los visitantes objetivo del público en general, pues cumplen con criterios establecidos. Este es el método principal para aumentar la efectividad de la campaña publicitaria, cuyo uso es un elemento irremplazable de la promoción de cualquier bien o servicio en Internet. Permite mostrar los anuncios publicitarios de acuerdo a los intereses de los usuarios.

<sup>34</sup> GOOGLE INC, *Cómo administrar la Actividad de voz y audio en Google*. [en línea] [Fecha de consulta: 09 Junio 2019]. [https://support.google.com/websearch/answer/6030020?co=GENIE.Platform%3DDesktop&hl=es-419].

## 2. DERECHO A LA INTIMIDAD, PROPIA IMAGEN, SECRETO DE LAS COMUNICACIONES, Y PROTECCIÓN DE DATOS, EN EL ÁMBITO DE GRABACIONES DE VOZ

### 2.1 DERECHO A LA INTIMIDAD

La intimidad personal parte del respeto hacia el otro, teniendo en cuenta que desde circunstancias abusivas y perturbadoras se impide el libre desarrollo de la personalidad, esto se conoce como violación a la intimidad. El respeto a la vida privada personal y familiar, se constituye de esta forma un valor que toda sociedad debe acatar<sup>35</sup>.

La Declaración Universal de los Derechos Humanos de 1948, reconoce en su artículo 12 que *“nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia ni de ataques a su honra o a su reputación y que toda persona tiene derecho a la protección de la ley contra esas injerencias o ataques[...]*”<sup>36</sup>.

El Convenio Europeo de Derechos Humanos en su artículo 8 el cual se titula Derecho al respeto a la vida privada y familiar señala en su artículo 1: *“Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia[...]*”<sup>37</sup>.

En el texto constitucional, puede verse reconocido el derecho a la intimidad en el artículo 18.1 que establece *“Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen[...]*”<sup>38</sup>. La carta superior reconoce no sólo al individuo aisladamente considerado en su intimidad, también protege su núcleo familiar.

El derecho a la intimidad se encuentra dentro la esfera más reservada de cualquier individuo, se reconoce este derecho en Sentencia 151 de 1997 donde se indica que *“En este sentido,*

---

<sup>35</sup> HERRÁN ORTIZ, Ana Isabel.. *El derecho a la intimidad en la nueva Ley Orgánica de Protección de Datos Personales*. Edición desconocida. Madrid: Dykinson, 2002.

<sup>36</sup> *La Declaración Universal de Derechos Humanos*. (BOE núm. 243, de 10 de octubre de 1979).

<sup>37</sup> *Convención Europea De Derechos Humanos*. Convenio Europeo de Derechos Humanos. Tribunal Europeo de Derechos Humanos. (BOE núm. 243, de 10 de octubre de 1979).

<sup>38</sup> *Constitución Española*. (BOE núm. 311, de 29 de diciembre de 1978).

*basta recordar nuestras afirmaciones relativas a que el derecho a la intimidad limita la intervención de otras personas y de los poderes públicos en la vida privada[...]*<sup>39</sup>.

Este derecho es reconocido incluso a personas expuestas al público, tal como lo enuncia la Sentencia 134 de 1999<sup>40</sup>, la cual indica que “*el derecho a la intimidad personal y familiar del art. 18.1 C.E, actúa como límite frente al derecho a comunicar libremente información, garantizando un ámbito vedado al conocimiento de terceros, constituyendo ese reducto el contenido esencial del mencionado art. 18, que debe preservarse mediante el reconocimiento de los oportunos mecanismos de garantía frente a una publicidad no deseada, innecesaria e imprevista[...]*”.

Igualmente en la misma Sentencia, puede verse cómo el Tribunal Constitucional pondera de la siguiente manera el derecho de intimidad de una persona pública y el derecho a la información de interés general: “*El elemento decisivo para determinar si ha habido o no una intromisión ilegítima en la intimidad de las figuras o personajes públicos es el dato objetivo de la relevancia pública de lo divulgado, así como que su relevancia esté justificada en función del interés público del asunto sobre el que se informa o del interés legítimo del público en su conocimiento[...]*”<sup>41</sup>.

El análisis legislativo muestra cómo la Ley orgánica 1 de 1982 la cual enuncia el ámbito de protección civil que goza el derecho a la intimidad, tal como se expone en su artículo 1,1: “*El derecho fundamental al honor, a la intimidad personal y familiar y a la propia imagen, garantizado en el artículo dieciocho de la Constitución, será protegido civilmente frente a todo género de intromisiones ilegítimas, de acuerdo con lo establecido en la presente Ley Orgánica[...]*”<sup>42</sup>.

---

<sup>39</sup>Sentencia 151 de 1997, De 29 De septiembre. (BOE núm. 260, de 30 de octubre de 1997).

<sup>40</sup>Sentencia 134 de 1999, de 15 de julio de 1999. (BOE núm. 197, de 18 de agosto de 1999).

<sup>41</sup> Ibidem.

<sup>42</sup> Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. (BOE núm. 115, de 14 de mayo de 1982).

La intimidad como derecho fundamental, puede definir a quien incluir o excluir sobre la vida privada de cada persona. Este derecho protege la vida privada y evita que situaciones externas afecten áreas reservadas para el libre desarrollo de cada persona<sup>43</sup>.

En cuanto a la intimidad frente al titular del teléfono del *PT* y los terceros intervinientes debe comprender, que estos terceros pueden derivarse de una conversación o interacción espontánea entre todos y cada uno de los presentes; por esto se debe analizar el derecho a la intimidad desde la esfera de cada uno de los partícipes.

El objeto del presente estudio supone la vulneración del derecho Constitucional a la intimidad, consecuente a la grabación de la voz como dato especial por parte del *AVG*, sin el consentimiento de terceros, donde presuntamente el asistente virtual interfiere en conversaciones privadas, capturando otras voces diferentes a las del *PT* y usándolas para otros fines que no fueron consentidos explícitamente<sup>44</sup>.

La respuesta a la hipótesis planteada en el presente *TFM*, debe develarse en la investigación donde las pruebas técnicas demostraran si en principio el *AVG* graba a terceros sin su consentimiento, y, por ende, las voces grabadas son tratadas mediante un procesamiento automático por parte de *Google*.

## **2.2 DERECHO A LA PROPIA IMAGEN**

El *Tribunal Constitucional* en el análisis de diferentes Sentencias, incluye los atributos más característicos del individuo como es el nombre, imagen física, y la voz. En la Sentencia 23 de 2010, referente a un caso de manipulación de imagen destaca lo siguiente<sup>45</sup>:

*“Mediante la garantía del ámbito de libertad «respecto de sus atributos más característicos, propios e inmediatos como son la imagen física, la voz o el nombre, cualidades definitorias del ser propio y atribuidas como posesión inherente e irreductible a toda persona»*

---

<sup>43</sup> BARRAGÁN, María Luisa. *Los derechos al honor, a la intimidad personal y familiar y a la propia imagen del menor*. 1ª edición. Anuario de justicia de menores, 2015, no 15, p. 702-703

<sup>44</sup> TELEFÓNICA, Fundación. *Sociedad Digital en España 2018*. Primera edición. Madrid: Fundación Telefónica, 2019. .

<sup>45</sup> *Sentencia 23 de 2010, de 27 de abril de 2010*. (BOE núm. 129, de 27 de mayo de 2010).

*Por ello el ámbito propio de protección del derecho a la propia imagen es la defensa frente a los usos no consentidos de la representación pública de la persona que no encuentren amparo en ningún otro derecho fundamental, muy destacadamente frente a la utilización de la imagen con fines puramente lucrativos a la que alude el art. 7. 6 de la Ley Orgánica 1 de 1982 de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen[...]*<sup>46</sup>.

Es importante destacar, como lo dice el párrafo anterior, lo contenido en la Ley Orgánica 1 de 1982, en el capítulo II denominado, *De la protección civil del honor, de la intimidad y de la propia imagen*, en el artículo 7 dicta lo siguiente en los siguientes numerales:

*“Tendrán la consideración de intromisiones ilegítimas en el ámbito de protección delimitado por el artículo segundo de esta Ley:*

*Uno. El emplazamiento en cualquier lugar de aparatos de escucha, de filmación, de dispositivos ópticos o de cualquier otro medio apto para grabar o reproducir la vida íntima de las personas.*

*Dos. La utilización de aparatos de escucha, dispositivos ópticos, o de cualquier otro medio para el conocimiento de la vida íntima de las personas o de manifestaciones o cartas privadas no destinadas a quien haga uso de tales medios, así como su grabación, registro o reproducción*

*Seis. La utilización del nombre, de la voz o de la imagen de una persona para fines publicitarios, comerciales o de naturaleza análoga[...]*<sup>47</sup>.

Los términos y condiciones de *Google* afirman que el consentimiento del *PT* autoriza fines de publicidad, mediante el tratamiento automatizado de la voz como dato, para indicar las preferencias y aficiones del usuario, basados en la analítica de datos realizada por *Google Inc.*

---

<sup>46</sup> Ibidem.

<sup>47</sup> Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. (BOE núm. 115, de 14 de mayo de 1982).

Se estaría en una presunta intromisión ilegítima del derecho a la propia imagen, en el caso, del posible uso de la voz de terceros sin el consentimiento explícito de estos, para el tratamiento de este dato especial con posibles fines publicitarios.

El uso del AVG como instrumento para captar conversaciones se debe examinar desde el punto de si la grabación realizada, se ajusta a los parámetros emitidos por la jurisprudencia, los cuales analizaremos más adelante.

### **2.3 DERECHO AL SECRETO EN LAS COMUNICACIONES**

El planteamiento subyace frente a lo dispuesto en el presente *TFM*, si las conversaciones que se derivan entre el *PT* y terceros pueden o deben revestirse del secreto de las comunicaciones, tal y como se considera en el artículo 18.3 de la Constitución de España que reza:

*“Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial[...]”*<sup>48</sup>.

El secreto de las comunicaciones es un derecho que protege la privacidad y seguridad sobre todas las redes de comunicaciones disponibles al público. Esta obligación se refleja en el capítulo III artículo 39.1 de la Ley 9 de 2014 General de Telecomunicaciones, reza: *“Los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público deberán garantizar el secreto de las comunicaciones de conformidad con los artículos 18.3 y 55.2 de la Constitución, debiendo adoptar las medidas técnicas necesarias[...]*”<sup>49</sup>

Acudiendo al artículo 10.2 de la Constitución de España, dice: *“Las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán de conformidad con la Declaración Universal de Derechos Humanos y los tratados y acuerdos internacionales sobre las mismas materias ratificados por España[...]*”<sup>50</sup>.

---

<sup>48</sup> *Constitución Española*. (BOE núm. 311, de 29 de diciembre de 1978).

<sup>49</sup> *Ley 9/2014*, de 9 de mayo, general de telecomunicaciones. (BOE núm. 114, de 10 de mayo de 2014).

<sup>50</sup> *Constitución Española*. (BOE núm. 311, de 29 de diciembre de 1978).



Es por ello por lo que la construcción del derecho al secreto de las comunicaciones procede de tres tratados internacionales suscritos por España<sup>51</sup>. La Declaración Universal de Derechos Humanos en el artículo 12 dice que “*nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques[...]*”<sup>52</sup>.

El Convenio Europeo de Derechos Humanos dice en el artículo 8.1 que: “*Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia[...]*”<sup>53</sup>.

Por su parte, el Pacto Internacional de Derechos Civiles y Políticos de 1966, en el artículo 17.1 señala que: “*nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia[...]*”<sup>54</sup>.

El individuo que elige su propia forma de vida basa sus gustos y preferencias bajo la mayor libertad que se pueda, evitando que alguien interfiera en su proyecto sin su consentimiento, y no desea que el Estado ni su Administración le indiquen qué debe hacer en su día a día. Es cunado surge la garantía de la no injerencia, ataques y vigilancias no autorizadas a la intimidad y privacidad de cualquier persona<sup>55</sup>.

Se diría entonces, que el derecho al secreto de las comunicaciones permite que cualquier persona pueda comunicarse con otra por medio de comunicación cerrada, sin que sea conocido el contenido por terceros ajenos a esta. Este derecho tiene en sí carácter formal, debido a que está inmerso en todo el envío y recepción de mensajes, sin importar el contenido

---

<sup>51</sup> RON ROMERO, José. Derecho al secreto de las comunicaciones telefónicas, un reto para la buena administración. *Anuario da Faculta de Dereito da Universidade da Coruña*. 2011, no 15, p. 103-128

<sup>52</sup> *La Declaración Universal de Derechos Humanos*. (BOE núm. 243, de 10 de octubre de 1979).

<sup>53</sup> *Convención Europea De Derechos Humanos*. Convenio Europeo de Derechos Humanos. Tribunal Europeo de Derechos Humanos. (BOE núm. 243, de 10 de octubre de 1979).

<sup>54</sup> *Instrumento de ratificación de España del pacto Internacional de Derechos Civiles y Políticos*, hecho en Nueva York el 19 de diciembre de 1966. (BOE núm. 103, de 30 de abril de 1977).

<sup>55</sup> RON ROMERO, José. Derecho al secreto de las comunicaciones telefónicas, un reto para la buena administración. *Anuario da Faculta de Dereito da Universidade da Coruña*. 2011, no 15, p. 103-128.

que se esté transmitiendo, pero se destaca que no es un derecho absoluto, puede verse limitado por orden judicial motivada<sup>56</sup>.

La interacción entre *PT* y terceros frente al derecho de secreto de las comunicaciones, estaría plasmado en el momento que dichas captaciones de voz solo tendrían acceso para el interesado, en este caso, el *PT*, quien es el único facultado para almacenar, reproducir y disponer de cada dato procesado en *Mi actividad de Google*; pero, el interrogante que se genera es, si el tercero a quien le fue captada su voz sin su consentimiento estaría en desventaja frente al *PT*, debido que no tiene acceso a la información que le compete, y se encuentra almacenada en servidores de *Google Inc.*

## **2.4 DERECHO DE PROTECCIÓN DE DATOS**

En el análisis de los términos y condiciones de *Google*, el tratamiento realizado a los datos que se recolectan por diferentes fuentes; por ejemplo, por medio del *AVG*, sirve como insumo para la creación de perfiles específicos de cada usuario. Podemos ver implícito el derecho a la protección de datos en cada una de las acciones de recolección, procesamiento, tratamiento, transferencia y destino que da la compañía a nuestros datos personales.

De este modo, se dará a conocer la protección de datos desde el contexto jurídico comprendido como un derecho autónomo, el cual tiene rango y protección Constitucional. *La Constitución de España* promulgada en 1978<sup>57</sup>, está catalogada como una de las más vanguardistas en referencia de introducción a la protección de datos, frente al uso informático. Se plantea que el constituyente tomo el ejemplo de la constitución portuguesa de 1976 en su artículo 35 el cual se titula *utilización informática* reza lo siguiente<sup>58</sup>:

---

<sup>56</sup> CASANOVA MARTÍ, Roser; PICÓ I JUNOY, Joan. *Las intervenciones telefónicas en el proceso penal*. Edición desconocida. Barcelona: José María Bosch, 2014.

<sup>57</sup> *Constitución Española*. (BOE núm. 311, de 29 de diciembre de 1978).

<sup>58</sup> *Constitución De La Republica Portuguesa de 2 de abril de 1976..*

1. “Todos los ciudadanos tendrán derecho a tomar conocimiento de lo que conste en forma de registros mecanográficos acerca de ellos y de la finalidad a que se destinan las informaciones y podrán exigir la rectificación de los datos, así como su actualización[...]”<sup>59</sup>.

2. “No se podrá utilizar la informática para el tratamiento de datos referentes a convicciones políticas, fe religiosa o vida privada, salvo cuando se trate de la elaboración de datos no identificables para fines estadísticos[...]”<sup>60</sup>.

Ahora bien, en la Constitución española se desarrolla en el apartado 4, del artículo 18, donde dice que “La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos”<sup>61</sup>.

En primer lugar, se consideró el derecho a la protección de datos como una vertiente del derecho a la intimidad, pero el desarrollo jurisprudencial que interpeló el Tribunal Constitucional demostró que se trata de un derecho independiente, a pesar de que pueda verse en muchos casos relacionados entre sí<sup>62</sup>.

*El convenio 108 del Consejo de Europa del año 1981*, relativo a la protección de las personas referente al *tratamiento automatizado de datos de carácter personal* el cual fue ratificado por España el 27 de enero de 1984. En el ámbito, objeto de la presente ley en su artículo 1 dice: “El fin del presente Convenio es garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al *tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona (“protección de datos”)* [...]”<sup>63</sup>.

La Sentencia 94 de 1998<sup>64</sup>, define como el derecho fundamental a la protección de datos, debe garantizar a toda persona el control de sus datos, el destino y el uso que se les dé. Todo

---

<sup>59</sup> Ibidem.

<sup>60</sup> Ibidem.

<sup>61</sup> *Constitución Española*. (BOE núm. 311, de 29 de diciembre de 1978).

<sup>62</sup> JIMÉNEZ, Cinta CASTILLO. Protección del derecho a la intimidad y uso de las nuevas tecnologías de la información. [en línea]. [Fecha de consulta: 13 Mayo 2019]. [http://rabida.uhu.es/dspace/bitstream/handle/10272/1565/b1205654.pdf].

<sup>63</sup> *Convenio 108 del Consejo de Europa*, de 28-1-1981, para la protección de las personas con respecto al *tratamiento automatizado de datos de carácter personal*. (BOE núm. 274, de 15 de noviembre de 1985).

<sup>64</sup> *Sentencia 94 de 1998*, de 4 de mayo. (BOE núm. 137, de 9 de junio de 1998).

con el fin de evitar un tráfico o transferencia ilícita donde pueda ocasionarse un daño lesivo que menoscabe la dignidad y los derechos de las personas afectadas.

El desarrollo constitucional de España en el artículo 18.4<sup>65</sup>, se puede ver reflejado en la *Ley Orgánica 5 de 1992 referente a la regulación del tratamiento automatizado de los datos de carácter personal*, denominada *LORTAD*, la cual a pesar de estar derogada, en su ámbito de aplicación contenía en el artículo 2.1: “*La presente Ley será de aplicación a los datos de carácter personal que figuren en ficheros automatizados de los sectores público y privado y a toda modalidad de uso posterior, incluso no automatizado, de datos de carácter personal registrados en soporte físico susceptible de tratamiento automatizado[...]*”<sup>66</sup>.

La *Directiva 95/46/CE* del Parlamento Europeo y del Consejo, de 24 de octubre de 1995<sup>67</sup>, respectiva a la protección de las personas físicas, en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, da lugar a que se redacte una nueva normativa en España, la cual fue la *Ley Orgánica 15 de 1999* referente a la protección de datos<sup>68</sup>. Gracias a la misma Ley Orgánica, se crea la Agencia de protección de datos, con el fin de velar el cumplimiento y registro de todos los ficheros público y privados que contenían datos personales y el establecimiento de un régimen sancionatorio.

El *Reglamento 2016/679 del Parlamento Europeo y del Consejo, 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*<sup>69</sup>, deroga la *Directiva 95/46/CE*<sup>70</sup>, dando nacimiento a la Ley Orgánica 3 de 2018, la cual se denomina *Protección de Datos Personales y garantía de los*

---

<sup>65</sup> *Constitución Española*. (BOE núm. 311, de 29 de diciembre de 1978).

<sup>66</sup> *Ley Orgánica 5/1992*, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. (BOE núm. 262, de 31 de octubre de 1992).

<sup>67</sup> *Directiva 95/46/CE del Parlamento Europeo y del Consejo*, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos. (DOCE núm. 281, de 23 de noviembre de 1995).

<sup>68</sup> *Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal*. (BOE núm. 298, de 14 de diciembre de 1999).

<sup>69</sup> *Reglamento 2016/679 del Parlamento Europeo y del Consejo, 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*. (DOUE L 119/1).

<sup>70</sup> *Directiva 95/46/CE del Parlamento Europeo y del Consejo*, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos. (DOCE núm. 281, de 23 de noviembre de 1995).

*derechos digitales* en su sigla *LOPDGDD*<sup>71</sup>. derogando la Ley *Orgánica 15 de 1999* referente a la protección de datos.

Teniendo en cuenta lo concerniente a la protección de datos, en hipótesis existe una vulneración a este derecho por el uso indebido del *AVG*, respecto de si un tercero es grabado sin su consentimiento, y es sometido este dato especial a un tratamiento automatizado por parte de la *AVA*. Estaríamos entonces frente a una ilicitud en el tratamiento de datos.

Es por ello que el tratamiento y procesamiento automatizado, se basa en principio al *PT*, en el estudio del *TFM*, encontramos a un tercero que no es interesado, y que no ha dado su consentimiento para el manejo de las políticas de privacidad del *AVG*.

## **2.5 DATOS BIOMÉTRICOS ESPECIALMENTE PROTEGIDOS**

El artículo 9 del *RGPD*, establece en el tratamiento de categorías especiales de datos personales, apartado 1. Queda prohibido el tratamiento de datos biométricos dirigidos a identificar de manera unívoca a una persona física<sup>72</sup>.

### **2.5.1 Que es un dato biométrico**

De los principios relativos al tratamiento, reglados por el artículo 5 del *RGPD*, tenemos en el apartado 14, que los datos biométricos son: “*datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos[...]*”<sup>73</sup>

En congruencia a lo anterior, la Agencia Española de Protección de Datos define datos biométricos como: “*aquellos aspectos físicos que, mediante un análisis técnico, permiten*

---

<sup>71</sup> Ley *Orgánica 3/2018*, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales. (BOE núm. 294, de 6 de diciembre de 2018).

<sup>72</sup> Reglamento 2016/679 del Parlamento Europeo y del Consejo, 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. (DOUE L 119/1).

<sup>73</sup> *Ibidem*

*distinguir las singularidades que concurren respecto de dichos aspectos en un sujeto y que, resultando que es imposible la coincidencia de tales aspectos en dos individuos, una vez procesados, permiten servir para identificar al individuo en cuestión. Así se emplean para tales fines las huellas digitales, el iris del ojo, la voz, etc. [...]”<sup>74</sup>.*

Dentro de los datos biométricos tenemos los siguientes: *“huellas dactilares, geometría de la mano, análisis del iris, análisis de retina, venas del dorso de la mano, rasgos faciales, patrón de voz, firma manuscrita, dinámica de tecleo, cadencia del paso al caminar, análisis gestual, análisis del ADN[...]”<sup>75</sup>*

### **2.5.2 La voz como dato biométrico**

De los anteriores, encontramos el patrón de voz como dato biométrico, teniendo en cuenta que la voz es una técnica de gran auge comercial, en el logro de diferentes estudios que implementan métodos para realizar la extracción de características, y la comparación<sup>76</sup>.

Las aplicaciones de reconocimiento de voz usan sistemas de la IA, como redes neuronales para aprender a identificar voces. El reconocimiento de voz es una técnica aplicada a la solución biométrica en dispositivos móviles, teniendo como objeto que el *smartphone* pueda fijar si quien emitió un texto somos nosotros u otra persona, accediendo de esta forma al desbloqueo del terminal<sup>77</sup>.

---

<sup>74</sup> Resolución: R/00900/2018. En el procedimiento sancionador PS/00002/2018, instruido por la Agencia Española de Protección de Datos a la entidad FITNESS MURCIA PROMOTIONS, S.L.

<sup>75</sup> LÓPEZ CALVO, José; y otros. *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos*. Primera edición. Madrid: Wolters Kluwer España S.A, 2018.

<sup>76</sup> INCIBE. *Tecnologías biométricas aplicadas a la ciberseguridad*. [en línea] [Fecha de consulta: 22 Mayo 2019].

[[https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia\\_tecnologias\\_biometricas\\_aplicadas\\_ciberseguridad\\_metad.pdf](https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_tecnologias_biometricas_aplicadas_ciberseguridad_metad.pdf)].

<sup>77</sup> Ibidem

### 2.5.3 Biometría y clonación de voz

Con técnicas como *Deep Voice*<sup>78</sup>, la cual puede clonar cualquier voz, con tan solo un fragmento de un minuto, se presentan situaciones donde la voz puede ser usada para crear noticias falsas. Empresas como *BaiduResrarch*<sup>79</sup> y *Lyrebird*<sup>80</sup>, ofrecen al público la opción de que con tan solo pronunciar ciertas frases de entrenamiento, pueda crearse cualquier dialogo con una voz clonada. Existen herramientas como la ofrecida por la empresa *Biometric Vox*<sup>81</sup>, que garantiza que por la aplicación “*FirVox*”, “*es capaz de identificar al usuario al otro lado del teléfono, y generar una firma electrónica mediante biometría[...]*”<sup>82</sup>.

## 2.6 TRATAMIENTO AUTOMATIZADO DE DATOS

El preámbulo de la Ley Orgánica 3 de 2018, de protección de datos personales y garantía de los derechos digitales, trajo a nivel legislativo, la concreción y desarrollo del derecho fundamental de protección de las personas físicas en relación con el tratamiento de datos personales, que tuvo lugar mediante la aprobación de la Ley Orgánica 5 de 1992, reguladora del tratamiento automatizado de datos personales, conocida como LORTAD, que deroga la disposición transitoria primera de la Ley de 1982 y que, a su vez, posteriormente es derogada por la Ley Orgánica 15 de 1999, de Protección de Datos de Carácter Personal<sup>83</sup>.

En concordancia el *RGPD*, en el último apartado del artículo 22, establece la prohibición general de adoptar decisiones individualizadas automatizadas basadas en datos personales sensibles, excepto cuando el interesado ha dado el consentimiento explícito, o por causa de interés público, siempre y cuando que se salvaguarden los derechos, libertades, e intereses

---

<sup>78</sup> GETMOVIL. *Deep Voice: la inteligencia artificial que imita tu voz* [en línea] [Fecha de consulta: 23 Mayo 2019]. [<https://getmovil.com/android/deep-voice/>].

<sup>79</sup> *Ibidem*.

<sup>80</sup> LYREBIRD. *We create the most realistic artificial voices in the world* [en línea] [Fecha de consulta: 23 Mayo 2019]. [<https://lyrebird.ai/>]

<sup>81</sup> BIOMETRIC VOX. *Soluciones mediante la voz* [en línea] [Fecha de consulta: 23 Mayo 2019]. [<https://biometricvox.com/>]

<sup>82</sup> *Ibidem*.

<sup>83</sup> *Ley Orgánica 3/2018*, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales. (BOE núm. 294, de 6 de diciembre de 2018).

legítimos del interesado<sup>84</sup>. “Del tratamiento automatizado de datos se derivarán la mayor parte de las vulneraciones del derecho al honor, a la intimidad y a la propia imagen en detrimento de las que pudieran derivarse de los otros procedimientos de comunicación[...]”<sup>85</sup>.

La voz como dato biométrico, se reviste de un carácter de dato especial; el AVG en su procesamiento automatizado realiza un perfilamiento que se basa en las solicitudes que se le hacen AVV, es decir que cada búsqueda, solicitud, recordatorio, sugerencias y conversaciones sostenidas con el AVG, ayudan a realizar un perfilamiento más detallado del PT. Pero en este caso debemos tener en cuenta que las voces de terceros están inmersas en ese tratamiento, el cual está ayudando a construir un perfil individualizado del PT con voces que a este no le pertenecen.

### **3. CONTRATO, POLÍTICA DE PRIVACIDAD, TÉRMINOS Y CONDICIONES.**

#### **3.1 EL CONTRATO A LA LUZ DE LA LEGISLACIÓN DE ESPAÑA**

Dentro la acción presentada entre el propietario del terminal PT que acepta los términos y condiciones de *Google*, para el uso y control del AVG, podemos inferir que se trata de un contrato electrónico, debido a que la aceptación de uso de este servicio se interpreta como la ratificación del contrato, por tanto, se explicará el contrato y sus características, al igual que los términos y condiciones.

---

<sup>84</sup> Reglamento 2016/679 del Parlamento Europeo y del Consejo, 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. (DOUE L 119/1).

<sup>85</sup> SÁNCHEZ ESCRIBANO, María Isabel Montserrat. Libertad informática y protección de datos: desarrollo en la jurisprudencia del Tribunal Constitucional y tutela penal en el delito de descubrimiento y revelación de secretos. *Anuario iberoamericano de justicia constitucional*. 2015, no 19, p. 323-363.



De acuerdo con el jurista español Díez Picazo, y Ponce de León, el contrato trata de regular los intereses entre dos o más personas, en el pleno uso de la libertad, iniciativa y autonomía privada<sup>86</sup>.

Los requisitos esenciales para la validez de los contratos, conforme al Capítulo II. Artículo 1261 del Código Civil, son:

- 1.º *“Consentimiento de los contratantes.*
- 2.º *Objeto cierto que sea materia del contrato.*
- 3.º *Causa de la obligación que se establezca[...]*”<sup>87</sup>.

Por su parte el artículo 1262 del mismo Código, expone que los *“contratos celebrados mediante dispositivos automáticos hay consentimiento desde que se manifiesta la aceptación[...]*”<sup>88</sup>. De igual forma, el mismo cuerpo legal en el Artículo 1278 refiere que *“los contratos serán obligatorios, cualquiera que sea la forma en que se hayan celebrado, siempre que en ellos concurran las condiciones esenciales para su validez[...]*”<sup>89</sup>.

### **3.1.1 Contrato electrónico**

Lo define la Ley 34 de 2002 del 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, reza en la letra “h) *“Contrato celebrado por vía electrónica” o “contrato electrónico”: todo contrato en el que la oferta y la aceptación se transmiten por medio de equipos electrónicos de tratamiento y almacenamiento de datos, conectados a una red de telecomunicaciones[...]*”<sup>90</sup>.

---

<sup>86</sup> DÍEZ PICAZO, Luis; DE LEÓN, Ponce. Contrato y libertad contractual. *THĒMIS-Revista de Derecho*. 2004, no 49, p. 15-21.

<sup>87</sup> *Real Decreto de 24 de Julio de 1889 por el que se publica el código civil*. (Gaceta de Madrid núm. 206, de 25/07/1889)

<sup>88</sup> *Ibidem*.

<sup>89</sup> *Ibidem*.

<sup>90</sup> *Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico*. (BOE núm. 166, de 12 de julio de 2002).

Dentro de las características de este tipo de contrato, encontramos que es: típico, puesto que ha sido regulado por la ley; principal, ya que no depende de la obligación de otro contrato; nominado, la misma ley le ha dado nombre; bilateral, en la medida que de él emanan obligaciones para ambas partes; conmutativo, las obligaciones a cargo de las partes se fijan como equivalentes y se presume armonía entre ellas; su ejecución es de tracto sucesivo, ya que no es susceptible de ser cumplido en un solo acto; y por adhesión.

### **3.1.2 Contrato por adhesión**

El contrato electrónico, en el cual se aceptan los términos y condiciones del AVG, es especialmente por adhesión.

Se trata de un acuerdo de voluntades por medio del cual uno de los contratantes, impone el contenido del contrato a la otra parte, mediante la redacción del clausulado, sin intervención de la otra, cuya libertad contractual queda limitada a manifestar o no la aceptación de sus estipulaciones, sin que esta, tenga ninguna posibilidad de discutirlo, ni de modificarlo, contando únicamente con la facultad de decidir libremente si contrata o no, bajo el clausulado ofrecido, dentro de un esquema de lo toma o lo deja<sup>91</sup>.

Las partes del contrato por adhesión son: el predisponente, es la parte que impone las condiciones generales en el contrato, en este caso es Google; y el adherente, que es la parte que se acepta los términos y condiciones, sin tener otra opción, o de lo contrario no usar el servicio<sup>92</sup>.

La Directiva 1993/13/CEE, de 5 de abril. LCEUR 1993\1071, en el Artículo 3, numeral 2. “*considera que una cláusula no se ha negociado individualmente cuando haya sido redactada previamente y el consumidor no haya podido influir sobre su contenido, en particular en el caso de los contratos de adhesión[...]*”<sup>93</sup>. La validez de este tipo de contrato

---

<sup>91</sup> POSADA TORRES, Camilo. Cláusulas Abusivas en los Contratos de Adhesión en el Derecho Colombiano. *Las. Rev. Derecho Privado*. 2015, vol. 29, p. 141.

<sup>92</sup> Ibidem

<sup>93</sup> *Directiva 93/13/CEE del Consejo*, de 5 de abril de 1993, sobre las cláusulas abusivas en los contratos celebrados con consumidores. (DOCE núm. 95, de 21 de abril de 1993).

se visualizado como “*hoy en día, la mayoría de las legislaciones admiten la validez del contrato efectuado por medios electrónicos. Al ser el pago un medio de ejecución del contrato, en este caso un medio electrónico de ejecución de un contrato electrónico, no vemos objeción alguna para declararlo legalmente admisible. [...]*”<sup>94</sup>.

### **3.2 LA CALIFICACIÓN JURÍDICA DE LA POLÍTICA DE PRIVACIDAD Y LOS TÉRMINOS Y CONDICIONES DE GOOGLE**

La calificación jurídica que podemos adaptar a la política de privacidad es la que encontramos definida en los términos y condiciones “*El uso de términos y condiciones es extremadamente frecuente en los contratos celebrados por medios electrónicos, ya sea para regular, por ejemplo, el uso de un determinado sitio web, de programas de software o, como sucede en el caso que se examina en estas páginas, para regular, parcialmente al menos, las tratativas preliminares del contrato. Pues bien, la pregunta que conviene formularse es cómo debe calificarse jurídicamente a los términos y condiciones. La respuesta, en mi opinión, es que se trata de declaraciones de una de las partes con “vocación contractual[...]”*”<sup>95</sup>.

A modo de ejemplo, la postura de la compañía *PROCD*, donde se detalla que los términos y condiciones están dentro de una caja sellada, “*leer los términos y de rechazarlos al utilizar el producto ProCD es si dinero ahora, términos después constituye un contrato (i) al momento de la orden de compra o (ii) cuando el comprador recibe la caja del software, ve el acuerdo de la licencia, y no regresa el software[...]*”<sup>96</sup>.

Tenemos entonces, que al aceptar los términos y condiciones y política de privacidad para el uso del *AVG*, el *PT* está consintiendo lo presente; no obstante, como podemos ver dentro del análisis realizado a la política de privacidad de *Google*, vemos que si bien *Google* advierte

---

<sup>94</sup> CÁRDENAS RINCÓN ERICK. *Manual de derecho de comercio electrónico y de internet* [en línea]. Primera edición. Bogotá: Centro Editorial Universidad del Rosario, febrero 2006 [Fecha de consulta 25 Mayo 2019]. [<https://books.google.es/books?hl=es&lr=&id=UBTmcWxWsDsC&oi=fnd&pg=PA14&dq=contrato+electronico&ots=pnHhxiJBSK&sig=yc8TopjpEJg1V2Qx0C-P4f9yV90#v=onepage&q=contrato%20electronico&f=false>]

<sup>95</sup> DE LA MAZA GAZMURI, Iñigo; MOMBERG URIBE, Rodrigo. Términos y condiciones: Acerca del supuesto carácter contractual de las autorizaciones para el tratamiento de datos personales en sitios web. *Revista chilena de derecho y tecnología*. 2017, vol. 6, no 2, p. 25-55.

<sup>96</sup> *Ibidem*.

que puede grabar otros sonidos, no deja claro que las voces de terceros serán sometidas a un tratamiento automatizado, y por ende estas voces harán parte de *Mi Actividad de Google*, estando presente en los datos que serán perfilados, con el fin de ofrecer búsquedas relativas a las preferencias del *PT* y productos o servicios que encajen con el perfilamiento realizado.

La política de privacidad y los términos y condiciones de Google Inc., muestren entonces que estamos frente un contrato de adhesión, donde el usuario o *PT* que no comparta las cláusulas allí contenidas no podrá acceder y usar los servicios

#### 4. EL CONSENTIMIENTO

*“El primero de los requisitos esenciales del contrato es el consentimiento. El consentimiento es el acuerdo de voluntades de dos o más personas sobre el objeto y la causa del contrato[...]*”<sup>97</sup>.

El artículo 2, letra h, de la Directiva 95/46/CE. Definen el consentimiento como *“toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen [...]*”<sup>98</sup>

El consentimiento en el *AVG* está implícito frente a el *PT*, quien acepta los términos y condiciones de *Google*, los cuales aclaran el tratamiento realizado a cada uno de los datos que son recolectados; pero, el consentimiento parte de la base de conocer, y estar enterado a que se accede y para qué fin.

En el presente *TFM*, el supuesto que los terceros no se enteran de la probabilidad de la grabación, captura, procesamiento, y almacenamiento de la voz, para luego realizar

---

<sup>97</sup> BERCOVITZ RODRÍGUEZ-CANO, Rodrigo. *Tratado de contratos: Contratación con consumidores, contratos de adhesión y contratación electrónica, contratos con finalidad traslativa de dominio, contratos de cesión temporal de uso y disfrute*. Madrid: Tirant lo Blanch, 2009.

<sup>98</sup> *Directiva 95/46/Ce del Parlamento Europeo y del Consejo*, de 24 de octubre de 1995, 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. (DOCE núm. 281, de 23 de noviembre de 1995)..

perfilamiento enfocado en publicidad dirigida al *PT*. Esto parte de dos escenarios, el primero es que el *PT* verá reflejado en la actividad de voz de *Google* que la voz de otras personas posiblemente está siendo grabada, y el segundo, es que vemos a un tercero desconociendo que su voz está siendo utilizada en un procesamiento automatizado por parte de un servicio de asistencia virtual, como el *AVG*, el cual no consintió al tercero para el uso de su voz y el tratamiento del mismo dato.

El consentimiento es una de las seis bases jurídicas para el tratamiento de datos personales, de acuerdo con el artículo 6 del *RGPD*<sup>99</sup>. Cuando se inician actividades que conllevan el tratamiento de datos personales, un responsable del tratamiento debe siempre detenerse a considerar cuál va a ser el fundamento jurídico del tratamiento previsto. El control del interesado es ilusorio y el consentimiento no será una base jurídica válida para el tratamiento, lo que convertirá dicha actividad de tratamiento en una actividad ilícita.

El consentimiento como tal está señalado en los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea.

#### **4.1 EL CONSENTIMIENTO EN EL *RGPD***

La obtención del consentimiento reconoce la obligación del responsable del tratamiento de respetar los principios del tratamiento consagrados en el *RGPD*; el artículo 5 de este Reglamento se refiere a la lealtad, necesidad y proporcionalidad, y calidad de los datos. Teniendo en cuenta que el tratamiento de los datos personales se base en el consentimiento del interesado, esto no legitima una recogida de datos que no sean necesarios para un fin concreto de tratamiento, y la misma sería esencialmente injusta.

Por su parte, el *GT29* indica que los requisitos concernientes al consentimiento en virtud del *RGPD* no se consideran como una obligación adicional, sino más bien como condiciones previas para un tratamiento lícito de los datos. Por tanto, un consentimiento válido se otorga

---

<sup>99</sup> *Reglamento 2016/679 del Parlamento Europeo y del Consejo, 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.* (DOUE L 119/1).

bajo los requerimientos estipulados en el *RGPD*, enmarcado en hechos que se determinen dentro de la aplicación de la Directiva de la privacidad y las comunicaciones electrónicas.

El artículo 4, apartado 11, del *RGPD* precisa que el consentimiento es toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

En conclusión, el consentimiento carece de validez ante cualquier influencia o presión inadecuada ejercida sobre el interesado que impida el ejercicio de su libre voluntad.

#### ***4.1.1 El consentimiento explícito***

Del consentimiento explícito dado al *AVG*, podemos precisar que siendo la voz un dato biométrico, tal como lo veremos más adelante en esta investigación, un *PT* al aceptar los términos y condiciones de *Google*, está enterado de la recolección de su voz y otros datos que ayudan a entregar resultados precisos a la hora de hacer búsquedas o acceder a ofertas del gigante tecnológico.

Si bien, el responsable de los datos, en este caso es *Google Inc.*, especifica el uso que realiza a la captura de voz; no es claro el tratamiento da a voces diferentes a las de *PT*, tampoco detalla si en caso de detectar voces que no son parecidas al del *PT*, este las deshace o no las procesa en su actividad

En el caso de llegar a capturar voces de terceros el *AVG*, estaríamos en ausencia del consentimiento explícito, que deriva del tratamiento de un dato biométrico, como la voz de los que no son partícipes de la relación contractual; la cual fue aceptada y consentida entre el *PT* y *Google Inc.*, pero no de terceros que desconocen el uso indebido de sus voces en un tratamiento automatizado por parte de *AVG*.

De acuerdo con el artículo 5, apartado 1, letra b), del *RGPD*, el consentimiento válido antepone la determinación de un fin explícito y legítimo para el tratamiento previsto. El consentimiento explícito garantiza que no se amplíen los fines para los que se realiza el

tratamiento de los datos, ya que darse otro fin diferente al especificado, se estaría dando una desviación del uso, suponiendo un riesgo al interesado y pérdida de control de su parte. Por su parte, el artículo 6, apartado 1, letra a), del *RGPD*, concreta que los interesados deberán siempre dar su consentimiento para un fin específico para el tratamiento de los datos, entendiendo que ejercen control sobre sus datos y que se tratará exclusivamente para los fines autorizados.

El Dictamen 3/2013 del *GT29*<sup>100</sup> nos habla sobre la limitación de la finalidad del consentimiento explícito dado por un fin vago o general, como; "mejorar la experiencia del usuario", "fines de mercadotecnia", "fines de seguridad informática" o "investigaciones futuras", los cuales no cuentan con suficientes detalles, y por esto no cumple el criterio de ser explícito.

#### ***4.1.2 La manifestación de voluntad informada***

De conformidad con el artículo 5 del *RGPD*, la transparencia es un principio fundamental, concerniente con la lealtad y licitud. Se debe dar la información necesaria al interesado previamente a la obtención del consentimiento, esto es indispensable para la toma de decisión. Si estos deberes no se cumplen por el responsable, el control del interesado será ilusorio y el consentimiento no contendrá validez para el tratamiento de los datos.

El responsable de tratamiento de datos en este caso *Google*, no puede manejar políticas de privacidad con difícil comprensión, ni dejar a cargo del interesado posibilidades de fines diferentes. Como en el presente *TFM*, que dentro de la política de privacidad de *Google*, el interesado no tiene que soportar la responsabilidad del tratamiento de datos que está efectuando el responsable, si se sale de los parámetros del consentimiento ya dado. De modo

---

<sup>100</sup> *Dictamen 3/2010 sobre el principio de responsabilidad*. Grupo de trabajo de protección de datos del artículo 29. Adoptado el 13 de julio de 2010.

que, si el consentimiento se solicita por medios electrónicos, la solicitud deberá ser separada y diferenciada y no podrá ser simplemente un párrafo dentro de los términos y condiciones.

#### ***4.1.3 Manifestación de voluntad inequívoca***

El artículo 4, apartado 11, del *RGPD* explica que el consentimiento válido necesita una manifestación inequívoca de la voluntad por medio de la declaración o clara acción afirmativa en armonía con la orientación previa publicada por el *GT29*.

El responsable del tratamiento de datos debe saber que el consentimiento no se puede obtener porque el usuario acuerde un contrato o acepte los términos y condiciones generales de un servicio. La aceptación global de los términos y condiciones generales no se considera una clara acción afirmativa que determine el consentimiento al uso de los datos.

#### **4.2 EL CONSENTIMIENTO EN EL MÓDULO DE ACTIVIDAD DE VOZ Y AUDIO DE GOOGLE.**

Al hacer uso de los productos de *Google*, se debe aceptar y consentir los términos que están dentro de la política de privacidad, el consentimiento se toma con la mera aceptación del formulario de *Google*, ya con ello se puede hacer uso de las funciones de los productos que se requieren.

En el módulo AVA de *Google* se ve lo siguiente: “*Solicitamos tu autorización para tratar tu información para finalidades determinados y tienes derecho a revocar tu consentimiento en cualquier momento. Por ejemplo, pedimos tu consentimiento para ofrecerte servicios personalizados, como anuncios. También pedimos tu consentimiento cuando recogemos tu actividad de voz y audio para el reconocimiento de voz*”. El consentimiento que aprueba el *PT* no es claro debido que el módulo de AVA de *Google*, dice que puede grabar otros audios o grabar voces que pueden ser similares, pero no especifica que esas voces de terceros serán sometidas a un tratamiento automatizado por parte de los servicios de *Google*.



### 4.3 CONSENTIMIENTO EN LAS GRABACIONES DE VOZ

De la Sentencia 56 de 2003 del Tribunal Constitucional<sup>101</sup>, se interpreta que el quebrantamiento al secreto de las comunicaciones se comete al transmitir información a otros, y con esto traspasar la esfera íntima del interlocutor; es decir, la mera captación de la voz entre las partes de una comunicación no se aprecia como una conducta ilícita.

Por tanto, el acto de grabación por uno de los interlocutores de la conversación no conculca secreto alguno impuesto por el art. 18.3 CE; sin embargo, la contravención constitucional sólo podría entenderse materializada por el hecho mismo de la difusión de tal grabación; para el caso del AVG sería el tratamiento automatizado que se da a la voz; si bien, la voz como dato está siendo grabada solo con el consentimiento del PT, ya que el tercero no está enterado ni ha dado el consentimiento explícito; hasta ese punto no estaríamos frente a ninguna vulneración de derechos, pero en el momento que el AVG trata y procesa estos datos, a partir de este punto es donde comienza la ilicitud de la conducta entendida como violación a la protección de datos, a la intimidad, y al secreto de las comunicaciones.

Por su parte, la Sentencia 1066 de 2009 del Tribunal Supremo Sala de lo Penal<sup>102</sup>, señala la legitimidad de las grabaciones en conversaciones privadas entre dos o más personas, tratándose de una comunicación grabada por uno de los interlocutores sin el consentimiento de los demás. Inicialmente, esta conducta cuenta como lícita, pues todo depende de que la conversación sea voluntaria, libre, y de forma espontánea por las partes, partiendo del principio de la buena fe.

En el caso que un tercero participante de una comunicación con su interlocutor, este siendo grabado por el AVG, y este no lo sepa, o no lo haya consentido; hasta ahí no hay ilicitud como tal, esta se vislumbra cuando el AVG da un tratamiento a la voz como dato especial, la procesa, y almacena, pues para esto si es indispensable el consentimiento explícito de todas las partes involucradas en la conversación, y es aquí donde se configura la vulneración a la intimidad, secreto de comunicaciones, y protección de datos, pues en ningún momento el

---

<sup>101</sup> Sentencia 56 de 2003 Tribunal Constitucional. (BOE núm. 91, de 16 de abril de 2003).

<sup>102</sup> Sentencia 1066 de 2009 del Tribunal Supremo Sala de lo Penal. ( Id CENDOJ: 28079120012009101128, de 4 de noviembre de 2009).

tercero está dando consentimiento explícito e informado para el uso y tratamiento de sus datos, teniendo en cuenta que la voz es un dato biométrico de especial protección.

De igual manera la Sentencia 114 de 1984 del Tribunal Constitucional<sup>103</sup>, expone que no hay «secreto» para quien la comunicación se dirige, ni implica contravención de lo dispuesto en el artículo. 18.3 C. E. El concepto de secreto, de acuerdo con el art. 18.3, tiene carácter formal en el sentido de que se predica de lo comunicado, sea cual sea su contenido y pertenezca o no el objeto de la comunicación misma al ámbito de lo personal, lo íntimo o lo reservado.

Comprendiendo lo dicho, una grabación entre personas que han participado de esta es lícita, aunque no exista el consentimiento de todos los participantes, y no significa ni siquiera, que sea una actuación preparatoria del ilícito constitucional. La conducta lícita se mantendrá siempre y cuando permanezca la grabación entre las partes y no se transmita a ningún tercero ajeno, ni se dé otro fin que violente la intimidad de quien fue grabado.

La Sentencia 4626 de 2011 del Tribunal Supremo, Sala de lo Penal <sup>104</sup>, enseña que la jurisprudencia ha fijado, que la grabación que un particular haga de sus propias conversaciones no supone un atentado al secreto de las comunicaciones, distinguiendo la diferencia entre grabar una conversación de otros y grabar una conversación con otros.

En todo caso, no se transgrede el derecho al secreto de las comunicaciones, siempre y cuando la misma persona que este grabando una conversación sea partícipe de la misma, muy diferente cuando graba conversaciones en las cuales no está participando, en este caso estaría cometiendo una contravención de carácter constitucional.

La Sentencia del Tribunal Supremo Sala de lo Penal 1322 de 1996<sup>105</sup>, explica que no hay violación al derecho de la intimidad, ni al secreto de comunicaciones cuando se produce una grabación subrepticia de una conversación entre varias personas, realizada por una de ellas.

---

<sup>103</sup> *Sentencia 114 de 1984* del Tribunal Constitucional. (BOE núm. 305, de 21 de diciembre de 1984).

<sup>104</sup> *Sentencia 4626 de 2011* Tribunal Supremo, Sala de lo Penal. (Id CENDOJ: 28079120012011100681, de 24 de junio de 2011)

<sup>105</sup> *Sentencia 1322 de 1996* del Tribunal Supremo Sala de lo Penal. (Id CENDOJ: 28079120011996102126, de 1 de marzo de 1996).

En concordancia la Sentencia 8421 de 1998 del Tribunal Supremo Sala de lo Penal<sup>106</sup>, considera que tampoco se vulneran tales derechos fundamentales por las grabaciones magnetofónicas realizadas por particulares de conversaciones mantenidas con terceras personas, ya que el secreto de las comunicaciones se refiere esencialmente a la protección de los ciudadanos frente al Estado.

De otro lado, la Sentencia 3077 de 1995 del Tribunal Supremo, Sala de lo Penal<sup>107</sup>, profiere que el secreto de las comunicaciones se vulnera cuando un tercero no autorizado interfiere y llega a conocer el contenido de las que mantienen otras personas, no cuando uno de los comunicantes se limita a perpetuar, mediante grabación mecánica, el mensaje emitido por el otro.

## **5. RESULTADOS OBTENIDOS QUE RESUELVEN LA HIPÓTESIS**

### **5.1 PRUEBAS TÉCNICAS AL MÓDULO DE ACTIVIDAD DE VOZ Y AUDIO DE GOOGLE EN DISPOSITIVOS ANDROID**

Dentro del presente *TFM*, con base en los experimentos realizados, se determinó que el *AVG* graba y procesa la voz de terceros sin el consentimiento explícito requerido para el tratamiento de datos especiales.

En las configuraciones realizadas en los tres terminales usados para las pruebas, se configuró la opción de *Voice Match*, con el fin de reconocer solo la voz del *PT*, como operador único de cada terminal.

---

<sup>106</sup> Sentencia 8421 de 1998 del Tribunal Supremo Sala de lo Penal. (Id CENDOJ: 28079120011998101827, de 29 de julio de 1998).

<sup>107</sup> Sentencia 3077 de 1995 del Tribunal Supremo, Sala de lo Penal. (Id CENDOJ: 28079120011995103129, de 30 de mayo de 1995).

Ahora bien, dentro del primero y segundo experimento contenido en el anexo 1, se contó con la ayuda de diez participantes de diferente sexo, y nacionalidades, quienes dieron su consentimiento para hacer uso de sus voces en diferentes ambientes, lo que ayudó a comprender mejor, si el AVG graba voces de terceros, y al ser grabadas, que proceso emerge de esto.

En el primer experimento, se pidió en la primera fase a cada uno de los participantes que pronunciaran la palabra “Ok Google” con el fin de observar si podían desbloquear el terminal tres<sup>108</sup>, el cual, como opción de desbloqueo, tiene el parámetro de la voz gestionada por el AVG. El resultado fue que tres personas pudieron conseguir el objetivo.

Ahora, en la segunda fase del primer experimento, se solicitó a los participantes que pronunciaran la palabra “Ok Google” pero en cada uno de los terminales desbloqueado. El resultado fue que 8 personas pudieron conseguir realizar consultas al AVG, y este procesó sus voces y registró cada procedimiento en “Mi Actividad”.

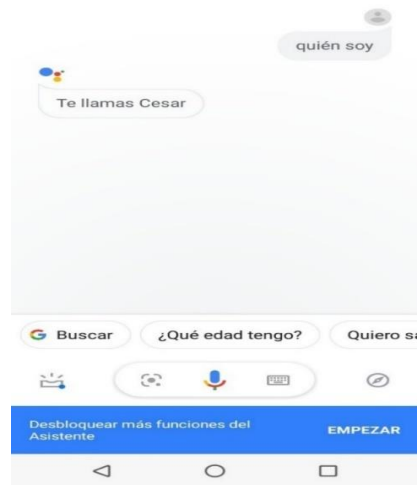
Dentro de los hallazgos encontrados en la fase 1 y 2 del primer experimento, se evidencia que el modo de detección de voz por el AVG, al estar bloqueado el terminal, es más estricto que cuando no está bloqueado. Se pudo ver reflejado el aumento de los participantes que pudieron interactuar con el AVG en más del doble para la segunda fase. Esto lleva a comprobar que los niveles de análisis de voz en ambas fases (bloqueado o desbloqueado) no son igual de rigurosos.

De este modo, con los resultados obtenidos, cabe preguntarse ¿Por qué el AVG posee niveles tan bajos de seguridad, al lograr el 30% de los participantes desbloquear el terminal 3, y el 80% consiguieron interactuar con el AVG, al estar desbloqueado todos los terminales, al punto que el mismo sistema reconoció a todos los que interactuaron como si fuera el PT?. En la siguiente imagen puede verse cuando cada uno preguntó al AVG ¿Quién soy?.

---

<sup>108</sup> Ver anexo Nro. 1, tabla 8. Equipos móviles usados.

Gráfico 3: pregunta al AVG



Fuente: copiada desde captura de pantalla en dispositivo Android

De los resultados obtenidos en el primer experimento, se prueba en el segundo experimento, las razones por las cuales puede el AVG someter a un procesamiento automático las voces de terceros.

Se realiza un análisis de la voz de cada participante, donde se pronuncia dos frases, ambas grabadas y procesadas por un programa de análisis de audio. Dentro de cada observación realizada, se encontró que los participantes que pudieron desbloquear el terminal 3, en la fase uno del primer experimento, la gráfica de análisis reveló que tenían tonos muy similares, y por tanto, se entiende que el AVG realiza una comparativa a nivel de tonos de voz, mas no un estudio biométrico de la misma; examen que puede evitar que personas con tonos de voz equivalentes puedan interactuar con el terminal, y por ende quebrantar la seguridad del mismo.

Lo interesante, es encontrar que al estar los terminales desbloqueados y activar el AVG por medio del comando de voz *Ok Google* y pronunciar la frase *“la perfección de la naturaleza se perturbó cuando intervino el error humano”*, se pudo encontrar que los tonos de muchas voces gráficamente no son tan símiles, al punto de no encontrar patrones que pudieran inferir que el examen realizado por el AVG fue estricto y exhaustivo. Es por ello que los resultados reflejaron nuevamente que el nivel de seguridad del AVG, en estado de reposo el terminal 3,

es más estricto, pero al estar el teléfono desbloqueado, es vulnerable a que terceros puedan manipular el AVG, realizando solicitudes no consentidas por el *PT*.

El tercer experimento, se llevó a cabo en diferentes espacios abiertos, donde varias personas interactuaron en diversas charlas. En diferentes momentos, se pudo ver que el AVG al estar activo, esperando orden alguna, pudo captar la voz de los presentes en recintos o en la vía pública; teniendo en cuenta que en varias conversaciones intervinieron más de dos personas, el AVG grabó a todos los intervinientes; pero solo realizó el respectivo procesamiento a la voz con el tono más alto.

Acorde a los tres resultados obtenidos en los tres experimentos, se puede responder al objetivo del presente *TFM*; si bien es claro que el AVG puede grabar voces de terceros y que estos al ser partícipes en la conversación con el *PT*, no requieren su consentimiento, no es entendible para el *PT* ni para los terceros, que *Google Inc* no esclarezca en las políticas de privacidad, que fuera de escuchar voces de terceros, estas serán sometidas a un tratamiento automatizado, para ser finalmente almacenadas en servidores de *Google Inc*.

Esto con el fin de realizar un perfilamiento basado en las métricas, que el mismo AVG ha capturado las voces de terceros, sin tener la facultad legal de realizar este tipo de tratamiento a un dato especialmente protegido por el *RGPD*, y reconocido como un dato biométrico, que permite identificar a cualquier persona por las voces que son almacenadas en “*Mi actividad*”.

Si bien, sólo el *PT* tiene acceso a “*Mi Actividad*”, el hecho de que *Google Inc*, exteriorice en una publicidad dirigida gustos o aficiones del *PT*, pero basándose en voces de terceros, es un claro ejemplo de la ilicitud del tratamiento de datos; ya que dicha conducta se exteriorizó a patrocinadores que saben bien a qué tipo de productos y servicios dirigir al interesado, pero todo esto fundado en datos especialmente carentes de consentimiento explícito.

Dentro de las conclusiones en el anexo 1, se puede resumir que el producto AVG no está preparado para cumplir lo requerido por el *RGPD*, en referencia al tratamiento de datos personales.

## 5.2 ANÁLISIS DE LA ENCUESTA ELECTRÓNICA: ASISTENTES VIRTUALES ACTIVADOS POR VOZ EN EL HOGAR Y SMARTPHONES (TELÉFONOS INTELIGENTES)

La encuesta electrónica arrojó el nivel de percepción sobre temas referentes al presente *TFM*. La muestra es de 100 participantes, residentes en: Alemania, Australia, Colombia, EEUU, y España. El cuestionario se desarrolló desde la herramienta de *Google Forms*<sup>109</sup>.

Dentro de los resultados se resalta que el 99% de encuestados, poseen teléfonos inteligentes, en especial los basados en sistema Android en un 79% y un 21 % de Apple.

El uso de *AVV*, no es muy común entre los participantes, en equipos bajo sistema *Android* del 79% de encuestados con este *S.O*, solo el 46 % usa el *AVG*.

En los equipos Apple, de 21 % encuestados con este tipo de teléfono inteligente, solo 43% usan el asistente virtual de voz *SIRI*, el 5% el *AVG* bajo sistema *IOS*.

A nivel de asistentes virtual de hogar solo el 10 % de los encuestados usan este tipo de dispositivos, siendo *Google Home* el más usado.

Lo anterior contrasta con una encuesta electrónica realizada por *AIMC* Asociación para la Investigación de Medios de Comunicación, la cual indica que:

*“Uno de cada cinco navegantes utiliza asistentes virtuales de voz con asiduidad aunque algo más de la mitad de los navegantes (53,6%) no utiliza los asistentes virtuales de voz (Siri, Cortana, asistente de Google, etc.), uno de cada cinco encuestados (20,0%) sí que lo hace con cierta asiduidad (varias veces a la semana o con una frecuencia mayor).*

---

<sup>109</sup>GOOGLE INC, *Google Forms*, [en línea] [Fecha de consulta: 23 Mayo 2019]. [<https://www.google.es/intl/es/forms/about/>]

*Si nos centramos en el uso de los nuevos asistentes del hogar o altavoces inteligentes, parece que, por el momento, no llaman demasiado la atención a los encuestados. Al 22,4% les parece atractivo poder disponer de este tipo de aparatos en contraposición con el 50,1% que no les despierta interés, al menos de momento” [...]”<sup>110</sup>.*

Lo anterior se visualiza en la siguiente grafica extraída del mismo estudio:

Gráfico 4: Uso de asistentes virtuales de voz



Fuente: copiada de:

[http://download.aimc.es/aimc/NoPU2G5Tt/190306\\_NP\\_Resultados\\_21Navegantes\\_Red.pdf](http://download.aimc.es/aimc/NoPU2G5Tt/190306_NP_Resultados_21Navegantes_Red.pdf)

Las razones encontradas en los encuestados, del por qué no usan un AVV, predominó en un 46% el que no es necesario para el encuestado, teme por su privacidad y prefiere comunicarse por otros medios. Se tiene en cuenta que esta pregunta era de múltiples respuestas.

En el ámbito de que los encuestados temen por su privacidad se contrastó con la pregunta que refería si el AVV, escucha sus conversaciones sin autorización para luego ofrecer publicidad dirigida, donde más del 61% cree que esto sucede.

Se reitera que el 55% de los encuestados quisieron conocer la política de protección de datos, se tomaron el trabajo de consultarla y aceptarla. Pero en la pregunta referente si

<sup>110</sup> ASOCIACIÓN PARA LA INVESTIGACIÓN DE MEDIOS DE COMUNICACIÓN, AIMC. *La mitad de los internautas considera que “no podría vivir sin internet en el móvil”*. [en línea] [Fecha de consulta: 10 Junio 2019]. [[http://download.aimc.es/aimc/NoPU2G5Tt/190306\\_NP\\_Resultados\\_21Navegantes\\_Red.pdf](http://download.aimc.es/aimc/NoPU2G5Tt/190306_NP_Resultados_21Navegantes_Red.pdf)].



los encuestados han leído los términos y condiciones del AVV, la respuesta fue que un 75% no los ha leído.

Esta encuesta, puede concluir que existe un *S.O* y un *AVV* predominantes, ambos propiedad de *Google Inc.* El *AVG* es el más usado entre los encuestados, gracias a que el sistema *Android* está presente en más del 75% de los dispositivos inteligentes. Teniendo en cuenta que *SIRI*, el asistente de voz de *Apple*, sólo opera en dispositivos de la misma marca, mientras que el *AVG*, puede operar en múltiples plataformas. En esta encuesta pudo verse que ciertos encuestados poseen un dispositivo de la marca *Apple*, pero usan el *AVG* como su *AVV*.

Lo anterior se puede comparar en la siguiente gráfica

Gráfico 5: Smartphone Market Share

Quarter	2017Q4	2018Q1	2018Q2	2018Q3	2018Q4	2019Q1
Samsung	18,9%	23,5%	21,0%	20,3%	18,8%	23,0%
Huawei	10,7%	11,8%	15,9%	14,6%	16,2%	18,9%
Apple	19,6%	15,7%	12,1%	13,2%	18,3%	11,8%
Xiaomi	7,1%	8,4%	9,5%	9,5%	6,7%	8,9%
Vivo*	6,0%	5,6%	7,9%	8,3%	6,9%	7,4%
OPPO*	6,9%	7,4%	8,6%	8,4%	7,9%	7,4%
Others	30,9%	27,6%	25,0%	25,7%	25,1%	22,7%
TOTAL	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%

Fuente: copiada de: <https://www.idc.com/promo/smartphone-market-share/vendor>

La gráfica revela que *Apple* solo tiene el 11,8% de presencia del mercado mundial de teléfonos inteligentes, mientras que más de un 75% posee marcas que tiene *S.O*

*Android*<sup>111</sup>, teniendo un 22 % de otros fabricantes que en su mayoría pueden operar bajo el *S.O de Google*, que en este caso es *Android*<sup>112</sup>.

## REFLEXIÓN

En el mundo actual estamos dispuestos a perder nuestra privacidad e intimidad con el fin de tener acceso a los servicios que nos ofrecen las diferentes plataformas tecnológicas. cabe recordar las palabras del autor Dan Brown, en su obra *La fortaleza digital*, “*Había luchado hasta la muerte por sus creencias: el derecho de todo individuo a la privacidad[...]*”<sup>113</sup>. Hoy en día nos enfrentamos a una lucha por recuperar nuestra privacidad e intimidad digital.

El mismo autor nos dice *¿Quién vigilará a los vigilantes? -Sí. Si nosotros somos los vigilantes de la sociedad, ¿Quién nos vigilará y procurará que no seamos peligrosos? [...]*<sup>114</sup>.

Las *GAFAM*<sup>115</sup>, son las compañías tecnológicas más importantes del mundo; pero no existe un ente que regule o vigile su código fuente. Entonces ¿Cómo podemos garantizar que sus operaciones no violentaran derechos, si no podemos ver que está ocurriendo detrás del telón?

---

<sup>111</sup> IDC, International Data Corporation. *Smartphone Market Share*. [en línea] [Fecha de consulta: 10 Junio 2019]. [<https://www.idc.com/promo/smartphone-market-share/vendor>]. IDC, International Data Corporation es un proveedor chino de inteligencia de mercado, servicios de asesoría y eventos para los mercados de tecnología de la información, telecomunicaciones y tecnología de consumo.

<sup>112</sup> Ibidem.

<sup>113</sup> BROWN, Dan. *La fortaleza digital*. Primera edición. Nueva York: St Martin’s Press-Nueva Cork, 2006.

<sup>114</sup> Ibidem.

<sup>115</sup> DE BUSTOS, Juan Carlos Miguel; CANO MORENO, Toñy. Los señores de los datos: Google-Alphabet, Amazon, Facebook, Apple y Microsoft. *Boletín del Centro de Documentación Hegoa*. 2018, no 53, p. 1-12.

## CONCLUSIONES

Del presente *TFM*, se concluye lo siguiente:

Primero: La ausencia del consentimiento explícito frente al tratamiento de datos de carácter especial, en este caso, datos biométricos como la voz.

Del tratamiento que realiza el *AVG* a la voz de los terceros que son grabados, se desprende la ilicitud del mismo, pues la voz de los terceros es sometida sin el consentimiento explícito a un procesamiento automatizado por el *AVG*.

Aunque no se requiera el consentimiento para grabar la voz de los partícipes dentro de una conversación, sí se requiere para el procesamiento y tratamiento de esos datos. En ningún apartado de la política de privacidad de *Google Inc*, indica que las voces capturadas sin el consentimiento de terceros serán sometidas a un tratamiento automatizado, que genera consecuencias en las preferencias y perfilamiento del *PT*.

Dentro de la política de privacidad, podemos concluir que el uso de la voz por parte del módulo de *AVA* de *Google Inc*, se encarga de procesar las búsquedas realizadas por el *AVG*, para luego ofrecer productos y servicios orientados al perfilamiento obtenido de todas las fuentes de datos, que son cada uno de los productos y servicios ofrecidos por la familia *Google Inc*. En el caso de la voz de terceros, es un tratamiento, con una finalidad no autorizada.

Segundo: Uno de los ofrecimientos por parte de *Google Inc*, para prestar el servicio de *AVG*, puede considerarse altruista cuando se trata de usuarios con diversidad funcional, que sólo pueden operar el dispositivo por medio de comandos de voz. En este contexto se considera una herramienta muy útil y práctica, al punto de salvar vidas, por ser los *AVV* necesarios para las personas que conducen vehículos y no pueden estar pendientes de la pantalla de sus dispositivos, o en una emergencia puedan realizar una llamada solo pronunciando ciertos comandos específicos.

Por esto, una herramienta como el *AVG* debe tener presente los controles más rigurosos a la hora de operar, debido a que un producto con tantas ventajas no debe desconocer que contiene

brechas que colocan en riesgo la seguridad de muchos dispositivos con este tipo de tecnologías, al comprometer la privacidad e intimidad de los *PT*; se puede evidenciar la carencia de protocolos más efectivos a la hora de reconocer y detectar solo la voz del *PT*.

Tercero: Los métodos para copiar la voz de cualquier persona son muy eficientes, pero existen métodos que ayudan a detectar con gran fiabilidad si la voz usada es o no de quien dice ser, por eso *Google Inc*, al ofrecer su *AVG*, debe tener todas las técnicas existentes en el mercado, que le permitiría no procesar ni tratar la voz de aquellos que no han dado su consentimiento, para evitar que su producto infrinja lo contenido en el *RGPD*, conforme al tratamiento de datos biométricos los cuales son de carácter especial.

Cuarto: No hay un estudio que hoy pueda garantizar que los dispositivos de *Google Inc*, que contienen un *AVG*, y al momento de estar en reposo puedan estar grabando sin autorización.

Debido que *Google* no abre su código para poder analizar cómo se comporta su software, y así garantizar que no está grabando sin autorización, y por ende, que está respetando la privacidad e intimidad de cada individuo.

En el presente estudio se ha demostrado que el *AVG* en ciertas condiciones puede grabar y procesar voces de terceros; por tanto, en otro tipo de estudio más profundo, posiblemente se puede develar si en realidad *Google Inc*, programa su *AVG*, para que en modo furtivo sus asistentes de hogar, o modo reposo de cualquier Smartphone, puedan estar grabando y procesando la voz de cualquier persona sin el consentimiento.

Vemos que el *AVG* requiere siempre del servicio internet para prestar la mayoría de sus servicios, y al pronunciar “Ok *Google*” existe unos milisegundos de silencio, antes de reconocer lo pronunciado, esto se distinguió en las pruebas realizadas (Ver anexo Nro. 1, numeral 4, ver gráficos de oscilograma), donde el *AVG* al estar operando procesa todo el audio circundante, esperando que se pronuncie la orden que lo activa para poder prestar sus servicios.

Por lo anterior se concluye que la voz de un tercero al ser capturada y procesada automáticamente por parte del *AVG*, sin el consentimiento explícito para tal fin, se convierte en una práctica ilícita por parte de *Google Inc*

## TABLAS

<i>Tabla 1: Lista Asistentes de voz. ....</i>	8
<i>Tabla 2: Cómo opera el asistente de voz de Google .....</i>	17

## GRÁFICOS

<i>Gráfico 1: Componentes de un sistema de ASR típico.</i> .....	6
<i>Gráfico 2: Actividad de voz y audio, captura de pantalla de Google.</i> .....	17
<i>Gráfico 3: pregunta al AVG</i> .....	44
<i>Gráfico 4: Uso de asistentes virtuales de voz</i> .....	47
<i>Gráfico 5: Smartphone Market Share</i> .....	48

## BIBLIOGRAFÍA

- ANTÓN MARTÍN, Javier. *Desarrollo de un sistema de reconocimiento de habla natural independiente del locutor*. Tesis de Licenciatura, Universidad Autónoma de Madrid escuela politécnica superior, Madrid, 2015.
- BARRAGÁN, María Luisa. *Los derechos al honor, a la intimidad personal y familiar y a la propia imagen del menor*. 1ª edición. Anuario de justicia de menores, 2015, no 15, p. 702-703.
- BROWN, Dan. *La fortaleza digital*. Primera edición. Nueva York: St Martin's Press-Nueva Cork, 2006.
- CÁRDENAS RINCÓN ERICK. *Manual de derecho de comercio electrónico y de internet* [en línea]. Primera edición. Bogotá: Centro Editorial Universidad del Rosario, febrero 2006 [Fecha de consulta 25 Mayo 2019]. [https://books.google.es/books?hl=es&lr=&id=UBTmcWxWsDsC&oi=fnd&pg=PA14&dq=contrato+electronico&ots=pnHhxiJBSK&sig=yc8TopjpEJg1V2Qx0C-P4f9yV90#v=onepage&q=contrato%20electronico&f=false]
- COBOS TORRES, Juan Carlos. *Integración de un Chatbot como habilidad de un robot social con gestor de diálogos*. Tesis de maestría, Universidad Carlos III de Madrid, Leganés, Madrid, 2013.
- CORTÉS OSORIO, JIMY ALEXANDER, MEDINA AGUIRRE, FRANCISCO ALEJANDRO, MURIEL ESCOBAR, JOSÉ A. *Sistemas de seguridad basados en biometría*. [en línea]. Pereira Colombia: vol. XVII, núm. 46, 2010 [Fecha de consulta 8 junio de 2019] Disponible en: <http://www.redalyc.org/articulo.oa?id=84920977016>.
- DE BUSTOS, Juan Carlos Miguel; CANO MORENO, Toñy. Los señores de los datos: Google-Alphabet, Amazon, Facebook, Apple y Microsoft. *Boletín del Centro de Documentación Hegoa*. 2018, no 53, p. 1-12.
- DE LA MAZA GAZMURI, Iñigo; MOMBERG URIBE, Rodrigo. Términos y condiciones:

- Acerca del supuesto carácter contractual de las autorizaciones para el tratamiento de datos personales en sitios web. *Revista chilena de derecho y tecnología*. 2017, vol. 6, no 2, p. 25-55.
- DÍEZ PICAZO, Luis; DE LEÓN, Ponce. Contrato y libertad contractual. *THĒMIS-Revista de Derecho*. 2004, no 49, p. 15-21.
- GRONDONA, N.; MAZZA, M.; DORFMAN, P. Asistentes virtuales de clase en la Educación Universitaria. *Una visió crítica: III Congr s Europeu de Technologies de la Informaci  en l'Educaci  i en la Societat*. 2012. p. 294-296.
- HARDY, Thomas. IA (Inteligencia Artificial). Polis: *Revista Latinoamericana*. 2001, no 2, p. 18.
- JIM NEZ, Cinta CASTILLO. *Protecci n del derecho a la intimidad y uso de las nuevas tecnolog as de la informaci n*. [en l nea]. [Fecha de consulta: 13 Mayo 2019]. [<http://rabida.uhu.es/dspace/bitstream/handle/10272/1565/b1205654.pdf>].
- L PEZ CALVO, Jos ; y otros. *El nuevo marco regulatorio derivado del Reglamento Europeo de Protecci n de Datos*. Primera edici n. Madrid: Wolters Kluwer Espa a S.A, 2018.
- CASANOVA MART , Roser; PIC  I JUNOY, Joan. *Las intervenciones telef nicas en el proceso penal*. Edici n desconocida. Barcelona: Jos  Mar a Bosch, 2014.
- MEDINA, Javier; CABEZA, Eduardo; PE A, Juan Luis Castro. Asistentes virtuales en plataformas 3.0. *IE Comunicaciones: Revista Iberoamericana de Inform tica Educativa*. 2013, no 18, p. 41-49.
- HERR N ORTIZ, Ana Isabel. *El derecho a la intimidad en la nueva Ley Org nica de Protecci n de Datos Personales*. Edici n desconocida. Madrid: Dykinson, 2002.
- BERCOVITZ RODR GUEZ-CANO, Rodrigo. *Tratado de contratos: Contrataci n con consumidores, contratos de adhesi n y contrataci n electr nica, contratos con finalidad traslativa de dominio, contratos de cesi n temporal de uso y disfrute*. Madrid: Tirant lo Blanch, 2009.
- RON ROMERO, Jos . Derecho al secreto de las comunicaciones telef nicas, un reto para la



buena administración. *Anuario da Faculta de de Dereito da Universidade da Coruña*. 2011, no 15, p. 103-128.

RUFINER, Hugo L.; MILONE, Diego H. Sistema de reconocimiento automático del habla. *Ciencia, Docencia y Tecnología*. 2004, vol. 15, no 28, p. 151-177.

SÁNCHEZ ESCRIBANO, María Isabel Montserrat. Libertad informática y protección de datos: desarrollo en la jurisprudencia del Tribunal Constitucional y tutela penal en el delito de descubrimiento y revelación de secretos. *Anuario iberoamericano de justicia constitucional*. 2015, no 19, p. 323-363.

SENSO, José A.; DE LA ROSA PIÑERO, Antonio. El concepto de metadato. Algo más que descripción de recursos electrónicos. *Ciência da Informação*. 2003, vol. 32, no 2.

SUCAR, Luis Enrique. Probabilistic graphical models. *Advances in Computer Vision and Pattern Recognition*. London: Springer London. 2015, vol. 10, p. 978-1.

TELEFÓNICA, Fundación. *Sociedad Digital en España 2018*. Primera edición. Madrid: Fundación Telefónica, 2019.

POSADA TORRES, Camilo. Cláusulas Abusivas en los Contratos de Adhesión en el Derecho Colombiano. *Las. Rev. Derecho Privado*. 2015, vol. 29, p. 141.

## **FUENTES NORMATIVAS**

*Constitución de la república portuguesa de 2 de abril de 1976*.

*Constitución Española*. (BOE núm. 311, de 29 de diciembre de 1978).

*Convención Europea De Derechos Humanos*. Convenio Europeo de Derechos Humanos. Tribunal Europeo de Derechos Humanos. (BOE núm. 243, de 10 de octubre de 1979).

*Convenio 108 del Consejo de Europa*, de 28-1-1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. (BOE núm. 274, de 15 de noviembre de 1985).

*Dictamen 3/2010 sobre el principio de responsabilidad.* Grupo de trabajo de protección de datos del artículo 29. Adoptado el 13 de julio de 2010.

*Directiva 93/13/CEE del Consejo,* de 5 de abril de 1993, sobre las cláusulas abusivas en los contratos celebrados con consumidores. (DOCE núm. 95, de 21 de abril de 1993).

*Directiva 95/46/Ce del Parlamento Europeo y del Consejo,* de 24 de octubre de 1995, 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. (DOCE núm. 281, de 23 de noviembre de 1995).

*Instrumento de ratificación de España del pacto Internacional de Derechos Civiles y Políticos,* hecho en Nueva York el 19 de diciembre de 1966. (BOE núm. 103, de 30 de abril de 1977).

*La Declaración Universal de Derechos Humanos.* (BOE núm. 243, de 10 de octubre de 1979).

*Ley 34/2002,* de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. (BOE núm. 166, de 12 de julio de 2002).

*Ley 9/2014,* de 9 de mayo, *general de telecomunicaciones.* (BOE núm. 114, de 10 de mayo de 2014).

*Ley Orgánica 1/1982,* de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. (BOE núm. 115, de 14 de mayo de 1982).

*Ley orgánica 15/1999,* de 13 de diciembre, de protección de datos de carácter personal. (BOE núm. 298, de 14 de diciembre de 1999).

*Ley Orgánica 3/2018,* de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales. (BOE núm. 294, de 6 de diciembre de 2018).

*Ley Orgánica 5/1992,* de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. (BOE núm. 262, de 31 de octubre de 1992).

*Real Decreto de 24 de Julio de 1889 por el que se publica el código civil.* (Gaceta de Madrid núm. 206, de 25/07/1889)

*Reglamento 2016/679 del Parlamento Europeo y del Consejo, 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.* (DOUE L 119/1).

*Resolución: R/00900/2018.* En el procedimiento sancionador PS/00002/2018, instruido por la Agencia Española de Protección de Datos a la entidad FITNESS MURCIA PROMOTIONS, S.L.

### **FUENTES JURISPRUDENCIALES**

*Sentencia 1066 de 2009 del Tribunal Supremo Sala de lo Penal.*( Id CENDOJ: 28079120012009101128, de 4 de noviembre de 2009).

*Sentencia 114 de 1984 del Tribunal Constitucional.* (BOE núm. 305, de 21 de diciembre de 1984).

*Sentencia 1322 de 1996 del Tribunal Supremo Sala de lo Penal.* (Id CENDOJ: 28079120011996102126, de 1 de marzo de 1996).

*Sentencia 134 de 1999,* de 15 de julio de 1999. (BOE núm. 197, de 18 de agosto de 1999).

*Sentencia 151 de 1997, De 29 De septiembre.* (BOE núm. 260, de 30 de octubre de 1997).

*Sentencia 23 de 2010,* de 27 de abril de 2010. (BOE núm. 129, de 27 de mayo de 2010).

*Sentencia 254 de 1993,* de 20 de julio de 1993. (BOE núm. 197, de 18 de agosto de 1993).

*Sentencia 3077 de 1995 del Tribunal Supremo, Sala de lo Penal.* (Id CENDOJ: 28079120011995103129, de 30 de mayo de 1995)

*Sentencia 4626 de 2011 Tribunal Supremo, Sala de lo Penal.* (Id CENDOJ: 28079120012011100681, de 24 de junio de 2011)

*Sentencia 56 de 2003 Tribunal Constitucional.* (BOE núm. 91, de 16 de abril de 2003).

*Sentencia 8421 de 1998 del Tribunal Supremo Sala de lo Penal.* (Id CENDOJ: 28079120011998101827, de 29 de julio de 1998).

*Sentencia 94 de 1998*, de 4 de mayo. (BOE núm. 137, de 9 de junio de 1998).

## OTRAS FUENTES

ALBERTO GARCÍA. *Google Assistant, Alexa o Siri: ¿cuál es el mejor asistente de voz para tu hogar?* [en línea] [Fecha de consulta 08 Marzo 2019].  
[<https://www.adslzone.net/reportajes/domotica/Google-assistant-alexa-siri>].

ASOCIACIÓN PARA LA INVESTIGACIÓN DE MEDIOS DE COMUNICACIÓN, AIMC. *La mitad de los internautas considera que “no podría vivir sin internet en el móvil”* [en línea] [Fecha de consulta: 10 Junio 2019].  
[[http://download.aimc.es/aimc/NoPU2G5Tt/190306\\_NP\\_Resultados\\_21Navegantes\\_Red.pdf](http://download.aimc.es/aimc/NoPU2G5Tt/190306_NP_Resultados_21Navegantes_Red.pdf)].

BASTERRA, BERTEA, BORELLO, CASTILLO Y VENTURI. *Android OS Documentation Release 0.1* [en línea] [Fecha de consulta: 09 Mayo 2019].  
[<https://buildmedia.readthedocs.org/media/pdf/androidos/latest/androidos.pdf#page=7&zoom=100,0,432>].

BIOMETRIC VOX. *Soluciones mediante la voz* [en línea] [Fecha de consulta: 23 Mayo 2019]. [<https://biometricvox.com/>]

GETMOVIL. *Deep Voice: la inteligencia artificial que imita tu voz* [en línea] [Fecha de consulta: 23 Mayo 2019]. [<https://getmovil.com/android/deep-voice/>]

GOOGLE INC. *Centro de Seguridad* [en línea] [Fecha de consulta: 11 Enero 2019].  
[<https://safety.google/intl/es/principles/>].

GOOGLE INC. *Cómo administrar la Actividad de voz y audio en Google* [en línea] [Fecha de consulta: 09 Junio 2019].  
[<https://support.google.com/websearch/answer/6030020?co=GENIE.Platform%3DDesktop&hl=es-419>].

GOOGLE INC, *Configuración de Voice Match*, [en línea] [Fecha de consulta: 09 Mayo

2019]. [<https://myactivity.google.com/>].

GOOGLE INC, *Gestionar la actividad de voz y audio de Google*, [en línea] [Fecha de consulta: 09 Junio 2019]. [<https://support.google.com/websearch/answer/6030020?co=GENIE.Platform%3DAndroid&hl=es>].

GOOGLE INC, *Google Forms*, [en línea] [Fecha de consulta: 23 Mayo 2019]. [<https://www.google.es/intl/es/forms/about/>]

GOOGLE INC, *Política de Privacidad de Google*, [en línea] [Fecha de consulta: 11 Enero 2019]. [<https://policies.google.com/privacy?hl=es>].

GOOGLE INC, *Ver y controlar la actividad de la cuenta*. [en línea] [Fecha de consulta: 09 Mayo 2019]. [<https://support.google.com/accounts/answer/7028918?co=GENIE.Platform%3DDesktop&hl=es>]

IDC, International Data Corporation. *Smartphone Market Share*. [en línea] [Fecha de consulta: 10 Junio 2019]. [<https://www.idc.com/promo/smartphone-market-share/vendor>].

INCIBE. *Tecnologías biométricas aplicadas a la ciberseguridad*. [en línea] [Fecha de consulta: 22 Mayo 2019]. [[https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia\\_tecnologias\\_biotricas\\_aplicadas\\_ciberseguridad\\_metad.pdf](https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_tecnologias_biotricas_aplicadas_ciberseguridad_metad.pdf)].

LYREBIRD. *We create the most realistic artificial voices in the world* [en línea] [Fecha de consulta: 23 Mayo 2019]. [<https://lyrebird.ai/>]

SENDPULSE. *Que es Publicidad dirigida* [en línea] [Fecha de consulta 09 Mayo 2019]. [<https://sendpulse.com/latam/support/glossary/targeting>].

## **ANEXOS**

1. Pruebas técnicas al módulo de actividad de voz y audio de Google en dispositivos Android.
2. Encuesta Electrónica. Asistentes virtuales activados por voz en el hogar y Smartphones (teléfonos inteligentes)