VNiVERSiDAD D SALAMANCA

CAMPUS DE EXCELENCIA INTERNACIONAL

TRABAJO FIN DE GRADO

GRADO EN DERECHO

Derecho Privado

Derecho Civil

Curso 2019/2020

TRATAMIENTO DE LA VOZ COMO DATO PERSONAL MEDIANTE EL ACCESO AL MICRÓFONO EN DISPOSITIVOS MÓVILES Y PRÁCTICAS ACTUALES DE APPS PARA RECABAR SU CONSENTIMIENTO

Nombre del/la estudiante: Isabella Andreina Rocafull Fernández

Tutor / Juan Pablo Aparicio Vaquero

Mes: Julio **Año: 2020**

TRABAJO FIN DE GRADO

GRADO EN DERECHO

Departamento

Área de conocimiento

TRATAMIENTO DE LA VOZ COMO DATO PERSONAL MEDIANTE EL ACCESO AL MICRÓFONO EN DISPOSITIVOS MÓVILES Y PRÁCTICAS ACTUALES DE APPS PARA RECABAR SU CONSENTIMIENTO

VOICE PROCESSING AS PERSONAL DATA THROUGH MICROPHONE ACCESS ON MOBILE DEVICES AND CURRENT APP PRACTICES TO OBTAIN CONSENT

Nombre del/la estudiante: Isabella Andreina Rocafull Fernández
e-mail del/a estudiante: isabellarocafull@usal.es

Tutor/a: Juan Pablo Aparicio Vaquero

RESUMEN (15 líneas)

El siguiente Trabajo de Fin de Grado tiene como fin realizar un análisis jurídico sobre la voz como dato personal y aquellos que se puedan desvelar a lo largo de una conversación a los que las aplicaciones móviles tienen acceso mediante el micrófono. Así como la caracterización de sus principales riesgos teniendo en cuenta el panorama de las redes sociales y la automaticidad de los usuarios al momento de consentir las políticas de privacidad y los respectivos permisos a los sensores y recursos de los dispositivos móviles. Se analizará tanto la perspectiva de la voz como dato biométrico, como la posibilidad de tener acceso a otros datos de tipo sensible. El análisis toma en cuenta los principales elementos del consentimiento según el actual RGPD, comparándolos con las políticas de privacidad de las aplicaciones Instagram y WhatsApp, y su adaptación a la actual normativa, y las distintas recomendaciones, informes y guías que propone tanto la AEPD y el Grupo de Trabajo del Artículo 29, para suplir los vacíos legislativos que presenta el Reglamento frente al nuevo fenómeno del Big Data.

PALABRAS CLAVE: DATOS, PERSONALES, VOZ, INSTAGRAM, WHATSAPP, POLÍTICA, PRIVACIDAD.

ABSTRACT

The following Final Degree Project is aimed at carrying out a legal analysis on voice as personal data and those that can be exposed during a conversation to which mobile applications have access through the microphone. As well as the characterization of its main risks taking into account the panorama of social networks and the automaticity of users when consenting to privacy policies and respective permissions to sensors and resources of mobile devices. Both the perspective of voice and biometric data, as well as the possibility of having access to other sensitive data, will be analyzed. The analysis takes into account the main elements of consent according to the current RGPD, comparing them with the privacy policies of the Instagram and WhatsApp applications, and their adaptation to the current regulations, and the various recommendations, reports and guides proposed by both the AEPD and the Article 29 Working Group, to fill the legislative gaps presented by the Regulation in the face of the new phenomenon of Big Data.

KEYWORDS: DATA, PERSONAL, VOICE, INSTAGRAM, WHATSAPP, POLICY, PRIVACY

ÍNDICE

1. Introducción.

En la actualidad, en medio de la implantación masiva del fenómeno Big Data en la red de empresas, junto con el uso casi intensivo en nuestro día a día de dispositivos móviles, surge la oportunidad de lucrarse económicamente a costa de nuevos datos personales, que sin el cumplimiento estricto de medidas, puede suponer una importante invasión a nuestra privacidad.

El usuario medio en el mercado de aplicaciones, no es consciente del poder y control que por su naturaleza debe tener sobre sus propios datos personales, en concreto su datos como su voz. Adolece de automaticidad al momento de aceptar cualquier tipo de tratamiento. Así como tampoco se toma la molestia de evaluar los posibles riesgos que se pueden producir en un marco ilícito y poco transparente.

A raíz de ello, este trabajo pretende colocar en la mesa el incumplimiento de los artículos y recomendaciones a fines para recabar un consentimiento específico, granular, libre, e informado, exponiendo como ejemplo dos de las aplicaciones más populares y más descargadas tanto en dispositivos Android como en dispositivos iOS, en lo que concierne al tratamiento de los datos que se disponen a partir del micrófono del nuestros móviles. El objetivo que nos ocupa en este trabajo es situar a la voz como dato personal y biométrico, dentro del Derecho de Protección de Datos, su posible tratamiento a través del micrófono de los dispositivos, ante una aceptación condiciones de una política de privacidad dotada de elasticidad, imprecisión, y abstracción. Así como también un análisis jurídico sobre las actuales políticas de privacidad de las aplicaciones, desde la perspectiva de un tratamiento sobre este dato biométrico.

Por ello, la metodología de este trabajo consiste en una revisión bibliográfica sobre el material más actualizado de los autores relevantes en el tema, como de un análisis jurídico sobre el actual RGPD, acompañado de dictámenes del Grupo de Trabajo del Artículo 29, asimismo de informes y resoluciones de la AEPD, como de la jurisprudencia más reciente. Para ayudar a entender los riesgos por los que se preocupa este trabajo, también se añade una encuesta realizada por mi persona.

2. La voz como dato personal.

Es preciso para este trabajo entender cómo encaja la voz dentro de la normativa de protección de datos. Según el artículo cuatro de Reglamento General de Protección de

Datos, se define como dato toda información sobre una persona física identificada o identificable, cuya identidad pueda determinarse directa o indirectamente mediante un identificador, entre los cuales nombra, elementos propios de la identidad física, fisiológica o genética, de dicha persona.[1]

Por otro lado, el Real Decreto 1720/2007 del 21 de diciembre en su artículo cinco, también hace una precisión sobre el concepto[2]. Clasifica como dato personal, información acústica, tal y como lo podría ser la voz.

El actual marco legal no excluye la voz como un dato personal, sino que incluso da cabida a ella. El uso de la expresión "*toda información*" se inclina por una interpretación no restrictiva, y las precisiones como información acústica o elementos de identidad fisiológica, dan a entender que la voz podría encajar en estas aproximaciones.

El Grupo de Trabajo del artículo 29[3] en uno de sus dictámenes enmarca a los datos que consisten en sonidos[4] como una forma de soporte para los datos personales, y serán considerados como tales, en tanto contengan información que por ella pueda determinar, directa o indirectamente a la identidad de la persona. Las grabaciones de audio se considerarían datos personales en formato de sonido, en tanto contenga información sobre una persona cuya identidad pueda identificarse. Sin embargo, la voz no es cualquier grabación de audio.

El informe 190/2009 de la AEPD parece descartar la idea de que la voz es un dato personal *per se*[5]. En ellos se afirma que la voz, o las grabaciones de voz comienzan a ser

---

[1] Artículo 4. 1) Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos.

[2] Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Boletín Oficial del Estado 19 de enero de 2008, núm 17.

[3] Con la directiva 95/46/CE se crea en virtud del artículo 29 un grupo de carácter consultivo e independiente, legitimado para publicar informes y dictámenes, que si bien no son jurídicamente vinculantes, poseen un gran valor doctrinal y resultan citados frecuentemente por legisladores como tribunales, tanto europeos como nacionales.

[4] "el concepto de datos personales incluye la información disponible en cualquier forma, alfabética, numérica, gráfica, fotográfica o sonora, por ejemplo." Dictamen 4/2007 del Grupo de Trabajo del artículo 29 «sobre el concepto de datos personales» p. 8.

[5] *"…tales grabaciones tienen trascendencia y entran dentro del ámbito de aplicación de la Ley desde el momento en que en las mismas puedan recogerse datos personales de los clientes que contactan con el servicio* (…) *Aun cuando nos hallemos ante un supuesto en que existan datos de carácter personal…*".

datos protegidos por la normativa, en tanto cumplan con las condiciones del artículo 4.1 del RGPD.

Contrario, a la idea anterior, la jurisprudencia reconduce la normativa, en la SAN de 19 de marzo de 2014, a su vez corroborada en la SAN del 29 de noviembre de 2018, afirmando que "*la voz de una persona constituye un dato personal, tal y como se deduce de la definición*"[6]. De esta manera, se reconoce que la voz goza de poder para identificar, como elemento inherente a ella, sin tener que demostrar que una grabación de una conversación aporta datos personales, diferentes a lo que sería la voz en sí. La voz sería entonces un dato personal como cualquier otro, como lo puede ser la imagen[7].

En agosto de 2019, la resolución de procedimiento sancionador contra la app de La Liga[8], juzga la captación de sonido que realiza la app, como tratamiento de datos, cuando esta capte una conversación en la que se desvelen datos de carácter personal. Si bien se debe aclarar que esta idea no es contraria, a entender que la voz conforma en dato personal, sino que en este caso, la grabación de sonido puede considerarse tratamiento cuando se den estas circunstancias. Sin embargo, más que la certeza de que efectivamente la conversación albergue datos, es "la posibilidad de recoger datos de carácter personal es la que le a este tratamiento tributario del cumplimiento"[9] de las distintas garantías y obligaciones de la normativa.

El considerando 26 del RGPD, tiene presente que para que un dato pueda identificar a una persona física, no sólo el dato debe ser óptimo para ello, sino que debe conjugarse con la razonabilidad de medios y el criterio de proporcionalidad[10]. De forma que el aplicando los medios y elementos necesarios, o bien en combinación con otros datos, tanto por el propio responsable como por cualquier persona deben ser capaces de identificar directa o indirectamente a la persona. En el caso del informe jurídico

---

Informe jurídico 190/2009 del 4 de enero de 2010, del Gabinete Jurídico de la Agencia Española de Protección de Datos, p. 2

[6] SAN del 29 de noviembre de 2018, p. 5.

[7] "*En consecuencia, la imagen así como la voz de una persona es un dato personal, al igual que lo será cualquier información que permita determinar, directa o indirectamente, su identidad, como por ejemplo, una matrícula de vehículo, una dirección IP, etc. y así lo ha considerado en reiteradas ocasiones esta AEPD.*" Informe jurídico 0139/2017 del 14 de septiembre de 2017, del Gabinete jurídico de la Agencia Española de Protección de Datos, p. 2

[8] Resolución del PS núm. 00329/2018 del 20 de Agosto de 2019

[9] Resolución del PS núm. 00329/2018 del 20 de Agosto de 2019, p. 45.

[10] ACED, E., HERAS, R., & SÁIZ, C. A. (2017). Código de buenas prácticas en protección de datos para proyectos big data. Agencia Española de Protección de Datos.

497/2007 se plantea que las grabaciones de voz, en efecto, son capaces de identificar a una persona perfectamente, cumpliendo con el considerando 26, no necesitando de esfuerzos o plazos desproporcionados para proceder a la identificación[11].

En términos más recientes esta cuestión vuelve a ser controvertida, en el caso de una aplicación llamada "Juasapp" dedicada a confeccionar bromas telefónicas grabando la voz del usuario para posteriormente compartirse entre distintos contactos. La AEPD calificó como no válido al consentimiento recabado por la aplicación, incumpliendo el artículo 6.1 de la LOPD, imponiendo una multa de 7.500 euros. La empresa afirmó en el recuso contencioso-administrativo que no podían vulnerar el artículo, al no existir un tratamiento de datos personales, puesto que la grabación de voz no resulta ser un dato personal debido a que su duración es tan corta, que no permite identificarse directa o indirectamente la identidad de la persona, a menos de que se empleen medios desproporcionados. El recurso fue desestimado, a lo que la empresa respondió con el respectivo recurso de casación[12]. Finalmente la STS del 18 de junio de 2020, calificó que el registro de voz y el número de teléfono, conjuntamente permiten la identificación de una persona. Sin embargo, considera que aunque la aplicación no almacenara el número telefónico, la voz constaría como un dato personal, debido a que terceros pueden acceder a las grabaciones de voz, permitiendo que allegados a los interesados puedan identificarlos, sin tener que aplicar medios desproporcionados. Si bien esta sentencia no deja en claro que el tratamiento de la voz es en sí un tratamiento de un dato personal, esta última circunstancia, por la que las grabaciones resultan ser identificables, no presume ser una condición especial requerida para el caso de que la voz pueda encajar en la definición del artículo 4.11, y distinta a las exigencias básicas que se demandan para que cualquier otro dato personal pueda directa o indirectamente identificar a una persona.

Finalmente, reconociendo la voz como dato personal, es pertinente clasificarlo. La voz es un dato biométrico[13], ergo, un dato sensible[14]. Es un dato que es atribuible a una sola

[11] Informe jurídico 497/2007 del 3 de Marzo de 2008, del Gabinete Jurídico de la Agencia Española de Protección de Datos, p. 2.
[12] Admitido por el ATS del 31 de mayo de 2019
[13] En el Dictamen 4/2007, afirma que los datos biométricos pueden definirse como: "*propiedades biológicas, características fisiológicas, rasgos de la personalidad o tics, que son, al mismo tiempo, atribuibles a una sola persona*." p. 9.
[14] No todos los datos tienen el mismo nivel de sensibilidad. Se consideran datos sensibles según el artículo 9 del Reglamento General de Protección de Datos: "*revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de*

persona. Los datos biométricos, sirven incluso como mecanismo de trasporte para otros datos personales. Es por ello que su determinación como dato personal, en el caso de la voz, presenta interpretaciones distintas. Puede ser tanto dato biométrico, como un agente para contener otros. Si bien la STS sobre el caso "Juasapp", como la resolución de la AEPD contra la Liga, omiten la calificación de la voz como dato biométrico, para este trabajo se tomará en cuenta la aproximación del Dictamen 4/2007[15].

3. Tratamiento de la voz por aplicaciones

Los dispositivos inteligentes son capaces de recoger datos personales a través de su simple uso. Mediante los permisos que concede el usuario a las aplicaciones, estas pueden interactuar con los sensores[16] que dispone el móvil, tales como el micrófono, el geolocalizador, la cámara, el bluetooth, entre otros. Pueden formar parte del hardware o del software del dispositivo. Normalmente las apps acuden a ellos para utilizar todas las funciones que su programa ofrece, y así ejecutarse adecuadamente. Sin embargo, esto no quiere decir, que al acudir a estos sensores, no se esté realizando un tratamiento.

El artículo cuatro del RGPD, entiende por tratamiento aquellas operaciones o conjunto de operaciones realizadas sobre datos personales, sean automatizadas o no. El *acceso* que obtienen las aplicaciones a partir de la autorización del usuario, conforma un tratamiento de datos: "o cualquier otra forma de habilitación de acceso"[17].

---

datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física"

[15] "*Ejemplos típicos de datos biométricos son los que proporcionan las huellas dactilares, los modelos retinales, la estructura facial, las voces, pero también la geometría de la mano, las estructuras venosas e incluso determinada habilidad profundamente arraigada u otra característica del comportamiento (como la caligrafía, las pulsaciones, una manera particular de caminar o de hablar, etc.).*" p. 9.

[16] Según la Agencia Española de Protección de Datos en el análisis de los flujos de información en Android herramientas para el cumplimiento de la responsabilidad proactiva, realizado junto con la Universidad Politécnica de Madrid, publicado el 7 de marzo de 2019, p. 6: los dispositivos móviles incorporan o pueden interoperar "*con sensores de diferente naturaleza (ej. GPS, cámara, micrófono, Wifi, sensores para salud y estado físico, etc.) que generan una cantidad considerable de datos personales (ej. localización, fotografías y notas de audios personales, temperatura, ritmo cardíaco, etc.) a los que las aplicaciones pueden acceder*"

[17] Artículo cuatro. 2) del Reglamento (UE) 2016/679: *"«tratamiento»:cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción*"

Una nota de voz, es un dato personal previamente tratado, que se encuentra en un formato[18] de audio. Sin embargo el almacenamiento, la captación, y la grabación, de voz son tratamientos en sí mismos, que deben hallar su legitimación en la normativa, debido a que la voz ya constituye un dato biométrico. Por otro lado, la grabación de un audio, distinto a la voz humana, se considera tratamiento a partir del momento en el que esta grabación pueda constar datos personales.

La activación del micrófono del dispositivo móvil, debe observarse diferente, dadas las circunstancias que implican poseer un móvil, se abre la posibilidad de efectuar un tratamiento, no sólo de cualquier información auditiva que pueda contener datos personales, sino de un tratamiento de un dato que es específicamente relevante: la voz.

En la resolución contra la app de La Liga[19], se juzga el tratamiento desde que la aplicación comienza a captar y recoger el audio, y no desde el momento en el se autoriza y la app empieza a tener habilitado el acceso al micrófono. Es a partir de este fundamento que se determina que la aplicación vulneró el principio de transparencia, al no aportar la información en el momento preciso cuando se lleva a cabo el tratamiento, como lo exige el considerando 39. No se tuvo en cuenta que el tratamiento se producía incluso antes de la captación.

La obtención de datos según la AEPD ocurre cuando el tratamiento se realiza efectivamente. La información de la app La Liga se proporciona, justo en el momento en el que se pide la autorización de acceso al micrófono, cuando según la Agencia, esta más bien, debió mostrarse cuando la utilización del micrófono tiene lugar[20]. Contradiciendo y descartando la idea de que "habilitación de acceso" es el primer tratamiento, atendiendo a la definición del artículo 4. Menos aún diferenciándola como tratamiento autónomo beneficiario del principio de transparencia

En el caso que nos ocupa, la captación o almacenamiento, cotejo o conversión suceden una vez que se consiente el acceso. Por las distintas deficiencias dentro de la política de

[18] Así lo indica el Dictamen 4/2007, página 8: *"Desde el punto de vista del formato o el soporte en que la información está contenida, el concepto de datos personales incluye la información disponible en cualquier forma, alfabética, numérica, gráfica, fotográfica o sonora, por ejemplo."*

[19] "*se puede afirmar que si la captación se produce durante una conversación donde se indican datos de carácter personal, estaremos ante una captación o recogida de datos de carácter personal, y por tanto ante un tratamiento de datos personales*" p. 45.

[20] Según la resolución, el momento en el que se ofrece la información del tratamiento "*dista en el tiempo respecto de cuando efectivamente, se usara el micrófono*" p. 56.

privacidad, como la falta de regulación específica ante el fenómeno de las apps, es desde el punto de vista del acceso al que este trabajo pretende hacer frente.

3.1. Los desarrolladores de aplicaciones

Los desarrolladores de las aplicaciones juegan un rol importantísimo en la protección de datos. Son ellos quienes se ocupan de crear los programas de la app, y en base a ello determinan cuáles son los accesos necesarios a las funciones del dispositivo móvil que la app requiere. En una aplicación como Whatsapp[21], el desarrollador quiere crear un sistema de mensajería instantánea, que sea capaz de enviar audios. Para ello, determina que la app debe disponer de la información que el micrófono pueda captar, si el usuario quiere enviar notas de voz. Son así los responsables del tratamiento, cuando sean ellos quienes determinen los fines y medios del tratamiento, según el artículo cuatro, apartado 7) del RGPD.

Es por ello que los desarrolladores, cuando cumplan con esta condición, serán responsables del cumplimiento del artículo 5.1, garantizando los principios de tratamiento leal, lícito y transparente, limitación de la finalidad y minimización de datos. Así como están obligados a satisfacer el deber de informar del artículo 13, bien a través de políticas de privacidad, notificaciones o bien mediante descripciones en las tiendas de aplicaciones, cuando sea posible.[22] Así como ajustarse a la finalidad, y a la legitimación en la que se basa el tratamiento.

4. Riesgos en la protección de datos ante el uso de las apps

Para hablar de los riesgos que se pueden ocasionar por parte de las aplicaciones para recaudar datos, es necesario hablar sobre el "Big Data". Se define así como un fenómeno que implica la utilización de un conjunto de tecnologías, algoritmos y sistemas que hacen posible tratar cantidades masivas de datos, que provienen de distintas fuentes, con la finalidad de asignarle una utilidad y un valor[23] . Asimismo el

[21] WhatsApp es una aplicación de mensajería instantánea que permite a los usuarios enviar fotos, videos, mensajes y grabaciones de voz.
[22] Acorde a la AEPD en su Análisis de flujos de información en Adroid, p.9
[23]GIL, E. (2016) Big data, privacidad y protección de datos. *Madrid: Agencia Estatal Boletín Oficial del Estado*. p. 15

concepto hace referencia también el volumen de datos en sí[24]. Una de las finalidades más comunes del "Big Data" es la publicidad comportamental. Las empresas y los fabricantes de aplicaciones buscan hacer más relevante y eficaz sus publicidades, encajando los anuncios emergentes con los intereses del usuario, y si bien esto beneficia tanto al usuario como al fabricante, pueden generarse intromisiones a la privacidad, en la esfera del derecho de protección de datos**.**

De forma coloquial se dice que cuando un producto es gratis, es porque el producto eres tú. El precio que pagan los usuarios por estas apps gratuitas son sus datos personales. Se han convertido "en materia prima y en una nueva fuente de inmenso valor económico"[25]. Aunque más importante es señalar la procedencia de los datos que usa actualmente el Big Data, que ya no sólo abarca las preferencias de un usuario que se desprenden de los motores de búsqueda[26] o el correo electrónico, sino que se plantean nuevas oportunidades de información a través de los sensores que contienen los dispositivos inteligentes.

Es a través de las API[27] una de las formas que los desarrolladores pueden servirse de datos que se derivan de la geolocalización, cámara, micrófono, y determinar intereses y patrones de conducta. El Grupo de Trabajo del artículo 29, considera que aquellas empresas que pretendan beneficiarse del Big Data, a través de un tratamiento ilícito y no adecuado de datos como la localización, los contactos, los registros de llamadas, los SMS, las fotografías y vídeos, y otros datos biométricos, que recogen las aplicaciones, pueden afectar significativamente la vida privada[28].

Uno de los problemas radica en la falsa sensación de control por el usuario sobre sus datos, al instalar una aplicación en su móvil. Debido al fraccionamiento que existe por

[24] GARRIGA DOMÍNGUEZ, A. (2016) *Nuevos retos para la protección de datos personales. En la Era del Big Data y de la computación ubicua*. Dykinson, p. 27.
[25] Ibid p. 28-43
[26] Los motores de búsqueda o buscador, como Google, Mozilla firefox o Microsoft Edge, son sistemas o programas que se dedican a buscar archivos almacenados en los servidores web a partir de la araña web. TRAMULLAS, J; OLVERA-LOBO, M (2001). *Recuperación de la información en Internet*. Madrid, Ra-Ma.
[27] Las siglas API identifican a lo que se conoce en inglés como *application programming interface,* en español *interfaz de programación de aplicaciones*. Son las interfaces que poseen los sistemas operativos que sirven a las aplicaciones para acceder a datos almacenados y funciones del dispositivo móvil. Dictamen 02/2003 del Grupo de Trabajo del artículo 29 «sobre aplicaciones de los dispositivos inteligentes.» p. 13.

[28] Así lo dispone en el Dictamen 02/2013 del Grupo de Trabajo del artículo 29 «sobre aplicaciones de los dispositivos inteligentes.»

los distintos procesos y actores que intervienen en el desarrollo de una aplicación, como en su ejecución, que va desde los fabricantes de los sistemas operativos de los móviles, como los desarrolladores de apps, hasta los distintos servicios de publicidad que analizan los datos recogidos por estas. El fundamento que da vida al derecho de protección de datos del interesado, como lo son la autodeterminación y disposición sobre los mismos, se va cada vez más desdibujando.

El usuario pierde su autonomía para elegir los datos y la condiciones en que van a ser tratados frente a la aceptación general de políticas de privacidad, al no disponer una normativa específica para este nuevo fenómeno, o bien al depender de guías o informes jurídicos que sí abarcan la problemática, pero que se ven obstaculizadas en su ejecución al no tener fuerza vinculante.

Estos riesgos se traducen en grandes problemas, y que son más comunes de lo que se pretende proteger, que enfrenta la protección de datos con las aplicaciones móviles, y de los que se tratará más adelante. Radican en el incumplimiento del principio de transparencia y la falta de granularidad, lo que se traduce en una imposibilidad para prestar un consentimiento libre, específico e informado por parte del interesado.

La normativa atribuye excesiva confianza al consentimiento como base legitimadora por excelencia, cuando muchas veces supone un ejercicio vacío[29]. No se cuestiona la idoneidad del consentimiento para ciertas formas de tratamiento, convirtiéndose en una vía de escape perfecta para que los desarrolladores de aplicaciones legitimen su tratamiento.

Al mismo tiempo, el concepto de *big data* es contrapuesto con el principio de minimización de datos, pues se basa en un análisis que necesita de la mayor cantidad de datos posible. La abundancia de datos que el Big data pretende recoger, obliga a las aplicaciones a acudir al consentimiento como base legitimadora de su tratamiento, debido a que muchos de estos datos no son estrictamente de interés legítimo del responsable.

5. Panorama actual de aplicaciones: el acceso al micrófono

[29] Gil, E. (2016). Big data, privacidad y protección de datos. *Madrid: Agencia Estatal Boletín Oficial del Estado*, p. 52-53

Las aplicaciones móviles son entonces unas de las principales fuentes de recopilación de datos. Whatsapp e Instagram[30] son algunas de las muchas apps que requieren del acceso al micrófono para ejecutar distintas actividades, como por ejemplo enviar mensajes de voz y capturar vídeos.

El formato que se utiliza para recabar el consentimiento por estas aplicaciones, al igual que el de muchas otras, consiste básicamente en la lectura y aceptación previa de las condiciones de su política de privacidad[31] a fin de poder empezar a utilizar la app. Posteriormente la aplicación solicita los respectivos accesos a los distintos recursos, bien sean los contactos, la cámara, la ubicación o el micrófono. Estas solicitudes emergen cuando el usuario acuda por primera vez a alguna función que requiera dichos sensores. Por ejemplo, en el caso del sistema operativo iOS[32], cuando quiera enviar un mensaje de voz, aparecerá un anuncio en el medio de la pantalla que indica lo siguiente: "WhatsApp quiere acceder al uso del micrófono. Esto permite hacer llamadas, enviar mensajes de voz y grabar vídeos con sonido"[33]. Debajo aparecen dos opciones: permitir y no permitir. Si no se permite, la app no posibilita al usuario realizar actividades que impliquen el uso del micrófono, al contrario de si este acepta. El mismo procedimiento se repite con Instagram[34]. Este formato es común para recoger la autorización del usuario en distintos sistemas operativos, como sucede también en Android[35].

Tanto en iOS como en Android se ofrece en la app de "Ajustes" un panel de control para cada aplicación descargada, en el que se presenta un resumen de los accesos que han sido concedidos[36] a distintos tipos de datos como sensores. La información expuesta únicamente permite al usuario distinguir que accesos han sido consentidos y cuáles no. No se indica la extensión o límites que implican dichas habilitaciones, salvo algunas excepciones como la localización[37].

Cuando se autoriza a la app para acceder al micrófono, desde la configuración del sistema operativo del dispositivo, se hace en su totalidad. Esto facultaría activar todas

[30] Instagram es una red social, con formato de aplicación, propiedad de Facebook Inc, así como WhatsApp.
[31] Véase el anexo 1
[32] iOS es el sistema operativo creado y utilizado por la marca Apple Inc. Para sus productos: iPhone, iMAC, iWatch, etc.
[33] Véase el anexo 2
[34] Véase el anexo 3
[35] Véase el anexo 4
[36] Véase el anexo 5 como ejemplo
[37] Véase anexo 6

las acciones posibles que el micrófono puede llevar a cabo según el sistema operativo. Se trata de consentir un abanico de posibilidades, un consentimiento dado en general e ilimitado, que sin una política de privacidad adecuada, crearía un riesgo de desviación de uso.

Acorde a la nota técnica de la AEPD, en donde analiza el software de los dispositivos Android "el número de permisos existentes, dista mucho del número de permisos que podrían ser gestionados humanamente, y ponen de manifiesto un déficit de transparencia de los aplicativos y del propio sistema operativo Android al mostrar únicamente al usuario una relación de permisos distinta de la real, limitando así su capacidad de decisión para gestionar su información personal y el ejercicio de su derecho a la protección de datos"[38]. El software sólo permite al usuario conocer que se ha dado un acceso general al micrófono, y que dicho acceso, podría usarse para realizar ciertas funciones, como enviar mensajes de voz, o bien grabar vídeos, sin embargo, estos no son los únicas actividades que se pueden llevar a cabo con el micrófono.

El destino de los datos no dependería de la decisión del usuario, sino en las configuraciones que han programado los desarrolladores en el manifiesto[39] de la aplicación. El acceso incluso podría involucrar una actuación en segundo plano[40], de estos sensores o recursos, sin su conocimiento, de manera que podría iniciarse una grabación constante, incluso cuando no se esté usando la aplicación, con este único acceso.

Muchas aplicaciones funcionan en segundo plano[41] para cumplir distintas tareas, como por ejemplo enviar notificaciones sin necesidad de uso por el usuario del móvil o la

---

[38] GAMBA, J., RASHED, M., RAZAGHPANAH, A., TAPIADOR, J., & RODRIGUEZ, N. (2019). *NOTA TÉCNICA Avance del estudio de IMDEA NETWORKS y UC3M: "Análisis del Software Pre-instalado en Dispositivos Android y sus Riesgos para la Privacidad de los Usuarios"*. Madrid, p. 6.

[39] El manifiesto es el archivo que todas las aplicaciones deben tener y que contiene la información esencial para su creación. En él se contienen todas las funciones, los permisos que necesitan, el nombre, las actividades y servicios que realizan. Describe la forma en la que se configura la app. De acuerdo con *Descripción general del manifiesto de una app.* (2020).

[40] "Las aplicaciones también pueden requerir que se ejecuten algunas tareas incluso cuando el usuario no usa la app de forma activa, por ejemplo, para hacer una sincronización periódica con un servidor en segundo plano o una búsqueda frecuente de contenido nuevo dentro de una app. También pueden requerir que los servicios se ejecuten inmediatamente hasta completarse incluso después de que el usuario haya terminado de interactuar con la app." *Guía para el procesamiento en segundo plano. (2020).*

[41] Prueba de ello es la mencionada resolución de la AEPD contra La Liga, que dejó en evidencia durante las actuaciones previas de inspección, que la aplicación seguía "funcionando y enviando información, incluso si no se está ejecutando en primer plano. Para la captación de los datos (micrófono y ubicación)

aplicación, o cuando así se permite en la geolocalización. Aunque, estas notificaciones no requieren de un tratamiento de datos para ejecutarse, y la geolocalización, además de tener la opción[42] en el caso iOS de controlar su acceso específicamente en casi todas las aplicaciones, en la política de privacidad se encuentra a menudo regulada. Un ejemplo de ello se halla en la política de privacidad[43] de Instagram que nos indica que uno de los datos que recopila es la ubicación, con el fin de personalizar y mejorar sus productos, como los anuncios, para que estos tengan mayor relevancia.

Por otro lado, el uso del micrófono se obvia en las políticas de privacidad de estas empresas. En el caso de Instagram, en el apartado primero de su política, afirma que recopila información y datos que provienen de estos permisos que el usuario concede desde la configuración del dispositivo, como la ubicación GPS, cámara y fotos. Pero no hace mención explícita sobre los datos procedentes del acceso al micrófono, ni su respectivo tratamiento[44].

Los riesgos de que se produzcan intromisiones o intervenciones no válidamente consentidas, se acentúan aún más cuando los dispositivos móviles se convierten en un aparato que nos acompaña a lo largo del día. Hoy en día las personas solemos mantener nuestros móviles en el bolsillo del pantalón, o al lado nuestro cuando nos quedamos dormidos.

Para entender de donde yace la problemática que pretende abordar este trabajo, se realizó una encuesta a alrededor de 100 individuos mayores de 18 años con diferentes rangos de edad por medio de la plataforma encuesta.com[45]. Una de las primeras preguntas, trataba sobre qué aplicaciones tenían los encuestados descargadas en su móvil[46]. Se presentaban tres opciones acumulables: WhatsApp, Instagram y Facebook. 86 personas eran usuarias de Instagram, 72 eran de Facebook, y todas usuarias de WhatsApp.

---

no es necesario que la aplicación esté ejecutándose en primer plano, existiendo procesos informáticos, ejecutándose en segundo plano (background) en el dispositivo móvil que permiten la recogida de los datos".

[42] Véase el anexo 7
[43] *Data Policy* | Facebook Help Centre. (2018).
[44] Como el que efectivamente sucede al recoger y enviar, notas de voz como mensajes, o incluso con la realización de vídeos, y su posterior publicación en la app.
[45] *Encuestas online* - Encuesta.com.
[46] Véase los resultados de la encuesta en los anexos: 8, 9, 10, 11.

Posteriormente se preguntó sobre los accesos que estas personas habían otorgado a las mencionadas apps, con el fin de que estas procedan a su normal uso. Se presentaron igualmente tres opciones de tipo acumulable. 93% de las personas afirmaron que daban acceso a sus fotos. 90% permitía el acceso a la cámara, y por último un 84% autorizaba a las apps que así lo solicitaban, el acceso al micrófono.

Con el fin de demostrar que las personas portan su teléfono la mayor parte del tiempo, y que este se encuentra al alcance de la mano o a una distancia cercana, siendo el micrófono capaz de captar información, mediante la grabación de audio, por ejemplo a partir de conversaciones, se preguntó lo siguiente: "¿Cuánto tiempo consideras que llevas o tienes tu teléfono a la mano o cerca de ti?". Se dieron tres opciones de las cuales un 48% de las personas respondió la opción A: "Siempre tengo el teléfono conmigo o cerca de mí. El siguiente 45% de los encuestados escogió la opción B: "lo tengo conmigo o cerca de mi gran parte del día". El último 7% escogió la opción C: "Sólo lo tengo conmigo o cerca de mí una parte del día".

Teniendo en cuenta que en la encuesta también existía la opción de no responder, estos resultados concluyen que si las aplicaciones quisieran grabar audio mediante el micrófono en segundo plano, o en primer plano, con respecto a la población que previamente da acceso al micrófono, casi la totalidad de los individuos, se verían proporcionalmente afectados.

Mientras más tiempo, más población, y más autorizaciones se concedan a las apps, mayor será la probabilidad de que la cantidad de datos manejados, tanto la voz en sí, como datos personales que se revelen a partir de las grabaciones de audio, sea mayor, y estos se vean tratados por las mismas.

Para confirmar que es posible el escenario donde diferentes datos tanto de carácter personal, como de carácter sensible[47] puedan tener lugar en las conversaciones, se preguntó sobre lo que suelen hacer los encuestados con respecto a su móvil, durante el desarrollo de conversaciones con amigos, familiares o su respectiva pareja. El 70% respondió que bloquea el teléfono y no lo usa, pero lo mantiene cerca. El 19% respondió que hacía uso del móvil mientras se llevaba a cabo la conversación. El 10% aseguró que además de bloquearlo lo apartaba lejos de sí. Y Sólo un 1% respondió que lo apagaba.

[47] Como por ejemplo: datos sobre origen étnico o racial, opiniones políticas, las convicciones religiosas o filosóficas, o sobre la afiliación sindical.

Más de la mitad de encuestados, pueden verse en el transcurso de una conversación, comprometidos con su privacidad, al revelar información personal o íntima, mientras portan sus móviles y los mantienen a una distancia corta, en el caso de que ocurra una grabación de segundo plano. Al mismo tiempo 19 de cada 100 personas, podrían ser objeto de una grabación tanto en segundo plano, como en primer plano.

Para completar estos escenarios de riesgo que enfrentan los usuarios al no poder siquiera conocer concretamente el tratamiento que llevan a cabo las aplicaciones mediante el micrófono, en el año 2016, un grupo de expertos de la empresa inglesa Pen Test Partners, en colaboración con BBC News, pusieron a prueba este dilema[48]. Los expertos Ken Munro y David Lodge crearon una aplicación capaz de escuchar las conversaciones, y transcribirlas con la finalidad de combinarla con servicios de publicidad. Ambos aseguraron que el proceso[49] perfectamente posible y con conocimientos en programación se puede conseguir un resultado similar. La aplicación tuvo algunos fallos, que sin embargo eran salvables si se empleaba más tiempo en su perfeccionamiento.

6. Tratamiento de un dato biométrico

Como ya se ha expuesto antes, la voz clasifica como dato biométrico, siendo esto determinante para evaluar las bases legitimadores para su tratamiento. No pudiendo fundamentarse en alguna de las razones enumeradas en el artículo 6 del RGPD de las que resulta lícito el tratamiento de un dato personal no sensible.

Es por ello que no se puede ejecutar un tratamiento de un dato como la voz, por razones como la ejecución de un contrato[50], como el que podría derivarse de una aceptación de la política de privacidad, o bien para la satisfacción de intereses legítimos perseguidos por el responsable[51], al necesitar acceso al micrófono para ejecutar alguna de las funciones de la app.

El artículo 9 del RGPD, como regla general, prohíbe el tratamiento de datos sensibles como lo son los datos biométricos. A su vez la LOPD obedece esta prohibición y aplica las mismas excepciones que el Reglamento en el caso de datos biométricos.

[48] BBC News. (2016). *Is your smartphone listening to you?*
[49] *How we made the listening-in Android app.* (2016). [Blog].
[50] Artículo 6. Apartado primero, letra b) del RGPD
[51] Artículo 6. Apartado primero, letra f) del RGPD

Este tipo de datos podrán tratarse bajo el consentimiento explícito por parte del interesado, o bien cuando se presente alguno de los supuestos en los que el legislador ha decidido admitirlo. Estos últimos van desde situaciones dentro del ámbito de Derecho laboral hasta circunstancias en los que se presente un interés público. Sin embargo, el tratamiento que realizan las aplicaciones no tiene la oportunidad de legitimarse en otra base distinta al consentimiento explícito previo para tratar datos procedentes del micrófono o geolocalización[52]. Posteriormente, estos datos pueden ser utilizados si surge alguna de las situaciones que enmarca el artículo, por ejemplo: cuando el tratamiento resulta necesario para el ejercicio o la defensa de reclamaciones en el marco de un procedimiento judicial, o bien se den razones de interés público.

Unido a esto último, el consentimiento ha sido defendido incluso en la Directiva 2002/58/CE[53], cuando se trate de datos que se materializan a través de los servicios de comunicaciones electrónicas, quedando prohibido todo tipo de tratamiento, incluyendo las grabaciones, la escucha o almacenamiento, a excepción del consentimiento del interesado. Este artículo refuerza la idea de que cualquier tipo de intervención sobre datos que emerjan de comunicaciones en aplicaciones, como el acceso al micrófono para grabar y captar el audio, para enviar mensajes de voz, debe quedar protegido al amparo de la decisión del usuario interesado.

7. Consentimiento y sus características

El RGPD en el artículo 4. 11, establece el consentimiento como "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"

El consentimiento es el fundamento jurídico por excelencia y más aún en el caso de los datos biométricos. Permite al interesado tener control sobre sus datos, teniendo en

[52]"*Dada la sensibilidad del procesamiento de los datos o pautas de datos de localización, el consentimiento fundamentado previo constituye también el principal factor aplicable para dar legitimidad al tratamiento de datos en lo que se refiere al procesamiento de las localizaciones de un dispositivo móvil inteligente en el contexto de servicios de la sociedad de la información*." Dictamen 13/2011 del Grupo de Trabajo del Artículo 29 «sobre los servicios de geolocalización en los dispositivos móviles inteligentes» p. 14.

[53] Articulo 5. Directiva 2002/58/CE del parlamento europeo y del consejo de 12 de julio de 2002 «relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas»

cuenta de que se trata de una decisión que puede implicar limitar un derecho fundamental. Para su validez debe contar con una serie de requisitos, de lo contrario, supondrá una falsa ilusión de poder sobre sus datos. Sin embargo, en la práctica, muchas veces supone un acto en vano[54]. En vista de ello, cuando se introdujo el RGPD este procuró incluir tres medidas que aseguraran el consentimiento del interesado como una verdadera manifestación de la voluntad.

La primera de ellas, fue la delimitación de la definición de consentimiento como un acto de aceptar, por medio de una declaración o una clara acción afirmativa[55]. El considerando 32 excluye las casillas premarcadas, el silencio o la inacción como modos de prestar consentimiento, que antes se consideraban legítimas.

En segundo lugar, el desarrollo del concepto de granularidad por el Grupo de Trabajo del 29 que deriva de la interpretación de la exigencia del consentimiento específico y libre, apoyándose en el considerando 43.

Por último la adición del principio de privacidad desde el diseño o privacidad por defecto, un principio que ha ido adquiriendo cada vez más importancia después de la adopción de la "Resolución sobre la Privacidad por Diseño" en el año 2010 por parte de la 32ª Conferencia Internacional de Comisionados de Protección de Datos y Privacidad, llegando a incluirse en el artículo 25 del Reglamento. Un principio que demanda la protección de datos personales durante todo el ciclo del tratamiento, incluyendo las primeras etapas de desarrollo[56].

7.1 Manifestación de voluntad libre

Según el GT 29, libre hace referencia a la oportunidad de elección y control del interesado. A pesar de las demás características que implica la *manifestación de voluntad libre*, para analizar las políticas de privacidad de las apps, se tendrá en cuenta desde el punto de vista de la disociación de los fines del tratamiento.

Un consentimiento libre implica la facultad del interesado para manifestar un consentimiento separado para cada finalidad que implican los tratamientos de datos.

[54] Así ha sido evidente en la encuesta anteriormente mencionada, al momento de realizar la siguiente pregunta: "Cuando descargas una aplicación en tu móvil ¿lees las condiciones y la política de privacidad que se muestra al inicio? A la que el 86% afirmó no leer las condiciones y la política de privacidad. Véase los resultados de la encuesta en el anexo 12

[55] Artículo 4, número 11) del RGPD

[56] Agencia Española de Protección de Datos. (2019). *Guía de Privacidad desde el Diseño*

Según el considerando 32 del RGPD, el consentimiento debe darse para todas las actividades del tratamiento que tengan el mismo o los mismos fines. Sin embargo cuando existan varios fines distintos, que es lo que suele suceder con las apps, el interesado debe poder decidir con que finalidad quiere que se traten sus datos. De esto se trata la granularidad, de un consentimiento diferenciado[57] y separado para cada uno de los tratamientos que ostenten distintas finalidades[58], de lo contrario no se prestaría libremente. Tiene que existir una disociación de fines, para que el usuario tenga la libertad de controlar el destino de sus datos.

Defendiendo esta idea, el considerando 43, entiende que no es válido el consentimiento cuando el proceso o el procedimiento que proporciona el responsable no permite autorizar aisladamente cada una de las distintas acciones de tratamiento[59] pese a ser adecuado. De manera que existe una presunción de que el consentimiento no se ha dado libremente cuando no se dé esta granularidad.

Si bien, no se trata de excluir la posibilidad de recoger un único consentimiento para varias operaciones. Teniendo en cuenta el considerando 32 y 43 del RGPD, ello sería posible siempre y cuando estas operaciones compartan el mismo fin. Por lo tanto, este deber de granularidad, exige a los desarrolladores de aplicaciones facilitar tantas solicitudes de consentimiento como fines haya.

Desafortunadamente, esta exigencia no se cumple en la práctica. Comúnmente se acepta en bloque los tratamientos que las apps pretenden realizar, por medio de enunciados como "He leído y acepto la Política de privacidad" o "Acepto los términos y condiciones generales de la Política de privacidad". Este método no obedece al concepto de granularidad[60], no es una manifestación de voluntad libre[61], cuando el tratamiento presente distintos fines cuya base legitimadora debe ser el consentimiento.

---

[57] "Se trata de un consentimiento que no fuera un todo o nada"… Teniendo la posibilidad de "aceptar unas condiciones y rechazar otras" Vilasau Solana, M. (2019). Capítulo VI. El consentimiento general y de menores. In A. Rallo Lombarte, *Tratado de protección de datos* (1st ed., pp. 206-208). Valencia: Tirant lo Blanch.

[59] "Se presume que el consentimiento no se ha dado libremente cuando no permita autorizar por separado las distintas operaciones de tratamiento de datos personales pese a ser adecuado en el caso concreto" cdo. 43. RGPD

[60] Así en el dictamen 02/2013 no considera un tratamiento granular a la aceptación de "*una larga serie de términos y condiciones y/o de su política de privacidad."*

[61] "…*Si el responsable del tratamiento ha combinado varios fines para el tratamiento y no ha intentado obtener el consentimiento para cada fin por separado, no puede considerarse que haya libertad*."

En un principio cuando descargamos Instagram por primera vez, al igual que como mencionamos con WhatsApp, al usar una función que requiere del micrófono o la cámara, emerge una ventana que solicita el acceso al micrófono, se presupone que el consentimiento sobre los datos derivados de estos recursos, se acuerda exclusivamente para los fines mencionados en el recuadro, siendo este el único momento en todo el ciclo de tratamiento que se nombra explícitamente el micrófono. Sin embargo estos no son los únicos fines para los que la aplicación tiene acceso, cuando se acepta la política de privacidad de Instagram[62].

En el apartado primero sobre qué tipo de información se recopila, se incluye la información sobre el dispositivo, como aquellos datos que provienen de los permisos que el usuario activa a través de la configuración del móvil[63], entre ellos, el micrófono. La política de privacidad, indica que dichos datos, se utilizarán para "mejorar la personalización de contenido", o las "funciones que ves cuando usas nuestros Productos… o bien con el fin de detectar si has realizado alguna acción en respuesta a un anuncio que te hemos mostrado en el teléfono u otro dispositivo."[64]. De la misma manera, los datos del micrófono también entremezclados con el resto de los fines mencionados en la política, como lo son: proporcionar y personalizar sus productos[65], proporcionar mediciones, análisis y otros servicios para empresas[66], fomentar la seguridad, la integridad y la protección[67] y enviar mensajes de marketing[68], debido a las expresiones utilizadas, como "toda la información que disponemos", resulta razonable

---

Directrices del Grupo de Trabajo del Artículo 29 (2017) «sobre el consentimiento en el sentido del Reglamento (UE) 2016/679», p. 11.

[62] Data Policy | Facebook Help Centre. (2018).

[63] Ídem. En la política indica como ejemplos "*como el acceso a la ubicación de GPS, la cámara y las fotos*". No siendo estos los únicos. El micrófono es igualmente un acceso que se activa por medio de la configuración correspondiente en el dispositivo, cumpliendo las mismas características, por lo tanto se ve afectado bajo la rúbrica de este apartado.

[64] Ídem.

[65] Ídem. "Utilizamos la información de la que disponemos para ofrecer nuestros productos para personalizar las funciones y el contenido, proporcionar sugerencias… (incluidos aquellos datos de categorías especiales que decidas facilitarnos y para los cuales nos concedas tu consentimiento explícito)". Este inciso abarca el acceso al micrófono.

[66] Ídem. "Usamos la información que tenemos con objeto de ayudar a los anunciantes y otros socios a medir la eficacia y la distribución de sus anuncios y servicios". el fragmento: "información que tenemos", incluye la información obtenida del acceso al micrófono.

[67] Ídem. "Utilizamos la información de la que disponemos para verificar cuentas y actividades, combatir conductas perjudiciales, detectar y prevenir spam y otras experiencias negativas, conservar la integridad de nuestros Productos y fomentar la seguridad tanto dentro como fuera de los Productos de Facebook." Instagram dispone de datos procedentes del micrófono.

[68] Ídem. "Usamos la información a nuestra disposición para enviarte mensajes de marketing, darte a conocer nuestros Productos e informarte acerca de nuestras políticas y condiciones. También la utilizamos para responderte cuando te pones en contacto con nosotros."

pensar que estos fines se emplearan para justificar el tratamiento de todos los datos recogidos.

El consentimiento de estas finalidades se materializa en la aceptación general de la política de privacidad, no habilitando al interesado a dar un consentimiento separado y diferenciado para cada fin. De modo que la utilización de datos derivados del micrófono, como la voz, y otros datos sensibles, para ofertar publicidad acorde ellos, se encontraría cubierta por su política de privacidad.

Teniendo en cuenta estos parámetros, el GT 29[69], afirma que una aplicación de móvil de edición de fotografías, que solicita a los usuarios la activación de la localización GPS para utilizar sus servicios y para demás fines de publicidad comportamental, no es un consentimiento libre. Debido a que ambas finalidades son distintas entre sí, requieren un consentimiento autónomo.

Podría pensarse que en estos casos existe un consentimiento granular gracias a que se solicita el consentimiento del interesado en dos ocasiones: una en un primer momento con la aceptación de la política de privacidad, y en un segundo momento cuando se solicita el acceso. Sin embargo, la solicitud de acceso al micrófono no supone ser una capa independiente y diferenciada de la primera. No se puede aceptar el acceso al micrófono exclusivamente para enviar mensajes de voz o grabar vídeos, sin aceptar el resto de finalidades primero.

La solicitud de acceso al micrófono es una condición necesaria para llevar a cabo el tratamiento conforme a los fines de la política de privacidad, y no una segunda solicitud de consentimiento para un tratamiento totalmente distinto y adicional. No se trata de un consentimiento granular, sino de un mismo tratamiento que es autorizado dos veces.

El consentimiento separado del micrófono no resultaría libre, debido a la carga de cláusulas anteriores a las que se sujeta el usuario[70]. Si bien existen dos posibilidades de consentimiento, esto no significa que el sistema protege más al usuario. La primera, no consagra un consentimiento diferenciado e independiente del segundo, sino todo lo contrario. Al aceptar la política de privacidad, ya se ha otorgado un consentimiento para

[69] Directrices del Grupo de Trabajo del Artículo 29 (2017) «sobre el consentimiento en el sentido del Reglamento (UE) 2016/679» p. 6.
[70] Al entender que los datos procedentes del micrófono y su tratamiento, se encuentran incluidos en los fines que se muestran en las políticas de privacidad de Instagram y Whatsapp.

tratar los datos obtenidos por el micrófono, y que se ejecutará una vez que el usuario haya aceptado el acceso[71].

7.2 Manifestación de voluntad específica.

El big data es pionero en formular nuevos usos a los datos[72]. Una vez obtenidos, el tratamiento puede servir para cubrir distintas necesidades de una empresa, y acumular varios enfoques y finalidades. Para asegurar el control del interesado sobre sus datos, es necesario que el consentimiento sea específico según el artículo 6 apartado 1, letra a) del Reglamento. Esto quiere decir que cuando el responsable recoge el consentimiento del usuario, debe precisarse de forma clara y exacta, tanto de la extensión como los motivos del tratamiento, conforme a los cuales se llevará a cabo.

Esta característica está relacionada con el principio del limitación del la finalidad del artículo 5.1b), que exige que los fines del tratamiento deben ser determinados, explícitos y legítimos. Por lo que deben plantearse con anterioridad al tratamiento y aportar una comprensión inequívoca[73]. Debe quedar suficientemente esclarecido que tipo de datos personales y según que procesamientos son tratados, pudiendo distinguir aquellos datos que no están incluidos.[74]

Al mismo tiempo, este principio protege al interesado ante la posible manipulación ulterior de los datos, contraria a los fines consentidos por el interesado y los cambios repentinos en las políticas de privacidad. La descripción de los propósitos del tratamiento por el responsable, comprende una auto-limitación, que prescribe el marco por el cual va a dirigirse a la hora de realizar el tratamiento. Sin embargo, este marco debe delimitarse adecuadamente.

Si una aplicación decide emplear los datos para funciones o fines incompatibles a los previamente consentidos, el responsable del tratamiento deberá solicitar nuevamente el consentimiento del interesado. Para los desarrolladores de aplicaciones supone una exigencia que implica asumir grandes costes, en ocasiones inviables. Por lo cual se ven forzados a incluir una descripción vasta y vaga del tratamiento, para así tener un amplio

[71] Segunda ocasión de consentimiento
[72] "precisamente, el valor del big data reside en que la nueva información que se crea permite dar nuevos usos a los datos." GIL, E. (2016). *Big data, privacidad y protección de datos*, p. 62.
[73] Puente Escobar, A. (2019). Capítulo IV. Principios y licitud del tratamiento. In A. Rallo Lombarte, *Tratado de protección de datos* (1st ed.). Valencia: Tirant lo Blanch.
[74]Opinion 03/2013 by Article 29 Data Protection Working Party «on purpose limitation», p. 15.

margen de apreciación sobre las operaciones que podrían encajarse en su política de privacidad. Sin embargo esto no obedece a un consentimiento específico. El consentimiento no puede recogerse para aceptar un conjunto impreciso de actividades como la fórmula: "mejorar nuestros productos"[75].

Al conocer y comprender la finalidad del tratamiento, el usuario crea una expectativa[76], a partir de cual el principio de minimización de datos[77] cobra vida. El tratamiento debe basarse únicamente en aquellos datos que son necesarios para cumplir con las finalidades del tratamiento, y evitar aquellos que resulten excesivos. Para ello la finalidad debe estar determinada, para identificar los márgenes y los límites del principio de minimización de datos.

Debe tratarse de una finalidad que requiera precisamente de un tratamiento de datos personales para conseguirse, de modo que no quepa lograrse sin el respectivo procesamiento de estos datos. En el caso de Instagram, se acoge entre sus finalidades, la personalización de contenido, ofreciendo publicidad en la aplicación. Resultaría excesivo utilizar los datos provenientes del micrófono para ofrecer publicidad personalizada, al poder alcanzar este propósito mediante otros datos que la app dispone, que han sido consentidos por el usuario, como lo es el historial de búsqueda. No resulta pertinente o necesario para la aplicación, y su tratamiento implicaría una vulneración al principio de minimización de datos, al existir otros mecanismos que implican una menor intromisión[78] a la intimidad, que son igualmente eficaces.

De la misma manera, resulta excesivo el tratamiento realizado por una aplicación, que posibilita funcionar a través de comandos de voz, si la captación de audio, se ejecuta continuamente, o en segundo plano. En el Dictamen 02/2013 se plantea el ejemplo de un tratamiento excesivo, cuando una aplicación de alarma, al tener la función de detener su sonido mediante un comando de voz, ella se aproveche del acceso al micrófono para grabar continuamente en momentos en los que la alarma no esté programada.

---

[75] Ibíd, p. 16: For these reasons, a purpose that is vague or general, such as for instance 'improving users' experience', 'marketing purposes', 'IT-security purposes' or 'future research' will - without more detail - usually not meet the criteria of being 'specific'.

[76] Ibíd, p. 13. "If a purpose is sufficiently specific and clear, individuals will know what to expect: the way data are processed will be predictable."

[77] Artículo 5.1. c) RGPD

[78] La AEPD, en la resolución contra La Liga, entiende que el tratamiento de datos personales obtenidos a través del micrófono, es uno de los tratamientos más intrusivos que existe, p. 55.

La minimización exige que los desarrolladores de aplicaciones traten únicamente aquellos datos que resulten idóneos[79] para cumplir con el propósito. Deben tratarse de datos pertinentes y adecuados en función de los fines. La utilización de una aplicación, no puede quedar limitada a la aceptación de tratamientos inncesarios para proporcionar sus servicios[80]. El consentimiento, no puede resultar un salto al vacío, por lo que se requiere un análisis del principio de minimización caso por caso.

Una manifestación específica de la voluntad, también es fiel a la granularidad, pese a lo cual, compañías como WhatsApp Inc.[81] afirman que un consentimiento específico no exige que el usuario deba aceptar o prestar su consentimiento a cada una de las operaciones del tratamiento para este ser válido, de acuerdo con los criterios del GT 29. WhatsApp defendió en el año 2016 su política de privacidad de ser específica puesto que recoge de forma clara el tratamiento que se lleva a cabo.

La granularidad como elemento del consentimiento específico no había sido desarrollado de forma sustancial en el dictamen 02/2013. La granularidad encajaba de manera más obvia en la libertad del usuario. El elemento "específico" del consentimiento se relacionaba más con un deber de suministrar información detallada sobre los propósitos y datos que abarcaba el tratamiento, en vez de reflejarse en la forma en la que el consentimiento es recogido.

Hasta entonces, un único consentimiento era apropiado para conceder varias operaciones, siempre y cuando fuere lo razonable, de tal forma que la granularidad en la forma de dar consentimiento específico era evaluada caso por caso, y no como una exigencia intrínseca.

Actualmente el GT 29 se asegura de que no quede duda que la granularidad es un requisito que debe respetarse tanto para otorgar un consentimiento libre como un consentimiento específico[82], acorde a la Guía sobre el consentimiento del año 2017[83]. El consentimiento no sólo debe obedecer a una descripción clara y precisa sobre los fines

[79] Puente Escobar, A. (2019). Capítulo IV. Principios y licitud del tratamiento. In A. Rallo Lombarte, *Tratado de protección de datos*

[80] Agencia Española de Protección de Datos. (2019). *el deber de informar y otras medidas de responsabilidad proactiva en apps para dispositivos móviles.* [PDF] p. 2.

[81] Véase la Resolución del PS núm. 00219/2017 del 6 de junio de 2018

[82] "Consent mechanisms must not only be granular to meet the requirement of 'free', but also to meet the element of 'specific'. This means, a controller that seeks consent for various different purposes should provide a separate opt-in for each purpose, to allow users to give specific consent for specific purposes." Article 29 Working Party, *Guidelines on consent under Regulation 2016/679.* (2017), p. 2.

[83] Ídem.

del tratamiento, sino que debe recogerse separadamente para cada uno de los fines. La aceptación de una serie de términos y condiciones de la política de privacidad de las aplicaciones, además de carecer del elemento "libre", tampoco resulta una manifestación específica.[84]

Para que una aplicación pueda recoger un consentimiento granular, debe recogerse "de forma selectiva e independiente para los distintos tratamientos y finalidades"[85] La solicitud de acceso al micrófono, no es más específica, ni goza de mayor granularidad, puesto que es codependiente de la política de privacidad. El permiso al micrófono, no excluye el resto de tratamientos con finalidades distintas[86], que se concretan a lo largo de la política de privacidad. Por consiguiente la fórmula utilizada no cumpliría con un consentimiento específico.

A modo de conclusión, la mayoría de aplicaciones que circulan en las tiendas de aplicaciones, incluyendo las más descargadas, Instagram y Whatsapp, utilizan constantemente esta técnica para recabar el consentimiento. Demandando primero la aceptación a la totalidad de las condiciones de la política de privacidad, y después solicitando el acceso a los recursos del móvil. Agrupan todos los objetivos y propósitos en la aceptación de la política de privacidad, sin existir casillas o un formato que permita segregar el consentimiento. Dichas prácticas, no cumplen con los estándares de granularidad que se presentan en la guía.

En sus políticas de privacidad, siempre se menciona el tratamiento respectivo a la geolocalización, sin embargo se omite el micrófono. Nos queda únicamente posicionarlo en aquellas expresiones como: "toda la información que disponemos", distorsionando la idea que tenemos sobre el uso que realiza una app sobre nuestro micrófono.

No resultan claras y precisas las consecuencias del consentimiento sobre el tratamiento de los datos del micrófono, distintas de la función para grabar vídeos o mensajes de voz, y si ellas implican la utilización de estos datos, conforme los fines de la política de

[84]Según el dictamen 2/2013, en su página 18, el GT 29 considera "El planteamiento alternativo de que los desarrolladores de aplicaciones pidan a sus usuarios la aceptación de una larga serie de términos y condiciones y/o de su política de privacidad no constituye autorización específica".

[85] Agencia Española de Protección de Datos. (2019). *el deber de informar y otras medidas de responsabilidad proactiva en apps para dispositivos móviles, p. 2.*

[86] Como lo son la personalización de contenido, análisis y otros servicios para empresas, seguridad, marketing, etc.

privacidad mencionados, como la personalización de publicidad. Desde este punto de vista, tampoco resulta un consentimiento específico.

En cuanto al principio de limitación de la finalidad, para conocer que usos subsecuentes podrían resultar contrarios a los fines autorizados, es indispensable entender sin lugar a duda cuales son estos fines. De esta forma el principio se ve vulnerado desde el momento en el que la información es suministrada, y ella no facilita una comprensión inequívoca al usuario, y a efecto dominó, no podría determinarse las operaciones que resultan afines o contrarias.

Más allá de si se considera que la información y el formato que presentan estas aplicaciones, es adecuada o no para garantizar un consentimiento específico, y cumplir con el principio de limitación de finalidad, lo cierto es, que el principio de minimización de datos, avala en cualquier caso, que la utilización de los datos obtenidos a través del micrófono para fines como personalización de publicidad resultarían excesivos, vulnerando el artículo 5.1. c).

7.3 Manifestación de voluntad informada.

Para prestar consentimiento válido[87], el usuario debe disponer de la información sobre el tratamiento, para poder tomar una decisión. El interesado debe ser capaz de construir un juicio sobre lo que implica el tratamiento y sus consecuencias, a partir de la información facilitada, de manera que conozca claramente las intervenciones que se llevarán a cabo a sus datos personales. Por esta razón la información siempre debe ser anterior al consentimiento, y evidentemente a cualquier tratamiento[88].

Este elemento de la definición de consentimiento está vinculado con el principio de transparencia del artículo 5.1 a), de manera que en el artículo 12 del RGPD se define lo que implica la transparencia de la información. Según este precepto, el responsable del tratamiento es quien tiene el deber de proporcionar información pertinente y necesaria, siguiendo los artículos 13 y 14 del reglamento.

Si bien no se específica en el RGPD el formato o los mecanismos por los cuales debe presentarse la información, concediendo una mayor libertad al responsable para

[87] Artículo 4.11 RGPD

[88] "there must always be information before there can be consent." Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent, p. 19.

adaptarse a las necesidades del tratamiento, ello no significa que está exento de respetar algunos requisitos para cumplir con el deber de informar y recabar un consentimiento informado.

Para que el consentimiento se considere informado, debe suministrarse al menos la identidad del responsable del tratamiento y los fines para los que será tratado cada dato personal[89]. La información debe ser clara, con un lenguaje sencillo, transparente, inteligible según lo dispuesto en el considerando 32.

"El «consentimiento específico» está intrínsecamente relacionado con el hecho de que el consentimiento debe estar informado."[90]. Para dar un aceptar cualquier intervención hacia los datos personales, y comprender las finalidades y el respectivo tratamiento, es esencial que el usuario disponga de la información íntegra y pertinente. En consecuencia, no sólo debe proporcionarse información, sino que ella debe ser suficiente para conceder consentimiento específico.

Debe ser lo suficientemente amplia para que el usuario pueda tomar una decisión, pero a la vez justa para no causar fatiga visual y sobrecarga informativa. Así los desarrolladores de apps hallan "una tensión entre facilitar información completa y hacerlo de forma concisa, transparente, inteligible y de fácil acceso… El responsable del tratamiento debe analizar de qué modo priorizar la información que debe facilitarse y los métodos de transmisión de la información apropiados"[91]. Por lo que el GT 29 recomienda que la información sea administrada a multinivel, es decir, por capas, mediante enlaces, íconos o etiquetas que permitan entrar más en detalle a cada apartado de la política de privacidad. Mas estas medidas presentan complicaciones, al ser un escape para los desarrolladores de aplicaciones para disminuir aquella información pertinente. En vista de ello el GT 29 se ocupó de elaborar una guía para el cumplimiento del deber de informar[92], en el cual describe que el modelo de información por capas consiste en presentar en un primer nivel, información básica y esencial, que contenga la identidad del responsable, la finalidad y los derechos del interesado según el artículo 11 LOPDGDD, y un segundo nivel que se encargue de ampliarla detalladamente, de

[89] Cdo. 42 RGPD
[90] Resolución de PS núm. 00219/2017 del 6 de junio de 2018, p. 66.
[91] VILASAU SOLANA, M. Ibíd. p. 9.
[92] Agencia Española de Protección de Datos. (2019). *el deber de informar y otras medidas de responsabilidad proactiva en apps para dispositivos móviles*

manera que los usuarios puedan navegar en la política de privacidad entre los distintos apartados y completar dicha información.

Asimismo, en un análisis de flujos de información sobre los dispositivos Android[93] se prevé la posibilidad que se incluyan avisos o notificaciones, para acceder a aquellos sensores que pueden aportar datos sensibles, sin embargo, estos no dejan de ser cuadros de diálogo que tan sólo informan de una cuarta parte del tratamiento que estas apps puede llevar a cabo en virtud de estos accesos.

Si bien la información por capas, es un mecanismo eficiente para cumplir con el principio de transparencia, no hay que confundir las ampliaciones de información mediante enlaces e hipervínculos, con las notificaciones que solicitan consentimiento explícito para utilizar los recursos del dispositivo. El cuadro de diálogo que emerge para solicitar el acceso al micrófono o la cámara, no amplían la información contenida en la política de privacidad, ni completa elementos que fueron resumidos en la información básica de la política de privacidad, sino que describen un tratamiento con una finalidad nunca antes mencionada: la grabación de audio para enviar mensajes de voz y vídeos[94], vulnerando desde esta perspectiva, el deber del artículo 13, teniendo que haber informado toda necesidad o finalidad que tuviese la aplicación para acceder a este sensor, en la política de privacidad[95]

Estos avisos o notificaciones, más que una segunda capa de información, son fuentes para recabar el consentimiento explícito, cuya "información mostrada no es suficiente en el contexto del RGPD ni la granularidad del permiso se precisa de forma correcta"[96]. Es por ello que el usuario depende de la política de privacidad para conocer precisamente el tratamiento que se le va a aplicar a los datos derivados del acceso al micrófono. Sin embargo, la palabra "micrófono" no se encuentra en ningún apartado de la política de privacidad de Instagram. No se incluye ni en la información básica, ni es especificada en segundas capas, ni siquiera en el apartado de categoría especial de datos

[93] Agencia Española de Protección de Datos, (2020). *Análisis de los flujos de información en android herramientas para el cumplimiento de la responsabilidad proactiva*

[94]Puesto que en la política de privacidad tanto de WhatsApp como de Instagram, no mencionan que el acceso del micrófono permite enviar mensajes voz y vídeos, sino que se informa mediante el cuadro de diálogo.

[95] Agencia Española de Protección de Datos. (2019). *el deber de informar y otras medidas de responsabilidad proactiva en apps para dispositivos móviles,* p. 5.

[96] Ídem.

que tratan. Se omite el permiso del micrófono cuando se mencionan los datos de la configuración del dispositivo. Por otro lado, en la política de privacidad de WhatsApp, el acceso al micrófono tampoco es mencionado en ningún momento, únicamente el tratamiento y el almacenamiento que ocurre sobre los mensajes de voz[97].

Si bien el artículo 13 del RGPD ni el artículo 11 de LOPDGDD especifica que una de las informaciones que el responsable debe suministrar es informar sobre los datos que en sí se recogen, esta carencia sí vulnera el principio de transparencia, puesto que según el considerando 39, debe quedar totalmente claro, para las personas que se están tratando sus datos personales, así como también el considerando 60 requiere que se informe sobre la existencia de la operación. Ambas aplicaciones fallan en este principio, puesto que no queda absolutamente claro el tratamiento y la habilitación de los datos del micrófono. Así como también sumerge al usuario en una incertidumbre temporal sobre los periodos en los que se efectúa y se activa dicho tratamiento.

En la resolución de la AEPD contra La Liga, se evidencia la necesidad de adaptar el principio de transparencia ante un tratamiento tan intrusivo como lo es la captación de datos por el micrófono, al igual como sucede en las aplicaciones mencionadas. El micrófono recoge datos que por sus características, además de la voz como dato biométrico, resultan desconocidos e inciertos para el usuario, en el momento el que este da su consentimiento en virtud de que se trata de datos "dinámicos y cambiantes"[98] por su propia naturaleza. No se trata de un dato específico, sino de una "categoría de datos siendo ajeno a esta situación el propio interesado". Esto quiere decir, que además de recoger la voz como dato biométrico, se puede llegar a recoger una categoría de datos más amplia con el paso del tiempo, por ejemplo datos sensibles, que se revelan de una conversación, al discutir información sobre la religión, ideología, origen racial, salud o vida sexual del propio interesado.

Según el considerando 60, el responsable debe facilitar toda la información complementaria que sea necesaria para garantizar un tratamiento transparente, en función de las circunstancias especificas del tratamiento, por lo que en este caso, se requiere un esfuerzo adicional por parte del responsable, implantando medidas

[97] Para tratar los mensajes de voz, previamente debe haber un acceso al micrófono, cuya habilitación supone un tratamiento por sí mismo. Los mensajes de voz son el resultado de un tratamiento ulterior al acceso: bien almacenamiento, transformación, o conversión.
[98] Resolución contra La Liga, p. 66.

apropiadas para cumplir con el principio de transparencia y recoger un consentimiento informado.

Como ya se ha mencionado antes, una captación continua de información a través del micrófono, incluso fuera de la app, se consideraría contraria al principio de minimización de datos. Ante ello, las aplicaciones de Instagram y WhatsApp, no recogen información sobre los momentos en los que se producirá la activación o utilización de este recurso. De manera que el instante en el que se consiente el acceso al micrófono, no tiene por qué coincidir con el momento en el que esta función se activa, a menos de que se trate de una continúa recogida de datos desde que se accede. Así como la app de La Liga, dichas aplicaciones aportan información insuficiente en sus políticas, provocando una inseguridad sobre el espacio temporal del tratamiento, que sólo puede ser "minorada"[99] mostrando algún ícono o señal que permita al usuario conocer que en ese preciso momento se están recogiendo o captando sus datos, incluso si ello ocurre en segundo plano. Esta recomendación también se prevé en el dictamen 10/2004 planteando la posibilidad de completar la información con íconos o notificaciones en tiempo real, de manera que sean "claros y autoexplicativos", medida que suele cumplirse tanto en iOS como en Android, cuando se produce el tratamiento de la geolocalización. Siguiendo esta recomendación, se cumpliría plenamente el considerando 39[100].

En el año 2017 samsumg lanzó la versión Android 8.0 Oreo. Como novedad incluía un monitor de permisos de aplicaciones, en los ajustes del móvil, que posibilita al usuario ver un historial de actividad sobre los accesos que las aplicaciones han utilizado a lo largo del mes, en segundo plano[101]. Al activar esta función de monitor, el sistema operativo se encarga de enviar al usuario una notificación cuando algún recurso o sensor, previamente concedido, se esté ejecutando fuera de la app. De esta manera el usuario puede conocer si la aplicación ha realizado un uso o tratamiento excesivo sobre sus datos.

Fue encontrado un comentario publicado en febrero de 2020 de un usuario del sistema Android, que reclamaba información sobre el monitor de permisos de app, adjuntando

[99] Ídem, p. 56.
[100] "Para las personas físicas debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados." Cdo. 39 RGPD
[101] Véase el anexo 13.

una captura de pantalla[102] en donde se podía apreciar que en el historial de permisos dos aplicaciones: Instagram y WhatsApp Business, realizaron uso de la cámara y micrófono respectivamente, en segundo plano, indicando la fecha y hora del tratamiento.

Actualmente, las versiones anteriores y posteriores a Android 8.0, no incluyen esta función en los ajustes del móvil, al igual que todas las versiones del sistema operativo de Apple. Si bien los fabricantes de los sistemas operativos y dispositivos determinan la extensión y el grado de acceso que tienen las aplicaciones a los sensores, de modo que sólo se dispongan los datos que resultan necesarios, los fabricantes en este caso no están obligados a ofrecer al usuario, la información referente al tratamiento, sino los propios desarrolladores de la aplicación.

7.4 Consentimiento explícito

Al estar en presencia de datos sensibles, el consentimiento para ellos debe suponer un esfuerzo adicional en comparación al resto de datos, debido al elevado riesgo que estos presentan para la intimidad, teniendo que cumplir con las características del artículo 4.11) del RGPD, debe ser libre, específico, informado e inequívoco, pero además según el artículo 9 del RGPD el consentimiento debe ser explícito para romper con la prohibición del tratamiento de datos biométricos.

No obstante, debido a que el actual RGPD añadió el elemento "inequívoco", no queda claro, en que se diferencia este requisito con respecto a un consentimiento explícito. Debido a que un consentimiento inequívoco requiere en sí una acción afirmativa, y el consentimiento explícito, es sinónimo de expreso[103].

En todo caso, el consentimiento explícito no quiere decir que el consentimiento deba recabarse mediante firma, bien electrónica, o bien hecha a mano, sino que además una acción afirmativa, se trata de una manifestación en la que quede claramente expresada su voluntad para aceptar cierto tratamiento de sus datos[104]. Debe ser una respuesta dada

[102] Véase el anexo 14.
[103] «In legal terms "explicit consent" is understood as having the same meaning as express consent. » Opinion 03/2013 «on purpose limitation», p. 25.
[104] Ibíd. P. 26. "individuals may give explicit consent, orally and also in writing, by engaging in an affirmative action to express their desire to accept a form of data processing. In the on-line environment explicit consent may be given by using electronic or digital signatures. However, it can also be given through clickable buttons depending on the context, sending confirmatory emails, clicking on icons, etc"

a una petición de tratamiento, con respecto a un uso particular, que exprese el acuerdo o el desacuerdo directo con la pregunta realizada[105].

La aceptación de la política de privacidad de una aplicación, en la que prevean una variedad de finalidades y usos, no corresponde con esta exigencia, puesto que no se contesta a una solicitud específica sobre un uso particular, sino a una multitud de usos. El consentimiento no sería así una respuesta inmediata de una petición, sino varas peticiones de tratamiento.

8. Conclusión.

Dentro del análisis expuesto, en vista de la subestimación que se le da a la voz como dato personal, tanto por usuarios como por desarrolladores de apps, se puede afirmar, que los accesos a los recursos y sensores de los dispositivos móviles, son efectivamente formas de tratamiento. La voz, es un dato biométrico como un formato para sostener otro tipo de datos, tanto personales, como sensibles. La posibilidad de tener acceso a datos personales, es más que suficiente para tener en cuenta esta operación como tributaria de las garantías y deberes que enmarcan el RGPD.

En vista popularización del formato estudiado, como método por defecto, para recabar el consentimiento para el tratamiento de datos personales, es importante tener en cuenta, que la aceptación de una política de privacidad con distintos fines, no proporciona un consentimiento válido cuando no exista la oportunidad de segregar y optar por separado cada fin. Asimismo, un consentimiento otorgado ante unos fines confusos, y abstractos, no permitirán al usuario formar juicio para tomar una decisión, por lo que el consentimiento no resultará específico, ni informado, por lo que no podrá cumplirse con el principio de limitación de la finalidad, tanto desde el punto de vista de compresión, como por el hecho de no poderse definir que usos resultan contrarios a los propios fines. Ni bien, que usos sobrepasan lo que se considera adecuado.

La precisión en las políticas de privacidad, se hace más necesaria que nunca, en virtud de los nuevos usos y nuevas fuentes de datos que existen actualmente, gracias a los dispositivos móviles, su uso generalizado y sus sensores disponibles. El tratamiento que

[105] Ibíd. P. 25. "It encompasses all situations where individuals are presented with a proposal to agree or disagree to a particular use or disclosure of their personal information and they respond actively to the question"

se realiza mediante el micrófono, debe ser examinado con lupa, y no conformarse con el mero roce de algunas medidas, sino su total cumplimiento.

9. Bibliografía.

MATERIAL BIBLIOGRÁFICO

- ACED, E., HERAS, R., & SÁIZ, C. A. (2017). *Código de buenas prácticas en protección de datos para proyectos big data.* Agencia Española de Protección de Datos. <https://www.aepd.es/sites/default/files/2019-09/guia-codigo-de-buenas-practicas-proyectos-de-big-data.pdf>
- AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, (2020). *Análisis de los flujos de información en android herramientas para el cumplimiento de la responsabilidad proactiva*. p.6. <https://www.aepd.es/sites/default/files/2019-09/estudio-flujos-informacion-android.pdf>
- GAMBA, J., RASHED, M., RAZAGHPANAH, A., TAPIADOR, J., & RODRIGUEZ, N. (2019). *NOTA TÉCNICA Avance del estudio de IMDEA NETWORKS y UC3M: "Análisis del Software Pre-instalado en Dispositivos Android y sus Riesgos para la Privacidad de los Usuarios"*. Madrid. <https://www.aepd.es/sites/default/files/2019-09/nota-tecnica-IMDEA-android.pdf>
- GARRIGA DOMÍNGUEZ, A. (2016). *Nuevos retos para la protección de datos personales. En la Era del Big Data y de la computación ubicua*. Dykinson
- GIL, E. (2016). Big data, privacidad y protección de datos. *Madrid: Agencia Estatal Boletín Oficial del Estado*.
- PUENTE ESCOBAR, A. (2019). Capítulo IV. Principios y licitud del tratamiento. In A. Rallo Lombarte, *Tratado de protección de datos* (1st ed.). Valencia: Tirant lo Blanch.
- TRAMULLAS, J; OLVERA-LOBO, M (2001). *Recuperación de la información en Internet*. Madrid, Ra-Ma.
- VILASAU SOLANA, M. (2019). Capítulo VI. El consentimiento general y de menores. In A. Rallo Lombarte, *Tratado de protección de datos* (1st ed., pp. 206-208). Valencia: Tirant lo Blanch.

REGULACIÓN CONSULTADA

- Dictamen 02/2013 del Grupo de Trabajo del artículo 29 «sobre aplicaciones de los dispositivos inteligentes». <https://www.aepd.es/sites/default/files/2019-12/wp202_es.pdf >
- Dictamen 13/2011 del Grupo de Trabajo del Artículo 29 «sobre los servicios de geolocalización en los dispositivos móviles inteligentes». <https://www.apda.ad/sites/default/files/2018-10/wp185_es.pdf>
- Dictamen 4/2007 del Grupo de Trabajo del artículo 29 «sobre el concepto de datos personales» <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf>
- Directiva 2002/58/CE del parlamento europeo y del consejo de 12 de julio de 2002 «relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas». <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32002L0058&from=ES>
- Directrices del Grupo de Trabajo del Artículo 29 «sobre el consentimiento en el sentido del Reglamento (UE) 2016/679», (2017). Disponible en <https://www.avpd.euskadi.eus/contenidos/informacion/20161118/es_def/adjuntos/wp259rev01__es20180709.pdf>
- *Guidelines on consent under Regulation 2016/67. By* Article 29 Data Protection Working Party. (2017).
- Opinion 03/2013 by Article 29 Data Protection Working Party «on purpose limitation»<https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf>
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Boletín Oficial del Estado 19 de enero de 2008, núm 17. < https://www.boe.es/eli/es/rd/2007/12/21/1720/con >
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos. <https://www.boe.es/doue/2016/119/L00001-00088.pdf>

INFORMES JURÍDICOS CONSULTADOS

- Informe jurídico 0139/2017 del 14 de septiembre de 2017, del Gabinete jurídico. <https://www.aepd.es/es/documento/2017-0139.pdf>
- Informe jurídico 190/2009 del 4 de enero de 2010, del Gabinete Jurídico. <https://www.aepd.es/es/documento/2009-0190.pdf>

JURISPRUDENCIA

- Resolución del PS núm. 00329/2018 del 20 de Agosto de 2019 <https://asociaciondpd.com/wp-content/uploads/2019/07/PS-00326-2018_ORI.pdf>
- SAN del 29 de noviembre de 2018 <http://www.poderjudicial.es/search/openCDocument/d6c3141dd81d8758599e4e9439214f914de783790fa0c08f >
- STS del 18 de junio de 2020 <https://supremo.vlex.es/vid/845571671?from_fbt=1&fbt=preview&fallbackURLB64=aHR0cDovL3N1cHJlbW8udmxleC5lcy92aWQvODQ1NTcxNjcx >

RECURSOS ELECTRÓNICOS

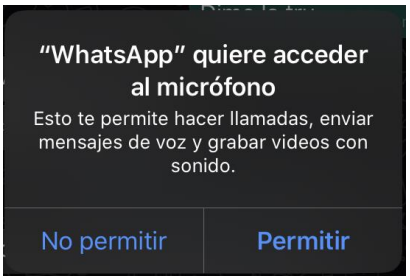
- Agencia Española de Protección de Datos. (2019). *el deber de informar y otras medidas de responsabilidad proactiva en apps para dispositivos móviles.* [PDF]. Madrid. Obtenido en: https://www.aepd.es/sites/default/files/2019-11/nota-tecnica-apps-moviles.pdf
- Agencia Española de Protección de Datos. (2019). *Guía de Privacidad desde el Diseño* [PDF] Obtenido de: <https://www.aepd.es/sites/default/files/2019-11/guia-privacidad-desde-diseno.pdf>
- BBC News. (2016). Is your smartphone listening to you? <https://www.bbc.com/news/technology-35639549>
- Data Policy | Facebook Help Centre. (2018). Obtenido de: < https://help.instagram.com/519522125107875>
- Descripción general del manifiesto de una app. (2020). Obtenido en: <https://developer.android.com/guide/topics/manifest/manifest-intro?hl=es-419>
- Guía para el procesamiento en segundo plano. (2020). Obtenido de: <https://developer.android.com/guide/background>

- How we made the listening-in Android app. (2016). [Blog]. Obtenido en: https://www.pentestpartners.com/security-blog/how-we-made-the-listening-in-android-app/

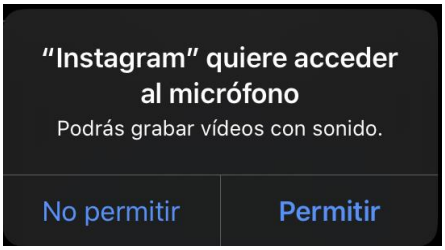
10. Anexos.

Anexo 1 Captura de pantalla en sistema iOS en la aplicación WhatApp.

Anexo 2. Captura de pantalla en sistema iOS en la aplicación WhatsApp

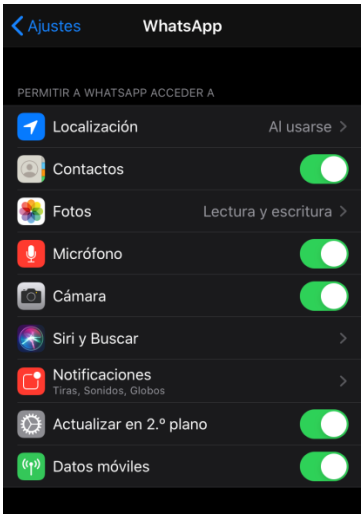


Anexo 3. Captura de pantalla en sistema iOS en la aplicación WhatsApp

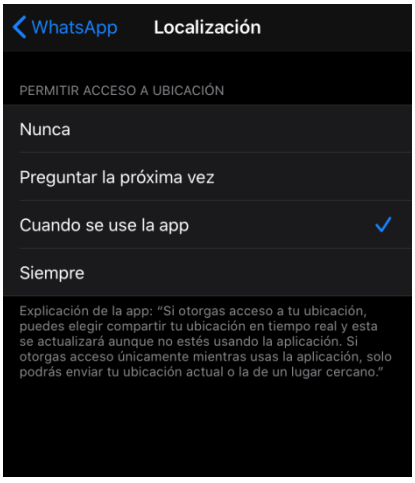


Anexo 4. Captura de pantalla en sistema Android en la aplicación WhatsApp

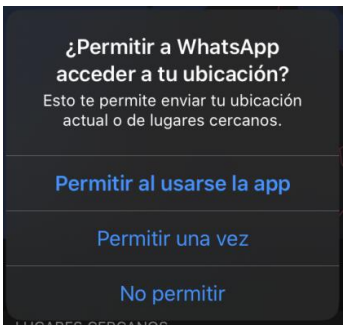
Anexo 5. Captura de pantalla en sistema iOS en la aplicación Ajustes



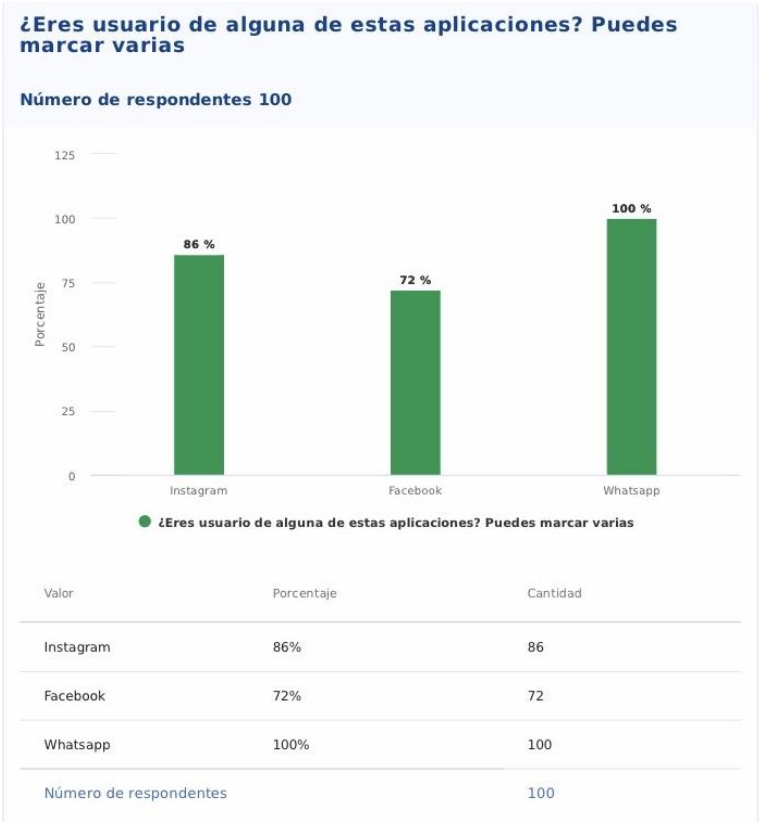
Anexo 6. Captura de pantalla en sistema iOS en la aplicación Ajustes



Anexo 7. Captura de pantalla en sistema iOS desde la aplicación WhatsApp



Anexo 8. Resultados de encuesta realizada a través de la plataforma encuesta.com

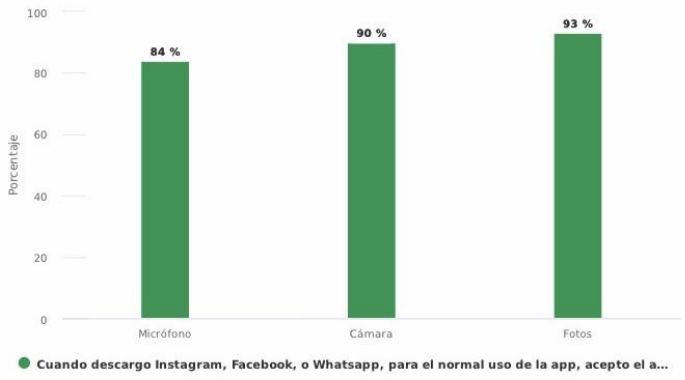


Valor	Porcentaje	Cantidad
Instagram	86%	86
Facebook	72%	72
Whatsapp	100%	100
Número de respondentes		100

Anexo 9. Resultados de encuesta realizada a través de la plataforma encuesta.com

Cuando descargo Instagram, Facebook, o Whatsapp, para el normal uso de la app, acepto el acceso a:Por favor marcar todos a las funciones que se da acceso

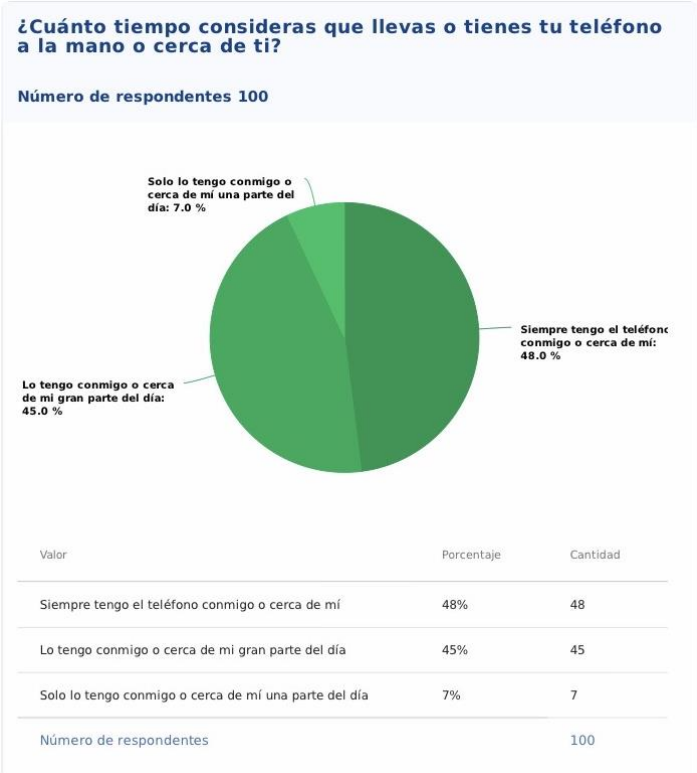
Número de respondentes 90



Cuando descargo Instagram, Facebook, o Whatsapp, para el normal uso de la app, acepto el a...

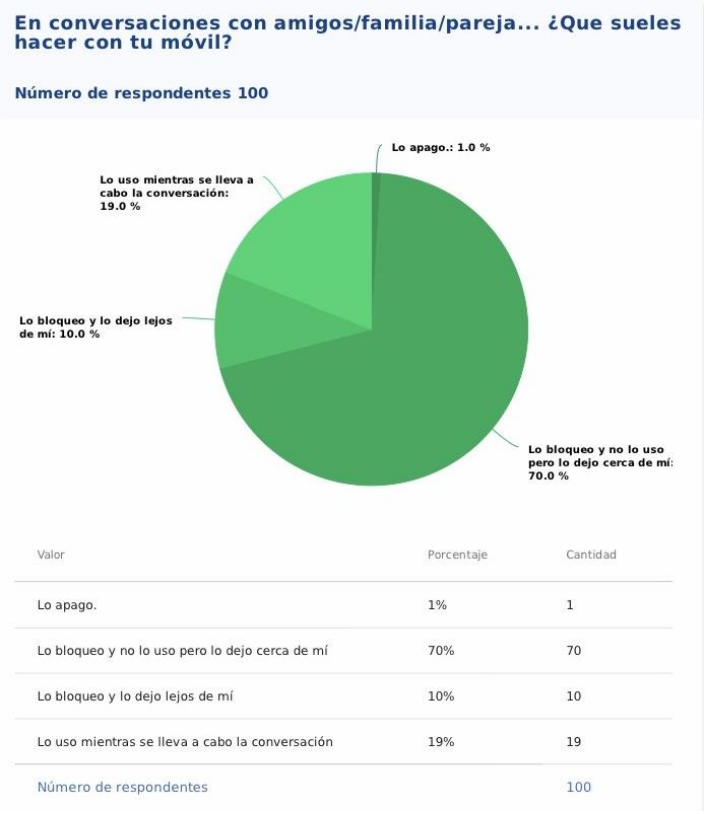
Valor	Porcentaje	Cantidad
Micrófono	84%	76
Cámara	90%	81
Fotos	93%	84
Número de respondentes		90

Anexo 10. Resultados de encuesta realizada a través de la plataforma encuesta.com



Valor	Porcentaje	Cantidad
Siempre tengo el teléfono conmigo o cerca de mí	48%	48
Lo tengo conmigo o cerca de mi gran parte del día	45%	45
Solo lo tengo conmigo o cerca de mí una parte del día	7%	7
Número de respondentes		100

Anexo 11. Resultados de encuesta realizada a través de la plataforma encuesta.com

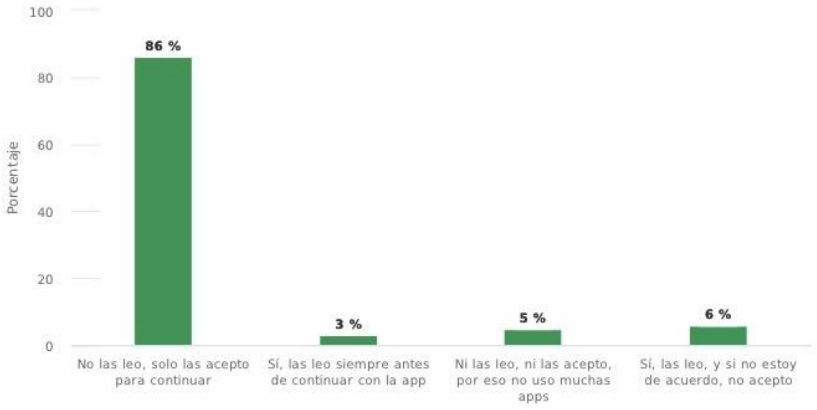


Valor	Porcentaje	Cantidad
Lo apago.	1%	1
Lo bloqueo y no lo uso pero lo dejo cerca de mí	70%	70
Lo bloqueo y lo dejo lejos de mí	10%	10
Lo uso mientras se lleva a cabo la conversación	19%	19
Número de respondentes		100

Anexo 12. Resultados de encuesta realizada a través de la plataforma encuesta.com

Cuando descargas una aplicación en tu móvil ¿lees las condiciones y la política de privacidad que se muestra al inicio?Elige sólo una respuesta

Número de respondentes 100



Cuando descargas una aplicación en tu móvil ¿lees las condiciones y la política de privacidad q...

Valor	Porcentaje	Cantidad
No las leo, solo las acepto para continuar	86%	86
Sí, las leo siempre antes de continuar con la app	3%	3
Ni las leo, ni las acepto, por eso no uso muchas apps	5%	5
Sí, las leo, y si no estoy de acuerdo, no acepto	6%	6
Número de respondentes		100

Anexo 13. Monitor de permisos Android

Anexo 14