MONOGRÁFICO

Documentación de las **Ciencias** de la **Información**
ISSN-e: 1988-2890

EDICIONES COMPLUTENSE

https://dx.doi.org/10.5209/dcin.77256

Aplicaciones de *deepfakes*. Manipulación de contenido audiovisual y riesgos para los usuarios basados en las políticas de privacidad[1]

Juan-José Boté-Vericad[2], Mari Vállez[3]

Recibido: 11 de julio de 2021 / Aceptado: 14 de septiembre de 2021

Resumen. El crecimiento de las noticias falsas provoca en los usuarios inseguridad cuando consumen información. Los formatos de noticias de tipo de textual son quizás los más extendidos, aunque, el vídeo está irrumpiendo con fuerza y se ha transformado en contenido informativo que puede manipularse y llevar a la desinformación de los usuarios. En este artículo, se analizan 63 aplicaciones para dispositivos móviles que permiten generar *deepfakes*. Se examinan las *app*s utilizando 16 indicadores clasificados en tres dimensiones: descripción de la aplicación, tratamiento de la imagen y protección de datos. Cada aplicación tiene sus particularidades respecto a la modificación de la fisionomía de una persona, en especial la cara. En algunos casos podría cuestionarse la legalidad de las aplicaciones, ya que pueden incidir en los derechos fundamentales de las personas. Se observa en los resultados que en muchos casos no se informa al usuario de la tecnología que emplean las aplicaciones ni los tipos de datos que se recogen. Se concluye que las *apps* permiten generar vídeos falsos manipulando la fisionomía de las personas, aunque hay una falta importante de información sobre las políticas de privacidad de los datos que recogen. Además, el uso de estas aplicaciones puede llegar a dañar la imagen o prestigio de una persona, e incluso suplantar su identidad.
Palabras clave: *Deepfake*; desinformación; manipulación de vídeos; *apps*; aplicaciones móviles.

[en] Deepfakes applications. Manipulation of audiovisual content and risks for users based on privacy policies

Abstract. The growth of fake news makes users insecure when they consume information. While text-based news is perhaps the most widespread, video is gaining ground quickly, and has been transformed into informative content that can be manipulated, leading to misinformation among users. This article analyses 63 applications for mobile devices that enable the creation of deepfakes. An analysis of the apps is carried out by examining 16 indicators across three dimensions: description of the application, treatment of the image, and data protection. Each application has its peculiarities regarding the modification of the physiognomy of a person, especially their face. In some cases, the legality of the applications is questionable as they can impact people's fundamental rights. The results demonstrate that, in many cases, the user is not informed of the technology used by the applications, nor the types of data that are collected. In conclusion the apps allow the generation of fake videos by manipulating the physiognomy of people, however, there is a lack of information surrounding the privacy policies of the data they collect. In addition, the use of these applications can damage the image and/or reputation of a person and even supplant their identity.
Keywords: *Deepfake*; disinformation; video manipulation; apps; mobile applications.

Cómo citar: Boté-Vericad, J.-J; Vállez, M. (2021). Aplicaciones de *deepfakes*. Manipulación de contenido audiovisual y riesgos para los usuarios basados en las políticas de privacidad, en *Documentación de las Ciencias de la Información*. 45 (1), 25-32.

1. Introducción

Generar noticias falsas o *fake news* en forma de texto, imágenes o vídeo aumenta día a día, y en algunas ocasiones ha llegado a ser un problema para que la ciudadanía esté informada correctamente de lo que ocurre. Algunos ejemplos notables son la transmisión de mensajes falsos con motivo de la aparición de la COVID-19 a través de aplicaciones de mensajería instantánea (Atehortua y Patino, 2021) o la genera-

[1] «Narración interactiva y visibilidad digital en el documental interactivo y el periodismo estructurado». RTI2018-095714-B-C21 (MICINN/FEDER), Ministerio de Ciencia, Innovación y Universidades (España).

[2] Departament de Biblioteconomia, Documentació i Comunicació Audiovisual & Centre de Recerca en Informació, Comunicació i Cultura. Universitat de Barcelona. C/ Melcior de Palau 140, 08014 ES, Barcelona.
E-mail: juanjo.botev@ub.edu
ORCID: http://orcid.org/0000-0001-9815-6190.

[3] Departament de Biblioteconomia, Documentació i Comunicació Audiovisual & Centre de Recerca en Informació, Comunicació i Cultura. Universitat de Barcelona. C/ Melcior de Palau 140, 08014 ES, Barcelona.
E-mail: marivallez@ub.edu
ORCID: http://orcid.org/0000-0002-3284-2590.

ción de noticias falsas desde Macedonia (Hughes y Waismel-Manor, 2021).

Las *fake new*s son mayoritariamente textuales; no obstante, también se manipulan imágenes o vídeos que son conocidas como *deepfakes*. Definimos *deepfake* como la generación de contenido audiovisual engañoso o falso mediante la manipulación de imágenes, sonidos o vídeos. Este contenido generado estará descontextualizado en cuanto a tiempo, forma o lugar.

Las *deepfakes* integran diferentes tipos de contenidos (imágenes, vídeos y audios) que, entrelazados, permiten crear un vídeo falso. Así, las *deepfake*s pretenden engañar al usuario manipulando un personaje o incluso creando una animación. Se trata de una personalización que se realiza con tecnología audiovisual que trabaja en diferentes niveles, como pueden ser la cara, la voz, el movimiento de los labios o las posturas. A pesar de que hay aplicaciones que permiten generar *deepfakes* a un coste reducido, crear vídeos profesionales, que realmente engañen al público, tiene un coste elevado, ya que supone la participación de expertos de diferentes áreas, como lingüistas, montadores de vídeo o especialistas en animación.

En los medios de comunicación, existen mecanismos que ayudan a identificar la información manipulada. En el caso de las *fake news*, se emplean filtros de verificación para la comprobación de hechos *(fact-checking*); y en las *deepfakes*, se utiliza el análisis biométrico o la tecnología *blockchain* (Hasan y Salah, 2019); sin embargo, hay que destacar que estas pueden suponer un elevado coste.

Por razones técnicas, tiene menos dificultad cambiar una fotografía que un vídeo. La imagen es estática y carece de elementos que pertenecen a la anatomía de la persona, como la voz o el movimiento. En el caso del vídeo, hay que señalar dificultades añadidas como las ya mencionadas, así como la resolución del propio vídeo, el formato digital del vídeo o el tiempo de duración. En la manipulación de imágenes, hay diferentes técnicas que se han empleado tradicionalmente. Quizás, la más conocida es la técnica de *morphing*, que surgió a partir de los años setenta para aplicaciones aeroespaciales. Consiste en transformar una imagen A en una imagen B y viceversa, mediante una metamorfosis (Ivakhiv, 2016).

En el entorno de los vídeos, existe tecnología más avanzada proveniente de la inteligencia artificial, en la que se pueden integrar otros aspectos, como la voz o el movimiento de los labios. Sin embargo, esta técnica todavía tiene ciertas limitaciones técnicas, como se observa en el vídeo que se creó por parte de *Future Advocacy* y *UK Artist Bill Posters*, donde Boris Johnson y Jeremy Corbin se respaldaban mutuamente en su candidatura a primer ministro del Reino Unido (BBC News, 2019). Al realizar este vídeo, se pudo observar cómo se pueden llegar a socavar aspectos tan importantes como la democracia. Aplicar estos cambios a un vídeo o a una fotografía en un contexto informativo, como una noticia, puede implicar que estos no sean percibidos o queden anulados por el prestigio de la fuente.

Este artículo persigue dos objetivos. El primero es analizar las aplicaciones para dispositivos móviles que permitan modificar contenido audiovisual y que, como resultado, generen material falso o *deepfake*. El segundo objetivo es estudiar las políticas de privacidad facilitadas por las apps en cuanto a la recogida de datos de los usuarios, ubicación y tratamiento de la información. En este contexto, el artículo responde a las siguientes preguntas de investigación:

- ¿Qué tipo de aplicaciones podemos encontrar para dispositivos móviles que permitan manipular la fisonomía de una persona en un vídeo?
- ¿Qué sucede con los datos que generan y recogen las aplicaciones?

El trabajo se estructura en cinco apartados, contando con esta introducción inicial. A continuación, se realiza una revisión de la bibliografía a modo de marco teórico de referencia para el tema de este trabajo. En la siguiente sección se describe la metodología utilizada para la obtención, el refinado y la normalización de los datos. Después se presentan los resultados obtenidos, seguido por un apartado dedicado a discutir los resultados. Por último, se acaba con las conclusiones obtenidas a raíz del análisis realizado y las limitaciones del estudio presentado.

2. Revisión de la literatura

En esta sección se analizan distintos aspectos que inciden de forma directa o indirecta en las *deepfakes.* Estos ámbitos son las técnicas de manipulación de imágenes o vídeos, los mecanismos existentes para detectar vídeos manipulados y la importancia de las políticas de privacidad.

2.1. Técnicas de manipulación de imágenes y vídeos

La principal técnica utilizada para manipular imágenes o vídeos es la denominada *morphing*. Esta consiste en identificar patrones entre dos fotografías para transformar una imagen en otra, sin ser una imagen que se mueva, sino que tiene su propio movimiento ya que va de un punto A un punto B (Ivakhiv, 2016; Scherhag et al., 2017). Esta técnica permite, por ejemplo, cambiar una cara por otra, integrando la cara de una persona en otra, o bien crear caricaturas mediante la exageración de características faciales. También ha tenido aplicaciones muy diversas, y un ejemplo son las grandes producciones del cine, como Indiana Jones y la última cruzada, que fue una de las primeras películas en utilizarla (Puerto, 2018). En el campo de la psicología, la técnica *morphing* se emplea para la percepción de la identidad o de la expresión (Kramer et al., 2017). A medida que la tecnología ha ido

evolucionando, y con ello su mejora de resultados, se plantean desarrollos de esta técnica con elementos 3D, por ejemplo, en expresiones faciales (Tang y Ni, 2019).

Otra de las técnicas existentes es el *warping,* que permite cambiar digitalmente la forma de las partes de una imagen con propósitos creativos para corregir sus distorsiones (Prathap *et al.,* 2016). Esta técnica tiene diferentes aplicaciones, como generar caricaturas a través de la exageración de rasgos personales. Además, esta técnica se emplea en el campo de la salud en la radioterapia (Veiga *et al*., 2015) o en la fotografía para la corrección de imágenes panorámicas en cámaras deportivas (Li, *et al.*, 2015). También ofrece soluciones para la postproducción de imágenes, que se acostumbran a utilizar para mejorar la estética de las fotos de las redes sociales (Islam *et al.*, 2017; Krylov *et al.*, 2014).

2.2. Detección de vídeos manipulados

De la misma forma que hay herramientas para contrastar noticias falsas textuales, también es posible encontrar herramientas que detecten vídeos falsos. Estas herramientas tienen un alto componente tecnológico, con un gran coste económico en su desarrollo. Se pueden encontrar diferentes propuestas tecnológicas con este objetivo, como puede ser el uso de redes neuronales recurrentes, donde se aprovechan las inconsistencias entre fotogramas del vídeo creado, y así se detecta si un vídeo está o no manipulado (Güera y Delp, 2018). También, en otro estudio, se detectó mediante el análisis de grandes conjuntos de datos que muchos vídeos falsos presentaban caras que no parpadeaban, lo que contribuyó a poder generar un *software* de detección de vídeos falsos (Li *et al.*, 2018). Además, se propone el uso de análisis multimedia forense como forma de asegurar la autenticidad de un vídeo y su origen (Rossler *et al.*, 2019).

No existe una solución definitiva para detectar un vídeo falso que manipule una persona, pero se plantea disponer de herramientas que dificulten o impidan crear nuevos tipos de vídeos falsos (Nguyen et al., 2019). También los análisis mediante métodos basados en algoritmos de aprendizaje automático o *machine learning* pueden aportar soluciones, como el análisis de frecuencias de imágenes, que permite identificar diferentes comportamientos dentro de un vídeo. Así pues, mediante el uso de tecnología avanzada es posible detectar vídeos falsos.

2.3. La importancia de las políticas de privacidad

Las políticas de privacidad en las aplicaciones móviles deberían servir para informar a los usuarios sobre el uso que se realiza de la información que el usuario facilita. Muchas aplicaciones comparten información con terceros, y los usuarios deben ser informados. Sin embargo, estas políticas no siempre son claras, y en algunos casos pueden poner en riesgo a la reputación individual del usuario o incluso su salud (Parker *et al.*, 2019). Los autores realizan un análisis sobre 61 *apps* vinculadas a la salud mental, donde encontraron que el 41 % de las aplicaciones analizadas no tenían políticas de privacidad para informar a los usuarios sobre cómo su información se recogía para terceras partes.

A su vez, en un estudio en la India, también en el ámbito de la salud, se analizaron un total 70 *apps* comparando la complejidad en la lectura de las políticas de privacidad entre aplicaciones de salud mental y diabetes (Powell *et al.*, 2018). En la investigación, se determinó que las políticas de privacidad estaban escritas para usuarios con un nivel universitario y que esta complejidad en la interpretación podría ser una barrera para tomar decisiones. En otro estudio realizado sobre 369 *apps* en salud mental, se determinó que, en las políticas de privacidad, la información no era transparente para los usuarios. Las aplicaciones eran demasiado genéricas y requerían un nivel de alfabetización universitario para su comprensión (Robillard *et al.*, 2019).

Por su parte, Zimmerle y Wall (2019), propusieron unas guías para evaluar las políticas de privacidad en las aplicaciones móviles para niños, así como para sus sitios web. Los autores definieron los elementos clave que se han de ofrecer en las políticas de privacidad: descripción de todos los datos personales que se recogen, detalle del uso que pueden realizar terceras partes de la información recogida, especificación de las opciones de control parental que pueden ejercer los padres/tutores y, por último, un enlace bien visible hacia las políticas de privacidad.

3. Metodología

Para realizar esta investigación, se han analizado las aplicaciones gratuitas para dispositivos móviles que permitían realizar modificaciones de la cara o que indicaban claramente en su descripción que creaban *deepfakes*. Además, las aplicaciones tenían que generar como resultado un objeto digital en formato GIF o en un formato de vídeo como MP4. Para ello, se ha escogido la plataforma Google Play (Google Play, 2020) que ofrece *apps* para dispositivos móviles. A pesar de la gran cantidad de aplicaciones que se pueden encontrar, Google Play no dispone de una opción de búsqueda avanzada de aplicaciones en su interfaz ni una búsqueda combinada con operadores booleanos o por diferentes campos. Esto puede generar cierto sesgo informacional cuando se buscan aplicaciones para dispositivos móviles. Una de sus posibles consecuencias es que una búsqueda abierta puede dar resultados inesperados, por lo que se decidió que el proceso de búsqueda se haría mediante búsquedas de términos exactos.

Para este proceso mediante términos exactos, se determinaron las siguientes palabras clave: *Deep Fake, DeepFake, FaceSwap, Face Swap, DeepFake*

Video, FaceSwap Video. Estos términos se emplean tanto en medios de comunicación como en literatura científica. En la Figura 1 se recoge el número de aplicaciones existentes para cada término de consulta en Google Play:

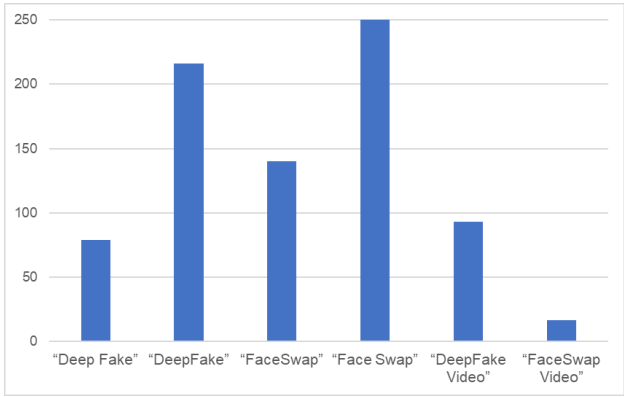

Figura 1. Términos de búsqueda y número de aplicaciones. Fuente: Elaboración propia.

Para poder llevar a cabo el análisis, se definieron un conjunto criterios de inclusión que las aplicaciones debían cumplir:

- permitir la manipulación de la fisionomía de una persona, bien cambiado la voz o partes del cuerpo, como la cara;
- generar un vídeo o un GIF como objeto digital final;
- eran gratuitas;
- indicaban en su título o ficha de descripción las palabras clave de búsqueda que la aplicación realizaba como cambios de cara o *deepfakes*.

Una vez que se obtuvieron los resultados junto con los criterios de selección, se registraron las aplicaciones en una hoja de cálculo de Microsoft Excel, y se generaron diferentes hojas para cada búsqueda. A partir de aquí se creó una lista definitiva, descartando las aplicaciones repetidas. También se realizó un análisis de cada una de ellas mediante la lectura del título y de la descripción, y se eliminó aquellas que no cumplían los criterios de inclusión fijados.

El proceso de búsqueda y registro se realizó del 1 de abril de 2020 al 15 de abril de 2020. Se seleccionaron 86 aplicaciones. En junio de 2021 se realizó una nueva revisión de las aplicaciones seleccionadas. Se encontró que algunas de ellas ya no existían y la muestra final de análisis se redujo a 63 *apps*.

Para analizar las apps se han establecieron 16 indicadores clasificados entre tres dimensiones, basándose en los criterios definidos en estudios previos citados en el marco teórico.

Tabla 1. Dimensiones e indicadores utilizados para valorar las aplicaciones. Fuente: Elaboración propia.

Dimensiones	**Indicadores**
Descripción de la aplicación	Ind.1 - Descripción de la tecnología Ind. 2 - Salida en formato vídeo o GIF Ind. 3 - Puntuación en Google Play Ind. 4 - Permiso de descarga o compartición Ind. 5 – País de la aplicación
Tratamiento de la imagen	Ind. 6 - Tipo de cambios morfológicos Ind. 7 - Modificación de la imagen de otros usuarios Ind. 8 - Tratamiento de una o más imágenes
Protección de datos	Ind. 9 - Uso de la aplicación por menores Ind. 10 - Proceso en servidor local o en remoto Ind. 11 - Recopilación de información personal Ind. 12 - Indicación sobre la recogida de rasgos faciales Ind. 13 - Conservación del material gráfico creado Ind. 14 - Geolocalización del usuario Ind. 15 - Recopilación de datos del dispositivo móvil Ind. 16 - Política de privacidad

4. Resultados

A continuación, se muestra el análisis de las aplicaciones a través de las tres dimensiones señaladas en la Tabla 1. De cada aplicación se han analizado los indicadores mostrados, por lo que se ha generado un conjunto de datos que están disponibles con licencia de acceso abierto (Boté-Vericad y Vállez, 2021).

4.1. Descripción de la aplicación

En esta dimensión se analizan las características básicas de las aplicaciones que suelen utilizarse para decidir su instalación. En la Tabla 2 se muestran los detalles de los tres primeros indicadores. En el indicador 1 se observa que son minoría (N=15, 23,8 %) aquellas aplicaciones que indican el tipo de tecnología que emplean para producir la modificación de la imagen: realidad aumentada, inteligencia artificial y *morphing*. Por su parte, en el indicador 2, solo 1 aplicación indica que su formato de salida es en GIF, mientras que la mayoría de

ellas (N=46, 73,01 %) informa que su formato de salida es en vídeo. En el indicador 3, se muestran cómo están puntuadas las aplicaciones en la Play Store de Google: G0 sin valoración, G1 puntuación entre 1 y 2, y así sucesivamente. Se observa que la mayor parte de las aplicaciones están valoradas entre el grupo 2, (N=18, 28,57 %) y el grupo 3 (N=25, 39,68 %).

Tabla 2. Agrupación de los indicadores 1, 2 y 3. Fuente: Elaboración propia.

Ind. 1	**N**	**Ind. 2**	**N**	**Ind. 3**	**N**
Realidad aumentada	3	GIF	1	G0	5
Inteligencia artificial	5	Vídeo	46	G1 ≥ 1	4
Morphing	7	V/G	16	G2 ≥ 2	18
Sin datos (n. d.)	48			G3 ≥ 3	25
				G4 ≥ 4	11
Total de *apps*	**63**		**63**		**63**

Al respecto del indicador 4, solo hay una aplicación que no indica ningún tipo de información al respecto de las condiciones para compartir el resultado de la producción. Por último, en el indicador 5 se observa que, en referencia a la procedencia por países, predominan aquellas *apps* que están ubicadas en los Estados Unidos (N=12, 19,04 %) y que un grupo importante de aplicaciones no indican el país (N=18, 25,57 %). Esto se puede observar en la Figura 2.

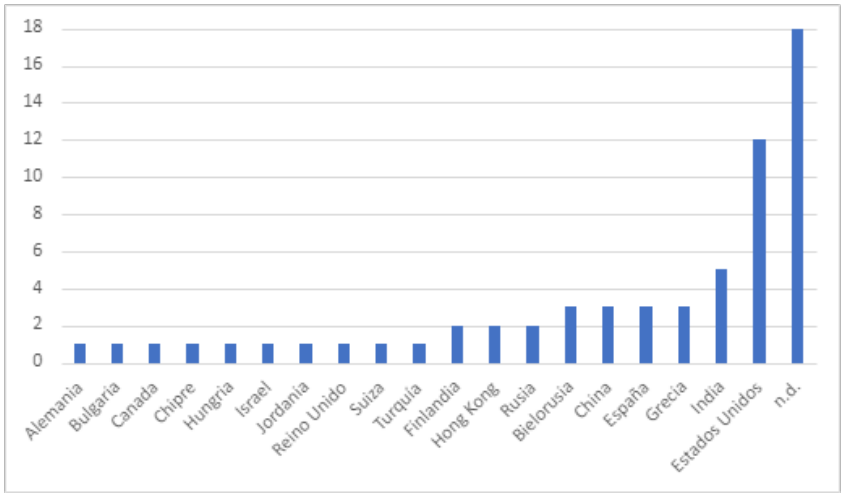

Figura 2. Distribución de las aplicaciones por países.

4.2. Tratamiento de la imagen

En esta dimensión se analiza la información facilitada en referencia a la manipulación que se puede realizar a las imágenes. En la Tabla 3 se muestra la información de los indicadores que forman parte de XXX. En el indicador 6, sobresalen aquellas aplicaciones que permiten transformar el rostro humano (N = 20, 31,74 %), seguidas de las que modifican un rostro humano en una caricatura (N = 15, 23,80 %). Al respecto del indicador 7, destaca que casi todas las *apps* permiten modificar un rostro humano que no sea el propio del usuario de la aplicación (N=62, 98,41 %). Finalmente, en el indicador 8, despuntan aquellas aplicaciones que solo modifican una imagen a la vez (N=55, 87,30 %), por lo que son minoritarias aquellas que permiten la modificación de varias imágenes.

Tabla 3. Agrupación de los indicadores 6, 7 y 8. Fuente: Elaboración propia.

Ind. 6	**N**	**Ind. 7**	**N**	**Ind. 8**	**N**
H	20	Usuario	1	5 imágenes	1
C	15	Otros usuarios	62	2 imágenes	7
H/C/A	4			1 imagen	55
H/A	12				

H/C	12				
Total de *apps*	**63**		**63**		**63**

A = Transformación del rostro en un animal; C = Transformación del rostro en una caricatura; H = Modificación del rostro humano.

4.3. Protección de datos

Esta dimensión es la que cuenta con más indicadores, ya que se estudia desde diversas perspectivas la protección de los datos que son recogidos por las aplicaciones. La información obtenida procede de la lectura de las políticas de privacidad de cada aplicación, recogidas en la Tabla 4 y 5.

En la Tabla 5, el indicador 9 muestra que normalmente no se indica una limitación de edad para este tipo de aplicaciones (N=41, 65,07 %). En el indicador 10, predominan las aplicaciones que no indican si el proceso de manipulación se realiza en un servidor local o remoto (N=57, 90,47 %). En referencia a la recogida de datos personales en el indicador 11, una gran mayoría apunta que sí lo hacen (N=44, 69,84 %).

Tabla 4. Agrupación de los indicadores 9, 10, 11. Fuente: Elaboración propia.

Ind. 9	**N**	**Ind. 10**	**N**	**Ind. 11**	**N**
< 18	5	No	2	No	13
< 13	17	Sí	4	Sí	44
n. d.	41	n. d.	57	n. d.	6
Total de *apps*	**63**		**63**		**63**

En referencia al indicador 12, solo una de las aplicaciones indica que recoge datos faciales, el resto de ellas (N=62, 98,41 %) no apunta nada al respecto.

En la Tabla 5, en el indicador 13, una gran parte de las aplicaciones no indica si se conserva el material gráfico creado por los usuarios (N=34, 53,96 %). De la misma forma, en el indicador 14, una gran parte de las *apps* tampoco apunta si recogen la geolocalización del usuario (N=33, 52,38 %). Finalmente, en el indicador 15, una gran mayoría de las aplicaciones señala que recogen datos del dispositivo móvil (N=51, 80,95 %).

Tabla 5. Agrupación de los indicadores 13, 14, y 15. Fuente: Elaboración propia.

Ind. 13	**N**	**Ind. 14**	**N**	**Ind. 15**	**N**
No	6	No	7	No	1
Sí	23	Si	23	Sí	51
n. d.	34	n. d.	33	n. d.	11
Total de *apps*	**63**		**63**		**63**

En referencia al indicador 16, todas las aplicaciones tenían disponible su política de privacidad en el momento de la recogida de los datos, con la excepción de dos aplicaciones.

5. Discusión

A raíz de los resultados del análisis de *apps* para móviles que generan vídeos falsos y el estudio de sus políticas de privacidad, hay una serie de cuestiones que merecen atención. En primer lugar, en la descripción de la aplicación, aunque se determina en todas ellas el tipo de producto final que se genera, no se puede saber qué tipo de tecnología hay detrás de ella en un alto porcentaje (63 %, N=48). Este aspecto es relevante dado que, en función de la tecnología que se aplique la manipulación, puede ser en mayor o menor intrusiva, lo cual puede generar en las personas sentimientos de vergüenza u otro tipo de daño (Kirchengast, 2020). El hecho de poder modificar un vídeo de forma artificial con tecnología ya supone falsear la propia realidad del vídeo. Esto también puede implicar falsear la percepción del usuario, lo que provoca que el mundo no sea real y comporta un vacío semántico (Wagner y Blewer, 2019). Además, un grupo importante de aplicaciones no indica el país de origen (N=18, 25,57 %). Esto puede deberse a que Google no demanda a los desarrolladores que indiquen dicha información.

En segundo lugar, al respecto del tratamiento de la imagen, si bien se detalla el tipo de tratamiento que se realiza con las imágenes, son aspectos que no se encuentran en las políticas de privacidad y deberían aparecer como información técnica (Bates et al., 2018). Además, las directrices analizadas en las políticas de privacidad de algunas de las apps no facilitan una información completa sobre el uso de los datos del dispositivo móvil. Las políticas de privacidad pueden generar dudas legales en determinados países. En el estudio de Mulder (2019) encontraron que la falta de información respecto a la gestión de los datos del usuario no cumplía con la normativa europea en materia de protección de datos.

En resumen, cuando se emplea este tipo de aplicaciones, cualquier parte del cuerpo es un dato personal. Tal y como se ha visto en la sección de resultados, muchas aplicaciones no indican qué tipos de datos recogen, y dejan al usuario en una incertidumbre legal en función del país en donde se emplee esta aplicación. Además, tampoco se precisa el hecho de que los datos puedan ser cedidos a terceros, como compañías asociadas con los propietarios de la aplicación, o incluso vendidos.

6. Conclusiones

Las aplicaciones destinadas a generar *deepfakes* disponen de un nicho de crecimiento, ya que se ob-

serva que de momento solo permiten transformar el rostro de una persona y no el resto de las partes del cuerpo. Cada vez más el uso de estas aplicaciones se está democratizando, especialmente en lo lúdico. Es cuestión de tiempo que estas aplicaciones se empleen cada vez más, no solo para modificar la fisonomía de una persona, sino también para realizar otro tipo de vídeos que puedan aportar un beneficio social.

Para generar *deepfakes* es necesario disponer de tecnología que permita manipularla fisonomía de una persona, pero también otros elementos, como paisajes o entornos que no tienen por qué ser animados. De este modo, para crear estas apps se precisan personas con un gran nivel de especialización, como lingüistas o especialistas en inteligencia artificial.

Sorprende el hecho de que se puedan recuperar tantas aplicaciones por los términos *deepfake* o *deepfake* video, entre otros, dado que no se observan etiquetas en las fichas de las aplicaciones en Google Play.

Las políticas de privacidad de las aplicaciones deberían ser más precisas en su formulación, ya que se emplean datos personales de los usuarios. El corpus legislativo en el mundo todavía es escaso, si bien en la Unión Europea se están dando los primeros pasos legislativos al respecto de las *fake news* y *deepfakes*. Mediante el empleo de este tipo de aplicaciones, posiblemente se entra en el terreno de los derechos fundamentales, como el derecho a la protección de datos de carácter personal o el derecho a la integridad de la persona (Unión Europea, 2012). En función del uso que se haga de una aplicación, se podría dañar la imagen o prestigio de una persona, e incluso se puede llegar a suplantar su identidad. En un corto espacio de tiempo, vistas las tendencias actuales, los vídeos falsos de todo tipo y situaciones serán mucho más frecuentes. Por tanto, habrá que ser muy cauto en el ámbito jurídico donde se requerirá de personal altamente cualificado y herramientas tecnológicas que ayuden a determinar la veracidad de una pieza audiovisual.

Por último, hay que hacer referencia a las limitaciones del estudio. La primera de ellas es que, en el proceso de búsqueda y revisión de las aplicaciones, a pesar de haber sido exhaustivo, es posible que alguna aplicación no se haya recogido, o que alguna haya desaparecido debido a la volatilidad del mercado. En segundo lugar, el estudio está enfocado en aplicaciones presentes en Google Play que funcionan con el sistema Android, sin incluir las aplicaciones creadas para iOS. En tercer lugar, aunque hay aplicaciones que se promocionan como generadoras de *deepfakes* explícitamente, hay otras que también tienen esta función. No obstante, estas últimas apps son anteriores a la popularización del término *deepfake* que se puede establecer a partir del mes de diciembre 2017 (Google Trends, 2021). Una cuarta limitación es la imposibilidad de acceder a plataformas de zonas geográficas que cuentan con sus propios *markets, como pueden ser los países asiáticos donde existe*n aplicaciones similares que no se han podido analizar.

4. Agradecimientos

Este trabajo forma parte del proyecto «Narración interactiva y visibilidad digital en el documental interactivo y el periodismo estructurado». RTI2018-095714-B-C21 (MICINN/FEDER), Ministerio de Ciencia, Innovación y Universidades (España).

5. Referencias bibliográficas

Atehortua, N. A., y Patino, S. (2021). COVID-19, a tale of two pandemics: Novel coronavirus and fake news messaging. *Health Promotion International, 36*(2), 524–534. https://doi.org/10.1093/heapro/daaa140.

Bates, D. W., Landman, A., y Levine, D. M. (2018). Health apps and health policy: What is needed? *JAMA, 320*(19), 1975–1976. https://doi.org/10.1001/jama.2018.14378.

BBC News. (12 de noviembre de 2019). Are You Fooled by This Johnson-Corbyn Video? *BBC News*. https://www.bbc.com/news/av/technology-50381728/the-fake-video-where-johnson-and-corbyn-endorse-each-other.

Boté-Vericad, J.-J. y Vállez, M. (2021). *Apps* para dispositivos Android que generan *Deepfakes*. [Data set]. https://doi.org/10.5281/zenodo.5528949.

Google Play. (2020). https://play.google.com.

Google Trends. (2021). Tendencia de búsqueda del término deepfake a nivel mundial. https://trends.google.com/trends/explore?date=2017-11-01%202021-06-26&q=Deepfake.

Güera, D., y Delp, E. J. (2018). Deepfake video detection using recurrent neural networks. En *15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)* (pp. 1-6). IEEE. https://doi.org/10.1109/AVSS.2018.8639163.

Hasan, H. R., y Salah, K. (2019). Combating deepfake videos using blockchain and smart contracts. *IEEE Access*, *7*, 41596–41606. https://doi.org/10.1109/ACCESS.2019.2905689.

Hughes, H. C., y Waismel-Manor, I. (2021). The macedonian fake news industry and the 2016 US election. *PS: Political Science & Politics, 54*(1), 19–23. https://doi.org/10.1017/S1049096520000992.

Islam, M. B., Lai-Kuan, W., y Chee-Onn, W. (2017). A survey of aesthetics-driven image recomposition. *Multimedia Tools and Applications, 76*(7), 9517–9542. https://doi.org/10.1007/s11042-016-3561-5.

Ivakhiv, A. (2016). The Art of Morphogenesis: Cinema in and beyond the Capitalocene. En S. Denson y J. Leyda (Hg.), *Post-Cinema. Theorizing 21st-Century Film* (pp. 724-749). REFRAME Books. https://doi.org/10.25969/mediarep/13475.

Kirchengast, T. (2020). Deepfakes and image manipulation: criminalisation and control. *Information & Communications Technology Law*, *29*(3), 308-323. https://10.1080/13600834.2020.1794615.

Kramer, R. S. S., Jenkins, R., y Burton, A. M. (2017). InterFace: A software package for face image warping, averaging, and principal components analysis. *Behavior Research Methods, 49*(6), 2002–2011. https://doi.org/10.3758/s13428-016-0837-7.

Krylov, A., Nasonova, A. y Nasonov, A. (2014). Image warping as an image enhancement post-processing tool. En *Proceedings of the 9th Open German-Russian Workshop on Pattern Recognition and Image Understanding* (132-135). University Koblenz-Landau. https://kola.opus.hbz-nrw.de/opus45-kola/frontdoor/deliver/index/docId/915/file/OGRW_2014_Proceedings.pdf#page=138

Li, D., He, K., Sun, J., y Zhou, K. (2015). A geodesic-preserving method for image warping. En *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)* (213–221). https://openaccess.thecvf.com/content_cvpr_2015/html/Li_A_Geodesic-Preserving_Method_2015_CVPR_paper.html.

Li, Y., Chang, M.-C., y Lyu, S. (2018). In ictu oculi: Exposing ai created fake videos by detecting eye blinking. *2018 IEEE International Workshop on Information Forensics and Security (WIFS)* (1-7). https://doi.org/10.1109/WIFS.2018.8630787.

Mulder, T. (2019). Health Apps, Their Privacy Policies and the GDPR. *European Journal of Law and Technology, 10*(1). https://papers.ssrn.com/abstract=3506805.

Nguyen, H. H., Yamagishi, J. y Echizen, I. (2019). Use of a capsule network to detect fake images and videos. *ArXiv:1910.12467 [Cs]*. http://arxiv.org/abs/1910.12467.

Parker, L., Halter, V., Karliychuk, T. y Grundy, Q. (2019). How private is your mental health app data? An empirical study of mental health app privacy policies and practices. *International Journal of Law and Psychiatry, 64*, 198–204. https://doi.org/10.1016/j.ijlp.2019.04.002.

Powell, A., Singh, P. y Torous, J. (2018). The complexity of mental health app privacy policies: A potential barrier to privacy. *JMIR MHealth and UHealth, 6*(7), e158. https://doi.org/10.2196/mhealth.9871.

Prathap, K. S. V., Jilani, S. A. K. y Reddy, P. R. (2016). A critical review on Image Mosaicing. *2016 International Conference on Computer Communication and Informatics (ICCCI)* (1-8). https://doi.org/10.1109/ICCCI.2016.7480028.

Puerto, S. (2018). Técnicas de animación e interrelación de imágenes bidimensionales. *Mosaic*, *165*. https://doi.org/10.7238/m.n165.1842.

Robillard, J. M., Feng, T. L., Sporn, A. B., Lai, J.-A., Lo, C., Ta, M. y Nadler, R. (2019). Availability, readability, and content of privacy policies and terms of agreements of mental health apps. *Internet Interventions*, *17,* 100243. https://doi.org/10.1016/j.invent.2019.100243.

Rossler, A., Cozzolino, D., Verdoliva, L., Riess, C., Thies, J. y Niessner, M. (2019). Faceforensics++: Learning to detect manipulated facial images. En *Proceedings of the IEEE/CVF International Conference on Computer Vision (ICCV)* (1-11). https://openaccess.thecvf.com/content_ICCV_2019/html/Rossler_FaceForensics_Learning_to_Detect_Manipulated_Facial_Images_ICCV_2019_paper.html.

Scherhag, U., Nautsch, A., Rathgeb, C., Gomez-Barrero, M., Veldhuis, R. N. J., Spreeuwers, L., Schils, M., Maltoni, D., Grother, P., Marcel, S., Breithaupt, R., Ramachandra, R., y Busch, C. (2017). Biometric systems under morphing attacks: Assessment of morphing techniques and vulnerability reporting. En *International Conference of the Biometrics Special Interest Group (BIOSIG)* (1-7). https://doi.org/10.23919/BIOSIG.2017.8053499.

Tang, J. y Ni, B. (2019). Progressive face dynamic morphing. En *2019 International Conference on Intelligent Computing, Automation and Systems (ICICAS)* (48–53). https://doi.org/10.1109/ICICAS48597.2019.00019.

Unión Europea, (2012). Charter of Fundamental Rights of the European Union. *Diario Oficial de la Unión Europea, C 326/02 de 26 de octubre de 2012.* https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:12012P/TXT&from=EN.

Veiga, C., Lourenço, A. M., Mouinuddin, S., van Herk, M., Modat, M., Ourselin, S., Royle, G. y McClelland, J. R. (2015). Toward adaptive radiotherapy for head and neck patients: Uncertainties in dose warping due to the choice of deformable registration algorithm: Dose warping uncertainties due to registration algorithm. *Medical Physics, 42*(2), 760-769. https://doi.org/10.1118/1.4905050.

Wagner, T. L. y Blewer, A. (2019). "The word real is no longer real": Deepfakes, gender, and the challenges of ai-altered video. *Open Information Science, 3*(1), 32-46. https://doi.org/10.1515/opis-2019-0003.

Zimmerle, J. C. y Wall, A. S. (2019). What's in a policy? Evaluating the privacy policies of children's apps and websites. *Computers in the Schools, 36*(1), 38-47. https://doi.org/10.1080/07380569.2019.1565628.