Aplicaciones de rastro COVID-19 vs privacidad

Autor: Víctor Morais Llahí

Fecha: 09/03/2021

Trabajo realizado para la asignatura **Arquitectura del PC**

Departament d'Arquitectura de Computadors
Facultat d'Informàtica de Barcelona
Universitat Politècnica de Catalunya

Resumen

Radar COVID-19 en España, Corona Warn en Alemania, NHS COVID-19 en el Reino Unido, TousAntiCovid en Francia, Immuni en Italia, Self-quarantine safety protection en Corea del Sur, HaMagen en Israel, Aarogya Setu en la India…. Países distintos, gobiernos distintos, nombres distintos, programadores distintos, lanzamientos distintos, presupuestos distintos y grado de aceptación distintos, pero un mismo objetivo: todas permiten rastrear contactos estrechos positivos por COVID.

En este escrito veremos las distintas aplicaciones que utilizan algunas de las naciones del mundo para doblegar a esta pandemia, cómo funcionan y, lo más importante, qué éxito están teniendo.

Resum

Radar COVID-19 a Espanya, Corona Warn a Alemanya, NHS COVID-19 al Regne Unit, TousAntiCovid a França, Immuni a Itàlia, Self-quarantine safety protection a Corea de Sud, HaMagen a Israel, Aarogya Setu a l'Índia .... Països diferents, governs diferents, noms diferents, programadors diferents, llançaments diferents, pressupostos diferents i grau d'acceptació diferents, però un mateix objectiu: totes permeten rastrejar contactes estrets positius per COVID. En aquest escrit veurem les diferents aplicacions que utilitzen algunes de les nacions de l'món per doblegar aquesta pandèmia, com funcionen i, el més important, quin èxit estan tenint.

Abstract

Radar COVID-19 in Spain, Corona Warn in Germany, NHS COVID-19 in the UK, TousAntiCovid in France, Immuni in Italy, Self-quarantine safety protection in South Korea, HaMagen in Israel, Aarogya Setu in India…. Different countries, different governments, different names, different programmers, different launches, different budgets and different levels of acceptance, but the same goal: they all allow to trace positive close contacts for COVID. In this writing we will see the different applications that some of the nations of the world use to overcome this pandemic, how they work and, most importantly, how successful they are.

Contenido

Índice de figuras

Introducción

Han sido muchos los países que, ante la caótica situación de emergencia sanitaria provocada por el COVID-19, apostaron en su momento por el uso de aplicaciones digitales como herramientas para la detección y localización de personas contagiadas. Como todos sabemos de sobras, uno de los principales peligros de este virus es su alta capacidad de transmisión. Conocer su expansión es vital para el control de la pandemia, para impedir nuevas olas de contagios y para evitar la saturación de los hospitales.

Las naciones de prácticamente todos los continentes han desarrollado una o varias aplicaciones de rastreo, ya sea mediante agentes privados o instituciones públicas, pero la triste realidad es que pocos han logrado que más de un 30% de su población llegara a descargársela. Y ya no digamos usarla.

¿Cuál es la razón? Usamos el teléfono móvil a diario. ¿Tener una aplicación que nos dijera si hemos estado expuesto a alguien contagiado no ayudaría a controlar mejor la expansión del virus? Si es así, ¿por qué no se la descarga la gente? Y, ya que estamos, ¿cómo funcionan exactamente estas aplicaciones? ¿Qué tipo de datos recogen y qué se hacen con ellos? ¿Puedo confiar en que no se invade mi privacidad y que la información extraída de mi teléfono es guardada a buen recaudo?

Este trabajo pretende dar respuesta a todas estas preguntas y a muchas otras que ni siquiera sabíamos que podíamos y debíamos formularnos. Se estudiará a conciencia en qué consisten y cómo funcionan estas aplicaciones de rastreo, en qué datos recogen, en cómo los tratan, en qué países se ha implementado su uso, de qué forma y cuáles son las diferencias entre ellas. Se profundizará en las razones por las cuales los sistemas propuestos han tenido un moderado éxito o, directamente, han fracasado y si dichas razones estaban infundadas en argumentos reales o eran meras conjeturas. Por último, se hará una breve reflexión sobre hasta qué punto es ética la invasión de la privacidad si es por un bien mayor y si en este ámbito y en estas circunstancias el fin puede llegar a justificar los medios.

Se citarán todas las fuentes de las que se ha extraído información para desarrollar este trabajo y se contrastará su fiabilidad. Se añadirá un enlace a cada referencia en un apartado final. Este escrito es un trabajo realizado para la asignatura de APC y para la Facultad de Informática de Barcelona.

Las aplicaciones de rastreo

¿Qué son y cuáles existen en el mundo?

"Aplicación de rastreo" es un término que, hoy en día, a pocos les es desconocido. La pandemia de COVID-19 que empezó a asolar nuestras vidas a principios del año 2020 ha hecho que incluyamos en nuestro vocabulario un conjunto de palabras que antes apenas usábamos. Seguro que no revelo nada si defino el concepto y digo que una aplicación de rastreo es una herramienta digital que ayuda a controlar la expansión de una pandemia y, en este caso en particular, del coronavirus SARS-CoV-2.

Sin embargo, si nos paramos a pensar en el verdadero significado que posee, descubrimos que este concepto es prácticamente nuevo, pues nunca antes en la historia de la humanidad se había destinado un producto software al control de una pandemia. Es increíble la facilidad con la que un hecho impensable años atrás ha pasado a formar parte tan rápidamente de nuestras vidas.

Una aplicación de esta índole funciona como una especie de registro de nuestros contactos estrechos. De esta manera, cuando alguna de las personas con las que hemos estado en contacto se contagia, es este mismo registro el que permite generar un seguimiento y formar una sucesión de contactos entre personas. Y tener esta sucesión es indispensable porque si sabemos por dónde se ha expandido el virus o, dicho de otra forma, si sabemos de qué individuo a qué individuo se ha transmitido, es entonces cuando podemos cortar la cadena de transmisión y evitar que más gente siga contagiándose. Y evitando contagios es como se salvan vidas.

¿Y qué se entiende por contacto estrecho? La respuesta a esta pregunta depende del país en la que la formulemos. En el caso de España, el Ministerio de Sanidad define un contacto estrecho como cualquier trato con un positivo a menos de 2 metros de distancia y por un tiempo mayor a 15 minutos.[1]

Las aplicaciones de rastreo de nuestros móviles pueden almacenar esta información para que ellas mismas o un rastreador, que a efectos prácticos es un agente de la Salud Publica y/o personal sanitario, se ponga en contacto con todas las personas afectadas desde dos días antes del inicio de los síntomas o, en caso de ser asintomático, desde dos días antes del diagnóstico.

Cómo podemos ver, las apps de rastreo son simplemente un método complementario para el rastreo de positivos que, como bien se ha demostrado en numerosas pruebas piloto en distintos países, incluido aquí en La Gomera, pueden ser de gran ayuda.

A lo largo de este documento veremos distintos ejemplos de aplicaciones de rastreo en varios países, aunque la que trataremos más en profundidad será la propuesta implementada en España, Radar COVID-19. La mención de otras herramientas se hará con la intención de señalar diferencias o para dar una explicación de un cierto razonamiento o reflexión.

En la Figura 1 se puede ver una tabla con algunas de las aplicaciones que han sido desarrolladas por distintos países pertenecientes a la Unión Europea. Por ahora no entraremos mucho en detalles puesto que solo se muestra para dar a conocer a algunos de los nombres que se irán mencionando más adelante. También se explicará en detalle el contenido de cada una de las columnas y se hará referencia a los datos mostrados en más de una ocasión.

País	App	Descargas	% de descargas	Fecha de lanzamiento	Casos diarios de Covid a 5 de Octubre*	Casos totales de COVID / 1 mill pob*
Irlanda	COVID Tracker	1.28 mln	26%	7 julio 2020	+ 517	7,784
Alemania	Corona-Warn App	18.4 mln	22%	16 julio 2020	+ 1,610	3,616
Reino Unido	NHS COVID-19	12.5 mln	19%	24 septiembre 2020	+ 12,504	7,584
Portugal	StayAway Covid	1.26 mln	12%	1 septiembre 2020	+ 904	7,768
Italia	Immuni	7 mln	12%	15 junio 2020	+ 2,257	5,420
Austria	Stopp Corona	1 mln	11%	25 marzo 2020	+750	5,421
España	Radar COVID	4.6 mln	10%	15 septiembre 2020	+ 2,099	10,239
Bélgica	Coronalert	0.65 mln	5,5%	30 septiembre 2020	+ 2,512	11,224

Figura 1: Tabla comparativa de los datos referentes a las distintas aplicaciones de rastreo de diferentes países de la Unión Europea a fecha de octubre de 2020. Fuente: Selectra

.

¿Cómo funcionan?

Todas las aplicaciones que se han podido ver en el apartado anterior funcionan de la misma forma y para el mismo propósito. Todas te comunican si has estado en contacto con algún positivo por covid-19 y todas te permiten, a la vez, indicar al sistema si eres tú quién se ha contagiado. Y, aunque parezca sorprendente, ninguna utiliza la geolocalización en ningún momento.

Radar COVID-19, al igual que el resto, se basa en la tecnología bluetooth y en el uso de una API de rastreo de contactos creada conjuntamente por Google y Apple que, de hecho, fue diseñada expresamente para su uso durante esta pandemia. En otras palabras, que las aplicaciones de rastreo ni siquiera hacen cálculos por sí mismas.

Puesto que parece ser que esta API es la que abastece en realidad a las aplicaciones oficiales de hasta 22 países de la Unión Europea, y a algunos del extranjero como Estados Unidos, se ha indagado un poco en cómo funciona exactamente y, para ello, se ha recopilado la siguiente información de su documentación oficial [2].

Al descargar e instalar una aplicación de rastreo, lo que sucede es que se habilita el sistema de notificaciones de exposición. Este sistema se encarga de generar una clave aleatoria que pretende funcionar como una especie de código identificador y que será intercambiado por otro en un rango de tiempo de entre 10 y 20 minutos. Las cualidades de este ID no permiten la identificación real de la persona en ningún momento y mucho menos el conocimiento de su localización pues varían en cortos márgenes de tiempo y no se asignan en base a ningún criterio en específico.

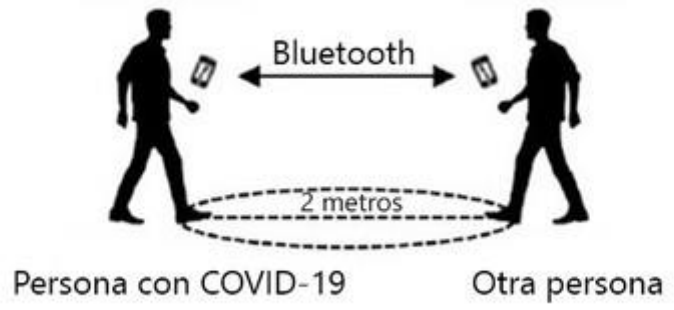


Figura 2: Ejemplo de funcionamiento de la API de rastreo.

Fuente: https://www.xataka.com/basics/radar-covid-que-como-funciona-app-oficial-rastreo-contactos-espana

Como bien podemos observar en la Figura 2, los teléfonos de las personas que tengan instalada la aplicación de rastreo emitirán varias veces por segundo su clave aleatoria y recibirán la del resto vía Bluetooth. Todo este proceso puede realizarse perfectamente en segundo plano por lo que en ningún momento es necesario tener la aplicación abierta. Incluso, se puede cerrar.

El sistema irá almacenando en una lista todos los identificadores que vaya captando vía Bluetooth y, periódicamente, revisará el registro publicado en la nube de identificadores positivos en busca de coincidencias. En el caso de encontrar una similitud, la aplicación alerta al usuario de que ha estado expuesto y le indica las instrucciones a seguir que recomiende el departamento de salud pública en ese momento.

El sistema busca identificadores a una distancia menor de 2 metros cada 5 minutos, y los guarda durante 14 días. Si una persona positiva indica mediante la aplicación que se ha contagiado, todos los identificadores aleatorios que le han sido asignados durante las últimas dos semanas serán marcados y todos aquellos teléfonos móviles que hayan captado uno o varios de ellos en algún momento serán advertidos.

Como puede verse este método, aparte de eficiente, es completamente anónimo ya que cuando nosotros recibimos una alerta por riesgo de contagio no sabemos en ningún momento con quién ha sido, ni dónde, puesto que la única información que existe es una secuencia numérica aleatoria.

La API, además, no solo encripta todos los metadatos asociados con el tráfico de Bluetooth, si no que utiliza un sistema descentralizado que sigue el protocolo DP-3T [3], un protocolo de código abierto de identificación de dispositivos mediante el uso de claves efímeras de 16 bytes llamados técnicamente EphID. Estos EphID son almacenados localmente en el dispositivo de un cliente receptor y nunca se transmiten a terceros ni son, por tanto, subidos a la nube o alojados en servidores.

Sin embargo, hay que recordar que esto es solo a nivel de API. El siguiente paso es saber cómo funciona realmente la aplicación y, ahora sí, nos centraremos exclusivamente en Radar COVID-19, la aplicación de rastreo española.

Para ello he instalado la aplicación en mi teléfono móvil y la he iniciado. Lo primero que aparece es información sobre la utilidad de la herramienta (Figura 3) y un recordatorio de que los datos obtenidos por el sistema no pueden identificar al usuario (Figura 4). También nos recuerdan que

en ningún momento tenemos la obligación legal de usar la aplicación. Algo que no sucede en otros países y de lo que hablaremos más adelante.

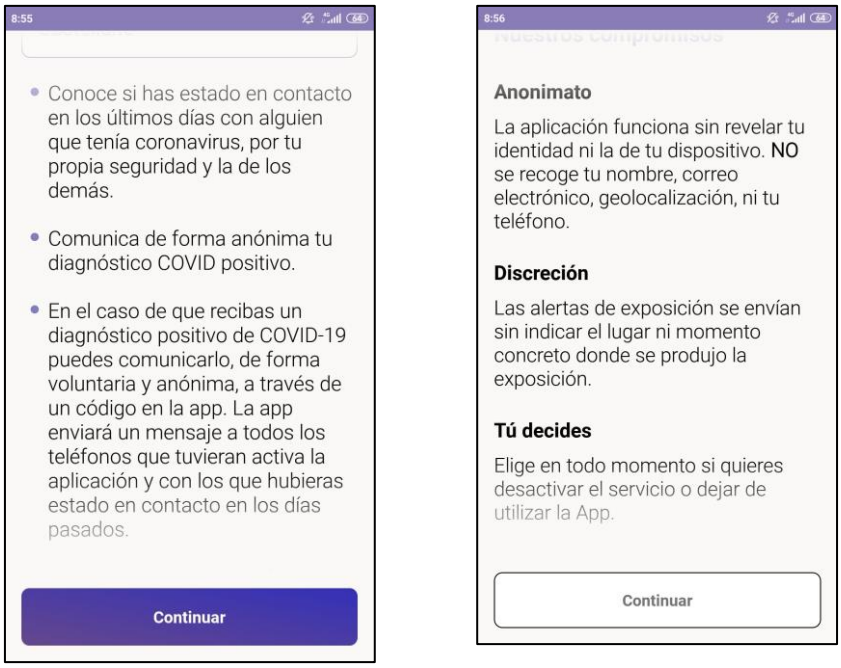


Figura 3 y 4: Capturas de pantalla del ingreso en Radar COVID-19. Fuente: Elaboración propia.

Lo cierto es que la aplicación no nos pide nada más a excepción de que indiquemos en qué idioma queremos visualizar la interfaz. Lo único que sí que obliga a hacer es a aceptar la política de privacidad y las condiciones de uso.

Tras leer detenidamente la política de privacidad [4] descubrimos varios detalles más concretos sobre el funcionamiento de la aplicación que desconocíamos por el momento. Uno de ellos es la titularidad de la aplicación. Radar COVID-19 pertenece a la Secretaría General de Administración Digital, y depende de la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital.

Por otro lado, sabíamos que la API de rastreo de contactos solo transmitía claves aleatorias y, en ningún momento, daba un dato que pudiera identificar realmente al usuario. En la política de privacidad se estipula que, a más a más, también se informa del día exacto del contagio. Esta discrepancia nos hace pensar que es una funcionalidad añadida de la aplicación pues en ninguna documentación sobre la API se ha encontrado una mención de este detalle.

En tercer lugar, también descubrimos que la creación de los identificadores aleatorios que son transmitidos y recibidos por Bluetooth no es completamente aleatoria, sino que se forma a partir de un código de 16 bytes al que llaman “clave de exposición temporal” que es generado diariamente. De él derivan los llamados “identificadores efímeros de Bluetooth” que son los que cambian cada 10-20 minutos y los que se transmiten.

Tu teléfono almacenará tus propias claves de exposición diarias, las 14 últimas que corresponden a los últimos 14 días, y todas las claves efímeras Bluetooth recibidas durante el mismo periodo de tiempo. Y está información queda exclusivamente en tu teléfono y no sale de ahí. No existe ningún tipo de copia o almacenamiento en un servidor ni nada por el estilo, como ya aseguraba el uso del protocolo DP-3T. En las Figura 5 podemos ver mi estado actual según la aplicación y, en la Figura 6, un ejemplo de la pantalla que nos saldría si hubiese estado en contacto con un positivo.

Figura 5 y 6: Pantallas de ejemplo de situación sin riesgo y situación de exposición alta. Fuente: Elaboración propia.

A pesar de esto, en el caso de que se nos diagnostique positivamente por COVID-19, deberemos, si queremos, introducir la clave que nos facilite el Servicio Público de Salud (Figura 7) y que será validada por la Secretaría General de Administración Digital. Al introducir esta clave y al dar

nuestro consentimiento, es entonces cuando por primera vez perdemos la posesión del registro de nuestras claves pues este es enviado a sus servidores para que las incluyan en el listado de claves de exposición temporal de personas contagiadas. El mismo listado que, como ya mencionábamos antes, el sistema revisa periódicamente con el fin de saber si hemos estado o no en riesgo de contacto.

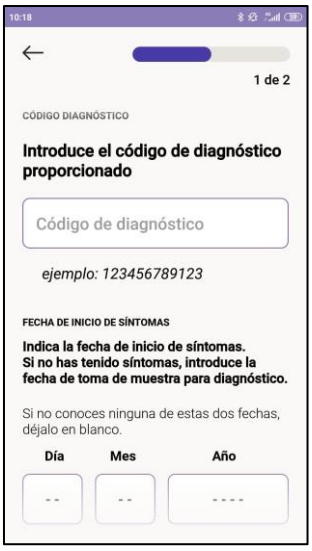


Figura 7: Captura de pantalla del proceso para indicar que se ha sido diagnosticado cómo positivo en COVID-19. Fuente: elaboración propia

La aplicación descarga periódicamente esta lista de claves de exposición temporal de personas contagiadas de los servidores que, eventualmente, han sido compartidas voluntariamente por los usuarios, y las compara con los códigos almacenados en estas últimas dos semanas como ya se ha explicado antes. Al encontrar una coincidencia, se ejecuta un algoritmo que determina el grado de exposición en base a la estimación de la distancia y duración del contacto y, en caso de sobrepasar un determinado lindar, manda o no una notificación de alerta al usuario que se ha visto expuesto. La información almacenada en los servidores de la Secretaría General de Administración Digital permanece ahí durante dos semanas desde que se reciben. Luego son eliminados.

Como podemos observar la utilidad de esta aplicación, como la de la mayoría de aplicaciones que han sido de uso voluntario, depende estrictamente de la responsabilidad del usuario. A sí mismo lo recoge la propia política de privacidad. Cito textualmente: “El éxito de la aplicación como herramienta que contribuya a la contención de la propagación está directamente vinculado a que los usuarios sean conscientes, y actúen en consecuencia, de que, a pesar de que comunicar a la aplicación que se ha obtenido un resultado positivo en la prueba de COVID 19 (previa acreditación de las autoridades sanitarias) es voluntario, el no comunicarlo y ser un mero receptor de información de terceros usuarios hace que la aplicación pierda su utilidad preventiva no solo para los demás usuarios sino para el resto de la población en general. El carácter completamente anónimo debería animar, sin duda, al ejercicio de esta actuación responsable.”

Y eso es algo que, más adelante, veremos que no hizo. Pero antes, falta comentar las condiciones de uso del sistema [5]. El principal elemento que la aplicación requiere es la concesión de permisos del uso de Bluetooth, por descontado. Se ha observado como también se solicita activar

la localización en nuestro teléfono, lo cual era de extrañar puesto que hipotéticamente la app no registra datos de este tipo. Pero más tarde se ha descubierto que esta solicitud se debe a que el propio Bluetooth requiere de este permiso para buscar los identificadores dado que el sistema operativo de algunos dispositivos Android sufre de esta limitación. Si se revisa los permisos que solicita la aplicación, vemos que en realidad no tiene autoridad para acceder a ningún dato relacionado con la ubicación.

¿Son seguras las aplicaciones descentralizadas?

Siguiendo con el caso de Radar COVID-19, nos encontramos con que la aplicación no recoge en ningún momento datos personales y, mucho menos, se invade nuestra privacidad. No solo se repite incansablemente en la política de privacidad y en las condiciones de uso tanto como de la aplicación como de la propia API, sino que además no se puede encontrar algún indicio que demuestre lo contrario. Según las mismas condiciones de uso consultadas en el anterior apartado, el usuario acepta:

- El envío anónimo de señales Bluetooth a otros dispositivos.
- La recepción y almacenamiento descentralizado de señales Bluetooth procedentes de otros dispositivos con aplicaciones compatibles con Radar COVID-19 por un periodo máximo de 14 días.
- La información que reciba sobre su posible riesgo de contagio.
- Recibir claves de positivos de otros países de la Unión Europea mediante su plataforma de interoperabilidad EFGS.
- Enviar sus propias claves de exposición temporal en caso de resultar positivo y bajo su propio consentimiento. Las cuales, a su vez, podrán ser también enviadas a través de la EFGS a otros países de la Unión Europea.

Como puede verse, nada que no supiéramos ya. Así que en este sentido la aplicación es segura. A pesar de esto, aún queda una pregunta por resolver: ¿Está asegurada la privacidad de mis datos, aunque no permitan identificarme, una vez salen de mi móvil y son almacenados en los servidores de la Secretaría General de Administración Digital?

Bien, como que la aplicación no trata datos personales, nosotros como usuarios no tenemos derecho de acceso, ni de rectificación, supresión, limitación, oposición ni portabilidad sobre los mismos. Una vez las claves de exposición son enviadas a los servidores de la Secretaría General

de Administración Digital, solo ellos como titulares tienen el derecho a tratar estos datos con la finalidad de asegurar el correcto funcionamiento de la app y de acuerdo con el Reglamento General de Protección de Datos. Esto les permite recogerlos, almacenarlos, modificarlos, estructurarlos y, finalmente, eliminarlos. Además, enumeran la siguiente legislación que les concede acceso a hacerlo:

- Reglamento (UE) 2016/679, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley 14/1986, de 25 de abril, General de Sanidad
- Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública.
- Ley 33/2011, de 4 de octubre, General de Salud Pública.
- Real Decreto 463/2020 de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19 que atribuye al Ministro de Sanidad la necesaria competencia en todo el territorio nacional.
- Orden Ministerial SND/297/2020 de 27 de marzo, por la que se encomienda a la Secretaría de Estado de Digitalización e Inteligencia Artificial, del Ministerio de Asuntos Económicos y Transformación Digital, el desarrollo de nuevas actuaciones para la gestión de la crisis sanitaria ocasionada por el COVID-19.

Recordemos que estos datos solo pueden ser las claves de exposición temporal, el código de validación única cedido por las autoridades sanitarias que se utiliza para indicar que, voluntariamente, otorgas tus datos cuando has sido positivo y, por último, un cuestionario voluntario sobre tu experiencia como usuario de la aplicación.

La protección de estos datos una vez salen de tu poder, viene dada por las medidas de seguridad implantadas y que pueden leerse en el anexo 2 titulado “Medidas de Seguridad” del Real Decreto 3/2010, de 8 de enero, en el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica [6]

Sin embargo, todo usuario tiene derecho a presentar una reclamación si así lo desea ante la Agencia Española de protección de datos. Aunque, tal y como recuerdan las condiciones de uso, hay que tener presente que como usuarios nos comprometemos a:

- Impedir el acceso de terceros a la aplicación.
- Notificar al titular cualquier indicio de fallo en la seguridad de la aplicación, de un uso inapropiado o prohibido.
- A hacer un buen uso de la aplicación, entre lo cual se incluye:
    - No hacer actos ilegales o fraudulentos con ella.
    - No tratar de sobrecargar y/o dañar el sistema.
    - Respetar los derechos de propiedad intelectual e industrial del titular.
    - No suplantar la autoridad de un tercero.
    - No proporcionar información falsa.

De esta forma, el usuario se declara como único responsable de la aplicación y el titular no será culpable de ninguna mala praxis o de fallos en el acceso, actualización, instalación, o la incompatibilidad o daños en los terminales de los dispositivos a causa del uso de la aplicación.

Análisis de otras alternativas

Hasta el momento hemos visto exclusivamente un tipo de aplicación de rastreo. Aquellas descentralizadas que, por lo general, suelen ser de uso voluntario. Pero este no es el único tipo de tecnología que podemos encontrar en este ámbito. Ni siquiera hace falta salir de la Unión Europea para encontrar algún ejemplo como lo puede ser Hungría, Eslovaquia o, incluso nuestro vecino al otro lado de la frontera, Francia.

En el caso de TousAntiCovid [7], la aplicación francesa, utiliza igualmente una tecnología basada en la compartición de claves efímeras vía Bluetooth, pero no lo hacen mediante la API ofrecida por Google y Apple si no que apuestan por un sistema centralizado creado por ellos mismos. El gobierno francés argumenta que esto es así porque no creen oportuno dejar esta especie de datos en manos de entidades internacionales puesto que esto plantea diversas cuestiones de soberanía. Del mismo modo, apuestan por un sistema centralizado propio ya que consideran que es más seguro que no el almacenamiento local en los dispositivos de los usuarios que, aunque encriptado, es más susceptible a ataques informáticos. Aunque, por otro lado, han optado por que el código sea open source de manera que cualquier ciudadano puede comprobar que, efectivamente, su libertad y privacidad no está siendo amenazada en ningún momento.

Hungría, en cambio, sería un ejemplo de país cuya aplicación utiliza datos que fácilmente pueden usarse para identificar el usuario pues, en vez de generar claves aleatorias, trabaja a partir del

número de teléfono móvil en el que se ha descargado la aplicación. Y esto es muy diferente de lo que hemos visto hasta ahora. Según las autoridades húngaras, el uso de VirusRadar [8] es voluntario, y requiere de un teléfono móvil al que asociar una clave única que será compartida, de nuevo, vía Bluetooth. El resto del funcionamiento es idéntico a los otros casos. Aunque los datos que se transmiten sean anónimos, en este caso si que se puede desvelar la identidad de un usuario si se descubre la relación entre la clave única y el número de teléfono asociado a ella. Pero el Ministerio de Innovación y Tecnología de Hungría asegura que los números de teléfono se almacenan en un servidor seguro en la Agencia de Desarrollo de Informática del Gobierno (KIFÜ).

Por último, la aplicación de Eslovaquia parece que todavía no tiene fecha de salida. He decidido comentarla de todas formas porque el principal motivo es que el las Cortes Constitucionales de la Republica de Eslovaquia han suspendido una parte de las leyes que permitirían la instauración de la aplicación porque, al parecer, no establecen de forma suficientemente clara las intenciones del procesamiento de datos personales y carecía de las garantías necesarias contra el posible uso indebido de los datos personales procesados.

Independientemente de si utilizan una tecnología descentralizada o no, todos los ejemplos vistos hasta ahora comparten una característica y es que su uso es voluntario. Pero esto no es así en todos los lugares del mundo y la diferencia entre los países que obligan a usar aplicaciones de rastreo a sus ciudadanos es, prácticamente, la misma que separa a oriente y occidente.

Mientras que occidente posee unas normativas de privacidad muy estrictas, lo cierto es que en los países orientales como China, Japón o Corea del Sur vemos que sucede completamente lo contrario puesto que su cultura tiene una forma de ver la privacidad muy distinta a la nuestra y, mientras que en lugares como la Unión Europea prevalece ante todo la garantía de la privacidad, en oriente es sacrificable si es a cambio de un bien común como es el control de una pandemia.

De hecho, hablaremos de la aplicación de rastreo surcoreana Self-quarantine safety protection que es una de las más estrictas del mundo y una herramienta totalmente opuesta a la que se defiende en occidente. La filosofía de Self-quarantine safety protection es que cuánto más privado sea el dato, más ayuda en el contexto epidemiológico. Esto se traduce en que la app no solo recoge nuestros datos personales, incluidos el género y la nacionalidad, sino que además indica tu estado de salud, tu localización actual GPS y un registro de todos los lugares que has visitado. Con esta información, la aplicación puede incluso notificar a las autoridades si incumplimos la cuarentena y, por supuesto, nos permite avisar al resto de personas si somos diagnosticados como positivos. Además, el uso de la aplicación es obligatorio en todos los ciudadanos y extranjeros de residencia

de larga duración. Según la ley de prevención de enfermedades infecciosas surcoreana, no usar la aplicación comporta penas de hasta 1 año de cárcel y multas de hasta 10 millones de wones (7.361,20 €) para los residentes y la expulsión del país para los extranjeros. Estos datos han sido cedidos por el Consulado General de la República de Corea de Barcelona [9].

Estas medidas, que sin duda alguna pueden parecernos sumamente intrusivas, han resultado ser muy eficaces en el control de la pandemia en oriente. En el siguiente apartado podremos verlo en más detalle.

El éxito de algunas pocas y el fracaso de muchas otras

El estrepitoso fracaso de Radar COVID-19 en España

Y ahora yo le pregunto: ¿Usa usted algún tipo de aplicación de rastreo? ¿Conoce a caso a alguien que las utilice? Hacernos estas dos preguntas bastan para darnos cuenta del poco éxito que las herramientas digitales han tenido en esta pandemia. Al menos en nuestro país. Ya lo veíamos al principio de este documento, en la Figura 1. La utilidad de este tipo de herramientas radica en que la gente las use y ninguno de los países de la Unión Europea ha alcanzado, ni siquiera, una cantidad de descargas considerable. Y ni tan solo eso importa, porque de nada sirve descargársela y luego no usarla.

La única forma de valorar hasta que punto a servido una herramienta digital de esta índole es comparar el número de contagios detectados por la aplicación en cuestión y el número real de positivos que se han registrado hasta la fecha en la nación. Es el momento de regresar al marco de Radar COVID-19 y ver esta diferencia.

La propia aplicación ofrece una sección de estadísticas en la que ver el número total de casos. Hoy, a día 12 de marzo de 2021, la aplicación ha declarado 53.250 casos positivos desde su lanzamiento el 19 de agosto de 2020. También podemos ver que se la han descargado un poco más de 7 millones de personas. La Figura 8 muestra una captura de pantalla del teléfono en el que descargamos la aplicación. Podemos observar que estos datos fueron actualizados por última vez hace casi una semana, el 7 de marzo de 2021.

Figura 8: Captura de pantalla de las estadísticas de Radar COVID-19. Fuente: Elaboración

Y, según los datos proporcionados por el Ministerio de Sanidad, Consumo y Bienestar Social al portal de estadísticas alemán Statista donde llevan un riguroso control de todas las cifras referentes al coronavirus en Europa, entre el 19 de agosto de 2020 y hoy se han diagnosticado 2.634.843 nuevos casos positivos de COVID-19 [10], por lo que el rango de detección de Radar COVID-19 a día de hoy es del 2,021%. Podríamos decir que su aportación al control de la expansión de la pandemia es prácticamente ínfima.

¿Por qué ha sucedido esto? ¿Por qué la gente no ha utilizado una herramienta que presuntamente iba a salvar miles de vidas? Tras recabar información tanto de artículos periodísticos, como reflexiones de expertos en distintos ámbitos y comentarios de los propios políticos, se distinguen las distintas razones.[11]–[14]

La falta del código de diagnóstico

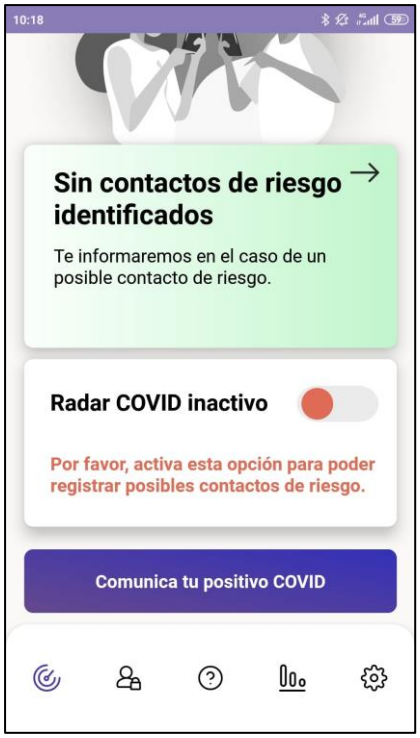
Recordemos que, en el caso de resultar ser diagnosticados como positivos por coronavirus, la agencia de Salud Pública debía darnos un código, con la correspondiente PCR positiva, que debíamos introducir en la aplicación para que nuestras claves de exposición temporal se subieran a los servidores de la Secretaría General de Administración Digital. A efectos prácticos, sin este código la aplicación no sirve de nada pues no puede alertar a todos los usuarios con los que hemos estado en contacto estrecho que están en riesgo de haberse contagiado. Son muchos los usuarios que, especialmente durante la tercera ola de la pandemia, denunciaron que en ningún momento se les facilitó tal código y la única explicación con la que se encontraron era que los servicios tanto de Atención Primaria como de Urgencias estaban muy saturados.

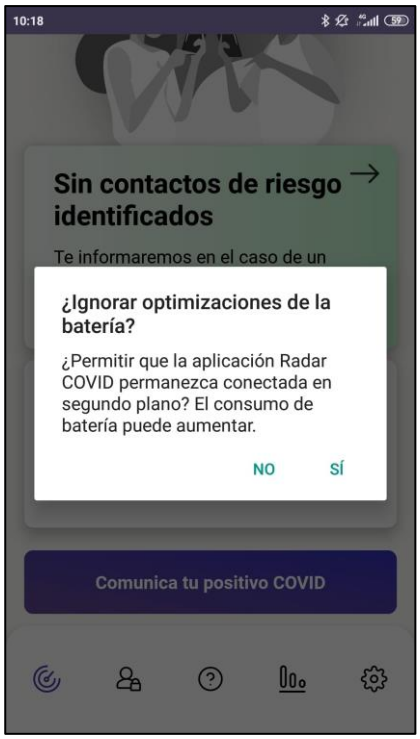
Se intentó solucionar esto recomendando a las comunidades autónomas que mandaran los códigos mediante SMS en vez de adjuntarlos con las pruebas PCR. La medida no produjo ninguna mejora significativa.

El consumo de la batería

Otra dificultad añadida en el éxito de esta aplicación fue, irónicamente, el tipo de tecnología que usa. Recordemos que el sistema requiere de tener acceso al Bluetooth de nuestro dispositivo para transmitir y recibir los códigos aleatorios de identificación.

Los usuarios no acostumbrados al uso de Bluetooth podrían perfectamente no activarlo porque desconocen que debe hacerse y esto inutiliza el sistema por completo. Además, los dispositivos Android versión 6 o superior y los IOS con versión igual o posterior a la 13 tienen, por defecto, una optimización de batería predeterminada en todas las aplicaciones. Incluida Radar COVID-19, por lo que no solo hay que activar el Bluetooth si no que hay que desactivar la optimización de batería. Como se puede observar en la Figura 9, a pesar de haber activado el Bluetooth vemos que el sistema aún no está registrando mis contactos estrechos. Y, cuando activo la opción, sale una ventana emergente que me advierte de que el hecho de permitir el funcionamiento en segundo plano de la aplicación puede comportar un aumento en el consumo de nuestra batería (Figura 10). La aparición de este mensaje, en mi opinión, podía hacer que mucha gente decidiera no utilizar la aplicación por miedo a quedarse sin batería en su teléfono. Además, alimenta la falsa creencia de que este tipo de tecnología consume un gran porcentaje de nuestra batería cuando la realidad es que, estando el móvil a pleno rendimiento, la media de consumo de Bluetooth en los dispositivos actuales es del 6,6% [15]. Por no hablar de que el tipo de Bluetooth que utiliza la API de Google es el de baja consumición, Bluetooth Low Energy. Lo que baja aún más ese porcentaje.





Figuras 9 y 10: Capturas de pantalla de la configuración Bluetooth. Fuente: Elaboración propia.

La falta de campañas de concienciación sobre su uso y la falta de sincronización

En tercer lugar, deberíamos recalcar que parte de la culpa del poco éxito de Radar COVID-19 en nuestro país es de las propias instituciones. Para empezar la aplicación llegó tarde. Aunque su fase beta ya estaba lista en el mes de agosto, no estuvo completamente operativa en todas las comunidades autónomas hasta el mes de octubre, mientras que otros países como Francia o Italia ya tenían aplicaciones funcionales a mediados de junio. Y no, no tiene nada que ver que ellos no utilicen la API de Google y Apple puesto que esta fue finalizada en mayo. ¿Cuál es la causa de esta demora en su implantación? Es triste reconocerlo, pero la verdad es que el único motivo es la poca rapidez en la toma de decisiones del Gobierno central y la falta de agilidad en la reacción de las instituciones públicas autonómicas. Una lentitud dada por las constantes delegaciones de responsabilidades, el temor, quizás, al error y por la propia inexperiencia en la gestión de situaciones como estas. No todas las comunidades autónomas integraron la aplicación en sus sistemas de salud a tiempo, no se diseñó ninguna campaña de concienciación en el uso de la aplicación que desmintiera la difamación a la que se estaba viendo sometida por cuestiones referentes a la privacidad de quien la usaba, no se detalló su funcionamiento, no se publicaron los resultados de la prueba piloto realizada en La Gomera y no se transparentó hasta mucho después el desarrollo en sí del sistema.

Fueron muchas las naciones que tuvieron el mismo problema, pero supieron reaccionar a tiempo. Por citar algún ejemplo, la app Alemana Corona Warn es de las que más éxito a cosechado dentro de la Unión Europa gracias a que hizo grandes esfuerzos por aumentar la confianza del pueblo alemán en su uso. Hizo campañas de concienciación, involucró a múltiples organizaciones de alta reputación y la convirtió en una aplicación de código abierto para que cualquiera pudiera ver su funcionamiento interno.

La falta de confianza y el temor por la privacidad

El equilibrio entre la seguridad y la privacidad fue, y es aún, un debate muy mediático. Desafortunadamente en el caso de Radar COVID-19 y de, prácticamente, la totalidad de las aplicaciones de rastreo de uso voluntario, han sufrido una reticencia de la población a su uso por miedo a que sus verdaderas intenciones fueran las de controlar lo que los usuarios hacen, dónde están y con quién están. Ha habido mucha desinformación y mucho ruido en las redes sociales y, como ya se ha comentado en el apartado anterior, no se han hecho quizás los esfuerzos suficientes para contrarrestar su difamación.

Ningún sistema es seguro 100%, por descontado. Y la sociedad hace bien en tener una especie de temor natural por su privacidad cuando se usan este tipo de dispositivos tecnológicos. Pero,

personalmente, creo que no se ha hecho suficiente hincapié en el propósito que estas aplicaciones tenían: salvar vidas, prevenir contagios y controlar una pandemia que lleva más de un año asolándonos. Recordemos que, las aplicaciones que utilizan la API de rastreo de contactos solo tienen acceso al Bluetooth del teléfono y que, en todo momento, no se nos pide ningún dato personal y la única información transmitida es un código aleatorio de 14 dígitos que no puede identificarnos de ninguna forma.

Paradójicamente, instalamos otras muchas aplicaciones en las que nuestra privacidad apenas esta asegurada y en las que no disponemos de ningún control de a donde va nuestra información y, nuestra privacidad, está totalmente expuesta. Esta paradoja puede verse reflejada en la Figura 11, donde comparamos los datos que recoge Radar COVID-19 con los que recoge la plataforma de mensajería WhatsApp, que cosecha más de 5000 millones de descargas. La información ha sido extraída de su propia política de privacidad [16].

Datos recogidos por Radar COVID-19	**Datos recogidos por WhatsApp** (marzo de 2021)
- Clave de exposición aleatoria generada diariamente. - Claves efímeras Bluetooth generadas cada 10-20 min. - Código de diagnóstico cedido por la Sanidad Pública (voluntario). - Encuesta sobre la experiencia de uso de la aplicación (voluntario).	- Número de teléfono. - Foto de perfil, historial de estados y de nombres de usuario. - Mensajes que no llegan a entregarse y archivos multimedia reenviados. - Tus contactos. - Método de pago, detalles de envío, tipo de transacción, importe (si utilizamos servicios de pago de WhatsApp). - Cualquier información que des al soporte técnico, incluso la copia de mensajes personales o la dirección de correo. - Información sobre tu actividad. - Información sobre tu configuración de ajustes. - Tiempo frecuencia y duración de uso. - Sitios web (enlaces visitados). - Última conexión en línea. - Nombre y foto de todos tus grupos. - Última vez que actualizaste tu perfil. - Archivos de registro. - Modelo del hardware, sistema operativo, nivel de batería, la potencia de señal y la versión del dispositivo. - La red móvil y el tipo de conexión. - El idioma. - La zona horaria. - La dirección IP - Nuestra ubicación constante.

Figura 11: Tabla comparativa entre los datos recogidos por Radar COVID-19 y por WhatsApp. Fuente: Elaboración propia.

Y no solo eso. WhatsApp puede incluso tener acceso a tu número de teléfono por el mero hecho de que figures en la lista de contactos de otro usuario. Además, aunque los mensajes están cifrados de extremo a extremo y por eso no aparecían en esta lista, si cualquier usuario hace una captura de pantalla de una conversación con otro usuario y la envía junto con un informe de reporte a la compañía, por mucho que el informe no tenga evidencias de que ese otro usuario haya hecho algo que incumpla la normativa de la empresa, una copia de esa conversación será almacenada en sus servidores por lo que en realidad en todo momento lo que envías es accesible.

Y, a pesar de esto, el fracaso de Radar COVID-19 se debió, en gran parte, al miedo de los usuarios por la violación de su privacidad. Da que pensar.

Los resultados de las aplicaciones de rastreo en el resto del mundo

A continuación, vamos a comprobar las estadísticas de otros países tanto de la Unión Europea como de otros continentes.

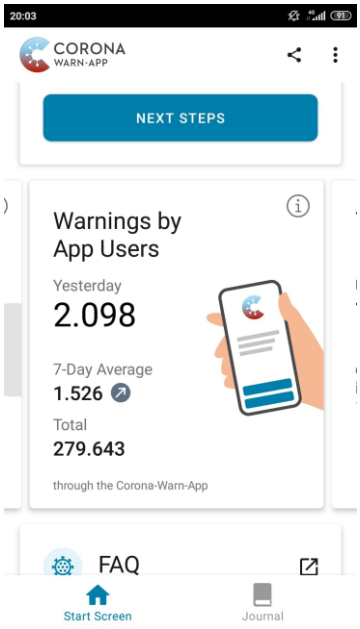


Figura 12: Captura de pantalla de las estadísticas de Corona Warn. Fuente: Elaboración propia.

Empezaremos por Alemania que, como ya se ha comentado brevemente, es a nivel europeo el país con más grado de aceptación de su aplicación de rastreo y que, además, utiliza la misma API que Radar COVID-19 por lo que, a efectos prácticos, es la misma propuesta con una interfaz más cuidada y detallada. Como podemos ver en las Figura 12, me he descargado Corona Warn en mi teléfono y he accedido al apartado de estadísticas. En la Figura 1 podíamos observar que su uso comenzó el 16 de julio de 2020 y, según los datos de la expansión de la pandemia [17], de los 2.349.938 casos confirmados desde ese momento hasta hoy, 279.643 han sido alertados por la aplicación, por lo que estaríamos hablando de un 11.9% de los casos totales diagnosticados. Hasta donde se tiene constancia, el resto de la Unión Europea tiene una media peor que esa.

Otro caso que merece la pena comentar es el de Reino Unido que sería un ejemplo de aplicación de rastreo voluntaria, con tecnología descentralizada, que si ha funcionado. A pesar de que si pide datos personales como nuestro código postal, o incluso puede

almacenar foto que hagamos con la app para registrar a los lugares que hemos ido, Inglaterra ha sabido sacar partido a su aplicación de rastreo.

Según una investigación de la Universidad de Oxford [18] de los casi dos millones de contagios producidos entre el 1 de octubre y el 31 de diciembre, un millón y medio fueron notificados mediante su la app lanzada por el Servicio Nacional de Salud (NHS). Estamos hablando de el 75% de los casos prácticamente. Los expertos estiman que se han prevenido entre 200.000 y 900.000 nuevos positivos y que, por cada 1% que incrementa el número de usuarios, el número de contagios en el territorio baja entre el 0,8% y el 2,3%. ¿Por qué esta diferencia? Ya hemos dicho que es descentralizada y voluntaria, igual que Radar COVID-19 y Corona Warn, y utiliza la misma API de Google y Apple e incluso sufrió errores de integración durante un tiempo. El Gobierno Británico asegura que NHS COVID-19 App ha estado rompiendo cadenas de transmisión desde que fue lanzada y que ha hecho que más de 1.700.000 usuarios fueran alertados de que algún contacto estrecho se había contagiado. Fue la segunda app más descargada del Apple Store en 2020 y acumula más de 21 millones de descargas (febrero 2021), lo que equivale al 56% de los ciudadanos británicos con teléfono inteligente y mayores de 16 años. Estos buenos resultados se deban quizás no solo a las fuertes campañas a favor del uso de la aplicación si no a la responsabilidad de los ciudadanos de Reino Unido.

En cambio, si vamos a hasta Israel, país líder en vacunación a nivel mundial, encontramos que su app de rastreo HaMagen fue un absoluto fracaso que acumuló muchas descargas pero que, debido a fallos técnicos, fue perdiendo usuarios hasta caer en el olvido. He probado a descargar en mi teléfono, pero la interfaz se ha quedado congelada en la pantalla principal en múltiples ocasiones.

Aún y así, el Gobierno israelí lanzó una segunda versión mejorada a mediados de junio, pero sufrió el mismo desenlace. A pesar de ser una de las primeras naciones en lanzar una aplicación de rastreo, no se hicieron suficientes campañas para explicar como y por qué usar aquella herramienta. Una vez más queda demostrada la importancia de esta medida. También estuvo sujeta a problemas judiciales por cuestiones éticas sobre la invasión a la privacidad, puesto que utiliza la geolocalización. Hoy en día tanto los ciudadanos como los mandatarios la han dejado de lado [19].

Y, para finalizar, veremos los resultados que cosecha la app más estricta de todas las mencionadas en este escrito. Recordemos: la app surcoreana no solo era obligatoria, sino que era de las más invasivas del mundo y era capaz de saber donde habías estado en cualquier momento e incluso denunciarte a las autoridades si violabas una cuarentena.

Según “Journal of sustainable tourism” [20] fue esto último lo que permitió al país mantener sus fronteras abiertas en todo momento. Incluyeron en el procedimiento de admisión la descarga e instalación obligada de su app de rastreo y te ayudaban a hacerlo en la misma terminal si era preciso. Según datos oficiales proporcionados por el Ministerio de Salud y Bienestar surcoreano, el 16 de mayo de 2020 el 93,1% de la población usaba Self-quarantine safety protection. Aunque no se han encontrado datos oficiales de cuantos casos han sido prevenidos gracias a la aplicación, lo que si que es cierto es que Corea del Sur ha sumado poco más de 95.000 casos a día de hoy y, mientras que España tiene una densidad de población de 94 habitantes por kilómetro cuadrado, la de Corea del Sur es de 515. Sus buenos resultados se deben tanto a la buena gestión de la pandemia como al uso obligado de la aplicación. Esto no hace más que alimentar el debate sobre dónde debe estar el equilibrio entre seguridad y privacidad.

Conclusiones

En este pequeño viaje alrededor del mundo hemos tenido la oportunidad de ver algunas de las aplicaciones de rastreo que los países utilizan hoy en día para controlar la expansión de la pandemia cortando cadenas de transmisión y rastreando contactos estrechos.

Hemos podido analizar en profundidad los distintos funcionamientos y tecnologías utilizadas tanto en Europa como en el resto de continentes y hemos visto la efectividad de las propuestas en base a las circunstancias epidemiológicas de las naciones, la cultura de su gente y el grado de implicación de los gobiernos.

También se ha demostrado la terrible influencia que puede llegar a tener la mentira sobre la verdad y como ha afectado eso al propósito de aquellas herramientas digitales que habían sido creadas para proteger al pueblo y no para controlarlo. Se ha hondado un poco más en el debate sobre los límites de la privacidad y lo que este comporta.

En el futuro, sería interesante ver como prosigue la evolución de este tipo de aplicaciones y analizar más en detalle su uso en otros países que no han sido contemplados en este informe. También resulta realmente sugerente el reflexionar sobre el papel que podría adoptar el uso de las nuevas tecnologías en el futuro de la epidemiología y en otras áreas científicas de la medicina ahora que se ha dado pie a su uso en este ámbito de la vida.

Referencias

[1] "PREGUNTAS Y RESPUESTAS SOBRE LA APLICACIÓN DE LOCALIZACIÓN DE CONTACTOS Radar COVID-19." Accessed: Mar. 10, 2021. [Online].

[2] "Notificaciones de exposición: Ayuda para combatir el COVID-19 - Google." https://www.google.com/intl/es_us/covid19/exposurenotifications/ (accessed Mar. 10, 2021).

[3] "Rastreo de proximidad descentralizado para preservar la privacidad - Wikipedia, la enciclopedia libre." https://es.wikipedia.org/wiki/Rastreo_de_proximidad_descentralizado_para_preservar_la_privacidad (accessed Mar. 11, 2021).

[4] "POLÍTICA DE PRIVACIDAD DE LA APLICACIÓN Radar COVID." https://radarcovid.covid19.gob.es/terms-of-service/privacy-policy.html (accessed Mar. 11, 2021).

[5] "Condiciones de uso | Radar covid19." https://radarcovid.gob.es/condiciones-de-uso (accessed Mar. 11, 2021).

[6] "BOE.es - BOE-A-2010-1330 Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica." https://www.boe.es/eli/es/rd/2010/01/08/3 (accessed Mar. 11, 2021).

[7] "TousAntiCovid: respuestas a sus preguntas - Ministerio de Solidaridad y Salud." https://solidarites-sante.gouv.fr/soins-et-maladies/maladies/maladies-infectieuses/coronavirus/tousanticovid (accessed Mar. 11, 2021).

[8] "Coronavirus: New App to Track Nearby Positive Cases Available to Download - Hungary Today." https://hungarytoday.hu/coronavirus-hungary-app-virusradar/ (accessed Mar. 11, 2021).

[9] "Descargar 'Self-Quarantine Safety Protection App' con antelación 상세보기|AvisosConsulado General de la República de Corea en Barcelona."

http://overseas.mofa.go.kr/es-barcelona-es/brd/m_21212/view.do?seq=33 (accessed Mar. 11, 2021).

[10] "• Coronavirus: casos confirmados por día España 2020-2021 | Statista." https://es.statista.com/estadisticas/1104275/casos-confirmados-de-covid-19-por-dia-espana/ (accessed Mar. 12, 2021).

[11] "El fracaso de Radar Covid: sólo rastrea 32.000 contagios de entre 1,6 millones." https://www.elindependiente.com/futuro/inteligencia-artificial/2021/01/20/el-fracaso-de-radar-covid-solo-rastrea-32-000-contagios-de-entre-1-6-millones/ (accessed Mar. 12, 2021).

[12] "'Radar Covid': ¿Es posible revertir el fracaso de la app?" https://www.consalud.es/pacientes/especial-coronavirus/radar-covid-es-revertir-fracaso-app-rastreo-contacto_90855_102.html (accessed Mar. 12, 2021).

[13] "'Si no metes el código, es como si no estuvieras infectado': lo que Radar COVID no tiene en cuenta | Sociedad | Cadena SER." https://cadenaser.com/ser/2020/10/18/sociedad/1603037603_279692.html (accessed Mar. 12, 2021).

[14] "¿Han servido para algo las 'apps' de rastreo de la covid-19? | Compromiso Empresarial." https://www.compromisoempresarial.com/opinion/2021/01/fracaso-apps-rastreo-covid19/ (accessed Mar. 12, 2021).

[15] "Does Bluetooth drain battery? We ran some smartphone tests to find out." https://www.androidauthority.com/does-bluetooth-drain-battery-1145853/ (accessed Mar. 12, 2021).

[16] "Política de privacidad." https://www.whatsapp.com/legal/updates/privacy-policy/?lang=es (accessed Mar. 12, 2021).

[17] "Alemania: los datos, gráficos y mapas más recientes sobre el coronavirus." https://graphics.reuters.com/world-coronavirus-tracker-and-maps/es/countries-and-territories/germany/ (accessed Mar. 12, 2021).

[18] "covid-19_instant_tracing/Epidemiological_Impact_of_the_NHS_COVID_19_App_Public_Release_V1.pdf at master · BDI-pathogens/covid-19_instant_tracing · GitHub." https://github.com/BDI-pathogens/covid-19_instant_tracing/blob/master/Epidemiological_Impact_of_the_NHS_COVID_19_App_Public_Release_V1.pdf (accessed Mar. 12, 2021).

[19] "How Israel's COVID contact tracing app rollout went wildly astray | CIO." https://www.cio.com/article/3591570/how-israels-hamagen-contact-tracing-app-rollout-went-wildly-astray.html (accessed Mar. 13, 2021).

[20] J. Choi, S. Lee, and T. Jamal, "Smart Korea: Governance for smart justice during a global pandemic," *Journal of Sustainable Tourism*, vol. 29, no. 2–3, pp. 540–549, 2021, doi: 10.1080/09669582.2020.1777143.