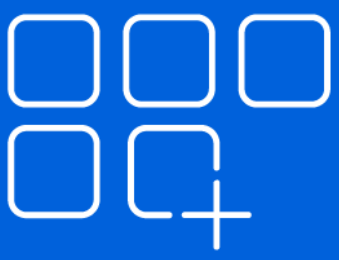
CENTRO
LATAM
DIGITAL

Tecnologías de interés público: el caso de las coronapps en América Latina



Escrito por: **Jacobo Nájera y Paola Ricaurte**

Edición: **Centro de Política Digital para América Latina, A.C.**

Diseño y diagramación: **Ápice Estudio**

Este trabajo deriva del estudio preliminar "Tecnologías frente a la pandemia: análisis del manejo de datos, el papel de los intermediarios y la privacidad en las aplicaciones desarrolladas por gobiernos de América Latina" realizado para el Centro de Investigación y Docencia Económicas, A.C. (CIDE) en 2020.

Este trabajo se llevó a cabo gracias a la subvención concedida por el Centro Internacional de Investigaciones para el Desarrollo (IDRC), Ottawa, Canadá.

Las opiniones aquí expresadas no representan necesariamente las del IDRC o su Junta de Gobernadores.

CENTRO
LATAM
DIGITAL

Índice

Autores

Jacobo Nájera
Tecnólogo e investigador en derechos humanos. Ha contribuido con investigación aplicada para la Free Software Foundation, Wikimedia, UNAM, y el laboratorio Stratosphere IPS de la Universidad Técnica Checa. Le fue otorgado junto a otros colegas el premio de periodismo Gabo 2019, en la categoría de innovación. Participa del desarrollo de la red Tor desde América Latina.

Paola Ricaurte
Profesora investigadora asociada del Tecnológico de Monterrey. Facultad Asociada del Berkman Klein Center for Internet & Society de la Universidad de Harvard. Co-fundadora de la red Tierra Común; integrante del comité de expertos de México en la Alianza Global para la Inteligencia Artificial, la Alianza A+ por los Algoritmos Inclusivos y el Sistema Nacional de Investigadores.

Introducción

Ante la crisis sanitaria mundial desencadenada a inicios de 2020 por la pandemia de Covid-19, los gobiernos del mundo reaccionaron de múltiples maneras. Sus acciones buscaron solventar el déficit de recursos para diagnosticar la enfermedad, de personal para atender pacientes y de mecanismos para dar seguimiento a los contagios. A la vez, se hizo apremiante la necesidad de acceder a datos e información de calidad para la definición de políticas públicas y para que las personas tomaran decisiones informadas con respecto a su salud.

Una de las primeras respuestas desplegadas por los gobiernos nacionales fue el desarrollo de aplicaciones móviles para hacer disponible información oportuna acerca del estado de la pandemia, ofrecer la posibilidad de realizarse un autodiagnóstico o, en algunos casos, hacer seguimiento de contactos. Para generar evidencia que permita evaluar el desarrollo de tecnologías de interés público[1], realizamos el análisis sociotécnico de nueve aplicaciones móviles (coronapps) desarrolladas por distintos gobiernos nacionales de América Latina (Bolivia, Brasil, Chile, Colombia, Ecuador, Guatemala, México, Perú, Uruguay) para enfrentar la pandemia causada por el virus SARS-CoV-2.

En el diseño de la investigación[2] se contemplan los siguientes objetivos: en primer lugar, *identificar* las funcionalidades ofrecidas por las aplicaciones y el tipo de datos recogidos; en segundo lugar, *analizar* a través de qué intermediarios operan dichas aplicaciones; y, por último, *evaluar* las políticas de privacidad para identificar prácticas de riesgo o de impacto en la privacidad de los datos. A partir del análisis de estas tres dimensiones: las funcionalidades de la aplicación a través de las interfaces de usuario; los actores intermediarios a través del análisis del tráfico de red; y las políticas de privacidad, se buscará caracterizar las prácticas de los gobiernos nacionales de América Latina en el diseño y desarrollo de tecnologías de interés público, en específico de las aplicaciones desarrolladas para combatir la pandemia. A partir de este ejercicio, se busca ofrecer un panorama que posibilite identificar los desafíos y las oportunidades para el desarrollo de tecnologías de interés público en el futuro.

El ecosistema de coronapps en América Latina

Como hemos mencionado, a partir de la pandemia de Covid-19, los gobiernos nacionales en América Latina respondieron con soluciones tecnológicas, en este caso aplicaciones móviles, para ofrecer y generar información en tiempo real con el fin de monitorear y predecir el curso de la enfermedad. Sin embargo, no fueron únicamente los gobiernos los que ofrecieron estas alternativas. En la región podemos identificar cinco actores en el desarrollo de aplicaciones móviles en respuesta al coronavirus: los gobiernos nacionales, los gobiernos locales, las organizaciones de la sociedad civil[3], los

[1] Abordamos la tecnología de interés público como un conjunto de praxis heterogéneas que plantean una conversación sobre los beneficios y daños de la tecnología digital, en este caso para la salud pública y su relación con otros derechos humanos como la privacidad. También recuperamos de la tecnología de interés público el ejercicio de exponer y discutir los valores con los que están alineadas las tecnologías y sus diseños, al igual que las medidas que pudieran contribuir a reducir los riesgos y daños. (Costanza-Chock et al. 2018)
[2] El análisis de los datos se llevó a cabo durante junio de 2020, aunque la recolección de datos se realizó entre abril y junio.
[3] Ese es el caso de Oxfam en Guatemala.

organismos internacionales[4] y las empresas privadas. Estas, además, conviven con aplicaciones apócrifas que buscan aprovecharse de la coyuntura para robar datos de sus usuarios.[5] Esta amplia oferta de desarrollos muestra la capacidad de reacción de los distintos actores sociales frente a la enfermedad y conforman un escenario que puede ser difícil de navegar para una persona usuaria.

En los países que decidieron implementar la funcionalidad del seguimiento de contactos se generaron, por un lado, reacciones de la sociedad civil frente al riesgo de violaciones de la privacidad y, por otro, dudas acerca de la capacidad de los estados para desarrollar aplicaciones sin depender de las grandes corporaciones tecnológicas.[6]

La lista de aplicaciones desarrolladas por los gobiernos nacionales frente a la pandemia en la región es la siguiente:

PAÍS	NOMBRE DE LA APLICACIÓN
ARGENTINA	CUIDAR
BRASIL	Coronavírus SUS
BOLIVIA	Bolivia Segura
CHILE	Coronapp
COLOMBIA	CoronApp-Colombia
COSTA RICA	EDUS (Incorporaron funcionalidades para Covid-19 a la aplicación Expediente Digital Único desarrollada antes de la pandemia por el sector Salud)
CUBA	COVID-19-InfoCU
ECUADOR	Salud EC
EL SALVADOR	N/A
GUATEMALA	Alerta Guate
HAITÍ	N/A
HONDURAS	Te Cuido
MEXICO	COVID-19MX
NICARAGUA	N/A
PANAMÁ	Protégete con Salud
PARAGUAY	CovidPy
PERÚ	Perú en tus manos

[4] Deutsche Belle (25 de mayo de 2020). El BID lanzó la aplicación David-19, con alcance en toda la región. Prensa Libre. https://www.prensalibre.com/internacional/deutsche-welle-internacional/david-19-la-aplicacion-para-combatir-el-coronavirus-en-america-latina-de-forma-anonima/

[5] AFP. (10 de junio de 2020). Aplicaciones falsas de rastreo del coronavirus buscan robar datos personales. MNS. https://www.msn.com/es-us/noticias/otras/aplicaciones-falsas-de-rastreo-del-coronavirus-buscan-robar-datos-personales/ar-BB15j3jz

[6] Dave, P. y Nellis, S. (7 de mayo de 2020). Problemas de la aplicación de coronavirus en Colombia muestran camino difícil sin tecnología de Apple y Google. Reuters. https://lta.reuters.com/articulo/salud-coronavirus-colombia-apps-idLTAKBN22J2YJ-OUSLT

REP. DOMINICANA	COVID-RD
URUGUAY	Coronavirus UY
VENEZUELA	N/A

En el caso de esta investigación, nos limitamos al análisis comparativo de nueve aplicaciones oficiales de gobiernos nacionales latinoamericanos, por considerar que en el caso de la crisis sanitaria los gobiernos nacionales son los que enmarcan la política pública. Estas coexisten con otras similares desarrolladas por gobiernos a nivel local, que tienen la capacidad de tomar decisiones que en ocasiones reflejen divergencias con respecto al contexto nacional. La muestra se determinó de manera intencional a partir de la disponibilidad de la aplicación en la tienda desde el lugar de conexión y la posibilidad de acceso a las funcionalidades sin requerir datos personales que no pudiéramos proveer.

Las aplicaciones que se contemplaron para esta investigación son Alerta Guate (Guatemala), Bolivia Segura, Coronapp Chile, CoronApp Colombia, Coronavírus SUS (Brasil), Coronavirus UY (Uruguay), Perú en tus manos y Salud EC (Ecuador). A continuación, presentamos las aplicaciones analizadas, el número de descargas, las reseñas de los usuarios en las tiendas (AppStore y Google Play), la población total del país, las cifras de contagios y decesos reportados en el momento de realización del estudio. (Tabla 1)

Tabla 1. Tabla de coronapps analizadas (junio de 2020)

PAÍS	APLICACIÓN	DESCARGAS	RESEÑAS	POBLACIÓN	CONTAGIOS	MUERTES
BRA	Coronavírus SUS	5,000,000+	3.0/5 con 3,100 reseñas, 3.6/5 con 20,537 reseñas	212,537,568	1,233,147	55,054
BOL	Bolivia Segura	50,000+	3.3/5 con 54 reseñas, 3.5/5 con 576 reseñas	11,670,183	28,503	913
CHI	Coronapp (Chile)	100,000+	2.4/5 con 418 reseñas	19,113,705	259,064	4,903
COL	CoronApp-Colombia	10,000,000+	2.5/5 con 45 reseñas, 3.8/5 con 67,515 reseñas	50,874,063	80,599	2,654
ECU	Salud EC	100,000+	2.7/5 con 29 reseñas, 2.7/5 con 1,065 reseñas	17,638,063	53,156	4,343
GUA	Alerta Guate	No disponible	No disponible	17,908,815	15,619	623
MEX	COVID-19MX	500,000+	4.2/5 con 567 reseñas, 3.6/5 con 3321 reseñas	128,910,809	202,951	25,060

PER	Perú en tus manos	1,000,000+	2.9/5 con 8503 reseñas	32,963,598	268,602	8,761
UY	Coronavirus UY	500,000+	4.1/5 con 36 reseñas, 3.9/5 con 4,087 reseñas	3,473,578	907	26

Propuesta analítica

Como eje de esta investigación, nos planteamos la siguiente pregunta general: ¿Qué características y patrones es posible identificar en el diseño y despliegue de coronapps como tecnología de interés público propuesta por los gobiernos nacionales latinoamericanos frente a la pandemia provocada por el virus SARS-CoV-2? De ella, se desprenden tres preguntas específicas: ¿Qué funcionalidades ofrecen estas aplicaciones?; ¿Cuáles son los principales intermediarios en la cadena de suministro de las aplicaciones?; ¿Qué prácticas se evidencian en las políticas de privacidad y el manejo de datos personales? Para responder a estas preguntas, el estudio contempla un modelo analítico (Tabla 2) que considera las siguientes dimensiones:

1. **Funcionalidades:** menú de opciones o posibilidades que ofrece la aplicación a través de la interfaz gráfica de usuario. Se realizó el análisis del tipo de datos provistos y recolectados por las aplicaciones, menú de opciones.
2. **Intermediarios:** los proveedores de conectividad de internet, infraestructura en centros de datos y servicios *over-the-top*. Se realizó el análisis de las conexiones destinos y de las infraestructuras que dependen cada una de las aplicaciones para su funcionamiento desde la óptica de la comunicación a nivel red.
3. **Políticas de privacidad y términos de uso de las aplicaciones:** conjunto de términos que establecen el marco legal que ampara el uso de la aplicación. Se realizó el análisis de los acuerdos y condiciones que establecen cada una de las aplicaciones desde la óptica de la privacidad, el tratamiento de los datos y sus responsables.

El modelo analítico propuesto busca articular una dimensión técnica, a través del análisis del tráfico de red para identificar a los intermediarios, junto con el análisis de las funcionalidades de la aplicación y las políticas de privacidad desde la interfaz de usuario. Consideramos que esta perspectiva que involucra el análisis de las funcionalidades, los intermediarios y las políticas de privacidad, provee la evidencia empírica necesaria para evaluar la pertinencia del desarrollo de tecnologías de interés público en sus distintas capas. Así, buscamos abonar al debate sobre los desarrollos tecnológicos por parte del sector público a través de una propuesta analítica que contemple la complejidad del fenómeno y que provea mayores elementos para elaborar una política tecnológica integral. Esperamos que este esquema analítico sea considerado un primer paso en la construcción de indicadores para evaluar los desarrollos tecnológicos en el contexto regional. A partir de estas dimensiones, se identificaron las características y patrones existentes en las aplicaciones analizadas.

Resultados y análisis

A continuación, presentamos los resultados del análisis de las tres dimensiones que componen el estudio. Consideramos que esta propuesta de análisis es la más

adecuada, frente a otras que se basan únicamente en el aspecto de la privacidad. Esta consideración estriba en que este estudio trata de poner en contraste las posibilidades que ofrece la aplicación a la persona usuaria (funcionalidades), la infraestructura que la sostiene (los intermediarios) y los datos recogidos (las políticas de privacidad) como parte de una propuesta para realizar una evaluación integral de tecnologías de interés público desarrolladas por los gobiernos.

1. Funcionalidades

Para el análisis de las funcionalidades se realizó la captura de las especificidades de cada aplicación desde la interfaz del usuario.[7] Los criterios para la sistematización de los datos recogidos por las aplicaciones se separaron en dos campos: por una parte, los datos generales sobre el diseño de la aplicación (información disponible en la tienda)[8] y, por otra, la caracterización de sus funcionalidades. A partir del análisis, es posible observar que con excepción de la aplicación COVID-19MX o Coronavírus-SUS en las que se puede utilizar todas las funcionalidades sin proveer datos personales, las aplicaciones requieren en general los datos personales de los usuarios (nombre, domicilio, edad, sexo, teléfono celular), o los datos del documento de identidad y que pueden ser cruzados con las bases de datos de los registros civiles (Ecuador) o prestadores de Salud (Uruguay) para corroborar su veracidad. En algunos casos requieren la activación forzosa del GPS (Ecuador) para utilizarla. En la matriz de funcionalidades podemos observar que los servicios que ofrece la aplicación son en realidad limitados: la mayoría ofrece autodiagnóstico, cifras, línea de atención, mapas (de centros de salud o de la distribución del contagio en el territorio), información general sobre el virus y la enfermedad, preguntas frecuentes. A cambio, como mencionamos, la mayor parte de esas aplicaciones requiere compartir ubicación y datos personales. Algunas de ellas (Colombia, Uruguay, Perú) ofrecen la funcionalidad de alerta de exposición.

A continuación, describimos los rubros que fueron considerados para el análisis (Tabla 2):

Tabla 2. Análisis de funcionalidades

1. Menú: si aparece o no una opción de menú (independientemente de si existen varias funcionalidades).
2. Seguimiento de contactos: si presenta la funcionalidad de trazabilidad.
3. Autodiagnóstico y diagnóstico de familiares/prueba de síntomas: conjunto de preguntas para constatar la evidencia de síntomas de la persona usuaria.

[7] Como se ha observado en otros análisis técnicos (Fundación Karisma, 2020), los gobiernos realizan actualizaciones de las aplicaciones que pueden modificar sus funcionalidades, por tanto, es importante aclarar que este ejercicio reporta los datos documentados en el momento de captura. Sería importante realizar una actualización del análisis para comprobar qué tipo de funcionalidades han sido modificadas en versiones posteriores. Las fechas de captura de datos de tráfico de red de las aplicaciones para este estudio fueron las siguientes:
Covid-19 mx: 2020-04-12
Coronapp Colombia: 2020-05-18
Coronavirus SUS: 2020-05-21
Alerta Guate: 2020-06-08
Perú en tus manos: 2020-06-09
Coronavirus uy: 2020-08-19
Coroapp Chile: 2020-06-15
Bolivia Segura: 2020-06-23
Salud EC: 2020-06-08

[8] Estos datos ya no fueron integrados en este reporte, pero constan de los siguientes rubros: sistemas operativos en los que funciona, solicitud de datos para ingresar a la aplicación, solicitud de datos para realizar diagnóstico, disponibilidad de código fuente, licencia, descripción de la aplicación, políticas de privacidad, idiomas, edad, developer (declarado en la tienda).

4. Solicitud de datos: qué tipo de datos solicita la aplicación para operar.

5. Geolocalización: si la aplicación ofrece la opción de geolocalización (obligatoria u opcional).

6. Información básica sobre el coronavirus: si se habla de aspectos básicos del virus, qué es, cómo se propaga, etc.

7. Cifras y gráficas: si ofrece cifras actualizadas de la enfermedad y mapas de las zonas de contagio.

8. Alerta sobre presencia del virus en la zona/avance del coronavirus en general: si ofrece la opción de alertar sobre el virus en la zona donde vive la persona usuaria.

9. Compartir ubicación/Monitoreo de datos en tiempo real/Seguimiento activo: si se encuentra la función de compartir ubicación para monitorear datos en tiempo real y realizar seguimiento activo.

10. Mapa: tipo de mapa y herramienta de mapeo (Google Maps, Apple Maps, Open Street Maps).

11. Comunicados oficiales: si se ofrecen comunicados oficiales sobre la enfermedad.

12. Noticias: si se despliegan noticias de medios digitales o redes sociales.

13. Agendar cita médica/calendario: si es posible agendar una cita en un centro de salud y marcar en el calendario.

14. Línea de atención: si se encuentra disponible desde la app una línea de atención al usuario.

15. Acceso desde fuera del territorio: si es posible acceder a la aplicación desde fuera del país.

16. Responsable de la recolección de datos: si se encuentra declarada la entidad responsable de la recolección de datos

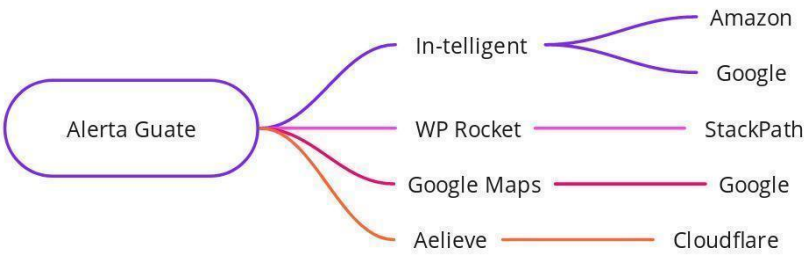
2. Intermediarios

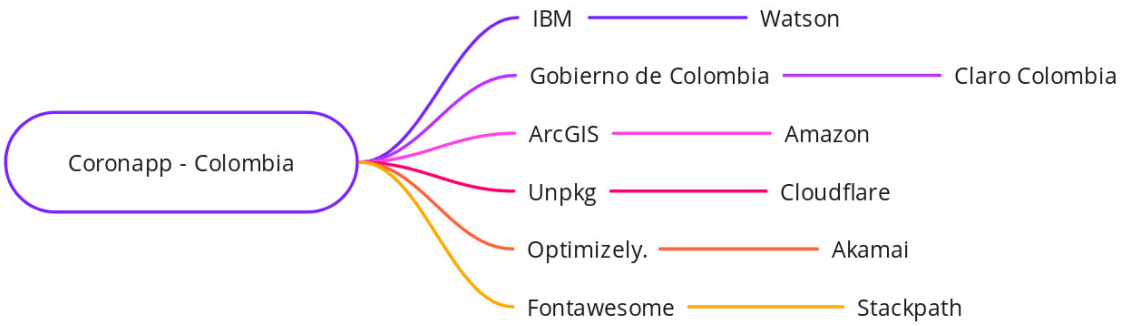
Para conocer los intermediarios de cada aplicación realizamos captura de tráfico de red durante un promedio de hora y media por aplicación en un ambiente controlado, previamente documentado y dedicado para la captura, tanto para el sistema operativo Android como iOS. Las capturas fueron resultado de grabar en tiempo real los paquetes TCP transmitidos y recibidos por la red a la cual los teléfonos fueron conectados, para un análisis posterior. Adicionalmente, realizamos capturas aleatorias para contrastar los hallazgos. En nuestro análisis de tráfico de red nos enfocamos en la capa de aplicación considerando como referencia conceptual el modelo OSI, para conocer los destinos IP y de dominio asociados y necesarios para el funcionamiento de cada aplicación.

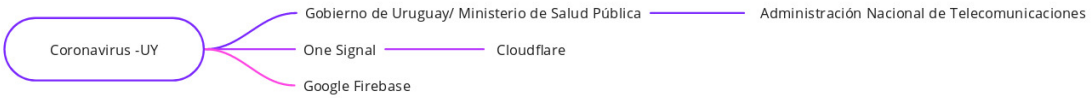
En el conjunto total de los análisis de tráfico de red de las nueve aplicaciones, documentamos que dependen de una gran variedad de intermediarios, que se pueden organizar en las siguientes categorías: redes de distribución de contenidos, telemetría, computación en la nube, servicios de cartografía y aprendizaje automático. Además, las aplicaciones en varios casos acceden a la tecnología subyacente instalada de manera previa en el teléfono móvil, tanto para Android como iOS, como parte de la instalación

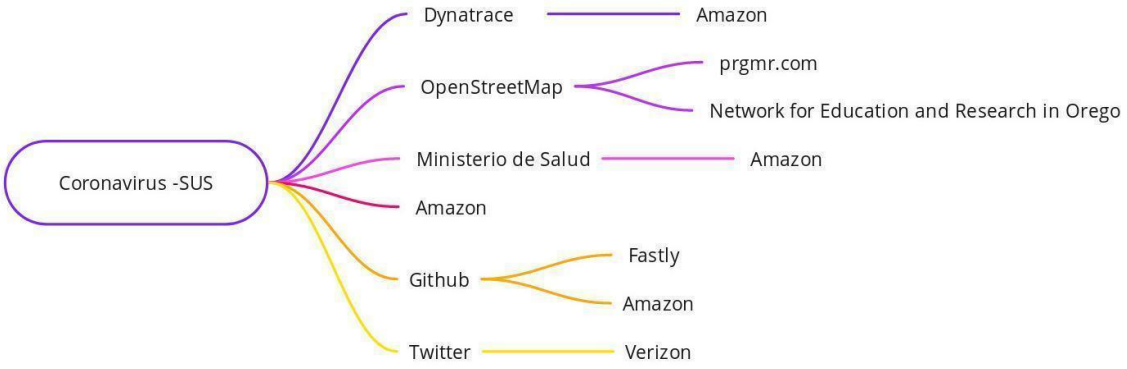
estándar del fabricante. Así ocurre, por ejemplo, para acceder al GPS o Bluetooth o interactuar con las tiendas de aplicaciones, como Google Services.

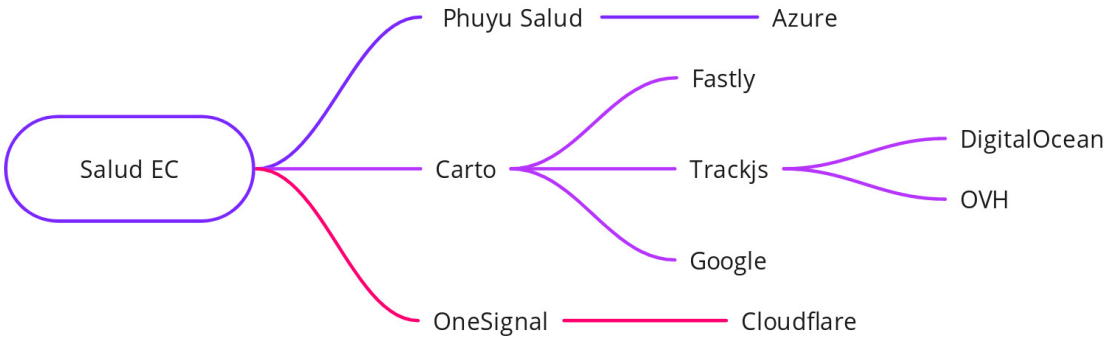
A continuación, presentamos los diagramas resultantes del reconocimiento de los servicios intermediarios, que fueron documentados durante la investigación a través del análisis de los destinos IP y de dominio. De esta manera fue posible identificar los actores y servicios asociados. En cada diagrama se mantiene la relación de dependencia entre servicios de acuerdo con su organización en términos de la arquitectura de red.

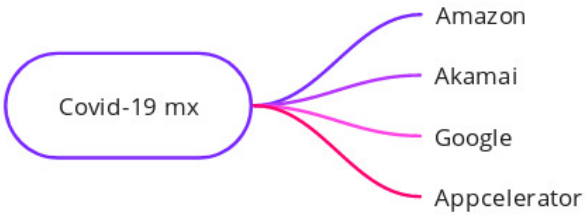


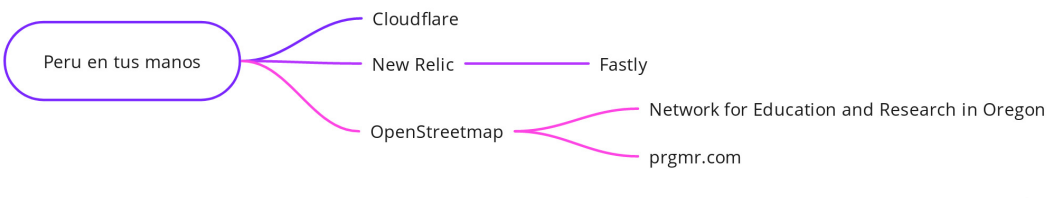



Coronavirus -UY
Gobierno de Uruguay/ Ministerio de Salud Pública
Administración Nacional de Telecomunicaciones
One Signal
Cloudflare
Google Firebase


Coronavirus -SUS
Dynatrace
Amazon
OpenStreetMap
prgmr.com
Network for Education and Research in Orego
Ministerio de Salud
Amazon
Amazon
Github
Fastly
Amazon
Twitter
Verizon


Salud EC
Phuyu Salud
Azure
Carto
Fastly
Trackjs
DigitalOcean
OVH
Google
OneSignal
Cloudflare


Covid-19 mx
Amazon
Akamai
Google
Appcelerator


Peru en tus manos
Cloudflare
New Relic
Fastly
OpenStreetmap
Network for Education and Research in Oregon
prgmr.com

Los diagramas permiten distinguir claramente un patrón o una tendencia a que las aplicaciones se ejecuten en una variedad de servicios especializados, que luego deriven a dos o tres infraestructuras finales comunes, salvo algunas excepciones de servicios. Esto plantea varias cuestiones de índole económica, política, técnica y legal. En primer lugar, el hecho de que las aplicaciones se desplieguen en las infraestructuras de intermediarios dominantes puede resultar en que los gobiernos favorezcan la concentración económica de ciertos actores preponderantes. En segundo lugar, en términos políticos, convierte a los gobiernos en clientes de empresas tecnológicas de las cuales depende para su operación general, restándole autonomía. En tercer lugar, en términos técnicos, de seguridad y privacidad, la multiplicidad de servicios implica que más actores están involucrados en las distintas capas del manejo de los datos. Es decir, hay más posibilidades de vulnerabilidad asociadas a las políticas propias de cada intermediario y las propias prácticas en el aseguramiento de los datos. Y, al mismo tiempo, cuando los intermediarios son grandes corporaciones tecnológicas, para ciertos actores sociales representan mayor seguridad en el manejo de los datos frente a gobiernos autoritarios o que no se caracterizan por un manejo responsable de los datos.

3. Políticas de privacidad y términos de uso

En esta propuesta de sistematización, como tercera dimensión, desarrollamos un marco en el que buscamos identificar varios criterios asociados con la privacidad y el manejo de los datos. Estos criterios son la política de privacidad (general o específica), la entidad responsable de la recolección de los datos, la finalidad de la aplicación, la limitación del propósito y la finalidad del tratamiento, la limitación de la conservación, la anonimización, la limitación de responsabilidad, la limitación del acceso, la seguridad de los datos, la transferencia, la accesibilidad de la política, la confidencialidad, el consentimiento, que explicaremos brevemente a continuación.

1. **Políticas de privacidad y términos de uso:** el desarrollo de una política de privacidad desarrollada de manera específica para la aplicación dentro de la legislación vigente o si se acogen al marco legal de protección de datos personales del país de manera general.

2. **Responsable de la recolección de datos:** quién es la entidad que aparece como responsable de la recolección de datos. Lo recomendable es que, por tratarse de una tecnología de interés público, la entidad responsable de los datos recogidos por la aplicación sea una entidad pública.

3. **Finalidad de la aplicación:** si en las políticas se describe el propósito que cumple la aplicación y si los datos que se recogen cumplen esa finalidad.

4. **Limitación del propósito y finalidad del tratamiento:** si se establecen límites al propósito de la aplicación y se hace explícito el tratamiento que se le dará a los datos.

5. **Limitación de la conservación:** si se establecen límites temporales a la conservación de los datos.

6. **Anonimización de datos:** proceso en el que son desagregados los datos personales de los datos. Desde el diseño del tipo de recolección y su tratamiento.

7. **Limitación de responsabilidad:** La declaración del grado de responsabilidad que tienen las diferentes instituciones y empresas sobre el tratamiento y protección de datos.

8. **Limitación del acceso:** mecanismos lógicos y acuerdos que orientan la seguridad de la información.

9. **Seguridad de los datos:** proceso que gestiona la disponibilidad, integridad y confiabilidad de los datos, como de los sistemas de los que dependen para su procesamiento, acceso y resguardo.

10. **Transferencia:** los diferentes acuerdos de intercambio de datos entre los diferentes actores e instituciones que participan del proceso de recolección, resguardo y procesamiento.

11. **Accesibilidad de la política:** si la política de privacidad es fácilmente accesible desde la aplicación y si se encuentra disponible para acceso fuera de la aplicación.

12. **Confidencialidad:** estado en el que se logra que la información sea accesible únicamente por quien está autorizado y acordado.

13. **Consentimiento:** si se solicita consentimiento para el manejo de datos recabados por la aplicación o si la recolección de datos se ampara en un marco legal más amplio.

Las políticas de privacidad de las aplicaciones analizadas dan cuenta de las variaciones en el tratamiento de los datos personales por parte de los gobiernos nacionales. En el análisis fue posible observar que, en la mayoría de los casos, no existe especificidad en cuanto a los criterios analizados. La falta de especificidad en los documentos de políticas de privacidad y términos de uso resultan un laberinto difícil de seguir para las personas usuarias, puesto que implica en ocasiones remitirse a la Ley de Protección de Datos Personales vigente en el país, que puede estar dispersa en varios documentos. A continuación, presentaremos tres casos salientes en cuanto a malas prácticas en el desarrollo y el manejo de los datos: Alerta Guate, Salud EC y CoronApp Colombia.

Caso: Alerta Guate

Entre las aplicaciones analizadas está el caso de Alerta Guate, que materializa las peores prácticas para el desarrollo de aplicaciones por parte de un gobierno. La aplicación fue desarrollada por la compañía In-telligent con base en Chicago, IL, quien además aparece como la entidad responsable de la recolección de los datos. Las políticas de privacidad mencionan que se conceden los datos a la compañía por 10 años y contempla su venta a terceros. Las políticas de privacidad desarrolladas por la compañía se encuentran disponibles únicamente en inglés. Este caso paradigmático nos sirve para evidenciar la relevancia de que los gobiernos establezcan marcos regulatorios para la privacidad de los datos que se encuentren centrados en derechos humanos y, también, como es el caso del manejo de datos personales sensibles (como los datos de salud), que exista una política de soberanía de datos.

Caso: Salud EC

Otro caso destacado es el de Ecuador. La aplicación, desarrollada por una empresa privada, declara: “PRICH para la funcionalidad de su aplicación móvil SaludEc, se acoge a los postulados legales de tratamiento de datos personales, así como al artículo 11 del Decreto Presidencial de Estado de Excepción N° 1017 emitido con fecha 16 de marzo de 2020, que cita textualmente:

> Artículo 1.- Para el cumplimiento de las restricciones del presente Decreto se podrán utilizar plataformas satelitales y de telefonía móvil para monitorear la ubicación de personas en estado de cuarentena sanitaria y/o aislamiento obligatorio, que incumplan las restricciones

dispuestas, a fin de ponerlas a disposición de las autoridades judiciales y administrativas competentes.

Es decir que la combinación de los datos de geolocalización, los datos ofrecidos a través de la línea de ayuda (171), el mapeo de lugares de aglomeración[9], con el decreto especial emitido por el gobierno, permite que una persona que no cumpla con su domicilio de cuarentena, pueda ser sujeto de penalidades judiciales o administrativas. La aplicación, al momento de utilizarla, solicita que se declare que la persona usuaria se encuentra en el lugar designado para su cuarentena. Es decir, funciona como una medida tecnológica de control de la población.

Caso: CoronApp Colombia

El caso de Colombia, que ha sido analizado ampliamente por la Fundación Karisma (Botero, 2020), también es otro ejemplo de malas prácticas basadas en hipótesis especulativas sobre la eficacia de las aplicaciones para contener los contagios. Después de que la funcionalidad de seguimiento de contactos presentara fallas, tuvo que ser eliminada y sustituida por el servicio ofrecido por Apple y Google. Las políticas de privacidad de CoronApp Colombia, un documento de 26 páginas, detalla la finalidad de la recolección. Entre ellas está la de "Acceder a la conexión Bluetooth del dispositivo para compartir con el INS la cercanía, en los últimos 21 días con otros dispositivos móviles que utilizan CoronApp, con la finalidad de saber si una persona confirmada con COVID-19 estuvo cerca del usuario e identificar potenciales cadenas de contagio del COVID-19. Esta funcionalidad se encuentra desactivada por defecto y sólo se activará para los usuarios confirmados por COVID-19 y aquellos que tengan síntomas muy probables de contagio. Aún así, la información será enviada sólo cuando los usuarios deseen compartir su historial de cercanías a través del menú de CoronApp Colombia."

Conclusión

A través de este análisis se propuso abordar, por una parte, la relación que existe entre las tecnologías y los intermediarios y, por otra, entre los procesos de desarrollo y los principios legales y éticos. A pesar de la heterogeneidad de opciones que encontramos en las distintas dimensiones de las aplicaciones analizadas (las funcionalidades de las aplicaciones, la red de intermediarios que permiten su operación y los marcos legales bajo los cuales se rigen), es posible identificar algunos patrones que sintetizamos a continuación.

1. Las aplicaciones

- Entre las funcionalidades de las aplicaciones se encuentran el auto-diagnóstico, el acceso a información sobre el virus, el mapeo de la infraestructura hospitalaria (en algunos pocos casos disponibilidad), análisis y gestión de la movilidad, esto último por medio de la analítica y la telemetría de plataformas socio-digitales y la tecnología subyacente de los sistemas operativos de Apple y Google.

2. Los intermediarios

- A partir del análisis del tráfico de red es posible identificar los servicios y proveedores utilizados por los gobiernos y entender las dinámicas y tendencias que existen en el ecosistema de intermediarios. Existe un patrón recurrente en los servicios utilizados por los gobiernos para el desarrollo y funcionamiento de

[9] Mintel presenta en Quito plataforma Covid-19 para mapear la emergencia. *El Comercio*. https://www.elcomercio.com/actualidad/michelena-alban-yunda-plataforma-covid19.html

apps. La principal concentración recae en las compañías Google y Amazon. Esta evidencia debería conducir a una reflexión sobre la necesidad de políticas públicas orientadas a la soberanía tecnológica y la soberanía de datos que permitan a los estados ser capaces de gestionar sus propias infraestructuras bajo los máximos estándares de seguridad y robustez. Los gobiernos dependen de las infraestructuras provistas por empresas tecnológicas extranjeras que se han consolidado como actores transnacionales con enorme poder político dentro de la sociedad digital.

3. Las políticas de privacidad y los términos de uso

- Las políticas de privacidad y los términos de uso aplicables a los servicios ofrecidos por las aplicaciones son insuficientes, poco accesibles o incomprensibles para un público general. La heterogeneidad de estructura y planteamiento dificulta la legibilidad, no ofrece la información necesaria y las garantías suficientes para que las personas usuarias tengan certeza y autonomía sobre sus datos.

Recomendaciones para políticas públicas

En el contexto de la pandemia de Covid-19 se desarrollaron aplicaciones móviles adoptadas por gobiernos de América Latina. Estas aplicaciones tienen características variadas en cuanto a las funcionalidades, los intermediarios, las políticas de privacidad y el manejo de los datos. A través de las aplicaciones, observamos cómo las políticas públicas sanitarias de los diversos gobiernos de América Latina reflejan sus visiones con respecto a los mecanismos idóneos para paliar la pandemia pero, además, el paradigma científico-técnico al que se adscriben.

El análisis de las funcionalidades, los intermediarios y las políticas de privacidad permitió visibilizar las dimensiones asociadas al diseño, desarrollo y uso de las aplicaciones, sus oportunidades y riesgos. Los diversos actores (gobiernos, empresas y sociedad civil) deben tener claras las dimensiones y los elementos que, desde el diseño y la arquitectura, se encuentran relacionados con las políticas de privacidad y términos de uso, pero también con las posibilidades del despliegue y eficacia de las tecnologías para atender los problemas para los cuales fueron diseñadas. A partir de este análisis, planteamos las siguientes recomendaciones de carácter general y específico para orientar las políticas públicas asociadas al desarrollo de tecnologías de interés público en un marco de respeto a los derechos humanos. Esperamos que los hallazgos y las recomendaciones plasmadas en este reporte contribuyan en términos de incidencia a generar estándares, protocolos e indicadores que sean contemplados en el diseño de tecnologías de interés público en la región.

1. Evaluar el propósito del desarrollo de tecnologías de interés público

Como punto de partida, es necesario identificar, definir y discutir la problemática que se busca atender y los objetivos que se busca alcanzar para evaluar si el despliegue de una tecnología de interés público (en este caso una aplicación) está justificado. Realizar este ejercicio permite además evaluar el tipo de diseño más adecuado y sus límites. Es importante, en varios momentos del proceso, sopesar si las motivaciones y los fines esperados de la aplicación se cumplen, es decir si la aplicación permite en la práctica atender efectivamente la problemática. Este análisis es necesario para entender el papel que juega la tecnología en la atención de problemas sociales y los límites asociados a cada implementación tecnológica, además de considerar su ciclo de vida y desarrollo.

2. Establecer acuerdos legales, técnicos y mecanismos de transparencia y rendición de cuentas en la relación con intermediarios privados

En el caso de que los gobiernos deban recurrir a la renta o uso de servicios especializados para la operación de infraestructuras tecnológicas para su gestión o para el desarrollo de tecnologías de interés público, es necesario que se definan los tipos de acuerdos en las políticas de privacidad, seguridad y desarrollo. Además, es necesario que estos acuerdos se rijan bajo políticas de transparencia, auditabilidad y rendición de cuentas.

Los gobiernos deben garantizar, en los acuerdos contractuales y legales con los intermediarios, el cumplimiento de las políticas de privacidad, pero además las condiciones técnicas y controles de ciberseguridad robustos para su salvaguarda. Y a la vez, los gobiernos, deben estar sujetos a leyes de transparencia y rendición de cuentas que garanticen el manejo responsable de los datos. Es decir, para el desarrollo de tecnologías de interés público, es necesario contemplar las dimensiones económicas, políticas, técnicas y legales que permitan tener un plano de control técnico común alrededor de todos esos servicios, en términos de seguridad, así como de desarrollo y privacidad.

3. Definir los principios del diseño y la implementación

Cualquier solución tecnológica debe considerar los principios éticos de respeto de la autonomía, proveer beneficios de salud, promover la justicia, prevenir nuevas infecciones sin causar daño, proteger la privacidad (Gasser, 2020).

4. Garantizar el derecho a la privacidad

El desarrollo de tecnologías de interés público debe responder a un marco regulatorio de derechos para la protección de datos. Privacy International (2018) propone siete principios básicos para la protección de datos: lealtad, legalidad y transparencia, limitación de finalidad, minimización, exactitud, limitación de la conservación, Integridad y confidencialidad y principio de responsabilidad. En caso de datos de salud, las garantías del respeto a los derechos humanos debe maximizarse. Por ejemplo:

a) **Limitación en la recopilación de datos:** Entre las consideraciones se encuentran: 1) Limitar la cantidad de datos recopilados y brindar posibilidad de acceso sin registros, 2) anonimización de los datos como política de reducción de daños sin perder los objetivos, 3) ofrecer mecanismos alternativos e interoperables de acceso a las tecnologías móviles para permitir a las personas decidir sobre sus derechos, 4) establecer mayores contrapesos desde la arquitectura, de tal manera que se centren en las decisiones de las personas y las protejan del abuso, 5) tener en cuenta que, en tecnologías que por diseño suelen estar expuestas a múltiples actores y modelos de negocio, existen mayores probabilidades de riesgo puesto que la recopilación de datos se ajusta a múltiples políticas de privacidad en función de cada uno de los términos establecidos por los intermediarios.

b) **Duración y retención de datos:** Un aspecto en la recolección de datos por las aplicaciones que llamó nuestra atención durante la investigación es el relativo a la duración de la retención de datos. Este es un aspecto que, en general, no se define con claridad salvo en la aplicación Alerta Guate, cuyas políticas de privacidad plantean que la compañía desarrolladora podrá mantener los datos personales por 10 años. La definición con claridad en los términos de uso y privacidad sobre la temporalidad de la retención de los datos recolectados puede contribuir a abordar las problemáticas asociadas a la recolección y procesamiento de acuerdo con los fines y motivaciones definidas en función del

beneficio esperado y así dimensionar los riesgos de daño.

c) **Datos responsables:** los gobiernos deben desarrollar un marco regulatorio integral y desde una perspectiva de datos responsables que ponga en el centro a las personas y sus derechos. En el caso de los datos personales sensibles, como los de salud, no es posible negociar la privacidad ante hipótesis de un beneficio común sin ofrecer evidencia empírica que lo demuestre.

5. Realizar un monitoreo sistemático, establecer indicadores y publicar reportes técnico-científicos

Durante el despliegue de tecnologías de interés público se debe garantizar que estas cumplan los propósitos para los cuales fueron diseñadas. Para esto, es necesario monitorear de manera sistemática y evaluar su implementación a través de indicadores y la publicación de reportes técnico-científicos regulares que garanticen la rendición de cuentas ante la ciudadanía y que esta pueda a su vez ser partícipe de la evaluación de su funcionamiento.

6. Garantizar la disponibilidad e integridad técnica de los datos

La concentración y centralización de los intermediarios, desde una perspectiva técnica, aumenta los riesgos de crear un único punto de falla para todo el ecosistema tecnológico en América Latina. Por ejemplo, presenta un sistema más vulnerable frente a un ataque informático o algún tipo de corte o interferencia en conectividad, energía eléctrica y suministros, o la propia pérdida o daño de los activos digitales. Para este punto se recomienda la exploración de modelos alternativos tecnológicos propios y regionales, en materia de desarrollo, despliegue y mantenimiento.

Referencias

- Access Now (2020). Recommendations on privacy and data protection in the fight against COVID-19. https://www.accessnow.org/cms/assets/uploads/2020/03/Access-Now-recommendations-on-Covid-and-data-protection-and-privacy.pdf
- Apple (2020, abril 10). Apple and Google partner on COVID-19 contact tracing technology. *Apple Newsroom* https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/
- AFP (2020, junio 10). Aplicaciones falsas de rastreo del coronavirus buscan robar datos personales. *AFP*. https://www.msn.com/es-us/noticias/otras/aplicaciones-falsas-de-rastreo-del-coronavirus-buscan-robar-datos-personales/ar-BB15j3jz
- Botero, C. (2020, mayo 16) CoronApp Colombia será amigable con la privacidad... ¿de verdad? Recuperado de https://www.elespectador.com/opinion/coronapp-colombia-sera-amigable-con-la-privacidad-de-verdad-columna-919831/
- Costanza-Chock, S. Wagoner, M., Taye, B., Rivas, C., Schweidler, C., Bullen, G. & the T4SJ Project, (2018). #MoreThanCode: Practitioners reimagine the landscape of technology for justice and equity. Research Action Design & Open Technology Institute. Recuperado de https://morethancode.cc.
- Dave P. y Nellis S. (2020, mayo 7). Problemas de la aplicación de coronavirus en Colombia muestran camino difícil sin tecnología de Apple y Google. *Reuters*. https://lta.reuters.com/articulo/salud-coronavirus-colombia-apps-idLTAKBN22J2YJ-OUSLT

- Deutsche Welle (2020, mayo 25). David-19, la aplicación para combatir el coronavirus en América Latina de forma anónima. *Prensa Libre*. https://www.prensalibre.com/internacional/deutsche-welle-internacional/david-19-la-aplicacion-para-combatir-el-coronavirus-en-america-latina-de-forma-anonima/
- Díaz A. (2020, marzo 25). Alerta Guate, la aplicación de la controversia. *RelatoGT*. https://www.relato.gt/tecnologia/alerta-guate
- EFE. (2020, junio 16). AI alerta de que algunas apps para rastrear la COVID-19 violan los derechos humanos. *Aguas Digital*. http://aguasdigital.com/actualidad/leer.php?idnota=16609661&t=e
- Forbes. (2020, mayo 14). Global Witness muestra preocupación por la aplicación "Alerta Guate". *Forbes Centroamérica*. https://forbescentroamerica.com/2020/05/14/global-witness-muestra-preocupacion-por-la-aplicacion-alerta-guate/
- Fundación Karisma (2020). Análisis de la aplicación CoronApp. Informe sintético de análisis técnico. https://web.karisma.org.co/wp-content/uploads/2020/04/Informe-p%C3%BAblico-t%C3%A9cnico-CoronApp-v170320-1-1.pdf
- Gasser, U., Ienca, M., Scheibner, J. Sleigh, J. & Vayena, E. (2020). Digital tools against COVID-19: taxonomy, ethical challenges, and navigation aid. *The Lancet*. https://doi.org/10.1016/S2589-7500(20)30137-0
- Global Witness. (2020, mayo 16). Investigación revela riesgos de privacidad en app "Alerta Guate". *Soy 502*.https://www.soy502.com/articulo/ong-investigo-riesgos-privacidad-app-alerta-guate-101025
- Google (2020, abril 10). Apple and Google partner on COVID-19 contact tracing technology. *Google Company News*. https://blog.google/inside-google/company-announcements/apple-and-google-partner-covid-19-contact-tracing-technology
- Ministerio de Salud Pública. Uruguay. (2020, junio 29). Información sobre la Aplicación Coronavirus UY. *gub.uy*. https://www.gub.uy/ministerio-salud-publica/politicas-y-gestion/informacion-sobre-aplicacion-coronavirus
- Ministerio de Salud Pública. Uruguay. (2020, junio 29). Guía para usuarios de la aplicación Coronavirus UY . https://www.gub.uy/ministerio-salud-publica/politicas-y-gestion/informacion-sobre-aplicacion-coronavirus
- Nazareno A. (2020, marzo 24). "Alerta Guate" La nueva app para que todo los guatemaltecos estén comunicados. *Deguate*. https://www.deguate.com/artman/publish/noticias-guatemala/alerta-guate-la-nueva-app-para-que-todo-los-guatemaltecos-esten-comunicados.shtml
- Panzarino M. (2020, abril 10). Apple and Google are launching a joint COVID-19 tracing tool for iOS and Android. *Techcrunch* https://www.theverge.com/2020/4/10/21216484/google-apple-coronavirus-contract-tracing-bluetooth-location-tracking-data-app
- Privacy International (2018). *Guía de protección de datos personales*. https://www.privacyinternational.org/es/report/2255/guia-de-proteccion-de-datos-personales-completa
- Tecno D. (2020, marzo 25). Así funciona la app Salud EC que promueve el Gobierno ante el coronavirus. *El Universal*. https://www.eluniverso.com/noticias/2020/03/25/nota/7794474/salud-ec-coronavirus-ecuador-citas-emergencia