Bogotá D.C., 3 de septiembre de 2021

Corte Constitucional
Honorable Magistrado
Alejandro Linares Cantillo

Asunto Expediente T- 8'197.643 - *Amicus curiae*

Accionantes: Juanita Goebertus Estrada
Alejandra Martínes Hoyos
Sol Marina de la Rosa Flórez
Claudia Julieta Duque

Accionados: Ministerio de Salud
Instituto Nacional de Salud
Aeronáutica Civil de Colombia
OPAIN S.A
Aeropuertos de oriente S.A.S
Airplan S.A.S

Cordial saludo,

Gaspar Pisanu, abogado, en mi carácter de Líder de Políticas Públicas para América Latina de la organización internacional de derechos humanos Access Now, me permito dirigirme a Usted, con el fin de solicitarle de la manera más respetuosa nos permita, como organización de sociedad civil, presentar una intervención en el presente proceso, amparándonos en el inciso segundo artículo 13 del Decreto 2591 de 1991 que establece "quien tuviere un interés legítimo en el resultado del proceso podrá intervenir en él como coadyuvante del actor o de la persona o autoridad pública contra quien se hubiere hecho la solicitud".

Access Now es una organización internacional sin ánimo de lucro, que desde su fundación en 2009, trabaja para defender y extender los derechos digitales de usuarios en riesgo alrededor del mundo. Nuestros temas de trabajo incluyen conectividad, acceso a internet, neutralidad de la red, libertad de expresión, privacidad, protección de datos personales, ciberseguridad, entre otros.

En el documento adjunto, remitimos a la Honorable Corte Constitucional nuestra intervención a manera de *amicus curiae* en relación con el expediente T-8'197.643 para contribuir con las valoraciones que este Alto Tribunal efectúe acerca del uso obligatorio de la aplicación CoronApp, su impacto en el derecho a la privacidad y a la protección de los datos personales y consideraciones respecto a la característica de rastreo de contactos en aras de enriquecer la discusión jurídica pero sobre todo, poder aportar elementos que permitan en última instancia amparar los derechos reclamados por las tutelantes.

Agradecemos su atención y quedamos a su disposición en caso de que sea oportuno ampliar el detalle de las razones que se expondrán a continuación.

Cordialmente

Gaspar Pisanu
Lider de Políticas Públicas para América Latina
Access Now
gaspar@accessnow.org

***

1. Los hechos del caso

Las señoras Claudia Julieta Duque, Juanita Goebertus, Sol Marina de la Rosa y Alejandra Martínez, acudieron a la acción de tutela el 27 de noviembre del año anterior para reclamar el amparo de sus derechos al *habeas data*, la libertad de locomoción y la unidad familiar, luego de haber sido obligadas en reiteradas ocasiones a descargar y registrarse en la aplicación móvil CoronApp como requisito previo para embarcar a sus vuelos a destinos nacionales.

Obligación que, en todo caso, había sido impuesta en su momento en la resolución[1] expedida por el Ministerio de Salud que impuso, entre los protocolos de bioseguridad que fueron habilitando progresivamente el regreso de ciertas actividades económicas, incluyendo las del sector aeronáutico, que se "*recomendara*" a los pasajeros el uso de la aplicación y se "*verificara*" el diligenciamiento de la funcionalidad de autodiagnóstico que ésta despliega.

Dicha acción, interpuesta contra las autoridades encargadas o partícipes del despliegue de la aplicación móvil[2] y las autoridades que condicionaron el ingreso a las instalaciones aeroportuarias en cada caso[3], fue fallada el día 11 de diciembre del mismo año por el Juzgado Cuarenta y Tres Administrativo de Oralidad del Circuito de Bogotá -Sección Cuarta-.

[1] Inicialmente se trató de la Resolución 1517 de 2020, que fue reiterada en 2021 a través de la Resolución n. 411 que expresamente obligaba al uso de la aplicación para volar a destinos nacionales.
[2] Ministerio de Salud y Protección Social, Agencia Nacional Digital e Instituto Nacional de Salud
[3] Aeronáutica Civil de Colombia (Aerocivil), OPAIN S.A, Aeropuertos de oriente S.A.S, y Airplan S.A.S

En dicho fallo se negaron las pretensiones de las accionantes. Sobre el derecho de *habeas data,* dicha negativa se fundó en que no se había configurado una vulneración en tanto que no se había probado que las entidades accionadas hubieran incurrido en "la transferencia o uso indebido de los datos personales de las aquí demandantes"[4], en desprecio de toda consideración sobre la importancia del consentimiento informado y la voluntad como principio indispensable de la protección de datos.

Frente a los otros derechos, el fallo estimó su improcedencia en tanto que las limitaciones a derechos durante la emergencia sanitaria y el Estado de excepción se había considerado como legítima.[5]

Más adelante, en segunda instancia[6] se mantuvo el sentido del fallo de la primera pese a que el escrito de impugnación radicado por las tutelantes dejó claro que, de acuerdo con una lectura sistemática de la Resolución 1517 de 2020 y la política de protección de datos de la aplicación CoronApp, su uso y descarga no podía ser obligatorio y que, aun cuando lo fuera, dicha obligación según la Ley Estatutaria de Protección de Datos 1581 de 2012 no sería en todo caso legal ni proporcional.

Es de hacer notar que en segunda instancia, sin embargo, solo un magistrado del Tribunal Administrativo de Cundinamarca concedió a las tutelantes la razón. En el texto de su salvamento de voto se lee que "el uso del canal digital [haciendo referencia a CoronApp] es voluntario y las personas pueden elegir si lo descargan y lo utilizan y no puede ser una acción obligatoria para los pasajeros, quienes pueden optar por otras modalidades de supervisión de los protocolos de bioseguridad. Circunstancia, que permitiría que a las peticionarias no se les exigiera el uso de la herramienta digital a la hora de viajar".[7]

Posteriormente, el fallo de segunda instancia fue remitido el 23 de febrero de 2021 a la Corte Constitucional cuya Sala de Selección Sexta, en audiencia del 29 de junio, decidió seleccionarlo para resolver el conflicto de derechos planteado por las tutelantes. Entre los problemas jurídicos que podrían llegar a ser advertidos por la Honorable Corte Constitucional, se encuentran los siguientes:

1. El análisis de impacto de las apps para el covid-19 en la privacidad y protección de datos de las personas, con un énfasis en el consentimiento de las personas.

---

[4] Ver pág 20, fallo de primera instancia del Juzgado Cuarenta y Tres Administrativo de Oralidad del Circuito de Bogotá -Sección Cuarta-, proferido el 11 de diciembre de 2020, radicación 1100133370432019-00319

[5] Ver pg. 23 fallo de primera instancia Juzgado Cuarenta y Tres Administrativo de Oralidad del Circuito de Bogotá -Sección Cuarta-, proferido el 11 de diciembre de 2020, radicación 1100133370432019-00319

[6] Emitido por el Tribunal Administrativo de Cundinamarca, Sección Tercera - Subsección B, Magistrado Ponente Henry Aldemar Barreto Mogollón, del 18 de febrero de 2021

[7] Ver pág 4, salvamento de Voto suscrito por el Magistrado Ponente Franklin Pérez Camargo, del 19 de febrero de 2021

2. El impacto en la transparencia y el acceso a la información de las políticas de privacidad de las apps para el covid-19, en tanto que la política de tratamiento de datos de CoronApp sigue conteniendo previsiones contradictorias que afirman a un mismo tiempo la libertad de las personas para usarla y la obligación que tienen de permanecer en ella una vez registran sus datos.
3. Riesgos para el secreto profesional de personas que ejercen el periodismo producto del uso obligatorio de apps para el covid-19 -recordando que una de las tutelantes es periodista-.

En el apartado que sigue, esta intervención se centrará específicamente en el impacto de las aplicaciones móviles utilizadas para combatir la crisis del COVID-19 y la necesidad de transparentar su desarrollo y utilización. Haremos especial foco en la aplicación CordonApp y los riesgos de forzar a la ciudadanía a utilizarla.

2. Intervención

2.1. Consideraciones preliminares

Access Now se encuentra comprometida a proteger los derechos humanos y a colaborar con la respuesta de los gobiernos frente al brote de la enfermedad del sars-covid-2 (COVID-19)[8]. Estas respuestas deben promover la salud pública sin dejar de lado otros derechos humanos como a la no discriminación, el acceso a información confiable y oportuna, la privacidad y la protección de los datos personales.

Comprendemos que las leyes nacionales e internacionales reconocen que las circunstancias extraordinarias requieren medidas extraordinarias. Esto significa la posibilidad de restringir algunos derechos fundamentales, incluidos los derechos a la privacidad y la protección de datos. Sin embargo, esto no lo convierte en una situación extralegal, sino que el imperio de la ley debe permanecer vigente, y se deben establecer limitaciones de tiempo y de alcance. Un estado de excepción no hace lícita a cualquier medida que se adopte en consecuencia.

Los derechos humanos fundamentales se deben seguir respetando durante los regímenes de excepción o los períodos de emergencia. Las restricciones de derechos solo deben aplicarse cuando esto sea necesario para prevenir y mitigar los riesgos que provoca la crisis en cuestión, y las medidas restrictivas no deben extenderse más allá del alcance estrictamente necesario y proporcional para las exigencias de las circunstancias.

[8] Access Now elaboró a inicios de 2020 la guía “Recomendaciones para la protección de la privacidad y los datos en la lucha contra el covid-19” y la publicación “Privacidad y salud pública: qué hacer y qué no en el desarrollo de aplicaciones de rastreo de contactos para combatir el COVID-19”. Más información en: https://www.accessnow.org/cms/assets/uploads/2020/04/Recomendaciones-para-la-proteccio%CC%81n-de-la-privacidad-y-los-datos-en-la-lucha-contra-el-COVID-19.pdf y https://www.accessnow.org/privacidad-y-salud-publica-que-hacer-y-que-no-en-el-desarrollo-de-aplicaciones-de-rastreo-de-contactos-para-combatir-el-covid-19/

2.2. Recopilación y uso de datos de salud

La información de salud es privada y sensible por naturaleza y revela detalles íntimos sobre la vida de las personas. Por esa razón, el tratamiento de esta información debe ser estrictamente limitado, tal como lo dispone el Artículo 6 de la Ley 1581. No obstante, en una crisis de la salud pública, el dilema no es si los gobiernos pueden usar los datos de salud para ayudar a combatir la crisis, sino cómo deben hacerlo para garantizar la dignidad y la privacidad individual en la mayor medida posible.

La información de salud recolectada debe ser rigurosamente protegida. Esto implica no solo establecer mecanismos de protección frente a ataques externos sino también limitar el acceso a quienes necesitan esta información para realizar tratamientos, investigaciones o acciones de otros tipos para abordar la crisis. Bajo ninguna circunstancia los datos de salud se deben vender o transferir a terceros que no trabajen en áreas de interés público.

El acceso irrestricto, las filtraciones de datos y divulgar información relacionada con la salud durante la crisis del COVID-19 (incluidos los resultados positivo o negativo de una persona) no solo incrementa los desafíos relacionados con la protección de la privacidad y los datos personales, sino que también pone en peligro la seguridad y el orden público, genera riesgos de discriminación y hasta puede provocar ataque físicos o en línea y amenazas de muerte[9]. Estos peligros son reales en Colombia donde incluso el personal de salud ha sido discriminado y agredido por la ciudadanía[10].

Para evitar generar estas consecuencias, los principios y derechos a la privacidad y la protección de datos deben continuar aplicándose. Entre ellos destacamos:

- La recopilación de datos de salud, así como su uso, divulgación, almacenamiento y otros procesamientos, deben limitarse a lo estrictamente necesario para la lucha contra el virus. Una pandemia no es una excusa para recopilar grandes cantidades de datos innecesarios.
- El acceso a los datos de salud debe limitarse a quienes necesitan esta información para realizar tratamientos, investigaciones o acciones de otros tipos para abordar la crisis. Estos datos se deben almacenar de manera segura en una base de datos separada.
- Los datos procesados en respuesta a la crisis solo se deben conservar mientras esta se encuentre vigente. Una vez finalizada la pandemia, se debe borrar la mayor parte de la información sanitaria, aunque algunos datos no identificables pueden retenerse con fines de investigación y registro histórico. Estos datos solo deben ser accesibles y utilizados con estos fines de interés público.
- Bajo ninguna circunstancia los datos de salud se deben vender o transferir a terceros que no trabajen en áreas de interés público.

[9] The New York Times. ”As Coronavirus Surveillance Escalates, Personal Privacy Plummets”. 2020. https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html
[10] Agencia EFE. “La COVID-19 desata la discriminación en Colombia contra quienes salvan vidas”. 2020. https://www.efe.com/efe/america/sociedad/la-covid-19-desata-discriminacion-en-colombia-contra-quienes-salvan-vidas/20000013-4211172

La aplicación móvil CoronApp no ha cumplido desde su despliegue con la mayoría de estos requisitos[11]. En primer lugar, emplea de forma muy amplia las excepciones a) y c) del artículo 10 de la ley de protección de datos sin establecer límites respecto de los datos que serán recolectados ni dispone el plazo de conservación de los mismos. Tampoco plantea claramente cuáles autoridades tienen acceso a qué datos ni por cuánto tiempo.

Dada la recolección de información personal y sensible, los gobiernos deberían haber involucrado a las comunidades de expertos en privacidad y salud para colaborar en el desarrollo y la implementación de mecanismos de seguridad para el uso de datos. Las comunidades con riesgo de marginalización, incluidas las mujeres y las niñas, las personas en condición de discapacidad, las personas que pertenencen a las comunidades indígenas, las personas de bajos recursos, la comunidad LGBTQ y las minorías religiosas o étnicas, con frecuencia sufren de discriminación y no tienen acceso a servicios de atención médica.

También, personas en riesgo por el ejercicio de su profesión u oficio, como los líderes y lideresas sociales, así como las personas que ejercen el periodismo (como sucede con Claudia Julieta Duque) deben poder gozar de medidas diferenciales debido al impacto que genera la puesta en marcha de una aplicación altamente invasiva de su privacidad, que puede desincentivar a la persona a la realización de ciertas actividades cuando se ve obligada a registrarse y usar una aplicación móvil en la que debe entregar sus datos sensibles e información sobre su paradero y lugar de destino.

Por lo tanto, estos grupos también deberían haber sido consultados a la hora de crear salvaguardas específicas efectivas. La aplicación CoronApp no tuvo en cuenta estas ninguna de estas consideraciones.

2.2. Rastreo y datos de geolocalización

Los datos de ubicación revelan una gran cantidad de información sobre la persona y otras que se relacionan con ella. Tan solo hacer un seguimiento de los movimientos de una persona mediante los datos de ubicación que procesa un teléfono móvil, permite deducir su domicilio y lugar de trabajo, sus interacciones con otras personas, sus visitas al médico y su nivel socioeconómico, entre otros datos. Si no se aplican los mecanismos de protección adecuados, las herramientas de rastreo y geolocalización pueden permitir procesos de vigilancia ubicuos. Esto es especialmente riesgoso cuando se trata de comunidades que requieren una especial atención como periodistas, activistas, opositores y defensores de derechos humanos

Estos mecanismos de seguimiento conllevan una gran cantidad de aspectos problemáticos. En primer lugar, es importante tener en cuenta que el rastreo de la ubicación geográfica de los

[11] Análisis realizado en base a la “Política de tratamiento de información (PTI) relacionada con la CoronApp Colombia”. Disponible en: https://www.ins.gov.co/Normatividad/PoliticasInstitucionales/politica-de-tratamiento-de-informacion-coronapp-colombia.pdf

teléfonos inteligentes proporciona información sobre el movimiento de los teléfonos de las personas, no del virus. Hacer un seguimiento de la evolución de la enfermedad mediante referencias cruzadas entre los datos geográficos de las personas con los casos de infección conlleva riesgos inherentes. En segundo lugar, incluso la supuesta "información de ubicación anónima" se puede reidentificar fácilmente; un estudio de 2013 demostró que las personas se podían volver a identificar a partir de solo cuatro puntos de referencia[12]. Tercero, la ubicación geográfica no siempre es útil. Las personas pueden conducir, caminar, tomar el metro o trabajar en el 50.° piso de un edificio de 80 pisos, de modo que, además de sacrificar la privacidad de las personas, esta información no es veraz o completa[13]. Por último, los casos previos de uso de registros telefónicos y datos de ubicación para responder a crisis humanitarias demostraron no se efectivos ni eficientes[14].

Reportes como el publicado por el Instituto Ada Lovelace[15], demuestran que no hay claras evidencias de que este tipo de aplicaciones ayudan a aplanar la curva de contagios del virus, basados en la información disponible al día de hoy. Hay numerosos problemas que hacen que el virus SARS-CoV-2 sea difícil de rastrear lo cual pone en duda la eficacia de esta tecnología.

Otra consideración para evaluar la eficacia de estas aplicaciones es que las personas clasificadas como de “alto riesgo” de contraer el virus o que experimentan severas consecuencias producto del contagio, como los adultos mayores, personas con condiciones preexistentes, personas con discapacidad o personas en condiciones de pobreza, muchas veces no tienen un teléfono inteligente o no pueden utilizar la aplicación ya que son muy pocas las desarrolladas teniendo en cuenta problemas de accesibilidad. Esto significa que los datos obtenidos de estas aplicaciones excluyen información sobre el sector población más importante al cual se debe hacer seguimiento. Este aspecto afecta seriamente la eficacia de la aplicación de Colombia. De acuerdo a datos publicados por la Comisión Económica para América Latina y el Caribe (CEPAL) el 48% de la población no tiene acceso a internet, el índice de penetración de internet fijo es de apenas 37,5% y solo del 6,2% en el sector rural y centros urbanos pequeños[16].

Los países que ya utilizan estas tecnologías no han visto necesariamente mejores resultados en la lucha contra el virus. Por ejemplo, gobiernos de todo el mundo han elogiado el trabajo de Singapur al “aplanar la curva” debido al uso de la aplicación TraceTogether sin tener en cuenta las

[12] Wired. Anonymized Phone Location Data Not So Anonymous, Researchers Find, 2013. https://www.wired.com/2013/03/anonymous-phone-location-data/
[13] Lawfare. Location Surveillance to Counter COVID-19: Efficacy Is What Matters, 2020. https://www.lawfareblog.com/location-surveillance-counter-covid-19-efficacy-what-matters
[14] CIS-India. Ebola: A big data disaster, 2016. https://cis-india.org/papers/ebola-a-big-data-disaster
[15] Ada Lovelace Institute. COVID-19 rapid evidence review. 2020. https://www.adalovelaceinstitute.org/evidence-review/covid-19-rapid-evidence-review-exit-through-the-app-store/
[16] CEPAL. Universalizar el acceso a las tecnologías digitales para enfrentar los impactos del COVID-19. 2020. https://www.cepal.org/sites/default/files/presentation/files/final_final_covid19_digital_26_agosto.pdf

otras medidas adoptadas por el país. Incluso, la semana pasada el país tuvo que extender el confinamiento debido al surgimiento de nuevos casos de contagio[17].

En conclusión, las medidas de rastreo exponen información privada que no es necesariamente relevante en la lucha contra el coronavirus y que someten a toda la población a una situación de monitoreo y vigilancia[18]. Este tipo de medidas inherentemente producen interferencias con los derechos humanos, especialmente con el derecho a la privacidad. Por ello, es fundamental que respeten los estándares legales de necesidad y proporcionalidad, lo cual también aplica al desarrollo de aplicaciones de rastreo de contactos.

2.3. Uso obligatorio de las aplicaciones y consentimiento

Uno de los requisitos esenciales para asegurar la confianza en la gestión de la pandemia y evitar futuros abusos en materia de derechos humanos, es que estas aplicaciones sean de uso voluntario. Incluso aquellas aplicaciones desarrolladas tomando en cuenta las recomendaciones emanadas por organizaciones e instituciones internacionales y locales en materia de seguridad deben ser voluntarias y los gobiernos brindar medios alternativos menos invasivos para la recolección de datos y rastreo de contactos.

Como advierte la Organización Mundial de la Salud, las aplicaciones para combatir la pandemia del COVID-19, dada su baja efectividad, solo son una herramienta complementaria las cuales en ningún caso pueden reemplazar el rastreo de contacto realizado de forma personal y otras medidas tradicionales de salud pública[19].

Pese a que los términos y condiciones de CoronApp, el modelo de Política de Tratamiento de Información de la Superintendencia de Industria y Comercio y la Resolución 1517 del Ministerio de Salud y Protección Social explicitan que su uso es voluntario, casos como los que se encuentran ahora en su despacho muestran una obligatoriedad de facto al exigir la utilización de dicha herramienta para acceder a determinados servicios. Esto implica forzar a la ciudadanía a dar su consentimiento, haciendo que este sea nulo por no reunir uno de los requisitos esenciales de un consentimiento válido: que sea otorgado libremente.

Adicionalmente, posterior a la expedición de la Resolución 1517 a la que refiere el caso en concreto, más adelante el Ministerio de Salud de Colombia expidió la Resolución Nº 411 del 3 de marzo de 2021 que, de manera explícita, incluyó la obligación de uso de la aplicación móvil para poder ingresar a los aeropuertos del país[20].

[17] The Guardian. Singapore extends lockdown as Covid cases surge past 9,000. 2020. https://www.theguardian.com/world/2020/apr/21/singapore-coronavirus-outbreak-surges-with-3000-new-cases-in-three-days

[18] European Data Protection Board. Processing of personal data in the context of the COVID-19 outbreak, 2020. https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-covid-19-outbreak_en

[19] Organización Mundial de la Salud. RENEW EUROPE Webinar on COVID-19 contact tracing applications. 2020. https://re.livecasts.eu/webinar-on-contact-tracing-applications/

[20] Anexo de la Resolución 411 de 2021, señala sobre la obligatoriedad de CoronApp lo siguiente:

El uso obligatorio o forzado de la aplicación afecta uno de los ejes centrales de nuestros sistemas jurídicos democráticos, el principio de respeto por la autonomía privada. Imponer su obligatoriedad puede violar derechos humanos fundamentales, especialmente de aquellas personas que no tienen acceso a un teléfono inteligente. En general, bajo ninguna circunstancia puede ser obligatorio el uso de herramientas que socavan la privacidad, que son de dudosa eficacia y que pueden poner en peligro la seguridad de las personas[21].

Adicionalmente, la falta de transparencia y acceso a la información dificulta la supervisión y la rendición de cuentas por el uso de dichas tecnologías, impide garantizar que los datos recopilados y procesados sean seguros y solo accedan a ellos los profesionales de la salud pública, y que serán eliminados una vez que ya no sean necesarios. En contextos políticamente represivos, los ciudadanos no tienen acceso a un recurso o un lugar para el resarcimiento si el gobierno viola su privacidad y hace un uso indebido de sus datos.

3. Petición a la Honorable Corte Constitucional

En virtud de lo expuesto, solicitamos respetuosamente se nos reconozca como intervinientes en el presente proceso, de acuerdo al art. 13 del Decreto 2591 de 1991, por haber probado nuestro interés legítimo para tal efecto y en consecuencia, se sirva la Honorable Corte Constitucional conceder la razón a las tutelantes atendiendo, entre otras, las razones que fueron expuestas anteriormente y que pueden resumirse así:

- Es posible que algunos derechos fundamentales sean restringidos en situaciones de emergencia como la actual pandemia del COVID-19

"3.1.3.1.3 "Verificar que todos los pasajeros nacionales hayan diligenciado personalmente la información solicitada en la aplicación CoronApp-Colombia, sin perjuicio de la asistencia que le pueda brindar el personal del operador aeroportuario cuando lo requieran. Se permitirá excepcionalmente el ingreso de aquellas personas que manifiesten no tener un dispositivo celular inteligente.
3.1.3.1.4 Revisar el código QR de la aplicación CoronApp-Colombia de cada pasajero para confirmar que está habilitado para viajar (color verde) y no reporta alerta de ser positivo para COVID-19.
3.1.3.1.5 Impedir el ingreso a los pasajeros nacionales y al personal que trbaja en el aeropuerto que reporte en la aplicación CoronApp Colombia una prueba positiva en los últimos 14 dias para COVID-19", pg. 5
"3.2.2.2 Informar a todos los pasajeros nacionales al momento de la compra del tiquete y al hacer el *check in* o su registro electrónico que se verificará previo al ingreso al aeropuerto que deben instalar en sus celulares o dispositivos móviles la aplicación CoronApp-Colombia y diligenciar personalmente la información solicitada en esta", pg. 9 https://www.minsalud.gov.co/Normatividad_Nuevo/Resoluci%C3%B3n%20No.%20411%20de%202021.pdf

[21] Amnistía Internacional. Qatar: Fallo de seguridad en aplicación de rastreo de contactos expone datos personales confidenciales de más de un millón de personas. 2020. https://www.amnesty.org/es/latest/news/2020/05/qatar-covid19-contact-tracing-app-security-flaw/

- La situación de emergencia no implica una situación extralegal, el imperio de la ley permanece vigente y los derechos y principios en materia de privacidad y protección de datos personales deben continuar siendo aplicados.
- Los datos de salud son fundamentales para el combate de la pandemia, sin embargo, dada su naturaleza sensible su tratamiento debe ser estrictamente limitado.
- La ausencia de debidos protocolos de seguridad, como la restricción de acceso y medidas técnicas de seguridad, afectan no solo a la privacidad y los datos personales de la ciudadanía sino que amenazan a la seguridad y al orden público, genera riesgos de discriminaición y pone en riesgo la seguridad física y moral de las personas.
- La aplicación CoronApp, tanto en su etapa de desarrollo como de implementación, no ha cumplido con los requisitos necesarios para garantizar la seguridad de sus usuarios al no disponer límites de recolección de datos, cláusulas de caducidad, reglas claras para el acceso, ni ha involucrado en su diseño a las comunidades que pueden verse afectadas.
- El uso de aplicaciones de rastreo de contactos implica el tratamiento de información sensible (su ubicación en tiempo real) y la posibilidad de inferir más datos de esta naturaleza (lugar de trabajo, nivel socioeconómico, etc.)
- Las aplicaciones de rastreo de contacto no han demostrado ser útiles para el combate de la pandemia por las numerosas razones expuestas ut supra.
- Las aplicaciones que cuentan con esta característica se presentan como una amenaza para derechos fundamentales ya que pueden ser utilizadas abusivamente como herramientas de vigilancia masiva.
- Tratándose de datos sensibles, la ciudadanía sólo puede entregar dicha información voluntariamente de acuerdo a lo dispuesto por la ley de protección de datos personales.
- Hacer obligatorio el uso de las aplicaciones de salud y de rastreo de contactos se opone a principios de derechos humanos y en materia de protección de datos personales que no dejan de estar vigentes por la situación de emergencia.