ENFOQUES JURÍDICOS
REVISTA MULTIDISCIPLINAR DEL CEDEGS
ISSN 2683 2070
Número 04
julio-diciembre 2021

DOI: https://doi.org/10.25009/ej.v0i04.2572

Estado de Derecho y emergencia sanitaria

Recibido 29 marzo 2021-Aceptado 29 junio 2021

María del Rosario Huerta Lara*
Universidad Veracruzana. Xalapa-Veracruz, México
rhuerta@uv.mx

***RESUMEN**: Aunque el mundo contemporáneo ya se ha enfrentado al SARS, la influenza H1N1, el MERS y el Ébola, lo cierto es que la escala global del brote de COVID-19, en cada parcela del orbe, supera en todo cualquier precedente. En esta crisis se debate de como las posibles respuestas tecnológicas a emergencias sanitarias, también pueden ser ocasión para quebrantar elementos esenciales del estado de derecho.*

Existen evidentes afectaciones al derecho a la privacidad debido a las respuestas tecnológicas a la COVID-19 y a las prácticas de vigilancia digital realizadas con el empeño y patrocinio de gobiernos y empresas tecnológicas, en el contexto de la pandemia y fuera de ella. Este artículo resume cómo la privacidad y la vigilancia digital están previstas por la ley internacional, particularmente las regulaciones a la privacidad, aplicables a los datos de salud.

***ABSTRACT**: Although the world has faced SARS, H1N1 Influenza, Mers and Ebola, the global scale of COVID-19 outburst in every place of this world, exceeds all expectations and precedents. In this crisis different possible technological answers and sanitary emergencies are debated, it can also be time to infringe essential elements of the rules of law.*

There are evident affectations upon the right to privacy due to the technological responses to COVID-19 and to the surveillance practices employed in and out of of the pandemics context. This article summarizes how digital privacy and surveillance are provided by the international law, particularly the regulations to privacy, applicable to health data. It also tries to give a general description to the digital surveillance measures unfolded in times of COVID-19, besides sketching some international legal

* Investigadora del Instituto de Investigaciones Jurídicas de la Universidad Veracruzana.

ISSN 2683 2070
Número 04
julio-diciembre 2021

María del Rosario Huerta Lara

DOI: https://doi.org/10.25009/ej.v0i04.2572

Brinda una descripción general de las medidas de vigilancia digital desplegadas en tiempos de COVID-19, además de esbozar algunos estándares legales internacionales contra los cuales se debe evaluar la legalidad de las medidas de vigilancia relacionadas con la pandemia.

Palabras clave: *Estado de Derecho. Derecho a la privacidad. Derecho internacional público. Emergencia sanitaria. Tecnología digital. Vigilancia epidemiológica.*

standards against which the legality of the surveillance measures related to COVID must be evaluated.

Keywords: *Rules of law. Right to privacy. Public international rights. Sanitary emergency. Digital Technology, Epidemiological surveillance.*

Introducción

La situación de emergencia sanitaria global, causada por la pandemia COVID 19, bajo ninguna circunstancia debe ser causa para debilitar o reducir la obligación estatal de respetar los derechos fundamentales, con motivo de un peligro o desastre que requiera la acción inmediata de los poderes públicos. La salud pública puede invocarse como causal para limitar ciertos derechos, con el fin de permitir que un Estado tome medidas frente a una amenaza grave para la salud de la población o de sus miembros. Estas medidas deben estar dirigidas específicamente a prevenir enfermedades o lesiones, brindar atención a los enfermos y heridos. Sin embargo, en el espectro de las decisiones gubernamentales, ha sido constante divisa aquella referida a los *tiempos extremos que requieren medidas extremas,* para justificar decisiones autoritarias durante la gestión de la pandemia en la escala global y nacional.

Paradójicamente, las nuevas tecnologías digitales que podrían permitir a los estados la mejor cooperación y solidaridad en materia de salud global, también podrán aplicarse con oportunidad y atingencia como herramientas de vigilancia de personas y colectivos, sin excusa, para restringir o limitar derechos fundamentales, poniendo en juego el acceso a la justicia y la gobernanza, responsables de resolver y decidir estos dilemas de la *res publica*.

Las capacidades tecnológicas de la era digital, desarrolladas durante la gestión de la emergencia sanitaria, están influyendo en múltiples áreas del Derecho, desde los principios de Derecho internacional público de no intervención y prohibición del uso de la fuerza, hasta los derechos humanos tan fundamentales como son la vida, la salud, el disfrute de las libertades públicas, entre otros mandatos orientados a la tutela de la población vulnerable;

ISSN 2683 2070
Número 04
julio-diciembre 2021

DOI: https://doi.org/10.25009/ej.v0i04.2572

de los que no se puede sustraer el Estado mexicano, en virtud de la jurisdicción internacional.

Se ha advertido sobre los peligros de una *vigilancia digital* basada en las nuevas tecnologías, afirmando que "las pandemias, como otras emergencias, a menudo han sido momentos catalizadores para la expansión permanente del gobierno" (Giglio, M., 2020). El futuro se encuentra lejos de ser un nicho de privacidades y es posible que una vez pasada la pandemia no finalice esa cualidad de alerta extraordinaria que imbuye a las sociedades actuales. El escenario posterior, puede aumentar aún más las preocupaciones por este derecho. Los Estados y las entidades corporativas que ahora aprovechan el impulso de la crisis sanitaria para probar sus capacidades de vigilancia, deben rendir cuentas de los estándares de *legalidad*, *necesidad* y *proporcionalidad* de derechos humanos. La *transparencia* y *supervisión* de las medidas de vigilancia, deben cumplirse con la intervención de actores nacionales e internacionales.

Superando toda disyuntiva entre privacidad y salud, los ciudadanos tienen el derecho para exigir un sistema de vigilancia sanitaria que respete la privacidad con total eficacia. Las garantías del derecho internacional de los derechos humanos no deben ser omitidas ni suspendidas en tiempos de pandemia, debido a que su aplicación en varios escenarios y al mismo tiempo, brindan a los estados la discreción necesaria para ponderar entre las preocupaciones de privacidad, con la necesidad objetiva de recopilar información. La protección de la persona frente al surgimiento de las innovaciones tecnológicas, debe ser preocupación nuclear de las sociedades que propugnen la preservación de los derechos y las libertades públicas.

El derecho internacional de los derechos humanos proporciona a los estados, instrumentos jurídicos que prevén *derogaciones* y *limitaciones* al derecho a la privacidad. Es de esperar que los estados que recurren a medidas de vigilancia, basadas en la tecnología digital durante la pandemia, utilicen este conjunto de herramientas de manera responsable, en total cumplimiento con los requisitos tanto sustantivos como de procedimiento. Cualquier medida potencialmente intrusiva a la privacidad debe tener una base legal sólida y ajustarse al objetivo declarado de combatir la pandemia. El estado de derecho en cualquier país se basa en la noción de confianza en el gobierno. La capacidad de manejar una emergencia de salud pública sin caer en el *panóptico* de vigilancia,[1] descrito por Michel

[1] El panóptico era un tipo de arquitectura carcelaria ideada por el filósofo utilitarista Jeremy Bentham hacia fines del siglo XVIII. El objetivo de la estructura panóptica era permitir a su guardián, guarecido en una torre central, observar a todos los prisioneros, recluidos en celdas individuales alrededor de la torre, sin que estos puedan saber si son observados. Formulado por Michel Foucault a la par de la noción Biopolítica que da significado a un poder que ejerce una influencia positiva en la vida, que se esfuerza por administrarlo, optimizarlo y multiplicarlo sometiéndolo a controles precisos y regulaciones integrales.

ISSN 2683 2070
Número 04
julio-diciembre 2021

DOI: https://doi.org/10.25009/ej.v0i04.2572

Foucault en *Vigilar y Castigar* (Foucault, M., 2002: 184-186), es una base esencial para la confianza y prevalencia del estado de derecho.

1. De la privacidad y el Derecho internacional

El *derecho* a la *privacidad* está consagrado en los principales instrumentos internacionales y regionales de derechos humanos, incluido el Pacto Internacional de los Derechos Civiles y Políticos (PIDCP), el Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales (CEDH) y la Convención Americana sobre Derechos Humanos (CADH).

Estos instrumentos de derechos humanos protegen la vida privada y familiar de las personas de interferencias ilegales, así como su domicilio y correspondencia. El derecho a la privacidad no es absoluto. Las disposiciones de los tratados de derechos humanos sobre privacidad reconocen este derecho y proporcionan un marco para las limitaciones legales del mismo. El artículo 17 del Pacto Internacional de Derechos Civiles y Políticos (PIDCP, 1988) ordena que las interferencias al derecho a la privacidad no deben ser arbitrarias o ilegales. El artículo 11 de la CADH (1969) establece que las interferencias no deben ser *arbitrarias o abusivas*. El artículo 8 del CEDH (04 de noviembre de 1950) dispone que,

> no habrá injerencia de una autoridad pública en el ejercicio de este derecho, salvo que sea conforme a la ley y necesario en una sociedad democrática, en interés de la seguridad nacional, la seguridad pública, la economía, el bienestar del país, para la prevención de desórdenes o delitos, para la protección de la salud, para la protección de los derechos y libertades de los demás. (CEDH, 1950)

En el vasto cuerpo de jurisprudencia relacionada con la vigilancia, el Tribunal Europeo de Derechos Humanos (TEDH) proporciona orientación sobre cómo deben interpretar estas limitaciones al derecho a la privacidad.

En el caso *Klass y otros versus Alemania*, (TEDH, 1978) el TEDH dictaminó que la limitación del derecho a la privacidad, en forma de escuchas telefónicas e inspección del correo, era legal, en relación al Convenio Europeo para la Protección de los Derechos Humanos (CEPDH, 198: parágrafo 60, p 23). Empero, de conformidad con la interpretación del Comité de Derechos Humanos, tales medidas son calificadas *arbitrarias* e *ilegales*, como *interferencias* a la *privacidad*, en virtud del artículo 17 del Pacto Internacional de Derechos Civiles y Políticos (1988), cuya demostración procesal requirió resolver las siguientes cuestiones:

La de establecer si existió una interferencia con el derecho a la privacidad. Para lo cual se espera que los solicitantes demuestren que las medidas controvertidas existen de hecho y constituyen una interferencia con la privacidad. Aunque de hecho está entrelazado, este requisito es formalmente independiente de demostrar que los solicitantes califican como víctimas de la presunta violación (ya sea directa, indirecta o potencial). La condición de víctima, junto con otras condiciones, debe probarse para demostrar la admisibilidad de la

solicitud ante el TEDH, pero es distinta del análisis sustantivo de la presunta violación. (TEDH, Guía de admisibilidad, 2014)

La de establecer si la interferencia se llevó a cabo de conformidad con la ley. Este requisito incluye dos elementos, a saber: la interferencia con la privacidad debe tener una base en la legislación nacional y, en segundo lugar, que la ley sea lo suficientemente "previsible", para que los ciudadanos pueden comprender en qué circunstancias pueden ser en algún momento, objeto de alguna vigilancia; qué mecanismos de supervisión se instrumentaran para proteger sus derechos y cuándo se eliminarán los datos recopilados. Se debe puntualizar que muchos de los ordenamientos nacionales que sancionan la vigilancia son imprecisos y vagos, sin arreglo al derecho internacional.

La de establecer si es necesaria la *injerencia* del *Estado* en la *vida privada* de los *ciudadanos* (democracia, estado de derecho), con la finalidad de cumplir con un objetivo legítimo, fundado y motivado en la ley. Este requisito, a veces dividido en dos (necesidad en una sociedad democrática y objetivo legítimo), está destinado a evaluar la proporcionalidad de los *fines* de la vigilancia (por ejemplo, seguridad nacional, seguridad pública, bienestar económico del país, prevención de desórdenes o delitos, protección de la salud o la protección de los derechos y libertades de los demás) y los *medios*. Se espera que las medidas de vigilancia legales hagan solo lo que sea "estrictamente necesario" (Klass and Others v. Germany, 1978, para. 43) y el caso (Weber and Saravia v. Germany, 2006, para. 78: 17-18) para la consecución del objetivo legítimo declarado.

En *Weber y Saravia versus Alemania*, el TEDH, a pesar de declarar el caso inadmisible (2006: 18), elaboró una lista de salvaguardas mínimas que los gobiernos deben observar para resolver qué medidas de vigilancia se consideren legales. La lista, que pasó a denominarse *Weber Six* (Lubin, A., 2018: 543), incluye las siguientes categorías de información que deben estar disponibles para los posibles objetivos de la vigilancia, esto es: los motivos que pueden dar lugar a la vigilancia; las categorías de personas que podrían estar sujetas a ella; el límite de duración; el procedimiento a seguir para examinar, utilizar y almacenar los datos obtenidos; las precauciones que se deben tomar al comunicar los datos a otras partes; y las circunstancias en las que los datos recopilados puedan o deban ser borrados.

Las primeras decisiones en materia de vigilancia, resueltas por el TEDH, en el caso *Klass y Weber*, no pudieron considerar el devenir digital de la vigilancia, sin embargo, proveyeron un marco sólido para analizar las intrusiones a la privacidad basada en la tecnología. A partir del año 2013 (Greenwald, G., 2013) se incorpora a la discusión pública, dentro y más allá de los internacionales marcos de derechos humanos, la agenda de privacidad digital. Muchos de los parámetros en torno a las intrusiones digitales en la privacidad, se emitieron a través de las Naciones Unidas [NU], resoluciones de la Asamblea, decisiones del Consejo de Derechos Humanos de la Organización de las Naciones Unidas [ONU] (Consejo de Derechos Humanos [CDH], 24 de marzo de 2015; 22 de marzo de 2017), y los informes de expertos

ISSN 2683 2070
Número 04
julio-diciembre 2021

DOI: https://doi.org/10.25009/ej.v0i04.2572

independientes de la ONU. En 2015, el Consejo de Derechos Humanos de la ONU estableció un nuevo mandato del Relator Especial sobre el derecho a la privacidad (CDH, 1 de abril de 2015) para abordar sus dimensiones en el estado de vigilancia. Todos los informes del Relator Especial sobre el derecho a la privacidad, se encuentran disponibles en el sitio web (Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos [OACNUDH], 2016).

2. Regulación de datos de salud

Aunque las reglas generales sobre privacidad se aplican a todos los aspectos de la vida de una persona, incluido su historial médico, la protección de los datos relacionados con la salud está sujeta a garantías de privacidad adicionales. Un ejemplo útil es el Reglamento general de protección de datos de la Unión Europea (RGPD), en virtud de sus amplias garantías a la privacidad y una protección especial a los datos relacionados con la salud.

El artículo 1 del RGPD define los "datos relacionados con la salud" como "datos personales relacionados con la salud física o mental de una persona física, incluida la prestación de servicios de atención médica, que revelan información sobre su estado de salud" (RGPD, 2016, artículo 1 [15]). El artículo 9 del RGPD prohíbe el procesamiento de "datos relacionados con la salud", a menos que dicho procesamiento esté justificado por uno de los diez motivos enumerados (RGPD, 2016, artículo 9), que incluyen, entre otros, el consentimiento explícito, la protección de intereses vitales de los pacientes y el interés público en el área de la salud. En principio, la recopilación y el procesamiento de datos sanitarios están sujetos a los mismos criterios de limitación que se aplican a otras interferencias de la privacidad. Es necesario evaluar la necesidad y proporcionalidad de las medidas impuestas, así como la adecuación de su base jurídica. Sin embargo, el lenguaje de RGPD deja en claro que la sensibilidad particular de los datos de salud requiere un mayor grado de escrutinio al evaluar si la recopilación de datos es permisible. Sin embargo, existe un descargo de responsabilidad importante. Aunque los datos de salud personales son confidenciales y justifican un alto grado de protección contra interferencias ilegales, el uso de la vigilancia sigue siendo fundamental para responder a emergencias de salud pública.

Según la Organización Mundial de la Salud (OMS), la vigilancia de la salud pública es la recopilación, el análisis y la interpretación continua y sistemática de datos relacionados con la sanidad, que son esenciales para la planificación, implementación y evaluación de la práctica médica (Centro para el Control y la Prevención de Enfermedades, 2019). Es imperativo que los estados generen datos estadísticos *despersonalizados* en torno a las pandemias (número de casos registrados y las tasas de mortalidad) disponibles para el público. Este tipo de vigilancia, a diferencia del rastreo de contactos individualizado, no afecta directamente las libertades individuales ni amenaza con revelar datos personales. Si bien, el riesgo de que los datos sean robados o filtrados como resultado de una intrusión de terceros, es en gran medida una cuestión de seguridad de los datos, más que de la

ISSN 2683 2070
Número 04
julio-diciembre 2021

DOI: https://doi.org/10.25009/ej.v0i04.2572

privacidad de los datos. En este caso, la recopilación de datos en sí, no tiene como objetivo violar los derechos de privacidad, pero la falta de suficientes medidas de *ciberseguridad* puede conducir a una violación de la privacidad.

Aplicaciones móviles y vigilancia física

Durante la pandemia se ha introducido una gran variedad de aplicaciones móviles (Alderson, E., 2020), por parte gobiernos, autoridades locales y empresas privadas. Algunas son voluntarias y otras obligatorias. Estas aplicaciones se basan en tecnologías de protocolo abierto y protocolo cerrado, como se aprecia en safesmart (https://safesmart.co.uk/open-closed-protocols-mean/); unas, dirigidas a rastrear los *contactos* de las personas infectadas; otras, para verificar el cumplimiento de las órdenes de confinamiento.

Una rápida cobertura por los principales diarios del mundo nos informa que Singapur fue pionero en el lanzamiento de la aplicación *Trace Together*, posteriormente subcontratada y utilizada por otros países para modelar sus propias aplicaciones, con dispositivos portátiles para rastrear la propagación del virus de manera más efectiva (Asher, S., 2020; Chiang, S., 2020). China fue el primer país en enfrentar la pandemia y uno de los primeros en recurrir a medios tecnológicos para contenerla. La aplicación *Alipay Health Code* es el producto de la cooperación entre el gobierno local de Hangzhou y *Ant Financial*, una empresa hermana del gigante del comercio electrónico *Alibaba* (Mozur, P., Zhong, R. y Krolik, A., 1 de marzo de 2020). Se proyectó en Hangzhou a principios de febrero del 2020 y se extendió rápidamente por todo el país. La aplicación asigna a los usuarios un código de color basado en el estado de salud y el historial de viajes, que las autoridades pueden escanear (Davidson, H., 2020). En general, las personas con un código verde pueden viajar con relativa libertad; un código amarillo, indica que el titular debe estar en aislamiento domiciliario y un código rojo, advierte que el usuario es un paciente COVID-19 confirmado y debe permanecer en cuarentena (Davidson, H., 2020). Según El New York Times, el usuario otorga al software acceso a datos personales, una parte del programa con la etiqueta "reportInfoAndLocationToPolice" envía la ubicación de la persona, el nombre de la ciudad y un número de código de identificación a un servidor, mientras que la conexión de la aplicación con la policía no se informa a los usuarios (Mozur, P., Zhong, R. y Krolik, A., 2020). Los *algoritmos*[2] exactos utilizados para determinar si las personas son epidemiológicamente *seguras* o *inseguras*, no están disponibles para el público, lo que a veces conduce a cambios arbitrarios del estado de "seguridad" codificado por colores. Esto arroja dudas sobre la

[2] RAE, Diccionario "Conjunto ordenado y finito de operaciones que permite hallar la solución de un problema." A lo largo de la historia varios autores han tratado de definir formalmente a los algoritmos utilizando modelos matemáticos. Esto fue realizado por Alonzo Church en 1936 con el concepto de "calculabilidad efectiva" basada en su cálculo lambda y por Alan Turing basándose en la máquina de Turing. Citado en Gurevich, Yuri (2000). «Sequential Abstract State Machines capture Sequential Algorithms».

efectividad de la aplicación para lograr el objetivo declarado de contener el virus y plantea otro problema de privacidad en China. Especialmente preocupante es la retórica de las autoridades para justificar el uso de la aplicación, incluso cuando la pandemia cede. De acuerdo a esto, la tecnología puede convertirse en un "guardián íntimo de la salud" para las personas y están explorando las posibilidades de ampliar el código de salud para clasificar a los ciudadanos con un "índice de salud personal" (Zhong, R., 26 mayo 2020).

Otra aplicación de seguimiento es la identificada como *Supervisión social*, lanzada por las autoridades de Moscú, criticada por su empleo como herramienta para el control punitivo de la cuarentena. El uso de esta aplicación es obligatorio para las personas que han dado positivo en la prueba de COVID-19 o que presenten síntomas de enfermedades respiratorias. La aplicación obtiene acceso a la ubicación del usuario, las llamadas, la cámara, la información de la red, los sensores y otros datos para garantizar que las personas a las que se les indique que se pongan en cuarentena no salgan de su hogar durante el período de dos semanas (Human Rights Watch Rusia, 21 de mayo de 2020). La aplicación envía notificaciones automáticas al azar, con la instrucción de que los usuarios se tomen y envíen inmediatamente una *selfie*, como prueba de que no han salido de casa sin el teléfono (Human Rights Watch Rusia). La falta de respuesta a una notificación, que puede llegar hasta la medianoche, da lugar a una multa automática de 4.000 rublos (aproximadamente US $ 56). No instalar la aplicación también resulta en una multa. Según *Human Rights Watch*, en mayo del año pasado, a la población residente en Moscú se le instaló la aplicación y se emitieron 53.000 multas (Human Rights Watch Rusia). La aplicación de *monitoreo social* y la práctica de usarla, no solo interfieren con los derechos de privacidad, que imponen una sustancial carga financiera para las personas ya afectadas por la crisis.

Vigilancia física: Las cámaras y los drones son un instrumento aún más tangible de la "biopolítica" relacionada con la COVID-19 La presencia (a menudo intimidante) de cámaras en espacios públicos ya ha sido controvertida antes de la pandemia. Sin embargo, la actitud de algunos actores por mejorar las capacidades de la videovigilancia, amenaza con normalizar las prácticas intrusivas a la privacidad. Según los informes de los medios, la vigilancia con drones se ha desplegado en los Estados Unidos (Governing, April 14, 2020), Malasia, España, Italia, y el Reino Unido. Las cámaras de vigilancia se han utilizado en Francia, en Rusia, en China, y Estados Unidos.

3. Principios rectores y estándares

La crisis sanitaria plantea desafíos a la privacidad, compeliendo la adopción de medidas que protejan la salud pública. La declaración conjunta de expertos de las Naciones Unidas (ONU), la Comisión Interamericana de Derechos Humanos (CIDH) y la Organización para la Seguridad y la Cooperación en Europa (OSCE) (OACNUDH, 19 marzo 2020), advierten contra las invasiones de la privacidad en el dictado de luchar contra la pandemia de COVID-19.

Dice, en parte relevante:

> … Somos conscientes del uso creciente de herramientas de tecnología de vigilancia para rastrear la propagación del coronavirus. Si bien entendemos y apoyamos la necesidad de realizar esfuerzos activos para enfrentar la pandemia, también es crucial que dichas herramientas sean de uso limitado, tanto en términos de propósito y tiempo, y que los derechos individuales a la privacidad, la no discriminación, la protección de los periodistas las fuentes y otras libertades están rigurosamente protegidas. Los estados también deben proteger la información personal de los pacientes. Instamos encarecidamente a que cualquier uso de dicha tecnología cumpla con las protecciones más estrictas y solo esté disponible de acuerdo con la ley nacional que sea consistente con los estándares internacionales de derechos humanos. (OACNUDH, 19 marzo 2020)

En este contexto, en el informe 2020 sobre pandemias, el relator especial de la ONU sobre la promoción y protección del derecho a la libertad de opinión y expresión, formuló seis principios que deben regir la *vigilancia* durante la actual emergencia sanitaria (Asamblea General de las Naciones Unidas [AGNU], 23 de abril de 2020):

> 1. Toda autorización de vigilancia debe estar contenida en leyes precisas y accesibles al público y solo debe aplicarse cuando sea necesario y proporcionado para lograr un objetivo legítimo (como proteger la salud pública);
> 2. La autorización de vigilancia de determinadas personas debe basarse en una evaluación independiente, preferiblemente por una autoridad judicial, con las limitaciones adecuadas en cuanto a tiempo, lugar, forma y alcance;
> 3. Debería exigirse un mantenimiento riguroso de los registros para que las personas y los órganos de supervisión puedan comprobar que la vigilancia se llevó a cabo con fines legítimos de salud pública;
> 4. Todos los datos personales recopilados deben estar sujetos a estrictas protecciones de privacidad para evitar la divulgación de información a cualquier persona no autorizada para fines de salud pública;
> 5. Algunos datos personales deben excluirse expresamente de la recopilación, como el contenido de las comunicaciones de una persona, y deben establecerse salvaguardias sólidas para evitar el uso indebido de dichos datos por parte del gobierno o de terceros, incluido el uso para fines no relacionados con la emergencia de salud pública.
> 6. Cuando los datos personales se anonimizan, el Estado y cualquier tercero que participe en la recopilación deben poder demostrar ese anonimato. (AGNU, 23 de abril de 2020)

Estos principios se basan en estándares de *legalidad, necesidad y proporcionalidad,* previamente establecidos en los tratados de derechos humanos, destacando los máximos y mínimos del derecho internacional, en relación al actuar de gobiernos y empresas privadas, dedicadas a la recopilación de datos (ONU, 2011).

4. Principios de Siracusa: derogar o limitar derechos

La salud pública puede invocarse como motivo para limitar ciertos derechos, a fin de permitir a los Estados adoptar medidas extraordinarias frente a una emergencia grave que amenace a la salud de la población o de alguno de sus miembros. Estas medidas deberán estar encaminadas específicamente a impedir enfermedades o lesiones, a proporcionar

cuidados a los enfermos y lesionados. De acuerdo al derecho internacional de los derechos humanos, que incluye el derecho a la privacidad, los estados cuentan con dos mecanismos legales para decidir sus respuestas a la emergencia sanitaria de la COVID 19, a partir del instrumento denominado *Principios de Siracusa* (ONU, 1985), relativo a la interpretación y aplicación de las disposiciones de *limitación* y *derogación* de los derechos comprendidos en el Pacto Internacional de Derechos Civiles y Políticos (16 de diciembre de 1966, artículo 4). Estas limitaciones y derogaciones, consagradas en tal instrumento, son compartidas con otras disposiciones similares en los tratados regionales de derechos humanos, se observa en el Protocolo núm. 11 y 14 del Convenio europeo para la protección de los derechos humanos y las libertades fundamentales (OEA, 22 de noviembre de 1969, artículo 27; Consejo Europeo [CE], 4 noviembre de 1950, artículo 15).

En el contexto de la COVID-19, la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos [OACNUDH] y el Comité de Derechos Humanos [CDH] de la ONU, han proporcionado directrices adicionales sobre el alcance de estas limitaciones y derogaciones durante la pandemia (CDH, 30 de abril de 2020; OACNUDH, 27 de abril de 2020). En situaciones de emergencia, el derecho internacional de derechos humanos permite a los Estados *derogar* ciertas obligaciones de derechos humanos, bajo ciertas medidas necesarias y solo en circunstancias urgentes. El mecanismo de derogación, en el marco del Pacto Internacional de Derechos Civiles y Políticos, presupone la existencia de una *emergencia nacional* que amenaza la vida y requiere que el estado *derogante* siga ciertos pasos procesales para declarar la derogación, varios tratados (CE, 4 de noviembre 1950, artículo 15; OEA, 22 de noviembre de 1969, artículo 27; PIDCP, 16 de diciembre de 1966) procuran los derechos humanos.

Las derogaciones se consideran un mecanismo que debe emplearse en circunstancias extraordinarias, mientras tales circunstancias continúen impidiendo a los Estados realizar plenamente los derechos humanos. El CDH de la ONU, que es responsable de la interpretación autorizada del Pacto Internacional de Derechos Civiles y Políticos, establece seis requisitos específicos que los estados deben cumplir, si quieren derogar sus obligaciones de derechos humanos. A saber:

Los Estados deben: 1) proclamar el estado de emergencia; 2) notificar formalmente al Secretario General de la ONU de su intención de derogar; 3) garantizar que las medidas de excepción cumplan estrictas pruebas de necesidad y proporcionalidad; 4) garantizar que las medidas de derogación no interfieran con otras obligaciones internacionales de derechos humanos; 5) garantizar que las medidas de excepción se apliquen de forma que no sea discriminatoria; y 6) continuar defendiendo los derechos inderogables (Centro de Recursos de Justicia Internacional [CRJI], 29 de abril 2020; CDH, 30 de abril de 2020, párr. 2, págs. 1-2).

ISSN 2683 2070
Número 04
julio-diciembre 2021

DOI: https://doi.org/10.25009/ej.v0i04.2572

Si bien la pandemia de COVID-19 puede calificar claramente como una emergencia potencialmente mortal, en todos los estados afectados por el brote, la adhesión a un mecanismo de derogación a menudo sigue siendo poco empleada por los estados. Incluso aquellos que han declarado un estado de emergencia nacional, no optan por el procedimiento de derogar los derechos humanos a nivel internacional. Las derogaciones son herramientas útiles para garantizar que las limitaciones a los derechos humanos, tengan un plazo determinado y se limiten a la emergencia pandémica (Greene, A. 01 de abril de 2020). Sin embargo, el hecho de que los estados no hagan uso del mecanismo, no significa que las respuestas a la pandemia, incluidas las relacionadas a los derechos de privacidad, no estén sujetos al derecho internacional de los derechos humanos. De hecho, la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (OACNUDH) recomienda que los estados se abstengan de utilizar el mecanismo de derogación cuando sea posible, afirmando que "aunque se permite la derogación o suspensión de ciertos derechos cuando se declaran tales emergencias, las medidas de suspensión de derechos deben evitarse, cuando la situación pueda tratarse adecuadamente *estableciendo restricciones o limitaciones* a ciertos derechos" (OACNUDH, 27 de abril de 2020).

Poner limitaciones a los derechos humanos inderogables es otra forma en que los estados pueden gestionar sus respuestas a la COVID-19. Los criterios para utilizar limitaciones son menos estrictos que los que rigen las excepciones. Los derechos humanos pueden limitarse legalmente incluso en momentos en los que no existe una emergencia urgente que ponga en peligro la vida. Eso no significa que las limitaciones a los derechos humanos no tengan límites razonables. Por el contrario, es necesario cumplir una serie de criterios para que las limitaciones se consideren legales. Si bien el mecanismo de limitaciones no tiene un artículo específico en El Pacto Internacional de Derechos Civiles y Políticos (ICCPR, por sus siglas en inglés) es un tratado multilateral general que reconoce Derechos civiles y políticos, establece mecanismos para su protección y garantía. Se refleja en varios artículos sustantivos del ICCPR (16 de diciembre de 1966, artículo 18 (3); Articulo 19 (3); Artículo 22 (2); CDH, 8 de abril de 1988) y se desarrolla en la jurisprudencia, (TEDH, 04 diciembre de 2015; TEDH, 13 de septiembre de 2018) y el análisis de expertos (Asociación Estadunidense para la Comisión Internacional de Juristas, 1985: 6-9). En el contexto de la vigilancia, la jurisprudencia del TEDH (TEDH, 2008; TEDH, 2010; TEDH, 2015; TEDH, 2018; Tribunal de Justicia de las Uniones Europeas [TJUE], 6 de octubre de 2015; TJUE, 16 de julio de 2020) es particularmente útil al interpretar las condiciones para las limitaciones legales de la privacidad, ya que ningún otro organismo judicial o cuasi judicial internacional se ha acercado a la experiencia del TEDH en el manejo de casos relacionados con la vigilancia. Los criterios del TEDH para las limitaciones legales de la privacidad también son consistentes con la interpretación del órgano de tratados del Pacto Internacional de Derechos Civiles y Políticos sobre las interferencias "arbitrarias o ilegales" en la privacidad de conformidad con el artículo 17 y la Observación general número 16 del Comité de Derechos Humanos

ISSN 2683 2070
Número 04
julio-diciembre 2021

DOI: https://doi.org/10.25009/ej.v0i04.2572

(OACNUDH 8 de abril de 1988, artículo 17). Según estas fuentes, las medidas de vigilancia introducidas para combatir el COVID-19 deben satisfacer de manera acumulativa criterios de legalidad, necesidad y proporcionalidad (OACNUDH, 30 junio de 2014).

5. Legalidad, Necesidad y Proporcionalidad

Legalidad. Las medidas en cuestión deben ser "de conformidad con la ley". Siguiendo el enfoque del TEDH, esto significa que la vigilancia debe estar claramente sancionada por la legislación nacional del Estado que la práctica. Sin embargo, la mera documentación de las medidas de vigilancia en papel no será suficiente para satisfacer este criterio. La ley que introduce medidas de vigilancia debe ser "previsible", es decir, suficientemente precisa "para dar a los ciudadanos una indicación adecuada de las circunstancias y condiciones en las que las autoridades públicas están facultadas para recurrir a cualquier medida [de vigilancia]" (TEDH, 13 de septiembre de 2018, párr. 306: 127). En el contexto de la COVID-19, esto significa que las personas objetivo de la vigilancia tienen derecho a saber qué información sobre ellos o sus contactos se recopilará, quién podrá acceder a la información recopilada y cuáles son los límites de retención de datos.

Necesidad. El criterio de necesidad implica que cualquier medida de vigilancia debe abordar una "necesidad social apremiante" (OACNUDH, 27 de abril de 2020). Si bien no existe un desacuerdo sobre si la pandemia de COVID-19 calificaría como tal, la necesidad de mantener las medidas de vigilancia en su lugar después de la COVID-19, prevenir futuras pandemias puede ser más discutible.

Proporcionalidad. El equilibrio entre los fines y los medios de vigilancia es fundamental. Si las medidas de vigilancia son ineficaces para manejar la pandemia y perjudican la privacidad individual, no cumplirían el criterio de proporcionalidad. Las intrusiones masivas a la privacidad no se justificarían por ganancias marginales en la contención de la pandemia. Las limitaciones al derecho a la privacidad deben representar la opción menos intrusiva entre las que podrían lograr el resultado deseado (27 de abril de 2020). Una consideración relevante al evaluar la legalidad de una limitación particular es si dicha limitación es discriminatoria o no. Si bien en la jurisprudencia del TEDH este aspecto suele abordarse como parte de una violación separada del artículo 14 del CEPDH (04 de noviembre de 1950), es frecuente tratarlo también como otro criterio para las limitaciones legales de los derechos humanos (Ponta, A., 20 de abril 2020). La limitación no es discriminatoria cuando no se dirige injustamente a los representantes de un grupo en particular. Sin embargo, no apuntar a un grupo demográfico específico de manera discriminatoria, debe distinguirse de la introducción de medidas de vigilancia masiva que abarcan demasiado, sin que nadie se inmiscuya en su privacidad. La aplicación de la prueba de limitación legal a las medidas de vigilancia reales aplicadas durante la pandemia de COVID-19 debe analizarse caso por caso. La idoneidad de las salvaguardias contra los abusos de la privacidad dependiente de varios factores: qué tan transparentes son los estados sobre las medidas de vigilancia, cuánta

ISSN 2683 2070
Número 04
julio-diciembre 2021

DOI: https://doi.org/10.25009/ej.v0i04.2572

información se recopila y qué tan útiles son los datos recopilados para combatir la propagación del virus. Para ilustrar el rango de resultados, una tabla que compare dos aplicaciones de vigilancia diferentes, con los tres requisitos de legalidad, necesidad y proporcionalidad, refleja el tipo de evaluación, caso por caso, que se requiere para valorar la legalidad de diferentes medidas. Ya sea que los estados adopten un marco de derogaciones o limitaciones realistas (siendo la última, una opción más), sus poderes de vigilancia no serán absolutos. Para evitar intrusiones ilegítimas a la privacidad, una evaluación como la anterior debería convertirse en una pieza central para analizar si determinadas medidas de vigilancia cumplen con el derecho internacional de los derechos humanos.

Conclusiones

Si bien la pandemia de COVID-19 ha generado un gran debate sobre el valor del rastreo de contactos y la dependencia de la tecnología que permite hacer un seguimiento de los ciudadanos y las personas con quienes se encuentran, el uso de la información y la tecnología no es nuevo en la gestión de las emergencias de salud pública. Resulta preocupante que en algunos Estados se utilice la tecnología y el grado de intromisión y control al que se somete a los ciudadanos, con escaso efecto en la salud pública. Pese a que aún no se dispone de una base empírica necesaria para determinar de manera concluyente si las medidas contra la COVID-19 que afectan la privacidad, son *necesarias* y *proporcionadas* en una sociedad democrática. Dos aspectos particulares de las repercusiones de la COVID-19 en el derecho a la privacidad se refieren a la *protección de datos y la vigilancia.* Las actividades de vigilancia y de rastreo de contactos, relacionadas con la pandemia, pueden adoptar diversas formas y pueden ser manuales o tecnológicas, anónimas o no, y consensuadas o no. Las inquietudes surgen cuando se propone o se despliega apresuradamente un aparato de vigilancia tradicionalmente empleado para fines de seguridad del Estado con el propósito de rastrear datos relacionados con la salud en beneficio de la salud pública en el contexto de una pandemia.

Si un Estado determina que es preciso aplicar medidas de vigilancia tecnológica como respuesta a la pandemia mundial, debe asegurarse, tras demostrar tanto la necesidad como la proporcionalidad de las medidas específicas, de disponer de una ley que prevea tales medidas explícitamente. La ley debe incluir salvaguardias que, si no se explican con suficiente detalle, no pueden considerarse adecuadas en virtud del derecho internacional. Sin embargo, se debe reconocer que hay muchas más cuestiones de privacidad en juego durante la pandemia, incluidas las relativas a los niños, el género y el papel que desempeñan los algoritmos, entre otras.

El rastreo de contactos es la herramienta clásica empleada por las entidades de salud pública para detener la propagación de enfermedades transmisibles. Constituye una intromisión en la vida privada, porque requiere que al paciente revele con quién ha estado

ISSN 2683 2070
Número 04
julio-diciembre 2021

DOI: https://doi.org/10.25009/ej.v0i04.2572

en contacto durante un período de tiempo determinado. Tradicionalmente, en la mayoría de los países, este ha sido de manera implícita uno de los casos excepcionales en que el derecho a la privacidad no tiene que ser absoluto. La necesidad de detener la propagación de una posible epidemia constituye uno de los poquísimos casos de bien común en los que el interés público se valora socialmente por encima del derecho a la privacidad o, incluso, de otros derechos como la libertad de circulación y la libertad de asociación. En pocas palabras, para evitar la propagación del cólera o la tuberculosis, por ejemplo, las autoridades tienen derecho a saber quién sufre la enfermedad y ordenar el aislamiento estricto bajo normas sanitarias estrictas, entre otras cosas. Sin embargo, es demasiado pronto para evaluar adecuadamente la eficacia de las medidas adoptadas en relación con la COVID-19 y para dar respuesta a las siguientes preguntas: ¿Qué funciona? ¿Qué funciona mejor? ¿Qué funciona mejor para quién? ¿Qué funciona mejor en qué lugar? Una vez individualizada una medida, la siguiente pregunta es: ¿por qué funcionó o funciona mejor esta medida, para quién y dónde? Se espera que las pruebas que se obtengan en los próximos meses permitan comprender mejor estas variables y otras, lo que ayudaría a los expertos en materia de privacidad a evaluar adecuadamente las medidas adoptadas contra la COVID-19, determinar si las medidas no consensuadas cumplen las estrictas pruebas de proporcionalidad y necesidad.

ISSN 2683 2070
Número 04
julio-diciembre 2021

DOI: https://doi.org/10.25009/ej.v0i04.2572

Fuentes de consulta

Alderson, E. (2020). Covid 19 Tracker Apps. https://fs0c131y.com/covid19-tracker-apps/

Asamblea General de las Naciones Unidas. (23 de abril de 2020). Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, sobre las pandemias de enfermedades y la libertad de opinión y expresión. Consultado en https://undocs.org/A/HRC/44/49

Asher, S. (5 july 2020). TraceTogether: Singapore turns to wearable contact-tracing Covid tech, en BBC News. Recuperado de https://www.bbc.com/news/technology-53146360

Asociación Estadunidense para la Comisión Internacional de Juristas. (1985). Principios de Siracusa sobre las disposiciones de limitación y el Pacto Internacional de Derechos Civiles y Políticos. Consultado en https://www.icj.org/wp-content/uploads/1984/07/Siracusa-principles-ICCPR-legal-submission-1985-eng.pdf

Caso Klass And Others V. Germany. (1978). Application no. 5029/71, Judgement of 6 September 1978, para. 43, ECtHR. Recuperado de https://dadun.unav.edu/bitstream/10171/55425/1/34198-95543-1-PB.pdf

Centro de Recursos de Justicia Internacional. (29 de abril de 2020). ACNUDH y el Comité de Derechos Humanos: las excepciones durante el COVID-19. Consultado en https://ijrcenter.org/2020/04/29/ohchr-human-rights-committee-address-derogation-during-covid-19/

Centro para el Control y la Prevención de Enfermedades. (2019). Preguntas frecuentes: Datos y vigilancia COVID-19. https://www.cdc.gov/coronavirus/2019-ncov/covid-data/faq-surveillance.html

Chiang, S. (2020). De la aplicación Trace Together al dispositivo portátil: por qué el rastreo de contactos no funcionaría en S'pore, Vulcan Post, https://vulcanpost.com/701007/why-contact-tracing-would-not-work-singapore/

Comité de Derechos Humanos. (30 de abril de 2020). Declaración sobre derogaciones del Pacto en relación con la pandemia COVID-19, CCPR / C / 128/2. Consultado en https://www.ohchr.org/Documents/HRBodies/CCPR/COVIDstatementEN.pdf

Consejo de Derechos Humanos. (24 de marzo de 2015). Resolución 28 / L.27, El derecho a la privacidad en la era digital. Consultado en https://documents-dds ny.un.org/doc/UNDOC/LTD/G15/061/64/PDF/G1506164.pdf

Consejo de Derechos Humanos. (01 de abril de 2015). Resolución sobre el derecho a la privacidad en la era digital. Consultado en https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/068/78/PDF/G1506878.pdf

Consejo de Derechos Humanos. (22 de marzo de 2017). Resolución 34 / L.7 / Rev.1, El derecho a la privacidad en la era digital. Consultado en https: // documentos-dds ny.un. org / doc / UNDOC / LTD / G17 / 073/06 / PDF / G1707306.pdf

Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales. (4 de noviembre de 1950). Recuperado de: https://www.acnur.org/fileadmin/Documentos/BDL/2002/1249.pdf

Davidson, H. (2020) Las aplicaciones del código de salud del coronavirus de China plantean preocupaciones sobre la privacidad. The Guardian. https://www.theguardian.com/world/2020/apr/01/chinas-coronavirus-health-code-apps-raise-concerns-over-privacy

Foucault, M. (2002). Vigilar y castigar: nacimiento de la prisión. Traducción de Aurelio Garzón del Camino. 1ª ed. Buenos Aires, Siglo XXI Editores Argentina. Recuperado de https://www.ivanillich.org.mx/Foucault-Castigar.pdf

Giglio, M. (22 April 2020). Would You Sacrifice Your Privacy to Get Out of Quarantine?, The Atlantic. Recuperado de https://www.theatlantic.com/politics/archive/2020/04/coronavirus-pandemic-privacy-civil-liberties-911/609172/

Governing. (April 14, 2020). Drones in Florida Remind Residents to Keep Their Social Distance. Consultado en https://www.governing.com/now/Drones-in-Florida-Remind-Residents-to-Keep-Their-Social-Distance.html

Greene, A. (01 de abril de 2020). Los Estados deberían declarar un estado de emergencia utilizando el artículo 15 del CEDH para hacer frente a la pandemia del coronavirus, Estrasburgo. Consultado en https://strasbourgobservers.com/2020/04/01/states-should-declare-a-state-of-emergency-using-article-15-echr-to-confront-the-coronavirus- pandemia/

Greenwald, G. (6 jun 2013). NSA collecting phone records of millions of Verizon customers daily, The Guardian. Recuperado de https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

Gurevich, Y. (2000). Sequential Abstract State Machines Capture Sequential Algorithms. ACM Transactions on Computational Logic 1 (1): 77-111. ISSN 1529-3785.

Human Rights Watch Rusia. (21 de mayo de 2020) La aplicación de seguimiento intrusivo impone multas erróneas a los moscovitas. Recuperado de https://www.hrw.org/news/2020/05/21/russia-intrusive-tracking-app-wrongly-fines-muscovites

Lubin, A. (2018). "We Only Spy on Foreigners": The Myth of a Universal Right to Privacy and the Practice of Foreign Mass Surveillance. Chicago Journal of International Law, Vol. 18, No. 2. Article 3, pág. 543. Consultado en https://chicagounbound.uchicago.edu/cjil/vol18/iss2/3

Mozur, P., Zhong, R. y Krolik, A. (01 de marzo de 2020). En Coronavirus Fight, China les da a los ciudadanos un código de color, con banderas rojas. New York Times. https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html

Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. (1988) Derecho a la privacidad, Artículo 17, Observación general No. 16. El derecho al respeto de la privacidad, la familia, el hogar y la correspondencia, y la protección del honor y la reputación, 8 de abril de 1988, consultado en https://www.acnur.org/fileadmin/Documentos/BDL/2005/3584.pdf

Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. (30 junio de 2014). Sobre el derecho a la privacidad en la era digital. https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

ISSN 2683 2070
Número 04
julio-diciembre 2021

DOI: https://doi.org/10.25009/ej.v0i04.2572

Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. (2016). Annual thematic reports of the Special Rapporteur on the right to privacy. Consultado en https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/AnnualReports.aspx

Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. (19 marzo 2020). COVID-19: Los gobiernos deben promover y proteger el acceso y el libre flujo de información durante una pandemia, consultado en: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25729&LangID=E

Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. (27 de abril de 2020). Medidas de emergencia y COVID-19: Orientación. https://www.ohchr.org/Documents/Events/EmergencyMeasures_COVID19.pdf

Organización de los Estados Americanos. (22 de noviembre de 1969). Convención Americana sobre Derechos Humanos. https://www.corteidh.or.cr/tablas/17229a.pdf

Organización de las Naciones Unidas. (1985). Consejo Económico y Social. Principios de Siracusa sobre las disposiciones de limitación y derogación del Pacto Internacional de Derechos Civiles y Políticos, Doc. De la ONU. E / CN.4 / 1985/4. Consultado en http://hrlibrary.umn.edu/instree/siracusaprinciples.html

Organización de las Naciones Unidas. (2011). Principios rectores sobre empresas y derechos humanos: implementación del marco de las Naciones Unidas "Proteger, respetar y remediar". https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf.

Pacto Internacional de Derechos Civiles y Políticos (16 de diciembre de 1966). Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. Consultado en https://www.ohchr.org/SP/ProfessionalInterest/Pages/CCPR.aspx

Ponta, A. (20 de abril 2020). Ley de derechos humanos en la época del coronavirus, ASIL, Volumen 24, Número 5. https://www.asil.org/insights/volume/24/issue/5/human-rights-law-time-coronavirus

Real Academia Española. (2021). Consultado en https://www.rae.es/

Reglamento General de Protección de Datos de la Unión Europea. (27 abril de 2016). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales y sobre la libre circulación, DO 2016 L 119/1. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679

Safesmart. (June 23, 2015) protocolos abiertos y cerrados: ¿qué significa todo? https://safesmart.co.uk/open-closed-protocols-mean/

Tribunal Europeo de Derechos Humanos. (2008). Liberty And Others vs The United Kingdom. Sentencia del TEDH, 1 de julio de 2008.

Tribunal Europeo de Derechos Humanos. (2010). Kennedy vs El Reino Unido, Sentencia de 18 de mayo de 2010.

Tribunal Europeo de Derechos Humanos. (2014). Guía de admisibilidad del TEDH sobre todos los criterios de admisibilidad; Consultado en: https://www.echr.coe.int/Documents/Admissibility_guide_SPA.pdf

Tribunal de Justicia de las Uniones Europeas. (6 de octubre de 2015). Max Schrems v. Data. Comisionado de Protección, C-362/14.

Tribunal Europeo de Derechos Humanos. (2015). Roman Zakharov Versus Rusia. Solicitud no. 47143/06, Sentencia de 4 de diciembre de 2015. Recuperado de https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-159324%22]}

Tribunal Europeo de Derechos Humanos. (2018). Big Brother Watch y otros contra el Reino Unido. Solicitud nos. 58170/13, 62322/14 y 24960/15, sentencia de 13 de septiembre de 2018.

Tribunal de Justicia de las Uniones Europeas. (16 de julio de 2020). Comisionado de Protección de Datos contra Facebook y Max Schrems, C-311/18.

Weber And Saravia V. Germany. (2006). Application no. 54934/00, Admissibility Decision of 29 June 2006, para. 78.

Zhong, R. (26 May 2020), China's Virus Apps May Outlast the Outbreak, Stirring Privacy

ISSN 2683 2070
Número 04
julio-diciembre 2021

DOI: https://doi.org/10.25009/ej.v0i04.2572

Fears, The New York Times. https://www.nytimes.com/2020/05/26/technology/china-coronavirus-surveillance.html