Recibido: 31-08-2020 • **Aprobado:** 26-10-2020

Vigilancia tecnológica versus derecho a la privacidad-intimidad. El caso de la pandemia

Technological vigilance versus the right to privacy-intimacy. The pandemic case

DOI: https://doi.org/10.29166/tyc.v1i21.2513

Lautaro Ojeda Segovia
Estudió Derecho y Filosofía en la Pontificia Universidad Católica del Ecuador (PUCE) y Sociología en la Universidad Católica de Lovaina-Bélgica. Profesor universitario durante 30 años en varias universidades públicas y privadas de postgrado: PUCE, Universidad Central del Ecuador (UCE), Universidad Andina Simón Bolívar (UASB), Facultad Latinoamericana de Ciencias Sociales (FLACSO-Ecuador), Academia de Guerra del Ejército, entre otras. Consultar de varios organismos nacionales e internacionales. Autor de libros 15 libros sobre temas de desarrollo social, descentralización y autonomía indígena, modernización, planificación nacional, seguridad ciudadana, poder miedo y seguridad. Ha publicado alrededor de 100 artículos en revistas nacionales e internacionales

Correo: lautarojeda@gmail.com

Resumen
Este artículo propone un modo de entender la aplicación de las políticas de vigilancia y control en el contexto de la pandemia del Covid 19. Se trata de identificar los modos en que los estados usan las tecnologías para acceder incluso a la información relacionada con la privacidad y la intimidad de las personas. Estas prácticas, que no son nuevas, se aplican con especial intensidad en momentos en que la humanidad vive un momento de gran vulnerabilidad en el que resulta difícil discernir dónde termina la seguridad y dónde comienza el derecho a la privacidad.

Palabras clave: pandemia, vigilancia, tecnologías, privacidad, derechos.

Abstract
This article proposes a way of understanding the application of vigilance and control policies in the context of the Covid 19 pandemic. It tries to identify the ways in which the countries use technology to access even information related to privacy and people intimacy. These practices, which are not new, are applied with particular intensity at the time when humanity is experiencing a time of great vulnerability when it is difficult to discern where security ends and where the right to privacy begins.

Keywords: pandemic, surveillance, technologies, privacy, rights.

> *Quienes están dispuestos a ceder su libertad básica a cambio de un poco de seguridad temporal no merecen ni la libertad ni seguridad* (Benjamín Franklin, 1755).
>
> *¿Por qué hay tantas personas en el mundo dispuestas a ceder a sus libertades a cambio de seguridad o prosperidad?* (John Kampfner, 2011).
>
> *El mantenimiento de la seguridad siempre ha sido un argumento o pretexto para el desarrollo de formas y mecanismos de vigilancia y control individual y colectivo* (Bauman, 2013).

Es un hecho que la tecnología digital y la Internet cambiaron el curso de la historia y están presentes en todos los aspectos de nuestra vida cotidiana, para bien y para mal.

Las tecnologías digitales, en especial las que se desarrollan por medio de los llamados teléfonos inteligentes, plantean un conjunto de problemas e interrogantes en torno a las aplicaciones internacionales de control y vigilancia tecnológicas (resoluciones de algunos organismos internacionales y países), pero también de oportunidades, desafíos y amenazas.

Al ser un tema tan sugerente como la *Vigilancia tecnológica versus derecho a la privacidad-intimidad*, diremos que la privacidad es muy importante, porque es un valor en sí mismo, esencial para el desarrollo de la personalidad y la protección de la dignidad humana. Permite protegernos de las interferencias injustificadas en nuestras vidas, nos ayuda a establecer fronteras para limitar quién tiene acceso a nuestros cuerpos y objetos, así como a nuestras comunicaciones y nuestra información.

En tanto que la intimidad no es más que aquella parcela de la vida personal que un individuo tiene derecho a esconder, ocultar y no mostrar ni a los poderes públicos ni a los demás ciudadanos.

Problemas

La sociedad digital de vigilancia se ha convertido en un verdadero mecanismo de control y vigilancia; está presente cotidianamente como una sombra que nos acompaña, persigue y rastrea.

Los avances tecnológicos se suceden tan rápidamente, que anestesian nuestra capacidad de asombro. Las novedades tecnológicas nos asombran durante un par de minutos y luego las incorporamos a nuestra vida como si siempre nos hubieran acompañado (Oppenheimer, 2019, p. 24).

La velocidad y fluidez de las señales electrónicas están cada vez más distantes del conocimiento y de la trasparencia de sus efectos, en todos los ámbitos del acontecer social. En otras palabras, están por encima de la capacidad de procesamiento de la mayoría de las personas para asimilar todos esos cambios.

En la actualidad, las nuevas técnicas de vigilancia no solo se han ampliado y diversificado, sino que han profundizado el control de la vida personal, pero además han cambiado la mayoría de hábitos y costumbres cotidianas. Los detalles más insignificantes de la vida diaria son vigilados, registrados y examinados como nunca antes y, a menudo, quienes son vigilados cooperan voluntariamente con los vigilantes.

El pensador John Kampfner (2011) va más allá y dice que la vigilancia tecnológica, basada en el procesamiento de la información, permite una nueva transparencia, en la que no solamente los ciudadanos como tal sino todos nosotros, en cada uno de los papeles que asumimos en nuestra vida cotidiana, somos constantemente controlados, observados, evaluados, valorados y juzgados.

En nombre del paradigma de la seguridad, por ejemplo, las tecnologías digitales nos han acostumbrado al uso de marcadores biométricos, generalmente con la indiferencia o aceptación de los ciudadanos.

Esto ha creado una suerte de familiarización con la tecnología, que ha ampliado los umbrales de tolerancia y ha hecho que muchos consientan, muchas veces, sin siquiera darse cuenta de la afectación e incluso abandono de su esfera privada y de sus derechos fundamentales. Y ello no solo en relación con las técnicas de vigilancia y fichado, sino también como instrumento de medida y captación de las vivencias individuales por parte del complejo mediático y publicitario (Mattelart, 2009, p. 252).

En realidad, son tecnologías que inciden y atentan a la concepción ética y la normativa establecidas que, además de facilitar la posibilidad de caer en adicciones a los dispositivos tecnológicos de seguridad, propician la profundización del control de la vida personal e incluso de la violación de los derechos a la privacidad y la intimidad. Y conducen a la necesidad de combinar el ámbito cuantitativo-estadístico con el hermenéutico.

Las tecnologías de vigilancia, en especial el control individual y colectivo, aportan con datos minuciosos, por lo general rígidos, que a la vez presentan limitaciones hermenéuticas, advierte Thomas Friedman (2019), pero con las que es posible formular explicaciones y escenarios que permiten adoptar decisiones consistentes y pertinentes, en aras de la libertad y del ejercicio de los derechos de privacidad e intimidad.

Es por esto que la aplicación de vigilancia digital, por parte de actores poderosos, además de ser rutinaria, se ha vuelto omnipresente y una estrategia central de muchos países y, por cierto, en el principal modelo de negocios de las grandes empresas de Internet, tarjetas de crédito, publicidad, etc.

Este tipo de vigilancia también posibilita la interferencia en las conversaciones ajenas, mediante sencillos aparatos que pueden adquirirse en numerosos establecimientos comerciales. Al ser tecnologías de uso masivo, inciden además en el aumento de delitos, particularmente de los ciberdelitos.

Parte de la opacidad con que se mueven los nuevos mecanismos de vigilancia tiene que ver con su carácter altamente sofisticado y los complejos flujos de datos entre distintas organizaciones. Un gran segmento de esa información personal, que las organizaciones conseguían con tanto esfuerzo, ahora es proporcionado por la gente al usar su móvil, al comprar en los centros comerciales, al viajar por vacaciones. Y lo hacemos al pasar nuestras tarjetas, repetir nuestros códigos y mostrar nuestro documento de identidad de manera rutinaria, automáticamente, por voluntad propia.

Solo que, de esta manera, hemos contribuido a esa parte de la opacidad de las aplicaciones de vigilancia, y hemos inundado el ciberespacio con toda la información que vamos almacenando consciente o inconscientemente.

Seguridad individual y colectiva

La vigilancia está desplegando formas de comunicación y control hasta ahora inimaginables, en particular respecto de la seguridad individual y colectiva. Sin duda, las tecnologías digitales han supuesto avances beneficiosos para la

sociedad, aunque como cualquier tecnología tiene un doble filo.

El mantenimiento de la seguridad, por ejemplo, siempre ha sido un argumento para establecer una vigilancia. Actualmente, las nuevas técnicas y tecnologías de vigilancia supuestamente nos protegen, no contra peligros concretos sino contra riesgos amorfos y misteriosos (Bauman, (2013).

No obstante, las personas no siempre son conscientes que están entregando o a quien entregan información y datos personales. Es posible que no sepan que cada vez que se obtiene algo "gratis" en el mundo digital, no somos el cliente sino el producto y que muchos usos de la tecnología presentados como una ventaja puedan tener un lado oscuro.

A propósito, hay que tener presente el alcance de la intromisión, a través de la información, por parte de los gobiernos a nivel global. Edward Snowden (2019) publicó en 2013 algunos de los secretos mejor guardados de la inteligencia estadounidense, donde reveló la deriva autoritaria del Estado, el acopio, catalogación y uso indiscriminado de la información privada de los ciudadanos, que incluía a Jefes de Estado y de Gobierno.

Según Snowden, alrededor del 90 por ciento de las comunicaciones interceptadas pertenecía a gente común. Este hecho le permite inferir que se trata de un sistema masivo global. En este nuevo milenio, la tecnología del Internet se encaminó a imponer la fidelidad de la memoria, la uniformidad identitaria y, por tanto, la conformidad ideológica (Vigilancia permanente, 2019).

La vigilancia masiva es ahora un censo infinito, sustancialmente más peligroso que cualquier cuestionario. Todos nuestros dispositivos, desde nuestros teléfonos a los ordenadores, son básicamente censadores en miniatura que llevamos en las mochilas o bolsillos: censadores que recuerdan todo y no olvidan nada. La vigilancia no es algo ocasional y selectivo en circunstancias legalmente justificadas, sino una presencia constante e indiscriminada: el oído que todo lo escucha, el ojo que todo lo ve, una memoria que no duerme y que es permanente (Snowden, 2019, p. 254).

La gran ironía, al conocer de este sistema, es cuando constatamos que la ley va siempre a la zaga de la innovación tecnológica.

Pandemia y vigilancia

Las aplicaciones de tecnologías digitales en época de pandemia también plantean serias dificultades sobre la privacidad. Por muy bien diseñadas que estén dichas aplicaciones, ninguna de ellas es confiable. Tanto es así que los mecanismos digitales de rastreo de contactos no pueden compensar la escasez de tratamientos efectivos, de equipos de protección personal y de pruebas rápidas, entre otros aspectos.

Por esta razón, las aplicaciones móviles para la pandemia son motivo de puntos de vista controversiales, sobre la metodología y las técnicas empleadas en la selección, procesamiento, interpretación, difusión y utilización de la información. Por un lado, es reconocida la utilidad de buena parte de las medidas adoptadas para controlar y limitar rápidamente la propagación del virus, pero a la vez está la posibilidad de que, con el pretexto o excusa de seguridad, los gobiernos amplíen los poderes de seguimiento y vigilancia.

Sin embargo, cabe destacar que sí es posible adoptar aproximaciones menos lesivas al ejercicio de derechos, aprovechando el poder de los datos agregados para el combate de la pandemia. Este tipo de trabajo han venido desarrollando operadores de telefonía en Europa, en países como Alemania, Austria, Francia e Italia.

La propia autoridad de Protección de Datos de la Unión Europea admite que: "Las reglas de protección de datos no obstaculizan las medidas tomadas en la lucha contra la pandemia de coronavirus". Y enfatiza que "incluso en estos momentos excepcionales, el controlador de bases de datos debe garantizar la protección de los datos personales de sus titulares".

Otros países como China, Corea del Sur, Singapur, Taiwán, Israel, Irán e incluso Colombia, entre otros, han desarrollado aplicaciones móviles para controlar la propagación del coronavirus y han realizado grandes inversiones en capacidad de testeo proactivo, infraestructura de respuesta y disposición de información confiable en forma coordinada. Todos estos elementos son citados por expertos como componentes vitales de una respuesta efectiva.

En el caso de Corea, sin embargo, el despliegue de la App *Self-quarantine Safety Protection*, a partir del 7 de marzo de 2020, se produjo cuando las principales medidas de contención, a través del testeo masivo y aislamiento de individuos y grupos infectados, ya se encontraban ampliamente aplicadas y la expansión de la pandemia mostraba signos relevantes de contención.

En esta misma línea, Hangzhou (región de Shanghái) se ha propuesto clasificar a las personas según sus hábitos de vida, por medio de teléfonos móviles que rastrean todos los movimientos personales, según sus hábitos en el fumar, beber y de sueño. Por beber un vaso de licor es probable perder puntos de confianza en el ciudadano. Esta propuesta pretende convertirse en norma, con profunda incidencia en la privacidad e intimidad.

Recomendaciones para los gobiernos

Frente a este panorama, cien organizaciones internacionales, entre ellas Amnistía Internacional, han firmado una carta abierta con una serie de recomendaciones para los gobiernos, tendientes a que se garantice plenamente los derechos humanos y digitales, en el empleo de las nuevas tecnologías para rastrear y monitorear a personas.

El planteo de estas organizaciones sostiene que la tecnología puede y debe desempeñar importantes funciones durante el esfuerzo que se realiza para salvar vidas, como difundir mensajes de salud pública y aumentar el acceso a los servicios de salud.

No obstante, el aumento de los poderes de vigilancia digital de los Estados, como tener acceso a los datos de localización de los teléfonos móviles, amenaza la privacidad, la libertad de expresión y la libertad de asociación de una manera que podría violar derechos y reducir la confianza en las autoridades públicas, con el consiguiente menoscabo de la eficacia de las respuestas de salud pública.

Además, tales medidas entrañan también un riesgo de discriminación y pueden perjudicar de manera desproporcionada a comunidades ya marginadas.

La carta pide a los gobiernos que no respondan a la pandemia de COVID-19 incrementando la vigilancia digital si no

se cumplen, entre otras, las condiciones siguientes:

1. Las medidas de vigilancia adoptadas para abordar la pandemia deben ser legales, necesarias y proporcionadas. Si los gobiernos amplían los poderes de seguimiento y vigilancia, tales poderes han de ser de duración limitada y prolongarse solo durante el tiempo necesario para abordar la pandemia actual.
2. No podemos dejar que la pandemia de COVID-19 sirva de excusa para ejercer vigilancia indefinidamente.
3. Los gobiernos deben hacer todo lo posible para proteger los datos personales, lo que incluye garantizar la debida seguridad de los datos recopilados y de los dispositivos, aplicaciones, redes o servicios utilizados en su recopilación, transmisión, tratamiento y almacenamiento. (Ranchal, 2020).

Asimismo, Ciudades y Gobiernos Locales Unidos (CGLU), Metrópolis y ONU-Hábitat, el 25 de marzo de 2020 lanzaron una Experiencia de Aprendizaje en Vivo (#BeyondTheOutbreak), por la que buscan reunir a gobiernos locales y regionales, asociaciones y organizaciones asociadas, para facilitar y promover un intercambio significativo en la confrontación de la crisis de la COVID-19. Y, al mismo tiempo, mantener un funcionamiento ordenado de los servicios públicos en sus ciudades y territorios.

Siguiendo una consulta inicial durante la sesión de inauguración, la cuarta sesión temática de esta serie, que tuvo lugar el 15 de abril, se centró en promover una reflexión colectiva sobre la relación entre la crisis y las tecnologías digitales (CGLU, 2020).

Derecho a la privacidad y protección legal en Ecuador

Con la excusa de gestionar una crisis producida por la pandemia, el gobierno del Ecuador no puede desatender, sin más, derechos como la privacidad y la libertad de expresión. Como anota la carta de las organizaciones internacionales, las medidas de vigilancia adoptadas para abordar la pandemia deben ser "legales, necesarias y proporcionadas". No podemos dejar que la pandemia de la COVID-19 sirva de justificación para ejercer vigilancia masiva en forma indiscriminada.

En Ecuador se ha dispuesto el uso de "plataformas satelitales y de telefonía móvil" para el control del movimiento de la población bajo aislamiento y cuarentena, a pesar de la preocupación de la sociedad civil a nivel regional, y también global, por la necesidad de resguardos explícitos, mucho más en un país donde todavía no existe siquiera una ley de protección de datos personales.

A pesar de aquellas preocupaciones, la medida, de aparente carácter excepcional, parece haber seguido su curso, y el Ecuador sigue siendo uno de los países más afectados en número total y proporcional de casos fatales en la región.

Ahora, más que nunca, los gobiernos deben garantizar estrictamente que toda restricción se ajusta a las salvaguardias de los derechos humanos ya establecidas, porque mientras la innovación legal siga estando detrás de la innovación tecnológica, las instituciones buscarán abusar de esa disparidad en beneficio a sus propios intereses.

Disposiciones sobre privacidad

A nivel internacional y nacional existen algunas disposiciones sobre el derecho a la privacidad. La Asamblea de Naciones Unidas, en octubre de 2016, reafirmó que "nadie debe ser objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, y el derecho a la protección de la ley contra tales injerencias". Estos derechos están establecidos en el artículo 12 de la Declaración Universal de Derechos Humanos y en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos (ONU, 2016).

Es decir, todas las personas tienen derecho a la protección de la ley contra intromisiones o interferencias en su vida privada, su familia, su domicilio o su correspondencia, que provengan del Estado o de personas físicas o jurídicas que no estén previstas en la ley.

En la actualidad, en ciertas partes del mundo existen enormes bancos de datos que manejan información personal (historial de búsqueda, ubicación, datos financieros y de salud) sobre cada mujer, hombre o niño, alertó la Alta Comisionada de las Naciones Unidas, Michelle Bachelet.

El Informe de Naciones Unidas sobre Derechos Humanos de noviembre 2018, enfatiza que: "En ocasiones elegimos renunciar a aspectos de nuestra privacidad. Cada vez que compramos algo en la red, o usamos un servicio wifi gratuito, renunciamos a cierto grado de privacidad a cambio de algo de valor" (Noticias ONU, 2018).

La Constitución ecuatoriana en el Art. 66, numeral 19, reconoce el derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley. En tanto, el numeral 20 reconoce y garantiza a las personas el "derecho a la intimidad personal y familiar", y el numeral 21 reconoce "El derecho a la inviolabilidad y al secreto de la correspondencia física y virtual (…)" (Constitución, 2008).

El Código Orgánico Integral Penal, en el artículo 178, establece el derecho a la intimidad personal y familiar; quien lo viole puede ser sancionado con prisión de uno a tres años (COIP, 2014).

Oportunidades

La tecnología digital y la Internet pueden causar un efecto profundo en la vida cotidiana, en muchos casos para bien. Contribuyen a resolver –o al menos mitigar– problemas en sectores laborales, financieros, sociales, agrícolas, educativos y de salud.

Garantizan a los ciudadanos el acceso a la información y a la comunicación con las autoridades competentes e, inclusive, vemos opciones tecnológicas de seguridad individual y colectiva.

En la pandemia, sin duda, han sido y son una oportunidad para aumentar y profundizar la vigilancia digital, con el objeto de tener acceso a los datos que faciliten la localización e identificación de las personas y grupos afectados por el virus y, con base en la información obtenida, adoptar medidas y acciones para enfrentarla.

La tecnología digital ha demostrado en esta época ser una herramienta útil y

necesaria para favorecer, en la primera línea de la emergencia, la prestación de servicios de salud. Ha facilitado que los gobiernos conozcan áreas territoriales infectadas por el coronavirus que se propaga por todo el mundo, y establecer restricciones importantes sobre el movimiento de personas, el funcionamiento de los servicios y las normas sobre distanciamiento físico.

Las oportunidades derivadas del uso de tecnologías digitales en respuesta a la COVID-19 incluyen el teletrabajo, la reducción de la brecha digital, la continuidad de la educación en línea, el aprendizaje y la promoción de la transición ecológica. Pero también potencia las ganancias y utilidades de las grandes empresas tecnológicas como Google, Facebook, Apple, Zoom, Netflix, Amazon, YouTube, Teams y otras.

Empresas como Netflix han aumentado varios millones de suscriptores. Goldman sube el precio objetivo de Amazon en 12 %, hasta los 2.900 dólares. Zoom llega a 300 millones de usuarios y vale en la Bolsa 46.000 millones, más del doble de Twitter.

El mundo, irremediablemente, se ha vuelto más dependiente de la Internet. El número de personas en línea a nivel global casi se ha triplicado, de 2.000 millones de individuos en 2015 pasó a 3.800 millones en 2017, y llegará a 6.000 millones de personas en 2020. Se estima que los gastos o inversión en seguridad cibernética se van a duplicar, de 3 trillones de dólares en 2016 a 6 trillones de dólares en 2021 (Oppenheimer, 2019, p. 341).

Por lo demás, la crisis de la pandemia nos brinda la oportunidad de demostrar la humanidad que compartimos. Para combatir la COVID-19, podemos hacer esfuerzos extraordinarios que sean compatibles con las normas de derechos humanos y el Estado de derecho. Las decisiones que los gobiernos tomen ahora, para afrontar la pandemia, determinarán cómo será el mundo en el futuro.

Amenazas

Las aplicaciones móviles para la pandemia son motivo de puntos de vista controversiales, que comprenden la metodología y las técnicas empleadas en la selección, procesamiento, interpretación, difusión y utilización de la información personal y colectiva.

La crisis generada por la COVID-19 ha ampliado y profundizado los sistemas de control social, implementados por los gobiernos en forma oscura y sin mecanismos de rendición de cuentas, que usan la pandemia para realizar un lavado de imagen que les permita sobrevivir a la crisis con una renovada justificación autoritaria. Crisis que no debe ser excusa para encubrir el inicio de una nueva era marcada por una expansión masiva de los sistemas de vigilancia digital invasiva.

Ello puede dar lugar a la aplicación de tecnologías digitales, como nunca antes, que permiten y facilitan nuevos controles, observaciones, valoraciones y juzgamiento de la vida privada, y la adopción de políticas de control individual y colectivo, así como de acciones y medidas de carácter represivo.

Las fuerzas del orden en el mundo tendrán a su alcance, de esta manera, múltiples posibilidades para ejercer el control social con una determinación concreta y precisa, pero que al mismo tiempo puede convertirse en peligrosa y amenazante para la sociedad y las organizaciones.

Desde el inicio de la pandemia por el coronavirus, distintos gobiernos de todo el mundo han diseñado y utilizado apps para teléfonos celulares, con el objetivo de detener, o al menos controlar, el contagio. Pero las aplicaciones pueden habilitar vigilancia digital que no debe prolongarse más allá de la crisis sanitaria que afecta al planeta.

Sin embargo, es altamente probable que la vigilancia tecnológica desarrollada y aplicada durante la pandemia se extienda durante mucho tiempo, al punto que sea parte de la vida cotidiana del mundo moderno.

El acceso a los datos de localización, identificación de características y comportamiento individual a través de los teléfonos móviles, amenaza la privacidad, la libertad de expresión y la libertad de asociación. La pérdida de privacidad es la primera idea en la que se piensa cuando se trata de vigilancia. La privacidad plantea problemas como la imparcialidad, la justicia, las libertades civiles y los derechos humanos.

Un examen apenas superficial de la proliferación de aplicaciones móviles en época de pandemia, permite encontrar incontables puntos de duda sobre el manejo de la información: ¿cómo se la manejará de manera anónima para no identificar individuos?, ¿quién tiene acceso a ella y cómo será utilizada?, ¿por cuánto tiempo y bajo qué condiciones se la almacenará? Las respuestas a estas interrogantes son todavía un misterio.

Además, este examen sugiere dos elementos significativos de vigilancia. El primero y más importante, el Estado ya no puede proteger a los ciudadanos porque el poder ligado a la política se ha evaporado en un flujo y reflujo continuo. Y, segundo, toda introducción de tecnología orientada a la vigilancia crea un mundo más inseguro. Y porque buscamos un falso ideal de seguridad y felicidad eterna, es que reglamentamos al otro desde la desconfianza que nos inspira su presencia.

No obstante, existe una creciente demanda de tecnologías digitales, con los consiguientes riesgos de que el acelerado empleo de estas aplicaciones durante la emergencia actual vulnere derechos, amplíe la brecha digital y las posibilidades de ser víctima de ciberdelitos.

En Ecuador, en junio de 2020, el tráfico de internet en los hogares, en medio de la pandemia, creció hasta en 63 % (El Universo, 2020), en tanto que, hacia fines de agosto, previo al inicio de clases en la Sierra, comenzó una alta demanda de dispositivos electrónicas, como computadoras, laptos, tablets, celulares, etc.

Desafíos

Las tecnologías digitales pueden plantear desafíos relacionados con varios derechos humanos y también derechos digitales, que en ni en la ley y menos aún en la práctica se hallan protegidos.

Es por ello que la aplicación de las tecnologías digitales es controvertida y es vista con recelo, puesto que pueden infringir derechos. Las tecnologías, que al principio parecen ser medidas efectivas para controlar y limitar la propagación del virus, en la práctica abren la posibilidad de usarlas en forma abusiva.

Por ello, es fundamental considerar posibles excesos, riesgos y consecuencias que tiene y podría tener la universalización de la vigilancia por medio del empleo de las tecnologías, especialmente digitales. Mucho más cuando observamos que la vigilancia tecnológica está estrecha-

mente asociada con el "control social" o el "Gran Hermano" (Orwell, 1984), pero ignora los contenidos ideológico-políticos que están detrás, así como las circunstancias que la hacen posible.

Las tendencias actuales de los gobiernos de ampliar y profundizar el seguimiento, la vigilancia y el control de las tecnologías digitales, que deberían ser de duración limitada, pone en riesgo la vigencia de los derechos.

Uno de los desafíos de mayor complejidad gira alrededor, precisamente, de la incidencia de estas tecnologías en los derechos a la privacidad, la intimidad, la libertad de expresión y de asociación, pues sus aplicaciones, entre otras funciones, facilitan el rastreo de patrones de comportamiento de la población y, en especial, de los movimientos de las personas, a través de los mecanismos de exploración de contactos y *big data*.

La rápida expansión de la COVID-19 puede obligar a las autoridades a tomar decisiones apresuradas y complejas que, posiblemente, pueden ser efectivas en el corto plazo, pero en el mediano plazo pueden tener impactos negativos sobre los derechos digitales y otras esferas de la gobernanza local.

Por el contrario, deben trabajar para garantizar que toda limitación observe celosamente el respeto y la protección de los derechos humanos, y no se elija entre el uso de aplicaciones destinadas a rastrear la propagación del virus y el control y protección total de la privacidad de las comunidades.

Es importante que la aplicación de cualquier iniciativa basada en tecnologías, orientadas al uso de datos, se enfoque también en resguardar los mecanismos de control de la propia autonomía y dignidad personal y colectiva.

Y cabe preguntarse: ¿Hasta qué punto la ética establecida o incluso la normativa sirven para tratar la vigilancia contemporánea? ¿Cómo resistir a la búsqueda obsesiva del falso ideal de seguridad que, a la postre, subyuga los derechos de libertad y el pretendido carácter neutral de las tecnologías, especialmente? ¿Cómo enfrentar el desmesurado aumento de los poderes de vigilancia y control digital de los Estados, con el argumento o pretexto de la seguridad individual o colectiva?

Las medidas de vigilancia ante la COVID-19, que han ido en aumento, no deben ser competencia de los organismos de seguridad o inteligencia, sino que tienen que estar sujetas a la supervisión efectiva de órganos independientes adecuados.

Las respuestas a la pandemia, que contengan medidas de recopilación de datos, deben incluir medios de participación libre, activa y significativa de las partes interesadas pertinentes, en particular de especialistas del sector de la salud pública y de los grupos de población más marginados.

Se debe, además, ofrecer a las personas la oportunidad de conocer e impugnar toda medida que se tome en relación con la COVID-19 para recopilar, agregar, conservar y emplear datos. Las personas que hayan sido sometidas a vigilancia han de tener acceso a medios efectivos para interponer recursos. Todo usuario de las tecnologías digitales debe incorporar mecanismos de rendición de cuentas y salvaguardias contra el uso indebido de sus datos.

No podemos dejar que la pandemia sirva de excusa para ejercer vigilancia masiva, indiscriminada e indefinida y prescindir de la concepción y de las normas de

ética y moral para tratar la vigilancia contemporánea. La vigilancia masiva es sustancialmente más peligrosa que cualquier otro mecanismo de control.

Por ello, el llamamiento a la vigilancia ética de las nuevas herramientas normativas del orden y de la seguridad, adquiere todo su sentido cuando se relaciona con las importantes lógicas que se desarrollan en los regímenes democráticos contemporáneos (Mattelart, 2009).

Por lo tanto, los datos recopilados, conservados y agregados para responder a la COVID-19 deben tener un alcance y duración limitados en función de la pandemia, y no utilizarlos con fines comerciales ni de otra índole. No podemos permitir que la pandemia de la COVID-19 sirva de pretexto para menoscabar el derecho personal a la privacidad. ¿O es que debemos redefinir el concepto de privacidad?

Pero en este caso también podemos preguntarnos ¿hasta dónde el gobierno y las empresas tecnológicas que ofrecen servicios "gratuitos" a cambio de recopilar información de sus usuarios, pueden hacer uso de nuestros datos personales? ¿No deberían comprometerse estas corporaciones a tratarla de manera transparente y a mantener informados de los usos? De ahí que es necesario conciliar la intimidad personal con la nueva sociedad tecnológica en la que estamos viviendo.

De otro lado, si bien es cierto que la introducción de la tecnología como un instrumento de mitigación de riesgos ha favorecido la vida social en muchos aspectos, sin embargo, no se puede dejar de observar que se ha creado "una falta" en la predisposición ética del sujeto, por su propio accionar cuando median las aplicaciones tecnológicas.

El gobierno nacional y los gobiernos locales desempeñarán un papel crucial en la configuración de las tecnologías digitales, de una manera que garantice procesos de toma de decisiones transparentes, abiertos e inclusivos.

Bibliografía

Arendt Hannah. (2018). *Verdad y mentira en la política*. Barcelona: Planeta.

Bauman Zigmunt & David Lyon. (2013). *Vigilancia Líquida*. Buenos Aires: Planeta.

Byung-Chul Han. (2018). *En el enjambre*. Barcelona: Herder Editorial.

Código Orgánico Integral Penal. (2014).

CGLU. (2020). "Las Experiencias de Aprendizaje en Vivo: más allá de la respuesta inmediata al brote". Recuperado de https://www.uclg.org/es/temas/experiencia-de-aprendizaje-en-vivo-beyondtheoutbreak

Constitución de la República del Ecuador. (2008).

Declaración Universal de Derechos Humanos. (1948).

El Comercio. (30 de agosto de 2020. "Alta demanda de computadores previo al inicio del año escolar no presencial". Recuperado de https://www.elcomercio.com/actualidad/alta-demanda-computadores-clases-virtuales.html

El Universo. (26 de junio, 2020). "El tráfico de internet en los hogares creció hasta 63 % en medio de la pandemia del COVID-19". Recuperado de https://www.eluniverso.com/noticias/2020/06/23/nota/7881924/internet-fijo-servicio-operadoras-demanda-cuarentena-covid-19

Friedman Thomas. (2019). *Gracias por llegar tarde*. Tercera edición. Barcelona: Planeta.

Kampfner John. (2011). *Libertad en venta* ¿Por qué vendemos democracia a cambio de seguridad? Barcelona: Ariel.

Mattelart Armand. (2009). *Un mundo vigilado*. Barcelona: Paidós.

Noticias ONU. (2018). Artículo 12: derecho a la intimidad. Recuperado de https://news.un.org/es/story/2018/11/1446671

Ojeda Segovia, Lautaro. (2013). S*eguridad ciudadana y Tecnologías de Información y Comunicación.* Quito: Editorial Rayuela.

ONU. (2016). "El derecho a la privacidad en la era digital". Recuperado de https://www.acnur.org/fileadmin/Documentos/BDL/2017/10904.pdf

Oppenheimer, Andrés. (2018). *¡Sálvese quien pueda!,* Bogotá: Penguin Random House Editorial.

Orwell George. (s.f.). 1984. Caracas: Corporación Lucemar.

Pacto Internacional de Derechos, Civiles y Políticos, adoptado por la Asamblea General de Naciones Unidas. (1966). En vigor marzo 1976.

Ranchal, J. (2020). "Covid-19 y privacidad ¿La excusa para una era de vigilancia digital masiva?" Recuperado de https://www.muyseguridad.net/2020/04/08/covid-19-y-privacidad/