¿Vigidemia? CoViD 19 y la falta de límites de siempre[1]

Mg. Celeste Box
Docente Ciencia Política
Facultad de Ciencias Sociales, UBA

El seguimiento de las comunicaciones, acciones o movimientos de una persona o grupo por otra entidad -fuere gobierno, empresa, grupo o persona-, sin previa autorización para esos fines, tiene nombre y apellido: Vigilancia digital. Será legal si está fundada en indicios de conducta delictiva y autorizada por una autoridad independiente. Será legítima si son lo menos intrusivas posible para alcanzar el resultado deseado, de manera que causen más beneficio que daño. Dadas las características de una pandemia, de suyo esta vigilancia digital devendrá masiva (no sería pertinente redireccionarla sólo hacia una persona o un grupo pequeño de ellas, sino que apuntaría a un conglomerado de individuos lo suficientemente grande como para alcanzar patrones y todo tipo de inferencias acerca de la conducta de personas y virus). Pero claro, esto no la hace ventajosa en todas sus dimensiones: si bien se vigila *para cuidar,* esta acción implica control de las comunicaciones (Internet y telefonía) de gran número de personas, sin que esté asegurado el fin de ese control ni el producto que se obtiene (una jugosa cantidad de datos). Además que su despliegue puede no cesar con la pandemia.

Por supuesto que vulnera nuestra privacidad. También altera el debido ejercicio de la libertad de expresión (dado que se entromete en tecnologías donde vehiculazamos y limita nuestras comunicaciones). Este aspecto ha estado a la orden del día en los últimos años: no es necesario pensar en el affair Snowden, intuir que los gobiernos y grandes empresas pueden tentarse con usar información a su alcance no parece algo impensable. Pero el problema reside en que se combina -a veces se mezcla, otras se esconde- con otros dispositivos muy interesantes desde el punto de vista de lo que pueden aportar a nuestra vida, como es el acceso a ingente cantidad de información que permite la toma de decisiones basada en evidencias, la inteligencia artificial que asiste diagnósticos, el aprendizaje automático al clasificar información ayudar al diagnóstico clínico, y tantos otros fenómenos que complejizan nuestro tiempo vivido en la Red.

La vigilancia masiva es ilegal acorde legislación internacional de derechos humanos. Los países tienen a su cargo legislar para garantizar la protección de las personas y así asegurar que sólo un juez pueda autorizar intervención en nuestras comunicaciones (la Declaración Universal de DDHH reconoce, en su artículo 12, el derecho de protección ante injerencias arbitrarias en la vida privada, domicilio o correspondencia de las personas). No alcanza con desestimar la acción ('no me importa que me espíen, no tengo nada que ocultar'): justamente porque no hay nada malo de por medio, no hay razón para vulnerar la privacidad. Y porque los Estados no pueden desatender sin más derechos

[1] Semblanza escrita para *Question* (UNLP), edición especial Incidentes III COVID 19, mayo de 2020

como la privacidad y la libertad de expresión con el pretexto de gestionar una crisis de salud pública, antes por el contrario, dado que los derechos humanos son interdependientes -no se puede garantizar uno y vulnerar al otro-, la protección de aquéllos también debe promover la salud pública. Bajo razones de fuerza mayor (usualmente seguridad interna, terrorismo, una guerra o una pandemia), se colecta información con datos personales que puede ser usada también para otros fines (seguir periodistas, perseguir a activistas, crear perfiles para discriminar a minorías y acabar con la libertad de expresión). Con el agregado que la historia posterior al 2001 nos ha enseñado que la vigilancia gubernamental traccionada por tiempos excepcionales luego deviene una necesidad permanente, con unas capacidades e infraestructuras perennes, que parecen justificarse por sí mismas. A esto hay que sumarle los problemas intrínsecos de esas tecnologías. Con esto no planteamos que sea un hecho, sino sólo una posibilidad: las tecnologías de inteligencia artificial deben ser intervenidas para que no aumenten sus posibilidades de discriminación ilícita y que no perjudiquen de forma es desproporcionada a comunidades ya marginadas. Los algoritmos opacos dentro de ellas pueden haber sido nutridos por datos sesgados, lo que influirá las decisiones que ese algoritmo tome, o bien informe para que los humanos decidan.

El problema es triple: por un lado, los gobiernos deben prohibir la vigilancia masiva y el intercambio ilegal de información confidencial. El problema reside en que, si hablamos de programas como el *Prism* (aquel que Snowden denunció) o la antigua alianza de inteligencia *Los Cinco Ojos,* o las muchas agencias de inteligencia menores, pues no sólo no la prohibirán sino que la conducen. Por el otro lado, para dar con tecnologías de vigilancia (o para servir a ellas), no tenemos que pensar en fastuosas estructuras gubernamentales: hoy resulta muy sencillo recolectar y procesar grandes volúmenes de información, por lo que una estructura muy modesta alcanza para comenzar o para colaborar con una mayor (pública o privada). Por último, también es un problema de contexto y de implementación: antes y durante la pandemia, los gobiernos buscan, conservan y utilizan datos de teléfonos móviles para conocer patrones de sus habitantes. La carencia de leyes que protejan a personas involucradas, la ausencia de medidas de protecciones añadidas como el anonimato o agregación, no hacen nada por dejar información personal que podría ser utilizada y reutilizada con los fines más diversos.

CoViD 19 y tecnología

La tecnología puede cumplir un rol apoyando una estrategia basada en principios epidemiológicos, para buscar y acumular información científicamente correcta y logísticamente eficiente. Corea del Sur, Japón, Hong Kong, Singapur e incluso China apostaron por ella (mientras en Argentina se reclamaban testeos masivos, en Corea del Sur, testear y trazar eran sinónimos). La excepcionalidad es un estado ideal para implementar medidas y metodologías que luego pueden no ser abandonadas y no son tan visibles (incluso, en el apremio, pueden ser ampliamente apoyadas por la mayoría de la población). Por eso en medio de un brote, podremos conceder que un gobierno utilice datos de telefonía para localizar a quien rompe cuarentenas, revise historiales de viaje y mida el riesgo de cada viajante, use cámaras térmicas.... Parece necesario *prima facie*, pero ¿esta es la única

información a la que se accede? Si, en el mejor de los casos, este monitoreo sólo dura mientras el paciente se encuentra atravesando la enfermedad y recuperación, esos datos históricos personalizados ¿serán anonimizados, eliminados o custodiados debidamente? (por cierto, aún en el caso de información anonimizada, cruces ulteriores con otros datos, la hacen pasible de inferencias válidas que sortean la anonimidad inicial).

Desde tiempos de John Snow (mitad del siglo XIX), el conocido médico británico considerado el padre de la epidemiología moderna, tras deducir que el patrón de contagio del cólera es por agua y no por aire, como se creía. Desde antes, y reforzado por Snow, sabemos que la evidencia de los datos -por entonces, un puñado-, puede acercarnos más a un mundo previsible, fuera de nuestras especulaciones o temores. En menos palabras, podemos conocer más de las consecuencias de nuestras acciones individuales y la combinación que producen las colectivas, como también responder al funcionamiento real del universo que nos rodea. Nuestro mundo se tornará más previsible. Es un hecho que sobre la CoViD 19 carecemos de certezas: si quitamos la capa de trascendidos, expresiones de deseo y manifiestas fake news, veremos que la ciencia está investigando sobre la marcha los comportamientos de un virus que aún no conoce por completo. Desde tiempos de Snow a las mieles de la actual big data nos diferencia la escala, un potencial de rastreo incomparable, el nivel de detalle de los datos (granularidad) y la facilidad de acceso como de permutaciones (literalmente, de computaciones) que podemos hacer con esos datos. Pero nada de esto debería llevarnos a un pensamiento esquizoide, donde utilizamos y pregonamos la cara favorable de la cuestión y omitimos otros aspectos que debemos y podemos gestionar (caso contrario, a futuro sin duda tendremos que costear).

Aún cuando las prácticas de seguridad estén aseguradas, y no podamos deducir ningún tipo de vigilancia a través de dispositivos, lo cierto es que no todo está zanjado: Sigue siendo procedente preguntarse por la validez de los cruces de información. Conocer el valor herramental de una tecnología no debería estar sólo en su novedad, deberíamos ver sus potenciales usos sin descontar, en ningún caso, si las interpelaciones que las personas que la usan realizan son efectivamente válidos. Conocemos investigaciones que hacen inferencias inválidas cruzando datos a los que conceden valor herramental (y pueden efectivamente tenerlo), pero asumen que esta operación intelectual los acerca a un patrón de funcionamiento que es sólo un a priori que le imprimieron a información que narra otros patrones significativos. Y todo esto es previo a la tecnología, pertenece al orden de la metodología de la ciencia, de la posibilidad de conocer efectivamente la realidad. Por ejemplo, la geolocalización, ¿arroja información que suple la falta de testeos?. Usualmente podemos llegar por diferentes rutas de información a reconstruir el rompecabezas que es la realidad (y aquí esto representaría diferentes tipos de datos), pero eso no quiere decir que unos reemplacen por completo a los otros. No poseemos testeos masivos, y las razones para ello pueden ser legítimas -no se justifica sanitariamente, no contamos con reactivos suficientes en esta coyuntura de carencia, y demás razones-, pero no obstante, los datos de localización ¿(sobre)compensan esta faltante? Podremos saber, gracias a la localización del móvil, si alguien rompe la cuarentena, ¿pero nos dice algo de la conducta de esa persona (distanciamiento, higiene, uso de barreras, etc.)?. Sin duda la geolocalización puede servir para cotejar la expansión del virus, pero no sería bueno que depositemos en ella más información que la que puede dar, y que cuando efectivamente la provea,

esta no sea concluyente para otros problemas que los que le son atinentes (en ese caso nuestra decisión basada en evidencia se caerá de bruces y sólo haremos la realidad más distante de nosotros). En pocas palabras: geolocalizar no nos hace tener más respiradores, tampoco compensa lo que brindaría una vacuna. Por eso, conocer los límites de la información que buscamos nos permitirá confiar en ella en los términos que ella determina (según lo que nos provea) y dejar erigirse como *factotum* de toda solución.

De vuelta en la tensión necesidad de cuidados y preservación de nuestra privacidad, en esta carrera contra un virus no todos los participantes parten del mismo punto inicial. Corea del Sur, el país que dejó de lado la privacidad y puso sobre la mesa el sistema de cuarentena preventiva combinada con el ratreo a las personas que tuvieron contacto con las infectadas. Su lema: 'trazar y testar' (es decir, seguir el decurso del virus como forma de control). Esto debe ser pensado históricamente: se habían visto las consecuencias de un virus como el SARS, y a partir de allí supieron que en pandemia las leyes podían ser un problema. Por eso avanzaron con dos modificaciones legislativas (2015 y 2018) para la privacidad en emergencias. Sin ellas, el Ministerio de Sanidad jamás hubiese podido acceder a datos de movimiento de los ciudadanos sin consentimiento (Cfr. aquí). Tanto es así que hoy, en plena pandemia, si una declaración personal es incompleta o denegada, el Ministerio de Salud puede hacerse de la información del paciente incluso por vía del uso de tarjetas de crédito, georreferenciamiento móvil, y cámaras de seguridad. De este modo, el gobierno envía material de apoyo sobre coronavirus acompañado de datos personales y con detalles de sus movimientos (mientras se envía un mensaje a los contactos para que se testeen y que permanezcan en sus domicilios obligatoriamente). Esto también quebranta el privadísimo dispositivo médico-paciente, y sin ninguna garantía de que esa información sea destruída post pandemia (o cuando algún criterio médico lo determine). En el caso chino, una combinación de escáneres inteligentes y reconocimiento facial en espacios públicos, rastrea la propagación. Una compañía preponderante como Alibaba usa datos de salud personal y clasifica a las personas (verde será seguro, amarillo precisa cuarentena de siete días, y rojo de catorce). En una sociedad donde la democracia está ausente, esto sólo parece ingeniería social lícita.

Al otro lado del globo, otra recolección sucede gracias al Internet de las Cosas (es decir, la capacidad de recolectar información a gracias a dispositivos de uso doméstico conectados, junto con otros propios de espacios semi públicos -como molinetes-, y de sensores varios). En Estados Unidos, el termómetro inteligente de la empresa Kinsa, releva y carga temperaturas de usuarios, lo que le permitió alcanzar predicciones que estuvieron hasta tres semanas por delante de las de los Centros para el Control y la Prevención de Enfermedades. Israel es otro caso para analizar: Netanyahu autorizó al Grupo NSO (una compañia israelí que desarrolla software de vigilancia para gobiernos) para que junto a la Agencia de Inteligencia Interna se utilice una tecnología de rastreo (desarrollada para combatir el terrorismo) con la finalidad de rastrear movimientos de pacientes con coronavirus y de las personas con quienes se contactaron (con dos semanas de información de la persona infectada, coteja con la ubicación de quienes estuvieron cerca por más de quince minutos proveniente de las compañías de teléfonos móviles). Este desarrollo les envía mensajes para que se aíslen obligatoriamente. Recordemos que Israel fue titular del famoso *Pegasus* (acusado de espionaje manifiesto), que incluso se apoderaba de mensajes cifrados (Amnistía Internacional

solicitó la revocación de la licencia de exportación infructuosamente porque varios países ya la probaron). Cada país es un mundo aparte, y eso incluye la opinión pública: en Israel, el servicio secreto y la vigilancia se perciben como herramientas de protección por lo que no se registran problemas en el uso de rastreo para controlar el virus. Las respuestas a esta diferencia son históricas y sociológicas. Exceden la pandemia con creces, pero también la influyen de manera directa.

Lamentablemente, el estado de excepción que implica una pandemia no sólo permite que los límites se corran en detrimento de la privacidad en aras del cuidado, sino que el hecho de que la vigilancia sobre un virus no pueda ser separada de quienes lo transportan, hace que vigilar al virus y a quien lo hospeda sea idéntico. Y esto es un problema no sólo por las fantasías basadas en errores que cualquier persona puede erigir: también lo es por las consecuencias de las declaraciones que líderes a cargo de gestionar sociedades en pandemia pueden tener. O bien generan expectativas que luego son una desilusión más (recordemos el anuncio de Trump sobre Google, asegurando que desarrollaría un sitio web de detección que dirigiría a las personas a testearse. Todo resultó ser *Verify*, un espacio que sólo está disponible para San Francisco, y no resulta lo que Trump aventuró); o bien apoyan y conducen procesos que tienen altos costos para la ciudadanía: Estados Unidos se encuentra en proceso de retirar normativa que protegía la privacidad de pacientes, por lo que muchas empresas tendrán acceso a datos personales de salud (Cfr. aquí), lo que significa que ellas darán esa información a una cantidad de agencias gubernamentales (el único requisito es la buena fe y asegurar que el fin reside en la salud pública). El problema es mayor que éste: lo cierto es que sería ingenuo interpelar sólo a las corporaciones poderosas (fueren multinacionales o gobiernos). Por ejemplo, más de la mitad de estadounidenses apoya el rastreo anonimizado del gobierno de celulares (recordemos que los datos anonimizados pueden ser cruzados con otras bases ulteriormente, y aún así podemos hacer inferencias aproximativas sobre esa información, por lo que anonimizar no implica el fin de la cualidad personal de una pieza de información). Este número proviene de una encuesta de Harris Poll (dos mil casos) a fines de marzo. No obstante, durante el 2019, la misma consultora sondeó que los estadounidense habían indicado que la privacidad de los datos era el mayor desafío que enfrentan las compañías. Parece que no percibimos de la misma manera la injerencia en nuestras vidas, y eso no siempre es bueno: es en estos cambios, basados en razones de fuerza mayor, donde se liberan controles, y los escrutinios parecen superfluos (cfr. aquí). Esto es un problema: cuando intentemos volver a implementarlos, el umbral de control será mucho menor.

Además es necesario tener en cuenta que esta pandemia no ocurre en vacío. Y que los problemas de privacidad y uso de la información son profundos y anteriores a ella. Por ejemplo, Google, uno de los *cinco grandes* (junto con Facebook, Apple, Microsoft y Amazon), en agosto de 2018 firmó un contrato con Ascensión, una cadena de hospitales y consultorios con sede en St. Louis. Eso le dio acceso a detalles de salud personales de millones de estadounidenses en más de veinte estados (Cfr. aquí). En una columna para Wired, propone forzar sus algoritmos para persuadir abiertamente a los usuarios aprovechando el conocimiento de su actividad en línea –bombardeando a los que no prestan atención a las medidas de prevención–, amplificar las acciones de solidaridad y utilizar la información que circula en las plataformas para distribuir la entrega de suministros.

La contracara de Estados Unidos es Alemania. Allí se critica el rastreo porque interferiría en el derecho fundamental a la autodeterminación informativa, sobre todo en la coyuntura de los cambios en la Ley de Protección contra Infecciones (que propuso el ministro de Salud), que implementaría una aplicación para monitorear los síntomas del coronavirus SARS (a esto se sumó el Instituto Robert Koch poniéndose al frente del desarrollo, pero que, según la normativa de protección de datos vigente, sólo puede obtener datos de rastreo remitidos de forma voluntaria, anónima y con fines no comerciales). Ulrich Kelber, el Comisario de Protección de Datos afirmó que las medidas de procesamiento de datos deben ser necesarias, adecuadas y proporcionales (cfr. aquí). Y remarcó que no hay evidencia de que los datos de ubicación individuales de los proveedores de teléfonos móviles puedan determinar las personas de contacto (Cfr. aquí). Por todo esto es interesante destacar el caso de la iniciativa de *Seguimiento Paneuropeo de Proximidad para Preservar la Privacidad* que reune el Instituto Fraunhofer Heinrich Hertz y una centena investigadores de ocho países y hasta la colaboración de Vodafone. Esta iniciativa implementa un uso anónimo de bluetooth de baja energía -acorde los límites del Reglamento General de Protección de Datos de la Unión Europea, por lo que no implica seguimiento de datos de ubicación-, y quienes no tengan móvil pueden usar bluetooth en pulseras. Esto lo hace menos intrusivo que el GPS móvil, y de hecho, quienes no tengan teléfono celular podrían usar brazaletes con Bluetooth). Además, sigue el modelo de la app *TraceTogether* de Singapur, registrando las conexiones entre teléfonos inteligentes en un dispositivo -y no un servidor central-, por dos semanas y con un cifrado seguro.

En pocas palabras: hay maneras de hacer bien las cosas. No podemos pensar en una gobernanza simple, que sólo esté integrada por la tríada gobiernos, empresas y consumidores, para conformar un sistema sólido de escrutinio colectivo, en que organizaciones colectivas representativas se conformen para colaborar con buenas prácticas y fiscalizar el funcionamiento acorde al respeto por derechos fundamentales.

Es necesario, también, ver ventajas en la cuestión. Estas líneas pretenden poner en la mesa una tensión dinámica que recorre las indudables ventajas de la tecnología en nuestras vidas, sin descuidar sus costos, para poder, finalmente, gestionarlos democráticamente. En este sentido tenemos el caso del Instituto de Big Data de la Universidad de Oxford, que a mediados de abril, compartió información epidemiológica para mejorar el trazado de contactos (Cfr. aquí). Según simulaciones que probaron (de una ciudada modelo de un millón de habitantes), si al menos el sesenta por ciento de la población utilizase este tipo de tecnología (rastreo de teléfonos) junto con otras intervenciones, el potencial de éxito que tendría es amenizar la pandemia y, fundamentalmente, reactivar la dinámica social dejando las cuarentenas (ofrece diferentes maneras de implementar cuarentenas en los contactos en riesgo y allí implementar diferentes testeos). Ellos descubrieron que alrededor de la mitad de los contagios ocurren antes de que se muestre sintomatología (adelantarse incluso un día a esto, puede torcer la pandemia, al reducir casos y el ingreso al sistema de salud). En el Big Data Institute saben que hay problemas de privacidad relacionados con el mal uso de la información: por eso ofrecen mecanismos de observación con múltiples partes -algo así como una observación conjunta de todo el proceso-, entre otras cuestiones, para evitar la conducta defensiva de las personas usuarias, como mentir.

Esta dinámica de administración y control por varias partes nos permite mostrar que se pueden implementar buenas prácticas, y esta es la tecnología que necesitamos. La tecnología no tiene que necesariamente invadirnos, este costo lo padecemos por la falta de gestión sobre procesos que no son sólo técnicos, sino también sociales. La falta de gestión sobre ella -o sobre sus potenciales consecuencias- deja lugar a los usos que se gobiernan por los hechos. Y donde no hay reglas, en realidad, suele haberlas, porque es el escenario ideal para que surjan las de quienes tienen más poder.

Veamos otro caso. Una inteligencia artificial (IA) que, desde la empresa que la implementa, se respetan buenas prácticas. Esta inteligencia artificial automatiza procesos de manera muy sencilla, Entelai Pic Covid 19, utilizada para la detección de coronavirus en radiografías de tórax (no diagnostica Covid 19, sino que descarta patrones producidos por otras neumonías para así justificar la realización del test PCR, junto con la evaluación clínica). Pic Covid 19 está disponible libre y gratuitamente para profesionales de la salud de todo el mundo. Es un proyecto útil porque ayuda a estandarizar la detectabilidad, aún cuando el ojo clínico sea irremplazable -y claro que también es apto para lograr la discriminación entre cuadros-, pero puede apoyar decisiones ante situaciones de cansancio o en personal de salud con insuficiente entrenamiento previo (típico en centro de salud con exceso de demanda). Este algoritmo aprende como los médicos en 'la clínica' -es decir, en la práctica de la revisación médica-: se lo nutre con imágenes. En este caso, se inició el proyecto con más de cien imágenes de casos confirmados con Covid-19, otros tantos con otras neumonías y un grupo control sin neumonía, con igual distribución de edad y género (eso permite que aprenda a diferenciar de otras características ajenas al Covid-19 como osificación y demás aspectos que se hallan en un grupo y no en otro). Igual que en la clínica, la cantidad importa: mientras más imágenes haya analizado el algoritmo, más preciso será. Por eso la empresa permite aportes de personal de salud, en la medida que sea material anonimo, y se compromete a eliminarlo luego de enriquecer el algoritmo. A futuro sería interesante que una regulación exhorte a ella junto con un Estado que constate ese acto, y existan mecanismos de gobernanza de actores de sociedad civil y universidades para acompañar este proceso.

¿Y después?

Este será un proceso largo. Al menos, todo lo largo que determine la posibilidad de acceder a un tratamiento efectivo y/o una vacuna. Sin contar que hasta ese momento, el riesgo de rebrote (y nueva cuarentena) existe. Muchas costumbres cambiarán, y las dinámicas sociales -macro como microsociales-, también se verán alteradas. Aprenderemos -y toleraremos-, que muchos espacios semi públicos (fueren una empresa con entrada y salida de personas, una oficina pública o una estación de transporte), posean dispositivos analógicos como una organización que priorice la separación entre personas, la falta de espera en un mismo espacio, la entrada por turns a ciertos establecimientos, y otros que requieren tecnología digital como los dispositivos de medición de temperatura. Por ejemplo, la Agencia Española de Protección de Datos (AEPD) advirtió que estas cámaras suponen una injerencia en los derechos de los afectados, más aún que no hay consentimiento explícito de por medio para poder eludir el criterio previo de las autoridades

sanitarias. En términos de información personal, el problema reside en que la temperatura corporal es un dato de salud en sí mismo -como cualquier otro valor médico-, y que presupone que una persona padece o no una enfermedad, por lo que la denegación posterior de ingreso de una persona al lugar al que se conducía -motivada por el registro- haría público un dato personal a terceros. Por eso la AEPD reclama a que sea el Ministerio de Sanidad uno protocolo claro sobre la toma masiva de temperaturas (cuál debe ser la temperatura de aviso, que protocolos tomar con la persona detectada o incluso qué tipo de medidas usar). A esto debería sumarse la validez de esa información, que debería incluir una conservación corta en el tiempo, y establecer la legalidad de, posterior a la medición, impedir el ingreso de una persona con la temperatura elevada al establecimiento. Más allá de la vigilancia por vía de los datos personales, también quedan otros espacios, antes privados, a los cuales tendremos que transigir nuestra privacidad y gran parte de nuestra libertad: viviremos una realidad más pasible de ser medida, más sujeta a estandarizaciones y aspectos médicos. Un caso interesante es el del Félix Hand Washing Control, un dispositivo que *invita* al personal de una compañía u organización a higienizar sus manos en el momento preciso, de acuerdo a un cronograma individual definido por la propia organización. El cumplimiento se registra, publicando las veces que realizó la tarea, y el tiempo que invirtió en hacerlo, junto con la notificación del horario programado de la próxima higienización. Se instala en las cercanías del lavabo y se activa con una tarjeta de aproximación para cada integrante de esa organización, y puede estar acompañado con una cámara que valida su identidad (además de contar con un software en la nube, que permite acceder a cualquier responsable al tanto del cumplimiento de este procedimiento). No podríamos afirmar si será un mundo más feliz, pero sin duda será uno más controlado.

Falta de límites (antes y durante la CoViD 19)

Hacia inicios de abril, Amnesty Internacional, junto con otras prestigiosas organizaciones del tercer sector (entre las que se encuentran Access Now, Algorithm Watch, Civil Liberties Union for Europe, CódigoSur, Fundación Vía Libre, Human Rights Watch, Open Knowledge Foundation, World Wide Web Foundation, entre otras), publicó una declaración donde exhortaba a los Estados a respetar los DDHH en su empleo de tecnología digital en el combate de la CoViD19. En este pedido se asume que una emergencia global precisa de una respuesta coordinada y global, o, al menos, de gran escala, para que no constituya la oportunidad de iniciar -o simplemente ponerle una capa más- a la expansión de los sistemas de vigilancia digital invasiva y masiva. Se afirma que la tecnología puede y debe desempeñar importantes funciones durante la pandemia (sobre todo en difusión de cuidados y en el acceso a la salud pública), pero el aumento del poder de vigilancia digital estatal reviste una amenaza a la privacidad, la libertad de expresión y la libertad de asociación.

Así, el pedido de las organizaciones del tercer sector, versa sobre implementar condiciones a la mayor vigilancia -justificada por la situación-, centrándose así en los límites, y no en la negación de la necesidad temporaria de medidas excepcionales por parte de los Estados como tampoco al uso de tecnología. De este modo, aclara que toda medida debe ser legal, necesaria y proporcionada (prevista por ley y en manos de autoridad competente). El correlato de esto reside en la transparencia de los gobiernos respecto de estas decisiones -es la única manera en que pueden ser

analizadas, modificadas y eventualmente anuladas-, como también la duración de las medidas, ancladas en el período de pandemia. La recopilación, conservación y agregación de de datos debe ser acotada a la pandemia y no alcanzar fines comerciales, políticos o de otra índole, y además, deben estar acompañado por un sistema de gobernanza, es decir, contar con la participación de las partes interesadas en ese proceso. Esto permite controlar otras situaciones como la reproducción de inequidades, (re) vulnerando a ciertos grupos en una coyuntura de pandemia).

El pedido también alcanza al proceso de anonimización: debe ser transparente, es decir, poder ser respaldado a posteriori en cuanto a la manera en que se han despojado de referencias personales. Lo mismo aplica al proceso de compartir datos con el Estado como -sobre todo- con el sector privado. Todo el proceso debe atenerse a la ley, además de ser escrutable para poder evaluar su impacto (la ciudadanía no puede desconocer con qué empresas se desencadena este proceso, y ellas deben atenerse al objetivo superior de palear la pandemia por sobre cualquier objetivo comercial). Y por último, tal vez lo más importante: el aumento de las medidas de vigilancia ante la COVID-19 no debe ser competencia de los organismos de seguridad o inteligencia, sino que tiene que ser pasible de supervisión por órganos independientes competentes como la Justicia, sin olvidar que las personas debemos poder ejercer el derecho a conocer e impugnar medidas relacionadas con la COVID-19 que impliquen recopilación, compilación, conservación y uso de datos (y por supuesto, toda víctima de vigilancia debe poder interponer recursos).

En esencia, el pedido de este grupo de organizaciones alude a que la excepción no implique una vía libre para todo tipo de acciones y menos aún, para la falta de contralor ciudadano.

No dudamos que las estrategias de intervención deben ser múltiples, pero el lugar de partida más interesante reside, sin dudas, en la sociedad civil (organizaciones del tercer sector de diferente tipo, universidades, centros de pensamiento, hasta asociaciones intermedias y personas físicas que no cuenten más que con su compromiso). A su vez, este mosaico debe estar organizado a su interior (con mecanismos de gobernanza que permitan su acción respetando su diversidad y sacando provecho de la complejidad). Su rol no debe ser sólo fiscalizador, es necesario un constante y creciente rol concientizador para el grueso de la población, en medidas más responsables con sus dispositivos y con la información que autorizan y vuelcan sobre ellos. Las demandas que articulen, los actores que logren comprometer, la incidencia que logren, no debe nublar un aspecto concomitante a este fenómeno de la vigilancia digital (con o sin situaciones de excepción): la dinámica social en la que se hacen esas demandas es diferente del pedido de legalidad sobre la información que recaba el Estado de hace una década y sin comparación a hace dos.

Antaño podíamos lidiar con la vigilancia analógica a manos de un gobierno, hoy esto se ha desplazado en compañías de enorme envergadura que pueden torcer al gobierno más íntegro (sobre todo, porque hemos volcado nuestras vidas en las herramientas y dispositivos que ellas proveen, por lo que incluso gobiernos que tengan en claro la protección de la ciudadanía, ostentan menos grados de libertad frente al poder que estas compañías detentan). Hoy son grandes y medianas empresas que proveen al Estado en esos servicios que el Estado debería regular, sólo que también se sirve de ellos, por lo que limitarlos sería ir en contra de algunos de sus fines propios fines... lamentablemente.

La información que interesa a los Estados ya no está sólo en manos de servicios de inteligencia nacionales y nucleados entre países, y es tan capilar, tan simple de cruzarse que su sola existencia facilita la vigilancia, inclusive amateur.

¿Dónde está el punto de equilibrio entre las ventajas de usarla y los costos en que incurrimos? Sin duda es un equilibrio dinámico -variará en el tiempo y deberá ajustarse a situaciones determinadas-, como también será diferente en cada país. Legislaciones de cumplimiento efectivo deberían estar a la orden del día: normativas como la GDPR queda desactualizada y acotada cada año, pero sin duda es un punto de partida del cual algunos paises no contamos. La sociedad civil organizada y la ciudadanía en general debería(mos) finalmente despertar y hacer algo por ello.

La vigilancia no empezó -ni terminará- con la COVID19. El aumento de recolección de información y la enorme capacidad de integración de ella es, por momentos, un desafío, por otros un problema y algunas veces una amenaza. Creemos, como Nayef Al-Rodhan, que se necesitó y se necesita un nuevo contrato social para proteger derechos y libertades individuales en un contexto de donde la tecnología permite hacer de cada una de nuestras acciones un hecho en sí mismo, fuere a partir de acciones voluntarias -como un click en una página-, o porque son producto de nuestras acciones pero no de nuestra voluntad explícita -como los provenientes de sensores-. Un nuevo contrato social permitiría pensar en un mecanismo de rendición rindan cuentas que no alcance sólo a gobiernos, sino que el valor esté anclado en el respeto a derechos fundamentales y alcance insumos, productos y servicios de las compañías que colaboran -o no- con los gobiernos... antes, durante y después de la pandemia. Corporaciones y gobiernos poseen ingente cantidad de información que no siempre autorizamos ni conocemos el fin con el que es utilizada. Algoritmos con eventuales sesgos se alimentan de esa información y toman decisiones. En situaciones extraordinarias como la CoViD 19, todo esto sigue activo, azuzado por la necesidad de obtener información en aras del cuidado de las personas y lograr acotar la pandemia. No sabemos del uso de esta última información en el después. Lo que sí sabemos es que en nuestro país -y en muchos otros-, no podemos ostentar una celosa supervisión ni una regulación robusta sobre el tema. Sólo podemos ostentar control, sólo que no somos titulares de él.