Fundación Vía Libre

Privacidad y Vigilancia en el Entorno Digital

Laura Siri

Módulo 4

Vigilancia estatal

Privacidad y Vigilancia en el Entorno Digital
Fundación Vía libre
Autora: Laura Siri[1]

La vigilancia estatal

El rol de los actores públicos en la recolección masiva de datos

Cuando hablamos de vigilancia y recolección de datos, las corporaciones de Internet son fundamentales pero, como veremos a continuación, son solo una parte de lo que Foucault llamaría un "régimen de gubernamentabilidad" orientado a la vigilancia, donde no solo intervienen actores privados, sino estados y gobiernos.

En efecto, para Foucault hay un sistema de poderes entrecruzados orientado a minimizar la desviación de la norma, premiando lo previsible y castigando lo anómalo. En este contexto, los estados actúan mediante mecanismos regulatorios orientados a la previsión, la anticipación y la minimización de riesgos. Para cumplir este objetivo requieren vigilar a las poblaciones. En ese sentido, es exactamente igual la vigilancia estatal orientada a prevenir crímenes o atentados terroristas que aquella destinada a saber a quién dar ciertos beneficios sociales. Es como si hubiera un pacto entre la población y el estado para garantizar la seguridad. Si alguien se enferma, el estado le brinda un seguro médico. Si pierde su empleo, le da una prestación. Si hay un desastre natural, el Estado constituye un fondo de ayuda. Y si proliferan los delincuentes o terroristas, el estado los combate con las fuerzas policiales.

Leer a Foucault es perturbador porque hace a uno preguntarse si es factible tener todos estos beneficios de la modernidad, que consideramos deseables, sin perder completamente la libertad. Por supuesto, uno también podría argüir que en muchos países no hay demasiado Estado de Bienestar y, sin embargo, igual hay un fuerte vigilantismo estatal.

Otro comentario que se podría hacer a lo que dice Foucault es que hoy no solo somos vigilados por nuestros propios gobiernos gracias a ese tácito intercambio de docilidad por seguridad, sino también por los de otros estados, que no nos dan nada a cambio. Esto es precisamente lo que destaparon las revelaciones de Snowden (aunque muchos ya lo sabían o lo sospechaban desde antes). Así lo detalla Julian Assange, el fundador de Wikileaks, en el prólogo de su libro Criptopunks (2013): Muchos gobiernos y ejércitos latinoamericanos resguardan sus secretos con hardware criptográfico. Se trata de aparatos y programas que codifican y descodifican mensajes. Los Gobiernos adquieren estos equipos para mantener sus secretos a salvo, a menudo con un alto costo para el pueblo, porque le temen, con razón, a la interceptación estadounidense de sus comunicaciones. Pero las compañías que venden estos costosos dispositivos gozan de lazos estrechos con la comunidad de inteligencia de Estados Unidos (Intelligence Community). Sus directores ejecutivos y funcionarios de alto rango son matemáticos e ingenieros de la NSA (sigla de National Security Agency, la Agencia de Seguridad Nacional de los Estados Unidos), quienes capitalizan las invenciones que crearon para el estado de vigilancia. […] Estados Unidos no es el único culpable.

En los últimos años, la infraestructura de internet en países como Uganda se ha visto enriquecida por la inversión directa china. Se reparten abultados préstamos a cambio de contratos africanos para que compañías chinas construyan la infraestructura de la red troncal que conecte escuelas, ministerios gubernamentales y comunidades al sistema de fibra óptica global. La disyuntiva que

plantea Foucault es culturalmente tan importante que numerosas obras de ficción la han tratado. De hecho, nuestra imagen mental sobre los estados hipervigilantes sin duda está moldeada de acuerdo con ciertas novelas y películas emblemáticas. Por ejemplo, El Proceso, de Franz Kafka (1914), donde un tal Josef K se defiende ante unos acusadores desconocidos acerca de cargos poco claros. También, por supuesto, la famosa 1984, de George Orwell (1948), donde se describe un opresivo Estado vigilantista personificado en el siniestro “Big Brother”. Lo interesante de ambas novelas es que muestran la posibilidad de imaginar este tipo de distopías bastante antes de que existieran las computadoras personales e Internet.

Entre las películas significativas, podemos recordar La Conversación (1974) y La vida de los otros (2006), que tratan fundamentalmente sobre escuchas de audio. Y no dejemos de mencionar La red (1995), Enemigo del Estado (1998) y Minority Report (2002), que sí describen un vigilantismo informático. Ya más cerca en el tiempo se han realizado películas sobre hechos de la vida real como la película "Snowden" (2016) dirigida por Oliver Stone.

La serie Person of Interest también es muy ilustrativa de una vigilancia típica de la era actual. Esto es: 1) deliberada; 2) rutinaria; 3) sistemática y 4) enfocada. Todo esto al servicio de administrar personas y poblaciones, de un modo crecientemente global, descentralizado e imperceptible para el ciudadano común.

Suele decirse que después de los atentados contra las Torres Gemelas en New York la ya existente vigilancia estatal se reforzó y que por eso muchos países, especialmente Estados Unidos, aprobaron leyes que permitían niveles de control e intromisión sin precedentes sobre los ciudadanos. Si bien algo de eso hubo,es posible afirmar que ése y otros atentados no hacen más que justificar lo que es fruto de un proceso histórico asociado con la génesis de la modernidad. Un proceso que comenzó hace aproximadamente 400 años y que culminó con el presente estado de capitalismo informacional.

Por otra parte, varios países de Latinoamérica que nada tienen que ver con las Torres Gemelas también practican el vigilantismo, como lo muestra por ejemplo su uso del tristemente célebre software de la firma italiana Hacking Team o las revelaciones recientes sobre el uso de Software Pegasus en México (2021). A continuación, un muy breve pantallazo sobre la vigilancia estatal en algunos países.

• Argentina

En febrero de 1968, en uso de las atribuciones conferidas por el artículo 5to. del Estatuto de la Revolución Argentina, el entonces presidente de facto Juan Carlos Onganía firmó el aún vigente decreto ley 17.671, "Ley de Identificación, Registro y Clasificación del Potencial Humano Nacional". En ese Decreto Ley se estructura la madre de todos los debates sobre privacidad y vigilancia estatal en Argentina.

El Registro Nacional de las personas ejercerá la inscripción, identificación de las personas, el registro de sus antecedentes de mayor importancia desde el nacimiento y a través de las distintas etapas de la vida, que se deben mantener actualizados, la clasificación y procesamiento de la información relacionada con ese "potencial humano" (sic), con vistas a satisfacer las siguientes exigencias: proporcionar al gobierno nacional las bases de información que permitan fijar la política demográfica que más convenga a los intereses de la Nación, poner a disposición de los organismos del Estado y entes particulares que lo soliciten los elementos de juicio necesarios para realizar una adecuada administración del potencial humano, posibilitando su participación activa en los planes de defensa y de desarrollo de la Nación, la expedición de documentos nacionales de

identidad, con carácter exclusivo, así como todos los informes, certificados o testimonios previstos, otorgados en base a la identificación dactiloscópica, entre otras funciones.

El Estado autoritario de la Revolución Argentina sentó así las bases de una política de administración del potencial humano nacional, en esos términos. El decreto 17.671 todavía está vigente y es el marco jurídico de una de las instituciones clave de la burocracia argentina, el Renaper. Argentina es uno de los países del mundo que tiene a toda su población catalogada, identificada con un Documento Nacional de Identidad y una base de datos que comenzó con la huella dactilar, la fotografía y continuó con el rostro y otros rasgos de identificación biométrica.

Desde 2011 Argentina cuenta con el SINTyS , o Sistema de Identificación Nacional Tributario y Social, dependiente del Ministerio de Desarrollo Social. Es una gigantesca central de datos con domicilios y datos laborales, entre otros. Por ejemplo, sabe quién es jubilado o pensionado, quién tiene seguro de desempleo o un plan social; la situación de cada uno en el sistema de salud, quién estudia y dónde, quién vive en una vivienda social; quién tiene auto, inmuebles o embarcaciones, quién es deudor financiero, quién debe impuestos y quién paga servicios públicos subsidiados. En este sistema se centralizan 1695 bases de datos de más de 380 organismos nacionales, provinciales y municipales. Los datos se refieren a unos 40 millones de personas físicas y más de 1,2 millones de personas jurídicas.

Otra causa de preocupación es el Sistema Federal de Identificación Biométrica para la Seguridad (SIBIOS), alimentado por fotografías, huellas dactilares y otros datos de casi toda la población.

Además, en Argentina hay un documento nacional de identidad obligatorio biométrico. Y para registrar una tarjeta de transporte público (SUBE) se solicitan los datos personales, lo que permite individualizar todos los movimientos de alguien. También hay proyectos de registro obligatorio de ADN para toda la población, aun no concretados.

Todo esto hizo a Julian Assange decir que Argentina tiene "el régimen de vigilancia más agresivo de todos los Estados latinoamericanos de tamaño mediano".
El país también fue cuestionado desde finales de 2011 cuando organizaciones sociales y sindicales denunciaron ante la Justicia la existencia de un sistema de espionaje, conocido como "Proyecto X", creado por la Gendarmería Nacional en 2002 con el fin de recabar información sobre ese tipo de activistas. Todo esto en el marco de la polémica Ley Antiterrorista vigente, tan abierta en su tipo penal que podría encuadrar numerosas conductas genéricas.

Hay que decir que, además de la Argentina, varios países más ya adoptaron o están por adoptar pasaportes biométricos y/o con chips, incluyendo a Brasil, Chile, Guyana Francesa, Paraguay, República Dominicana y Venezuela. Venezuela y Brasil también tienen entre sus políticas controversiales el uso del voto electrónico que, según muchos especialistas, no garantiza el secreto del sufragio. En la Argentina también hay mucha presión por implementarlo y ya se lo ha hecho en algunos distritos. En 2015 se votó en la Ciudad Autónoma de Buenos Aires con un sistema carente de suficientes resguardos para la seguridad del secreto del voto. En 2016, un proyecto de ley de reforma del sistema electoral a nivel nacional logró media sanción en la Cámara de Diputados.

Con el correr de los años se produjeron notables incorporaciones de tecnologías de uso público que contrastan con las garantías de protección de datos personales. La incorporación del DNI digital, la aplicación Mi Argentina y la integracioń de diversas aplicaciones en el campo de la administración pública suponen una situación sería de vulnerabilidad de los datos pesonales de la ciudadanía.

En la Ciudad Autónoma de Buenos Aires se incorporaron tecnologías de vigilancia del espacio público basadas en reconocimiento facil que generaron la reacción de los diversos grupos de activistas vinculados con la defensa de derechos humanos. El propio relator de Naciones Unidas para el Derecho a la Privacidad, Joe Cannataci advirtió que no se podía desplegar ese tipo de tecnología sin un análisis de impacto sobre Derechos Humanos.

Otro tanto podemos afirmar del descontrol en materia de servicios de inteligencia, el rol de la Agencia Federal de Inteligencia, uno de los organismos que requiere una urgente modificación estructural y un nuevo y riguroso marco normativo.

La pandemia de Covid 19 aportó lo suyo en relación a la vigilancia pública. Con el argumento de la vigilancia epidemiológica se libraron permisos de circulación y se tornó mandatoria la instalación de diversas aplicaciones para hacer seguimiento de casos, entre otras funciones. ¿Qué pasará con esos datos cuando dejen de cumplir su función?

Toda tecnología que pueda ser usada para la vigilancia será efectivamente usada para la vigilancia, expresa Shoshana Zubbof. La vigilancia estatal es uno de los más grandes y serios problemas de las democracias actuales.

El factor global

Como dicen Bigo, Bauman, Lyon et al.:
"Al parecer, los diferentes servicios a cargo de su propia seguridad nacional, al perseguir la reunión e intercambio de información, solicitan a otros servicios de seguridad la realización de algunas de sus tareas, traspasando las limitaciones de la inteligencia exterior al usar un "supermercado de la privacidad del ciudadano" donde se intercambia con otro servicio la vigilancia sobre los propios ciudadanos. De esta manera, lo que es nacional y lo que es extranjero se vuelve bastante irrelevante para las operaciones organizadas de modo transnacional."

El efecto de esta situación es que, cuando tus datos son utilizados por organismos de tu país, te amparan algunos derechos. Pero cuando los mismos datos los utiliza otro Estado, ¿a quién le vas a reclamar?

Por otra parte, dicen los autores, la vigilancia no está en las manos de entidades tan abstractas como "los estados", sino en las de una elite de profesionales de la seguridad que constituyen más lazos comunitarios entre sí que con los gobiernos que les dan su mandato. De hecho, no es raro que tengan agendas propias y conflictos de intereses. Por eso es que los tres procesos que caracterizan la vigilancia masiva actual son: transnacionalización, digitalización y privatización.
Está claro que esta situación diluye el concepto mismo de democracia y unos cuantos derechos civiles. Por eso se puede aplicar lo que el filósofo Giorgio Agamben denominó "un espacio vacío de ley", donde todas las determinaciones legales están permanentemente en suspenso y la misma distinción entre público y privado pierde sentido (Agamben, 2003). De este modo, la estructura política fundamental es un "estado de excepción permanente" donde lo que debería ser una anomalía se transforma en norma.

Principales metodologías para la vigilancia estatal

Muchos de los métodos de la vigilancia corporativa aplican también a la estatal. En todo caso, son tecnologías que obedecen a un "ensamblaje de vigilancia", porque habitualmente los estados acuden a las empresas para concretar sus políticas por medio de dispositivos específicos, como lo han mostrado los Spy Files publicados por Wikileaks. Por ejemplo:

• Cada vez que alguien usa Internet, como hemos visto, deja huellas que pueden ser utilizadas por gobiernos, así como por empresas, con diversos fines. Lo crucial es que los intercambios comunicativos que hacemos con otros, en el ámbito digital, no son efímeros. Y dichos intercambios no solo son registrados, sino también analizados en búsqueda de patrones "sospechosos".
• Los teléfonos móviles dan información sobre la ubicación del usuario, lo cual puede usarse como evidencia criminal.
• Dispositivos llamados "Stingrays" simulan ser antenas de telefonía móvil y pueden interceptar comunicaciones. Cuando lo hacen, no recolectan solamente las de la persona sospechada, sino la de varias más al azar.
• En todas partes hay cámaras de vigilancia. Las usan no solamente las fuerzas de seguridad, sino también la vigilancia privada de edificios y tiendas. Algunas cámaras incluso registran conversaciones.
• Existen sistemas que escanean automáticamente chapas identificatorias de los autos, y las cotejan contra una base de sospechosos. Lo mismo puede hacerse con rostros.
• Cada vez es más frecuente en muchos países que se tomen muestras de ADN a todo detenido, y no se las elimina si luego se verifica que no tenía responsabilidad en ningún hecho criminal.
• También crece la presión por tomar muestras de ADN compulsivas a toda la población de undistrito o país, para facilitar la investigación de delitos que se cometerán en el futuro pero aún no se han cometido.
• Aunque en unos pocos países no es obligatorio tener ni portar un carnet de identidad con datos biométricos ni chips, es cada vez más frecuente.
• Los pasajeros que viajan a destinos internacionales son sometidos a toda clase de escrutinios, incluso escaneos de cuerpo completo y, por supuesto, huellas digitales y escaneo de retina.
• Los metadatos de nuestras comunicaciones telefónicas y nuestro uso de Internet está siendo monitoreado por varios servicios de inteligencia, que pueden o no ser de nuestro propio país.
• Los registros de consumos mediante tarjetas de crédito y débito son analizados por las oficinas impositivas, y no siempre con fines legítimos de comprobar si la persona está evadiendo obligaciones.
• Las etiquetas RFID son insertadas en cada vez más objetos, incluso hay países que las han aprobado para su implantación en el cuerpo humano con fines de identificación.
• Se implementa obligatoriamente la historia clínica digital, sin suficientes resguardos por la privacidad y quebrando la confidencialidad entre médico y paciente. Así, si alguien figura como consumidor de psicotrópicos recetados, no sería raro que eso salte a la luz pública "por un lamentable error" o como "filtración anónima" en el caso de que proteste contra su gobierno o decida tener cualquier actividad política.
• Se están popularizando los "drones" o vehículos no tripulados que sobrevuelan y filman multitudes, poblaciones, construcciones e individuos.
• Hay dispositivos que permiten ver huellas térmicas a través de paredes, con lo cual se elimina la necesidad de conseguir una orden para ver lo que hay dentro de un domicilio.

El caso específico de la biometría

En lugar de identificar a una persona por algo que tiene (como una tarjeta de identidad), algo que recuerda (palabra clave o PIN) o algo que hace (como una firma), la biometría la identifica por algo que es. Se basa en la recolección de ciertos identificadores biológicos que caracterizan a los individuos y suele usarse para las tarjetas de identificación obligatorias (inteligentes o no). Para fines de vigilancia, se prefieren aquellos rasgos que no cambien a lo largo de la vida de las personas y puedan identificarla con alto grado de univocidad. Los ejemplos más comunes son las huellas digitales y el ADN. Pero, hoy en día, se utilizan incluso escáneres que reconocen las proporciones faciales de alguien y las combinan con imágenes térmicas para incrementar la probabilidad de una identificación positiva. Indicadores de los patrones de movimiento, la estructura retinal, la escritura y la voz también son de tipo biométrico.

Los indicadores biométricos pueden y suelen usarse en combinación con otro tipo de indicadores. Algunos reconocimientos biométricos podrían hacerse incluso sin que la persona los perciba. Por ejemplo, puede haber sistemas de reconocimiento facial que vayan analizando rostros en la vía pública o en protestas sociales callejeras, contrastándolas contra una base de fotografías y nombres.

De todos modos, se debe subrayar que ninguna identificación biométrica permite un cien por cien de exactitud, aunque sí puede hacerlo con una muy alta probabilidad, según cuál sea el elemento biométrico utilizado. La huella digital es uno de los más exactos y es usual el empleo de un AFIS (Automatic Fingerprint Identification System) para recuperar cualquier imagen escaneada de una impresión dactilar de modo rápido y eficaz.

Un sistema cada vez más popular es la identificación por medio de la geometría de la mano y de los dedos. Un escáner registra noventa medidas distintas de la misma y genera un patrón digital de nueve bytes de la imagen tridimensional de su contorno. Luego se transfiere la información a una base de datos para ubicar a la persona que está siendo identificada. A este patrón puede agregársele un PIN secreto para mayor seguridad. Este tipo de dispositivos no registra huellas digitales, sino solamente rasgos morfológicos distintivos de la mano de cada individuo. En consecuencia, podría haber dos personas con el mismo patrón de la mano. Este hecho puede conducir a que, en ocasiones, el sistema rechace o acepte por error el ingreso o egreso de una persona a un lugar. Es lo que se llama “falsa aceptación” o “falso rechazo”.

El biométrico que más preocupación causa, por su potencial discriminatorio, es el monitoreo y almacenamiento de datos relativos al ADN, ya que tecnologías del tipo PCR (reacción en cadena de la polimerasa) permiten detectar genes “fallados”, que codifican proteínas mal construidas, mucho tiempo antes de que den lugar a la enfermedad que supuestamente dicha falla pudiese ocasionar. Por otra parte, el análisis del ácido desoxirribonucleico (ARN) permite distinguir a una persona en siete mil millones. Para eso alcanza una muestra del orden de la milmillonésima parte de un gramo. Los restos de saliva en una estampilla, por ejemplo, son suficientes para identificar a un individuo. Incluso se llega a clasificar el ARN de criminales registrados según el tipo de crimen que cometieron, en un intento de predictibilidad. Es decir, de discriminar a priori a aquellos en cuyos genes se suponga el origen de una determinada tendencia delictiva, aunque jamás se haya hecho manifiesta. Para saber más sobre la biometría y sus riesgos, recomendamos estos informes de la Asociación por los Derechos Civiles, de Argentina.

La recolección masiva de datos como parte del diseño de políticas públicas, tensiones entre proporcionalidad y fines perseguidos

Lo que uno esperaría en democracia es que las políticas públicas se debatan en las instituciones previstas por la ley, a la vista de todos y legitimadas por mayorías. Sin embargo, en la práctica, el vigilantismo estatal implica aplicar políticas públicas que muchas veces se dan por hechas, o llegan por simples vías administrativas, o sin suficiente debate. Esto significa que los ciudadanos serán clasificados en diferentes categorías, accederán o no a determinados beneficios o serán etiquetados como sospechosos sin que las vías de participación democrática de la ciudadanía hayan tenido intervención.

Por otra parte, en algunos casos la masa de información que circula en los estados acerca de los ciudadanos adquiere “vida propia”. No solamente el público no tiene idea de qué agencias gubernamentales la comparten entre sí, con qué reglas y en qué circunstancias, sino que la misma burocracia vigilantista termina operando con relativa autonomía, sin que los gobernantes elegidos por el voto necesariamente estén en el detalle de cómo funciona. Así, es posible que ningún funcionario tenga que enfrentarse a la desagradable tarea de discriminar a alguien por lo que “los

datos” dicen de él o ella: es un sistema impersonal quien lo hace. El vigilantismo desplaza así la responsabilidad por las políticas públicas desde las personas hacia las cosas. Además, la lógica vigilantista difiere en la de las viejas burocracias de otras eras en que su objetivo es cada vez menos la inclusión, sino la exclusión de aquellos considerados “indeseables”.

En una democracia no es aceptable que una limitación a los derechos humanos se produzca de este modo casi “inconsciente” y sin responsabilidades claras. Al contrario, si este tipo de limitaciones se produce deben ser de forma necesaria, proporcional, y con el fin de alcanzar un conjunto de fines permitidos. Dichos límites deben ser establecidos por ley, y no deben ser arbitrarios. Recordemos brevemente qué significan estos términos:

- Necesidad: si un objetivo de interés general perseguido por la vigilancia puede ser alcanzado de un modo menos intrusivo, entonces debe preferirse este último.
- Adecuación: no es suficiente que el método elegido “pueda” alcanzar el objetivo declarado. Se debe mostrar que realmente existe la posibilidad de que lo haga.
- Proporcionalidad: la vigilancia es esencialmente intrusiva y así debe reconocerse en forma explícita. Así que solo es legítima si hay garantías (por ejemplo, autorización judicial en el marco de una causa concreta, no “por las dudas” a todo el mundo) y si la intrusión que se piensa emprender es proporcional al bien que se desea proteger (por ejemplo, no se pueden poner cámaras de vigilancia en un baño por las dudas a alguien le diera por hurtar más papel sanitario que el que precise).

Fundación
Vía Libre