

Módulo 4: Vigilancia estatal

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

Como hemos analizado en el módulo anterior, las corporaciones de Internet son fundamentales para el vigilantismo pero, como veremos a continuación, son solo una parte de lo que Foucault llamaría un “régimen de gubernamentalidad” 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 armadas o 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 vigilante 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.

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, mi opinión personal es 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](#).

A continuación, un muy breve pantallazo sobre la vigilancia estatal en algunos países. Disculpen que le dedique a continuación un poco más de espacio a Argentina pero, como ciudadana del país, es el caso que más conozco:

- **Argentina**

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.

- **México**

Durante 2014, los operadores de telefonía móvil de este país registraron [más de 55.000 solicitudes](#) de las autoridades para obtener información sobre llamadas de ciudadanos, sus mensajes y datos de localización, casi un 25 por ciento más que en el 2013. El año pasado, agencias federales y estatales también gastaron más que cualquier otro país en el software de espionaje de la empresa italiana Hacking Team, según documentos filtrados recientemente. Sólo tres por ciento de las peticiones de vigilancia electrónica en México el año pasado fueron aprobadas por un juez, mientras que la autorización para el resto fue dejada en manos de las empresas de telecomunicaciones.

- **China**

El "[Gran Cortafuegos](#)" de censura y vigilancia china es tan paradigmático que, antes de las revelaciones de Snowden, Estados Unidos la ponía en primer lugar en la lista de lo que no hay que hacer. Ahora ya sabemos que en todas partes cuecen habas, lo cual no implica que China siga siendo un fuerte caso de vigilantismo y censura. Por ejemplo, [de acuerdo con un nuevo informe realizado por los Estudios en Educación Ideológica](#), una publicación que difunde el mismo Ministerio de

Educación chino, se estarían usando técnicas de Big Data para crear “una base de datos de ideología política” alimentada con información de los registros de bibliotecas, encuestas, reacciones en redes sociales y otras fuentes.

- **Rusia *et al***

Rusia también es un país donde la datavigilancia, sumada a la censura, preocupa al activismo mundial por los derechos digitales. Entre otras cosas, tiene un “sistema predictivo y de control” para vigilar las acciones relacionadas con marchas y protestas prohibidas dentro de las redes sociales. Además, allí los proveedores de Internet [están obligados](#) a vigilar y registrar todo el tráfico, incluidas las direcciones IP, números de teléfono y nombres de usuario. No obstante, la retención de datos es una práctica creciente en otros países, como lo muestra la infografía de [esta nota](#) acerca de la normativa al respecto en América Latina y Europa. [España](#) y otros estados también monitorean las redes a la pesca de posibles delincuentes o terroristas.

- **Reino Unido**

Además de ser uno de los “Cinco Ojos”, recientemente este país protagonizó una polémica por un nuevo proyecto de ley de vigilancia de las comunicaciones que no solo establecerá un registro de tráfico sino que también permitirá al Estado [introducir software malicioso](#) en dispositivos como ordenadores y teléfonos móviles para recopilar el mayor número de datos posibles del usuario.

- **Francia**

[Una nueva legislación](#) permite a los servicios secretos contar con una amplia cobertura legal en la interceptación de comunicaciones, acceso a las bases de datos y a las redes. También otorga más facilidades para obligar a las compañías de Internet a entregar información al Estado. Dichas empresas deben comunicar a los servicios secretos las actividades de usuarios sospechosos de terrorismo o de espionaje. Los agentes de seguridad pueden interceptar ordenadores y teléfonos móviles, rastrear localizaciones y espiar correos electrónicos y otras comunicaciones sin necesidad de control judicial. Todo esto no sirvió para prevenir los atentados recientes en París.

- **Perú**

El 27 de julio de 2015 se promulgó la conocida como [Ley Stalker](#), que habilita a la policía a acceder en tiempo real y sin orden judicial a la información de geolocalización de cualquier dispositivo asociado a una línea de telefonía móvil, y crea la obligación de las empresas de telecomunicación de conservar los datos de tráfico de sus usuarios por un período de tres años.

- **Chile**

[Este artículo](#) de Carlos Lara, de Derechos Digitales, dice que “Chile se destaca entre todos los demás países de América Latina (exceptuando a El Salvador) porque carece de protección constitucional de los datos personales, y no cuenta con canales legales adecuados para enfrentar diversas violaciones a las leyes de protección de datos. Y si bien las actividades relacionadas a la protección de información personal parecen estar cambiando en las agencias estatales (como ocurre en todo el mundo), ha habido situaciones de violación a los derechos a la privacidad sin que éstas

hayan impactado demasiado en las políticas ni en la legislación”.

- **Centroamérica**

La Fundación Acceso [publicó recientemente una investigación](#) sobre los marcos legales existentes en cuatro países de la región, para la protección de la privacidad digital de las personas defensoras de derechos humanos, mediante la cual se determinó, que a pesar de existir las normativas, este sector es vulnerable, existe una cultura del secreto alrededor de los temas de vigilancia y se encuentra expuesto a la violación de su privacidad.

- **Colombia**

Para un panorama completo del estado del vigilantismo en este país, te recomiendo leer el informe de la ONG británica Privacy International [Un estado en la sombra: vigilancia y orden público en Colombia](#). Allí se ilustra cómo diversos organismos estatales están creando sus propios sistemas de vigilancia sin escrutinio suficiente ni base legal. Asimismo, en el informe [Demanda y oferta: la industria de la vigilancia al descubierto](#), expone a las empresas que han construido sistemas de vigilancia altamente invasivos y que han sido utilizados por el gobierno colombiano. También te recomiendo [este video](#) del II Simposio de LAVITS donde Katitza Rodríguez, de Electronic Frontier Foundation, revela cómo el gobierno colombiano, así como otros de la región, solicita ayuda a organismos de Estados Unidos para obtener datos de sus propios ciudadanos (minuto 1:11:00).

El factor global

Lo que dice Katitza en ese video es relevante también para subrayar el carácter global de la vigilancia masiva, que hace equivocado analizarla solamente país por país. Como dicen Bigo, Bauman, Lyon et al. [en el artículo que ya te mencioné varias veces](#) en los otros módulos:

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.

Referencias

AGAMBEN, G. *État d’Exception – Homo Sacer*. Paris: La Seuil, 2003.

FOUCAULT, M. *História da sexualidade. I – A vontade do saber*. Lisboa: Relógio D’Água Editores, 1994a.

_____. *Dits et écrits – 1976-1979*. Paris: Gallimard, 1994b. Vol. III.

_____. *Vigilar y castigar, Nacimiento de la prisión*. Madrid: Siglo XXI Editores, 2009.

4.2. 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 un

distrito 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.

4.2.1. 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, te recomiendo [estos informes](#) de la Asociación por los Derechos Civiles, de Argentina.

4.3. 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 vigilanista 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 vigilanismo desplaza así la responsabilidad por las políticas públicas desde las personas hacia las cosas. Además, la lógica vigilanista 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).

Para saber más sobre estas cuestiones te recomiendo [este artículo](#) de Katitza Rodríguez.

Y, por supuesto, quiero resaltar que “necesario”, “adecuado” y “proporcionado” son términos que siempre tienen cierto grado de subjetividad, así que mucho dependerá su aplicación de cómo se interpreten y, sobre todo, de quién lleve a cabo dicha interpretación.

4.4. Legalidad y límites

Existen múltiples instrumentos para intentar poner límites a la vigilancia masiva. Cada uno tiene sus méritos y también sus debilidades.

En primer lugar, están los tratados internacionales de derechos humanos que ya hemos mencionado en otro módulo. Son marcos fundamentales que modelan las legislaciones particulares de muchos países, y esa es su principal fortaleza. Sin embargo, su aplicación concreta en cada geografía depende de cómo se los haya interpretado mediante leyes y reglamentaciones locales.

En segundo lugar tenemos justamente esas leyes y reglamentaciones locales orientadas a controlar la recolección, distribución y procesamiento de información personal. Existen en muchos países y, donde existen, lo habitual es que también haya una autoridad de aplicación que supuestamente supervisa su cumplimiento. Sin embargo, tanto las legislaciones como las autoridades de aplicación en muchos casos han sido acusadas de legitimar la vigilancia, más que regularla. En la Argentina, por ejemplo, la ley de protección de datos parece excelente. Pero tiene inconvenientes que, en la práctica, la hacen casi inútil, como explica [este informe](#) de la Asociación por los Derechos Civiles. Por ejemplo, permite omitir la exigencia de permiso previo del interesado cuando los datos se “recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal”. También habilita a las distintas dependencias del Estado a compartir entre sí datos personales. Con lo cual, sería posible que una de ellas tuviera excelentes prácticas de seguridad y los comparta con otra cuyos procedimientos fueran muy deficientes. Además, el órgano de control del cumplimiento de esta ley depende del Poder Ejecutivo. Con lo cual, no puede sorprender que las 137 inspecciones realizadas entre 2008 y 2012 fueron realizadas a empresas privadas, jamás a una dependencia estatal.

Por otra parte, la mayor parte de las leyes de protección de datos del mundo no se adaptan fácilmente a ciertas prácticas de vigilancia, como el análisis de metadatos.

Tiendo a estar de acuerdo con [Kevin Haggerty](#) cuando dice que:

Los abogados y reguladores dominan las discusiones sobre privacidad y leyes de privacidad. En contraste, yo soy un científico social interesado en los grandes rasgos y lo que nuestra situación actual podría sugerir acerca de mayores tendencias sociales, políticas e históricas. [...] Nunca hubo más leyes sobre privacidad, ni un discurso profesional más rico sobre el tema, ni una red más extensa y dedicada de profesionales de la privacidad. Uno podría entonces anticipar que hay una correspondientemente grande y bien preservada esfera privada. Y el caso es justo lo opuesto. En el curso de muchas décadas la vigilancia se ha expandido e intensificado casi en todas partes, convirtiéndose en una práctica organizacional dominante.

El autor también resalta que, para ser compensado por el daño cuando uno ya ha sido víctima de una violación a su privacidad, hay que ir a la justicia. Pero muchos ciudadanos simplemente no pueden pagar un abogado ni emprender acciones legales. Tampoco uno puede ir entablando una demanda cada vez, por ejemplo, que es filmado por una cámara de vigilancia sin haberlo autorizado. Las dependencias estatales y las corporaciones, en cambio, sí tienen bien aceitados los departamentos legales para defenderse de cualquier demanda que les puedan hacer. El problema de la vigilancia es, por lo tanto, un problema de asimetría de poder.

Otro modo de controlar las violaciones a la privacidad, el preferido de las corporaciones, es la autoregulación. El problema es que implica poner al lobo a cuidar a las ovejas. Es decir, poner a

controlar su propia vigilancia precisamente a quien la está ejerciendo. Privatizar la regulación.

También es posible atenuar los efectos de la vigilancia mediante el uso de tecnologías orientadas a mejorar la privacidad (*Privacy-enhancing Technologies*, o PET). Por ejemplo, encriptar los propios datos a medida que son almacenados o fluyen a lo largo de las redes, usar navegadores como TOR, etc. Sin duda es mejor usar estas tecnologías que no usarlas. Te recomiendo [este sitio en castellano](#) donde podrás aprender bastante sobre ellas. Pero no te ilusiones. Si crees que con este tipo de herramientas estarás a salvo de la vigilancia, quizá hasta te estés convirtiendo en un blanco. Por ejemplo, se sabe que [la NSA considera especialmente sospechosos a quienes pesca usando TOR](#).

Siguiendo con los métodos antivigilancia, en Estados Unidos parece ser que una opción popular es la “autoayuda individual”. Esto es, intentar controlar individualmente lo que uno deja trascender, incluso entablando demandas legales. Puede ser el único método que quede si uno no cuenta con la posibilidad de enfrentar la vigilancia de un modo más institucional, colectivo y político.

En realidad, es preferible en lo posible canalizar el esfuerzo antivigilancia de un modo menos solitario, por ejemplo formando parte de grupos de activismo por los derechos humanos en ámbitos tecnologizados. En general, si no actuamos solos tendremos mejor chance de estar alertas ante nuevas situaciones de preocupación que impliquen mayor vigilantismo, advertir a los medios de comunicación, petitionar a las autoridades y ejercer presión sobre las empresas abusivas. [Aquí](#) podrás encontrar algunas asociaciones de la región que, como la [Fundación Vía Libre](#) en la Argentina, no pierden ocasión de luchar contra la vigilancia masiva. Grupos de tecnólogos, como los de [Riseup](#), y de académicos, como los de la red [LAVITS](#), también convendría que estuvieran en tu “mesa de ayuda”.