Vigilancia y Sociedad

Translated by Abner Roa | May 23, 2023 | Read Time: 21 minutes
Enciclopedia de Teoría Social, 2005.

Por Gary T. Marx

Profesor *e meritus*, MIT

Este artículo ofrece una visión general y una introducción.

Vigilancia tradicional

Un miembro de la delincuencia organizada es condenado a prisión gracias a unas escuchas telefónicas. Se descubre que un miembro de un grupo de protesta es un confidente de la policía. Estos son casos de *vigilancia tradicional*, definida por el diccionario como "observación minuciosa, especialmente de una persona sospechosa".

Sin embargo, la vigilancia va mucho más allá de su asociación popular con la delincuencia y la seguridad nacional. En diversos grados, es una propiedad de cualquier sistema social, desde dos amigos hasta un lugar de trabajo o el gobierno. Pensemos, por ejemplo, en un supervisor que controla la productividad de un empleado; un médico que evalúa la salud de un paciente; un padre que observa a su hijo mientras juega en el parque; o la conductora de un vehículo que circula a gran velocidad a la que se pide que muestre su permiso de conducir. Cada uno de estos casos también implica vigilancia.

Los límites de la información y los concursos se encuentran en todas las sociedades y, más allá, en todos los sistemas vivos. Los seres humanos son curiosos y también tratan de proteger sus fronteras informativas. Para sobrevivir, los individuos y los grupos ejercen la vigilancia y se protegen de ella. La búsqueda de información sobre los demás (ya sea dentro o fuera del propio grupo) es característica de todas las sociedades. Sin embargo, la forma, el contenido y las normas de la vigilancia varían considerablemente: desde recurrir a informadores hasta interceptar señales de humo o tomar fotografías por satélite.

En el siglo XV, la vigilancia religiosa era una forma poderosa y dominante. Incluía la búsqueda de herejes, demonios y brujas, así como la vigilancia más rutinaria de la

conciencia religiosa, los rituales y las normas (por ejemplo, el adulterio y el matrimonio). Las organizaciones religiosas también llevaban registros básicos de nacimientos, matrimonios, bautizos y defunciones.

En el siglo XVI, con la aparición y el crecimiento del embrionario Estado-nación, que tenía tanto nuevas necesidades como una capacidad en desarrollo para recopilar y utilizar información, la vigilancia política adquirió una importancia cada vez mayor en relación con la vigilancia religiosa. A lo largo de los siglos siguientes, se produjo un cambio gradual hacia una sociedad "vigilada" en la que los agentes del Estado y de la economía llegaron a ejercer un control sobre áreas sociales, geográficas y temporales cada vez más amplias. Aparecieron formas como un censo ampliado, registros policiales y de otro tipo, documentos de identidad e inspecciones, que difuminaron la línea entre la vigilancia política directa y una gobernanza o administración neutral (incluso en algunos aspectos) más benigna. Estos formularios se utilizaron para la tributación, el reclutamiento, la aplicación de la ley, el control de fronteras (tanto de inmigración como de emigración) y, más tarde, para determinar la ciudadanía, la elegibilidad para la participación democrática y en la planificación social. En los siglos XIX y XX, con el crecimiento del sistema fabril, las economías nacionales e internacionales, la burocracia y los estados regulados y de bienestar, el contenido de la vigilancia se amplió de nuevo a la recopilación de información personal detallada con el fin de mejorar la productividad y el comercio, proteger la salud pública, determinar la conformidad con un número cada vez mayor de leyes y reglamentos y determinar la elegibilidad para diversos programas de bienestar e intervención como la Seguridad Social y la protección de la infancia. Los usos gubernamentales, a su vez, se han visto complementados (y en cualquier escala cuantitativa probablemente superados) por los usos contemporáneos del sector privado de la vigilancia en el trabajo, en el mercado y en entornos médicos, bancarios y de seguros. El Estado comercial contemporáneo, con su énfasis en el consumo, es inconcebible sin la recopilación masiva de datos personales. Un Estado con credenciales, organizado burocráticamente en torno a la certificación de la identidad, la experiencia y la competencia, depende de la recopilación de información personal. La dependencia de las tecnologías de vigilancia para autenticar la identidad ha aumentado a medida que se han incrementado las interacciones remotas no cara a cara a través de las distancias y las interacciones con extraños. La sociedad urbana moderna contrasta notablemente con las comunidades rurales o de pueblos pequeños, en las que la interacción cara a cara con las personas conocidas era más habitual. Cuando las personas y las organizaciones no conocen la reputación de las personas con las que tratan o no pueden estar seguras de

ello, recurren a la tecnología de vigilancia para aumentar la autenticidad y la responsabilidad.

El microchip y el ordenador son, por supuesto, fundamentales para el desarrollo de la vigilancia y, a su vez, reflejan fuerzas sociales más amplias puestas en marcha con la industrialización. La mayor disponibilidad de información personal es una pequeña parte de la constante expansión del conocimiento que se ha producido en los dos últimos siglos y de la importancia de la información para el funcionamiento de la sociedad contemporánea.

La nueva vigilancia

Las formas tradicionales de vigilancia señaladas en el párrafo inicial contrastan de manera importante con lo que puede denominarse la *nueva vigilancia*, una forma que se hizo cada vez más prominente hacia finales del siglo XX. La nueva vigilancia social puede definirse como "el escrutinio mediante el uso de medios técnicos para extraer o crear datos personales o de grupo, ya sea de individuos o de contextos". Algunos ejemplos son las cámaras de vídeo, el cotejo informático, la elaboración de perfiles y la extracción de datos; el seguimiento laboral, informático y electrónico de la ubicación; los análisis de ADN; las pruebas de detección de drogas; los escáneres cerebrales para detectar mentiras; diversas pruebas autoadministradas y las imágenes térmicas y de otro tipo para revelar lo que hay detrás de paredes y recintos.

El uso de "medios técnicos" para extraer y crear la información implica la capacidad de ir más allá de lo que se ofrece a los sentidos sin ayuda o se informa voluntariamente. Gran parte de la nueva vigilancia implica un proceso automatizado y amplía los sentidos y las capacidades cognitivas mediante el uso de artefactos materiales o software.

El uso del verbo más amplio "escudriñar" en lugar de "observar" en la definición llama la atención sobre el hecho de que las formas contemporáneas a menudo van más allá de la imagen visual para implicar sonido, olor, movimiento, números y palabras. Los ojos contienen la gran mayoría de los receptores sensoriales del cuerpo, y lo visual es una metáfora maestra de los demás sentidos (por ejemplo, decir "veo" para entender). Sin embargo, al ojo, como principal medio de vigilancia directa, se unen o sustituyen cada vez más otros medios. El uso de múltiples sentidos y fuentes de datos es una característica importante de gran parte de la nueva vigilancia.

Tradicionalmente, la vigilancia implicaba la observación minuciosa por parte de una persona, no de una máquina. Pero con las prácticas contemporáneas, la vigilancia puede llevarse a cabo desde lejos, como con las imágenes por satélite o la supervisión remota de las comunicaciones y el trabajo. Tampoco es necesario que sea cercana, como en el caso de la vigilancia detallada, ya que gran parte de la vigilancia inicial consiste en exploraciones superficiales en busca de patrones de interés que posteriormente se perseguirán con mayor detalle. La vigilancia se ha hecho más lejana y más cercana que antes. Se produce con una absorbencia similar a la de una esponja y una especificidad similar a la de un láser.

En una innovación sorprendente, la vigilancia también se aplica a contextos (lugares y espacios geográficos, periodos de tiempo concretos, redes, sistemas y categorías de personas), no sólo a una persona concreta cuya identidad se conoce de antemano. Por ejemplo, la policía puede centrarse en los "puntos calientes" donde se producen con más frecuencia los delitos callejeros o tratar de seguir el rastro del dinero a través de las fronteras para identificar el contrabando de drogas y las redes delictivas relacionadas. Las nuevas tecnologías de vigilancia suelen aplicarse de forma *categórica* (por ejemplo, se somete a todos los empleados a pruebas de detección de drogas o se registra a los viajeros, en lugar de a aquellos de los que hay algún motivo para sospechar).

La vigilancia tradicional implicaba a menudo una relación de no cooperación y una clara distinción entre el objeto de la vigilancia y la persona que la llevaba a cabo. En una época de criados que escuchaban a puerta cerrada, prismáticos e interceptaciones telegráficas, esa separación tenía sentido. Era fácil distinguir al vigilante de la persona que vigilaba. Sin embargo, en el caso de la nueva vigilancia, con sus formas ampliadas de autovigilancia y vigilancia cooperativa, la fácil distinción entre agente y sujeto de la vigilancia puede resultar borrosa.

Al analizar el surgimiento de las formas modernas de control social, el filósofo francés Michele Foucault (1977) se basó en la idea del *Panóptico* del teórico jurídico británico Jeremy Bentham. Bentham propuso un sistema altamente organizado para gestionar grandes poblaciones dentro de estructuras físicamente cerradas, como una prisión, una fábrica o una escuela, en las que las autoridades podían ver todo pero no ser vistas. Desde el punto de vista del control social, esto creaba incertidumbre. Los reclusos nunca podían saber con certeza si estaban siendo vigilados y, por lo tanto, se esperaba que, por interés propio y por costumbre, se autodisciplinaran.

Las advertencias contemporáneas bien publicitadas (por ejemplo, que una zona está bajo videovigilancia) reflejan esta pauta al tratar de crear autocontrol. La disponibilidad de productos que permiten que las personas se autoanalicen (por ejemplo, para medir el nivel de alcohol, la presión sanguínea o el embarazo) también fomenta un espíritu general de autovigilancia.

En otras formas relacionadas, los sujetos pueden cooperar voluntariamente, sometiéndose a vigilancia personal para obtener beneficios para el consumidor (por ejemplo, descuentos para viajeros frecuentes y compradores) o por comodidad (por ejemplo, carriles de vía rápida en autopistas de peaje en los que las tasas se pagan por adelantado).

Los chips implantados que transmiten la identidad y la ubicación, que en un principio se ofrecían para mascotas, ahora también están disponibles para sus dueños (y otras personas). En algunos entornos laborales, las tarjetas inteligentes que llevan los individuos hacen lo mismo, aunque no con el mismo grado de voluntariedad.

La nueva vigilancia, en relación con la vigilancia tradicional, tiene poca visibilidad o es invisible. La manipulación, frente a la coacción directa, ha adquirido mayor protagonismo. La vigilancia puede camuflarse a propósito, como ocurre con una cámara de vídeo oculta en un osito de peluche o en un reloj. O simplemente puede convertirse en algo rutinario y darse por sentado a medida que la recopilación de datos se integra en las actividades cotidianas (por ejemplo, el uso de una tarjeta de crédito para realizar compras transmite automáticamente información sobre el consumo, la hora y la ubicación).

Con la tendencia a la ubicuidad de la informática, la vigilancia y los sensores, en cierto sentido, desaparecen en las actividades y objetos ordinarios: vehículos, teléfonos móviles, aseos, edificios, ropa e incluso cuerpos. El código de barras de los bienes de consumo, relativamente laborioso y que requiere un escaneado manual, pronto podrá ser sustituido por económicos chips informáticos RFID (identificación por radiofrecuencia) integrados que pueden leerse automáticamente desde distancias cortas.

La teledetección de preferencias y comportamientos ofrece muchas ventajas, como el control de la temperatura y la iluminación de una habitación o la reducción de los costes de envío y comercialización, al tiempo que genera registros que pueden utilizarse para la vigilancia.

Puede que sólo haya un breve intervalo entre el descubrimiento de la información y la adopción automática de medidas. El individuo, como sujeto de la recogida y el análisis de datos, también puede convertirse casi simultáneamente en objeto de una intervención, ya se trate de la activación de una alarma o de la concesión (o denegación) de algún tipo de acceso, por ejemplo, para entrar por una puerta, utilizar un ordenador o realizar una compra.

Los nuevos formularios son relativamente baratos por unidad de datos recogida. En comparación con los formularios tradicionales, es fácil combinar datos visuales, auditivos, textuales y numéricos. Es relativamente más fácil organizar, almacenar, recuperar, analizar, enviar y recibir datos. Los datos están disponibles en tiempo real y la recogida de datos puede ser continua y ofrecer información sobre el pasado, el presente y el futuro (como las predicciones estadísticas). Se crean modelos simulados de comportamiento.

La nueva vigilancia es más exhaustiva, intensiva y extensa. La proporción entre lo que el individuo sabe sobre sí mismo y lo que sabe la organización que lo vigila es menor que en el pasado, aunque objetivamente se sepa mucho más.

Una forma de pensar sobre el tema es observar que muchos de los tipos de vigilancia, que antes sólo se encontraban en entornos militares y penitenciarios de alta seguridad, se están filtrando a la sociedad en general. ¿Nos estamos convirtiendo en una *sociedad de máxima seguridad* en la que cada vez se conoce y se controla más nuestro comportamiento?

Seis características de la sociedad de máxima seguridad son 1) una sociedad *de expedientes* en la que los registros informatizados desempeñan un papel fundamental 2) una sociedad *actuarial* en la que las decisiones se toman cada vez más sobre la base de predicciones acerca del comportamiento futuro como resultado de la pertenencia a categorías agregadas y de las comparaciones con éstas 3) una sociedad *sospechosa* en la que todo el mundo es sospechoso 4) una sociedad *de ingeniería* en la que las opciones están cada vez más limitadas y determinadas por el entorno físico y social 5) una sociedad *transparente*, en la que los límites de tiempo, distancia, oscuridad y barreras físicas que tradicionalmente protegían la información se debilitan y 6) una sociedad *autocontrolada*, en la que la autovigilancia desempeña un papel destacado.

Estructuras de vigilancia

Varios tipos de estructuras sociales definen las relaciones de vigilancia. Existe una diferencia importante entre la *vigilancia organizacional* y la *vigilancia no organizacional* ejercida por los individuos.

Las grandes organizaciones han adquirido una importancia cada vez mayor a la hora de influir en las oportunidades vitales de los individuos. Las organizaciones son la fuerza motriz de la recopilación instrumental de datos personales. A nivel organizativo, la vigilancia formal implica a un grupo de interés. La *circunscripción* se utiliza en sentido amplio para referirse a aquellas personas con alguna relación o conexión potencial definida por las normas con la organización, ya se trate de una pertenencia formal o de meras formas de interacción con ella, como alquilar un vídeo o mostrar un pasaporte en una frontera. Todas las organizaciones tienen diversos grados de vigilancia interna y externa.

Los numerosos tipos de vigilancia de empleados o reclusos, como en el caso de las "instituciones totales" estudiadas por Goffman (1961), son ejemplos de la *vigilancia interna que se da en las organizaciones*. Aquí los individuos "pertenecen" a la organización en un doble sentido. Pertenecen como miembros. También, en cierto sentido, son "pertenencias" de la organización, ya que están sometidos directamente a su control de un modo que no lo están los no miembros. A menudo existe una vaga analogía con la propiedad.

La *vigilancia de los grupos externos* implica vigilar a aquellos que mantienen algún tipo de contacto con la organización, por ejemplo, como clientes, pacientes, malhechores o ciudadanos sujetos a las leyes del estado, pero que no "pertenecen" a la organización del mismo modo que un empleado o un recluso. Las empresas de tarjetas de crédito y los bancos, por ejemplo, controlan las transacciones de sus clientes y también buscan clientes potenciales mediante la extracción y combinación de bases de datos. O pensemos en las actividades de control de una agencia gubernamental encargada de hacer cumplir la normativa de salud y seguridad. Una organización de este tipo es responsable de que las categorías de personas sujetas a sus normas las cumplan, aunque no sean miembros de la organización. Las organizaciones no gubernamentales que auditan, conceden calificaciones, licencias y certificaciones tienen la misma función de cumplimiento.

Las organizaciones también se dedican a la *vigilancia externa no institucional* al supervisar su entorno más amplio observando otras organizaciones y tendencias sociales. El campo de la inteligencia empresarial, en rápido crecimiento, busca información sobre competidores, condiciones sociales y tendencias que puedan afectar a una organización. El espionaje industrial es una variante. La planificación también requiere este tipo de datos, aunque suelen tratarse de forma agregada y no de forma identificable personalmente. Con la accesibilidad generalizada (¿democratización?) de las técnicas de vigilancia y la percepción de que son necesarias y están justificadas, ya sea por razones de protección, estratégicas o lascivas, la vigilancia personal, en la que un individuo vigila a otro individuo al margen de una función organizativa, es algo habitual.

Puede tratarse de *vigilancia de relaciones de rol*, como ocurre con los miembros de la familia (padres e hijos, el cónyuge sospechoso) o los amigos que se vigilan mutuamente (por ejemplo, controlando la ubicación a través de un teléfono móvil). O puede tratarse de una *vigilancia de relaciones no relacionadas con el papel*, como ocurre con las actividades flotantes del voyeur, cuya observación no está relacionada con un papel legítimo.

Con respecto a los papeles que se desempeñan, podemos identificar al *agente de vigilancia* (vigilante/observador/buscador) que desea información personal sobre un *sujeto vigilado*. Todas las personas desempeñan ambos papeles, aunque difícilmente de la misma forma o en el mismo grado, y esto cambia dependiendo del contexto y a lo largo del ciclo vital como se ha señalado, los papeles a veces se difuminan.

Dentro de la categoría de agente de vigilancia, la función de vigilancia puede ser fundamental para el papel, como ocurre con la policía, los detectives privados, los espías, los supervisores de trabajo y los reporteros de investigación. O puede ser simplemente una parte *periférica* de una función más amplia cuyos objetivos principales están en otra parte, como en el caso de los cajeros que reciben formación para buscar a los ladrones o los dentistas a los que se anima (o se exige) que informen sobre sospechas de abuso infantil cuando ven moratones en la cara.

Una distinción rica en implicaciones empíricas y éticas es si la situación afecta a quienes participan en la generación y recopilación de datos (*participantes directos*) o si, por el contrario, afecta a *un tercero*. Un tercero puede obtener legítimamente información personal a través de un contrato con el agente de vigilancia (por ejemplo, para realizar pruebas de detección de drogas o para comprar listas de preferencias de consumidores).

O puede obtenerse porque el agente viola la confidencialidad o porque un tercero la obtiene de forma ilegítima (escuchas telefónicas, piratería informática).

La presencia de terceros plantea una importante cuestión de "uso secundario", es decir, ¿pueden utilizarse los datos recogidos para un fin sin el permiso de una persona para fines no relacionados? En Europa, la respuesta suele ser "no", aunque no tanto en Estados Unidos, donde el mercado de la información personal es mucho más libre.

Una distinción importante que a menudo implica diferencias de poder es si la vigilancia es *no recíproca* o *recíproca*. La primera es unidireccional, con datos personales que van del vigilado al vigilante (por ejemplo, empresarios, comerciantes, policía, guardias, profesores, padres). Con la vigilancia recíproca, es bidireccional (por ejemplo, muchos conflictos, concursos y juegos recreativos).

La vigilancia recíproca puede ser *asimétrica* o *simétrica* en cuanto a medios y objetivos. Así, en una sociedad democrática, los ciudadanos y el gobierno participan en formas recíprocas pero distintas de vigilancia mutua. Por ejemplo, los ciudadanos pueden vigilar al gobierno a través de solicitudes de libertad de información, audiencias y reuniones abiertas, y declaraciones de conflictos de intereses y otras declaraciones exigidas como condición para presentarse a las elecciones. Pero los ciudadanos no pueden realizar escuchas telefónicas legales, registros en virtud de la Cuarta Enmienda o ver las declaraciones de la renta de otros. En entornos delimitados, como una manifestación de protesta, puede haber una mayor equivalencia con respecto a determinados medios, por ejemplo, que la policía y los manifestantes se graben mutuamente.

En entornos organizativos, el poder rara vez está en manos de un solo bando, sean cuales sean los contornos de la autoridad formal. Los miembros de menor estatus no carecen de recursos para vigilar a sus superiores y neutralizar o limitar la vigilancia. Las herramientas de videovigilancia y audiovigilancia están ampliamente disponibles. Los empleados pueden documentar el acoso y la discriminación con una grabadora oculta y presentar denuncias que movilicen a otros a escrutar a un superior.

Incluso sin equipos, estar en el lugar de los hechos permite la vigilancia a través de los sentidos. A pesar de las diferencias de poder, a menudo se cree que los mayordomos, sirvientes y valets saben mucho más sobre sus empleadores que a la inversa, aunque esto no esté formalmente definido por la función.

Muchos escenarios de conflicto organizativo muestran una *vigilancia simétrica recíproca* en la que las partes contendientes son aproximadamente equivalentes. Juegos como el póquer implican esto, al igual que algunos acuerdos contractuales y tratados (por ejemplo, la disuasión mutua del control de armas nucleares que se busca mediante la vigilancia recíproca).

Las formas simétricas pueden estar presentes incluso en ausencia de acuerdos formales. Los espías (o más neutralmente) los agentes de inteligencia, ya trabajen para países, empresas o equipos deportivos, suelen ser imágenes especulares unos de otros. Ofensivamente buscan descubrir la información de su oponente y defensivamente proteger la suya propia.

La *vigilancia iniciada por el agente*, que es especialmente característica de los controles de conformidad, como la inspección de un camión o un barco, puede diferenciarse de la vigilancia iniciada por el sujeto, como la presentación del expediente académico, someterse a una prueba de osteoporosis o solicitar un puesto de trabajo que requiere una investigación exhaustiva de los antecedentes. En estos casos, el individuo hace una reclamación o solicita ayuda y, en esencia, invita o al menos acepta el escrutinio.

Con la vigilancia iniciada por un agente, siempre se pretende servir a los objetivos de la organización. Sin embargo, esto no tiene por qué entrar en conflicto con los intereses del sujeto; pensemos, por ejemplo, en la protección que ofrecen los guardias de tráfico en las escuelas o en un servicio bibliotecario eficaz que dependa de unos buenos registros de circulación. La salud pública y la vigilancia médica tienen múltiples objetivos, ya que protegen tanto a la comunidad como al individuo. Las empresas gestionadas eficazmente proporcionan puestos de trabajo y servicios. Proporcionar una cantidad limitada de información personal en un formulario de garantía y hacer que un chip registre el uso de un aparato, como un cortacésped o un vehículo, puede servir a los intereses tanto de los consumidores como de las empresas (por ejemplo, recibir una notificación si el fabricante detecta un problema u ofrecer una prueba del uso correcto si el aparato falla).

La vigilancia iniciada por el sujeto puede reflejar objetivos que sirven a los intereses del iniciador pero que a menudo se solapan con los objetivos de la organización que vigila. Pensemos en algunos servicios de protección que tienen la capacidad de vigilar a distancia el interior de hogares y empresas (vídeo, audio, calor, gas, detección de movimiento) o sistemas sanitarios para vigilar a distancia a ancianos y enfermos (por ejemplo, el envío de una alarma si no se abre el frigorífico de una persona que vive sola

después de 24 horas). Como es más probable que los formularios impliquen el consentimiento informado, son menos controvertidos que la vigilancia de agentes realizada en secreto. Lo que es bueno para la organización también puede ser bueno para el individuo, aunque no siempre es así y, por supuesto, depende del contexto. La comprensión social y la evaluación moral requieren prestar atención a los diversos contextos y objetivos de la vigilancia. Los numerosos contextos y formas de vigilancia impiden cualquier explicación fácil sobre sus causas. Es posible identificar una multiplicidad de causas a distintos niveles, y su importancia relativa varía con el tiempo y entre distintos ámbitos, así como en función del tipo de pregunta que se formule (por ejemplo, el desarrollo de la tecnología, los patrones de difusión, la adopción inicial frente al uso continuado o la desaparición).

Se pueden identificar dos visiones opuestas de la nueva vigilancia. Una, optimista, deposita una gran fe en el poder de la tecnología y acoge con satisfacción una vigilancia cada vez más potente como algo necesario en el mundo actual, en el que se valora tanto la eficacia y en el que existen múltiples peligros y riesgos.

Más pesimista es la opinión Frankensteiniana/Ludita de que la tecnología de la vigilancia es inhumana, destructiva de la libertad e indigna de confianza. Está claro que la vigilancia es una espada con múltiples filos. El tema es fascinante precisamente porque no existen respuestas científicas o morales fáciles.

Existen conflictos de valores y necesidades y consecuencias irónicamente contradictorias que dificultan la adopción de una postura amplia y coherente a favor o en contra de ampliar o restringir la vigilancia. Por ejemplo, valoramos tanto al individuo como a la comunidad. Queremos libertad y orden. Buscamos la privacidad y, a menudo, el anonimato, pero también sabemos que el secreto puede ocultar actos viles y que la visibilidad puede hacer que se rindan cuentas. Pero demasiada visibilidad puede inhibir la experimentación, la creatividad y la asunción de riesgos.

En nuestra sociedad saturada de medios de comunicación, queremos ser vistos y ver, pero también que nos dejen en paz. Valoramos la libertad de expresión y la libertad de prensa, pero no queremos que se difame o acose a nadie. Deseamos honestidad en la comunicación y también civismo y diplomacia. Valoramos el derecho a saber, pero también el derecho a controlar la información personal. El amplio tratamiento universalista que esperan los ciudadanos puede entrar en conflicto con el tratamiento específico impulsado por la eficacia que hace posible la vigilancia personal perfeccionada.

Sean cuales sean las medidas que se adopten, es probable que haya costes, beneficios y compensaciones. En el mejor de los casos, podemos esperar encontrar una brújula en lugar de un mapa y un equilibrio móvil en lugar de un punto fijo para la toma de decisiones.

Las prácticas de vigilancia están determinadas por costumbres, políticas organizativas y leyes que se basan en una serie de principios de valores de fondo. Muchos de ellos se expresaron por primera vez en el Código de Prácticas de Información Justas desarrollado en 1973 para el Departamento de Salud, Educación y Bienestar de Estados Unidos. El Código ofrecía un principio de consentimiento informado en el que la recogida de datos no debe hacerse en secreto; las personas deben ser conscientes de cómo se utilizarán y, en circunstancias ideales, dar su consentimiento; un principio de inspección y corrección en el que las personas tienen derecho a saber qué tipo de información se ha recogido y a ofrecer correcciones y enmiendas; un principio de seguridad de los datos, según el cual la información estará protegida y deberán tomarse precauciones para evitar usos indebidos de los datos; un principio de validez y fiabilidad, según el cual las organizaciones tienen la responsabilidad de garantizar la idoneidad de los medios utilizados y la exactitud de los datos recopilados; y un principio de uso unitario, según el cual la información recopilada para un fin no se utilizará para otro sin consentimiento.

A medida que han ido apareciendo nuevas tecnologías y problemas de vigilancia, han ido surgiendo principios adicionales. Entre ellos se incluyen el principio de minimización, según el cual sólo se recopila la información que es directamente relevante para la tarea en cuestión; el principio de restauración, según el cual, en un contexto de monopolio de las comunicaciones, aquellos que alteren el statu quo de la privacidad deben asumir el coste de restaurarlo; el principio de red de seguridad o equidad, según el cual un umbral mínimo de información debe estar disponible para todos; el principio de inviolabilidad de la persona y la dignidad, según el cual existen límites (incluso con consentimiento) a la mercantilización y la oferta de información personal; el principio de actualidad, según el cual se espera que los datos sean actuales y la información que ya no lo sea debe destruirse; un principio de propiedad conjunta de los datos transaccionales, según el cual ambas partes de una transacción de creación de datos deben estar de acuerdo con cualquier uso posterior de los datos, incluido el reparto de beneficios si procede; un principio de coherencia, según el cual las prácticas de vigilancia se rijan por ideales generales y no por las características específicas de una tecnología; un principio de revisión humana, según el cual una decisión automatizada esté siempre sujeta a la

revisión de una persona; y un principio de reparación, según el cual las personas sometidas a una vigilancia inadecuada dispongan de mecanismos adecuados para descubrir el daño y ser compensadas por él.

Referencias cruzadas

El cuerpo
Desviación
Disneyización
Fordismo/Postfordismo
Foucault
Mirada masculine
Esfera pública
Instituciones totales

Bibliografía

M. Foucault, 1977. Disciplinar y castigar: El nacimiento de la prisión. New York: Pantheon.

E. Goffman, 1961. Asilos: Ensayos sobre la situación social de los enfermos mentales y otros reclusos. Garden City, NY: Anchor Books.

Sugerencias de lecturas complementarias

Allen, A. 2003. Responsabilidad por la vida privada. Lanham, MD: Rowman y Littlefield.

Bennett, C. y Grant, R. (ed) 1999. Visiones de la intimidad. Toronto: Prensa de la Universidad de Toronto.

Brinn, D. 1999. La sociedad transparente. Nueva York: Perseus.

Ericson, R., y Haggerty, K. La vigilancia de la sociedad del riesgo. Toronto: Prensa de la Universidad de Toronto.

Lyon, D. 2001. El Ojo Electrónico: El auge de la sociedad de la vigilancia. Polity/Blackwell.

Marx, G. 2004. Ventanas al alma: vigilancia y sociedad en la era de la alta tecnología. Chicago: Prensa de la Universidad de Chicago.

Marguilis, S.T. (ed.) 2003. "Perspectivas contemporáneas sobre la privacidad: Sociales, Psicológicas y Políticas" Revista de Temas Sociales, Vol. 59, nº 1.

Regan, P. 1995. Legislando la privacidad: Tecnología, valores sociales y políticas públicas. Chapel Hill: Prensa de la Universidad de Carolina del Norte.

Staples, W. 2000. La vigilancia cotidiana: Vigilancia y visibilidad en la vida posmoderna. Lanham, MD: Rowan and Littlefield.

Original article: http://web.mit.edu/gtmarx/www/surandsoc.html