LA VIGILANCIA COTIDIANA

Información personal y clasificaciones sociales

DAVID LYON*
TRADUCCIÓN DE HÉCTOR GUZMÁN

La vigilancia con medios electrónicos es una manera de gobernar cada vez más significativa en las llamadas sociedades basadas en el conocimiento o sociedades de la información. Como dice Rose, "la vigilancia está 'integrada al diseño' de los flujos de la vida cotidiana".[1] Las rutinas diarias están sujetas a infinidad de formas de revisión, observación, registro y análisis, hasta el punto de que con frecuencia suponemos que dejamos marcas y rastros dondequiera que estemos y hagamos lo que sea. Pero tales marcas y rastros, por justificados que estén, no son inocentes. Vistos en su conjunto, se localizan dentro de una red de relaciones que nos dan servicios, nos sitúan y ayudan a organizar y poner en orden nuestras vidas sociales.

La vigilancia contribuye cada vez más a la reproducción y el reforzamiento de las divisiones sociales. En este contexto, la vigilancia es una atención enfocada en los detalles personales, con miras a ejercer una influencia sobre o manejar los objetos de los datos, o "sujetos de datos",[2] como se les llama a veces. Aunque la palabra vigilancia frecuentemente tiene connotaciones de amenaza, involucra procesos ambiguos que no deben considerarse sólo con una visión negativa. Gran parte de la

* Profesor de sociología y director del Surveillance Project en la Universidad Queen's de Toronto, Canadá.

comodidad, eficiencia y seguridad cotidianas dependen de la vigilancia. Es más, esto sucede en un mundo en el que otros tipos de "visibilidad mediada"[3] —sobre todo a través de la televisión, pero también con el uso de cámaras que transmiten por la Internet (*webcams*) y otros medios— están disponibles y tienen gran variedad de efectos. La vigilancia es sólo un aspecto de este mundo mediado. También muestra una cara suave y otra dura, entre las que debe distinguirse. Sin embargo, la vigilancia lleva a formular preguntas acerca del poder, la ciudadanía y el desarrollo tecnológico, así como de la política, la reglamentación y la resistencia de la información.

En las siguientes páginas se ofrece un argumento sencillo y directo acerca de la vigilancia cotidiana, que sin embargo entra en conflicto, en algunos aspectos significativos, con otros tratamientos de los mismos temas. Alego, por ejemplo, que el auge de la vigilancia rutinizada y sistemática tiene orígenes más bien mundanos que en primera instancia no se deberían ver como socialmente siniestros. Aquí la vigilancia es vista como una respuesta al "cuerpo que desaparece" de las relaciones sociales integradoras, activada por los medios modernos de comunicación y el manejo de la información. Pero los resultados de este proceso no carecen de consecuencias en lo que concierne al orden y el control sociales. El auge de infraestructura invisible de información que facilita la clasificación y el procesamiento de datos personales y la porosidad cada vez mayor de sus sitios de almacenamiento generan preguntas distintas acerca de la vigilancia cotidiana, las cuales demandan respuestas críticas que vayan más allá de los discursos convencionales de la intimidad que con tanta frecuencia salen a relucir como contrapuntos para la vigilancia.

¿CÓMO SE VOLVIÓ TAN IMPORTANTE LA VIGILANCIA?

Durante la mayor parte de la historia la interacción social predominante ha sido cara a cara. Digo "ha sido" y no "fue" para hacer hincapié en que este tipo de relación sigue siendo importante. Pero la comunicación que se da en presencia de una u otras personas, en ciertos locales, ha sido complementada con varias formas de comunicación que no requieren la copresencia y que se difunden a través del espacio. Es un rasgo clave de la modernidad que al utilizar nuevos medios de comunicación la gente puede interactuar e incluso permanecer en relaciones integradas con otros aunque estén separados por la distancia. Se han desarrollado nuevas formas de interacción como resultado del estiramiento de las relaciones por el espacio y, en cierta forma, del tiempo. Las nuevas tecnologías están implicadas en ellas porque las hacen posibles. Las formas de la relación no son causadas por las nuevas tecnologías —que con frecuencia tienen usos y efectos diferentes de los que buscaban sus productores— pero sí mediadas por ellas. Destaca, por ejemplo, que ni el teléfono ni la Internet se concibieron como medios para ayudar a las personas a charlar entre ellas sino que es el uso que se les ha dado.[4] Durante los últimos dos siglos han surgido formas de interacción mediada con una reciprocidad mucho menos obvia que la de las llamadas telefónicas o las conversaciones por correo electrónico. Se puede pensar en los medios masivos, donde los mensajes pueden ser en gran medida unidireccionales pero en los que las personas están unidas en la comunicación y el intercambio simbólico. Ahora los programas con teléfono abierto en la radio y las respuestas por correo electrónico a los programas de televisión o los artículos del periódico aumentan las posibilidades dialógicas de estos medios.

Menciono esta variedad de nuevos tipos de relaciones mediadas para indicar que la vigilancia es sólo una entre muchas formas de comunicación que han surgido al tiempo que a las relaciones de copresencia cara a cara se han añadido tantas otras.[5] Entonces, ¿qué tiene de especial la vigilancia? Sugiero que a medida que las nuevas tecnologías han ido permitiendo hacer más y más cosas a distancia se buscaron algunas compensaciones a la cara que se desvanece, el cuerpo que desaparece. Antes las compensaciones adecuadas incluían una firma o un sello en una carta para autenticar su origen personal, pero en los cada vez más complejos escenarios sociales de la modernidad se buscaron otras muestras de confianza que compensaran la falta de pistas y señales visuales y corporales, como apretones de mano o contacto ocular. Desde luego que la búsqueda de muestras de confianza se dio en instituciones poderosas y en contextos informales, lo que hace necesario un análisis crítico.

Al llegar el siglo xx no sólo se requería el pasaporte o los papeles nacionales de identificación sino también otras formas de evidencia documental para fines administrativos y comerciales.[6] Para identificación en la escuela, el lugar de trabajo o la admisión en ciertos sitios, para retirar dinero de un banco o pagar compras se requerían muestras de confianza, de valía, de autenticidad. Hoy nuestras carteras y bolsos están llenos de tarjetas de crédito, membresía, teléfono, seguro social, biblioteca, salud, clubes de comprador frecuente y licencias de manejo, que pueden utilizarse cuando no hay otro cuerpo presente para la transacción —por ejemplo en un cajero electrónico— o la otra parte es un completo desconocido que necesita algún tipo de validación para que el intercambio se dé.

El cuerpo ha desaparecido de las relaciones a un ritmo constante pero la comunicación sigue, a distancia, mediada de manera aplastante por los medios electrónicos. Desde el punto de vista de la organización o dependencia que emite la franja magnética, el código de barras o el número de identificación personal (NIP), verificar la inclusión o la identidad es un medio para clasificar y categorizar a los sujetos de datos. ¿Y qué sucede si se mira desde el otro lado? Los datos personales pueden partir —con conocimiento o sin él— de aquellos a quienes se refieren y ser comunicados a otros (el banco, el departamento de beneficencia, la línea aérea) que se interesan en ellos. Es probable que estos datos sean también la base de la comunicación con los sujetos de datos pero, más allá de esto, con frecuencia se combinan de nuevas maneras y se comunican entre máquinas mucho más que con sujetos de datos. Estos últimos desconocen mucho de lo que sucede con esos datos a medida que se procesan, aunque pueden adivinar una parte cuando una factura de peaje de caminos, una publicidad personalizada o el correo electrónico chatarra (*spam*) aparece en el buzón o en la pantalla.

Abundan las paradojas. La intimidad, que con tanta frecuencia se percibe en peligro a causa de estos desarrollos, de igual manera se puede considerar un generador clave de la vigilancia. A medida que surgían los usos más anónimos de la moderna "sociedad de desconocidos" y se daba más valor a la intimidad, también crecía la necesidad de presentar pruebas de confianza para mantener la integridad de las relaciones entre esos desconocidos.[7] Mientras que la persona conocida a escala local, con un cuerpo, se perdía de vista en la trama de las relaciones sociales, crecía la importancia de las credenciales, la identificación y otras evidencias documentales. La otra paradoja, como ya lo insinué, es que el mismo proceso muestra facetas muy diferentes. Los medios para mantener la confianza entre los desconocidos sirven al mismo tiempo para llevar un registro de los detalles de la vida cotidiana. La intimidad produce vigilancia, la que, se dice, amenaza a la intimidad.

Pero no sólo a la intimidad. Conforme se volvió un componente central, constitutivo de la modernidad, la vigilancia también se volvió cada vez más un mecanismo de ordenamiento social que crece a paso firme. Esto sucedió cuando más y más organizaciones burocráticas realizaron actividades de vigilancia para lograr la máxima eficiencia y eficacia. Llevar un registro es crucial para asegurar la eficiencia de una organización, como lo demostró Max Weber de manera clásica,[8] pero ello requiere de medios cada vez más sofisticados de clasificación y categorización que se alimentan de los datos de la vigilancia y estimulan la demanda de ellos en las organizaciones. Medios tan comunes como el llenado de formularios muestran cómo funciona este proceso porque, como dicen Brown y Duguid, "Los formularios son el medio crucial por el que una organización mete al mundo heterogéneo en línea con sus procesos".[9] Aun con su aparente exactitud, tiene muchas improvisaciones para cerrar brechas y hacer que las realidades sociales concuerden con el proceso, sobre todo en categorías residuales de lo "otro". Incluso en el trabajo policiaco, donde sería de esperar definiciones cerradas, pueden usarse categorías elásticas, como "conducta molesta", para crear perfiles formulistas de las "zonas calientes" en ciudades como Toronto.[10]

LA VIGILANCIA DEPENDE de infraestructura de información, armazones invisibles que ordenan a los datos de acuerdo con ciertos criterios, propósitos e intereses

La vigilancia depende, entonces, de infraestructura de información, armazones invisibles que ordenan a los datos de acuerdo con ciertos criterios, propósitos e intereses. A finales del siglo xx la infraestructura de información fue computarizada, lo que la hizo aún menos visible y más poderosa, y también produjo ciertos tipos específicos de codificación.[11] Y los tipos de interés tras las clasificaciones crecieron para incluir no sólo departamentos del gobierno y servicios policiales o de seguridad sino también a una multitud de organizaciones comerciales.[12] Además, ciertos tipos de agencias se han vuelto prominentes —sobre todo las compañías de seguros— y con frecuencia sus intereses trascienden a los de carácter gubernamental o comercial. Aunque sea una consecuencia no intencional de sus actividades, se han convertido en actores sociales muy poderosos en el escenario contemporáneo.[13]

Sólo por mencionar un ejemplo, existe abundante evidencia de que las compañías de seguros contribuyen de manera importante al trabajo policial en Canadá. Como lo muestran Ericson y Haggerty, los esquemas de "riesgología" y clasificación de instituciones externas como las compañías de seguros tienen profunda influencia en la policía, la que de hecho se vuelve un trabajador de ellas. Las exigencias de las compañías de seguros llevan a un cambio de territorios a clases de población con niveles de riesgo variables. Se buscan datos biográficos de personas

para obtener sus perfiles en términos de probabilidades y posibilidades, lo que vuelve a la vigilancia cada vez más sistemática. La computarización extiende todo el proceso hasta el punto de que al final los autores afirman que "El control coercitivo cede el paso a la categorización contingente. El conocimiento del riesgo es más importante que la culpabilidad moral y el castigo. La inocencia declina y se asume que todos son 'culpables' hasta que el sistema de comunicación de riesgo revele otra cosa [...]"[14]

Pero se trata no sólo de que la infraestructura de información tenga conexiones significativas con el auge de la administración de riesgos y las clasificaciones de seguros sino que también permite la expansión de la capacidad de vigilancia en varios aspectos importantes.[15] El primero es que admite aditamentos (*plug-ins*) provenientes de otros tipos de mecanismos tecnológicos, y el segundo, que permite una mayor porosidad entre los sitios de almacenamiento. Dos de los aditamentos que tengo en mente son la vigilancia con video y televisión en circuito cerrado (TVCC), por una parte, y la biométrica y la vigilancia genética por otra. Una tiene que ver con la visibilidad de las conductas corporales, incluyendo en algunos casos el reconocimiento de las identidades de cuerpos, y la otra con la identificación personal por medio de partes únicas del cuerpo y la predicción de conductas y condiciones a partir de la lectura de secuencias genéticas.

Es importante hacer notar que estos aditamentos dependen de la infraestructura de información para elevar su capacidad de vigilancia porque, a pesar de que cada uno puede contribuir de manera específica al aumento de la vigilancia —al agregar capas de visibilidad o producir identificaciones o predicciones más precisas— su dependencia de la infraestructura de información basada en computadora les da su poder peculiar. Sin la asistencia de una capacidad de procesamiento de datos compleja y sofisticada, estas nuevas tecnologías seguirían siendo relativamente débiles como medios de vigilancia. Desde el punto de vista de las políticas, se trata de un desarrollo decisivo porque el nivel de aceptación no cuestionada de las tecnologías de información y comunicación es mucho más alto que el de la crítica y la evaluación ética y política.

La segunda forma en que la infraestructura de información tiende a apoyar la capacidad de vigilancia es que permite la comunicación en red entre diferentes bases de datos. En tanto que alguna vez fue bastante seguro asumir que los expedientes personales que se elaboran con fines como salud, trabajo policial, seguridad social, banca y licencias de manejar se almacenarían en depósitos relativamente herméticos, la computarización de ellos significa que son fácilmente manejables en distintas formas de integración. Dado el inmenso valor que tienen los datos personales, tanto para su explotación comercial como para la administración de riesgos, se ejerce gran presión sobre estos depósitos para que revelen sus secretos de manera que se puedan compartir.

SE EJERCE GRAN PRESIÓN sobre los depósitos de datos personales para que revelen sus secretos

En todos los sectores aparecen métodos similares de pareo de datos o enlace de expedientes, lo que hace más fácil la tabulación cruzada. Los departamentos de gobierno buscan formas de ayudarse unos a otros a cumplir con su trabajo, pero las organizaciones comerciales también intercambian datos personalizados categorizados, en un esfuerzo por llevar sus productos al mercado con mayor efectividad. En ocasiones se dan procesos similares en el mismo lugar con propósitos diferentes. En los aeropuertos los datos de viajeros frecuentes, captados a medida que franquean el mostrador de documentación, pueden usarse para la publicidad de renta de autos. Pero los datos personales de los clientes de las aerolíneas también pueden intercambiarse por razones de seguridad, sobre todo después de los ataques terroristas del 11 de septiembre de 2001 en Estados Unidos. Las autoridades fronterizas estadunidenses y canadienses ahora comparten estos datos y es probable que lo mismo suceda en otros contextos.[16]

Una cuestión relacionada con lo que se podría llamar "datos flotantes" es que al haber fracasado algunas empresas "punto com", sus bases de datos con expedientes personales quedan entre los activos que pueden venderse para pagar a los acreedores. Por ejemplo, cuando en 2000 una empresa quebrada llamada ToySmart.com trató de vender los datos personales que poseía, encontró oposición y fue obligada a vender únicamente el sitio de Internet completo y sólo a una compañía relacionada.[17] Otros casos pueden no salir a la luz o ser menos claros. Una vez más, existen límites técnicos y legales para ello en la mayoría de las jurisdicciones, pero esto no significa que los depósitos con goteras vayan de pronto a dejar de absorber datos uno del otro.[18]

Una de las características clave de lo que Castells llama la "sociedad en red" es que se trata de un "espacio de flujos".[19] Junto con los puntos nodales y los centros de un sistema,[20]

LA VIGILANCIA SE HA CONVERTIDO EN UN MEDIO SIGNIFICATIVO DE GOBERNAR Y REFORZAR LAS DIFERENCIAS SOCIALES, Y POR ESO SE TRATA DE UN TEMA IMPORTANTE

los grupos dominantes determinan cómo y con qué fines opera la infraestructura material. Entre las secuencias de intercambio e interacción que forman estos flujos están los datos de vigilancia, la comunicación de riesgos y la información personal; éstos, como cualquier otro flujo, circulan según la lógica enquistada en las asimetrías del poder organizacional. Norris y Armstrong ofrecen ejemplos concretos de esto cuando hablan de la TVCC.[21] Los estadios de futbol son vigilados por las cámaras en busca de señales probables de desorden, los lugares de trabajo se vigilan para asegurar que cumplan con los reglamentos de seguridad e higiene y los centros de las ciudades se vigilan para mantener condiciones ideales para el consumo. Los grupos dominantes garantizan la dispersión de la disciplina y de su cualidad ondulante y cambiante, a medida que los intereses de los distintos sectores desempeñan su papel.

Un resultado de esto que no se debe pasar por alto es que de esta manera las llamadas sociedades de la información son, por su constitución misma, sociedades de vigilancia, que no son un resultado malévolo o accidental de procesos perversos en las sociedades de información. Éstas —tal vez mejor dicho, sociedades en red—[22] en las que las estructuras avanzadas de información con base en la electrónica son un medio preponderante de coordinación e intercambio, operan por medio, entre otras cosas, de operaciones avanzadas de vigilancia. Pero no necesariamente se trata de sociedades de vigilancia máxima, posibilidad que preocupó a George Orwell y que James Rule analizó a través de la sociología en los setenta. Si bien el potencial totalitario siempre está presente, en especial en regímenes que ya muestran esas tendencias, es más probable un desarrollo más sutil de la capacidad de vigilancia.

Según las entiende este trabajo, a las sociedades de vigilancia no las caracteriza un solo sistema que todo lo abarca y penetra, lo que Orwell temía más que nada. Como dicen Norris y Armstrong acerca de la vigilancia con cámaras: "La TVCC se ha implantado no como un sistema predominante sino como una serie de sistemas discretos, localizados, administrados por una multitud de organizaciones diferentes más que por un solo monolito del estado".[23]

El hecho de que no exista un solo sistema que abarque todo no es, sin embargo, un llamado a la complacencia. El sistema —tal vez mejor dicho el "ensamblaje"—[24] se expande y pasa por mutaciones constantes. No sólo aumenta en organizaciones jerárquicas del tipo de las que muestran al Hermano Mayor que vigila todo desde el ápex del *panopticoninspector* que asoma de la torre sino, con más frecuencia, dentro de redes que se propagan de manera horizontal, que se extienden aquí y se contraen allá pero encuentran siempre nuevas maneras de buscar y procesar datos personales con miras al manejo y la influencia.

¿POR QUÉ ES IMPORTANTE LA VIGILANCIA?

Antes sugerí que la vigilancia se ha convertido en un medio significativo de gobernar y reforzar las diferencias sociales, y por eso se trata de un tema importante. No deseo menospreciar los temores de quienes sientan que su intimidad puede ser impugnada o invadida por nuevas tecnologías de vigilancia. Se trata de temores reales y merecen ser discutidos. Pero si se consideran sólo los temores personales acerca de la intimidad esto posiblemente distraiga de las cuestiones públicas en torno a la vigilancia.[25] Cuando sugiero que la vigilancia se ha convertido en un medio de gobernar quiero decir que sirve para organizar las relaciones sociales y contribuye a formar patrones de ordenamiento social, en gran medida a través de lo que Foucault llamó biopoder, dar forma a la gente al clasificarla de acuerdo con categorías. En el mundo de la vigilancia, éstas se relacionan con el riesgo y la oportunidad. De cualquier manera, lo normal desde el punto de vista de la estadística o de la organización se convierte en la piedra de toque para distinguir lo que es correcto, o por lo menos apropiado.[26]

La categorización es un proceso antiguo, pero se volvió crucial para la organización social racionalizada de la modernidad. Por medio de la convención social y de la costumbre, la gente acepta su lugar en la jerarquía o aprende a verse a sí misma en relación con la posición de los demás. ¿Qué sucede cuando las líneas tradicionales de autoridad y relación se desmantelan y sustituyen con reglas burocráticas y prácticas organizacionales? Al final, éstas también son aceptadas, aunque tal vez ahora parezcan mucho más mutables. ¿Quién lo dice? Esa es la pregunta que se oye en las situaciones democratizadoras del siglo XX; en el parlamento, el sindicato o la escuela preparatoria. Pero se podría decir que tales preguntas eran mucho más comunes en las situaciones en las que predominaba la interacción cara a cara. A medida que el cuerpo desaparece de las relaciones sociales integradoras y es remplazado por pruebas abstractas, también las categorías se vuelven más abstractas y actuarias y, por lo mismo, benignas en apariencia. Cuando los científicos de la información diseñan, delegan y eligen sistemas de clasificación rara vez los ven como una "materialización de elecciones morales y estéticas que a su vez forman las identidades, las aspiraciones y la dignidad".[27] Pero como señala Suchman: "las categorías tienen política".[28]

LOS USUARIOS DE LA INTERNET DESEAN LOS BENEFICIOS DEL COMERCIO ELECTRÓNICO AUN CUANDO QUIEREN GARANTÍAS DE QUE SUS DATOS PERSONALES ESTÁN SEGUROS

Los sistemas masivos de clasificación asistida por computadora desarrollados durante los últimos 30 años son la infraestructura cuya existencia se da por hecho en las sociedades de la información. Representan una concatenación de estándares, prácticas y códigos más o menos interconectados, al grado de que —en el caso de las clasificaciones de vigilancia que aquí se consideran— fluyen de manera constante datos personales y de población por los puntos nodales y los centros de la red. Aunque existen obvias asimetrías de poder, ninguna persona o cuerpo está a cargo de los sistemas de vigilancia ni puede cambiarlos. Sin embargo ayudan a darnos forma, a naturalizarnos ante las instituciones y dependencias que inventan y elaboran las categorías. Y ayudan a crear un sentido de quién y qué está incluido o excluido con razón; quién es éste, aquél o el otro.[29] Por supuesto, es una cuestión empírica saber hasta qué punto y bajo qué condiciones acepta la gente como propias las categorías que le asignan los sistemas contemporáneos de vigilancia.[30] Se trata de un proceso reflexivo. Pero la historia de la categorización médica, moral, criminal y de consumo sugiere que mucha gente acepta dichas etiquetas y vive en consecuencia.

No estoy sugiriendo que la clasificación y vigilancia sean procesos socialmente negativos. Son aspectos necesarios en todas las situaciones sociales y cumplen fines sociales, desde los vitales hasta los viciosos. Lo importante es que, como medios poderosos de gobierno, de ordenamiento social, también son cada vez menos visibles y con facilidad se dan por supuestos. Las clasificaciones de administración de riesgos (y otras) de las sociedades de vigilancia implican categorías inherentemente políticas que requieren una inspección ética. Tampoco sugiero que cada una de dichas clasificaciones sea poderosa de igual manera. Como se entiende aquí, la vigilancia existe en un amplio espectro, a lo largo del cual se recogen y procesan datos para una gama de fines que van desde el trabajo policial y la seguridad hasta el consumo y el entretenimiento. Produce, en un extremo, la sospecha por categorías —como los perfiles étnicos en los puntos de seguridad de los aeropuertos— y la seducción por categorías —como la localización de clientes potenciales para renta de autos en las listas de viajeros frecuentes de las líneas aéreas— en el otro. Pero de cualquier manera las categorías tienen ética; los códigos tienen política.

Por esto la vigilancia importa. Es cierto que a veces provoca preocupación por la intimidad. Pero, según se ha expresado, estas inquietudes personales suelen ser temporales y coyunturales, con frecuencia relacionadas con errores y fallas en los sistemas de bases de datos o telecomunicaciones, o con la pérdida del acceso a pruebas de confianza como tarjetas de crédito o licencias de conducir. No tienen prioridad en ninguna agenda política. Y cuando, por ejemplo, los usuarios de la Internet que participan en encuestas afirman que les importa la intimidad en línea, paradójicamente, ¡las mismas personas "teclean" sus NIP y números de tarjeta de crédito y los ponen en línea![31] Desean los beneficios del comercio electrónico aun cuando quieren garantías de que sus datos personales están seguros y no se usan con otros fines que no sean la transacción inmediata. Cuando se trata de poner restricciones legales a la vigilancia, sea ésta considerada como protección de datos o como leyes para resguardar la intimidad, suele ser el sujeto de datos quien tiene que apelar. La ley sólo actúa como garantía de algún derecho a la autoprotección. Por eso los límites legales, aunque tienen importancia, apenas rascan la superficie de las cuestiones sociales que surgen debido a los niveles de vigilancia en la vida cotidiana, que crecen con rapidez.

Véase, por ejemplo, el tema del voto en las elecciones. En décadas recientes la influencia de la televisión en el proceso electoral se ha hecho notar a menudo. Todo el discurso de la política ha sido moldeado por la necesidad que perciben los políticos de convertirse en "personalidades" de los medios en su intento de ejercer influencia sobre el electorado. Pero el éxito de sistemas como la mercadotecnia mediante bases de datos ha impulsado nuevas formas de obtener apoyo, entre las cuales no carece de importancia la elaboración de perfiles de individuos que pudieran hacer donativos. La firma consultora estadunidense Aristotle International utiliza fuentes públicas, como los registros de vehículos automotores, el servicio postal o la oficina del censo, para recabar datos como la edad, el sexo, el número de teléfono, el ingreso estimado, la etnia, si tiene casa propia y la afiliación partidista de las personas. También registra qué marcas y modelos de autos poseen, para quién trabajan y a qué se dedican, si son o no donadores en campañas y con qué frecuencia votan.[32] Estos datos se manipulan para extraer perfiles individuales de las personas que son objetivos probables.

Este ejemplo no hace uso explícito de la Internet (aunque podría desear hacerlo), y sólo se refiere a datos personales ya a disposición del público. Es más, en Canadá las actividades de este tipo no serían tocadas por la legislación existente (con la posible excepción de Québec), y no está claro si serían cubiertas por la Ley de Protección de Información Personal y Documentos Electrónicos, que entró en vigor el 1 de enero de 2001. Si bien algunas personas objetan que sus actividades electorales son privadas —y, después de todo, las democracias modernas tienen como doctrina cardinal la idea del voto secreto—, de esta manera son clasificadas y agrupadas en

categorías para fines particulares con los que pueden no estar de acuerdo. El consentimiento o la negación de éste no entran en este momento en ecuaciones de recolección de datos como ésta, aunque las consecuencias —para la diseminación de la información política y para un conocimiento equilibrado de las políticas alternativas— puedan tener gran alcance. La intimidad es una cuestión, la discriminación es otra.[33]

¿QUÉ PUEDE HACERSE ACERCA DE LA VIGILANCIA?

Tendría sentido que algunas prácticas sociales y determinados sistemas tecnológicos que afectan a todas las personas fueran comprendidos y negociados por todos. No es el caso. Lo más frecuente es que la conveniencia y la eficiencia sean lo único que se hace notar en sistemas con aspectos de vigilancia, por lo que los sujetos de datos suelen no estar enterados de otras dimensiones de discriminación y clasificación de dichos sistemas. Las políticas y legislaciones para la protección de datos y de la intimidad han dado pasos importantes en las últimas décadas, pero en algunos casos pueden ser minimalistas e incluso cínicas. La protección de datos y de la intimidad siguen siendo preocupaciones vitales, aun si su impacto en los aspectos negativos de la categorización social todavía no es muy grande. Por otra parte, el minimalismo se manifestaría en reglas que sólo contemplan el derecho a la autoprotección, y el cinismo es evidente donde las leyes se han promulgado para facilitar los negocios con un socio comercial y no debido a una auténtica preocupación por sus efectos en las vidas y posibilidades de los sujetos de datos.

Al mismo tiempo, la vigilancia no se da a espaldas de la gente. Participamos en ella y —aunque no siempre de manera consciente— disparamos la captura de datos al hacer llamadas telefónicas, usar tarjetas de crédito, pasar nuestras manos por lectores electrónicos de ingreso, reclamar premios, caminar por una calle vigilada con cámaras, navegar por la red. No se sabe mucho de qué manera se alinea con, negocia con y se resiste a la vigilancia la gente en su vida cotidiana. Pero es claro que los trabajadores tienen sus reservas, si no es que se oponen a algunos dispositivos electrónicos como la vigilancia mediante video, audio y computadora, sin mencionar las revisiones y filtros biométricos y genéticos. La gente que utiliza espacios públicos como las calles y privados como los centros comerciales está consciente de que hay sistemas de vigilancia por circuito cerrado de televisión y video, y los evita o actúa para ellos. Los usuarios de cuentas de correo electrónico en la red y los compradores en línea a veces son precavidos y no proporcionan sus datos personales cuando se les solicitan, sobre todo si parece que tienen poco que ver con la transacción en cuestión. Saben que otra parte de datos suyos circulan en el ciberespacio y lo aceptan como el precio que se paga por algún beneficio o recompensa.

Pero no basta asumir que con el tiempo la gente, de alguna manera, se va a "poner lista" ante la proliferación de sistemas de vigilancia. Éstos son un medio de clasificación y ordenamiento social no siempre sujeto a inspecciones ni a reglas. Afectan las oportunidades y opciones de la gente, y por eso exigen que se les reconozca. Además, su crecimiento demanda escrutinio técnico y participación democrática. Por supuesto que en todos ellos existe ambigüedad, que la vigilancia muestra más de un rostro. Pero el que recibe publicidad es el de la organización que funciona sin problemas, la respuesta rápida a las exigencias del consumidor o a la demanda de seguridad, la flexibilidad de la estructura de administración, y no los aspectos negativos y posiblemente indeseables del procesamiento de datos personales. El poder de discriminación de la vigilancia contemporánea es enarbolado por grandes organizaciones con fuertes intereses en valiosos datos personales. Las personas de quienes se extraen éstos enfrentan, en este sentido, una desventaja inherente.

Durante las últimas dos o tres décadas se han dado varios tipos de respuestas a la vigilancia, se puede pensar en ellas como regulatorias y movilizadoras.[34] El primer aspecto se ve de manera más obvia en las distintas leyes de protección de datos y de la intimidad que existen en la mayoría de los países que dependen de la infraestructura de información. Pero también es evidente en una serie de remedios voluntarios, de mercado y técnicos para lo que comúnmente se considera amenaza a la intimidad. Las medidas voluntarias incluyen la adherencia de una compañía a los principios correctos de la información. La mayoría de los bancos y muchos operadores de sitios de la Internet ofrecen hoy, por iniciativa propia, detalles de sus "políticas de privacidad". Las soluciones de mercado incluyen cada vez más la noción de hacer que los datos personales ganen el equivalente a regalías, de manera que el sujeto de datos obtenga un retorno tangible a cambio del uso de los suyos. Las soluciones técnicas son variadas, y con frecuencia se relacionan con la seguridad. El ejemplo que más publicidad ha recibido es la firma electrónica.

Los "principios correctos de información" (que requieren que quienes recopilan datos los usen sólo para los fines declarados, que soliciten sólo los necesarios para sus propósitos inmediatos y que aseguren de que se obtuvieron con el conocimiento y consentimiento del sujeto de datos) a los que se refieren la mayoría de las leyes sobre la intimidad, no abordan de forma directa la categorización que llevan a cabo los sistemas de vigi-

lancia. Dependen, de manera implícita pero importante, de la idea de que los sujetos de datos pueden tener interés en controlar la circulación de ellos. Esto se relaciona con el deseo éticamente correcto de abrirse ante otros sólo de manera voluntaria y limitada, y en relaciones de confianza. Estas prácticas correctas de información, cuando se instauran, pueden mitigar algunos efectos negativos de la categorización discriminatoria.

Pero las prácticas correctas de información no persiguen una inspección ética de las categorías en cuestión, menos aún examinar de qué manera la fuerza combinada de múltiples categorizaciones puede restringir en forma estricta las oportunidades y opciones de algunas personas y al mismo tiempo abrir oportunidades para otras. Esto exige un punto de vista más allá de los reclamos de intimidad y de los alegatos marxistas acerca de nuevas formas de dominación del capitalismo a través de la información. Aunque la primera lleva, cuando mucho, a la protección legal, ésta con frecuencia se reduce a derechos de propiedad privada sobre los datos personales. En cuanto a la segunda, mientras que señala con razón asimetrías en el poder de la información, puede menospreciar con facilidad el papel de las mediaciones tecnológicas y el del sujeto. Un punto de vista ético, que demanda el escrutinio democrático de los sistemas de información, da lugar a cuestiones cruciales de responsabilidad y propone formas de crítica inmanente, desde la cultura de la información.[35]

Por otra parte, las respuestas de movilización han crecido en número y volumen desde los ochenta. Organizaciones no gubernamentales y movimientos de consumidores han tratado de comprender las realidades de la expansión de raíces proliferantes de la vigilancia. Pueden adquirir la forma de protesta organizada o de grupos de vigilancia —como Privacy International o el Electronic Privacy Information Center— o dar respuestas *ad hoc* a cuestiones específicas. De esta manera el intento de crear una tarjeta electrónica llamada Australiacard para todos los ciudadanos a mediados de los ochenta tuvo como respuesta un movimiento social que rechazó con éxito la propuesta, y lo mismo sucedió con intentos similares en Corea del Sur. También se han montado campañas contra empresas y productos específicos, como el programa de Lotus Mercados: Hogares, en 1994, o el procesador Pentium III de Intel, con su identificador único para todas las computadoras, en 1999. El uso de la Internet para promover la resistencia es parte importante del proceso.

Estas respuestas movilizadoras pueden señalar el camino hacia nuevos modos de negociar y resistir en el siglo XXI aspectos de la vigilancia que tienen imagen negativa. Son los códigos, tanto simbólicos como electrónicamente inscritos, los que brindan los medios para que fluya el poder de la vigilancia. Como alega Deleuze, las barreras físicas y el encierro en ciertos lugares hoy importan menos que los códigos que activan y desactivan, admiten y excluyen, acreditan o desacreditan.[36] Los protocolos audiovisuales y digitales permiten entrar y moverse en la ciudad en lugar de las antiguas puertas de la ciudad que daban tanta importancia al contenedor físico.[37] Melucci

NOTAS

1. Rose, Nikolas. *Powers of freedom: reframing political thought,* Cambridge University Press, Cambridge/Nueva York/Melbourne, 1999, p.234.

2. El término *data subjects* se traduce como "sujetos de datos" por su relación de sentido con las expresiones "base de datos" o "banco de datos", en tanto que se les ve como sujetos en los que están depositados los datos que se busca obtener (N.T.)

3. Thompson, John. *The media and modernity,* Polity Press, Cambridge, 1995, capítulo cuatro.

4. Marvin, Carolyn. *When old technologies were new,* Oxford University Press, Oxford/Nueva York, 1988; Slevin, James. *The Internet and society,* Polity Press, Cambridge, 2000.

5. Lyon, David. "Cyberspace sociality: controversies over computer-mediated communication", en Loader, Brian (ed.), *The governance of cyberspace, Routledge,* Londres/Nueva York, 1997.

6. Torpey, John. *The invention of the passport: surveillance, citizenship, and the state,* Cambridge University Press, Cambridge/Nueva York/Melbourne, 2000.

7. Nock, Steven L. *The costs of privacy: surveillance and reputation in America,* Walter de Gruyter, Nueva York, 1993.

8. Dandeker, Christopher. *Surveillance, power, and modernity,* Polity Press, Cambridge, 1990.

9. Brown, John Seely y Paul Duguid. *The social life of information,* Harvard Business School Press, Boston, 2000, p.108.

10. Verma, Sonia. "Police double crime 'hot-spot' targets", en *The Toronto Star,* 23 de julio de 1999, pp.A1 y A21.

11. Lessig, Lawrence. *Code and other laws of cyberspace,* Basic Books, Nueva York, 1999.

12. Lyon, David. *The electronic eye: the rise of surveillance society,* Polity Press/Blackwell, Cambridge/Malden, 1994; Gandy, Oscar H. *The panoptic sort: a political economy of personal information,* Westview, Boulder, 1993.

13. Strange, Susan. *The retreat of the state: the diffusion of power in the world economy,* Cambridge University Press, Cambridge/Nueva York/Melbourne, 1996.

14. Ericson, Richard V. y Kevin Haggerty. *Policing the risk society,* University of Toronto Press, Toronto, 1997, p.449.

15. Rule, James. *Private lives, public surveillance,* Allen-Lane, Harmondsworth, 1973.

16. Whittington, Les y Tim Harper. "Ottawa to boost terror laws," en *The Toronto Star,* 23 de noviembre de 2001, p.A1; Lyon, David. "Surveillance after september 11 2001", en *Sociological Research Online,* www.socresonline.org.uk, 2001.

17. Stellin, Susan. "Dot-com liquidations put consumer data in limbo", en *The New York Times,* 4 de diciembre de 2000.

18. Flaherty, David. *Protecting privacy in surveillance societies,* University of North Carolina Press, Chapel Hill, 1989; Bennett, Colin. *Regulating privacy: data protection and public policy in Europe and the United States,* Cornell University Press, Ithaca, 1992.

19. Castells, Manuel. *The rise of the network society,* Blackwell, Oxford/Malden, 1996, p.412.

20. La palabra inglesa *hub* se refiere, en su acepción

observa que ahora los movimientos sociales se preocupan cada vez más por percibir riesgos e identificarlos como cuestiones públicas, con un proceso de "códigos de desafío".[38] Afirma que a medida que las preocupaciones cotidianas acerca de la identificación personal y las oportunidades en la vida se vuelvan, de manera más obvia, en contra de los flujos globales de datos y poder, surgirán nuevas políticas de oposición, adecuadas a la "era de la información".

Dicho esto, sigue siendo cierto que los procesos asociados con las tecnologías de comunicación e información aún se ven más bien color de rosa. Hay gran alharaca en torno al desarrollo de la Internet y del mundo en red en general, pero los beneficios genuinos de tener sistemas de vigilancia en su lugar tienden a desviar la atención de las desigualdades asociadas con varias dimensiones discriminatorias de la vigilancia, y algunas tecnologías simplemente salen mejor libradas que otras a los ojos del público. En tanto que la biotecnología puede ser vista como "meterse con el cuerpo humano", las tecnologías de la información rara vez reciben respuestas tan negativas por su capacidad ya sea para "meterse con la mente" o —todavía menos— para producir sutiles mecanismos de ordenación social.[39] Puede resultar, por supuesto, que a medida que prevalezcan más formas biométricas y genéticas de vigilancia surjan dudas mayores acerca de la capacidad de clasificación de los códigos actuales.

Así, la pregunta "¿qué se puede hacer?" puede responderse de manera práctica más que abstracta. Han surgido muchas respuestas a la vigilancia y, como sugerí antes, esto es apropiado dada la vigilancia creciente de la vida cotidiana. Mientras que las instancias legales pueden tomar la iniciativa en algunos casos son necesarias otras respuestas en varios niveles. La ley sólo puede ayudar a crear una cultura de considerar el procesamiento de datos personales; no le es posible atender todos los temas, mucho menos mantenerse al día acerca de los avances en la búsqueda de datos, generación de perfiles, localización de mercados y mercadeo mediante bases de datos, localización de vehículos o teléfonos celulares, etcétera.

Las respuestas conspiratorias y paranoicas son contraproducentes porque los aspectos negativos de la vigilancia con frecuencia surgen como resultados no intencionales o subproductos de otros procesos, aceptables o incuestionables, de administración de riesgos o mercadotecnia. Tampoco son apropiadas para situaciones de vigilancia en red, donde no existe una torre panóptica de inspección ni un Hermano Mayor omnipotente. Más bien se requiere una vigilancia constante de instancias de gobierno, empresas, grupos de gestión y consumidores, así como de los usuarios y ciudadanos, sobre todo a los regímenes de pánico resultantes de los ataques terroristas del 11 de septiembre de 2001. Se necesita una atención ética concentrada, junto con propuestas serias, para establecer responsabilidades de manera democrática, lo mismo que iniciativas que impulsen la educación y generación de conciencia, si se quiere entender adecuadamente la vigilancia cotidiana y, cuando sea necesario, enfrentarla y desafiarla. ■

original, al centro de una rueda (lo que en español se conoce como la "maza" o el "cubo"), de donde parten los rayos. En el ámbito tecnológico un *hub* es un centro de redistribución de redes o de servidores. Por extensión se llama *hub*, en diversos ámbitos, a los puntos donde se concentran y de donde vuelven a partir caminos, mensajes o transacciones (N.T.)

21. Norris, Clive y Gary Armstrong. *The maximum surveillance society: the rise of TVCC*, Berg, Londres, 1999, p.8.

22. Castells, Manuel. "Materials for an exploratory theory of the network society", en *British Journal of Sociology*, núm.51, Londres, 1998, p.1.

23. Norris, Clive y Gary Armstrong. *Op. cit*, p.7.

24. Haggerty, Kevin, y Richard V. Ericson. "The surveillant assemblage", en *British Journal of Sociology*, núm.51, Londres, 2000, p.4.

25. Regan, Priscilla. *Legislating privacy: technology, surveillance, and public policy*, University of North Carolina Press, Chapel Hill, 1995.

26. Hacking, Ian. *The taming of chance*, Cambridge University Press, Cambridge/Nueva York, 1990.

27. Bowker, Geoffrey. y Susan L. Star. *Sorting things out: classification and its consequences*, The MIT Press, Cambridge, 1999, p.4.

28. Suchman, Lucy. "Do categories have politics? The language/interaction perspective reconsidered", en *Computer-Supported Cooperative Work*, núm.2, 1994, pp.177-190.

29. Bourdieu, Pierre. *Distinction: a social critique of the judgement of taste*, Routledge, Londres/Nueva York, 1984, pp.470-478.

30. Jenkins, Richard. "Categorization: identity, social process, and epistemology", en *Current Sociology*, vol.48, 2000, pp.3, 7-25.

31. "Internet users seek assurances over on-line use of personal data", en *The Washington Post*, 20 de agosto de 2000.

32. "One consulting firm finds voter data is hot property", en *The New York Times*, 9 de septiembre de 2000.

33. Gandy, Oscar H. "It's discrimination, stupid!", en Brook, James e Ian A. Boal (eds.), *Resisting the virtual life: the culture and politics of information*, City Lights, San Francisco, 1995.

34. Lyon, David. *Surveillance society: monitoring everyday life*, Open University Press, Buckingham, 2001, capítulo ocho.

35. Lyon, David. "Facing the future: seeking ethics for everyday surveillance", en *Information, Technology and Ethics*, 2001.

36. Deleuze, Gilles. "Postscript on the societies of control", en *October*, núm.59, 1986, pp.3-7.

37. Virilio, Paul. "The over-exposed city", en Leach, Neil (ed.), *Rethinking architecture*, Routledge, Londres/Nueva York, 1997, p.383.

38. Melucci, Alberto. *Challenging codes: collective action in the information age*, Cambridge University Press, Cambridge/Nueva York/Melbourne, 1996.

39. Nelkin, Dorothy. "Forms of intrusion: comparing resistance to information technology and biotechnology in America", en Bauer, Martin (ed.), *Resistance to new technology*, Cambridge University Press, Cambridge/Nueva York/Melbourne, 1995.

LA TUMBAHOMBRES. ACUARELA/PAPEL, 152 x 103 cm, *Cueva Coxala, 1997*