novática
Revista de la Asociación de Técnicos de Informática

Novática, revista fundada en 1975 y decana de la prensa informática española, es el órgano oficial de expresión y formación continua de **ATI** (Asociación de Técnicos de Informática), organización que edita también la revista **REICIS** (Revista Española de Innovación, Calidad e Ingeniería del Software).

<http://www.ati.es/novatica/>
<http://www.ati.es/reicis/>

ATI es miembro fundador de **CEPIS** (*Council of European Professional Informatics Societies*) y es representante de España en **IFIP** (*International Federation for Information Processing*); tiene un acuerdo de colaboración con **ACM** (*Association for Computing Machinery*), así como acuerdos de vinculación o colaboración con **AdaSpain**, **AI2**, **ASTIC**, **RITSI** e **Hispalinux**, junto a la que participa en **ProInnova**.

Coordinación Editorial, Redacción Central y Redacción ATI Madrid
Padilla 66, 3º, dcha., 28006 Madrid
Tlfn.914029391; fax.913093685 <novatica@ati.es>
Composición, Edición y Redacción ATI Valencia
Av. del Reino de Valencia 23, 46005 Valencia
Tlfn. 963740173 <novatica_prod@ati.es>
Administración y Redacción ATI Cataluña
Via Laietana 46, ppal. 1ª, 08003 Barcelona
Tlfn.934125235; fax 934127713 <secregen@ati.es>
Redacción ATI Aragón
Lagasca 9, 3-B, 50006 Zaragoza.
Tlfn./fax 976235181 <secreara@ati.es>
Redacción ATI Andalucía <secreand@ati.es>
Redacción ATI Galicia<secregal@ati.es>
Suscripción y Ventas <novatica.subscripciones@atinet.es>
Publicidad Padilla 66, 3º, dcha, 28006 Madrid.
Tlnf.914029391; fax.913093685 <novatica@ati.es>
Imprenta: Derra S.A., Juan de Austria 66, 08005 Barcelona.
Depósito legal: B 15.154-1975 -- ISSN: 0211-2124; CODEN NOVAEC
Portada: Lenguaje primario - Concha Arias Pérez / © ATI
Diseño: Fernando Agresta / © ATI 2003

sumario

Nº 222, marzo-abril 2013, año XXXIX

Tema del próximo número: "Minería de procesos"

Privacidad y vigilancia: Una guía básica

Aaron Martin
London School of Economics and Political Science

<A.K.Martin@lse.ac.uk>

Traducción: Josep Moya Pérez (Grupo de Trabajo de Lengua e Informática de ATI)

***Resumen**: Activistas, académicos y legisladores reconocen cada vez más que la vigilancia excesiva (a menudo posibilitada por nuevas tecnologías de la información y las comunicaciones) puede ser perjudicial para la sociedad. Pero para entender cómo estos desarrollos de la vigilancia pueden actuar en detrimento del fomento de sociedades sanas, abiertas y democráticas, debemos saber primero dónde buscar una base conceptual, y más importante aún, qué buscar una vez la encontremos. Por lo tanto, este artículo repasa cuestiones y conceptos clave sobre la privacidad y la vigilancia para profesionales y defensores deseosos de comprender e involucrarse en estos temas multifacéticos, dado que los debates sobre los beneficios y riesgos de divulgar y compartir nuestros datos se vuelven cada vez más dinámicos y relevantes.*

***Palabras clave:** Privacidad, **r**esumen conceptual, tecnología, vigilancia.*

Autor

Aaron Martin ha investigado temas de privacidad y vigilancia desde 2004, más recientemente como analista de políticas tecnológicas tanto en la OCDE como en el Centro Común de Investigación de la Comisión Europea. En 2011 obtuvo un doctorado en política de biometría en la London School of Economics, a la vez que trabajaba como analista de privacidad en el Grupo Vodafone, donde se centró en áreas de vigilancia en comunicaciones y en privacidad en la ubicación. También colabora regularmente con Privacy International, una organización civil que defiende el derecho a la intimidad en todo el mundo. Estas experiencias le proporcionan una perspectiva única (que abarca los mundos de la investigación, la política, la industria y la sociedad civil) desde la que analizar el estado actual del panorama de la privacidad y la vigilancia.

1. Introducción

En los círculos de los negocios y tecnología está en boga declarar la muerte de la privacidad. Mark Zuckerburg ya lo dijo. Lo mismo hizo Eric Schmidt.

La increíble popularidad de las redes sociales, las aplicaciones gratuitas y los servicios *online* dan testimonio de los vastos cambios que se están produciendo. Incluso simples palabras como "gratis" ya no expresan lo que una vez significaron. Utilizar una plataforma gratuita se supone que equivale ahora a dar consentimiento para que la información personal sea recogida, manipulada, y vendida. "*Si no estás pagando por él, tú eres el producto*", o eso dicen.

En esta nueva, asombrosa economía digital, los datos de carácter personal son punto de referencia. Las plataformas se han convertido en una parte tan esencial de la sociedad que proporcionar un nombre, una dirección de correo electrónico o parte del historial del navegador parecen un pequeño precio a pagar a cambio de acceder a la corriente dominante. Esta es exactamente la clase de divulgación voluntaria sobre la que Zuckerburg habla, pero no siempre es voluntaria y definitivamente no es "libre" en el sentido político tradicional del término.

Por supuesto, la realidad es mucho más compleja. Los argumentos que Zuckerburg y otros hacen son ingenuos, tal vez intencionadamente ingenuos. La privacidad no está muerta y es probable que nunca muera, a pesar de que proliferen nuevos modelos de negocio que utilizan gran cantidad de datos y de que la vigilancia se hace menos costosa, más eficaz y mucho más omnipresente.

Está en juego quién controla y hace uso de la información personal: Facebook quiere regular las reglas para compartir, pero aún más importante es que desea el dominio sobre grandes cantidades de información sobre lo que hacemos y a quién conocemos; por su parte, Google compite para saber más sobre lo que estamos buscando y por dónde navegamos. De todas maneras, al centrarnos en esas dos organizaciones como hacen tantas historias, se pasan por alto las cuestiones de mayor importancia sobre los entornos sociales y tecnológicos, rápidamente cambiantes, en los que estamos luchando constantemente para valorar la repercusión de los nuevos desarrollos.

Necesitamos entender cómo estos avances son perjudiciales para el fomento de sociedades sanas y abiertas. Antes de que podamos hacer un esfuerzo coordinado para aprovechar estas tecnologías en beneficio de sociedades abiertas, primero tenemos que saber dónde mirar y qué buscar. Por esta razón, es muy necesaria una revisión de las cuestiones clave en privacidad y vigilancia, e intentaremos aquí ofrecerla.

2. La privacidad como problemática

La privacidad es uno de los conceptos más polémicos de la sociedad. A los academicos les encanta discutir sobre la definición del término. Existe cierto debate sobre si la privacidad es una creación exclusivamente occidental que tiene poco o ningún sentido en otros lugares. Argumentos basados en el relativismo cultural se aplican igualmente a muchos temas, pero apelar al relativismo cultural es también cuestión de poder y de oportunidad: raramente consideramos debates sobre si el derecho intelectual es culturalmente relativo. Diferentes culturas pueden definir lo que es privado de diferentes maneras. A menudo el problema es encontrar el lenguaje apropiado para discutir sobre asuntos relacionados con la privacidad con los de una cultura diferente, sociedad o comunidad.

Comunitaristas[1] como Amitai Etzioni sostienen que el derecho a la intimidad debe estar equilibrado con el bien común, y que los derechos de privacidad individual no pueden ser absolutos [1].

Los defensores del comunitarismo ofrecen un conjunto de criterios para equilibrar el derecho del individuo respecto al bien de la sociedad, incluyendo la evaluación de alternativas respetuosas con la intimidad, con el objetivo de inmiscuirse mínimamente en la vida privada de uno y reducir las consecuencias no deseadas. Estos principios se reflejan en muchas declaraciones internacionales sobre privacidad y derechos humanos.

También hay una interesante crítica feminista que desafía el concepto histórico de intimidad. Siegel señala que los hombres han utilizado históricamente reclamaciones de privacidad para proteger su hogar ("el hombre es el dueño de su dominio"), uniendo de ese modo lo privado con la armonía doméstica de tal manera que legitima el abuso marital. "*Este derecho a la intimidad es un derecho de los hombres 'a ser dejados solos' para oprimir a las mujeres de una en una*" [2].

El desafío moderno es considerar cómo se reflejan estos debates en nuestras sociedades tecnológicas y en economías cambiantes. Sin

> "Mucho se ha dicho sobre la capacidad democratizadora de las tecnologías de la información y la comunicación. Sin embargo, poco se ha discutido sobre cómo Internet y otras tecnologías relacionadas democratizan la vigilancia en sí misma"

duda, la privacidad debe equilibrarse y el criterio puede variar a través de los sistemas jurídicos, pero, ¿cómo se negocia esto si tenemos en cuenta el diseño de nuevas infraestructuras tecnológicas?; ¿añadimos el 'equilibrio' en nuestros diseños, asegurándonos quizás de que todos los ordenadores tengan vulnerabilidades encubiertas para facilitar el acceso a la policía local?

Asimismo, la tecnología está cambiando el entorno familiar moderno y hay nuevos desafíos sobre privacidad que debemos tener en cuenta con respecto a las relaciones y a los niños. Pero las protecciones podrían democratizarse en lugar de estar sólo disponibles para las fuerzas dominantes en las sociedades.

3. Enmarcar el debate

Mientras que estas críticas son importantes y nos obligan a pensar críticamente sobre el valor de la intimidad, ninguna de ellas ofrece una refutación total [3].

Un tratamiento sistemático esencial del concepto proviene del jurista Daniel Solove, que proporciona alguna claridad práctica en su *Taxonomía de la privacidad* [4]. La taxonomía capta las diversas facetas de la vida privada sin desmembrarla o desunirla. Solove se mueve más allá de discusiones teóricas (¿es la privacidad un derecho humano, un derecho legal, un derecho del consumidor, una creación cultural, etc?) para examinar más evidencias prácticas de la intimidad en acción: acciones que plantean problemas de privacidad. Así, identifica cuatro categorías principales (recolección, procesado, difusión e invasión) explorando y analizando cada una en profundidad y proporcionando un marco sólido para organizar la discusión sobre la privacidad y la vigilancia.

Este debate lo es todo. Si la intimidad es un derecho negociado, que debe equilibrarse respecto a otros derechos y por seguridad nacional o para el progreso económico, debemos tener un debate sobre cómo se marcan los límites. La falta de este debate es lo que conduce a los problemas más graves. La imposibilidad de revisar anteriores debates puede ser un inhibidor del progreso y la innovación. Por lo tanto, el aspecto prometedor sobre la privacidad es que en muchos sitios clave el debate está en marcha volviéndose más enérgico y más fuerte. Eso, en todo caso, es una buena cosa.

4. Procesos de vigilancia: categorización y clasificación social

La privacidad no es sólo una condición individual. A gran escala, los sociólogos de la vigilancia como Oscar Gandy [5] y David Lyon [6] han dilucidado diferentes formas en las que las tecnologías de la información trabajan para discriminar entre individuos y grupos de personas con el fin de controlarlos.

La vigilancia es un proceso de niveles. Como proceso previo a la vigilancia surge la categorización, que es realmente un evento en dos fases: primero la etiqueta, y después la clasificación. Siempre hacemos esto: Por ejemplo, masculino y femenino, solvencia crediticia y alto riesgo, viajero seguro y amenaza potencial, etc.

No hay nada intrínsecamente malo en la categorización. Como Michel Foucault dejó claro en *The Birth of the Clinic* [7], la clasificación es un componente clave del conocimiento humano y un aspecto indispensable de nuestro poder para cambiar nuestra realidad.

En primer lugar, distinguimos entre "saludable" y "enfermo", con evidentes beneficios prácticos. Entonces podemos diferenciar entre personas con problemas oculares y personas con problemas en los pies, por ejemplo, y así en adelante. Agrupándolas juntas como pacientes y eliminando los casos atípicos, aprendemos más acerca de su condición, y a través de este conocimiento obtenemos el poder para cambiarla.

Por supuesto, la categorización tiene también su lado oscuro. Alguien marcado como 'criminal', se le relaciona con otros criminales y puede continuar siendo asociado con ese grupo, aunque esté oficialmente exonerado.

La categorización es importante porque facilita la clasificación social. Una vez los sujetos son etiquetados y agrupados, pueden ser ordenados, gestionados y potencialmente controlados, lo que podría tener los impactos beneficiosos que Foucault observó en la clínica, pero también podría degradar derechos fundamentales y libertades como moverse y expresarse e incluso las posibilidades en la vida.

Los académicos se preocupan por los aspectos perjudiciales de la vigilancia, pero un merecido escrutinio no debería negar sus potenciales aspectos positivos.

Esto no se trata de una relación inversa; es simplemente para decir que cuando estas prácticas son transparentes o se vuelven incuestionables, aumentan las posibilidades de que se produzcan resultados negativos. Los defensores de lo privado siempre ponen al descubierto y diseccionan los sistemas de vigilancia y categorización para comprender sus lógicas, operaciones y consecuencias sociales, para hallar el límite entre sus usos beneficiosos y perjudiciales.

5. Sitios donde actúa la vigilancia

Trazar esta frontera es más parecido a cartografiar galaxias que a distinguir entre las habitaciones de una casa: saber dónde buscar es una condición previa en ambos casos, pero es un desafío mucho mayor en el primer caso que en el segundo. En consecuencia, descubrir dónde se produce la vigilancia se está volviendo cada vez más importante. Hay una larga y creciente lista de sitios de seguimiento y observación, protegidos regularmente por avances tecnológicos y nuevas políticas que requieren una mayor recogida de información.

Muchos de estos sitios, como los controles de seguridad de los aeropuertos, nos son familiares y corrientes, aunque la política subyacente es menos clara, como muestra el trabajo de Mark Salter [8].

Algunos sitios son menos obvios. Nuestros cuerpos son asiduamente lugares donde se vigila, como cuando los dispositivos biométricos y los escáneres corporales trabajan para categorizarnos en base a nuestras características físicas. La vigilancia en el puesto de trabajo es también bastante corriente (por ejemplo, monitorizando la actividad de Internet) y las escuelas son cada vez más sitios donde se vigila continuamente (por medio de la grabación de vídeo, del seguimiento electrónico de las asistencias y faltas a clase, etc.), como Torin Monahan y sus colegas han demostrado [9].

La observación en sitios públicos se está convirtiendo en la norma en nuestras ciudades, especialmente cuando la tecnología para controlar estos espacios se hace más barata y más fácil de usar. Y durante las protestas y grandes aglomeraciones la vigilancia pública se suele intensificar con el propósito de

> "El hecho de que todas nuestras acciones en la sociedad actual generen datos sobre estas acciones o interacciones, es grano para el molino de la '*dataveillance*'"

controlar a las masas y para reforzar la ley, como durante los recientes movimientos de ocupación. Identificar la diferencia entre espacios públicos y privados y los correspondientes derechos de los individuos ha sido durante mucho tiempo polémico, pero los nuevos límites en nuestras vidas y los nuevos espacios que creamos dan lugar a nuevas reglas y dominios.

A pesar de su predominio, la vigilancia no se distribuye por igual en toda la sociedad. Algunos grupos son más fáciles de controlar que otros. Por ejemplo, John Gilliom ha documentado cómo los pobres (ha estudiado a madres de los Apalaches con bajos ingresos) están desproporcionadamente sujetos al seguimiento del Estado [10]. Podemos valorar el deber público del Estado de prevenir el fraude en los beneficios sociales y otras acciones indeseables, pero no podemos perder de vista la posible privación de derechos políticos y económicos que pueden derivar de un mayor control. Por lo tanto, debemos examinar críticamente cómo se distribuyen los lugares donde se vigila para ver cómo afecta esto a una potencial sociedad abierta y equitativa.
El seguimiento *online* (o 'cíbervigilancia') proporciona un giro interesante en la idea de "espacios" para la vigilancia. La medida en que el cíberespacio es realmente un espacio es discutible [11], pero lo cierto es que la vigilancia *online* es galopante.

Tanto las redes de Internet como las de los móviles se prestan al seguimiento y la recopilación de una amplia información. En principio, el seguimiento en línea tuvo un objetivo comercial durante muchos años, impulsado sobre todo por el deseo de limitar el acceso a contenidos basados en la ubicación del usuario y de entregar publicidad. Sin embargo, recientemente la vigilancia política *online* se ha intensificado, siendo el más reciente y poderoso ejemplo la Primavera Árabe. Las actividades disidentes se organizaron *online* y los gobiernos amenazados intentaron desesperadamente identificar a los involucrados.

La cibervigilancia también altera la dinámica socio-económica de la privacidad. Los beneficiarios de prestaciones sociales de Gilliom fueron vigilados de forma desmesurada por organismos del Estado, pero las economías de escala para la vigilancia en línea y sobre redes de telefonía móvil hacen muy fácil identificar, clasificar y discriminar a todo el mundo que está conectado. Mucho se ha dicho sobre la capacidad democratizadora de las tecnologías de la información y la comunicación. Sin embargo, poco se ha discutido sobre cómo Internet y otras tecnologías relacionadas democratizan la vigilancia en sí misma.

6. Formas de vigilancia

El cómo de la vigilancia es además complejo. Estas son sus diferentes formas.

Cuando nos hablan de la vigilancia, muchos pensamos en la monitorización visual. El Gran Hermano de Orwell en *1984* estaba siempre observando, y esa idea ha quedado asociada. Aunque el seguimiento visual es sin duda una importante forma de vigilar, no es el único del que deberíamos preocuparnos. Ahora lo que es observable no es necesario que sea visual. La "*Dataveillance*" es un desafío creciente. Roger Clarke creó el término para describir "la vigilancia sistemática de acciones o comunicaciones de las personas a través del uso de tecnologías de la información" [12].

El hecho de que todas nuestras acciones en la sociedad actual generen datos sobre estas acciones o interacciones, es grano para el molino de la '*dataveillance*'. Y estos datos emergentes pueden decir más que la actividad misma. Una cámara de CCTV solitaria puede capturar tu ubicación en un momento determinado, y lo que observe puede revelar lo que quieres compartir, sin embargo la grabación y registros de tus comunicaciones pueden potencialmente mostrar una gama de información sensible sobre tu vida (con quién hablas, cuándo, posiblemente dónde, y todo durante un largo período de tiempo [13]), a cualquiera que pueda acceder a ellos.

El seguimiento de la ubicación [14] también es cada vez más importante. Los teléfonos móviles modernos son un buen ejemplo de una tecnología de control de localización. Tras revelaciones sobre el seguimiento oculto de la ubicación de los usuarios [15], esta forma de vigilancia se ha convertido en una preocupación importante para los políticos (ver más abajo). Los académicos están comenzando a determinar los aspectos relacionados con la privacidad del control de la ubicación, lo que muestra cuán rápidamente evolucionan estas cuestiones.

La biometría automáticamente identifica o verifica a la gente, en base a características de sus cuerpos. Las tecnologías y técnicas biométricas incluyen el reconocimiento facial, el escaneo del iris del ojo, las huellas digitales y los perfiles de ADN, por citar unas cuantas.

En *Our Biometric Future* ("Nuestro futuro biométrico"), Kelly Gates explica por qué las tecnologías de reconocimiento facial fueron consideradas como una solución al problema del terrorismo internacional después de los atentados del 11 de septiembre de 2001, y explora lo que se tuvo que descartar o minimizar de la tecnología para que pudiera ser considerada como una solución de seguridad adecuada a los complejos y multifacéticos retos de la lucha contra el terrorismo [16]. La creencia generalizada de que nuestra verdadera identidad se encuentra en nuestro cuerpo significa que esta forma de control, con toda probabilidad, continuará expandiéndose.

Dejando opiniones comunes a un lado, el simple hecho es que ninguna de estas formas ofrece información perfecta sobre una persona. Cada una sólo posibilita una comprensión parcial y limitada de nuestras identidades, relaciones, paradero, comunicaciones y así sucesivamente, dependiendo de qué información se recopila y cuán precisa pueda ser por la forma en que se consigue. de cualquier manera, los organismos e industrias que impulsan nuevas innovaciones en vigilancia se esfuerzan en reducir estas limitaciones, con el objetivo final (pero no imposible) de conseguir un seguimiento perfecto, omnipresente, y que lo abarque todo.

7. Subjetividades de la vigilancia

Sin embargo, la vigilancia no necesita ser perfecta para ser efectiva. Incluso un seguimiento imperfecto puede ser una herramienta de control social, porque tiende a dar lugar a la autocensura y la inhibición del comportamiento. Esta es una de las más importantes ideas sobre el seguimiento, primero insinuada por Jeremy Bentham y posteriormente desarrollada por Foucault.

El Panopticon de Bentham fue una prisión diseñada de modo que un guardia pudiera vigilar a todos los internos sin que ellos supieran si estaban siendo observados (ver **figura 1**). La mera posibilidad de ser espiados se pensó que sería suficiente para condicionar el buen comportamiento.

En el Panopticon, no es que los que no tengan nada que ocultar no tengan nada de qué temer, sino que los presos tienen que temer

> "Lo fundamental es desafiar la dinámica de poder inherente a la vigilancia para forzar la transparencia en las organizaciones que la llevan a cabo"

de todo porque no tienen manera de ocultar nada. Por lo tanto, controlan su conducta por sí mismos, creando una sociedad normalizada sin coacción física.

En '*Discipline and Punish: The Birth of the Prison*' ("Vigilar y castigar: El nacimiento de la prisión"), Foucault extendía el postulado de Bentham a toda la sociedad, que él creía disciplinaria por naturaleza. Para Foucault, no sólo las cárceles normalizan nuestro comportamiento, sino casi todas las instituciones [17]. La mera posibilidad de ser observado es suficiente para cambiar el comportamiento. Como el periodista disidente libio Khaled Mehiri comentó tras la caída de Gaddafi: "sólo la vigilancia basta para aterrorizar a la gente" [18].

8. Economías políticas de la vigilancia

Una y otra vez, hemos visto empresas privadas surgir como principales impulsores de innovaciones en la vigilancia y la privacidad. Las economías políticas de la vigilancia son así objeto de análisis: ¿qué modelos de negocio necesitan una ingente cantidad de información personal, y cómo estos modelos de negocio respetan a la privacidad? ¿Hay una relación de seguridad militar o estatal entre los medios y motivaciones de la vigilancia? ¿Qué empresas fabrican y venden equipos y software de seguimiento? Esta lista es interminable.

El caso de los drones, aviones no tripulados de vigilancia [19], proporciona un magnífico ejemplo de las cuestiones que están en juego. Estos vehículos aéreos no tripulados (UAV, *Unmanned Aerial Vehicles*) fueron diseñados originalmente por los militares de EE.UU. para el reconocimiento de campos de batalla. Sin embargo, desde entonces han sido desplegados en otros contextos, como a lo largo de las fronteras mexicana y canadiense [20]. E incluso la policía británica ha mostrado interés en utilizarlos internamente, para controlar a los conductores, a manifestantes y la descargas de escombros en lugares no autorizados [21].

Este fenómeno (conocido como 'desbordamiento' en la literatura [22]) es el proceso por el cual las tecnologías adoptadas para un objetivo son reutilizadas posteriormente para lograr otros propósitos políticos.

Las empresas de tecnología de vigilancia suelen operar y comerciar en secreto; ha sido difícil discernir la escala de la industria y los tipos de tecnologías que ofrecen a las agencias policiales y de inteligencia, dificultando la rigurosa investigación científica en esta área.

Sin embargo, investigadores y activistas han comenzado a penetrar en las reuniones secretas y en los lugares en que estos acuerdos se realizan y posteriormente han empezado a revelar este comercio. Queda mucho trabajo por hacer antes de que esta oscura industria y sus operaciones se comprendan.

9. Regulación y gobierno

La regulación y el control de la privacidad y la vigilancia es casi uniforme [23]. Muchos países ofrecen garantías constitucionales de la privacidad. Algunos otros no. También hay naciones que tienen leyes para controlar la obtención estatal y comercial de datos personales, y su uso posterior. Otras no lo hacen [24].

Ciertas jurisdicciones observan un acceso gubernamental regido por leyes a ciertos tipos de datos de comunicaciones, así como regulaciones para "interceptación legal": las circunstancias bajo las cuales está legalmente permitido interceptar comunicaciones. Leyes específicas también pueden regular ciertas clases de datos (por ejemplo, sobre salud, datos financieros, o información biométrica).

Un problema con las leyes sobre privacidad y vigilancia es que suelen quedar obsoletas poco después de entrar en vigor, al evolucionar tan rápidamente las tecnologías y la innovación. Incluso donde existen importantes leyes, éstas no se pueden hacer cumplir.

En general, para que estas leyes se cumplan se necesita de un organismo específico en temas de privacidad, protección de datos o vigilancia que supervise su aplicación, y algunos países (incluso aquellos con leyes de privacidad) no han establecido dichas autoridades. Donde estas agencias existen suelen ser insuficientes o ineficaces.

Muchas jurisdicciones están respondiendo a llamamientos para que se legisle sobre la privacidad, pero los defensores de la privacidad deben cuidarse de la llamada 'política de blanqueo', un fenómeno que Gus Hosein ha examinado en profundidad [25].

Los países sin políticas nacionales o normas para proteger la intimidad o limitar los poderes de la vigilancia copian a veces defectuosas o ineficaces leyes desde otras jurisdicciones, así como sus efectos. Otra oportunidad para

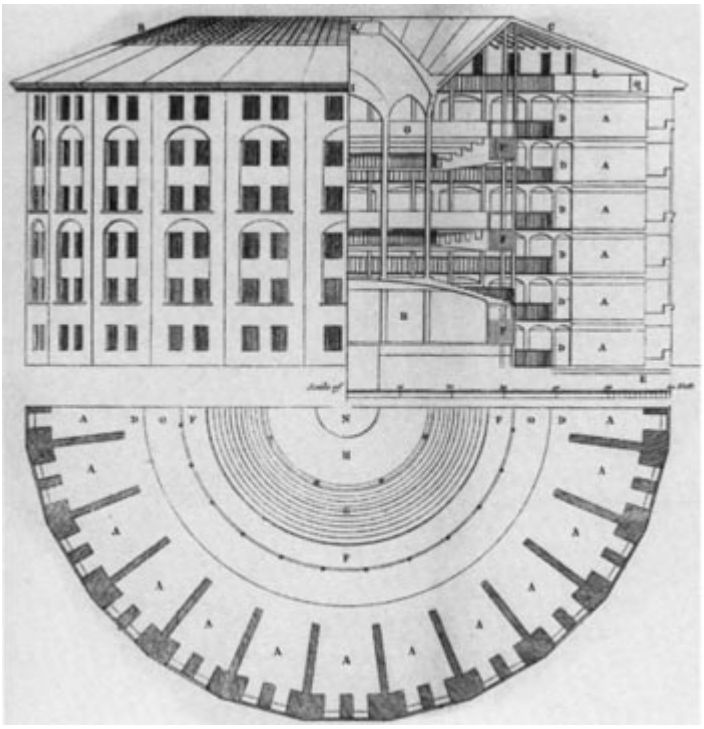

Figura 1. Plano del Panopticon, la prisión ideada por Jeremy Bentham.

> "La difusión generalizada de las PET's marcaría un hito importante en el avance de la privacidad, pero hasta la fecha sólo una pequeña minoría de usuarios hace uso de ellas"

Figura 2. Diferentes maneras de aplicar maquillaje para distorsionar nuestra apariencia.

sus defensores implica luchar por garantías constitucionales más fuertes para la intimidad, lo que ofrecerá una protección ante las tímidas o ineficaces leyes que se establezcan.

10. Resistencia

Entre las ideas más creativas de resistencia a la vigilancia está el concepto de '*sousveillance*' propuesto por Steve Mann [26]. La '*sousveillance*', o contravigilancia, invierte el seguimiento para fijar la mirada en las organizaciones que participan normalmente en asuntos de vigilancia. Lo fundamental es desafiar la dinámica de poder inherente a la vigilancia para forzar la transparencia en las organizaciones que la llevan a cabo.

Una popular manifestación de la contravigilancia es el uso ciudadano de los teléfonos móviles con cámara para capturar la brutalidad policial, como ocurrió en el año 2009 en el BART[2] durante el abatimiento por disparos de la policía de Oscar Grant en Oakland, California[3].

Otro proyecto interesante de resistencia consiste en el '*hacking*' de los sistemas de reconocimiento facial mediante el uso de maquillajes y accesorios para impedir que los algoritmos reconozcan los rostros. Adam Harvey descubrió que los sistemas de detección facial pueden confundirse aplicando maquillaje en ciertas partes de la cara (ver **figura 2**) [27]. Al distorsionar nuestro aspecto recuperamos la capacidad de resistir a la vigilancia y proteger así nuestra privacidad, si así lo queremos.

Junto a otros investigadores hemos explorado las redes de resistencia que emergen ante los proyectos de vigilancia. Mientras que la mayoría de la literatura académica sobre seguimiento se centra en las relaciones de oposición entre el observador y el observado, vemos que hay diferentes maneras de entender el qué y el cómo de la resistencia para la elaboración de un marco multilateral para comprender mejor las complejas relaciones de rebeldía que surgen en contextos locales [28].

11. Diseño de tecnologías de privacidad

El objetivo de Harvey se puede clasificar como un proyecto de tecnologías de "protección de la privacidad" en que se pretende usar herramientas (en este caso, tecnologías no informativas como el maquillaje y el uso de gafas) para impedir el reconocimiento facial. En general, las tecnologías de protección o de mejora de la privacidad (*Privacy-Enhancing Technologies*, PET) ofrecen medios técnicos para combatir la vigilancia aumentando el control de las personas sobre sus datos personales, reduciendo al mínimo la información revelada a empresas privadas y al Estado, haciendo que el tratamiento de datos que no respetan la privacidad sea más transparente y convirtiendo en anónimas las comunicaciones entre las partes.

En la creación de sus herramientas, los diseñadores de PET's están activamente impugnando y luchando contra las políticas y los valores que Nissenbaum y Howe sostienen que se hallan incorporados en los sistemas de vigilancia [29].

Ejemplos reales de éxito de PET's incluyen utilidades como **Tor**, que proporciona un medio seguro para navegar por Internet y comunicarse privadamente, y **Ghostery**, un *plug-in* para navegadores que muestra etiquetas de rastreo, balizas web, píxeles y señales que están incrustadas en las páginas web. La difusión generalizada de las PET's marcaría un hito importante en el avance de la privacidad, pero hasta la fecha sólo una pequeña minoría de usuarios hace uso de ellas; Hay una alta probabilidad de que usted no las emplee, y es casi seguro que su abuela no lo hará.

Así, el auténtico desafío es conseguirlas integradas en las infraestructuras. ¿Por qué no los principios que subyacen en Tor pueden incorporarse en los *routers* de acceso a Internet? ¿O los principios de protección de la intimidad y la identidad [30] subyacentes en las Leyes de identidad de Kim Cameron [31] integrarse en tarjetas nacionales de identidad? Podría deberse a lo complejo de estas técnicas, o quizás porque hay un interés comercial y de seguridad nacional en garantizar sistemas que dividan, identifiquen y revelen.

12. Identidad, seudónimos y anonimato

Una de las batallas más importantes de la privacidad es la continua lucha sobre las políticas de identidad *online*. Durante años fue posible el uso de Internet de forma anónima, pero el aumento del acoso en línea, las preocupaciones sociales sobre los pedófilos que engañan y acechan a los niños en los *chat*, y los temores exagerados a los terroristas que pueden usar Internet para planificar ataques han dado lugar a que los usuarios sean rastreables e identificables *online* en todo momento.

De esta creencia han surgido las llamadas *nymwars*. Por un lado, están los proveedores de servicios *online*, las redes sociales e incluso webs de videojuegos como Blizzard (creadores del World of Warcraft [32]) que insisten en que la gente utilice sus nombres "reales" como hacen en sitios como Google +. Por otro lado, están los académicos, defensores y activistas que sostienen que hay muchas razones legítimas para que las personas se reserven el derecho a permanecer en el anonimato o usar seudónimos *online* [33], como los disidentes políticos o cualquier persona que se enfrente a análogas conse-cuencias, para un comportamiento digital aceptable.

El aspecto positivo es que se trata de debates que los académicos han estado planteándose

desde hace años. La lista de lecturas recomendadas es amplia, pero para empezar sugiero el volumen editado de *Lessons from the Identity Trail* [34], y *Global Challenges for Identity Policies* [35], de Whitley y Hosein, que explora cómo la extraña pareja de política y tecnología algunas veces se vincula por la fuerza para hacer frente a los complejos desafíos de la políticas de identidad.

13. Selección, seguimiento y movilidad

Otro campo muy necesitado de participación y promoción es el *targeting* o selección y el rastreo *online*. El uso de tecnologías como las *cookies* de seguimiento en línea es muy frecuente. Pueden ser inofensivas, pero como los servicios gratuitos *online* proliferan, cada vez más sitios y aplicaciones dependen de los ingresos por publicidad sensible al rastreo. Estas empresas recogen mucha información sobre los usuarios para poder enviar publicidad con mayor precisión.

Los usuarios que se sienten incómodos por ser rastreados pueden limitar el número de *cookies* que se instalan en sus ordenadores, pero las redes de publicidad se han vuelto más agresivas en sus acciones apoyándose en nuevas técnicas como las cookies basadas en Flash [36] y otras formas [37] para un seguimiento encubierto pero constante.

En los Estados Unidos y otros países, han habido llamamientos para que se introduzca una legislación que prohíba a las empresas que rastreen a las personas *online* sin su consentimiento, pero queda por ver qué tecnologías apoyarían estas políticas y la eficacia con la que se podrían aplicar estas disposiciones. Se trata de un ecosistema complejo, en el que es difícil ejercer un control total sobre los datos de carácter personal (como la ubicación). Hay numerosos actores involucrados en la recolección y procesado de información, y tal como están las cosas, es difícil distinguir desde dónde están fluyendo nuestros datos y cómo se usan.

De cualquier manera, tanto el *targeting* y el rastreo *online* como la intimidad móvil presentan emocionantes ocasiones para activistas para que se involucren en el diseño de tecnologías (como utilidades de visualización para aumentar la transparencia en los procesos de vigilancia *online*, o a través de herramientas para comunicaciones seguras, como las que la empresa Whisper Systems ha desarrollado para los teléfonos Android) o trabajando para mejorar políticas y reglamentación en este terreno.

El gran desafío está en que como los sistemas de Internet y telefonía móvil se hacen cada vez más estructurados, con intermediarios necesarios (proveedores de acceso a la red), otros terceros (proveedores de hardware, desarrolladores del sistema operativo) y servicios (aplicaciones, navegadores, plataformas), las soluciones fragmentadas resultantes serán en última instancia inútiles.

14. ¿Qué falta?

Algunas áreas de investigación muy interesantes se están alejando inevitablemente de la discusión anterior. El cometido de la vigilancia es uno: ¿qué alimenta la práctica de la videovigilancia y qué papel juegan en el proceso cosas como las emociones [38] y el estrés [39]?

La metodología de la vigilancia es otra vía interesante: ¿cómo podemos medir el seguimiento, tanto cuantitativa como cualitativamente, con el objeto de saber si se intensifica o no?. Y si es así, ¿cómo se producen estos cambios? Kevin Haggerty ha examinado estos interrogantes metodológicos [40].

La historia de las diferentes tecnologías de vigilancia también merece una mayor profundización. La exposición histórica de Simon Cole de métodos de toma de huellas dactilares en medicina forense sirve como un rotundo ejemplo de esta clase de investigación. Muestra cómo la idea que da por sentado que nuestras huellas digitales son únicas (y por tanto capaces de identificar individualmente a las personas) es realmente un artefacto epistemológicamente complejo [41].

¿Y qué hay acerca de los errores en la vigilancia? Con demasiada frecuencia nos fijamos en exitosas políticas y sistemas de seguimiento, pero tendemos a olvidar todos los proyectos que son abandonados, que han fracasado o quedado suspendidos.

¿Hay alguna larga lista de tecnologías para el seguimiento que no lo haya hecho (recuérdese *Total Information Awareness* [42])? ¿Por qué tales proyectos han fallado y cómo algunos planes aparentemente muertos han sido reactivados y después incorporados a nuevas iniciativas (como por ejemplo, las partes de *Total Information Awareness* que todavía siguen activas [43])?

Agradecimientos

Esta guía ha sido financiada con una subvención del programa de información de la *Open Society Foundations*, con las contribuciones intelectuales de Daniel Bernhard, Becky Hogge y Gus Hosein.

Referencias

[1] A. Etzioni. *The Limits Of Privacy*. Nueva York: Basic Books, 1999.
[2] R. B. Siegel. "The Rule of Love": Wife Beating as Prerogative and Privacy. *The Yale Law Journal,* 150(8): pp. 2117-2207, 1996.
[3] S. T. Margulis. On the Status and Contribution of Westin's and Altman's Theories of Privacy. *Journal of Social Issues*, 59(2): pp. 411-429, 2003.
[4] D. J. Solove. A Taxonomy of Privacy. *University of Pennsylvania Law Review*, 154(3): pp. 477-564, 2006.
[5] O. H. Gandy. *Coming to Terms With Chance: Engaging Rational Discrimination and Cumulative Disadvantage*. Burlington: Ashgate, 2009.
[6] D. Lyon. *Surveillance As Social Sorting: Privacy, Risk, and Digital Discrimination*. Londres: Routledge, 2003.
[7] M. Foucault. *The Birth of the Clinic: An Archeology of Medical Perception*. Nueva York: Vintage, 1973.
[8] M. B. Salter (ed.). *Politics at the Airport.* Minneapolis: University of Minnesota Press, 2008.
[9] T. Monahan, R. D. Torres (eds.). *Schools Under Surveillance: Cultures of Control in Public Education*. Nueva Jersey: Rutgers University Press, 2009.
[10] J. Gilliom. *Overseers of the Poor: Surveillance, Resistance, and the Limits of Privacy*. Chicago: University of Chicago Press, 2001.
[11] M. Dodge, R. Kitchin. *Mapping Cyberspace*. Londres: Routledge, 2000.
[12] R. Clarke. Information Technology and Dataveillance. *Communications of the ACM*, 31(5): pp. 498-512. 1998.
[13] A. Escudero-Pascual, I. Hosein. Questioning lawful access to traffic data. *Communications of the ACM*, 47(3): pp. 77-82, 2004.
[14] D. Kravets. Feds Seek Unfettered GPS Surveillance Power as Location-Tracking Flourishes. *Threat Level*, 7 noviembre de 2011: <http://www.wired.com/threatlevel/2011/11/gps-tracking-flourishes/all/1>.
[15] B. X. Chen, M. Isaac. Why You Should Care About the iPhone Location-Tracking Issue. *Gadget Lab*, 22 abril de 2011: <http://www.wired.com/gadgetlab/2011/04/iphone-location>.
[16] K. A. Gates. *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance.* Nueva York: New York University Press, 2011.
[17] M. Foucault. *Discipline & Punish: The Birth of the Prison*. Nueva York: Vintage, 1979.
[18] M. Coker, P. Sonne. Life Under the Gaze of Gadhafi's Spies. *Wall Street Journal.* 14 de diciembre de 2011: <http://online.wsj.com/article/SB10001424052970203764804577056230832805896.html>.
[19] M. R. Calo. The Drone as Privacy Catalyst. *Stanford Law Review Online*, 64: pp. 29-33, 2011.
[20] J. Rayfield. One Nation Under The Drone: The Rising Number Of UAVs In American Skies. *TPM Muckraker*, 22 de diciembre de 2011: <http://tpmmuckraker.talkingpointsmemo.com/2011/12/one_nation_under_the_drone.php>.
[21] P. Lewis. CCTV in the sky: police plan to use military-style spy drones. *The Guardian*, 23 de enero de 2010: <http://www.guardian.co.uk/uk/2010/jan/23/cctv-sky-police-plan-drones>.
[22] T. Monahan, N. A. Palmer. The Emerging Politics of DHS Fusion Centers. *Security Dialogue*, 40(6): pp. 617-636, 2009.

[23] C. J. Bennett, C. D. Raab. *The Governance of Privacy: Policy Instruments in Global Perspective*. Burlington: Ashgate, 2003.
[24] D. Banisar. *National Comprehensive Data Protection/Privacy Laws and Bills 2012 Map*, 2012: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951416>.
[25] I. Hosein. The Sources of Laws: Policy Dynamics in a Digital and Terrorized World. *The Information Society*, 20(3): pp. 187-199, 2004.
[26] S. Mann, J. Nolan, B. Wellman. Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments. *Surveillance & Society*, 1(3): pp. 331-355, 2003.
[27] D. Goodin. Reverse-engineering artist busts face detection tech. *The Register,* 22 de abril de 2010: <http://www.theregister.co.uk/2010/04/22/face_detection_hacking>.
[28] A. K. Martin, R. E. Van Brakel, D. J. Bernhard. Understanding resistance to digital surveillance: Towards a multi-disciplinary, multi-actor framework. *Surveillance & Society*, 6(3): pp. 213-232, 2009.
[29] D. C. Howe, H. Nissenbaum. TrackMeNot: Resisting Surveillance in Web Search. En *Lessons from the Identity Trail: Anonymity, Privacy, and Identity in a Networked Society*. Oxford: Oxford University Press, pp. 417-436, 2009.
[30] S. A. Brands. *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy*. Cambridge: MIT Press, 2000.
[31] K. Cameron. *The Laws of Identity*, 2005: <http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf>.
[32] BBC News. World of Warcraft maker to end anonymous forum logins. *British Broadcasting Corporation,* 7 July 2010: <http://www.bbc.co.uk/news/10543100>.
[33] J. C. York. A Case for Pseudonyms. *Electronic Frontier Foundation,* 29 July 2011: <https://www.eff.org/deeplinks/2011/07/case-pseudonyms>.
[34] I. R. Kerr, V. M. Steeves, C. Lucock (eds.). *Lessons from the Identity Trail: Anonymity, Privacy, and Identity in a Networked Society*. Oxford: Oxford University Press, 2009.
[35] E. A. Whitley, I. Hosein. *Global Challenges for Identity Policies*. London: Palgrave Macmillan, 2009.
[36] A. Soltani, S. Canty, Q. Mayo, L. Thomas, C. J. Hoofnagle. *Flash Cookies and Privacy*, 2009: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862>.
[37] M. Ayenson, D. J. Wambach, A. Soltani, N. Good, C. J. Hoofnagle. *Flash Cookies and Privacy II: Now with HTML5 and eTag Respawning*, 2011: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1898390>.
[38] G. J. D. Smith. Exploring Relations between Watchers and Watched in Control(led) Systems: Strategies and Tactics. *Surveillance & Society*, 4(4): pp. 280-313, 2007.
[39] E. Bumiller. Air Force Drone Operators Report High Levels of Stress. *New York Times,* 18 de diciembre de 2011: <http://www.nytimes.com/2011/12/19/world/asia/air-force-drone-operators-show-high-levels-of-stress.html>.
[40] K. D. Haggerty. Methodology as a Knife Fight: The Process, Politics and Paradox of Evaluating Surveillance. *Critical Criminology*, 17(4): pp. 277-291, 2009.
[41] S. A. Cole. *Suspect Identities: A History of Fingerprinting and Criminal Identification*. Cambridge: Harvard University Press, 2002.
[42] J. Rosen. Total Information Awareness. *New York Times Magazine,* 15 de diciembre de 2002: <http://www.nytimes.com/2002/12/15/magazine/15TOTA.html>.
[43] M. Williams. The Total Information Awareness Project Lives On. *MIT Technology Review*, 26 April 2006: <http://www.technologyreview.com/news/405707/the-total-information-awareness-project-lives-on/>.

Notas

[1] El comunitarismo es una filosofía que enfatiza la relación del individuo con la comunidad <http://es.wikipedia.org/wiki/Pensamiento_comunitario>.
[2] *Bay Area Rapid Transit* (Tráfico Rápido del Área de la Bahía), un sistema de transporte rápido que funciona en la Bahía de San Francisco (California).
[3] <https://en.wikipedia.org/wiki/BART_ Police_shooting_of_Oscar_Grant>.