TOMANDO DECISIONES INTELIGENTES SOBRE VIGILANCIA

UNA GUÍA COMUNITARIA PARA TRANSPARENCIA, RENDICIÓN DE CUENTAS Y SUPERVISIÓN

ACLU DE CALIFORNIA
ABRIL 2016

La vigilancia está aumentando en nuestras comunidades, pero la presencia de la más básica transparencia, supervisión y rendición de cuentas sigue siendo la excepción, no la regla. La policía está gastando miles de millones de dólares en sofisticada e invasiva tecnología de vigilancia, desde lectores de placas hasta monitores de teléfonos celulares, tecnología de reconocimiento facial y vehículos aéreos no tripulados (*drones*). Demasiados de estos programas avanzan sin ser discutidos con la comunidad, sin considerar cuidadosamente el costo y los beneficios y sin establecer políticas adecuadas para evitar su uso indebido y proteger los derechos. Como resultado, la vigilancia permite la creación de perfiles raciales altamente tecnológicos, la perpetuación de los sistemas de abuso policial y socava la confianza en las agencias de la ley, particularmente en las comunidades de color en donde la conducta indebida de la policía ha sido extensa y las relaciones comunitarias han sido tensas. Es hora de un cambio.

Las comunidades deben ser socios equitativos en todas las decisiones relacionadas con el uso de la tecnología de vigilancia. Necesitan saber por qué y cómo se está considerando usar la vigilancia, cuál es su intención y cuál será el costo real, tanto en dólares como en derechos individuales. Necesitan asegurar que toda propuesta incluirá sólidos mecanismos de transparencia, rendición de cuentas y supervisión. Si no es así, la confianza del público puede ser fácilmente deteriorada y las comunidades pueden terminar cargando con sistemas demasiado invasivos, muy costosos y mucho menos efectivos para alcanzar los objetivos de seguridad que inicialmente imaginó la comunidad.

Esta guía establece un marco detallado para plantear las propuestas de vigilancia, evaluar adecuadamente su costo real y establecer políticas que permitan que haya transparencia, supervisión y rendición de cuentas. También incluye un listado de verificación que puede ayudar a los miembros de la comunidad, a los responsables políticos y a los agentes de la ley a hacer las preguntas esenciales y a encontrar respuestas sobre las propuestas de vigilancia e incluye docenas de casos de estudio que resaltan enfoques inteligentes y errores que se deben evitar. Esta guía concluye con un ejemplo del tipo de contenido que los responsables políticos pueden adoptar para asegurar que se aplique el proceso correcto cada vez que se considere una propuesta de vigilancia.

Esperamos que encuentre útiles este documento y sus materiales de apoyo (disponibles en línea en **aclunc.org/smartaboutsurveillance**) y que ayuden a su comunidad a tomar decisiones informadas sobre la vigilancia.

Nicole A. Ozer
Directora de Tecnología y Libertades Civiles
ACLU de California

Peter Bibring
Director de Prácticas Políticas
ACLU de California

CONTENIDO

Autores: Chris Conley, Matt Cagle, Peter Bibring, Jessica Farris, Linda Lye, Mitra Ebadolahi y Nicole Ozer de la ACLU de California

Escritores colaboradores: Addison Litton y Thomas Mann Miller

Diseño y diagramación: Gigi Pandian y Daniela Bernstein

Esta publicación fue publicada con el apoyo de la Fundación ACLU y de los generosos donantes y miembros de la ACLU.

PUBLICADO POR LA ACLU DE CALIFORNIA
SEGUNDA EDICIÓN — ABRIL 2016

DESCRIPCIÓN DE LA TECNOLOGÍA

LECTORES AUTOMÁTICOS DE PLACAS VEHICULARES (ALPR, por sus siglas en inglés): sofisticados sistemas de cámaras instalados en los vehículos policiales o en postes de luz que escanean las placas vehiculares cuando están a la vista. Con frecuencia se usan para ubicar vehículos de interés, como automóviles robados, pero en el proceso pueden registrar la hora a la que pasa cada vehículo en un área específica.

CÁMARAS CORPORALES: pequeñas cámaras que usa la policía para grabar audio y video. Estas cámaras pueden grabar desde las interacciones usuales del público con la policía hasta sonidos o imágenes durante mítines políticos o incluso bromas lascivas en el auto patrulla. Algunas cámaras corporales están siempre encendidas y otras son controladas por el oficial de policía.

DRONES: vehículos aéreos no tripulados que pueden estar equipados con cámaras, micrófonos y otros sensores o dispositivos. Los drones pueden ser desde pequeños "cuadricópteros" que pueden volar desde cerca del suelo hasta tan alto como los aviones con cámaras extremadamente poderosas. Los drones con frecuencia son más silenciosos que los vehículos aéreos tradicionales haciendo que sea fácil usarlos para vigilar de forma encubierta.

VIDEOVIGILANCIA: sistema de cámaras que permite observar o grabar remotamente las actividades en espacios públicos. La transmisión puede ser monitoreada activamente con la intención de detectar delitos cuando ocurren o grabarlos para usar la grabación en investigaciones y casos penales potenciales. Los estudios han demostrado continuamente que las cámaras son costosas y su eficacia es limitada para evitar y resolver delitos graves.

RECONOCIMIENTO FACIAL: programas informáticos que identifican a una persona en fotografías o videos en base a varias características del rostro de la persona. La precisión del programa de reconocimiento facial puede variar enormemente.

RASTREO DE LA UBICACIÓN: diversas técnicas que se usan para rastrear de forma remota la ubicación de una persona. Dispositivos GPS (siglas en inglés de Sistema de Posicionamiento Global) que van desde modernos teléfonos celulares hasta "dardos" que pueden ser disparados hacia un automóvil en movimiento, determinan su propia ubicación usando señales satelitales. Los dispositivos electrónicos de comunicación, incluyendo teléfonos celulares, pueden ser rastreados identificando las torres de telefonía celular o las redes inalámbricas que usa el dispositivo. La información de la ubicación está disponible en pocos segundos y su precisión es de unos cuantos pies.

MONITOREO AUTOMATICO DE LAS REDES SOCIALES: herramientas informáticas que recopilan mensajes y otra información en plataformas sociales como Twitter y Facebook. Estas herramientas también pueden analizar la información recopilada para obtener información como conexiones sociales u opiniones políticas.

RECEPTOR DE IDENTIDAD DE SUSCRIPTORES MÓVILES INTERNACIONALES ("IMSI"): dispositivo que imita a una torre de telefonía celular para interactuar con los teléfonos cercanos. Los receptores IMSI, usualmente llamados *Stingrays* (la marca de uno de estos dispositivos), identifican a los dispositivos cercanos y pueden ser configurados para interceptar y capturar el contenido de las comunicaciones, incluyendo llamadas telefónicas, mensajes de texto o

actividad en internet. Muchos receptores IMSI operan de forma generalizada recopilando la información de todos los teléfonos que estén dentro de su rango.

EXTRACCIÓN DE INFORMACIÓN: técnicas para descubrir patrones estadísticos, tendencias y otros datos en la información recopilada. Por ejemplo, analizar las conexiones en las redes sociales puede revelar información secreta y confidencial como la orientación sexual de una persona.

PREGUNTAS CLAVE QUE SE DEBEN RESPONDER ANTES DE ADOPTAR UNA PROPUESTA DE VIGILANCIA

¿POR QUÉ ESTÁN CONSIDERANDO USAR LA VIGILANCIA?

- ¿Qué problema específico está tratando de solucionar en la comunidad?
- ¿Qué tan efectiva será la vigilancia para abordar este problema?
- ¿Existen alternativas más efectivas, menos costosas y que tengan menos impacto sobre las libertades civiles?

¿CUÁLES SON LOS COSTOS Y LOS RIESGOS?

- ¿Cuál es el costo económico de la vigilancia, incluyendo capacitación, operación y mantenimiento a largo plazo?
- ¿Qué impacto tendrá la vigilancia en la privacidad, la libertad de expresión y los derechos civiles?
- ¿Cómo puede afectar la vigilancia la confianza en las agencias de la ley?
- ¿Se ha redactado un Informe de Impacto de la Vigilancia?

¿PARTICIPÓ LA COMUNIDAD EN LA EVALUACIÓN DE LA PROPUESTA DESDE EL PRINCIPIO?

- ¿Se solicitó la opinión de todos los segmentos de la comunidad sobre las prioridades, los costos y los riesgos?
- ¿Se publicaron el Informe de Impacto de la Vigilancia y la Política de Uso de la Vigilancia para que la comunidad pueda evaluarlos?
- ¿Se realizarán audiencias y debates públicos antes de solicitar fondos o adquirir la tecnología?

¿ES EL USO DE LA VIGILANCIA LA DECISIÓN CORRECTA?

- ¿Evaluaron los responsables políticos el Informe de Impacto de la Vigilancia y la Política de Uso de la Vigilancia? ¿Tuvieron la oportunidad de escuchar las inquietudes del público?
- ¿Votarán los responsables políticos locales específicamente para aprobar el proyecto? ¿Ocurrirá esto antes de solicitar fondos o comprar tecnología?
- ¿Reevaluará la comunidad los programas de vigilancia cada año y determinará si deben continuar, ser modificados o ser abandonados?

¿SE RESPONDERÁN ESTAS PREGUNTAS EN CADA CASO INDIVIDUAL?

¿Aprobó la comunidad una Ordenanza de Vigilancia y Seguridad Comunitaria para asegurar que estas preguntas sean hechas y respondidas de forma consistente cada vez que se considera el uso de tecnología y asegurar que haya adecuada transparencia, supervisión y rendición de cuentas?

Por qué es importante: costos y consecuencias de la vigilancia

La tecnología de vigilancia a menudo es propuesta como una herramienta eficaz para mejorar la seguridad pública. Pero con demasiada frecuencia las propuestas ignoran no solo el verdadero costo económico de la tecnología de vigilancia, sino también el potencial de violar los derechos civiles y socavar la confianza pública y las prácticas policivas eficaces. Las comunidades deben identificar y evaluar todos los efectos nocivos y costos de la vigilancia lo más temprano posible del proceso de consideración para determinar si seguir adelante con la tecnología de vigilancia es verdaderamente la decisión correcta.

A. IMPACTO DE LA VIGILANCIA EN LOS DERECHOS CIVILES Y EN LA CONFIANZA DE LA COMUNIDAD

La comunidad general puede pagar un alto precio si se adquiere y utiliza la tecnología de vigilancia sin evaluar su impacto sobre los derechos civiles y su potencial de abuso. La vigilancia puede fácilmente afectar los derechos individuales de los residentes y visitantes, perpetuar las prácticas policivas discriminatorias o afectar la libertad de expresión, de asociación y de religión (libertades que los funcionarios públicos han jurado proteger).[1] Como resultado, la vigilancia puede socavar la confianza en las autoridades haciendo que sea más difícil que los oficiales y los miembros de la comunidad colaboren para mantener a la comunidad segura.

"Los programas de vigilancia perpetúan la larga trayectoria de la policía de enfocarse en las personas afroamericanas y en otros grupos minoritarios… Necesitamos un futuro en una ciudad en la que nuestro departamento de policía y otras instituciones públicas estén sujetos a una verdadera supervisión comunitaria y rindan cuentas de sus actos." Reverendo B.T. Lewis y Taymah Jahsi, organizadores de Faith in Community in Fresno[2]

1. LA VIGILANCIA PUEDE AFECTAR LOS DERECHOS DE LOS MIEMBROS DE LA COMUNIDAD

El costo más grande de la tecnología de vigilancia puede no ser económico, sino personal: la invasión y violación de los derechos civiles. Varios tipos de tecnología de vigilancia son capaces de capturar y guardar grandes cantidades de información de los miembros de la comunidad y de sus visitantes, como los mítines políticos y servicios religiosos a los que asisten, los servicios de salud que usan, las parejas románticas que tienen y mucho más. Tan solo la posibilidad de ser vigilado tiene el potencial de afectar a los miembros de la comunidad disuadiéndolos de participar en actividades políticas, oponerse a la conducta indebida de la policía, considerar sus opciones reproductivas, explorar su sexualidad y participar en otras actividades que están claramente protegidas por la Constitución federal y la Constitución de California. Con demasiada frecuencia, esta percepción se basa en hechos, tal como demuestra el uso de Fresno de programas para monitorear las redes sociales que identificaron a la etiqueta "#blacklivesmatter" como un indicador de actividad criminal.[3]

El documento *Principios de derechos civiles en la era de macrodatos* que fue firmado por catorce de los principales grupos de derechos civiles y humanos de la nación, resalta cómo la tecnología de vigilancia con frecuencia afecta desproporcionadamente a las comunidades de color y a las minorías religiosas y étnicas. Solicita que la tecnología sea "diseñada y usada en formas que respeten los valores de igualdad de oportunidades e igualdad de justicia" e insta a los usuarios a "dejar de usar alta tecnología para la creación de perfiles" y "preservar los principios constitucionales". El documento también solicita que la

policía use órdenes judiciales y tenga otros tipos de supervisión independiente y "claras limitaciones y sólidos mecanismos de auditoría para asegurar que, si estas herramientas son usadas, se haga de una forma responsable y equitativa."[4]

Hay muchos ejemplos de vigilancia indebida basada en la raza, la etnia, las asociaciones o las actividades religiosas o políticas de una persona. La policía de Santa Clara usó un dispositivo GPS para monitorear a un estudiante debido al vínculo de su padre con una asociación de la comunidad musulmana.[5] La policía de Michigan solicitó "información sobre todos los teléfonos celulares congregados en un área en donde se esperaba que ocurriera una protesta sindical".[6] La Agencia de Seguridad Nacional (NSA, por sus siglas en inglés) monitoreó específicamente a varios musulmanes-estadounidenses prominentes a pesar de que no existía ninguna evidencia de conductas indebidas.[7] En Gran Bretaña, en donde la vigilancia es generalizada, un estudio del Parlamento Europeo reveló que "los jóvenes, los hombres y las personas de raza negra son vigiladas de forma sistemática y desproporcionada no debido a su participación en delitos o disturbios, sino debido a "razones que no eran obvias".[8]

Los programas de vigilancia que no se enfocan en individuos específicos pueden ser particularmente problemáticos. Monitorear a grupos enteros de comunidades extiende la "culpabilidad por asociación" a quienes no han hecho nada malo, disuade a las personas de participar en actividades locales y aísla a los miembros de la comunidad. Además, cuando los miembros del grupo son contaminados por estas sospechas, es fácil justificar entrometerse en sus vidas privadas o incluso amenazarlos con peores consecuencias si no cooperan con iniciativas de vigilancia adicionales.[9]

VIGILANCIA DE ACTIVISTAS POLÍTICOS Y SOCIALES

El gobierno tiene una larga y problemática historia de abusar de su poder para vigilar a los activistas políticos y sociales. Desde los "Escuadrones Rojos" de principios del Siglo 20 y los esfuerzos del FBI de infiltrar y desacreditar a los activistas que luchaban contra la guerra y a favor de los derechos civiles en la década de los sesenta hasta la reciente vigilancia del movimiento Black Lives Matter.

- El Departamento de Seguridad Nacional monitoreó las cuentas en las redes sociales de los miembros de Black Lives Matter y recopilaron detalles de la ubicación de los miembros y de los planes de protestas pacíficas en Ferguson, Baltimore y la Ciudad de Nueva York. Esto hizo que muchos cuestionaran por qué el DHS, que fue creado para combatir el terrorismo, estaba vigilando un pacífico movimiento doméstico de justicia social.[10]

- La policía de Fresno en California adquirió y probó secretamente varias herramientas de vigilancia en las redes sociales para rastrear etiquetas (*hashtags*) como #BlackLivesMatter, #dontshoot y #wewantjustice y asignó a cada persona un "grado de amenaza". Esto resultó en atención negativa por parte de la prensa nacional e hizo que los miembros de la comunidad solicitaran reformas lo que obligó al jefe de policía a disculparse públicamente.[11]

- Los funcionarios del Departamento de Justicia de Oregón fueron criticados cuando revelaron que un investigador había usado programas para monitorear etiquetas en las redes sociales,

> incluyendo #BlackLivesMatter, lo que identificó a defensores de los derechos civiles, incluyendo al presidente de la Liga Urbana de Portland. La historia hizo que el fiscal general de Oregón se disculpara públicamente y que se realizara una investigación interna.[12]

> Reformas a la forma cómo se recopila inteligencia debido a demandas y pesquisas de los congresistas han hecho que muchas agencias de la ley prohíban la recopilación de información sobre activismo político y otras actividades protegidas por la Primera Enmienda si no existe sospecha justificada de actividades criminales. Pero el monitoreo de *Black Lives Matter* demuestra que aún existe la necesidad de restricciones similares en el uso de tecnología de vigilancia para asegurar que no se use para afectar o socavar el activismo social y político.

La vigilancia estratégica con frecuencia se enfoca en las comunidades de color. Por ejemplo, en Oakland, la policía ha usado desproporcionadamente lectores de placas vehiculares en los vecindarios afroamericanos y latinos.[13] En Compton, la policía hizo sobrevolar durante semanas un avión equipado con cámaras de vigilancia de alto poder sin el conocimiento o consentimiento del público.[14] Como involucra la recopilación de grandes cantidades de información, la vigilancia estratégica también crea el potencial de cometer todo tipo de abusos, desde el monitoreo de parejas románticas por parte de los analistas de la NSA[15] hasta el chantaje de los parroquianos de un bar *gay* por parte de un teniente de la policía de D.C.[16]

> "Una de las partes más alarmantes de esta historia, ha sido la forma cómo se ha usado la vigilancia contra las personas negras que abogan por justicia. Se ha usado para desacreditar, abusar y encarcelar." Opal Tometi, cofundadora de Black Lives Matter[17]

> "Quienes crecimos en comunidades marginadas vivimos en un entorno que fue moldeado por la vigilancia que ha sido usado para fortalecer el sistema de justicia penal y aumentar las deportaciones…" Steven Renderos, Center for Media Justice[18]

La vigilancia conlleva amenazas a la privacidad y a la libertad de expresión incluso si se realiza únicamente en lugares públicos. Esto es particularmente cierto cuando la información que se obtiene a través de esta vigilancia se combina para crear un robusto perfil que puede "revelar mucho más en combinación que como información aislada."[19] Tal como mencionó Sonia Sotomayor, juez de la Corte Suprema de Justicia, "un registro preciso y exhaustivo de los movimientos públicos de una persona… refleja muchos detalles sobre sus afiliaciones familiares, políticas, profesionales, religiosas y sexuales". Además, "saber que el Gobierno puede estar observándonos afecta negativamente las libertades de asociación y de expresión."[20]

B. *LA VIGILANCIA PUEDE SOCAVAR LA CONFIANZA EN LAS AGENCIAS DE LA LEY*

Cuando las autoridades explican claramente el impacto que tiene la vigilancia a los miembros de la comunidad –o lo que es peor, eluden por completo el proceso democrático adquiriendo y usando tecnología de vigilancia sin discutirlo con el público– se erosiona la confianza aún más haciendo que sea más difícil para los oficiales de policía trabajar con la comunidad para solucionar delitos y proteger la seguridad pública.

Después de los ataques del 11 de septiembre, el Departamento de Policía de Nueva York creo una división secreta de inteligencia que infiltró los vecindarios musulmanes con oficiales encubiertos para monitorear la

vida diaria y crear informes sobre la participación de los musulmanes-estadounidenses en actividades protegidas por la Constitución en cafés, bibliotecas y residencias privadas sin que hubiera evidencia de actividades ilegales.[21] Estas actividades afectaron grandemente la confianza de la comunidad en las agencias de la ley y terminaron en varios años de procesos legales, en un acuerdo que prohibió que el NYPD realizara investigaciones basadas en la raza, religión o etnia de una persona y ordenó la implementación de una serie de reformas diseñadas para evitar la vigilancia no justificada.

"Las secuelas de la vigilancia en las comunidades musulmanas de Nueva York han sido devastadoras… Los vínculos de los miembros de la comunidad con las delegaciones policiales locales se han deteriorado debido a la desconfianza y el temor." Hina Shamsi, directora del Proyecto de Seguridad Nacional de la ACLU[22]

En Compton se difundieron las noticias de la existencia de un programa de vigilancia aérea que observaba a toda la comunidad y que el Departamento del Alguacil mantuvo en secreto para evitar que el público se quejara de la violación a sus derechos civiles. Tanto ciudadanos como legisladores se quejaron porque no habían sido informados del uso de esta invasiva vigilancia. Los enojados miembros de la comunidad se preguntaban con razón, "¿por qué somos blanco de esta vigilancia? Como ciudadanos merecemos [saber] que se está usando. No todos somos criminales… Es una invasión a nuestra privacidad". El alcalde solicitó una "política para proteger la privacidad de los ciudadanos" para asegurar que la comunidad sea notificada antes de que se despliegue o utilice cualquier nuevo equipo de vigilancia.[23]

B. LA VIGILANCIA TIENE COSTOS INMEDIATOS Y CONTINUOS

Además del costo para los derechos y las libertades civiles, el impacto fiscal de la vigilancia puede ser extenso. Modificar la infraestructura actual, operar y mantener los sistemas y entrenar al personal puede consumir limitado tiempo y dinero, incluso cuando subsidios federales o estatales financian el costo inicial. Las tecnologías de vigilancia pueden también fracasar o ser mal utilizadas lo que puede terminar en costosas demandas. Para calcular el costo económico total de la tecnología de vigilancia, las comunidades deben mirar más allá del costo inicial.

1. LA VIGILANCIA REQUIERE INFRAESTRUCTURA, PERSONAL, ENTRENAMIENTO Y MANTENIMIENTO

"Al considerar el uso de nueva tecnología, es importante evaluar no solo el costo inicial sino también el costo del mantenimiento y de las mejoras que se necesitarán más adelante." Capitán Michael Grinstead, Departamento de Policía de Newport News (VA)[24]

El costo oculto de la infraestructura, el entrenamiento y la adquisición de personal, la operación y el mantenimiento y el potencial de exceder el presupuesto pueden eclipsar el costo de adquirir la tecnología de vigilancia. Las comunidades que no calcularon correctamente el verdadero costo económico de un sistema de vigilancia han tenido que hacer frente a masivos excedentes y han terminado con programas que no cumplen con el propósito inicial. Por ejemplo, Filadelfia tenía planificado gastar $651,672 en un programa de videovigilancia que incluía 216 cámaras, pero después de un año habían gastado $13.9 millones en el proyecto y tenían solo 102 cámaras funcionales, algo que el contralor de la ciudad describió como "excesivamente alarmante y totalmente excesivo, especialmente porque $13.9 millones equivale al costo de añadir 200 nuevos policías a nuestras calles".[25] Para evitar un incidente similar en su comunidad, es esencial identificar todos los

costos que requiere la instalación, el uso y el mantenimiento de la tecnología de vigilancia antes de decidir si la adoptarán o no.

2. LA VIGILANCIA PUEDE CREAR RIESGOS ECONÓMICOS, INCLUYENDO LITIGIOS Y FILTRACIÓN DE INFORMACIÓN

Los programas de vigilancia que no incluyan las medidas de seguridad necesarias para evitar errores y usos indebidos y proteger la libertad de expresión, de asociación y de religión o que apliquen inadecuadamente estas medidas de seguridad pueden terminar en costosos litigios que desvían recursos de otros servicios públicos. Por ejemplo, los residentes musulmanes de Orange County interpusieron una demanda por discriminación cuando se enteraron de que las agencias estatales enviaban informantes a las mezquitas para recopilar información sobre la identidad y las actividades de los fieles.[26] El Departamento de Policía de NY tuvo que pagar $2 millones en honorarios legales por espiar a las comunidades musulmanas de Nueva York.[27] Incluso los problemas técnicos pueden potencialmente crear costosas demandas y otros gastos. La Ciudad de San Francisco estuvo involucrada en una demanda de varios años por la violación de los derechos civiles tras detener, esposar y encañonar a una mujer inocente debido a un error en su sistema ALPR.[28]

"Después de la reacción del público al propuesto Centro de Conocimiento del Ámbito de Oakland tuvimos que reevaluar cómo íbamos a proceder." Renee Domingo, excoordinadora de Servicios de Emergencia de Oakland[29]

La recopilación de información también puede crear el riesgo de filtraciones, lo que puede conllevar significativos gastos públicos y poner en peligro la privacidad y seguridad económica de los residentes. Incluso si se siguen las prácticas óptimas (lo que de por sí puede requerir gastos significativos) esto no es suficiente para evitar todas las filtraciones de información. La ley de California requiere que las agencias locales notifiquen a los residentes cuando ocurren filtraciones de información.[30] El costo fiscal de la filtración de información confidencial puede ser muy alto; un informe del 2015 reveló que las empresas pagaron un promedio de $3.7 millones para solucionar problemas de seguridad.[31] Mientras más información se recopile y se retenga en la comunidad, mayor será el riesgo y costo potencial de la filtración de información.

3. LA FALTA DE PROCESOS ADECUADOS PUEDE MALGASTAR TIEMPO Y DINERO

No discutir las propuestas de vigilancia exhaustivamente y escuchar las inquietudes de la comunidad en las primeras fases del proceso puede generar una masiva reacción adversa y malgastar tiempo y fondos cuando los planes se suspenden o en última instancia se cancelan. Oakland se vio obligada a descartar la mayor parte de los planes de su desafortunado Centro de Conocimiento del Ámbito de Oakland y reducir el proyecto considerablemente cuando los miembros de la comunidad protestaron debido a la engañosa declaración de la misión y la falta de transparencia del proyecto.[32] En el Condado de Santa Clara, un proceso secreto para adquirir un dispositivo de vigilancia *Stingray* para celulares fue descarrilado por el órgano ejecutivo del Condado por esquivar necesarios debates comunitarios y la supervisión del Condado.[33]

"El SJPD debió hacer un mejor trabajo comunicando a nuestra comunidad el propósito y la adquisición del dispositivo UAS (siglas en inglés de Sistema Aéreo No Tripulado) … La comunidad debe tener la

oportunidad de aportar sus comentarios, hacer preguntas y expresar sus inquietudes antes de que el proyecto pueda avanzar." Departamento de Policía de San José[34]

Los miembros de la comunidad detuvieron la compra secreta de drones de San José y la policía tuvo que disculparse por la falta de transparencia y no solicitar la opinión de la comunidad.[35] Hablar con la comunidad antes de tomar los pasos necesarios para adoptar una propuesta de vigilancia es esencial para evitar errores similares que provoquen la indignación generalizada de la comunidad y malgasten tiempo y recursos.

C. LA VIGILANCIA DEBE TOMAR EN CUENTA LA EVOLUCIÓN DE LAS LEYES DE PRIVACIDAD

El uso de tecnología de vigilancia enfrenta cada vez más escrutinio y limitaciones. Los tribunales y legisladores estatales y federales, motivados por la creciente preocupación del público sobre su privacidad, están tomando medidas para proteger los derechos individuales y las libertades civiles. Como resultado, la comunidad necesita tomar en cuenta tanto las leyes existentes como su potencial de cambiar, incluyendo las políticas e inquietudes sobre los derechos individuales que están motivando el cambio, al evaluar una propuesta de vigilancia.

"Que la tecnología actual permita que una persona tenga en sus manos este tipo de información no hace que la información sea menos merecedora de la protección por la que lucharon los padres de la nación." Riley vs. California, Corte Suprema de EE. UU.[36]

En los últimos años los tribunales federales han ratificado repetidamente las protecciones legales de los derechos individuales en el contexto de la tecnología existente. En el 2015, la Corte Suprema de EE. UU. unánimemente les dijo a las agencias de la ley que deben "obtener una orden judicial" para inspeccionar el teléfono celular de las personas que arrestan. En otro fallo unánime, la Corte también determinó que es necesario tener una orden judicial para usar un localizador GPS para rastrear el vehículo de un sospechoso y la mayoría de los miembros de la Corte sugirieron que usar la tecnología para rastrear la ubicación de una persona, incluso en público, durante un periodo de tiempo prolongado requiere de un escrutinio constitucional.[37] Finalmente, varios tribunales federales declararon que la recopilación de macrodatos telefónicos sin tener una orden judicial de la NSA es ilegal y criticaron su alcance "casi orwelliano".[38] Los programas de vigilancia que no toman en cuenta esta tendencia pueden ser considerados inconstitucionales y las investigaciones criminales que se basan en evidencia recopilada a través de estos programas pueden correr peligro.

La Constitución de California protege aún más la privacidad de los miembros de la comunidad, incluyendo en los espacios públicos. El derecho a la privacidad del estado expresamente les da a los californianos el "derecho a que los dejen en paz" que es legal y aplicable y que protege los intereses de privacidad incluso fuera de su hogar.[39] La Corte Suprema de California ha dicho que "infiltrar" y monitorear de forma encubierta las actividades de estudiantes y profesores durante clases y reuniones públicas sin que existan indicativos de actividades criminales está en contra de la Constitución de California[40] al igual que usar un dispositivo aéreo para vigilar el patio trasero de un residente sin tener una orden judicial.[41] El derecho a libertad de expresión de los californianos se extiende fuera de su hogar, incluso en áreas que son de propiedad privada como centros comerciales.[42]

También se han promulgado muchas leyes y regulaciones que limitan o crean requerimientos para el uso de la tecnología de vigilancia. La Ley Federal de Escuchas Telefónicas y su contraparte en California limitan el uso de la tecnología de vigilancia que sea capaz de interceptar el contenido de las comunicaciones en vivo. En el 2015, los legisladores de California promulgaron tres leyes que abordan específicamente problemas relacionados con la tecnología de vigilancia:

- **Recopilación de información electrónica:** la Ley de Privacidad de las Comunicaciones Electrónicas de California requiere que exista una orden judicial cuando se recopila información electrónica usando tecnología de vigilancia, como la tecnología para rastrear teléfonos celulares. También requiere una orden judicial al inspeccionar dispositivos electrónicos o solicitar información de los correos electrónicos, la localización y otros metadatos a los proveedores de servicios. La ley crea medidas de seguridad procesales adicionales, incluyendo notificar al sospechoso, y permite los tribunales ordenen la supresión o la eliminación de información que fue obtenida o retenida en formas que violan esta ley.[43]

- **Lectores automáticos de placas vehiculares:** una nueva ley de California requiere la oportunidad de expresar comentarios públicos, la existencia de una política de uso que esté a disposición del público que sea "consistente con el respeto a la privacidad individual y libertades civiles de una persona" y medidas de seguridad razonables para el uso de los lectores automáticos de placas vehiculares. Las personas pueden demandar por daños y perjuicios si ocurren filtraciones de información u otras difusiones de información no autorizadas.[44]

- **Tecnología para el rastreo de teléfonos celulares:** una nueva ley de California requiere de un proceso público, de la aprobación legislativa local de todas las agencias además del alguacil, de una política de uso y privacidad que sea "consistente con el respeto a la privacidad individual y las libertades civiles" y que se hagan públicos los acuerdos con otras agencias en lo que respecta al uso de receptores IMSI y otras tecnologías para el rastreo de teléfonos celulares. Esta ley también permite que una persona demande a una agencia por violar estas disposiciones.[45]

También ha habido cambios legales bipartidistas a nivel federal y estatal para frenar la vigilancia. En el 2016, los legisladores federales adoptaron reformas relacionadas con el espionaje de la NSA.[46] Dieciocho estados más han promulgado leyes que restringen el acceso de las autoridades a información de la ubicación de una persona[47] y una mayoría de estados ha propuesto legislaciones para reducir el uso de drones con propósitos de vigilancia.[48]

ENCUESTA DE VOTANTES PROBABLES DE CALIFORNIA DEL 2016 REVELÓ UN SÓLIDO APOYO POR REFORMAS EN EL USO DE TECNOLOGÍAS DE VIGILANCIA POR PARTE DE LAS AGENCIAS DE LA LEY

Los votantes estales probables encuestados en California en el 2016 apoyaron significativamente reformas en el uso de tecnología de vigilancia por parte de las agencias de la ley a nivel local y estatal.[49] Este es un resumen de los resultados clave de la encuesta:

Apoyo a las propuestas de reformas	Apoyo
Requerir que el Consejo Municipal o la Junta de Supervisores vote para aprobar la nueva tecnología de vigilancia antes de ser usada por la policía local.	67%
Establecer y hacer cumplir las políticas locales que limitan el uso de la tecnología de vigilancia por parte de la policía.	65%
Establecer y hacer cumplir las políticas estatales que limitan el uso de la tecnología de vigilancia por parte de la policía.	64%
Requerir que las autoridades reporten públicamente la frecuencia con la que usan la tecnología de vigilancia.	62%
Notificar al público con anticipación antes de que la policía adquiera nueva tecnología de vigilancia	58%

Estos cambios a nivel estatal y federal son motivados por un evidente cambio en la actitud pública hacia la vigilancia. Los miembros de la comunidad quieren y esperan que existan reformas a nivel estatal y local para aumentar la transparencia, la rendición de cuentas y la supervisión al usar la tecnología de vigilancia. Dos tercios de los votantes de California quiere que sus funcionarios electos, como concejales o supervisores, aprueben las nuevas tecnologías de vigilancia antes de que sean usadas. De igual forma, una gran mayoría de votantes quiere que existan políticas a nivel local (65%) y estatal (64%) establecidas y ejecutadas para limitar el uso de la tecnología de vigilancia por parte de la policía. Los votantes también quieren que se tomen medidas para requerir que las autoridades reporten la frecuencia con que usan las tecnologías de vigilancia (62%) así como notificar al público antes de comprar nuevas tecnologías de vigilancia (58%).[50]

"Si existen ordenanzas sobre los equipos de vigilancia, todo el equipo que tenga Oakland o que adquiera en el futuro debe pasar por el proceso de evaluación." Brian Hofer, presidente del Comité de Privacidad del Centro de Conocimiento del Ámbito de Oakland[51]

Todos estos factores han hecho que muchas comunidades adopten ordenanzas locales para asegurar la transparencia, la rendición de cuentas y la supervisión de todas las tecnologías de vigilancia.[52] Su comunidad debe seguir este ejemplo y evaluar exhaustivamente toda propuesta de vigilancia para proteger los derechos de los miembros de la comunidad, identificar costos y riesgos económicos ocultos y asegurar que se cumpla con las leyes existentes y que sean consistentes con las crecientes inquietudes públicas sobre la privacidad.

PROMULGAR UNA ORDENANZA SOBRE VIGILANCIA Y SEGURIDAD COMUNITARIA PARA ASEGURAR QUE SE SIGA SIEMPRE EL DEBIDO PROCESO.

Aprobar la Ordenanza sobre Vigilancia y Seguridad Comunitaria que aparece en el Anexo de esta guía ayudará a su comunidad a evitar problemas futuros porque cumplirá siempre con el debido proceso. También asegura que haya un análisis comunitario de la tecnología de vigilancia cuando sea esté considerando su uso, que los legisladores locales aprueben cada paso y que todo programa de vigilancia aprobado incluya una Política de Uso de la Vigilancia que proteja los derechos individuales y mecanismos de transparencia y de rendición de cuentas para asegurar que se cumpla la Política.

Pasos necesarios al momento de considerar una propuesta de vigilancia

Se puede abusar de la vigilancia de muchas formas que perjudican a los miembros de la comunidad, socavan los objetivos de seguridad pública y hacen que los contribuyentes paguen por gastos innecesarios por lo que es necesario evaluar pública y exhaustivamente las propuestas de vigilancia. La siguiente sección ayudará a su comunidad –incluyendo a la diversidad de residentes, funcionarios públicos y a las agencias de la ley– a trabajar en grupo para determinar si la vigilancia es necesaria y a establecer sólidas reglas para asegurar el uso adecuado, la supervisión y la rendición de cuentas si su comunidad decide adoptar la propuesta de vigilancia.

La Oficina de Privacidad y la Oficina de Derechos Civiles y Libertades Civiles del Departamento de Seguridad Nacional (DHS, por sus siglas en inglés) publicó *CCTV: Desarrollando prácticas óptimas de privacidad*, un informe que insta a las agencias del gobierno a incluir consideraciones sobre la privacidad, los derechos y las libertades civiles en el diseño, adquisición y operación de los sistemas de videovigilancia. Un anexo resalta la necesidad de cumplir los principios prácticos de la información justa: transparencia, participación individual, especificidad del propósito, minimización de la información, limitaciones de uso, calidad e integridad de la información y seguridad, rendición de cuentas y verificación.[53]

A. EVALUAR COLECTIVAMENTE LA EFICACIA, COSTO Y ALTERNATIVAS ANTES DE TOMAR DECISIONES SOBRE VIGILANCIA

Menos del 15% de las comunidades de California debatieron públicamente los programas de vigilancia antes de que fueran adoptados. (ACLU 2014)[54]

La vigilancia debe solo ser la forma de lograr un propósito, no debe ser el propósito. Esto quiere decir que su comunidad debe tener un propósito específico o un problema en mente que requiera atención antes de considerar el uso de la tecnología de vigilancia. Cuando haya sido identificado pueden evaluar colectivamente si la vigilancia puede ayudarlos a lograr sus objetivos con eficacia y también calcular el costo en materia del presupuesto de su comunidad y de los derechos individuales.

1. DECIDIR COMO COMUNIDAD: PROMOVER LA PARTICIPACIÓN DE TODA LA COMUNIDAD DESDE EL PRINCIPIO

La mejor forma de evaluar si la vigilancia es la decisión correcta y evitar cometer costosos errores es promover la participación de toda la comunidad –incluyendo las autoridades, los legisladores locales y los miembros del público– en una exhaustiva discusión sobre toda propuesta de vigilancia. Los distintos segmentos de su comunidad traerán al proceso valiosos puntos de vista para evaluar si se debe adquirir y usar la tecnología de vigilancia. El momento de incluir a la comunidad es al principio de proceso, *antes* de solicitar fondos, adquirir tecnología o utilizar el sistema.

"El debate público que requerirá la ordenanza de vigilancia para las nuevas tecnologías y su uso beneficiará a todos, incluyendo a los funcionarios de la ciudad, para ayudarlos a comprender mejor cómo funcionan estos programas y lo que significan para el público." Joe DeVries, asistente del administrador de la Ciudad de Oakland[55]

Al considerar las propuestas para introducir o expandir la vigilancia, varias ciudades han encontrado útil promover la participación activa de los miembros de la comunidad a través de grupos de trabajo y comités *ad hoc* para moldear las políticas y proporcionar supervisión. El Departamento de Policía de Redlands convocó un Consejo de Privacidad Ciudadana en el que podían participar todos los residentes de la ciudad para aportar ideas sobre las políticas de las cámaras de vigilancia y supervisar el uso de las cámaras por parte de la policía.[56] Richmond creó un comité *ad hoc* para evaluar las políticas de su programa de videovigilancia.[57]

"La tecnología solo puede ayudar a la democracia en la medida en la que sea democratizada." Malkia Cyril, directora del Center for Media Justice[58]

En el 2014, después de que la comunidad rechazara y votara para no expandir el Centro de Conocimiento del Ámbito de Oakland, el Consejo de la Ciudad creo un Comité Asesor *Ad Hoc* sobre Privacidad y Retención de Información formado por una diversidad de miembros de la comunidad para crear medidas de seguridad, proteger el derecho a la privacidad y evitar el uso indebido de la información de un sistema reducido que será usado por el Puerto de Oakland.[59] La Ciudad de Oakland ahora tiene una Comisión de Privacidad formal que brinda asesoramiento sobre las prácticas óptimas para proteger el derecho a la privacidad en conexión con la compra y uso de la Ciudad de equipo de vigilancia y de otras tecnologías que recopilen o almacenen información.[60]

- *¿Está la comunidad participando en un debate informado para cada propuesta de vigilancia?*

  Nunca es demasiado temprano para debatir públicamente una propuesta de vigilancia. Los miembros de la comunidad deben saber, desde las etapas más tempranas del proceso, qué tipo de vigilancia se está considerando, cuál es su objetivo y cómo los afectará para que sus comentarios aporten información importante, resalten las inquietudes de la comunidad, ayuden a evitar problemas imprevistos y el rechazo de la comunidad.

CASO DE ESTUDIO: CONDADO DE SANTA CLARA CANCELA COMPRA DE STINGRAY DEBIDO A INQUIETUDES DE TRANSPARENCIA

En el 2015 el órgano ejecutivo del Condado de Santa Clara rechazó la propuesta del Alguacil de comprar un Stingray cuando la Junta de Supervisores cuestionó los gastos y el secretismo del proyecto. La Junta de Supervisores cuestionó por qué pedían que asignaran más de $500,000 del dinero de los contribuyentes a una compra que estaba siendo mantenida en secreto hasta para la Junta Directiva. El órgano ejecutivo del Condado rechazó en última instancia la compra porque la compañía que vendía el Stingray se rehusó a "aceptar hasta los criterios más básicos en términos de la solicitud de registros públicos… Tuvimos que hacer lo que consideramos era lo correcto".[61]

El público debe ser notificado con suficiente anticipación de que se está considerando el uso de los sistemas de vigilancia. Notificar con suficiente anticipación implica más que incluirlo en la agenda de una reunión pública. Las autoridades deben contactar proactivamente a los grupos comunitarios, incluyendo a los que representan a comunidades étnicas y religiosas, y a los medios de comunicación locales para informar al público desde las primeras etapas del proceso y promover el interés de toda la comunidad.

CASO DE ESTUDIO: CENTRO DE CONOCIMIENTO DEL ÁMBITO DE OAKLAND SE VE OBLIGADO A REDUCIR SU ESCALA POR MANTENER A LA COMUNIDAD A CIEGAS

En el 2013 la Ciudad de Oakland trató de expandir su *Centro de Conocimiento del Ámbito de Oakland*, que originalmente se enfocaba en el Puerto de Oakland, para crear una red de vigilancia en toda la ciudad que vinculaba a las cámaras locales de las calles y las escuelas, a las cámaras viales y a los micrófonos que detectan disparos. En lugar de solicitar la opinión del público sobre la expansión del sistema desde temprano, Oakland trató de seguir adelante sin la participación significativa de la comunidad. Los residentes estaban indignados y el Consejo de la Ciudad votó contra de la expansión del sistema.[62]

Un debate informado también requiere que la comunidad tenga acceso a una amplia gama de información para evaluar cómo funcionaría la vigilancia en la práctica y si ayudará a alcanzar los objetivos locales. Reuniones comunitarias con varios presentadores que representen distintos puntos de vista (no solo a las agencias de la ley o al vendedor de la tecnología) pueden ayudar a la comunidad a comprender cómo funciona realmente la tecnología de vigilancia y cuáles son sus implicaciones potenciales. La entidad que trate de adquirir nueva tecnología de vigilancia también debe preparar y publicar un Informe del Impacto de la Vigilancia y una Política de Uso de la Vigilancia para ayudar a todos a comprender cómo funcionará la tecnología, su costo potencial y las medidas de seguridad que evitarán su uso indebido si se aprueba la propuesta. La comunidad también puede considerar convocar a un comité *ad hoc* compuesto por residentes, expertos y defensores locales que trabajen juntos para hacer recomendaciones o ayudar a llenar estos documentos.

"Es muy importante para nuestro sistema judicial y nuestra democracia que el público y nuestros representantes electos estén informados del uso de estos dispositivos para que podamos discutir sus

implicaciones para la privacidad y tomar decisiones informadas sobre sus políticas de uso." Joe Simitian, supervisor del Condado de Santa Clara[63]

USAR EL INFORME DEL IMPACTO DE LA VIGILANCIA PARA TOMAR UNA DECISIÓN INFORMADA

El alcance y el costo potencial de la tecnología de vigilancia deben ser evaluados y hechos del conocimiento de la comunidad a través de un Informe del Impacto de la Vigilancia. Este informe debe incluir:

- Información que describa la tecnología, cómo funciona y qué información recopila, incluyendo las hojas de especificaciones de la tecnología provenientes de los fabricantes
- Los propósitos propuestos de la tecnología de vigilancia
- Los lugares en donde se usará y las estadísticas de delitos en estos lugares
- Una evaluación que identifique todos los impactos potenciales para las libertades y los derechos civiles y que discuta todos los planes para proteger los derechos del público
- El costo fiscal de la tecnología de vigilancia, incluyendo la compra inicial, el personal y los gastos continuos y las fuentes de financiamiento reales y potenciales.

Tenemos disponible una hoja de trabajo para ayudar a la comunidad a preparar un Informe del Impacto de la Vigilancia en aclunc.org/smartaboutsurveillance.

CASO DE ESTUDIO: CONCEJALES DE SANTA CRUZ NO TIENEN SUFICIENTE INFORMACIÓN AL TOMAR UNA DECISIÓN SOBRE LOS LECTORES AUTOMÁTICOS DE PLACAS VEHICULARES (ALPR)

Cuando el Consejo de la Ciudad de Santa Cruz aprobó el uso de fondos federales para comprar los ALPR para el departamento de policía, los concejales mencionaron que al tomar la decisión no tenían mucha información sobre la tecnología o su impacto para la comunidad. Cuando se le preguntó a uno de los concejales qué efecto podían tener los lectores para los miembros de la comunidad, respondió: "No conozco suficiente sobre la tecnología". Otro dijo que no estaba consciente de problemas de privacidad, "El consejo no recibió mucha correspondencia sobre el potencial de socavar los derechos civiles que tienen estos tipos de dispositivos…"[64]

¿Cómo decidirá la comunidad si debe adoptar una propuesta de vigilancia?

Los miembros de la comunidad merecen más que solo información sobre las propuestas de vigilancia, deben tener la oportunidad de ayudar a determinar si la propuesta beneficia realmente a la comunidad y cómo la beneficia y su adopción requiere que puedan expresar su opinión a los responsables políticos locales en audiencias públicas o votando sobre el asunto.

En cualquier caso, se debe obtener la aprobación inicial de la comunidad antes de tomar medidas para adquirir la tecnología de vigilancia, incluyendo solicitar fondos a entidades externas. Esto garantizará que los subsidios externos no esquiven el proceso democrático adecuado y excluyan a los miembros de la comunidad. Los responsables políticos locales o la comunidad general deben tener más oportunidades de expresar su opinión si la propuesta cambia o más detalles están disponibles.

CASO DE ESTUDIO: *DRONE* DE SAN JOSÉ NO PUEDE DESPEGAR HASTA QUE SEA APROBADO POR LA COMUNIDAD

Los residentes de San José se sintieron indignados cuando se enteraron de que su departamento de policía había comprado un *drone* (vehículo aéreo no tripulado) sin realizar ningún debate público. En medio de la cobertura de los medios de comunicación y las protestas de los grupos de la comunidad y de los defensores de los derechos civiles, la policía se disculpó y dijo que dejarían al *drone* en tierra hasta que pudieran llevar a cabo los esfuerzos de difusión apropiados.[65]

2. DEFINIR EL PROPÓSITO: PREGUNTAR CÓMO LA TECNOLOGÍA PUEDE AYUDAR Y AYUDARÁ REALMENTE A LA COMUNIDAD

La comunidad no puede determinar si la vigilancia es la solución adecuada si no han identificado el problema primero. Definir el propósito o problema específico que la vigilancia tratará de solucionar es esencial para evaluar la potencial efectividad de la vigilancia e identificar alternativas que pueden ser mejores para las necesidades y el presupuesto de la comunidad. Puede ayudar a resaltar quiénes son las personas o comunidades que serán más afectadas por la vigilancia y a asegurar que sus comentarios e inquietudes sean comprendidos plenamente. También es un punto de partida para crear una Política de Uso de la Vigilancia al definir los objetivos específicos que requieren de la vigilancia y evitar su uso con cualquier otro propósito.

- *¿Cómo se beneficiará la comunidad específicamente con la adopción de esta tecnología?*

Un propósito comunitario bien definido debe incluir un problema específico y un resultado mensurable que desee la comunidad. Propósitos ambiguos como "proteger a nuestra ciudad de los criminales" pueden hacer que sea difícil que la comunidad comprenda cómo se puede usar la vigilancia o cómo se puede evaluar su efectividad. En cambio, un propósito como "aumentar la recuperación de vehículos robados" identifica claramente un resultado deseado por los miembros de la comunidad y ayuda a crear un marco para la discusión pública. Esta discusión puede hacer que se reduzcan o modifiquen los propósitos para los que se usará la vigilancia, si es que deciden adoptarla.

CASO DE ESTUDIO: OAKLAND GASTA 2 MILLONES DE DÓLARES EN TECNOLOGÍA POLICIAL "CASI SIN USAR"

La Ciudad de Oakland, que de por sí tiene problemas de liquidez, aprendió una difícil lección de primera mano al adquirir nueva tecnología para la policía sin identificar claramente su propósito y malgastar tiempo y dinero. Una auditoría de la ciudad reveló que la ciudad desperdició $2 millones en tecnología para la policía que estuvo casi sin usar entre el 2006 y el 2011. El auditor recomendó se tomarán medidas para asegurar que las compras de tecnología se basen en objetivos estratégicos específicos y que se realice una evaluación regular de su efectividad.[66]

- *¿Puede ayudar esta tecnología de vigilancia a alcanzar los objetivos de la comunidad?*

Cuando la comunidad haya identificado los propósitos potenciales de la tecnología de vigilancia, deben evaluar si la tecnología propuesta puede realmente ayudar a alcanzar estos propósitos. La descripción del fabricante no se puede tomar al pie de la letra y definitivamente no debe ser lo único que se tome en cuenta. En lugar de hacer esto, la comunidad debe evaluar toda la evidencia y todos los argumentos que sugieren que la tecnología de vigilancia puede ayudar a alcanzar o no sus propósitos específicos.

CASO DE ESTUDIO: SAN FRANCISCO RECONSIDERA SUS PLANES DE EXPANDIR PROGRAMA DE CÁMARAS DE SEGURIDAD QUE NO MEJORA LA SEGURIDAD DE LA COMUNIDAD

En el 2005 San Francisco se dio a la tarea de reducir los delitos violentos y proporcionar a la policía una herramienta de investigación instalando videocámaras en las áreas con más delitos y con mayor tráfico vehicular de la Ciudad. Sin embargo, después de la instalación, las estadísticas criminales que se publicaron para cumplir con un mandato de una ordenanza de la Ciudad revelaron que las cámaras no redujeron el crimen y no ayudaban a solucionarlos de ninguna forma significativa. De hecho, las cámaras solo lograron que seis sospechosos fueran procesados por el SFPD entre el 2005 y el 2008. Como resultado, la Comisión de la Policía reconsideró sus planes de expandir el programa.[67]

- *¿Existen mejores alternativas para lograr los propósitos deseados?*

Incluso sin la tecnología de vigilancia propuesta parece que puede ayudar a su comunidad a lograr sus propósitos, todavía hay otras alternativas que pueden ser igual (o más) efectivas, menos costosas y/o menos propensas a ser usadas indebidamente o a afectar negativamente a los miembros de la comunidad.

Se deben comparar específicamente la efectividad y el costo de las soluciones tecnológicas para hacer frente al problema con el costo de los enfoques no tecnológicos. Por ejemplo, varios estudios han demostrado que los enfoques tradicionales, como instalar más iluminación o patrullar a pie, reducen significativamente el crimen.[68] No se debe asumir automáticamente que la tecnología de vigilancia será lo más efectivo.

CASO DE ESTUDIO: CIUDADES REEMPLAZAN LAS CÁMARAS DE LOS SEMÁFOROS CON LUCES AMARILLAS DE MAYOR DURACIÓN

Las ciudades de California están desactivando cada vez más cámaras de los semáforos a medida que la evidencia demuestra que las cámaras aumentan, en lugar de reducir, los accidentes de tránsito. Por ejemplo, en Walnut, un estudio reveló que las cámaras de los semáforos aumentaron dramáticamente las "colisiones al atravesar la luz roja" (400%), "colisiones traseras" (71%) y "colisiones laterales" (100%) y que "no se podía argumentar que las fotografías mejoraran la seguridad… en la ciudad de Walnut. De hecho, el uso de las cámaras de los semáforos parece reducir la seguridad y hacer que los usuarios corran mayor peligro". Debido a esta evidencia, más de la mitad de las ciudades de California que usaban cámaras en los semáforos han puesto fin a estos programas y están usando otras alternativas que han comprobado ser más efectivas para evitar accidentes, como luces amarillas de mayor duración en las intersecciones peligrosas.[69]

3. *IDENTIFICAR EL COSTO Y LOS RIESGOS: ANALIZAR LAS CONSECUENCIAS ECONÓMICAS, LEGALES Y PRÁCTICAS*

Incluso si la tecnología específica es apropiada para los propósitos de la comunidad, todavía pueden existir inquietudes económicas, legales y prácticas que pueden hacer que su adopción no sea deseable. Esta sección puede ayudarlos a evaluar el costo de la vigilancia para que puedan determinar si superan los beneficios esperados.

- *¿Cuánto le costará a la comunidad la adquisición y operación de la tecnología?*

Decidir cómo usar los fondos comunes es una de las tareas más importantes de su comunidad. Cada dólar que gasta su comunidad en tecnología de vigilancia es un dólar que no puede invertir en alguna otra necesidad de la comunidad. Los gastos relacionados con la tecnología de vigilancia incluyen tiempo de trabajo, capacitación, mantenimiento y cuidado y los costos asociados con la red y el almacenamiento de la información que recopila la comunidad. También se debe evaluar el costo potencial y el riesgo de que ocurran filtraciones de información o demandas basadas en el uso abusivo de la vigilancia.

"Una pregunta que también debemos hacernos es si estamos tomando en cuenta la infraestructura necesaria para apoyar a la tecnología –el costo de monitorearla y de encontrar personal para las unidades tecnológicas en una época en la que los departamentos están dando de baja a su personal. Debemos pensar realmente en todos los aspectos de la tecnología cuando se haga la inversión inicial". Foro Ejecutivo de Investigación de la Policía, "¿Cómo afectan las innovaciones tecnológicas las actividades de la policía?"[70]

Las preguntas sobre el costo no pueden ignorarse simplemente porque la comunidad está solicitando un subsidio para pagar por la tecnología. Estos subsidios son atractivos por razones obvias, parecen permitir que la comunidad adquiera nueva tecnología sin tener que gastar el dinero de los contribuyentes locales. Pero los subsidios externos pueden no cubrir el costo total que se requiere después de adoptar la tecnología, particularmente el costo a largo plazo de su operación, reparación y del personal necesario. La clave es

calcular este costo de la forma más precisa posible y asegurar que estos cálculos sean compartidos con la comunidad y sean parte del debate sobre la adopción de la vigilancia.

- *¿Cuáles son los riesgos legales y los costos potenciales asociados con la propuesta de vigilancia?*

La tecnología de vigilancia puede conllevar varios riesgos y requisitos legales significativos, en parte debido a los rápidos cambios en las leyes de privacidad y vigilancia. Incluso bajo la ley actual, el uso indebido de los sistemas de vigilancia o problemas técnicos fuera del control de los usuarios pueden hacer que la comunidad sea vulnerable a demandas. Como los tribunales y legisladores reevalúan de forma continua cómo se deben salvaguardar los derechos de privacidad y de libertad de expresión en la era digital, existe el riesgo de que el equipo de tecnología de vigilancia en el que invirtió la comunidad no se pueda seguir usando legalmente para el propósito inicial. Estos factores deben ser tomados en cuenta en el análisis costo-beneficio de toda propuesta de vigilancia.

CASO DE ESTUDIO: FBI REMUEVE RASTREADORES GPS CUANDO LA CORTE SUPREMA FALLÓ QUE EL RASTREO SIN ÓRDENES JUDICIALES INVOLUCRA A LA CUARTA ENMIENDA

El FBI había instalado aproximadamente 3,000 rastreadores GPS en automóviles de todo Estados Unidos sin tener una orden judicial cuando la Corte Suprema de EE. UU. determinó en el 2012 que su uso involucraba a la Cuarta Enmienda. Como resultado, el FBI desactivó los rastreadores instalados sin una orden judicial y sus agentes tuvieron que removerlos físicamente. Obtener las órdenes judiciales antes de usar los rastreadores GPS hubiera garantizado la constitucionalidad de la evidencia obtenida y le hubiera ahorrado al FBI una cantidad considerable de tiempo y esfuerzo.[71]

- *¿Cómo pueden las propuestas de vigilancia tener un impacto negativo en la seguridad pública y en los derechos individuales?*

Las propuestas de vigilancia diseñadas para beneficiar a la comunidad pueden tener efectos secundarios que socavan este objetivo. Los sistemas que no son seguros pueden ser un blanco tentador para los piratas informáticos (*hackers*), lo que potencialmente puede afectar la seguridad de la comunidad. Los programas de vigilancia que se enfocan o afectan desproporcionadamente a las comunidades de color o a otros grupos marginados pueden hacer que sea más difícil que las autoridades trabajen en coordinación con estos grupos para investigar el crimen. La vigilancia también puede afectar la participación política y social, como asistir a mítines políticos, exposiciones de armas de fuego o ceremonias religiosas, si los miembros de la comunidad temen que sus vidas sean monitoreadas constantemente. Identificar los perjuicios y los beneficios de la vigilancia es parte importante de evaluar las propuestas.

CASO DE ESTUDIO: REDLANDS DESPLIEGA UN RED DE CÁMARAS QUE NO ES SEGURA

La red de cámaras de vigilancia de la Ciudad de Redlands estuvo en las noticias por las peores razones posibles cuando expertos en seguridad informática demostraron lo fácil que era piratear las cámaras. A pesar de que el departamento de policía había expresado su preocupación en caso de que "personas con intenciones criminales usaran el contenido filmado por las cámaras para

vigilar hogares o empresas o monitorear la fuerza policial", la red fue desplegada sin mecanismos de seguridad. Incluso después de que la historia saliera a la luz pública, la red fue asegurada con un anticuado protocolo de codificación que uno de los investigadores describió como "poner el cerrojo de un diario en la puerta de entrada".[72]

B. CREAR UNA POLÍTICA PARA EL USO DE LA VIGILANCIA QUE MITIGUE SUS EFECTOS NOCIVOS Y PROTEGER LOS DERECHOS

Si después de un análisis cuidadoso y de un exhaustivo debate público la comunidad decide que una tecnología de vigilancia específica es digna de ser adoptada, se debe asegurar que haya políticas que aseguren que se use debidamente. Una Política de Uso de la Vigilancia clara y legalmente ejecutable que sea una guía de cuándo y cómo usar la vigilancia puede proteger los derechos individuales mientras protege a las autoridades locales y a la comunidad de costosas demandas, de la publicidad negativa, de la pérdida de la confianza de la comunidad y mucho más. Reconociendo la necesidad de tener políticas de uso, Seattle y Spokane en Washington aprobaron hace poco ordenanzas que requieren que la policía establezca normas para el uso del equipo de vigilancia antes de usarlo.[73]

CASO DE ESTUDIO: CONDADO DE ALAMEDA SOLICITA LA OPINIÓN DEL PÚBLICO PARA ESTABLECER LA POLÍTICA DE USO DE STINGRAY

Antes de modernizar su tecnología de vigilancia para los teléfonos celulares, el fiscal de distrito del Condado de Alameda publicó su borrador de la política de uso y solicitó que la comunidad expresara su opinión. Como respuesta a los comentarios, el Fiscal de Distrito realizó cambios que permitieron la creación de una política que requiere de una orden judicial para el uso del dispositivo y establece estrictos límites para el uso de la información. Este proceso transparente y democrático ayudó a fortalecer la confianza de la comunidad y aseguró la implementación de medidas de seguridad más robustas desde el principio.[74]

Estos son algunos de los elementos clave de una Política de Uso de la Vigilancia sólida y legalmente ejecutable:

1. USAR DEBIDAMENTE: ESTABLECER CLAROS LÍMITES PARA LA VIGILANCIA

Si la comunidad ha estado siguiendo los pasos que propone esta guía, ya ha definido los propósitos comunitarios que justifican el uso de una tecnología específica. El siguiente es paso es usar estos propósitos para decidir y codificar tanto los usos aceptables que beneficiarán a la comunidad como aquellos que estarán prohibidos. Hacer esto evita el uso de la tecnología en formas que no eran la intención de la comunidad.

- *¿Cuándo se permite o prohíbe el uso de la vigilancia?*

El primer paso es simple pero muy importante: definir cómo y cuándo se puede usar la tecnología. Todo organismo de la comunidad que participe en la vigilancia debe tener una política que especifique claramente los usos apropiados de cada tecnología y prohíba todos los demás usos.

Menos de 1 de cada 5 programas de vigilancia de California tenían políticas de uso públicamente disponibles (de acuerdo con un estudio de la ACLU del 2014).[75]

Para que la tecnología beneficie a la comunidad y refleje su opinión sobre la supervisión, solo se debe usar para el propósito específico para la que fue adquirida. Todo nuevo uso que se proponga debe estar sujeto al miso proceso de discusión pública que la adquisición de la nueva tecnología permitiendo que la comunidad exprese su opinión sobre su idoneidad para cualquier expansión de su uso.

La política debe ser consistente con las garantías constitucionales de privacidad, igualdad de protección, libertad de expresión y libertad de religión. De hecho, la política de uso no solo debe de manera clara abordar los usos claramente ilegales sino los usos potencialmente ilegales de la tecnología de vigilancia. Si hay preguntas sobre la legalidad de una práctica específica, la política de uso también debe prohibir dicha práctica hasta que se tenga una respuesta definitiva.

La policía debe "dialogar más con el Consejo porque somos nosotros los que aprobamos la decisión de asignar fondos y queremos asegurarnos de que… escuchen todo lo que nosotros escuchamos". Bruce Harrell, concejal de Seattle[76]

- *¿Qué proceso legal o interno se requiere para usar la vigilancia?*

También es importante asegurar que se sigan todos los procesos requeridos legalmente y los procesos internos cada vez que se usa la tecnología de vigilancia. Estos procesos ayudan a evitar usos no autorizados o claramente ilegales y aseguran que incluso los usos apropiados de la tecnología de vigilancia minimicen el impacto sobre los derechos individuales.

En muchos casos, la mejor forma de asegurar que se cumplan con los requisitos legales es requerir una orden judicial antes de realizar la vigilancia, lo que permite que nuestro sistema legal participe en la supervisión del programa. Gracias a un moderno y sencillo proceso de solicitud de órdenes judiciales, los oficiales pueden solicitar la aprobación de un juez de forma rápida y fácil haciendo una llamada telefónica o usando un dispositivo móvil.[77]

Mantener registros internos, incluyendo identificar la razón de cada uno de los usos de la vigilancia, también puede ayudar a asegurar que se cumpla con la política de uso debidamente crea un registro de auditoría para permitir comentarios y supervisión continua.

- *¿Cómo son capacitados los oficiales antes de realizar la vigilancia?*

Las políticas claras no funcionan si las personas que usan la tecnología o la información que recopila no saben cómo cumplir con estas políticas. Los programas de capacitación para toda persona que participa

en la vigilancia deben ser exhaustivos e incluir no solo la tecnología y la Política de Uso de la Vigilancia, sino también los propósitos y reglas legales usadas para crear la política. La capacitación debe explicar claramente las obligaciones de toda persona que use la tecnología y las consecuencias de incumplir la política.

- *¿Se estará recopilando solo información necesaria?*

Asegurar que la tecnología de vigilancia se use para cumplir con el propósito establecido sin recopilar información adicional es una forma sencilla de reducir el riesgo de invadir la privacidad. Por eso es por lo que el estatuto federal que autoriza pinchar los teléfonos desde el principio requirió la "minimización", un esfuerzo para asegurar que incluso al tener una orden judicial y recopilar información la policía solo pueda interceptar comunicaciones relevantes para la investigación, no todas las comunicaciones que haga el sujeto que está siendo investigado.[78]

El mismo principio debe aplicarse a otros tipos de vigilancia y se debe requerir un esfuerzo razonable para evitar recopilar información superflua. Por ejemplo, un departamento de policía que envíe drones a la escena de un accidente para identificar rápidamente si se necesita de la intervención de la policía o del personal de emergencias no tiene que grabar o retener la grabación.

CASO DE ESTUDIO: LA PATRULLA DE CAMINOS DEL ESTADO DE OHIO RETIENE SOLO LA INFORMACIÓN RELEVANTES DE LOS ALPR

La política de la Patrulla de Caminos del Estado de Ohio sobre el uso de los lectores automáticos de placas vehiculares (ALPR, por sus siglas en inglés) especifica que toda "información irrelevante capturada sea borrada de inmediato". El objetivo del programa ALPR es ubicar vehículos robados, Alertas Amber y personas que tienen órdenes de arresto pendientes. Retener la información de los vehículos que no son relevantes no ayuda con este propósito y la política de borrar la información de inmediato protege a la comunidad de riesgos innecesarios.[79]

2. EVITAR EL USO INDEBIDO DE LA INFORMACIÓN: LIMITAR CUÁNDO SE PUEDE USAR LA INFORMACIÓN Y QUIÉN PUEDE TENER ACCESO A ELLA

Incluso la información que se recopila con propósitos legítimos puede ser usada de forma ilegítima. Es esencial que la comunidad establezca claras reglas para que la información recopilada a través de la vigilancia se use solo para los propósitos que han sido aprobados. Hacerlo no solo evita el abuso de la información que puede socavar la confianza pública, también evita que la "ampliación de la misión" afecte el balance que fue establecido entre las acciones del gobierno y las libertades individuales.

- *¿Cómo se mantendrá segura la información recopilada a través de la vigilancia?*

El primer paso para evitar el uso indebido de la información es asegurar que se almacene en un lugar seguro. Se necesitan medidas de seguridad técnicas para ayudar a proteger la información de los miembros de la comunidad de filtraciones accidentales y de uso indebido. Se debe consultar con los

expertos e implementar medidas de seguridad en varios niveles que protejan la información en todo momento de su vida útil.

Puede que la comunidad tenga un espacio seguro para guardar la información que sea independiente de otras bases de datos y sistemas informáticos. Esto proporciona un obvio nivel de control. Si deciden almacenar la información en otro lugar, deben asegurar que sea seguro y que esté sujeto a las medidas de seguridad necesarias. La comunidad también debe designar a alguien que tenga autoridad o custodie con responsabilidad la información de los miembros de la comunidad y los sistemas de almacenamiento.

CASO DE ESTUDIO: FILTRACIÓN DE INFORMACIÓN EN EL CONDADO DE MONTEREY DEBIDO A PRÁCTICAS INFORMÁTICAS "TOTALMENTE OBSOLETAS"

Los sistemas informáticos del Condado de Monterey fueron infiltrados en el 2013 y la información personal de más de 140,000 residentes fue robada. Una investigación de un gran jurado determinó que la filtración se debió a prácticas informáticas "totalmente obsoletas" y por no hacer cumplir las leyes de privacidad. El gran jurado advirtió que podía haber "graves consecuencias económicas" si el condado no cambiaba sus prácticas.[80]

➢ *¿Bajo qué circunstancias se puede acceder o usar la información recopilada?*

Además de tener medidas de seguridad técnicas para proteger la información, también se deben limitar las circunstancias bajo las que se puede acceder o usar legítimamente. Estos límites se deben basar en los propósitos específicos que la comunidad aceptó al adoptar la tecnología. Por ejemplo, si el propósito de la tecnología es hacer frente a delitos violentos específicos, la política puede permitir que se use la base de datos para buscar información que sea parte de una investigación oficial de un delito violento y solo la información relacionada con esta investigación. El acceso a la información y políticas de uso que sean consistentes con los propósitos establecidos para el sistema orientarán a los operadores y sembrarán confianza en la comunidad al evitar los abusos que pueden ocurrir al permitir el acceso sin restricciones de la información recopilada a través de la vigilancia.

El objetivo de la comunidad de balancear la privacidad y la seguridad será más fácil de cumplir si el acceso a la información y los límites de uso están acompañados de pasos que aseguren que se cumplan las reglas. El acceso a las bases de datos debe ser limitado. Por ejemplo, permitiendo que el personal subalterno solo acceda la información con el permiso y la orientación de los funcionarios de alto nivel o limitando el acceso solo a los funcionarios de alto nivel. Como mencionamos antes, capacitar al personal es esencial. Restringir el acceso a una cantidad limitada de empleados capacitados reduce el potencial de que la información de los miembros de la comunidad se use indebidamente. Para asegurar que la información se use de la forma adecuada, puede ser necesario requerir una orden judicial u otro proceso externo similar antes de tener acceso a la información.

CASO DE ESTUDIO: POLÍTICAS DE LAX PERMITEN EL ABUSO *LOVEINT*

Si no existen sólidas políticas que limiten el acceso a la información, la tentación de usar indebidamente las bases de datos del gobierno para intereses personales es difícil de resistir. La NSA incluso tiene un término específico, *LOVEINT*, para los empleados que monitorean a sus parejas amorosas. Dos oficiales de Fairfield en California pueden enfrentar cargos criminales por usar la base de datos de la policía del estado para investigar a mujeres que usan los sitios de internet para encontrar citas en línea.[81]

- *¿Qué límites existen para compartir la información con organismos externos?*

Limitar cómo se usa la información es un excelente primer paso, pero terceros que pueden recibir la información recopilada pueden no tener los mismos límites. Para proteger la privacidad de los residentes y evitar el uso de la información en formas que van en contra de los deseos de la comunidad, es importante articular cuándo los propósitos de la tecnología justifican compartir la información recopilada, si es que alguna vez lo hacen. Durante el debate público sobre la Política de Uso de la Vigilancia, la comunidad debe decidir cuándo se permitirá compartir la información y cuándo estará prohibido.

Si se puede compartir la información, la comunidad también debe determinar cómo asegurar que la entidad que recibe la información cumpla con los estándares de la comunidad. Esto puede requerir contratos vinculantes que hagan que los terceros cumplan con las políticas y medidas de seguridad. Por ejemplo, la Ciudad de Menlo Park en California tiene una ordenanza que requiere específicamente que cualquier acuerdo con el centro de fusión del Norte de California exija que se cumpla con la política de retención de la Ciudad.[82] Si el receptor potencial de la información no acepta las políticas o condiciones, la mejor opción es no compartir la información.

3. *LIMITAR LA RETENCIÓN DE INFORMACIÓN: GUARDAR LA INFORMACIÓN SOLO DURANTE EL TIEMPO QUE SEA NECESARIO*

Mientras más tiempo se retiene la información, mayor es el potencial de incurrir en riesgos de privacidad y seguridad. La forma más fácil de minimizar estos riesgos es retener solo la información necesaria y borrarla cuando se haya logrado el propósito para la que fue recopilada.

"Si hay algo de naturaleza criminal grabado en video es capturado e inventariado en pocas horas. Casi todo lo demás no se vuelve a ver, por lo que puede ser purgado automáticamente." Comandante Steven Caluris, Departamento de Policía de Chicago[83]

- *¿Ayuda la retención de información a lograr los propósitos para los que se adquirió la tecnología?*

Para maximizar la utilidad de la tecnología y minimizar las inquietudes relacionadas con las libertades civiles, el periodo de retención no debe ser más largo de lo necesario para lograr los propósitos directos de la comunidad. Por ejemplo, usar lectores automáticos de licencias vehiculares para localizar vehículos robados o asociados con una Alerta Amber no se beneficia de la recopilación previa de

información. Retener la información "en caso de que sea útil" aumenta el riesgo de usar la información en formas contrarias al propósito aceptado por la comunidad y puede terminar en manos de una persona que puede ser perjudicial. Retener la información también puede aumentar el costo de la vigilancia requiriendo soluciones de almacenamiento costosas y haciendo que sea más difícil usar el sistema efectivamente. Enfocarse en el propósito específico que se supone debe tener la vigilancia puede ayudar a determinar un periodo de retención que balancee este objetivo con el costo y con los riesgos asociados con la retención de la información.

- *¿Hay otras razones legales o políticas que deben ser tomadas en cuenta en la política de retención de información?*

Puede haber otras razones legales y políticas que afecten a la política de retención de información debido a consideraciones legales no relacionadas con los propósitos de la comunidad. Por ejemplo, la comunidad debe decidir el periodo de retención que balancee el deseo de ser receptivo a las solicitudes de registros públicos y las libertades civiles de los residentes, incluyendo el derecho a la privacidad. Ser receptivo a las solicitudes de registros públicos no debe ser la justificación principal de un periodo de retención extenso, sin embargo, las inquietudes que puede tener la comunidad con la vigilancia se abordan mejor al retener menos información desde el principio.

- *¿Qué pasa cuando expira el periodo de retención de la información?*

Para evitar el uso indebido de la información cuando termina el periodo de retención que desea la comunidad, hay que asegurar que la información sea borrada tan pronto como esto ocurra. Esto se puede lograr implementando medidas técnicas automáticas o realizando auditorías periódicas.

Antes de recopilar la información, la comunidad también debe decidir si habrá circunstancias específicas que justifiquen la retención de la información más allá del periodo de retención escogido por la comunidad. Por ejemplo, puede ser apropiado guardar la información relacionada con una investigación específica, información necesaria para investigar el uso indebido interno de la información e información relacionada con el caso de una persona acusada de un delito. Todas estas condiciones deben cumplir con los propósitos de la comunidad y deben ser articuladas claramente en la Política de Uso de la Vigilancia.

C. ASEGURAR QUE SE RINDAN CUENTAS HACIENDO CUMPLIR LAS POLÍTICAS Y PROMOVIENDO UNA CONTINUA PARTICIPACIÓN PÚBLICA

Incluso si la comunidad ya está usando la tecnología de vigilancia, la comunidad general juega un importante papel para asegurar que los intereses públicos se beneficien con su uso. Una pregunta clave es si la Política de Uso de la Vigilancia está protegiendo efectivamente los derechos individuales y evitando abusos. La segunda es si lo que se asumió al aprobar la vigilancia inicialmente sigue siendo cierto al tener experiencia con la tecnología y su impacto. Modificar o incluso cancelar un programa ineficaz o desigual es mejor que malgastar tiempo y dinero y socavar la confianza de la comunidad en una herramienta que hace más daño que bien.

1. IDENTIFICAR Y HACER FRENTE A LOS ABUSOS: USO DE TECNOLOGÍAS DE AUDITORÍA E INFORMACIÓN PARA ABORDAR TODO USO INDEBIDO

Las medidas de seguridad de la Política de Uso de la Vigilancia solo son efectivas cuando se cumple la política. Pero debido a la naturaleza secreta de muchos tipos de vigilancia, asegurar este cumplimiento requiere de esfuerzos conscientes. Una supervisión y auditoría interna y externa puede ayudar a identificar abusos aislados o sistémicos de la tecnología de vigilancia y a establecer sanciones legalmente ejecutables que pueden evitar ambas cosas.

➢ *¿Cómo se supervisará a los operadores?*

La gestión del personal y las medidas técnicas facilitan la supervisión interna de la tecnología y de la información. Designar una cadena de mando para las tecnologías de vigilancia específicas ayuda a que el personal comprenda sus responsabilidades sobre el equipo y la información y hace que sea fácil rastrear el uso inadecuado de la información. Todo esto ayuda a la comunidad a evitar abusos y garantiza que los recursos se usen de la mejor forma.

"Como guardianes de los intereses públicos sabemos que el gobierno no puede simplemente decir "confíen en nosotros" y seguir adelante, tenemos que ganarnos esta confianza cada día. Debemos ser responsables y transparentes…" Jean Quan, exalcaldesa de Oakland[84]

➢ *¿Cómo se identificarán los usos indebidos de la tecnología?*

La mejor forma de identificar el uso indebido de la vigilancia es "observar a quienes nos observan" manteniendo registros exhaustivos de cada vez que se usó la tecnología de vigilancia o la información recopilada a través de la tecnología de vigilancia. Las personas responsables de supervisar deben ser independientes, deben tener acceso total a la tecnología y a la base de datos y deben ser empoderados para escuchar las quejas de uso indebido y tomar decisiones que pueden tener consecuencias legalmente ejecutables. Para captar lo que la supervisión humana puede no capturar, la comunidad debe asegurar que se implementen medidas técnicas, incluyendo controlar el acceso y tener registros de auditoría. Otorgar autoridad de supervisión a terceros, como al Consejo de la Ciudad o a un panel de ciudadanos, también puede aumentar la probabilidad de identificar los usos indebidos.

CASO DE ESTUDIO: FRESNO ADOPTA AUDITORÍA ANUAL DE SU VIDEOVIGILANCIA

Cuando el Departamento de Policía de Fresno propuso un programa de videovigilancia para toda la Ciudad usando cámaras con transmisión en vivo, el Consejo de la Ciudad requirió una auditoría independiente anual para asegurar que todas las normas de privacidad y seguridad para el uso del sistema se estuvieran cumpliendo. Jerry Dyer, jefe de la Policía de Fresno, dijo que apoyaba la auditoría: "No cabe duda de que la auditoría será muy útil para nuestras operaciones de videovigilancia continuas". La Ciudad designó a un juez jubilado del tribunal federal de distrito como auditor para analizar el uso del sistema y hacer recomendaciones políticas específicas.[85]

- *¿Qué sanciones legalmente ejecutables existen para evitar el uso indebido y el abuso de esta tecnología?*

Al establecer consecuencias si se violan las reglas, la comunidad promueve el uso adecuado de la tecnología y deja claro que los valores de la comunidad se aplican a todos. Dependiendo de las circunstancias, sanciones que van desde volver a participar en capacitaciones o multas, suspensiones o despidos pueden ser apropiadas si se viola la Política de Uso de la Vigilancia. La comunidad también debe establecer un remedio apropiado para toda persona que haya sido víctima de un abuso. Las sanciones legalmente ejecutables evitan el uso indebido y ayudan a subsanar los daños sufridos por los miembros de la comunidad.

2. MANTENER EL DIÁLOGO ABIERTO: PROMOVER LA SUPERVISIÓN PÚBLICA Y LA DISCUSIÓN CONTINUA

La supervisión y comentarios de la comunidad son esenciales para asegurar que todo programa de vigilancia existente beneficie a la comunidad. Primero, ser transparente cuando se usa la vigilancia abusivamente permite que la comunidad determine si la Política de Uso de la Vigilancia o las sanciones asociadas deben ser modificadas para abordar el problema. Segundo, a medida que la comunidad determina si la vigilancia es efectiva y cómo afecta a distintas personas y grupos, es posible que quieran reevaluar los propósitos para los que se debe usar la vigilancia o incluso si debe seguir usando. La vigilancia debe estar bajo el control de la comunidad en todo momento, no solo cuando se está considerando su uso.

- *¿Cómo puede la comunidad permanecer informada sobre el programa de vigilancia?*

Es importante que los mecanismos de supervisión de la comunidad no solo estén en vigor antes de usar la vigilancia, sino que sigan estando en vigor durante el programa de vigilancia o mientras exista información recopilada. Esto permite que la comunidad siga determinando y comentando sobre la efectividad y el impacto de la vigilancia y proporciona información necesaria para evaluar futuros cambios.

Una de las formas más efectivas de mantener a la comunidad informada es preparar un informe anual sobre cada una de las tecnologías de vigilancia que se usaron el año anterior. Este informe debe incluir:

- Una descripción de cómo y con cuánta frecuencia se usó la tecnología
- Información, incluyendo estadísticas del crimen, que indique si la tecnología ha logrado cumplir efectivamente con su propósito
- Un resumen de las quejas e inquietudes que tenga la comunidad sobre la tecnología
- Información sobre toda violación a la Política de Uso de la Vigilancia, filtración de información o incidentes similares, incluyendo las acciones que se han tomado para solucionarlos o los resultados de las auditorías internas

- Si y cómo la información adquirida a través del uso de la tecnología fue compartida con alguna entidad externa
- Estadísticas e información sobre las solicitudes bajo la Ley de Registros Públicos, incluyendo cómo han sido manejadas.
- El costo total anual de la tecnología, incluyendo el salario del personal y otros gastos continuos, y los fondos externos disponibles para financiar parte o la totalidad de estos gastos el año siguiente.

También puede haber otras formas de informar a la comunidad sobre la operación y efectividad del programa de vigilancia. Responder a las solicitudes bajo la Ley de Registros Públicos con tanta información como sea posible, tomando en cuenta factores como el derecho a la privacidad de las personas cuya información puede ser parte de la información solicitada, es una forma de permitir que los miembros de la comunidad interesados tengan acceso a información concreta sobre el programa. Crear comités permanentes de miembros de la comunidad, realizar regularmente eventos y foros públicos y establecer periodos de inspección abierta de la tecnología también puede mantener informada a la comunidad.

- *¿Cómo reevaluarán los funcionarios locales y el público la decisión de permitir el uso de vigilancia o las políticas y medidas de seguridad existentes?*

La decisión de la comunidad de aprobar la vigilancia debe ser reconsiderada anualmente. Si existe evidencia que cuestione si los beneficios de la vigilancia superan el costo y las inquietudes o si hay mejores formas de lograr el mismo propósito que cueste menos y conlleve menos riesgos, los responsables políticos deben solicitar la opinión de la comunidad y tomar las medidas que sean necesarias para abordar sus inquietudes. Esto puede requerir limitar el propósito o el alcance de la vigilancia, requerir modificaciones a la Política de Uso de la Vigilancia o explorar alternativas que aborden mejor las necesidades de la comunidad.

Conclusión

Las comunidades están comprendiendo cada vez más la necesidad de tomar decisiones inteligentes sobre el uso de la tecnología de vigilancia y asegurar que el tiempo, la energía y los recursos no se usen en sistemas que cuestan más, hacen menos y ponen en peligro los derechos de los miembros de la comunidad. Los miembros de la comunidad exigen y merecen que su voz sea escuchada en toda decisión sobre la tecnología de vigilancia. Transparencia, rendición de cuentas y supervisión adecuadas deben ser la regla al considerar toda propuesta sobre tecnologías de vigilancia. Esperamos que las recomendaciones de esta guía los ayuden a establecer políticas locales y estatales que aseguren que exista un proceso público consistente cada vez que se considera el uso de tecnología de vigilancia.

Anexo: Modelo de una ordenanza de vigilancia y seguridad comunitaria

A. PRINCIPIOS BÁSICOS DEL MODELO DE LA ORDENANZA

- **Debate público informado desde las primeras etapas del proceso:** notificar al público, distribuir información sobre la propuesta y realizar un debate público antes de solicitar fondos o avanzar con las propuestas de tecnología.
- **Determinar si los beneficios superan los costos e inquietudes:** los líderes locales, después de facilitar un debate público informado, deben considerar el costo (fiscal y para las libertades civiles) y determinar que la tecnología de vigilancia es adecuada o no antes de continuar.
- **Exhaustiva política de uso de la vigilancia:** los responsables políticos deben aprobar una Política de Uso de la Vigilancia legalmente ejecutable que incluya sólidas medidas de seguridad que protejan las libertades civiles, los derechos civiles y la seguridad.
- **Supervisión y rendición de cuentas continua:** adecuada supervisión y rendición de cuentas de la tecnología de vigilancia a través de un informe anual, evaluación de los responsables políticos y mecanismos de garantizar el cumplimiento.

B. TEXTO DEL MODELO DE LA ORDENANZA

[El Consejo de la Ciudad/ la Junta de Supervisores] han determinado que toda decisión sobre el uso de tecnología de vigilancia debe equilibrar sensatamente la necesidad de proteger los derechos y las libertades civiles, incluyendo la privacidad y libertad de expresión, y el costo para [la Ciudad/el Condado]. [El Consejo de la Ciudad/ la Junta de Supervisores] ha determinado que una transparencia, supervisión y rendición de cuentas adecuadas son esenciales para minimizar el riesgo potencial de las tecnologías de vigilancia. [El Consejo de la Ciudad/ la Junta de Supervisores] ha determinado que es esencial sostener un debate público informado lo más temprano posible para decidir si se debe adoptar o no la tecnología de vigilancia. [El Consejo de la Ciudad/ la Junta de Supervisores] ha determinado que es necesario establecer medidas de seguridad legalmente ejecutables para proteger las libertades y los derechos civiles antes de desplegar cualquier tipo de tecnología de vigilancia. [El Consejo de la Ciudad/ la Junta de Supervisores] ha determinado que, si se aprueba la tecnología de vigilancia, debe haber supervisión continua y realizar una evaluación anual para asegurar que las medidas de seguridad se estén cumpliendo y que los beneficios de la tecnología de vigilancia superen su costo.

POR CONSIGUIENTE, SE ACUERDA que [el Consejo de la Ciudad/ la Junta de Supervisores] de [la Ciudad/el Condado] adopte lo siguiente:

Sección 1. Título

Esta ordenanza llevará el nombre de Ordenanza de Vigilancia y Seguridad Comunitaria.

Sección 2. Requisito de aprobación por parte [del Consejo de la Ciudad/de la Junta de Supervisores]

1) Un ente de [la Ciudad/el Condado] debe obtener la aprobación [del Consejo de la Ciudad/de la Junta de Supervisores] durante una audiencia pública que se anuncie oportunamente antes de:

a) Solicitar fondos para la tecnología de vigilancia, incluyendo sin limitación aplicar para subsidios o solicitar o aceptar fondos estatales o federales o donaciones en especie y otros tipos de donaciones.
b) Adquirir nueva tecnología de vigilancia, incluyendo sin limitación procurar la tecnología sin intercambiar dinero o consideraciones.
c) Usar nueva tecnología de vigilancia o usar tecnología de vigilancia existente para un propósito, de una forma o en un lugar para lo que no fue aprobada por [el Consejo de la Ciudad/la Junta de Supervisores].
d) Celebrar un acuerdo con una entidad que no sea parte de [la Ciudad/el Condado] para adquirir, compartir o de cualquier forma usar tecnología de vigilancia o la información que recopile.

2) [Una Ciudad/Un Condado] debe obtener la aprobación [del Consejo de la Ciudad/de la Junta de Supervisores] antes de participar en cualquiera de las actividades descritas en la subsección (1)(b)-(d).

Sección 3. Información necesaria

1) La entidad de [la Ciudad/el Condado] que solicite la aprobación bajo la Sección 2 debe entregar [al Consejo de la Ciudad/a la Junta de Supervisores] un Informe del Impacto de la Vigilancia y una propuesta de la Política de Uso de la Vigilancia por lo menos cuarenta y cinco (45) días antes de la audiencia pública.
2) [El Consejo de la Ciudad/la Junta de Supervisores] debe hacer público de forma impresa o en línea el Informe del Impacto de la Vigilancia y la propuesta de la Política de Uso de la Vigilancia por lo menos treinta (30) días antes de la audiencia pública.

Sección 4. [El Consejo de la Ciudad/la Junta de Supervisores] debe determinar si los beneficios superan los costos y problemas potenciales

[El Consejo de la Ciudad/la Junta de Supervisores] solo puede aprobar una acción descrita en la Sección 2, subsección (1) de esta ordenanza después de determinar si los beneficios que la tecnología de vigilancia tendrá para la comunidad superarán su costo y que la propuesta protegerá las libertades y los derechos civiles.

Sección 5. Idoneidad de la tecnología de vigilancia existente

Todo organismo de [la Ciudad/el Condado] que posea o use tecnología de vigilancia antes de que esta ordenanza entre en vigor debe entregar una propuesta de la Política de Uso de la Vigilancia a más tardar noventa (90) días antes de que esta ordenanza entre en vigor para su evaluación y aprobación por parte [del Consejo de la Ciudad/de la Junta de Supervisores]. Si esta evaluación y aprobación no ocurre antes de que transcurran sesenta (60) días de la fecha de entrega, el organismo [de la Ciudad/del Condado] debe dejar de usar la tecnología de vigilancia hasta que ocurra dicha evaluación y aprobación.

Sección 6. Supervisión después de la aprobación [del Consejo de la Ciudad/de la Junta de Supervisores]

1) Un organismo de [una Ciudad/un Condado] que haya obtenido la aprobación para el uso de la tecnología de vigilancia debe entregar un Informe de Vigilancia de cada una de las tecnologías de vigilancia [al Consejo de la Ciudad/a la Junta de Supervisores] antes de que transcurran (12) meses de la aprobación [del Consejo de la Ciudad/de la Junta de Supervisores] y anualmente el 1 de noviembre de cada año o antes.
2) Dependiendo de la información que contenga el Informe de Vigilancia, [el Consejo de la Ciudad/la Junta de Supervisores] debe determinar si los beneficios para la comunidad de la tecnología de vigilancia superan los costos y si las libertades y los derechos civiles están protegidos. Si los beneficios no superaran los costos o los derechos y las libertades civiles no están protegidas, [el Consejo de la Ciudad/la Junta de Supervisores] debe ordenar que se deje de usar la tecnología de vigilancia y/o requerir modificaciones a la Política de Uso de la Vigilancia que solucionen los problemas mencionados arriba.
3) A más tardar el 15 de enero de cada año, [el Consejo de la Ciudad/la Junta de Supervisores] debe realizar una reunión pública y publicar de forma impresa o en línea un informe que incluya la siguiente información del año anterior:
    a. Un resumen de todas las solicitudes aprobadas por parte [del Consejo de la Ciudad/de la Junta de Supervisores] bajo la Sección 2 o Sección 5, incluyendo si [el Consejo de la Ciudad/la Junta de Supervisores] aprobó o rechazó la propuesta y/o si requirió que se cambiara una Política de Uso de la Vigilancia propuesta antes de ser aprobada
    b. Todos los Informes de Vigilancia entregados.

Sección 7. Definiciones

Las definiciones que aparecen a continuación se aplican a esta Ordenanza:

1) "Informe de Vigilancia" se refiere a un informe escrito sobre una tecnología de vigilancia específica que incluye todo lo siguiente:
    a. Una descripción de cómo y con cuánta frecuencia se usó la tecnología.
    b. Si y con qué frecuencia la información adquirida a través del uso de la tecnología de vigilancia fue compartida con entidades externas, el nombre de la entidad que recibió la información, el(los) tipo(s) de información que se compartió, qué estándares legales se usaron para compartir la información y las razones que justifican haber compartido la información.
    c. Un resumen de las quejas y las inquietudes que tenga la comunidad sobre la tecnología.
    d. Los resultados de las auditorías internas, la información sobre las violaciones a la Política de Uso de la Vigilancia y las acciones tomadas al respecto.
    e. Información, incluyendo estadísticas de las actividades criminales, que puede ayudar a la comunidad a evaluar si la tecnología de vigilancia ha sido efectiva para alcanzar los propósitos que fueron identificados.
    f. Estadísticas e información sobre las solicitudes bajo la Ley de Registros Públicos, incluyendo las tasas de respuesta.

g. El costo total anual de la tecnología de vigilancia, incluyendo el salario del personal y los gastos continuos, y la fuente que financiará la tecnología el próximo año.

2) "Entidad de [la Ciudad/ el Condado]" se refiere a todo departamento, oficina, división o unidad de [la Ciudad/ el Condado].
3) "Tecnología de vigilancia" se refiere a todo dispositivo electrónico, todo sistema que usa un dispositivo electrónico o dispositivos similares usados, diseñados o cuya intención principal sea recopilar, retener, procesar o compartir información de audio, video, ubicación, térmica, olfativa o información asociada específicamente con, o capaz de estar asociada a, una persona o un grupo.
4) "Informe del Impacto de la Vigilancia" se refiere a un informe publicado que contenga como mínimo: (a) información que describe la tecnología de vigilancia y cómo funciona, incluyendo la descripción de los productos de los fabricantes; (b) información de los propósitos propuestos para la tecnología de vigilancia; (c) los lugares donde será desplegada y las estadísticas del crimen en esos lugares; (d) una evaluación que identifica el impacto potencial sobre las libertades civiles y derechos civiles y una discusión de los planes para proteger los derechos del público y (e) el costo fiscal de la tecnología de vigilancia, incluyendo su compra inicial, personal y otros gastos continuos y todas las fuentes actuales y potenciales de financiamiento.
5) "Política de Uso de la Vigilancia" se refiere a una política hecha del dominio público y legalmente ejecutable para el uso de la tecnología de vigilancia que como mínimo especifique lo siguiente:
    a. **Propósito:** propósitos específicos que se supone que la tecnología de vigilancia debe lograr.
    b. **Uso autorizado:** usos que han sido autorizados, las reglas y procesos requeridos antes de estos usos y los usos que están prohibidos.
    c. **Recopilación de información:** información que puede ser recopilada por la tecnología de vigilancia.
    d. **Acceso a la información:** personas que pueden acceder o usar la información recopilada y las reglas y procesos requeridos antes de acceder o usar la información.
    e. **Protección de la información:** medidas de seguridad para proteger la información de acceso no autorizado, incluyendo codificación y mecanismos para controlar el acceso.
    f. **Retención de la información:** periodo de tiempo, si es que ha sido establecido, durante el que se retendrá regularmente la información recopilada por la tecnología de vigilancia, la razón por la que dicho periodo de retención es adecuado para lograr los propósitos de la vigilancia, los procesos que se usan para borrar regularmente la información cuando termine el periodo y las condiciones específicas que deben ser satisfechas para retener la información después de este periodo.
    g. **Acceso público:** cómo la información recopilada puede ser accedida o usada por los miembros del público, incluyendo las personas acusadas de un delito.
    h. **Compartir información con terceros:** si y cómo otras entidades de [la Ciudad/el Condado] o entidades que no son de [la Ciudad/el Condado] pueden acceder o usar la información, incluyendo las justificaciones o estándares legales necesarios para hacerlo y las obligaciones impuestas al receptor de la información.
    i. **Capacitación:** capacitación que requiere toda persona autorizada para usar la tecnología de vigilancia o tener acceso a la información recopilada por la tecnología de vigilancia, incluyendo los materiales usados para la capacitación.

j. **Auditorías y supervisión:** mecanismos para garantizar que la Política de Uso de la Vigilancia se cumpla, incluyendo el personal interno asignado para asegurar que se cumpla la política, los métodos internos para archivar información sobre el uso de la tecnología o el acceso a la información recopilada por la tecnología, las medidas técnicas para monitorear el uso indebido, toda persona o entidad independiente con autoridad de supervisión y las sanciones legalmente ejecutables en caso de violaciones a la política.

Sección 8. Cumplimiento

1) Toda violación a esta Ordenanza se considera un agravio y toda persona puede interponer procesos de medidas cautelares, medidas declarativas o mandatos judiciales en cualquier tribunal que tenga jurisdicción competente para hacer cumplir la Ordenanza.
2) Un tribunal puede ordenar el pago de los costes y honorarios legales razonables a la parte vencedora de la acción legal promovida para hacer cumplir esta Ordenanza.
3) Además, en el caso de violaciones voluntarias, intencionales e imprudentes de esta Ordenanza, una persona puede ser considerada culpable de un delito menor y puede ser sancionada con una multa no mayor a $1,000 por violar la ordenanza, encarcelamiento en la cárcel del condado durante no más de seis meses o tanto la multa y el encarcelamiento.

Sección 9. Divisibilidad

Las disposiciones de esta Ordenanza son divisibles. Si cualquier parte o disposición de esta Ordenanza o la aplicación de esta ordenanza a cualquier persona o circunstancia se considera inválida, el resto de esta Ordenanza, incluyendo la aplicación de dicha parte o disposición a otras personas o circunstancias, no se verá afectada por esta retención y debe seguir en vigor.

Sección 10. Fecha de vigencia

Esta Ordenanza entrará en vigor el [FECHA].

Notas finales

[1] Por ejemplo, la Declaración de la Misión del Departamento de Policía de San Francisco establece que "las estrategias policivas deben preservar y promover los valores democráticos" y que "la policía debe respetar y proteger los derechos de todos los ciudadanos que son garantizados por la Constitución del estado". Declaración de la Misión, Departamento de Policía, http://sf-police.org/index.aspx?page=1616.

[2] B.T. Lewis & Taymeh Jahsi, *Stop using social media to monitor south Fresno's protesters*, The Fresno Bee*,* Feb. 10, 2016, *disponible en* http://www.fresnobee.com/opinion/readers-opinion/article59388976.html.

[3] Matt Cagle. *This Surveillance Software is Probably Spying on #BlackLivesMatter*, ACLU of Northern California (Dec. 15, 2015), https://www.aclunc.org/blog/surveillance-software-probably-spying-blacklivesmatter.

[4] *Ver* Press Release, Leadership Conference, Civil Rights Principles for the Era of Big Data, http://www.civilrights.org/press/2014/civil-rights-principles-big-data.html.

[5] Terrence O'Brien, *Caught Spying on Student, FBI Demands GPS Tracker Back*, Wired.com, Oct. 7, 2010, http://www.wired.com/2010/10/fbi-tracking-device/.

[6] Michael Isikoff, *FBI Tracks Suspects' Cell Phones Without* a Warrant, Newsweek, Feb, 18, 2010 (updated Mar. 13, 2010), *disponible en* http://www.newsweek.com/fbi-tracks-suspects-cell-phones-without-warrant-75099.

[7] David Kravets, *Rights Groups Decry New NSA Leak: Snooping on Muslim-Americans' E-mail*, Ars Technica (July 9, 2014), http://arstechnica.com/tech-policy/2014/07/rights-groups-decry-new-nsa-leak-snooping-on-muslim-americans-email/.

[8] Matt Apuzzo and Al Baker, *New York to Appoint Civilian to Monitor Police's Counterterrorism Activity*, N.Y. Times, Jan. 7, 2016, *disponible en* http://www.nytimes.com/2016/01/08/nyregion/new-york-to-appoint-monitor-to-review-policescounterterrorism-activity.html; Case page, Raza v. City of New York – Legal Challenge to NYPD Muslim Surveillance Program, Jan. 7, 2016, https://www.aclu.org/cases/raza-v-city-new-york-legal-challenge-nypd-muslim-surveillanceprogram.

[9] *Ver* Tanvir v. Holder, Case No. 13-CV-6951 (S.D. N.Y. Apr. 22, 2014) (First Amended Complaint), *disponible en* http://apps.washingtonpost.com/g/documents/world/lawsuit-accusing-us-of-putting-people-on-no-fly-list-after-theysay-they-wont-spy/941/.

[10] George Joseph, *Exclusive: Feds Regularly Monitored Black Lives Matter Since Ferguson*, The Intercept, July 24, 2015, https://theintercept.com/2015/07/24/documents-show-department-homeland-security-monitoring-black-lives-mattersince-ferguson/.

[11] Matt Cagle. *This Surveillance Software is Probably Spying on #BlackLivesMatter*, ACLU of Northern California (Dec. 15, 2015), https://www.aclunc.org/blog/surveillance-software-probably-spying-blacklivesmatter; *ver también* Shaun King, *Fresno police join group of officials monitoring #BlackLivesMatter hashtag, labeling a peaceful movement a threat*, N.Y. Daily News, Dec. 17,
2015, *disponible en* http://www.nydailynews.com/news/national/king-monitoring-blacklivesmatter-labels-movementthreat-article-1.2468808.

[12] David Rogers, *Black Lives Matter Supporters in Oregon Targeted by State Surveillance*, ACLU Speak Freely blog, Nov. 11, 2015, https://www.aclu.org/blog/speak-freely/black-lives-matter-supporters-oregon-targeted-state-surveillance; Courtney Sherwood, *Oregon attorney general 'appalled' by probe of Black Lives Matter*, Reuters, Nov. 11, 2015, http://www.reuters.com/article/us-oregon-race-idUSKCN0T104N20151112.

[13] Jeremy Gillula and Dave Maass, *What You Can Learn from Oakland's Raw ALPR Data*, Electronic Frontier Foundation, Jan. 21, 2015, https://www.eff.org/deeplinks/2015/01/what-we-learned-oakland-raw-alpr-data.

[14] Angel Jennings, *Richard Winston & James Rainey, Sherriff's Secret Air Surveillance of Compton Sparks Outrage*, L.A. Times, Apr. 23, 2014, *disponible en* http://www.latimes.com/local/lanow/la-me-ln-sheriffs-surveillance-compton-outrage-20140423-story.html.

[15] Andrea Peterson, *LOVEINT: When NSA Officers Use Their Spying Power on Love Interests*, Wash. Post, Aug. 24, 2013, *disponible en* http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/24/loveint-when-nsa-officers-use-theirspying-power-on-love-interests/.

[16] *Ver* Julia Angwin & Jennifer Valentino-DeVries, *New Tracking Frontier: Your License Plates*, Wall St. J., Sep. 29, 2012, *disponible en* http://online.wsj.com/news/articles/SB10000872396390443995604578004723603576296.

[17] Jenna McLaughlin, *The FBI v. Apple Debate Just Got Less White*, The Intercept, Mar. 8, 2016, https://theintercept.com/2016/03/08/the-fbi-vs-apple-debate-just-got-less-white/.

[18] Rania Khalek, *Activists of Color Lead Charge Against Surveillance, NSA*, Truthout, Oct. 30, 2013, http://www.truthout.org/news/item/19695-activists-of-color-at-forefront-of-anti-nsa-movement.

[19] Riley v. California, 134 S. Ct. 2473, 2489 (2014).
[20] *United States v. Jones*, 132 S.Ct. 945, 955, 56 (2012).
[21] Adam Goldman & Matt Apuzzo, *NYPD Defends Tactics over Mosque Spying; Records Reveal New Details on Muslim Surveillance*, Huffington Post (Feb 25, 2012), http://www.huffingtonpost.com/2012/02/24/nypd-defends-tacticsover_n_1298997.html; Adam Goldman & Matt Apuzzo, *New York Drops Unit That Spied on Muslims*, N.Y. Times, April 15, 2014, *disponible en* http://www.nytimes.com/2014/04/16/nyregion/police-unit-that-spied-on-muslims-isdisbanded.html.
[22] Hina Shamsi and Ramzi Kassem, *The NYPD spied on Muslim Americans. Will a court settlement change anything?*, The Guardian, Jan. 8, 2016, http://www.theguardian.com/commentisfree/2016/jan/08/nypd-spied-muslim-americans-willcourt-settlement-bring-change.
[23] Angel Jennings, Richard Winston & James Rainey, *Sherriff's Secret Air Surveillance of Compton Sparks Outrage*, L.A. Times, Apr. 23, 2014, *disponible en* http://www.latimes.com/local/lanow/la-me-ln-sheriffs-surveillance-compton-outrage-20140423-story.html.
[24] [24] *Police Executive Research Forum, How Are Innovations in Technology Transforming Policing?* 26 (Jan. 2012) [hereinafter PERF Report], *disponible en* http://www.policeforum.org/assets/docs/Critical_Issues_Series/how%20are%20innovations%20in%20technology%20transforming%20policing%202012.pdf.
[25] Comunicado de prensa, Office of the Controller, *Butkovitz Alarmed by Police Camera Program*, June 20, 2012, http://www.philadelphiacontroller.org/page.asp?id=792.
[26] *Ver* Fazaga v. FBI, 844 F. Supp.2d 1022 (C.D. Cal. 2012).
[27] Adam Goldman, *NYPD settles lawsuits over Muslim monitoring*, Wash. Post, Jan. 7, 2016, *disponible en* https://www.washingtonpost.com/world/national-security/nypd-settles-lawsuits-over-muslimmonitoring/2016/01/07/bdc8eb98-b3dc-11e5-9388-466021d971de_story.html.
[28] *Ver* Tim Cushing, *Another Bogus Hit from a License Plate Reader Results in Another Citizen Surrounded by Cops with Guns Out*, TechDirt (May 23, 2014), https://www.techdirt.com/articles/20140513/07404127218/another-bogus-hit-license-platereader-results-another-citizen-surrounded-cops-with-guns-out.shtml.
[29] Simposio *The Value of Privacy*, U. Cal.-Hastings School of L. Const. L. Q., Apr. 7, 2014 (oral remarks), *disponible en* http://livestre.am/4P7Lk.
[30] Cal. Civil Code § 1798.29 (2014).
[31] Larry Ponemon, *Cost of Data Breaches Rising Globally, Says '2015 Cost of a Data Breach Study: Global Analysis,'* May 27, 2015, https://securityintelligence.com/cost-of-a-data-breach-2015/.
[32] Will Kane, *Oakland to Limit Surveillance Center to Port, Airport*, S.F. Gate, Mar. 6, 2014, *disponible en* http://www.sfgate.com/bayarea/article/Oakland-to-limit-surveillance-center-to-port-5290273.php.
[33] Cyrus Farivar, *In rare move, Silicon Valley county gov't kills stingray acquisition*, Ars Technica, May 7, 2015, http://arstechnica.com/tech-policy/2015/05/in-rare-move-silicon-valley-county-govt-kills-stingray-acquisition/.
[34] Comunicado de prensa, *San Jose Police Provide Statement Regarding Purchase of Unmanned Aerial System (UAS)*, San Jose Police Dept., Aug. 5, 2014, *disponible en* http://www.sjpd.org/iNews/viewPressRelease.asp?ID=1874.
[35] Robert Salonga, *San Jose: Police apologize for drone secrecy, promise transparency*, San Jose Mercury News, Aug. 5, 2014, *disponible en* http://www.mercurynews.com/crime-courts/ci_26279254/san-jose-police-apologize-secret-drone-purchasepromise.
[36] *Riley v. California*, 573 U.S. (2014), Slip Op. at *28.
[37] U.S. v. Jones, 132 S. Ct. 945, 954 (2012) (Sotomayor, J., concurring); *id.* at 957 (Alito, Ginsberg, Breyer, and Kagan, J., concurring in the judgment).
[38] Charlie Savage and Jonathan Wiseman, *N.S.A. Collection of Bulk Call Data Is Ruled Illegal*, N.Y. Times, May 7, 2015, *disponible en* http://www.nytimes.com/2015/05/08/us/nsa-phone-records-collection-ruled-illegal-by-appeals-court.html; Klayman v. Obama, Civ. No. 13-0851 (D.D.C. Dec. 16, 2013).
[39] Ballot Pamplet., Proposed Amendments to Cal. Const. with Arguments to Voters, Gen. Elec. (Nov. 7, 1972).
[40] White v. Davis, 533 P.2d (Cal. 1975).
[41] People v. Cook 41 Cal. 3d 373 (1985).
[42] Robins v. Pruneyard Shopping Center, 592 P.2d 899 (Cal. 1979) (estableciendo que bajo la Constitución de California los miembros del público tienen derecho legal a distribuir folletos y solicitar firmas en un centro comercial de propiedad privada), *aff'd*, .447 U.S. 74 (1980).
[43] Cal. Penal Code §§ 1546-1546.4. *See generally* Tracy Seipel and Eric Kurhi*, California digital privacy laws boosted, protecting consumers from Big Brother, big business*, San Jose Mercury News, Oct. 9, 2015, *disponible en* http://www.mercurynews.com/health/ci_28948653/california-digital-privacy-laws-boosted-protecting-consumersfrom.

[44] Cal. Gov't Code § 53166.
[45] Cal. Civil Code §§ 1798.29, 1798.82, and 1798.90.5.
[46] Jennifer Steinhauer and Jonathan Weisman, *U.S. Surveillance in Place Since 9/11 Is Sharply Limited*, N.Y. Times, Jun. 2, 2015, *disponible en* http://www.nytimes.com/2015/06/03/us/politics/senate-surveillance-bill-passes-hurdle-butshowdown-looms.html?_r=0; *see also* U.S.A. Freedom Act, H.R. 2048, 114th Cong. (2016).
[47] Allie Bohm, *Status of Location Privacy Legislation in the States*, ACLU Free Future (April 8, 2014), https://www.aclu.org/blog/technology-and-liberty-national-security/status-location-privacy-legislation-states (as of May 6, 2014).
[48] Allie Bohm, *Status of 2014 Domestic Drone Legislation in the States*, ACLU Free Future (April 22, 2014), https://www.aclu.org/blog/technology-and-liberty/status-2014-domestic-drone-legislation-states (as of May 6, 2014).
[49] *Smart About Surveillance*, ACLU of California, http://www.aclunc.org/smartaboutsurveillance.
[50] *Id.*
[51] Entrevista con Brian Hofer, *Transparency over secrecy: Oakland's surveillance policy*, KALW Local Public Radio, *disponible en* http://kalw.org/post/transparency-over-secrecy-oakland-s-surveillance-policy#stream/0.
[52] *See* Bonnie Eslinger, *Menlo Park Council Approves Ordinance Regulating Police Use of Surveillance*, San Jose Mercury News, May 14, 2014, *disponible en* http://www.mercurynews.com/breaking-news/ci_25766277/menlo-park-council-approvesordinance-regulating-police-use; *Seattle City Council Enacts Groundbreaking Legislation Protecting Residents' Civil Liberties*, Local Progress (May 1, 2013), http://localprogress.org/seattle-city-council-enacts-groundbreaking-legislation-protectingresidents-civil-liberties/.
[53] U.S. Dep't of Homeland Security, *CCTV: Developing Best Practices* (2007), disponible en http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_cctv_2007.pdf.
[54] *State of Surveillance in California – Findings and Recommendations,* ACLU of California, Jan. 2015, *disponible en* https://www.aclunc.org/sites/default/files/201501-aclu_ca_surveillancetech_summary_and_recommendations.pdf.
[55] Redlands Police Department, Citizen Privacy Council, http://www.cityofredlands.org/police/CPC.
[56] Halima Kazen, *Watching the Watchers: Oakland Seeks Control of Law Enforcement Surveillance*, The Guardian, July 13, 2015, *disponible eb* http://www.theguardian.com/us-news/2015/jul/13/oakland-law-enforcement-surveillance.
[57] Memorando, *Establishing Ad Hoc Committee to Review the Community Warning System and Industrial Safety Ordinance* (Sept. 18, 2012), http://64.166.146.155/agenda_publish.cfm?mt=ALL&get_month=9&get_year=2012&dsp=agm&seq=12339&rev=0&ag=241&ln=23604&nseq=0&nrev=0&pseq=12303&prev=0.
[58] Discurso de Malkia Cyril, *Targeted Surveillance, Civil Rights, and the Fight for Democracy*, Center for Media Justice, Oct. 13, 2015, *disponible en* http://centerformediajustice.org/2015/10/13/targeted-surveillance-civil-rights-and-the-fightfor-democracy/.
[59] *Ver memorando,* City Administrator's Weekly Report (Apr. 25, 2014), http://www2.oaklandnet.com/oakca1/groups/cityadministrator/documents/report/oak046804.pdf.
[60] http://www2.oaklandnet.com/Government/o/CityAdministration/d/PrivacyAdvisoryCommission/index.htm
[61] Matt Richtel, *A Police Gadget Tracks Phones? Shhh! It's Secret*, N.Y. Times, Mar. 15, 2015, *disponible en* http://www.nytimes.com/2015/03/16/business/a-police-gadget-tracks-phones-shhh-its-secret.html?_r=0; Cyrus Farivar, *In rare move, Silicon Valley county gov't kills stingray acquisition*, Ars Technica, May 7, 2015, http://arstechnica.com/tech-policy/2015/05/in-rare-move-silicon-valley-county-govt-kills-stingray-acquisition/.
[62] Ali Winston, *Oakland City Council Rolls Back the Domain Awareness Center*, East Bay Express (Mar. 5, 2014), http://www.eastbayexpress.com/SevenDays/archives/2014/03/05/oakland-city-council-rolls-back-the-dac.
[63] Cyrus Farivar, *In rare move, Silicon Valley county gov't kills stingray acquisition*, Ars Technica, May 7, 2015, http://arstechnica.com/tech-policy/2015/05/in-rare-move-silicon-valley-county-govt-kills-stingray-acquisition/.
[64] John Malkin, *Surveillance City?* GoodTimes, Jan 29, 2014, http://www.gtweekly.com/index.php/santacruznews/goodtimescoverstories/5386surveillancecity.html.
[65] Robert Salonga, *San Jose: Police Apologize for Drone Secrecy, Promise Transparency*, San Jose Mercury News, Aug 5, 2014, *disponible en* http://www.mercurynews.com/crime-courts/ci_26279254/san-jose-police-apologize-secret-drone-purchasepromise.
[66] *Ver* Oakland City Auditor, *Police Technology Performance Audit: FY 2006–07 through 2010–11* (2012), *disponible en* http://www.oaklandauditor.com/images/oakland/auditreports/0pd%20tech.pdf.
[67] *Ver* Citris, *Cistris Study on SF Public Cameras Released* (Jan. 9, 2009), http://citris-uc.org/citris-study-on-sf-publiccameras-released/.
[68] *Ver* David P. Farrington & Brandon C. Welsh, *Effects of Improved Street Lighting on Crime: A Systematic Review,* Home Office Research Study 251 (Aug. 2002), p. 42; Ronald V. Clarke, U.S. Department of Justice, Office of Community

Oriented Policing Services, *Improving Street Lighting to Reduce Crime in Residential Areas* (Dec. 2008), *disponible en* http://cops.usdoj.gov/Publications/e1208-StreetLighting.pdf; Jay Beeber, *Collision Analysis of the Photo Enforced Intersection in Walnut, CA*, http://www.thenewspaper.com/rlc/docs/2014/ca-walnut.pdf.

[69] *Ver* Steve Scauzillo, *Red Light Cameras Being Stopped*, L.A. Daily News (Jan. 21, 2014), http://www.dailynews.com/general-news/20140121/red-light-cameras-being-stopped.

[70] Informe PERF, *supra* note 24, at 44.

[71] United States v. Jones, 132 S. Ct. 945 (2012); Joann Pan, *FBI Turns Off 3000 GPS Devices After Ruling*, Mashable (Feb. 27, 2012), http://mashable.com/2012/02/27/fbi-turns-off-3000-gps-devices/.

[72] Kashmir Hill, *Whoops, Anyone Could Watch California City's Police Surveillance Cameras*, Forbes.com (Aug. 21, 2014), http://www.forbes.com/sites/kashmirhill/2014/08/11/surveillance-cameras-for-all/.

[73] *Seattle City Council Enacts Groundbreaking Legislation Protecting Residents' Civil Liberties*, Local Progress (May 1, 2013), http://localprogress.org/seattle-city-council-enacts-groundbreaking-legislation-protecting-residents-civil-liberties/; Jamela Debelak, ACLU of Washington, *Surveillance: Spokane Acts to Protect Privacy and Provide Transparency* (Aug. 21, 2013), https://aclu-wa.org/blog/surveillance-spokane-acts-protect-privacy-and-provide-transparency.

[74] Matt Cagle, *Alameda County Just Got a Privacy Upgrade – Alameda County, It's Your Move*, ACLU of Northern California blog, Nov. 17, 2015, https://www.aclunc.org/blog/california-just-got-privacy-upgrade-alameda-county-its-your-move.

[75] Matt Cagle, *Alameda County Just Got a Privacy Upgrade – Alameda County, It's Your Move*, ACLU of Northern California blog, Nov. 17, 2015, https://www.aclunc.org/blog/california-just-got-privacy-upgrade-alameda-county-its-your-move.

[76] Seattle City Council, Public Safety, Civil Rights and Technology Committee May 2, 2012, Seattle Channel, at 38:55, http://www.seattlechannel.org/mayor-and-council/city-council/20122013-public-safety-civil-rights-and-technologycommittee/?videoid=x23397.

[77] Terry McFadden, *Technology Helping Police to Receive Warrants Faster*, WNDU.com (July 8, 2013), http://www.wndu.com/news/specialreports/headlines/Technology-helping-police-to-receive-search-warrants-faster--214651051.html.

[78] 18 U.S.C. § 2518(5) (2014).

[79] Ohio State Highway Patrol Policy No. OSP-103.29 (revisado Dec. 23, 2008).

[80] Julia Reynolds, *Monterey County Grand Jury Finds Computer Data Risks*, Monterey Herald, Aug. 21, 2014, *disponible en* http://www.montereyherald.com/news/ci_26009592/monterey-county-grand-jury-finds-computer-data-risks.

[81] Dianne Feinstein, *NSA Officers Spy on Love Interests*, Wall St. J., Aug. 23, 2013, *disponible en* http://blogs.wsj.com/washwire/2013/08/23/nsa-officers-sometimes-spy-on-love-interests/; Anjali Hemphill, *Dating on Duty: Officers Accused of Screening Dates Using Police System*, CBS 13 Sacramento (Aug. 22, 2014), http://sacramento.cbslocal.com/2014/08/22/dating-on-duty-officers-accused-of-screening-dates-using-police-system/.

[82] *Ver* Bonnie Eslinger, *Menlo Park Council Approves Ordinance Regulating Police Use of Surveillance*, San Jose Mercury News, May 14, 2014, *disponible en* http://www.mercurynews.com/breaking-news/ci_25766277/menlo-park-council-approvesordinance-regulating-police-use.

[83] PERF Report, *supra* note 24, at 36.

[84] Dan Brekke*, Oakland Approves Scaled-Back Version of Disputed Surveillance Center,* KQED.com, Mar. 5, 2014, http://ww2.kqed.org/news/2014/03/04/oakland-mayor-jean-quan-suggests-scaling-back-domain-awareness-center.

[85] George Hostetter, *Former Judge Wanger Writes Far-Ranging Audit on Fresno Video Policing*, Fresno Bee, Jan. 7, 2014, *disponible en* http://www.fresnobee.com/2014/01/07/3701754/judge-wanger-delivers-impressive.html.

Citas de la contraportada

Editorial, *ACLU offers a smart safeguard for using surveillance technology*, The Los Angeles Times, Nov. 23, 2014, *disponible en* http://www. latimes.com/opinion/editorials/la-ed-surveillance-and-privacy-20141123-story.html.

Editorial, *Bay Area governments must protect citizen privacy*, San Francisco Chronicle, Feb. 25, 2015, *disponible en* http://www.sfchronicle. com/opinion/editorials/article/Bay-Area-governments-must-protect-citizen-privacy-6101993.php.

Steven Greenhut, *Surveillance is sneaking its way into cities*, The San Diego Union-Tribune, Nov. 17, 2014, *disponible en* http://www.sandiegouniontribune.com/news/2014/nov/17/surveillance-sneaking-cities-model-ordinance-aclu/.

Editorial, *ACLU push for surveillance policy is timely*, San Jose Mercury News, Nov. 13, 2014, *disponible en* http://www.mercurynews.com/ opinion/ci_26932183/mercury-news-editorial-aclu-push-surveillance-policy-is.

(Back Cover)

La policía gasta miles de millones de dólares en tecnología de vigilancia muy sofisticada e invasiva. Muchos de estos programas son lanzados sin ser discutidos con el público, sin considerar con cuidado los costos y beneficios o tener políticas adecuadas para evitar su uso inadecuado y proteger los derechos de las personas.

Esta guía proporciona un marco paso a paso para hacer las preguntas correctas y recibir las respuestas necesarias sobre las propuestas de vigilancia e incluir mecanismos apropiados de transparencia, rendición de cuentas y supervisión. Esta guía también incluye docenas de casos de estudio que resaltan enfoques inteligentes, errores que se deben evitar y ejemplos del contenido que los responsables políticos pueden adoptar para asegurar que se use el debido proceso cada vez que consideran una propuesta de vigilancia.

"El enfoque de la ACLU para evaluar nuevas tecnologías es tan pragmático que sería una tontería que las ciudades, los condados y las agencias del orden público de toda California no lo adoptaran."
–Editorial, Los Angeles Times

"Instamos a los gobiernos de más ciudades y condados a… [considerar] una ordenanza que establecería reglas específicas sobre lo que se puede hacer con la información privada de los ciudadanos."
–Editorial, San Francisco Chronicle

"Es fácil comprender el valor del enfoque de [la ACLU] en todas las áreas del gobierno…"
–Steven Greenhut, San Diego Union-Tribune

"Los funcionarios electos, no los departamentos de policía, debe establecer las políticas para el uso del equipo de vigilancia. Esto es lo que recomienda la ACLU y es lo más sensato." –Editorial, San Jose Mercury News

Footers:

TOMANDO DECISIONES INTELIGENTES SOBRE VIGILANCIA: UNA GUÍA PARA LAS COMUNIDADES

EN LÍNEA EN ACLUNC.ORG/SMARTABOUTSURVEILLANCE