UNalienable

INTERCAMBIO DE DATOS ENTRE AGENCIAS

MARZO DE 2021

ACLU Mississippi

Antecedentes / Resumen Ejecutivo

Si bien gran parte de la cooperación entre las agencias locales, estatales y federales se produce a simple vista, los avances en la tecnología han facilitado una arena separada y más secreta en la que este enredo también tiene lugar. A través de programas de intercambio de datos como **Comunidades Seguras** (S-Comm) y vigilancia interjurisdiccional, las agencias de aplicación de la ley y de inmigración en todos los niveles del gobierno pueden compartir los datos personales de las personas bajo la apariencia de seguridad pública. Sin embargo, la evidencia muestra que estas prácticas tienen el efecto contrario de interferir con la policía local, facilitar la discriminación y violar nuestros valores constitucionales con poca o ninguna responsabilidad.

Este resumen de políticas describe los daños que surgen cuando las agencias gubernamentales intercambian los datos personales de las personas con el propósito de hacer cumplir la ley de inmigración y comparte recomendaciones para mitigar el abuso.

Comunidades Seguras

En el momento de un arresto, los agentes del orden público estatales o locales recopilan datos de huellas digitales que se envían automáticamente a la Oficina Federal de Investigaciones (FBI) y se comparan con su sistema de identificación biométrica. A través de S-Comm, que fue reemplazado brevemente por el Programa de cumplimiento prioritario, los datos de huellas digitales también se comparten con el Departamento de Seguridad Nacional (DHS), que los ejecuta a través de su propio sistema biométrico para revisar el historial de inmigración de las personas. La sugerencia de una infracción de inmigración a menudo hace que el Servicio de Inmigración y Control de Aduanas (ICE) envíe a la agencia de arresto una **solicitud de retención**, que puede últimamente resultar en la transferencia del detenido a la custodia del Servicio de ICE y su eventual deportación. ICE sacó a **más de 600** Misisipianos indocumentados de sus comunidades en el año fiscal 2018 usando S-Comm. Pero mientras que los partidarios de este programa lo defienden como un instrumento de investigación útil, S-Comm presenta una serie de desafíos dañinos a nivel local y en la práctica.

Desempoderamiento De Las Fuerzas Del Orden Locales

S-Comm desempodera a las fuerzas del orden local por **integrar a fuerzas** a ICE en sus operaciones. Las jurisdicciones no tienen voz sobre si deben incluirse o no en el programa S-Comm, ni sobre qué datos se comparten con su oficina local de ICE o qué acción de aplicación de la ley de inmigración es apropiada después de una orden de detención. Esta imposición del gobierno federal viene en contra de la fuerte **resistencia** de los organismos estatales y locales. Las oficinas locales de aplicación de la ley son las que mejor saben cómo mantener seguras a sus comunidades, pero S-Comms dificulta su capacidad para hacerlo. Sonia Lin de La Clinica de Inmigraciion de la facultad de derecho de Cardozo **advirtió** que, al impulsar S-Comm como un programa obligatorio, las agencias federales “ignoraron las serias preocupaciones sobre la vigilancia comunitaria, la carga sobre los socios locales y estatales, los derechos de privacidad y el mayor riesgo de discriminación racial”.

Perfiles Policiales

La **investigación** por organizaciones como el Consejo Estadounidense de Inmigracion (American Immigration Council) sugiere que S-Comm inflama la elaboración de perfiles y facilita prácticas policiales arbitrarias y discriminatorias. Por ejemplo, un oficial puede arrestar a una persona de color simplemente para verificar su estatus migratorio. A través de S-Comm, estas prácticas se manifiestan de manera más devastadora contra la comunidad hispana: Aunque representan solo el 77 por ciento de la población estadounidense indocumentada,

los hispanos representan el **93 por ciento** de los identificados para deportación a través del programa.

Fracaso Al Avanzar La Seguridad Pública

Al alejar el control de los actores locales, se espera que S-Comm no avance la seguridad pública. ICE afirma que S-Comm solo se dirige a delincuentes graves y agresores violentos, pero **los estudios muestran** que los infractores de bajo nivel, las víctimas de delitos (incluyendo las víctimas de violencia doméstica) y aquellos que fueron arrestados injustamente a menudo terminan envueltos en su operación. Estos efectos colaterales surgen porque las huellas digitales se comparten automáticamente con DHS, **incluso cuando** el arresto fue ilegal y/o se desestimó el cargo penal. **Un estudio de 2014** publicado en el Journal of Law & Economics encontró que, a pesar de las más de 250,000 detenciones que habían ocurrido bajo S-Comm en ese momento, "el programa no ha cumplido su objetivo central de hacer que las comunidades sean más seguras." No hubo una reducción significativa de la delincuencia en los 3,000 condados estudiados, incluyendo los delitos violentos.

Ciudadanos Como Daño Colateral

Los errores de la base de datos y otros defectos en el procedimiento de S-Comm también han tenido un impacto alarmante en muchos **ciudadanos estadounidenses**. **Datos** recopilados en octubre de 2011, sólo tres años y medio después de la iniciación de S-Comm, encontraron que ICE ya había arrestado a unos 3,600 ciudadanos americanos a través del programa. Más de un tercio de todos los individuos arrestados bajo S-Comm también informaron tener un ciudadano estadounidense como cónyuge o hijo.

Registros de la Ley de Libertad de Información (FOIA) **obtenidos** por el Centro de Derechos Constitucionales (CCR), la Red Nacional de Organización de Jornaleros y la Clínica de Justicia de Inmigración de Cardozo en 2011 resaltan aún más el alcance del abuso posible bajo S-Comm. Estos registros muestran que, mientras ICE estaba usando S-Comm para acelerar la aplicación de la ley de inmigración, el FBI estaba usando el programa como pretexto para desarrollar su iniciativa de Identificación de Próxima Generación (NGI): un sistema de vigilancia que, según la CCR, "busca recopilar y distribuir cantidades masivas de información biométrica sobre ciudadanos y no ciudadanos por igual." Una década después, el FBI **continúa** recolectando una variedad de datos biométricos incluyendo huellas digitales, huellas de palmas, mapas faciales y escaneos de iris a través de esta secreta y **peligrosa** operación. Dada la falta de justificación empírica de S-Comm como instrumento de seguridad pública, no es razonable sobrevivir al programa como un alimentador de las operaciones de vigilancia federal más ampliamente.

Vigilancia Avanzada

Hay muchos **diferentes tipos** de tecnologías de vigilancia, todas las cuales requieren una aplicación cuidadosa para evitar violaciones de los derechos constitucionales de los estadounidenses. Si bien las operaciones de vigilancia siguen siendo relativamente oscuras, lo que sabemos sobre su uso en la aplicación de la ley de inmigración en Mississippi y en todo el país deja en claro que se necesita una mayor supervisión y regulación.

Corredores Privados

A nivel federal, ICE rara vez recopila o mantiene bases de datos por sí mismo, confiando en empresas intermediarias para hacerlo. Sin embargo, muchos de estos corredores privados tienen un historial documentado de violaciones de los derechos humanos y civiles. Por ejemplo, el contrato entre ICE y Clearview AI—una empresa de reconocimiento facial que una vez lanzó su software a un político **supremacista blanco** como una herramienta para la "investigación de la oposición extrema"—está actualmente bajo **escrutinio** público y se enfrenta un **litigio** tras la noticia de que raspó **billones** de imágenes de las redes sociales y otros sitios de Internet sin el consentimiento de los usuarios para construir su base de datos de reconocimiento facial.

Otro corredor implicado en la vigilancia del gobierno es Palantir, una empresa de análisis de datos que sirve a **DHS** y cuyo software permite a ICE desarrollar perfiles de individuos privados. Una investigación reciente e **informe** sobre la empresa llevó a Amnistía Internacional a concluir: "Existe un alto riesgo de que Palantir esté contribuyendo a graves violaciones de los derechos humanos de migrantes y solicitantes de asilo." No se puede negar esta afirmación en Mississippi, ya que ICE confio en el software de Palantir para llevar a cabo las redadas de 2019 en las fábricas avicolas que fueron dirigidas contra cientos de miembros de la comunidad indocumentados, incluidos muchos guatemaltecos indígenas que emigraron para escapar del genocidio.

Los lectores automáticos de matrículas (ALPR) de Vigilant Solutions, que merecen un escrutinio particular, también desempeñan un papel cada vez más importante en el intercambio de datos entre agencias locales y federales. A través de un contrato con ICE de dos años y $6.1 millones firmado en 2018, la compañía, que también es un proveedor popular entre las fuerzas del orden local, dio a más de 9,000 oficiales de ICE **acceso** a 500 millones de ubicaciones de matrículas recopiladas por más de 80 agencias policiales locales a través de todo el país, agregando a los 5 billones de registros que la base de datos ya había reunido a través de empresas privadas. Vigilant Solutions e ICE pueden acceder a un promedio de **150 a 200 millones** de escaneos únicos de matrículas al mes al dirigirse activamente a las agencias policiales locales para que se inscriban en este programa. En su sitio web, Vigilant Solutions **afirma** a las agencias locales que unirse a su "red de intercambio" es "tan fácil como agregar un amigo" en las redes sociales. ICE, en el otro extremo del esfuerzo de reclutamiento, ofrece **sesiones de entrenamiento** para agentes federales y una guía paso a paso sobre cómo involucrar a la policía local en estos acuerdos de intercambio de datos.

Lectores Automáticos De Matrículas

Todas las prácticas de vigilancia representan alguna amenaza para las libertades civiles de los estadounidenses, y **los registros** recopilados por la Electronic Frontier Foundation muestran que varias jurisdicciones en Mississippi han utilizado videovigilancia al aire libre, centros de fusión y/o drones de vigilancia a partir de 2017. Pero de las tecnologías de vigilancia avanzadas utilizadas en nuestro estado, los ALPR parecen estar entre las más comunes.

ALPRs son **cámaras de alta velocidad** que registran la matrícula, la ubicación, la hora y la fecha de cada automóvil que pasa. Las placas de matrícula registradas no son únicamente de automóviles detenidos en puntos de control de inmigración o retenes policiales—son plausibles de todos los automóviles en la carretera, independientemente del historial criminal o de inmigración del conductor. Las cámaras ALPR en los coches de policía, las señales de tráfico y los pasos a desnivel de las autopistas hacen posible esta amplia colección de datos personales. La información recopilada se almacena durante años y crea perfiles detallados de la vida privada de los residentes, incluyendo cómo adoran, cuándo van al médico y dónde van a la escuela sus hijos.

La guía de privacidad de ICE técnicamente limita el uso de ALPR en ubicaciones sensibles, pero esa guía es imposible de aplicar cuando los datos se transmiten en masa, y ICE elude regularmente estas y otras reglas de privacidad a través de "centros de fusión" como **el de Mississippi** en el que colaboran varias agencias de aplicación de la ley (por ejemplo, cuando los agentes federales les **piden a los detectives locales** que analicen los números de placa).

Mientras que la **política** de ICE también requiere que todo uso de ALPR sea documentado y justificado, los registros de FOIA recopilados por **La ACLU del Norte de California** muestran que muchos de los intercambios entre las fuerzas de seguridad locales y ICE son informales y sin control. En ausencia de salvaguardias sólidas, la tecnología ALPR es vulnerable al abuso; por ejemplo, un oficial de policía de DC una vez **confesó** haber usado el sistema ALPR de su agencia para buscar las matrículas de los autos estacionados cerca de un bar gay y chantajear a sus dueños.

Las agencias en Mississippi que usan o han usado ALPRs incluyen, pero no se limitan a, los departamentos de policía de Ridgeland, Madison y Hattiesburg; las oficinas de alguaciles del **condado de Lamar** y Jones; la Oficina de Seguridad Nacional del Departamento de Seguridad Pública de Mississippi; y Patrulla de Carreteras

de Mississippi. En respuesta a una solicitud de registros de MuckRock, La Oficina del Sheriff del condado de Lamar informó en 2018 que estaban compartiendo datos de ALPR con más de 500 agencias locales, federales y privadas a través de todo el país. Con una población poco **más de 60,000**, el intercambio de datos personales del condado de Lamar a esta escala no tiene sentido.

Los acuerdos de vigilancia a menudo operan en secreto y la información disponible sobre su papel en Mississippi está últimamente limitada. El condado de Rankin, por ejemplo, ha ignorado **48 solicitudes de registros** de MuckRock a partir de febrero de 2021 sobre información relacionada con su contrato de **2017** con Vigilant Solutions. Otras agencias de Mississippi que han compartido datos con ICE a través de Vigilant Solutions **incluyen** la Oficina del Sheriff del Condado de Jasper y el Departamento de Policía de Oxford; sin embargo, los detalles de estos acuerdos, incluyendo si todavía están en vigor o no, siguen sin estar claros. Entre diciembre de 2020 y enero de 2021, DHS, ICE, Aduanas y Protección Fronteriza (CBP) y los Servicios de Ciudadanía e Inmigración de los Estados Unidos (USCIS) se han visto afectados por demandas, una por **Center for Democracy and Technology** y otro de **ACLU**, por no responder a las solicitudes de FOIA sobre sus prácticas de recolección de datos.

La Seguridad y Protección Pública

Las agencias que utilizan tecnologías de vigilancia han argumentado que compartir datos personales les permite mejorar la seguridad pública. Por ejemplo, el intercambio de datos biométricos podría ayudar a los agentes a identificar a delincuentes recurrentes y hacer arrestos de los delincuentes violentos conocidos antes de que puedan reincidir. Otros afirman que estas prácticas son necesarias para proteger la seguridad nacional, y los pedidos para más de estas prácticas han **aumentado** desde la insurrección del 6 de enero. Sin embargo, en la práctica, la vigilancia por parte de las fuerzas del orden ofrece pocos beneficios comprobados para el público estadounidense, al mismo tiempo que inflige amplias subversiones de la privacidad y seguridad personal de las personas.

Los que más sufren de estas violaciones son invariablemente miembros de grupos marginados. El representante Bennie Thompson y Kathleen Rice se encuentran entre los muchos legisladores que han **criticado** el uso de los recursos de los contribuyentes por parte de los agentes de inmigración para vigilar a los estadounidenses, incluyendo los ciudadanos estadounidenses y especialmente aquellos que abogan por los inmigrantes, mientras ejercen su derecho a la reunión pacífica bajo la Primera Enmienda. Esta estrategia de aplicación de la ley sigue una tradición de vigilancia gubernamental control los líderes de derechos civiles, incluyendo el ahora célebre ministro y activista **Dr. Martin Luther King Jr.**

El Departamento de Justicia (DOJ) ofrece **orientación** a los agentes federales encargados de hacer cumplir la ley a fin de protegerse contra la conducta discriminatoria, pero esta guía incluye excepciones para cuando existe una sospecha de "una amenaza a la seguridad nacional o de la patria" o "una violación de ley federal de inmigración," lo que ha creado espacio para el perfil continuo de inmigrantes. Por ejemplo, el DOJ establece que los agentes del FBI pueden perseguir razonablemente a individuos de un grupo étnico en particular si hay una pandilla conocida cuyos miembros pertenecen a ese grupo. Esta laguna alguna vez justificó la vigilancia de una amplia franja de la población latinoamericana, que incluía, por ejemplo, a los mexicanos—que representan más de un tercio de la **población inmigrante** de Mississippi—debido a las amenazas planteadas por **una pandilla** que fue fundada por inmigrantes salvadoreños.

Conclusión

En todo el país, hay más de una docena de **diferentes tipos** de tecnología de vigilancia usada contra residentes de los EE. UU., a menudo de forma indiscriminada, en secreto y con poca supervisión o rendición de cuentas. En un **caso de 2017** sobre el intercambio de datos interjurisdiccionales, un juez

del Noveno Circuito advirtió que la ausencia de medidas fiables de rendición de cuentas "permite que inmigración y otras agencias de aplicación de la ley se aprovechen de las comunidades inmigrantes y de clase trabajadora." Sin estos mecanismos, escribe, "los agentes del orden pueden arrestar inconstitucionalmente a personas con apariencia de migrantes, obtener sus nombres y luego buscar en las bases de datos del gobierno para descubrir información incriminatoria." Cuatro años después de esta sentencia, y todavía envuelto en secreto, el intercambio de datos y la vigilancia por parte de las fuerzas del orden locales, estatales y federales plantean serios motivos de preocupación.

Recomendaciones

Para organismos estatales y locales

- Poner fin a los contratos de intercambio de datos
  - que permiten tecnologías de intercambio de información sin restricciones y la recopilación biométrica hacia y desde ICE, y
  - con intermediarios de datos privados que trabajan con ICE.
- Implementar regulaciones sobre la compra y uso de tecnología de vigilancia, tales como:
  - Políticas **Control Comunitario sobre Vigilancia Policial** (CCOPS) y/u ordenanzas que involucran a los miembros de la comunidad en los procesos de toma de decisiones sobre si y cómo se recopilan y usan sus datos personales;
  - Prohibiciones específicas sobre tecnologías de vigilancia específicas, como la prohibición del reconocimiento facial en **Jackson, Mississippi** y otros 13 **gobiernos municipales** a partir de enero de 2021; y/o
  - Regulaciones generales sobre la adquisición y uso de nueva tecnología por parte de la policía local.

Para la administración de Biden y las agencias federales

- Poner fin a los acuerdos obligatorios de intercambio de datos entre agencias federales, estatales y locales.
  - Ordenar a DHS que ponga fin a S-Comm y desmantele todo el intercambio de información electrónica que redirige las presentaciones de huellas digitales de la policía local a DHS para el propósito de hacer cumplir la ley de inmigración civil.
  - Poner fin a cualquier arreglo o contrato que le proporcione a ICE acceso a bases de datos estatales y/o locales con el propósito de hacer cumplir la ley de inmigración civil.
- Dar prioridad a la seguridad y protección pública.
  - Revisar las directrices de seguridad existentes para incluir evaluaciones objetivas de la medida en que una persona representa un riesgo de fuga significativo de un peligro genuino para la comunidad y dirigir los recursos respectivamente
  - Aprobar legislación como la **Ley Nacional de Privacidad Biométrica** para extender explícitamente los derechos de privacidad para incluir datos biométricos.

Para agencias locales, estatales y federales

- Mejorar la transparencia y la rendición de cuentas.
  - Llevar a cabo una investigación sobre el uso de perfiles raciales por parte de la policía, prohibir el uso de perfiles basados en prejuicios, implementar salvaguardias y garantizar la rendición de cuentas por el abuso.
  - Mejorar la transparencia de los programas de intercambio de datos a través de informes públicos regulares.
  - Crear pautas claras sobre cuándo es apropiado que los empleados de las agencias gubernamentales divulguen información personal confidencial de las personas.