**Electronic Privacy Information Center**

# *Privacy and Human Rights 2005*

# *Privacidad y Derechos Humanos 2005*

## An International Survey of Privacy Laws & Developments

Marc Rotenberg and Cédric Laurant
Ula Galster and Katitza Rodríguez Pereda

# Executive Summary

# Resumen Ejecutivo

(Translation into Spanish: David Casacuberta)

Este informe anual del Centro de Privacidad (Electronic Privacy Information Center) y Privacidad Internacional (Privacy International) revisa la situación de la privacidad en la sociedad de la información en más de 70 países del mundo. Como cada año, presentamos el conjunto de medidas legales existentes para proteger la privacidad y un resumen de los temas más importantes tanto en el área de privacidad como en el de la vigilancia. Cada uno de los capítulos se concentra en un país concreto, incluyendo sus regulaciones nacionales en el campo de la protección de la privacidad y la monitorización legal de las comunicaciones por las fuerzas del orden público. Múltiples juicios relevantes, trabajo de sensibilización de organizaciones no gubernamentales y grupos de derechos humanos y otros casos relacionados también forman de este trabajo.

Muchas de la actividades relacionadas con la privacidad y la vigilancia son el resultado de la necesidad de los gobiernos por incrementar la seguridad después de los eventos de carácter terrorista acaecidos en los últimos años en Asia, Europa, Estados Unidos y Oriente Medio. Muchos países del mundo han perseguido cambios reguladores y legislativos para dotar a sus gobiernos con la capacidad de incrementar la vigilancia sobre los ciudadanos. Algunas de estas medidas incluyen la incorporación de nuevos sistemas de identificación y la vigilancia de las comunicaciones. Al mismo tiempo que se potencian estos sistemas técnicos, diferentes agentes trabajan sin descanso para debilitar las políticas de protección de datos. A esta intensificación en la recogida de

información tanto de fuentes privadas como públicas se une la mayor dispersión de dicha información en un conjunto más amplio de agencias del orden público.

*1. Medidas gubernamentales contra el terrorismo*

De manera global, la mayoría de los gobiernos ha seguido trabajando en políticas que legitiman el uso de la vigilancia masiva para combatir el terrorismo. Una de las mayores tendencias ha sido la puesta en funcionamiento de medidas que garantizan la identificación de individuos en tránsito entre países. Muchos países han seguido la pauta marcada por Estados Unidos incorporando información biométrica en diferentes distintos documentos oficiales y empleando sistemas más avanzados para estudiar los perfiles de los viajantes. Como resultado, nuevas tecnologías como el escáner de iris, el reconocimiento facial, las etiquetas de radiofrecuencia o el reconocimiento digital de huellas dactilares están (o están en vía de ser) implementados. Estos sistemas, que inicialmente estaban diseñados para mantener la información de los extranjeros viviendo en un país, han sido progresivamente extendidos para controlar y vigilar a otros grupos sociales.

Este año, nuevas políticas que intentan combatir el terrorismo han sido aprobadas. Algunas de ellas son resultado de propósitos legítimos, pero otras, se han limitado a dotar a las fuerzas del orden público con nuevos poderes no alineados con el propósito inicial y especifico de luchar contra el terrorismo. Estas nuevas leyes dotan no solo de mayor poder de vigilancia pero también con la capacidad de compartir los datos, que anteriormente estaban clasificados como de inteligencia, con otras agencias extranjeras. En algunos casos, las nuevas medidas legislativas han dado lugar a la creación de agencias dedicadas exclusivamente a la lucha contra el terrorismo. Sin embargo, mucha de la legislación no contempla mecanismos eficaces para vigilar su correcta y legitima implementación. Una tendencia preocupante es que se permita a entidades privadas la recogida, procesamiento y almacenamiento de información altamente sensible.

*2. Otras medidas gubernamentales*

Los gobiernos no sólo se han limitado a la puesta en marcha de medidas tradicionales de vigilancia para responder directamente contra el terrorismo. A la vigilancia tradicional se han incluido nuevos aliados tecnológicos como el uso de tecnología biométrica, tarjetas inteligentes, y la explotación de los datos de todo tipo de bases de datos, incluidas las de información media. Al amparo de garantizar la seguridad pública, se han financiado sistemas de videovideovigilancia aún más avanzados en lugares públicos, redes de transporte y aduanas.

Es más común que en años anteriores la implementación gubernamental de tarjetas inteligentes o “smart cards” en un amplio abanico de aplicaciones y documentos oficiales incluyendo: pasaportes, carnets de conducir o la identificación electrónica en

sistemas de régimen fiscal, bancario o de salud. Muchos de estos nuevos documentos contienen información de carácter biométrico que permiten su uso con nuevos servicios gubernamentales en la red. Es importante mencionar que en la mayoría de los casos estos sistemas se han implementado inicialmente en grupos reducidos de población, como refugiados o inmigrantes ilegales, pero existen planes para su puesta en marcha con toda la ciudadanía. Muchas de las críticas a estos sistemas es la falta de protecciones legislativas en muchos países y los riegos potenciales a nuevos tipos de robo de identidad.

Es notable el crecimiento en el uso de ADN y las bases de datos con información médica. No solo ha crecido su uso sino también su finalidad: se tratan más tipos de delitos con un grupo más amplio de individuos y con al ampliación de la retención de dichos datos. Las bases de datos también se han empleado con una finalidad diferente a su diseño inicial. Su propósito inicial se ha extendido a su uso para seguridad nacional, investigación medica o el seguimiento de gastos en el área de la salud. Es preocupante la falta de simples mecanismos para controlar como son realizados los test genéticos y como se emplean después los resultados. Son comunes las críticas que cuestionan su legalidad y constitucionalidad y la poca o ninguna información pública al respecto.

Algunos de los países estudiados han implementado medidas drásticas de censura como mecanismo de control de la población, desde la intercepción del correo electrónico o las búsquedas de los usuarios en Internet hasta los SMSs, el teléfono o el fax. Estas medidas se han implementado no solo ha nivel individual y privado pero también en accesos públicos como cybercafés.

### *3. Vigilancia en el sector privado*

Estas amenazas no solo están presentes en el sector público, compañías privadas practican la vigilancia incorporando tecnologías como cámaras de vigilancia y las etiquetas de radio frecuencia o RFIDs. Las RFID que inicialmente se usaban en el seguimiento de productos y en el control almacenes ahora se usan en servicios públicos como librerías o incorporadas a nuevos sistema de pago. Es común encontrar empresas promoviendo esta tecnología y su capacidad de seguir a las personas, como prisioneros o otros grupos minoritarios e incluso como mecanismo de seguimiento del personal en las empresas y en zonas de alta seguridad.

Aunque las etiquetas de radiofrecuencia pueden dar lugar a grandes avances en ciertos campos de aplicación, los riesgos son mucho mayores cuando la tecnología se introduce para controlar a los consumidores, y a las organizaciones civiles y políticas. Conscientes de su peligro, legisladores y agencias de protección de datos están abordando sus implicaciones en la privacidad. En este campo destacan las numerosas campañas de sensibilización promovidas por organizaciones defensoras de la privacidad.

Aunque el crecimiento de videovigilancia es constante en los últimos 12 meses, muy pocos países han reaccionado adecuadamente, los medidas para evitar sus abusos son mayoritariamente insuficientes.

La lucha contra el correo basura o no deseado (spam) ha dado lugar a la propuesta y/o aceptación de nueva legislaciones. Muchos de los países de la Comunidad Europea han transpuesto la *Directiva de protección de datos en las comunicaciones electrónicas*; hasta la fecha este esfuerzo legislativo es la mayor iniciativa para armonizar legalmente la lucha contra el spam en distintas jurisdicciones. Ésta no es la única iniciativa a nivel internacional, esfuerzos se han intensificado para encontrar otras soluciones basadas en incrementar la colaboración legal entre países y el desarrollo de nuevas medidas de carácter puramente técnico. Al mismo tiempo que han aparecido numerosas organizaciones de lucha contra el spam (anti-spam), los tribunales están condenando dichas intrusiones. Este tipo de protestas son aún más comunes en las agencias de protección de datos.

Muchas compañías de EEUU orientadas a la recogida de datos de consumidores y usuarios en Internet han sufrido intrusiones "indeseadas" en su seguridad, poniendo en peligro la confidencialidad de todos sus datos. Las empresas, cuyo modelo de negocio es vender estudios basados en esa información a terceros, han hecho público (bajo la presión legal) la fuga de datos de sus sistemas. Estos casos ponen de manifiesto el alto riesgo que implica el procesamiento de datos de carácter personal, sino existen marcos legales adecuados, que impongan medidas técnicas y humanas para la protección de la información. Como consecuencia, existe un aumento en el riesgo de robo de identidad y la perdida de confianza de los usuarios en Internet. Aunque la mayoría de los casos conocidos de mala gestión de los datos de carácter personal tiene lugar en EEUU, su impacto se ha hecho notar a nivel global. Los legisladores insisten en la creación de normativas que refuercen la seguridad y protección de datos recogidos por organizaciones tanto públicas como privadas. Casos de robo de identidad y fraude han empezado también a aparecer en países en vías de desarrollo.

*4. Nuevas leyes de protección de datos*

En este periodo nuevas leyes de protección de datos se han decretado y otras están en vías de aprobación. Mientras los 25 países de la Comunidad Europea han armonizado su marco legal, otros países activos en Asia o Europa están siguiendo los pasos de Europa. El año pasado ha sido clave para las nueva *Directiva* europea, al ser en este último periodo en el que más países la han implementado.

*5. Organizaciones civiles y ONGS contra la intrusión en la privacidad.*

En varios países, las invasiones de la privacidad han encontrado fuerte oposición en grupos de derechos humanos. En Australia, organizaciones de derechos civiles fueron capaces de parar una propuesta del gobierno que hacia un uso extensivo de las base

de datos del censo. En Malasia, el caucus de derechos humanos del Parlamento y un grupo de ciudadanos expresaron su oposición a que agentes del gobierno pusieran controles y vigilancia a las prácticas religiosas de los ciudadanos. Es común que departamentos islámicos de Malasia realicen "incursiones" contra musulmanes acusados de cometer actos inmorales. Como respuesta a esta vulneración de la privacidad y bajo las presiones de los grupos de derechos humanos, el gobierno insistió en la necesidad de que este tipo de acciones deben tener permiso oficial policial. En Tailandia, la policía ha pedido al gobierno la redacción de una ley que les permita, sin autorización legal, interceptar las comunicaciones electrónicas y las búsquedas en viviendas privadas. La idea no fructiferó como resultado de la oposición que calificó el intento como un atentado contra los derechos humanos y las libertades civiles. Fruto del trabajo del los últimos años de las organizaciones civiles en Estados Unidos, la iniciativa CAPPS 2, un sistema de perfilado de pasajeros en el transporte aéreo, fue paralizada.

*6. Desarrollo en el área Transparencia Gubernamental*

En este área destaca la creación de nuevas leyes y regulaciones (Ecuador, Macedonia, Uganda) y numerosas propuestas a la espera de aprobación (Alemania, Guatemala, Mongolia, Nigeria, Sri Lanka). En Costa Rica, es notorio un caso que garantiza el derecho público de acceso a información gubernamental y en el Reino Unido la implementación completa de la ley de libertad de expresión.

*7. Acciones de Organizaciones Gubernamentales Internacionales*

Las acciones de las organizaciones gubernamentales internacionales como el Consejo de Europa han tenido una influencia en las políticas de lucha contra el terrorismo. Su influencia no es siempre conocida a nivel público y aunque estas organizaciones han sido muy activas a nivel global no existen buenos mecanismos democráticos para regular su control. Este es el Caso del Consejo de la Unión Europea que han trabajado por armonizar las políticas europeas en la lucha contra el terrorismo descuidando el equilibrio con las medidas que deben proteger la privacidad.