

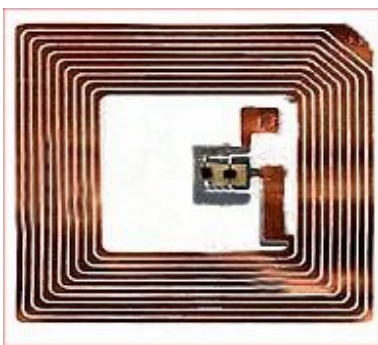
<https://info.nodo50.org/Pasaportes-biometricos-un-estado.html>



[video]clonados los datos de identidad personal de
pasaportes electrónicos norteamericanos

Pasaportes biométricos, ¿un estado de vigilancia permanente?

- Noticias - Noticias Destacadas -



Fecha de publicación en línea: Viernes 4 de septiembre de
2009

Copyright © Nodo50 - Todos derechos reservados

El pasaporte biométrico – que incorpora un chip electrónico con datos personales, imágenes faciales y huellas digitales – está en camino de convertirse en un requisito previo global para viajes. Hasta entonces los actuales pasaportes seguirán siendo válidos para viajes a la mayoría de los países. Alemania, Francia y Holanda ya han comenzado a emitir los nuevos documentos. Los parlamentarios de la UE accedieron a la demanda de EE.UU. y aprobaron una decisión a fines de 2005 que dice que su objetivo es combatir la inmigración ilegal, el terrorismo y el crimen organizado.

https://info.nodo50.org/local/cache-vignettes/L95xH48/EPassport_logo-0d1a3-eb6f8.png **Identificador de pasaporte biométrico**

Uno de los dulces placeres de la vida es viajar. Gracias a la creciente cantidad de vuelos a bajo coste, los viajes al extranjero ya no son un lujo reservado para los pocos privilegiados. Al mismo tiempo, sin embargo, hay un alarmante aumento en la demanda de datos personales de los turistas y no existe un marco legal transatlántico sobre el intercambio de datos personales. Aunque terceras partes como aerolíneas y operadores de aeropuertos tienen derecho a leer esos datos, no sabemos lo que pasa con ellos posteriormente.

Bajo legislación introducida después de los ataques del 11 de septiembre, EE.UU. ha reforzado las medidas de seguridad para turistas extranjeros que entran a su país. La última medida requiere que hasta 2012, cada viajante que entre a EE.UU. como parte de un programa de exención de visa tiene que tener un pasaporte biométrico o se verá forzado a solicitar una visa.

El pasaporte biométrico – que incorpora un chip electrónico con datos personales, imágenes faciales y huellas digitales – está en camino de convertirse en un requisito previo global para viajes. Hasta entonces los actuales pasaportes seguirán siendo válidos para viajes a la mayoría de los países. Alemania, Francia y Holanda ya han comenzado a emitir los nuevos documentos. Los parlamentarios de la UE accedieron a la demanda de EE.UU. y aprobaron una decisión a fines de 2005 que dice que su objetivo es combatir la inmigración ilegal, el terrorismo y el crimen organizado. Pero la excusa de que los nuevos pasaportes ayudarán a impedir el terrorismo internacional es cuestionable ya que ante todo los agentes de seguridad tendrán que saber qué cara o huellas digitales buscan.

Inicialmente, Washington fijó un plazo hasta 2006 para los 27 países en la UE y otros países exentos de visa como Noruega, Islandia y Suiza, pero luego extendió la fecha hasta junio de este año para dar a esos países más tiempo para preparar la tecnología necesaria para emitir los pasaportes biométricos. El Departamento de Estado de EE.UU. comenzó a introducir pasaportes-e en 2006 y se proyecta que todo dueño de un pasaporte en EE.UU. tenga uno hasta 2017.

Mientras tanto, hay poco entusiasmo para estos nuevos requerimientos. Protectores de datos y activistas por los derechos humanos argumentan que esta regulación trata a cualquiera como un criminal en potencia, violando así la protección de los datos personales de los ciudadanos e imponiendo un estado de constante vigilancia.

Peter Hustinx, Supervisor Europeo de Protección de Datos, dijo en una conferencia de prensa sobre la implementación de pasaportes biométricos en 2007 que las medidas de seguridad orientadas a prevenir el terrorismo son aumentadas frecuentemente a costa de la privacidad. Hustinx está a cargo de asesorar a los gobiernos y a los organismos de la UE respecto a estándares de seguridad de datos y actúa independientemente de las instituciones de la UE. Advirtió que la UE se “precipita hacia una nueva era” de uso de identificadores biométricos para controles de seguridad mientras que los estándares para la protección de datos aún no están claros.

“Es muy importante que los datos biométricos sean sólo conservados en el pasaporte y no en bases de datos externas. Hasta ahora no hay regulaciones internacionales que lo garanticen,” dijo Peter Schaar, Comisionado Federal Alemán para Protección de Datos, en una conferencia sobre protección de datos realizada en marzo de este año en Berlín.

En 2005 cuando se publicó esa decisión, no tuvo lugar un intenso debate político en Alemania, pero hubo algunas voces de disenso. El periódico de izquierdas **Die Tageszeitung** publicó un artículo diciendo que desde el 11-S la seguridad interior había ganado más importancia que la protección de los derechos fundamentales del ciudadano. Además, expertos en seguridad han advertido ante el peligro y la facilidad con la que hackers y agencias estatales podrían abusar de los registros de datos y de la información personal delicada que rastrear.

https://info.nodo50.org/local/cache-vignettes/L194xH174/RFID_Chip-7446c-2ed06.jpg **RFID Chip**

En los hechos, el pasaporte-e, que supuestamente debe proteger a los Estados contra ataques terroristas, no es en nada seguro. En 2006 en la conferencia de seguridad **Black Hat** realizada en Las Vegas, *Lukas Grunwald*, consultor en seguridad informática alemán, demostró que los datos en los chips son fáciles de copiar. Demostró que se podría portar un pasaporte con su verdadero nombre y foto impresos en las páginas, pero con un chip con información diferente clonada del pasaporte de algún otro. Sin embargo, esto podría ser fácilmente evitado si el funcionario de seguridad examina el pasaporte para asegurar que el nombre y la foto impresos corresponden a los datos leídos del chip.

Aún más inquietante para los activistas y los protectores de datos, la Unión Europea está a punto de iniciar conversaciones con EE.UU. para darle acceso a los datos bancarios. El plan podría ir más allá de un acuerdo existente con la UE que permite que las líneas aéreas transatlánticas transfieran datos de tarjetas de crédito, direcciones de correo electrónico, pasaportes, itinerarios de viaje y otros pertenecientes a pasajeros europeos a funcionarios de EE.UU. EE.UU. ya ha estado examinando transacciones manejadas por la *Sociedad para las Comunicaciones Financieras Interbancarias Internacionales* (SWIFT) desde el 11-S. SWIFT, que está basada en Bélgica, planea transferir sus servidores y base de datos de EE.UU. a Europa. Ya que las leyes de privacidad de datos son mucho más estrictas en Europa, EE.UU. necesitaría entonces permiso de la UE antes de poder obtener acceso a esa delicada información.

La protección de la privacidad y de los datos personales de un ciudadano es vital para toda sociedad democrática, y debería ser respetada tanto como la libertad de expresión o de movimiento. Algunos funcionarios en EE.UU. y en la UE, harían bien en volver a leer el *Artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea* que dice lo siguiente:

“Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. Estos datos se tratarán de modo leal, para fines determinados y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación. El respeto de estas normas quedará sujeto al control de una autoridad independiente.”

En la busca paranoica de más seguridad, a menudo se sacrifica la libertad y la privacidad. Todos somos vigilados por el “Gran Hermano,” ¿pero quién vigila al “Gran Hermano”?

© 2009 The Women's International Perspective All rights reserved.

Traducido del inglés para Rebelión por Germán Leyens

::Fuente [Rebelión](#)

:: Artículo original: <http://www.alternet.org/story/142239/>

Vera von Kreuzbruck nació en Argentina. Comenzó su carrera en periodismo en el periódico en idioma inglés *Buenos Aires Herald*. Después de una beca en Alemania hace tres años, decidió establecerse en Berlín. Actualmente trabaja como periodista independiente y colabora con medios en Europa y Latinoamérica. Sus artículos se concentran en noticias internacionales y cultura en Alemania y la Unión Europea.

RFID en pasaportes USA es vulnerable: Construyen un dispositivo de 250 \$ para clonar la identidad de pasaportes

Utilizando un sistema con componentes de bajo costo, de tan solo US\$ 250, el experto en seguridad informática **Chris Paget** ha creado una plataforma móvil que puede clonar grandes números de identificadores electrónicos que son usados en los pasaportes de EEUU y que usarán en la próxima generación de licencias de conducir.

El sistema que el investigador Chris Paget ha construido en su tiempo libre puede ser operado desde un vehículo y contiene todo lo necesario para captar y luego clonar tags RFID. Durante una reciente prueba en la que Paget condujo su automóvil por 20 minutos en el centro de San Francisco, pudo copiar con éxito dos tags RFID de dos pasaportes sin el conocimiento de sus propietarios.

El dispositivo construido por Page consiste en un lector de RFID Symbol XR400 manufacturado por Motorola, una antena Motorola AN400 montada tras la puerta derecha de la parte trasera de un Volvo XC90. Un portátil Dell 710m conectado al lector RFID y que corre sobre el sistema operativo Windows. La mayoría de estos elementos fueron comprados a través de eBay.

Las etiquetas RFID a las que se accede con este dispositivo no almacenan información personal, pero sí aportan un identificador personal único que apunta a un registro de datos personales en la base de datos del Departamento de Seguridad de Fronteras. A causa de ello la American Civil Liberties Union y otras organizaciones han puesto el grito en el cielo ante lo que consideran una vulneración del derecho a la privacidad de los datos de carácter personal. Clonar este identificador electrónico único es el primer paso para la creación de pasaportes falsos suplantando identidades reales. Estas tarjetas electrónicas almacenan también diversas licencias que podrían ser utilizadas por terceras personas para la vida en clandestinidad con una identidad falsa.

Se puede ver en este video:

::Fuente [1](#) y [2](#)

:: Noticias originales en inglés:[1](#) y [2](#)

Más información de interés

- [Biometrics Passports](#). Wikipedia
- [Hacker clone e-passports](#). Wired. 2006
- [Nuevo Pasaporte Digital del 2008 hackeado en minutos](#)
- [rfdump.org](#)