Universidad Interamericana de Puerto Rico
Facultad de Derecho

16 de mayo de 2009

El Nuevo Riesgo de Viajar en la Era Tecnológica

Por: Carmen Boyer, Enrique Rodríguez Álamo

Escrito de la clase "Cyber Law"
Professor Frederick Vega

Introducción:

Una nueva política de seguridad nacional (Homeland Security) establece que las laptops y otros dispositivos electrónicos como ipods, teléfonos celulares, ect., podrán ser retenidos por tiempo indeterminado por agentes de seguridad, aun cuando no haya ningún fundamento para sospechar que el portador esta incurriendo en algún delito.[1]

No tan solo examinan la data, sino que también la copian para analizar el contenido de cualquier laptop o equipo electrónico personal que pase por los controles de los aeropuertos o puestos fronterizos.[2]

Los agentes del gobierno no tan solo están autorizados para detectar posibles terroristas y narcotraficantes, sino también a los que infrinjan leyes de "copyright". Esto conlleva la detención de un viajero extranjero o norteamericano si lleva consigo software, mp3, juegos, libros o películas descargadas ilegalmente. [3]

Fotos y videos familiares, cartas personales y documentos confidenciales podrán ser copiados, examinados y distribuidos por funcionarios federales discrecionalmente y sin orden judicial. Es claro que esta nueva política de seguridad es indignante por constituir una invasión a la privacidad de los ciudadanos y a su propiedad privada. Es preocupante la profundización del "estado policial" en los Estados Unidos.[4]

[1] Electronic Frontier Foundation, Travel Screening, http://www.eff.org/issues/travel-screening (August 8, 2008).
[2] Ibid.
[3] Ibid.
[4] Ibid.

Quien viaje desde y hacia los Estados Unidos con equipo electrónico debe asumir el riesgo de que sea decomisado, si el viajero tiene aspecto o nacionalidad que no agraden a un agente del Homeland Security. [5]

Aun así la Corte Suprema del noveno distrito de Estados Unidos a determinado, que en efecto Aduana y los agentes de los puestos fronterizos pueden hacer registros rutinarios sin orden de registro, ni motivos fundados, ni sospecha alguna, a las laptops, teléfonos celulares y cualquier otro dispositivo electrónico. ¿No es esta medida una práctica clara de invasión inconstitucional a la privacidad de la persona, en total lesión a sus derechos fundamentales, según la cuarta enmienda de la Constitución de los Estados Unidos?[6]

Se conoce que la Constitución de los Estados Unidos, prohíbe los registros irrazonables sin una orden judicial. El Congreso de los Estados Unidos parece obviar este derecho fundamental sobre la protección de la privacidad del ciudadano, en esta nueva era de la informática.[7]

No tan solo el gobierno invade la propiedad privada de las personas, sino que mantendrá dicha información de data digital obtenida por cuarenta (40) años. Estando esta información disponible a las agencias federales, estatales, locales y foráneas. [8]

En abril 21 del 2008 el noveno circuito de de los Estados Unidos, determino en el caso de United States v Arnold, que la 4ta enmienda no requiere que los agentes del gobierno tengan duda razonable para registrar las laptops y otros dispositivos electrónicos en las aduanas de los

[5] Ibid.
[6] Ibid.
[7] Ibid.
[8] Ibid.

aeropuertos y en los puestos de las fronteras. Dentro del "riesgo" envuelto esta propiedad registrada es constitucionalmente aceptada. [9]

Hay muchas personas disgustadas con esta medida de registrar la propiedad ajena sin orden, ni motivos fundados tan siquiera. Entre los mas indignados están la Asociación de Prensa y sus periodistas, exigen una restricción a estos registros o cateos, de la ATS del 2006 (Automated Targeting System). [10]

La política de las agencias federales de la protección de la frontera

El 16 de julio de 2008, Aduana y Protección de Fronteras de los Estados Unidos de América (conocida por sus siglas en ingles como la "CBP") adopto una nueva política sobre los registros de información electrónica en las fronteras. Esta política sirve de guía a los oficiales del CBP, Patrulla Fronteriza, Fuerzas Navales y Aéreas, Asuntos Internos y cualquier otro oficial autorizado por la CBP para llevar acabo registros fronterizos. Específicamente, esta política sienta las bases legales y procesales, las cuales viene obligado el oficial a cumplirlas cuando se realiza algún tipo de registro o examen de información electrónica. El propósito principal es asegurar que se cumplan con las leyes federales en las fronteras. El oficial está autorizado para examinar documentos, libros, panfletos, computadoras, discos, procesadores u otro almacenador de información digital. El CBP dice que esta práctica es vital para descubrimiento de información sumamente importante (como por ejemplo; detectar información relacionada al terrorismo, narcóticos, derechos de autor y marcas, contrabando de pornografía infantil, entre otros asuntos de seguridad nacional).

Los registros en las fronteras solo lo puede llevar a cabo un oficial autorizado por la CBP. El mismo, puede intervenir con cualquier persona que trate de entrar o salir de la frontera sin ser

[9] Electronics Frontier Foundation , U.S. v. Arnold , http://www.eff.org/cases/us-v-arnold (June 12, 2008).
[10] Ibid

necesario alguna sospecha individualizada. Durante la intervención, el oficial procederá a revisar cualquier información documental o electrónica que el intervenido transporte. También, podrá copiarla y retenerla por un periodo razonable de tiempo. De no encontrarse ningún material que pudiese ser delictivo, la copia de la información electrónica pasaría a destruirse y el original devuelto. Todo este proceso de detención, revisión y retención tiene que ser documentado por el oficial y certificado por su supervisor. Hay situaciones donde el CBP podría solicitar asistencia a otras agencias federales (por ejemplo; en casos de que la información digital este codificada). Tampoco se necesita una sospecha individualizada previa de parte oficial para solicitar la asistencia, pero al hacerlo tiene que estar bien documentada. Este proceso puede tomarse días sin que se llegue a una conclusión final. La política de CBP es que el mismo se complete en un periodo razonable de tiempo.

En caso de encontrar material, que probablemente pudiera constituir una violación de ley, el oficial retendrá en su poder el original y/o la copia de la información digital. El original o la copia de los documentos, dispositivos, procesadores u otro artefacto electrónico retenidos por lo antes mencionado, podrían ser compartidos con otras agencias estatales y federales, solamente lo concerniente a la violación en ley. Concluido el proceso, en la mayor parte de los casos, las agencias las cuales el CBP le solicito asistencia estarían obligadas en eliminar la información suministrada. En ausencia de causa probable, el CBP solo retendrá la información relacionada con asuntos a inmigración. Concluido el proceso de asistencia, la información es enviada devuelta al CBP en la mayor brevedad posible. En adición, la entidad o agencia federal tiene que certificarle al CBP que la copia de la misma fue destruida.[11]

[11] U.S. Customs and Border and Border Protection, Policy Regarding Border Search of Information (July 16, 2008).

La doctrina de registros de fronteras y la Cuarta Enmienda

Según la política reciente de registro o cateo fronterizo del departamento de Homeland Security de Estados Unidos, fechada el 16 de julio y emitida por dos agencias federales; Protección de Fronteras y Aduanas e Inmigración y Aduanas. Dispone que los agentes federales podrán tomar una laptop o cualquier dispositivo electrónico de un viajero y llevarla a un lugar apartado por un periodo indefinido sin sospecha de conducta delictiva alguna. Podrán entonces revisar, analizar, copiar y compartir el contenido de la laptop con otras agencias gubernamentales o entidades privadas y hasta traducir el contenido en otro idioma. [12]

Algunos grupos de defensa de libertades civiles, protección de viajeros de negocios y muchos legisladores de diversos estados han presionado al gobierno para que revele sus procedimientos, esto debido a que muchos viajeros se han quejado sobre estos cateos, en violación a los derechos civiles fundamentales, como el derecho a la libertad y el derecho a la privacidad, estipulados en la Constitución de los Estados Unidos. [13]

Entonces es meritorio preguntarse, ¿Qué impacto tiene esta situación en un proceso penal? Si seguimos la relación probatoria e investigativa del proceso penal, veremos que la evidencia se construye desde la raíz hacia los frutos, según la doctrina del "árbol podrido" de procedimiento procesal penal. O sea que si la raíz esta podrida los frutos del proceso penal lo estarán a la larga. Si aplicamos al inicio o en cualquier etapa procesal pruebas dudosas, ilegales o que afecten garantías constitucionales como la privacidad o que nadie puede ser obligado a

---

[12] Noticias 24, Gobierno de Estados autoriza para "tomar" laptops de viajeros, http://www.noticias24.com/tecnologia/noticia/775/si-viajas-a-eeuu-el-gobierno-puede-tom(Agosto 01, 2008).
[13] Ibid.

declarar en su contra, entre otras, el defecto de las pruebas en su origen serán inadmisibles en un juicio. [14]

Por ende si la obtención de la evidencia digital en un proceso penal no es adecuada al cumplimiento de las garantías, del debido proceso de ley o afectan cualquier otro derecho constitucional jamás deben ser utilizados en un juicio en contra de un sujeto. [15]

La primera garantía que entra en juego en cualquier proceso donde se involucre información contenida en equipos electrónicos es el derecho a la privacidad que según la primera enmienda y la cuarta enmienda de la Constitución de los Estados Unidos, que dispone; "Congress shall make no law respecting an establisment of religión, or prohibiting the free excersise thereof; or abridging the freedom of speech, or the press; or the right of the people peaceably to assemble, and to petition the goverment for a redress of grievances". "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and the particularly describing the place to be searched, and the persons or things to be seized".[16]

Por ende si el viajero titular de la información y en su caso el propietario o poseedor del medio de soporte, coloca la información en un formato tal es para que nadie pueda acceder la misma sin su autorización expresa. Aunque esta garantía es relativa, por que un juez puede ordenar el registro de la propiedad de una persona, siguiendo o respetando los principios que le dan la facultad para emitir la orden de registro o cateo. Por ejemplo para abrir un correo electrónico se debe respetar las garantías que atañen la comunicación postal o para intervención de equipo de "sniffing" se respetan los derechos de terceros involucrados de igual manera que se

[14] Ibid.
[15] Ibid.
[16] U.S. Const. art.VII, amend. I,IV

hace con las intervenciones telefónicas y cualquier otra posible violación al derecho de la privacidad. Todos estos cateos deben realizarse siempre con una orden expresa de un juez. [17]

Esta situación también depende de la propia valoración que pueda darle el juez interviniente a las evidencias digitales, de manera que a mayor información obtenida de los equipos electrónicos que se catean, mayor la relevancia para una sentencia condenatoria o absolutoria. [18]

Otro factor seria la credibilidad que pueda tenerse en la obtención y conservación de los equipos y la evidencia en ellos contenida, como así también la inviolabilidad o no de la adulteración del contexto obtenida de la laptop del viajero. Si la evidencia puede ser manipulada o es obtenida de forma ilegal se corre el riesgo de no ser admisible tal evidencia digital, además que se caigan otras partes importantes del proceso que pudieran resultar beneficiosas o perjudicantes para el sujeto, aunque este claramente sea imputable del delito. [19]

Otro punto que se debería probar es que el dueño de la laptop o dispositivo electrónico fue quien cometió el delito, el hecho no es suficiente para condenar al titular del equipo informático. Se debe ubicar al sujeto activo en tiempo y lugar con el mismo equipo que comete el acto delictivo imputado. Por ejemplo “blogs” de inicio de sesión o las contraseñas o cualquier otra marca digital de quien era el supuesto operador del equipo, ya que esta persona puede compartir sus claves con otras personas o alguien tuvo acceso a tal equipo electrónico. Aquí se estaría presentando una evidencia circunstancial, simplemente. [20]

En el caso de United States v. Arnold 523 F.3d 041 (9th Cir. 2008) la corte de apelaciones parece haber obviado estas garantías o derechos constitucionales adquiridos, siendo

[17] Ibid.
[18] Ibid.
[19] Ibid.
[20] Ibid.

la Constitución la ley suprema, ante cualquier doctrina de frontera y su cuarta enmienda de tal Constitución y las reglas de procedimiento penal, sobre el debido proceso de ley. Esta corte determino que la cuarta enmienda de la Constitución no requiere que los agentes fedérales del gobierno tengan sospechas razonables para el registro de las laptops o otros dispositivos electrónicos en fronteras o en los aeropuertos, ya que se justifica con la doctrina de fronteras y la soberanía que tiene la nación norteamericana para proteger su territorio y sus personas. [21]

Esta decisión a causado preocupaciones y controversias sobre la interpretación de la corte de apelaciones sobre la cuarta enmienda y la protección de la privacidad a las personas, mas aun en la revisión de tal decisión fue confirmada por la Corte Suprema de los Estados Unidos.[22]

Hay compañías que tienen información sensitiva de negocios, legales, información de clientes, productos nuevos entre otras data digital que temen que los agentes federales puedan divulgar.[23]

Hay muchos legisladores intentando crear nuevas leyes, pero no se ha podido hacer nada, ya que el gobierno se escuda detrás de la seguridad nacional para hacer esta intromisión o invasión a la privacidad, es alarmante. [24]

Es cuestionable, si el gobierno de Estados Unidos lo que busca con estos registros o cateos es dar con organizaciones de terrorismo o organizaciones de narcotraficantes, como es posible entonces que arrestaran a Arnold, cuando lo que encuentran son dos fotos de mujeres desnudas. Aunque

[21] U.S. v. Arnold 523 F.3d 041 (9th Cir. 2008).
[22] Bahía Pirata IX, Agentes de EE.UU. autorizados para "tomar" Laptops de viajeros, http://www.bahiapirata.org/2008/08/04/agentes-de eeuu-autorizados-para-tomar-laptops-d... (Agosto 04, 2008).
[23] Gabriel Andrés Campoli, @ alfa-redi, Manual Básico de Cateo y Aseguramiento Evidencia Digital: Revista de Derecho Informático (2006), http://www.alfa-redi.org/rdi-articulo.shtml?x=7693.
[24] Ibid.

luego lo acusan por pornografía infantil, el propósito del cateo no era encontrar este material aunque delictivo, este registro era irrazonable por ende no debería ser admisible en una corte, según el debido proceso de ley. [25]

La orden de cateo fue obtenida dos semanas después que Arnold fue dejado en libertad. Arnold solicito la supresión de evidencia y la corte de distrito la concede. Pero el estado apela en una corte de apelaciones, alegando que la doctrina de fronteras tenía precedencia a la cuarta enmienda de la Constitución de los Estados Unidos, con relación a la protección del registro irrazonable, como excepción. [26]

Arnold alego que una laptop es muy similar a la privacidad de la casa o la privacidad de la mente humana, ya que la laptop contiene información tan personal y que la cuarta enmienda lo protegía en lo que respecta a su privacidad, por ende este derecho no debía ser violado. [27]

La fundación de fronteras electrónicas emitió un "amicus brief " apoyando la posición de Arnold. La EFF y la ACTE argumentaron que la posición del gobierno en tales registros era inconstitucional e invasiva a la privacidad del viajero y su equipo electrónico, entre muchas otras alegaciones. (28)[28]

El gobierno argumento que ellos tenían la tarea de asegurarse de la seguridad de los ciudadanos de su territorio y por ende tienen el derecho en esta frontera o punto de registro de verificar a las personas y sus pertenencias. Afirmaron que los registros en las fronteras son razonables

[25] Ibid.
[26] Ibid.
[27] Ibid.
[28] Ibid.

simplemente, por ser el punto de registro de un aeropuerto o una frontera para entrar a los Estados Unidos o salir de este. A virtud de la doctrina de fronteras el registro es permisible y la cuarta enmienda no requiere entonces sospecha razonable.[29]

La cuarta enmienda de la Constitución de los Estados Unidos, carga una excepción sobre la doctrina de las fronteras establecidas en United States v. Ickes, 393 F.3d 501 (4th Cir. 2005).

> 1- protección de comunicación terrorista
>
> 2- creación de un estándar de trabajo, adonde los agentes deciden que material esta cubierto en los registros razonables, de la cuarta enmienda..
>
> 3- contrarrestar el peso de la Corte Suprema y sus precedentes, refutando las acciones del gobierno a un mayor escrutinio, con respeto a la cuarta enmienda, esto cuando se invoque la protección que dispone la cuarta enmienda.[30]

Con estas razones se justifica el interés del gobierno en no aceptar personas indeseables en su territorio. Las contrapartes continúan manteniendo su posición en que una laptop es tan reveladora en cuanto a información personal, que tal invasión requiere que los agentes tengan sospecha razonable para poder justificar su intromisión, según la cuarta enmienda. La Corte Suprema ha dejado la pregunta abierta sobre las circunstancias que hace el registro particularmente ofensivo y por ende irrazonable. [31]

Conclusión:

---

[29] Ibid.
[30] United Status v. Ickes, 393 F.3d 501 (4th Cir. 2005).
[31] Ibid.

La Cuarta Enmienda de la Constitución de Los Estados Unidos protege a sus ciudadanos contra registros y allanamientos irrazonables. Desafortunadamente, como visto en el caso de Arnold, esta garantía no aplica totalmente en las fronteras y puntos de entradas internacionales del País.

Estas medidas han sido implementadas para velar por la seguridad nacional, que siempre ha sido prioridad para el Estado, especialmente posterior a los ataques del 9/11.[32] Esto ha llevado a que las personas tengan mayor tolerancia de los registros a su persona y pertenencias. Pero lo que se debe analizar es, ¿hasta qué punto llega la tolerancia de las personas a permitir estos registros?, ¿las razones para el registro?, ¿qué se debe registrar?, y ¿de qué forma deben ser realizados los registros? En fin, ¿cuán flexible es el límite permisible para que no violente el derecho a la intimidad?

El Tribunal Supremo de los Estados Unidos le ha dado el visto bueno al gobierno para poder hacer registros de especie "rutinarios" sin la necesidad de mera sospecha.[33] Aparentemente el Noveno circuito entiende que examinar detalladamente los documentos y archivos electrónicos, caen bajo este renglón.

Se debe establecer un límite para estos registros, ya que la invasión a la intimidad de las personas es masiva y se pierde en gran medida la privacidad. Se entiende el propósito que persigue el Estado, y además, debe existir un control sobre quien o que entre a la nación, pero hacer registros en archivos y documentos personales sin sospecha alguna, es sumamente irrazonable. El énfasis debe ser dirigido a inspecciones sobre los artículos, incluyendo también los aparatos electrónicos, pero no en cuanto a su contenido da archivos personales. Estos últimos no prueban un peligro eminente suficiente para violarles el derecho a las personas de ser registradas.

---

[32] US Customs and Border Protection, Securing America's Borders at Ports of Entry: Office of Field Operations Strategic Plan FY 2007-2011, .pg. 48. (available at http: vali

[33] U.S. v. Ramsey, 431 U.S. 606 (1977)