Más seguridad, menos libertades

30/10/2001 - Autor: Osvaldo León - Fuente: www.pantalla.galeon.com

No es ninguna novedad que los gobiernos traten de sacar el máximo provecho de una situación de desconcierto, para ganar posiciones que en otras circunstancias provocarían resistencias. Es básicamente lo que la administración del presidente George W. Bush se encuentra empeñada en lograr, en el tiempo más corto posible y en todos los frentes, tras los atentados terroristas contra Estados Unidos del 11 de septiembre, antes de que se enfríen los ánimos de indignación de sus conciudadanos.

Entre las medidas para desencadenar la guerra contra el terrorismo, el presidente Bush incluyó un paquete de disposiciones legales para ampliar la competencia de las autoridades de control, judiciales y ejecutivas, que afectan libertades y derechos civiles consagrados.

Un primer paso en este sentido se dio a tan sólo dos días de los atentados, cuando el Senado norteamericano aprobó la *"Ley de Combate al Terrorismo de 2001"* que, entre otras disposiciones, incrementa las atribuciones de la policía para vigilar las comunicaciones electrónicas.

Esta Ley, que todavía se encuentra en debate en la Cámara de Diputados, permitiría la escucha electrónica de cualquier persona considerada sospechosa por hasta 48 horas, sin orden de un juez, y las nuevas ofensas criminales -terrorismo y hacking- pasarían al rango de los casos por los cuales se puede solicitar a la corte una orden de escucha electrónica. Además, autorizaría nuevas áreas de monitoreo del correo electrónico, sin orden de la corte, que en principio no contempla el contenido de los mensajes sino el "*ruteo*" y " *direccionamiento*", pero estos términos son poco precisos y podrían ser interpretados de manera más amplia.

Desde 1978 existe la Ley de Monitoreo de Inteligencia Extranjera (FISA), que permite a las agencias del gobierno ciertas actividades de monitoreo por períodos de hasta un año, sin pedir autorización a la corte. Pero, normalmente, no puede ser aplicada a los ciudadanos estadounidenses.

De hecho, las presiones para que se incrementen las atribuciones de los cuerpos policiales para intervenir las comunicaciones electrónicas han estado presentes desde hace un buen tiempo, pero no habían logrado prosperar mayormente debido a la oposición de movimientos ciudadanos y defensores de los derechos humanos. Con los acontecimientos del 11 de septiembre, sin embargo, los tiempos se han acelerado y las demandas se han tornado mayores.

El fiscal general, John Ashcroft, por ejemplo, está presionando para que un juez pueda autorizar la escucha electrónica a una persona (que utilice cualquier línea telefónica fija o móvil) y no sólo a una línea telefónica en particular, como es actualmente el caso. En tanto

que el senador republicano Judd Gregg ha levantado de nuevo la propuesta (que hasta ahora no había prosperado en el Congreso) de introducir la obligatoriedad de una *"puerta trasera"* en las tecnologías de encriptación de mensajes, que permitiría a los gobiernos tener acceso a una clave para desencriptar los mensajes, en caso de peligro. No obstante, existe oposición en el propio Congreso a tal medida, por los riesgos que implica no sólo para la privacidad personal sino también para la seguridad de las empresas y del propio gobierno.

En la perspectiva de quienes pugnan por mayores controles, el paso siguiente será lograr que se apliquen a la Internet las leyes de la intervención telefónica y, así, se dé carta blanca a la utilización de Carnivore, un programa de seguimiento de correo electrónico del Departamento de Justicia, y a la red de espionaje internacional Echelon.

El Gran Hermano

Cuando se habla de las implicaciones de las nuevas tecnologías de información y comunicación para la democracia, lo que poco se comenta es que las características propias de éstas también se pueden prestar ventajosamente para fines poco o nada democráticos, como la violación sistemática a la correspondencia privada y el espionaje, en general, o el almacenamiento y venta, sin pedir permiso, de datos personales. Quienes han abordado estos aspectos, lo han hecho evocando la imagen del *Big Brother* (Gran Hermano) de George Orwell, que en los tiempos que corren se presenta bajo la forma de *Echelon*.

Echelon es el nombre de un sofisticado programa de espionaje a las comunicaciones que opera a escala mundial, montado por los países anglosajones (Estados Unidos, Gran Bretaña, Canadá, Nueva Zelanda y Australia), pero bajo el mando y ejecución de la Agencia Nacional de Seguridad (NSA) estadounidense. Su existencia fue ratificada formalmente hace poco tras una investigación del Parlamento Europeo.

En operación por lo menos desde 1988, aunque sus antecedentes remontan al acuerdo suscrito por tales países en 1948, esta red de espionaje se apoya en una poderosa infraestructura que es capaz de interceptar, mediante satélites -se calcula que al menos 120-, flotas de aviones militares, submarinos y otros medios, prácticamente cualquier información transmitida por correo electrónico, fax y teléfono desde cualquier punto del planeta. Potentes computadoras rastrean las comunicaciones en búsqueda de palabras claves, frases, personas y lugares, pero también pueden controlar sistemáticamente las comunicaciones de ciertas fuentes preidentificadas.

Diseñado para recolectar informaciones de inteligencia durante la guerra fría, el informe europeo demuestra que Echelon está siendo utilizado para intervenir comunicaciones personales y comerciales. En el primer caso, hay evidencias de espionaje, entre otros, a organismos de derechos humanos. En cuanto al espionaje comercial, se ha denunciado casos donde empresas norteamericanas han arrebatado grandes contratos a concurrentes europeos, gracias a la obtención de información confidencial, como el caso, en 1998, de la firma estadounidense Raytheon, que obtuvo un contrato que la francesa Thomson lo tenía casi asegurado, para la venta de radares a Brasil para el Sistema de Vigilancia de la Amazonia (SIVAM).

Para no quedarse a la zaga, los países miembros de la Unión Europea han implementado, desde 1995, el programa de espionaje Enfopol, y se aprestan a aprobar un cuerpo regulatorio que, entre otros puntos, dispone que cada llamada telefónica, fija o móvil, cada fax, cada mensaje electrónico, todo contenido de las páginas Web y toda utilización de la red, se produzca donde se produzca y la efectúe quien la efectúe, quedará debidamente registrada, archivada y disponible por espacio de al menos siete años.

En Inglaterra, al amparo de la legislación aprobada en el año 2000 para prevenir el crimen internacional, muchas de esas disposiciones ya se encuentran en vigor, y es así como tras los últimos acontecimientos las autoridades han pedido a las empresas telefónicas y proveedores de servicios Internet que recolecten y graben todas las comunicaciones de sus usuarios.

Todo parece indicar que, ahora, no sólo que se reforzarán todos estos sistemas de espionaje electrónico sino que también se incrementarán las presiones para establecer la censura en Internet. Después de todo, los críticos al libre flujo de información en la red siempre se han escudado en argumentos de seguridad.

En un testimonio ante el Congreso estadodunidense, en septiembre de 2000, James Dempsey, del *Center for Democracy and Technology*, colocaba el debate en estos términos:

"Mientras el Departamento de Justicia frecuentemente subraya cómo las tecnologías digitales plantean nuevos retos para hacer cumplir la ley, es un hecho que, en la balanza, la revolución digital ha resultado de gran ayuda para el monitoreo y recolección de información por parte del gobierno. El FBI estima que en la próxima década, con las mejorías previstas en la colección y análisis de comunicaciones, la cantidad de escuchas electrónicas aumentará el 300%. Los archivos de computadora son una fuente rica de evidencias: en un solo caso, el año pasado el FBI recogió la suficiente evidencia computarizada como para llenar la Biblioteca del Congreso casi dos veces...

El FBI en su solicitud de presupuesto para el año financiero 2001 pide fondos adicionales para minar datos en estas fuentes públicas y privadas de información digital, por su valor para el trabajo de inteligencia. Sin embargo, las leyes de privacidad en la computación y las comunicaciones no han sido actualizadas desde 1986."

Servicio Informativo "Alai-amlatina"
