17-01-2005

# No eres paranoico si de verdad te persiguen

Jorge Cortell
Revista PCI 24

Parafraseando a un amigo, eso es lo que me contesta cada vez que, en mi obsesión por la privacidad, le pregunto si parezco paranoico: "no eres paranoico si de verdad te persiguen".

Desde finales de los años 80, cuando vivía en los EEUU (entreteniéndome con la búsqueda de listados de números de acceso a BBS, passwords por defecto, etc), he intentado mantener mis datos a cubierto. Pero mi verdadera obsesión por la privacidad vino tras un breve período (en 1999) en el que colaboré con varias agencias gubernamentales de la administración Clinton. Allí me revelaron la existencia del sistema ECHELON. Tuve que firmar documentos prohibiéndome la revelación de dicho sistema. Pero era tan grave lo que vi, que no podía dormir por las noches. Por suerte, la Comisión Europea lo llevaba investigando desde 1997, y en 1999 "alguien" les dio los datos que necesitaban para desenmascarar el asunto al completo. En 2001 la Comisión publicó su informe (accesible a través de su web, incluso en castellano) definitivo en el que desenmascaraban todo el sistema.

ECHELON (para los que aun no lo sabéis) es una red internacional de interceptación de señales de telecomunicaciones (principalmente microondas). Así que los que controlan el sistema (EEUU y Gran Bretaña, junto con Canadá, Australia y Nueva Zelanda), interceptan TODAS las telecomunicaciones del planeta. En teoría lo hacen "para defendernos del mal" (primero fue el comunismo, luego el narcotráfico, ahora el terrorismo ...). En teoría también, después de filtrarlos con palabras clave, sólo "graban" los mensajes que contienen determinadas palabras clave (que establecen y analizan las agencia de seguridad nacionales de dichos países, como la National Security Agency de EEUU). Pero en realidad está demostrado que emplean el sistema para otros muchos usos (como el control de la población civil, o espionaje comercial, político, y militar, espiando a todos: adversarios y aliados políticos, aliados y enemigos militares, y socios y competidores comerciales).

Aquí es donde empecé a preocuparme seriamente por la privacidad de mis mensajes. Pero esto fue sólo el inicio de un largo camino de descubrimientos espeluznantes.
Han existido, y hoy en día existen, multitud de programas destinados a recabar información privada de todos los ciudadanos. Los que más conozco son los sistemas de EEUU (aunque en Europa pasa lo mismo, con sistemas como ENFOPOL). Programas como el Carnivore (empleado por el FBI para interceptar correos electrónicos, y que "accidentalmente" destruyó mensajes de ciudadanos inocentes), y propuestas como el Clipper (que pretendía dar la posibilidad al Gobierno de EEUU de acceder a cualquier dispositivo electrónico que emplease encriptación), el Total Information Awareness y Life-Log (que pretendían convertirse en una gigantesca base de datos sobre todos los ciudadanos del país), o el más reciente Proyecto Matrix (se empeñan en ponerles nombres tan ridículos que parecen broma). En este último, por ejemplo, la empresa Seisint, Inc. creó un sistema informático que, recopilando y cruzando ciertos datos de los ciudadanos de EEUU (como origen étnico, religión, dirección, multas de tráfico, etc) genera una escala de "potencial terrorista". Imagínense lo que le pasa a un musulmán de origen Saudí al que le han puesto varias multas: por lo menos van y lo interrogan, y lo más probable es que lo detengan. ¿Exagero? No: más de 120.000 personas en EEUU han sido "marcadas" como potenciales terroristas, y varios han sido ya detenidos si ninguna otra prueba que una serie de datos "sospechosos". A algunas de esas personas ya no se les permite viajar en avión, o pedir un crédito. Todo esto en un país que, aunque se autocalifica de "defensor de la justicia, la igualdad, y la democracia", ha aprobado secretamente una

ley (la Patriot Act II) que permite cosas como que el FBI, la NSA, o la CIA puedan exigir documentos y datos de clientes y usuarios a organismos y empresas como agencias de viajes, hospitales, bancos, empresas de telefonía, webs (como eBay), o bibliotecas, sin necesidad de orden ni supervisión judicial; o donde en el sexto piso del Departamento de Justicia, en Washington D.C. tienen un tribunal secreto (la Foreign Intelligence Surveillance Court, quien actúa sin supervisión pública, ni del Congreso, ni siquiera de los mismos acusados) que aunque se supone que investiga casos de contraespionaje, ha admitido a trámite 12.178 casos y sólo ha denegado 1.

Si a eso añadimos la localización por GPS, la constante vigilancia "a lo Gran Hermano" (como las cámara ubicadas en las vías públicas, de las cuales Londres tiene el record mundial, y que está demostrado que son manipuladas y empleadas para otros usos que no son la seguridad ciudadana), el reconocimiento facial (como el que se emplea en algunas vías públicas de California), o la facilidad con la que cualquiera puede encontrar información personal de una persona en la red (a través de servicios de pago como Intelius o PeopleData, o gratuitos, como Anybirthday, los registros de divorcios, de automóviles, o donaciones políticas), entenderéis porqué es mejor ser un poco paranoico.

Y por si yo no os he asustado bastante, os recomiendo una sesión triple de cine: *Enemigo Público* (para la cual se contó con ayuda de ex-agentes de la NSA, y que por increíble que parezca es bastante realista), *Gattaca* y *1984*. ¿Convencidos de que todos debemos emplear claves, encriptación, navegación anónima, etc?. Por cierto, ya os hablaré de la LOPD (Ley Orgánica de Protección de Datos) en otro artículo.

"Aquellos que están dispuestos a cambiar libertad por seguridad no merecen ni libertad ni seguridad" Benjamin Franklin. Esperemos que la lucha se decante por los derechos civiles y la libertad, y no por el control militar/policial/gubernamental.