# Estado de vigilancia y necesidad de privacidad.

Victor Buen. Director Auditoria TI Andbank.

8 de mayo 2017

Robert Bobo dirigía una multinacional. Tenía más poder que cerebro, un cuerpo atlético pagado a precio de entrenador personal y algunos ajustes estéticos. Le gustaba ser el centro de atención y aprovechar el cambio de temporada para lucir una nueva chica cada vez más joven. De candidatas no le faltaban, pero no tenía bastante con las que de manera voluntaria ya se le acercaban.
Carla Atormentada le había contado a su novio que el director de la compañía la estaba acosando de manera descarada y que ya no podía más. Pau Manetas le había pedido sólo un poco de paciencia para darle un escarmiento. No le costó mucho encontrar un agujero de seguridad en la red de la empresa, secuestró el ordenador de Robert y esperó que el gran director sincronizara los correos y contactos a través de su móvil. Ya tenía el control de sus conversaciones virtuales y, de paso también, de las intimidades de sus perfiles sociales. Pau colocó un programa espía y cada vez que el móvil enviaba su señal a la antena de telefonía más cercana, también lo hacía de su posicionamiento GPS. El chico sabía en todo momento donde estaba el desaliñado del 'jefe' de Carla. Y esperó sólo un poco más a que el móvil se conectara al sistema de manos libres del coche del Robert, para introducir un segundo programa espía con capacidad de tomar el control del sistema informático del automóvil.
Primero Pau jugó con Robert como un gato lo hace con un ratón. Hasta que decidió detener el coche en medio de una carretera muy secundaria y inutilizó el móvil que se negó a funcionar. Aquello sólo fue la pequeña venganza perpetrada con la connivencia de Carla. Se acordaría toda la vida de la caminata que tuvo que hacer.
La gran y definitiva llegó al día siguiente. Robert no se había recuperado de la marcha a pie con miedosa nocturnidad que se vio obligado a hacer, cuando se tuvo que tragar el desayuno con todas sus miserias expuestas y compartidas a medios de información y blogs. Antes de sentarse en la sala de juntas para dar explicaciones, el consejo de administración de la multinacional ya había comenzado el proceso de búsqueda de un sustituto menos imprudente y bobo.

En el relato anterior, Pablo utiliza la tecnología y sus conocimientos para escarmentar al jefe de su novia desde el

anonimato. Y no sólo lo consigue, sino que muchos de nosotros aprobamos sus actos, aunque sea por aquello de la justicia poética. Pau representa a un usuario muy avanzado de la informática, más bien un justiciero que una amenaza. Pero nos hace patente una vez más nuestra vulnerabilidad tecnológica. Una vulnerabilidad que empieza por nuestro smartphone.

Una de las atracciones del último Mobile World Congress en Barcelona fue el restyling del histórico e indestructible Nokia 3310. Es decir un aparato que no permite instalar aplicaciones, aunque sí tiene mensajería de voz y texto, navegación, una cámara muy básica y la posibilidad de escuchar música en MP3.

La cuestión es, ¿por qué alguien querría volver a un móvil desde el que no se puede utilizar el WhatsApp, ni las redes sociales, ni consultar el correo electrónico o la cuenta del banco, ni hacer fotos para subir a Instagram, ni desplazarse utilizando el posicionamiento GPS?

Más allá de la apropiación que enseguida se ha hecho el colectivo 'hipster' de este modelo de móvil, el resto de usuarios se ha podido sentir interesado por motivos como el precio (unos 50 €), la necesidad de aislarse de la pérdida de tiempo que conllevan las redes sociales, por la autonomía de la batería (dura 25 días en reposo) o la falsa sensación de que estaremos menos controlados.

Seguramente si llevas un Nokia 3310 en el bolsillo, el control que pueden hacer sobre ti es menor que un móvil inteligente o smartphone, aunque sea porque al no utilizar aplicaciones no se recogen todo tipo de datos propios o porque sin un GPS no nos puede geo localizar.

Pero es una apreciación errónea. Tu compañía de teléfonos puede determinar tu ubicación física aproximada con la señal que emite tu móvil vía la antena que le está dando servicio. La directiva 2006/24 / CE del Parlamento Europeo y del Consejo de 15 de marzo de 2006 indica que las empresas telefónicas deben conservar los datos de todos sus usuarios por un periodo de tiempo que no sea inferior a seis meses ni superior a dos años a partir de la comunicación. Cualquier conexión a la red, desde tu móvil, tableta u ordenador personal está registrada en las bases de datos de tu compañía.

Tu móvil es una fuente de información inagotable y las compañías telefónicas pueden conocer tus horarios y tus

movimientos: donde vives, trabajas, si vas a un centro deportivo de forma regular, si visitas el médico -y qué médico-, si asistes a servicios religiosos, etc. En definitiva tienen una radiografía de tus costumbres. Y eso crece exponencialmente de acuerdo a la utilización que hagas de redes sociales, programas de mensajería instantánea (como el WhatsApp), la vídeo conferencia con plataformas como Skype, programas para consultar el saldo de la cuenta de tu banco .... Si añadimos a este cóctel de seguimiento personal las tarjetas de crédito y las de fidelidad de supermercados y tiendas, tendremos cedidos a terceros información sobre nuestros hábitos alimenticios, de preferencias en el vestido y nuestro poder adquisitivo.

Los ejemplos anteriores son una pequeña muestra de cómo estamos de vigilados. Pero yo, pobre mortal, tengo que preocuparme de todo este rastro que estoy dejando? Pues depende, si compro regularmente libros por internet, igual ya me está bien que de forma automática me recomienden títulos con mis gustos literarios; pero si esta información la captura un tercero que está haciendo cruzada en contra de mis opiniones que pueden quedar reflejadas por la compra de libros que hago regularmente, podría ser un objetivo de acoso por parte de este individuo (o colectivo) en contra de mi voluntad. Por lo tanto, toda esta información que generamos conforma nuestro perfil y nuestros antecedentes, y nos hace vulnerables ante situaciones que no podemos prever.

Y qué escenario se nos presenta como situaciones imprevistas que nos pueden dar problemas? Al viajar a un país que no admite según qué puntos de vista, al optar a un proceso de selección laboral, al aspirar a un cargo político o de trascendencia pública, ...

La cuestión es si podemos proteger este rastro que estamos dejando a Internet. Y como no se trata de ser apocalípticos, la respuesta es que sí, aunque la lista de prevenciones que debemos tener en cuenta es larga y no fácil de implementar. Pero vale la pena prestar atención y actuar con más prudencia. El nivel de privacidad que quieras adoptar puede ir desde fórmulas más permisivas, con conexiones seguras en la red y navegación en modo privado; a soluciones más restrictivas que van desde renunciar a utilizar redes sociales o Google; a prescindir del móvil y no utilizar tarjetas de pago.

Nunca tendremos la privacidad garantizada al 100%, pero ser conscientes de la situación nos hará sentir menos ingenuos y nada bobos.