Privacidad en la Red

Introducción: el vasto territorio de la privacidad

Alfonso Escolano[1], Isabel Hernando Collazos[2], Stephanie Teufel[3]
[1] Universidad de La Laguna, [2] Universidad del País Vasco, [3] Universidad de Friburgo (Suiza)

<aescolan@ull.es>
<ihernando@legaltek.net>
<stephanie.teufel@unifr.ch>

La sensación que se tiene al utilizar Internet no debe estar muy lejos de la que tuvieron en su momento los primeros colonizadores del Oeste. Aunque no vayamos en caravana, el territorio que se tiene por delante es vasto, inexplorado y lleno de peligros, aunque también es grande la esperanza de llegar a una tierra prometida.

Durante la última década hemos pasado de movernos por un terreno conocido y razonablemente seguro, de tener una privacidad que quedaba garantizada por el uso del correo, o el correo certificado, a entrar en un nuevo territorio inexplorado, donde el uso generalizado de sistemas de comunicación electrónicos va a ser la norma.

En este territorio las actividades de la vida cotidiana se realizarán --se están realizando ya en muchos casos-- de forma virtual. Ya no es imprescindible acudir a Hacienda a presentar nuestra declaración de la renta, o no tenemos que ir al banco para realizar cualquier tipo de transacción bancaria o bien podemos comprar casi cualquier mercancía sin salir de casa. Podemos leer periódicos, escuchar la radio o ver la televisión de cualquier punto del mundo, en nuestra casa y esto disponiendo únicamente de un ordenador y una línea telefónica. Dentro de poco habremos asimilado esta auténtica revolución y todas estas actividades pasarán a formar parte habitual de nuestra vida, de forma que no podremos concebir ésta sin tener a nuestra disposición todas estas y otras facilidades. Llegarán a ser tan familiares como lo son en la actualidad la electricidad o el teléfono.

Pero mientras llegamos a ese territorio, donde muchas de nuestras actividades se realizarán con toda naturalidad en la Red, habremos de atravesar un entorno hostil en el que deberemos ir dotándonos de los mecanismos de defensa que hagan que hagamos estas actividades sintiéndonos seguros.

Actualmente, la mayoría de las actividades diarias se hacen de forma individual y con la intervención de, como máximo, unos pocos actores. Conocemos el entorno que nos rodea y a lo largo de siglos la sociedad ha adquirido pautas de conducta e instaurado mecanismos que permiten defendernos de los ataques a nuestra privacidad. Por ley está establecida la inviolabilidad de nuestro domicilio, nuestra correspondencia no puede ser abierta, se asegura la prohibición de intervenir las telecomunicaciones y, en los países democráticos, está instaurada la libre propagación de ideas. Las restricciones que existen son mínimas.

Internet: un panorama novedoso

El panorama que se nos ofrece en el nuevo territorio, en Internet, es completamente novedoso. La sensación inicial es de euforia ante la perspectiva que se nos presenta. Pero hasta en los paisajes más hermosos existen toda una serie de amenazas ocultas y que pueden ser todavía mas dañinas si nuestra euforia nos hace olvidar tomar las más elementales precauciones.

En este territorio nuestras actividades se realizan utilizando un número de participantes desconocido de antemano y sobre los que, además, no vamos a tener control. También, y de forma general, cada una de las acciones que realicemos pondrá al descubierto aspectos más o menos importantes de nuestra personalidad, agravado por el hecho de que todas estas actividades utilizan en exclusiva medios que son capaces de obtener y grabar de forma automática todas las huellas que vamos dejando. Puede quedar al descubierto la parte más íntima de nuestro pensamiento (correo electrónico), o poner en evidencia nuestra forma de ser (compras en la red, periódicos o televisiones visitados) o incluso dar información de otros aspectos especialmente sensibles, como son nuestros datos económicos y financieros.

El derecho a la intimidad y a la privacidad aparece especialmente atacado cuando se utilizan tecnologías que facilitan el ataque y vulneración de esos derechos. Es preciso proteger la comunicación bien a través de leyes o bien utilizando técnicas que imposibiliten o dificulten estos ataques.

Sin embargo, frente a estas aspiraciones, aparecen enemigos poderosos en forma de intereses comerciales o gubernamentales que pueden dañar de forma irreversible estos derechos. Por un lado el mercado, con su lógica implacable. Por otro lado, la así llamada seguridad nacional, que con la amenaza del terrorismo o el narcotráfico, hace que entren en conflicto los intereses de las personas y del Estado.

Un paradigma de la situación existente es la aplicación en España de la nueva **Ley Orgánica de Protección de Datos** (**LOPD**), que deroga a la **LORTAD**, en lo que se refiere a la puesta en marcha de los mecanismos que permiten a los ciudadanos proteger su derecho a la intimidad. Valga el ejemplo de que está permitido que se les indique a los clientes de una compañía, mediante un envío masivo de correo ordinario, que, salvo negativa expresa, se van a tratar

y vender sus datos personales. El afectado que no quiera entrar en este juego ha de perder su tiempo y enviar una carta indicando su negativa a este tratamiento. Bien, lo hace pero aquí no acaba el problema, porque el destinatario --o sea, la empresa--, no tiene obligación de contestar y así el afectado no sabe si se ha recibido su petición. Si en un caso hipotético la empresa tirase todas las cartas recibidas a la papelera, no pasaría nada, ya que no existe ningún tipo de constancia de su recepción. Esto aparentemente se podría arreglar enviando la carta certificada e incluso con acuse de recibo. Pero la situación sería la misma, ya que lo que se certifica es el envío, pero no el contenido, por lo que el destinatario eventualmente podría aducir que ha recibido un escrito, pero sobre otro tema.

Así pues la solución es ir personalmente a un centro de la compañía y hacer sellar el duplicado del escrito presentado (pero esto muchas veces es imposible, ya que se trata de compañías muy alejadas geográficamente del domicilio del usuario o que tienen una sola sede), o bien enviar un telegrama o un burofax, en el que efectivamente se certifica el contenido, pero a un coste y con una pérdida de tiempo que no son asumibles por la mayoría de los ciudadanos. Como por otro lado la percepción de ataque a la intimidad es ciertamente minoritaria, las pocas personas que quieran ejercer esta opción ven que en la práctica les resulta prácticamente imposible ejercer sus derechos. Todas las ventajas se han puesto del lado del que va a comerciar con los datos y el ciudadano se encuentra en la práctica inerme para ejercer sus derechos.

Los conflictos criptográficos

Como en el ejemplo que poníamos al principio, el de la caravana de colonos que avanza por las llanuras del salvaje Oeste, ésta atraviesa de forma sinuosa y abriendo caminos. Estos caminos que se están abriendo son las leyes que se deben promulgar para hacer este territorio habitable para todos. En este territorio de arenas movedizas aparece el derecho a garantizar la inviolabilidad de la correspondencia. La forma de asegurarlo es mediante la utilización de criptografía. ¿Qué ocurre si la utilizan terroristas u organizaciones criminales para comunicarse? ¿No debería prohibirse o regularse? Aquí todos los gobiernos actúan de la misma manera, intentando tener el absoluto control. Pero a veces los coches son utilizados por bandas de atracadores. O los teléfonos se usan para cometer actividades ilegales. Pero ni se ha prohibido el uso de los coches ni los teléfonos, ni se ha prohibido que las cartas vayan cerradas, ni se controla la correspondencia de forma generalizada para evitar actividades delictivas.

Por ello, el intento de prohibir o controlar la criptografía debe ser evitado a toda costa. No es imaginable que la información de todo tipo que viaja por Internet (declaraciones de la renta, ordenes bancarias, historiales médicos...) no pueda viajar cerrada, esto es, criptografiada.

No se puede regular la criptografía sin causar daños irreversibles. Los ciudadanos normales se verían gravemente afectados en derechos fundamentales (inviolabilidad de la correspondencia), mientras que los delincuentes buscarían caminos alternativos a su alcance.

Por otro lado, el estrepitoso fracaso americano en el intento de prohibir y controlar el uso y exportación de tecnología criptográfica es todo un ejemplo.

Dada la imposibilidad de prohibir o regular esta actividad, se intenta utilizar el «almacenamiento de claves», que consiste en la necesidad de comunicar de forma previa las claves criptográficas utilizadas a un organismo dependiente del gobierno. Así, bajo control judicial y en caso de sospecha fundada de realización de actividades ilegales, la policía podría controlar la información cifrada. Sería el equivalente a las actuales autorizaciones para «pinchar» las llamadas telefónicas.

Esto, que sobre el papel está bien, presenta múltiples inconvenientes. Porque, si alguien quiere cometer una actividad ilegal, seguramente no dará sus claves para que le controlen ¿y que ocurriría si alguien utiliza esta información para espiar las informaciones de los competidores? ¿y si alguien accede a este organismo centralizado y roba la información? Además, el sistema de almacenamiento centralizado de claves rompe una regla fundamental en un sistema criptográfico seguro: la clave depende única y exclusivamente del usuario.

En España, la **Ley General de las Telecomunicaciones** (disponible en *http://www.sgc.mfom.es/legisla/teleco/lgt/indice.htm)* dice, en su TÍTULO III (Obligaciones de servicio público y derechos y obligaciones de carácter público en la prestación de los servicios y en la explotación de las redes de telecomunicaciones), CAPÍTULO III (Secreto de las comunicaciones y protección de los datos personales y derechos y obligaciones de carácter público vinculados con las redes y servicios de telecomunicaciones):

«Artículo 52. Cifrado en las redes y servicios de telecomunicaciones.

1. Cualquier tipo de información que se transmita por redes de telecomunicaciones, podrá ser protegida mediante procedimientos de cifrado. Podrán establecerse condiciones para los procedimientos de cifrado en las normas de desarrollo de esta Ley.

2. El cifrado es un instrumento de seguridad de la información. Entre sus condiciones de uso, cuando se utilice para proteger la confidencialidad de la información, se podrá imponer la obligación de notificar bien a un órgano de la Administración General del Estado o a un organismo público, los algoritmos o cualquier procedimiento de cifrado utilizado, a efectos de su control de acuerdo con la normativa vigente. Esta obligación afectará a los fabricantes que incorporen el cifrado en sus equipos o aparatos, a los operadores que lo incluyan en las redes o dentro de los servicios que ofrezcan y, en su caso, a los usuarios que lo empleen.

3. Los operadores de redes o servicios de telecomunica-

ciones que utilicen cualquier procedimiento de cifrado deberán facilitar a la Administración General del Estado, sin coste alguno para ésta y a efectos de la oportuna inspección, los aparatos descodificadores que empleen, en los términos que se establezcan reglamentariamente».

Como se ve, en el apartado 1 se autoriza el libre uso de la criptografía. Pero en el apartado 2, se dice que: «*...se podrá imponer la obligación de notificar bien a un órgano de la Administración General del Estado o a un organismo público, los algoritmos o cualquier procedimiento de cifrado utilizado, a efectos de su control de acuerdo con la normativa vigente...*».

El que se tenga que notificar el algoritmo de cifrado no representa ningún problema, ya que estos algoritmos deben estar sometidos a escrutinio público. Pero cuando se regula que «*...cualquier procedimiento de cifrado utilizado...*». se da pie a que en el futuro se pueda tener la obligación de entregar las claves utilizadas, con lo que estamos teniendo los inconvenientes que ya hemos descrito al hablar de la técnica de «almacenamiento de claves».

Una conclusión

La conclusión final, en la línea de lo descrito anteriormente y persiguiendo uno de los objetivos de esta monografía, consiste en que es preciso poner sobre aviso a todos aquellos que quieran aventurarse por este territorio sobre la necesidad de dotarse de medios de autodefensa individual y colectiva, de forma que las penalidades que puedan surgir por el camino puedan ser salvadas. De forma que sepamos colonizar de forma ordenada y provechosa este nuevo territorio; de forma que se convierta en un nuevo país en el que todos podamos convivir razonablemente sin tener que estar sujetos a más amenazas virtuales de las que ya tenemos en nuestra vida real.