

ANÁLISIS

La transformación social de las evidencias electrónicas

JOSÉ MARÍA ANGUIANO

El próximo 15 de junio hará un año que pusimos en marcha un apasionante proyecto: "El foro de las evidencias electrónicas". Probablemente muchos se pregunten qué puede haber detrás de una denominación tan poco usual. La respuesta es muy sencilla: hay un grupo de personas, cada vez más, que pensamos que la transformación que la realidad digital está ocasionando en la sociedad es mucho más profunda de lo que se piensa.

Superada la crisis tecnológica, las aguas han vuelto a su cauce y el avance tecnológico en el que estamos inmersos es tan silencioso como inexorable. Este avance supone que nuestros hábitos y formas de operar están cambiando a gran velocidad.

El derecho ha de ser entendido como una herramienta que sirve para generar normas que posibiliten y faciliten las relaciones en sociedad. Por este motivo, las normas han de adecuarse a la realidad social del momento en el que se aplican. Si las normas que establecen las reglas de juego de una sociedad no se adaptan a la realidad de la misma, la consecuencia es evidente.

Por este motivo, un grupo de técnicos y de juristas decidimos que sería interesante compartir conocimientos, experiencias, dudas, miedos, logros... Eso es el "foro de las evidencias electrónicas".

Es posible que a muchos lectores todo esto les suene a algo ajeno, lejano, inócuo. Probablemente quienes así piensan tengan bastante razón, pero también es cierto que las consecuencias del paso de lo tangible a lo intangible están creando situaciones a las que una sociedad

madura no tiene más remedio que reaccionar.

Me refiero a situaciones como el anonimato en el que algunos se amparan para delinquir en la red, a situaciones como la que vive la música y cada vez más expresiones culturales por el único motivo de ser digitalizables o la situación provocada por fenómenos como el *phishing*.

Mediante este método los ciberdelincuentes remiten un correo electrónico a los usuarios de la banca electrónica indicándoles en el mismo que están procediendo a la actualización o mantenimiento de sus bases de datos. El usuario de la entidad, rellena los campos solicitados sin percatarse de que en realidad no está accediendo a la entidad financiera sino a una máscara de la misma, gracias a lo cual los cyberdelincuentes se hacen con los datos para disponer de los fondos de incauto usuario.

A mi juicio, el clima de inseguridad jurídica que se respira en muchas actividades electrónicas debería ser una preocupación general en apoyo de los afectados. Despreocuparse de situaciones tan dramáticas como la que vive buena parte del mundo de la cultura es, en mi opinión, irresponsable.

Pensar, por ejemplo, que un simple avance tecnológico puede privar a alguien del legítimo derecho de ser remunerado por su trabajo o por su riesgo empresarial es simple y sencillamente intolerable. Si aceptamos planteamientos como éste, tenemos que asumir el riesgo de asentar un peligroso precedente que antes o después tendrá importantes consecuencias.

Aceptando como cierto que vivimos en un mundo electrónico que no tiene las

más elementales dosis de seguridad jurídica, conviene plantearse de dónde viene esa inseguridad y qué podemos hacer para solucionarla.

En la actualidad, la mayoría de los problemas de inseguridad jurídica que se plantean en el entorno telemático vienen del anonimato con que se actúa en las redes. Los ciberdelincuentes campan a sus anchas por la red con la seguridad que da saber de la inmensa dificultad que en muchas ocasiones entraña saber quién es la persona que se encuentra sentada en un ordenador. Por lo tanto, a mi

El anonimato y la suplantación de la personalidad son dos de los problemas graves

El clima de inseguridad jurídica que se respira es motivo de preocupación

juicio el reto que tenemos ante nosotros es la identificación. Para lograr ésta hay que adoptar con urgencia algunas medidas:

a) En primer lugar, obligar a los prestadores de servicios de la sociedad de la información a adoptar las medidas de índole técnico que permitan establecer la trazabilidad (posibilidad de seguimiento) de las comunicaciones electrónicas de tal forma que los Cuerpos y Fuerzas de Seguridad del Estado no pierdan el rastro informático de los cyber delincuentes en los servidores de acceso, en los

proxy corporativos o en los cibercafés.

b) Otra medida imprescindible es desplegar a la mayor celeridad posible el Documento Nacional de Identidad electrónico que permita una identificación unívoca de quien actúa en la red cuando sea necesario.

c) Es preciso crear el hábito de uso de la firma electrónica en determinadas transacciones *online* que por la importancia de las mismas o por el contenido económico que estas pudieran tener, resultara aconsejable.

Asimismo, hemos de asumir que ante la nueva realidad tecnológica a la que nos enfrentamos, hemos de generar los mecanismos técnicos necesarios que nos permitan la generación y custodia de la prueba electrónica.

Para ello parece imprescindible la actuación coordinada de técnicos y juristas, así como un apoyo decidido de todos nosotros a los Cuerpos y Fuerzas de Seguridad del Estado y a la Judicatura que facilite la identificación, persecución e incriminación de aquellos que hoy en día viven amparados en la impunidad electrónica.

Si no lo hacemos, la brecha de inseguridad jurídica entre el mundo presencial y el digital crecerá y será inevitable que la lista de afectados por la inseguridad electrónica aumente.

El año pasado era ya preocupante la situación del mundo de la cultura gracias a fenómenos como el P2P. Este año han sonado las alarmas en el mundo financiero con el *phishing*... Podemos reaccionar o esperar sentados a ver como aumenta la lista.

▼ José María Anguiano es socio de Garrigues Abogados y Asesores Tributarios.