CARMEN FERNÁNDEZ
Directora

REFLEXIONES EN EL AVE

Autocontrol contra 'fake' y 'junk news'

Es curioso pero justo en el momento en que las noticias basura (*junk news*) y las noticias falsas (*fake news*), aupadas especialmente por las redes sociales, representan un problema mundial de primera magnitud, la publicidad goza de mayor autocontrol, y por ello de credibilidad, que nunca.

En un seminario sobre publicidad y salud organizado por la Fundación Víctor Grifols y el Centro de Estudios de Ciencia, Comunicación y Sociedad, de la Universidad Pompeu Fabra, Charo Fernando, subdirectora general de Autocontrol, un asociación privada con más de 500 socios directos y 2.000 indirectos que representan el 70 por ciento de la inversión publicitaria en España, destacó el nivel de autoexigencia en la materia y relató toda la actividad de asesoramiento previo y control *a posteriori* para asegurar el cumplimiento de la legislación específica.

Autocontrol, según Fernando, atendió el año pasado 43.536 consultas jurídicas y revisó 31.568 proyectos de campañas publicitarias antes de su difusión (*copy advice,* que puede pedir la empresa anunciante, una agencia de publicidad o de medios o un medio de comunicación), 263 de ellas sobre medicamentos, 150 de productos sanitarios y 134 de centros sanitarios y tratamientos. Esos datos sitúan a España como el segundo país del mundo donde más campañas de publicidad se revisan, después de Gran Bretaña. Además, 217 casos de presunta desviación (de ellos sólo 5 casos sobre medicamentos, tres de centros sanitarios y tratamientos y uno de productos sanitarios) se resolvieron por el jurado de la publicidad, un órgano independiente que analiza denuncias de empresas de la competencia, consumidores o la Administración. Al parecer, apenas llegan casos sobre publicidad a la justicia ordinaria. En paralelo, hay activos en España veinte códigos de conducta sectoriales que van más allá de lo previsto en la legislación; entre ellos los de Farmaindustria, Anefp, Aeseg y Fenin. El sistema, aseguró Fernando, garantiza a los consumidores que la publicidad es leal, honesta y veraz; para las empresas, elevar el estándar de responsabilidad mejora su reputación y credibilidad, y a la Administración le certifica el cumplimiento de las normas vigentes.

La experiencia de Autocontrol en materia de publicidad en España debe ser tenida en cuenta para abordar el problema de la información basura y la falsa.

La experiencia de Autocontrol en publicidad debería ser tenida en cuenta como tercera vía y mejor alternativa -junto con mecanismos para discriminar la información falsa (pone en riesgo desde las democracias liberales hasta la salud pública) de la verdadera- por todos los gobiernos y parlamentos, incluido el de la Unión Europea, que se debaten ahora entre implantar o no controles estrictos.

UNA FRASE CON HISTORIA

"Escucha, serás sabio; el cominezo de la sabiduría es el silencio".

PITÁGORAS,
FILÓSOFO Y MATEMÁTICO GRIEGO (C. 569-475 A. C.)

COLUMNA INVITADA

Ciberamenazas sanitarias, necesaria labor de concienciación

MARÍA TERESA GÓMEZ CONDADO
Directora general de Ametic

La transformación digital en la que se encuentra inmerso el sector salud trae consigo nuevos riesgos, necesidades tecnológicas y de seguridad, que se deben atender de manera inminente por parte de todos los agentes que intervienen en la cadena de valor del sistema sanitario. Las nuevas tecnologías que están cobrando protagonismo (big data, *machine learning* o *blockchain*), junto con nuevos y variados dispositivos tecnológicos (sensores, equipos médicos, *wearables*, etc.) incrementan la complejidad de este escenario y agudizan la necesidad de contar con un sólido posicionamiento en materia de ciberseguridad.

Según el informe "Top 10 Health Technology Hazards for 2018", elaborado por el Instituto ECRI, que presenta las diez principales amenazas tecnológicas en el sector salud a nivel internacional en 2018, la ciberseguridad ocupa el primer lugar en el *ranking*. Además, según el estudio realizado por el Instituto Ponemon en 2016, el 90 por ciento de los establecimientos que prestan servicio de atención clínica ya han experimentado algún tipo de violación de datos en los últimos dos años, y el 70 por ciento de las organizaciones y centros sanitarios creen que son más vulnerables que otras industrias frente a las ciberamenazas.

Los ataques cibernéticos a los que se enfrenta el sector salud son conocidos, al igual que las motivaciones de quienes intentan materializarlas. Desde el *phishing* -basado en intentar obtener datos confidenciales a través de la suplantación de identidad-, pasando por el *ransomware* -que, a través de un virus infeccioso, bloquea el acceso al sistema y pide un rescate a cambio de eliminar esta restricción-, no es necesaria una alta sofisticación para que el ataque afecte de manera grave a los servicios sanitarios y extraiga la información más valiosa: la de los pacientes.

Otro análisis del Instituto Ponemon referente al primer semestre de 2017 indica que, a nivel mundial, el 25 por ciento de las brechas de ciberseguridad afectaron al sector sanitario, con un incremento del 423 por ciento respecto al mismo periodo de 2016. Asimismo, se estima que los datos relacionados con la salud tienen un valor en el mercado negro diez veces mayor que el de las tarjetas de crédito. Por lo tanto, parece razonable incrementar los esfuerzos para minimizar el impacto de estas agresiones en todas y cada una de sus fases.

A esta alarmante situación se une una realidad incontestable: faltan expertos en ciberseguridad a nivel mundial. Esta dificultad para encontrar personal altamente cualificado hace que las organizaciones sean extremadamente exigentes a la hora de contratar un servicio de ciberseguridad.

> "En los primeros 6 meses de 2017, el 25% de las brechas de ciberseguridad afectaron al sector sanitario, un 423% más que en el mismo periodo de 2016"

> "Ningún plan de ciberseguridad será suficientemente robusto si no integra a todos los agentes que intervienen en la cadena de valor del sistema sanitario"

En materia de reglamentación, también es importante abordar esta cuestión. El sector sanitario va a ser objeto de una legislación específica en materia de ciberseguridad para este año. La ya clásica afectación de la Ley Orgánica de Protección de Datos (LOPD) se transformará en la nueva LOPD, basada en el Reglamento General de Protección de Datos europeo, con plena vigencia a partir de mayo de 2018. Asimismo, según la Ley de Protección de Infraestructuras Críticas (Ley PIC 8/2011), el sector salud es un sector crítico y, aunque todavía no se está desarrollando esta ley en el área sanitaria, podría producirse en cualquier momento.

IMPLICACIÓN Y CONCIENCIACIÓN

Todas estas amenazas que actualmente tenemos sobre la mesa requieren de una actitud activa y proactiva.

La administración sanitaria debe ser consciente de este importante reto y, en consecuencia, proponemos la inclusión de la ciberseguridad como una de sus líneas prioritarias de trabajo, planificando un presupuesto e inversiones acordes. Simultáneamente, la industria tiene la obligación de responder ofreciendo soluciones que permitan a los gobiernos central y autonómicos afrontar esos desafíos.

Por último, queremos recalcar que ningún plan en materia de ciberseguridad será lo suficientemente robusto si no integra a todos los agentes que intervienen en la cadena de valor del sistema sanitario.

En este sentido, es necesaria una labor de concienciación dirigida a los profesionales y pacientes sobre su importante contribución a la gestión de riesgos y prevención en materia de ciberseguridad.