Ciberseguridad y la Abogacía

Con el uso de las nuevas tecnologías, la mayoría de la información es intercambiada en entornos digitales; todos los días, despachos de abogados tratan datos de sus clientes en el ejercicio de su profesión, estando sujetos a obligaciones de confidencialidad, privacidad y por supuesto, de seguridad.

Por otro lado, los ciberataques han estado alrededor de nosotros desde hace más de dos décadas. Desde el primer Ransomware “Aids” o “PC Borg” en 1989 hasta “SamSam” en 2018, la sociedad en su conjunto ha sido impactada de alguna forma, sin que ninguna institución pública o privada haya podido quedar exenta de sufrir un ciberataque. Esto tiene su lógica, ya que conforme la tecnología continúa su desarrollo, los ciberataques también lo hacen, siendo cada vez más sofisticados y mejor dirigidos, lo que dificulta su detección y el establecimiento de acciones de respuesta.

Este fenómeno tiene especial relevancia para la **abogacía**. Con motivo del inicio de la aplicación del Reglamento General de Protección de Datos (“RGPD”) el pasado 25 de mayo, la mayoría de las empresas españolas se han puesto manos a la obra adoptando las medidas necesarias para dar cumplimiento a la normativa de protección de datos. Es frecuente escuchar a nuestros colegas de profesión comentar sobre el gran volumen de consultas y actividades que se ha desencadenado desde los momentos previos a su aplicación.

En paralelo, los despachos de abogados han tenido que recorrer su propio camino de adaptación al RGPD y adoptar las medidas que garanticen la seguridad de los datos que les son confiados, por ello, vale la pena detenerse a analizar si las medidas de prevención, detección y defensa frente a ciberataques cumplen con los principios establecidos en el RGPD.

No es trivial este cuestionamiento, no sólo por el monto de las sanciones que pueden derivarse por una falta de adecuación con la normativa, las cuales en sí mismas son incentivo al cumplimiento, sino también por el eventual daño reputacional que pueden sufrir, destruyendo uno de los principales activos de nuestra profesión: la confianza de los clientes.

Antes de la aplicación del RGPD, la cuestión sobre las medidas técnicas y organizativas necesarias para dar cumplimiento a las obligaciones de seguridad estaba relativamente resuelta por la Ley Orgánica 15/1999 y su Reglamento de desarrollo (RD 1720/2007) (RLOPD), en tanto que establecía un catálogo de medidas de seguridad en función del tipo de datos y su tratamiento por parte del responsable.

Una vez iniciada la aplicación del RGPD es necesario valerse de otros criterios. El Reglamento es una normativa dinámica por lo que se refiere al principio de seguridad para el tratamiento de datos personales; así se desprende de sus artículos 5.1 f) y 32 y el considerando 83, que establecen, por un lado, la obligación de tratar los datos de manera que se garantice su seguridad y, por otro, las bases de las medidas técnicas y organizativas apropiadas para lograr un balance entre dicho nivel de seguridad que se corresponda al riesgo que aprecie el impacto en los derechos y libertades de las personas.

El extinto Grupo de Trabajo del artículo 29, ahora denominado Comité Europeo de Protección de Datos (*European Data Protection Board*), emitió el 13 de febrero de 2018 la *Guía de Notificación de Brechas de Datos Personales* el cual señala que uno de los elementos necesarios de cualquier política de seguridad consiste en prevenir la brecha de seguridad (cuando sea posible) y que en caso de que suceda, se reaccione de manera oportuna.

Nuestro referente a nivel nacional proviene de la Agencia Española de Protección de Datos, quien ha publicado por lo menos tres guías relevantes en esta materia. En primer lugar, la *Guía Práctica para las Evaluaciones de Impacto en la Protección de los Datos Sujetas al RGPD*; en segundo la *Guía Práctica de Análisis de Riesgos en los Tratamientos de Datos Personales sujetos al RGPD,* y finalmente la *Guía para la Gestión y Notificación de Brechas de Seguridad*.

Esta última guía nos aporta elementos adicionales sobre las medidas de seguridad recomendables para entornos virtuales, citando al RLOPD, el Esquema Nacional de Seguridad aprobado mediante Real Decreto 3/2010 de 8 de enero (modificado por RD 951/2015 de 23 de octubre) como criterio para definir incidentes o brechas de seguridad, y dirige a las organizaciones al Instituto Nacional de Ciberseguridad para comprobar el grado de preparación frente a ciberataques.

Con mucho criterio, la guía señala que en todas las organizaciones existen brechas de seguridad, lo que distingue a una organización bien preparada frente a otras es precisamente la calidad de los procesos y mecanismos que se tienen para su gestión. Mecanismos que, en mi opinión, se resumen en tres acciones: detección, protección y respuesta.

Como en la mayoría de los casos, la herramienta principal es la formación. En este campo, no solo es nuestro deber familiarizarnos con la regulación aplicable, es necesario igualmente utilizar tecnología fiable que nos permita tratar los datos de nuestros clientes en un entorno seguro, desarrollar buenas prácticas de uso de la tecnología y tener un plan en condiciones de respuesta en caso de incidencias. Pero todo inicia con los datos. Si se desconoce el tipo de datos que se están tratando, difícilmente podrán adoptarse medidas adecuadas de seguridad.

En resumen, los abogados tenemos un papel fundamental para generar entornos seguros en la economía de los datos aplicando los siguientes principios:

- **Formación constante.** Estamos en una era donde es necesario adoptar una actitud de aprendizaje constante, si bien hay principios que permanecen en el tiempo, como lo son la privacidad, la seguridad y la transparencia, lo cierto es que la normativa y la tecnología no dejará de ser dinámica en esta materia.
- **Flexibilidad.** Por supuesto que es necesario con- tar con procesos estructurados que nos permitan prevenir, detectar y responder a incidencias, también es necesario ser flexibles porque los riegos y amenazas son contantes, cambiantes y cada vez más sofisticadas.
- **Finalmente, sentido común.** El usuario tiene igualmente responsabilidad de utilizar herra- mientas informáticas fiables, actualizadas y debidamente licenciadas.