

Usar armas legítimas; por Pedro Martínez, fiscal del Tribunal Superior de Justicia de Madrid

El día 6 de noviembre de 2009 se publicó en el diario El Mundo un artículo de Pedro Martínez en el cual el autor opina sobre el software de interceptación de las comunicaciones electrónicas Sitel.

USAR ARMAS LEGÍTIMAS

La sociedad de la vigilancia ha llegado sin que casi nos hayamos dado cuenta. En parte, resulta esencial para facilitar los servicios que necesitamos. En parte, resulta cuestionable y puede resultar injustificable, intrusiva y opresiva.

En Europa todo comienza con la Resolución sobre Interceptación Legal de las Comunicaciones de 19 de mayo de 1999, que fue la que dio a conocer la palabra Enfopol al mundo, que abre el camino a un sistema de interceptación y vigilancia de las comunicaciones en todo el territorio de la Unión Europea. La extensión de los poderes otorgados a las policías europeas mediante este plan, unido al secretismo que ha rodeado su gestación y desarrollo, lo convierten en una grave amenaza potencial para la intimidad en la Europa del nuevo milenio.

En España, es a partir de los atentados del 11 de septiembre de 2001 cuando el Gobierno (entonces, del PP) se implicó decididamente en este proyecto. Adquirió e implantó el software de interceptación de las comunicaciones electrónicas Sitel (versión española de Enfopol). Tras el 14-M, el PSOE, con todo su discurso sobre el buen gobierno, la ética y la transparencia, generalizó el uso del sistema sin debate alguno y sin control judicial efectivo, escondiéndolo en una disposición de ínfimo rango normativo para ocultar, o al menos disimular, su existencia, para que los medios no hicieran preguntas.

Sitel no reúne los requisitos para ser utilizado en una sociedad democrática:

- 1.º. Los jueces no han recibido información y formación sobre esta tecnología.
- 2.º. Las operadoras de telefonía deben facilitar, sin que lo autorice el juez, datos personales de sus clientes, como su identificación, domicilio, cuenta corriente o su DNI.
- 3.º. Las operadoras de telefonía deben facilitar datos personales de los interlocutores, aunque la orden de interceptación no los incluya expresamente, como la localización de los interlocutores.

4.º. No existe garantía alguna de la autenticidad de la información que se aporta a los juzgados, ya que no existe autoridad certificadora que garantice la autenticidad, y los discos se entregan sin firma electrónica y sin encriptar.

5.º. Toda la información que se intercepta queda almacenada sine die en unos servidores que se encuentran en los llamados Centros de Interceptación de las Comunicaciones, a disposición del Poder Ejecutivo.

Es probable que Sitel haya servido para atrapar a algunos delincuentes, aunque las estadísticas criminales no dejan de crecer. También puede ser que desde el Gobierno se haya usado para dar un zarpazo a sus rivales políticos, lo cual es gravísimo y debe ser investigado, pero tampoco olvidemos que quienes ahora alzan su voz acusadora demandando justicia también son padres de la criatura. Nadie niega que el Estado pueda utilizar la tecnología para la lucha contra la delincuencia. Pero el Estado de Derecho no puede usar armas que no sean legítimas, a menos que la sociedad empiece a perder su alma democrática. Pero si el escándalo actual sirve para instalar controles democráticos y judiciales eficaces, bienvenido sea.