Nuevas polémicas respecto de la protección de los datos personales.

Por Brenda Salas

Recientemente el New York Times publicó en su periódico una polémica existente respecto del programa de vigilancia que ha desplegado la Agencia de Seguridad Nacional de los usuarios de Internet mediante el uso del programa Prism. Redes Sociales como Facebook y empresas de carácter tecnológico como Google, Apple, Microsoft, AOL y Yahoo negaron haber participado en algún tipo de espionaje mediante el uso de éste. No obstante, el presidente Obama y el director Nacional de inteligencia confirmaron la existencia de dicho programa.

Pese a ello, persisten dudas respecto de quién está diciendo la verdad y cuál es el alcance del programa en el sentido de determinar hasta donde Prism puede espiar. La discusión ha ido más allá. En efecto, este tipo de cuestiones genera varias inquietudes, entre ellas la relativa a la potestad de las empresas que tienen acceso a información de sus consumidores de verse involucradas en programas confidenciales de gobierno¹.

Para Thomas Sporkin, antiguo oficial de la S.E.C. y socio de Buckleysandler, este tipo de problemas revela la dificultad en que se encuentran las empresas, esto porque éstas están obligados en favor de sus usuarios a garantizar la confidencialidad y la privacidad de su información. De otro lado, gracias a sus deberes legales éstas se encuentran obligadas a participar de los programas confidenciales gubernamentales.

En los Estados Unidos, éste tipo de situaciones ha sido regulado por la Section 702 of the Foreign Intelligence Surveillance Act, la cual establece que si el Gobierno legítimamente solicita dicha información, las empresas se encuentran obligadas a brindarla. Como consecuencia de ello, redes sociales como Facebook advierte a sus usuarios antes de acceder el servicio, que ellos, es

statements-on-u-s-spying/?hp

-

¹ "But perhaps just as important, the episode also raises questions about how publicly traded companies with hundreds of millions of consumers — companies that are regulated by the Securities and Exchange Commission and the Federal Trade Commission — can, and should, react to news when pressed about involvement in confidential government programs". http://dealbook.nytimes.com/2013/06/10/tech-companies-tread-lightly-in-

decir, Facebok, podrá compartir la información como respuesta a una solicitud legal, por ejemplo, una orden de un juez².

Ahora bien, en Colombia, la protección de los datos personales parte del derecho fundamental al habeas data reconocido en el artículo 15 de la Constitución que establece lo siguiente: **Artículo 15.** "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.

La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley.

Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley".

El legislador desarrolló este derecho al promulgar las leyes estatutarias 1266 de 2008 y 1581 de 2012. Estas leyes tiene por objeto: "desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma". La diferencia de las mismas radica en el ámbito de aplicación, mientras la ley estatutaria 1266 de 2008 regula "el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países"; la ley estatutaria 1581 de 2012 tiene un espectro más amplio y general.

Estas leyes se caracterizan por establecer una serie de definiciones y principios que actúan como criterio orientador para la interpretación de las mismas. Al igual

² "We may access, preserve and share your information in response to a legal request (like a search warrant, court order or subpoena) if we have a good faith belief that the law requires us to do so." http://dealbook.nytimes.com/2013/06/10/tech-companies-tread-lightly-in-statements-on-u-s-spying/?hp

que la legislación norteamericana, nuestro ordenamiento jurídico también establece que los datos personales³ e incluso los datos sensibles⁴ pueden ser objeto de tratamiento cuando medie una orden judicial. Para mayor información http://dealbook.nytimes.com/2013/06/10/tech-companies-tread-lightly-in-statements-on-u-s-spying/?hp

³ "La autorización del Titular no será necesaria cuando se trate de: a) Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial";

⁴ Para los propósitos de la presente ley, se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos