“Data privacy en México”

Mauricio Domingo Donovan,
Director Jurídico de Microsoft (México)

Resumen
No queda la menor duda que es necesario legislar en materia de privacidad. No obstante, la legislación en relación con este tema no es nueva. El derecho a la privacidad de los ciudadanos respecto a los gobiernos ha sido contemplado y legislado desde las primeras Constituciones, como parte fundamental del pacto social en los gobiernos Republicanos y demócratas.
En una relación gobierno – gobernado, el derecho a la privacidad ha sido un derecho *prima face*. Es decir, nadie puede ser molestado en sus bienes, posiciones, papeles, etc, sin que medie una orden judicial por escrito que funde y motive las razones por la cual la autoridad esta facultada para invadir la privacidad u otros derechos de las personas. Esto es en México, una garantía individual y mundialmente un Derecho Fundamental de los ciudadanos. Como podemos observar, esto no es nada nuevo en el marco regulatorio.
En el otro sentido, también es claro que los gobernados tienen derecho a obtener información del gobierno, es decir, lo que ahora conocemos como transparencia. Bajo el contrato social, es también fundamental la premisa que el gobierno trabaja a favor de los gobernados y, más aun, todos los gobernados aportan para el sostenimiento del Estado, como concepto jurídico. Por ende, es un derecho fundamental de los gobernados, saber cómo es que el gobierno trabaja en su beneficio, y conocer cómo está utilizando, precisamente los recursos que aportan. Este concepto, lo podemos ver plasmado en nuestra Carta Magna como Garantía Individual en el Artículo 6º. Constitucional.
Así las cosas, el gobierno no puede invadir nuestra privacidad sin que medien ciertos mecanismos de protección al gobernado, por ejemplo una orden judicial y, por otra parte, el gobernado tiene el derecho de exigirle al gobierno acceso a la información a efecto de verificar que, efectivamente el Estado está trabajando en beneficio del gobernado.
Estas relaciones de supra a subordinación se elevan al carácter de derechos fundamentales. Necesariamente, entonces, son sólo respecto a estas relaciones a lo que se refiere el *habeas data* o cualquier alusión a la privacidad como derecho fundamental.

Ahora bien, el concepto de privacidad *lato sensu*, consiste en cuatro temas fundamentales:

- El primero es el derecho a la privacidad, relacionado con la integridad corporal de las personas. A manera de ejemplificar a qué se refiere este primer concepto, podemos aludir a la no-exigencia por parte de cualquier persona, como patrones o el mismo estado de pruebas de consumo de drogas o condiciones médicas, como por ejemplo embarazo o VIH, o cualquier otra condición.

- El segundo, es el derecho a la intimidad o privacidad en el hogar. Es decir, la protección del hogar y las actividades que uno efectúa en la privacidad de su casa.

- El tercero es la privacidad de las comunicaciones, es decir el derecho de tener comunicaciones privadas por medio de los teléfonos, por Internet o cualquier otro medio.

- El cuarto y ultimo, es la privacidad de la información personal o datos personales. Es decir, qué es lo que se puede recopilar, quién puede exigir información, cómo se puede utilizar, cómo se puede difundir.

Es este cuarto tema, la privacidad de los datos personales a lo que se refiere el presente estudio. Primero hablemos de los datos personales que son retenidos o manejados por las entidades de gobierno. No queda duda que cualquier uso de información en un ámbito de supra a subordinación se eleva a un carácter de derecho fundamental. Es decir, el gobierno no puede utilizar arbitrariamente nuestros datos personales. Imagínense ustedes la responsabilidad que debe tener el SAT, respecto a toda la información que detenta sobre cada uno de nosotros, por lo menos los que sí pagamos impuestos. Especialmente bajo el estado actual, en donde la delincuencia está desatada. Aclaro, tiene la responsabilidad, no estoy haciendo comentario alguno respecto a si cumple o no con dicha responsabilidad. Ejemplos de cómo el estado está obligado a proteger nuestros datos personales podemos pensar en miles. Estos supuestos de manejo de datos personales por parte de entidades de gobierno, los temas de transparencia y acceso a la información pública gubernamental, son los que han ocupado buena parte de la discusión jurídica durante esta administración. Finalmente, son también los que están resueltos –bien o mal, pero finalmente resueltos–, en instrumentos jurídicos tales como las leyes de transparencia.

Pero en esta ocasión quiero enfocarme más a la discusión, más actual, de los datos personales que son retenidos o manejados por entidades privadas, por particulares. Mucho he oído del tema de “habeas data” en este ámbito. Como lo he dejado ver anteriormente, el “habeas data” o la protección de los datos personales como un tema de una garantía individual frente al gobierno, es un concepto que sólo cabe aplicar respecto

de datos personales que retiene o maneja el gobierno. Es decir, en relaciones de supra-subordinación; de gobierno y gobernados.

El problema es cuando queremos incorporar al habeas data las relaciones de coordinación; es decir, entre particulares. En efecto, el uso indebido de datos personales por parte de un particular puede tener consecuencias gravísimas para una persona; desde recibir montones de publicidad no deseada o llamadas publicitando algún producto o servicio en la privacidad de nuestro hogar, o incluso en nuestro celular, hasta el robo de identidad. Ciertamente, por estas razones y muchas otras, es necesario y conveniente legislar en materia de privacidad, específicamente del manejo de datos personales retenidos o manejados por entidades privadas, pero bajo las condiciones que se exponen en el presente análisis.

Los europeos han sido precursores en materia de regulación de datos personales. Han legislado en esta materia desde hace más de 30 años, por medio de directivas, primeramente, que han llevado a la incorporación de dicha regulación en cada una de las legislaciones de los países miembros. En la cumbre de Niza que tuvo lugar el 7 de diciembre del 2000, se efectuó la Proclamación de la Carta de Derechos Fundamentales de la Unión Europea. El articulo 8º. De dicha Proclamación establece bajo un título denominado "Protección de datos de carácter personal" lo siguiente:

"1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.

2. Estos datos se trataran de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la concimen y a su rectificación.

3. El respeto de estas normas quedará sujeto al control de una autoridad independiente."

En efecto, la Directiva y diversas legislaciones Europeas han regulado la protección de los datos personales bajo las siguientes premisas, expuestas de manera muy general:

Objeto de Protección. El uso de dichos datos personales está regulado sin importar quién dispone de ellos. Es decir, el objeto primordial de regulación es la base de datos y el uso de dichas bases de datos por parte de las personas. Además, no hace diferencia alguna entre autoridad y gobernado; no hay diferencia entre las relaciones de supra a subordinación.

- **Consentimiento.** Basa el uso de dicha información en la aceptación expresa de a quien los datos se refiere; "Opt in".

- **Transferencia Internacional de Datos.** Sólo autoriza la transferencia de datos personales a países que tengan un nivel adecuado de protección de la privacidad. El artículo 25 de la Directiva establece como principio general que "los Estados miembros dispondrán que la transferencia a un país tercero de datos personales que sean objeto de tratamiento o destinados a ser objeto de tratamiento con posterioridad a su transferencia, únicamente pueda efectuarse cuando, el país tercero de que se trate garantice un nivel de protección adecuado."

- **Órgano Regulador**. Estable la creación de un órgano regulador, dependencia de gobierno, pero de carácter independiente al mismo, que controle las actividades de procesamiento de datos. En corto, se pretende que este órgano sea el medio de coerción para el cumplimiento de la regulación.

El modelo denominado ya como "modelo de regulación europeo" ha mostrado ser útil en muchos aspectos, pero también ha reflejado un sinnúmero de debilidades. En concreto, no ha podido contrarrestar los grandes problemas derivados del uso indebido de esta información como es el robo de identidad y otros graves problemas.

De manera específica aunque breve, me permito efectuar las siguientes observaciones al multi-citado marco regulatorio:

- **Objeto de Protección.** Como he dicho, sólo se puede considerar *habeas data* o derecho fundamental, los actos de gobierno para con los gobernados. Las relaciones entre particulares son y deben estar regidas, ante todo, por el consentimiento (tácito o expreso) o las condiciones contractuales que existan o pacten entre ellos. No es posible considerar como parte del *habeas data* a las actividades efectuadas entre particulares; es decir, en relaciones de coordinación. Las garantías individuales, en todo marco regulatorio, tienen alguna institución de control a efecto de velar su cumplimiento. En el caso de México, dicho mecanismo de control se denomina Juicio de Amparo. Entonces es aceptable decir que todo derecho fundamental que es violado por una entidad de gobierno, una autoridad, es susceptible de ser hecho valer mediante el juicio de amparo. Por ende, es sólo la autoridad quien puede violar garantías constitucionales en este contexto. Luego entonces, no es posible que actividades entre particulares, o bien, en un plano de coordinación, sean consideradas en ese mismo contexto de garantías constitucionales o derechos fundamentales. Los ciudadanos se amparan respecto de actos de gobierno, de actos de autoridad; no respecto de actos de particulares.

  La legislación europea regula a las bases de datos *per se* y al manejo de las mismas. Falla al no regular el primer paso de esta cadena, que es la obtención de la información y los fines de la misma, como se analiza más adelante.

- **Consentimiento.** La regulación en comento aparentemente olvida que existe un consentimiento tácito. Obliga, necesariamente, a un consentimiento expreso por parte de quien revela los datos. Estimo que esta premisa es excesiva, puesto que es claro que quien revela datos para un fin, en ese acto está dando un consentimiento, aunque éste sea tácito. Por tal virtud, es necesario analizar los fines para los cuales se utilizará la información y con base en ellos, crear un

esquema de otorgamiento del consentimiento, más *ad hoc* a la realidad. Lo anterior se podría alcanzar mediante un modelo mixto de consentimiento, tácito (Opt out) y expreso (Opt in), como se analiza más adelante.

- **Transferencia Internacional de Datos.** La legislación europea, acertadamente, identifica que éste es un problema de carácter internacional y que de poco sirve si no se homologa una legislación a nivel mundial. Por tal virtud, sólo se autoriza la transferencia de datos personales a países que tengan "un nivel adecuado de la protección de la privacidad". La primera pregunta, especialmente en países civilistas como México, es determinar qué "es un nivel adecuado". No obstante, es evidente que lo que pretende dicha premisa es evitar la creación de "paraísos informáticos", conocidos como "*data heavens*". Es decir, jurisdicciones en donde la carencia de protección de datos, las transforme en sitios atractivos para el uso de dichos actos que pudieren ser violatorios de otras leyes de privacidad. El pequeño detalle, es que Estados Unidos no tiene una legislación única que regule la protección de los datos personales en la manera en que la legislación europea los regula, sino que tiene un modelo combinado de legislaciones y disposiciones reglamentarias mixtas y mecanismos auto-regulatorios. Si México fuera a adoptar un modelo de legislación similar al europeo, en donde una de las premisas fundamentales, es precisamente, el evitar "*data heavens*"; y siendo que Estados Unidos resulta ser nuestro socio comercial principal, este premisa representa un reto sumamente importante, sino es que insuperable, para México en relación a una posible adopción de un modelo europeo.

- **Órgano Regulador**. Aunque no se considera una mala idea tener un órgano regulador en materia de privacidad de datos, sí puede ser excesivo en cuanto se refiere, específicamente, a México. La carga burocrática con la que ya carga este país se convierte cada día más insostenible, y no estimo que sea una buena opción tener un organismo adicional a los ya existentes. Se considera mejor opción facultar a alguna autoridad administrativa ya existente, como podría ser PROFECO, en el contexto de relaciones de consumo.

Dados estos retos, es menester tomar lo bueno que contiene la legislación o modelo europeo, pero sería muy triste que México no aprovechara la oportunidad de aprender de los errores evidenciados a lo largo del tiempo en Europa en lo que a regulación de datos personales se refiere.

En efecto, no queda duda que es necesario legislar en materia de privacidad de datos, pero dicha legislación no puede ser anacrónica y debe tomar lo mejor del derecho comparado. Dicha legislación debe de aplicar, tanto a la recolección de información "en línea", como a la que se obtiene por otros medios no electrónicos, ya que la obtención de datos privados, no es exclusivo a medios electrónicos. La problemática de datos personales no es exclusiva de las nuevas tecnologías, basta una comunicación verbal, escrita o, incluso, una simple encuesta, para obtener datos personales. Lo anterior a efecto de contar con un mismo plano regulatorio y así no comprometer el flujo de información que pudiere darse entre los dos medios de recolección de datos. Las premisas propuestas son las siguientes (en relación con datos personales recolectados y tratados por entidades privadas):

- **Notificación de privacidad obligatoria para quienes la recolectan cuando información personal identificable es obtenida**. Antes de que cualquier entidad pueda recolectar información personal identificable de parte de una persona, debe de notificarle de tal hecho, informando además, del uso que se le dará a la información, así como las prácticas de revelación a terceros. Esto es lo que en el derecho anglosajón se conoce como aviso de privacidad o "Privacy Notice". Además, la notificación debe incluir, como mínimo lo siguiente:

    - Identificación respecto al tipo de información personal identificable que la entidad esté recolectando, usando y revelando a terceras entidades. Esto incluye tanto el propósito primario para la cual dicha información personal identificable es utilizado y, en su caso revelado, como puede ser una transacción comercial, entregar algún producto o servicio solicitado, o responder a una duda, así como

cualquier propósito secundario, como puede ser alguna actividad de mercadeo directo o cualquier otro propósito no considerado como primario.

- Las terceras entidades a las cuales la información podría ser revelada para la obtención del objeto, tanto primario, como secundario.

- Los medios por los cuales una persona puede limitar el uso y revelación de dicha información para propósitos secundarios.

- Información respecto a cómo una persona puede acceder su información y contactar a la entidad para conocerla, comunicarse o modificarla.

- **Notificaciones adicionales para uso o revelación de información para propósitos secundarios.** Las entidades que deseen utilizar o revelar información para propósitos secundarios deben proveer información adicional o información de consentimiento, al momento de recolectar la información, haciéndoles saber que dicha información podría ser utilizada para un propósito secundario.

- **Obtención de consentimiento para uso y revelación de información para propósitos secundarios.** En términos generales, las entidades recolectoras de información, sólo podrán utilizar o revelar la información obtenida para un propósito secundario si el individuo otorga su consentimiento para tal efecto. Para el uso de información para un propósito secundario, el consentimiento se puede obtener de las siguientes maneras:

    - *Consentimiento implícito basado en una notificación robusta*. Para el uso de información para propósitos secundarios que estén condicionados a recibir un servicio o beneficio continuo, la entidad debe proveer una notificación robusta o suficiente a la persona y recibir aceptación por parte de ésta.

- *Consentimiento por "Opt out"*. Como mínimo, la entidad recolectora de información debe proveer a las personas la capacidad de negar su consentimiento, en cualquier momento, cuando el uso o revelación de la información tiene propósitos secundarios. Dicha opción debe ser libre de costo y continuo.

- *Consentimiento por " Opt in"* Como alternativa, una entidad recolectora de información puede obtener un consentimiento de "*Op in"*, o expreso para ese propósito específico, siempre que la persona pueda retirar el consentimiento en cualquier momento.

- **Luego entonces, una entidad recolectora de información, necesariamente deber de obtener consentimiento de la persona para propósitos secundarios, ya sea "*Opt in*" o "*Opt out*" según sea el caso.**

- ***"Opt in"* o consentimiento expreso cuando el uso o revelación sea de información "sensible."** Antes de que una entidad recolecte o revele información "sensible", como puede ser información de carácter médico o financiero, para propósitos secundarios, necesita obtener siempre una aceptación expresa por parte de la persona (Opt in).
- **"*Opt in*" o consentimiento expreso para el re-uso de la información o re-distribución de la misma por parte de entidades terceras, bajo las siguientes premisas:**

  - Entidades que revelen información con base en el consentimiento expreso, están obligadas a dar a conocer a los terceros las limitaciones del propósito para el cual la persona otorgó su consentimiento originalmente.
  - Las entidades terceras que reciban dicha información no podrán re-usar o re-distribuir dicha información, salvo que obtengan un consentimiento expreso de la persona.

- En caso de que la entidad recolectora de información desee cambiar su política de privacidad, debe notificar a la persona de la cual obtuvo dicha información y obtener su consentimiento expreso.
- **Medidas de Seguridad suficientes.** A efecto de preservar la privacidad de las personas, las entidades recolectoras de información deben tomar medidas suficientes para proteger la información de pérdida, mal uso, acceso no autorizado, destrucción y error. Estas medidas deben ser administrativas, técnicas y físicas.

- **Derechos de acceso por parte de las personas.** A efecto de maximizar el control que tengan los individuos sobre la información, la entidad recolectora les deberá dar acceso a dicha información para corregir o cambiar cualquier información no correcta.
- **Coerción.** Dado que la premisa en la cual nos basamos son relaciones de coordinación, es decir, entre particulares, debe ser una entidad administrativa la encargada de velar porque estas reglas generales sean cumplidas.

Como se puede observar, la propuesta pretende regular la raíz del problema que conlleva el mal uso de la obtención de datos personales y basa la solución en el consentimiento.

Esto es, se trata de una variación sutil, pero muy importante, de la premisa de regulación, en el sentido de que no es jurídicamente válido que una entidad privada recolecte o use información o datos personales de sus informantes, a no ser de que dé los avisos de privacidad requeridos por la ley, respecto de los objetos primarios y secundarios para los cuales se recolecta la información.

Es un modelo combinado de esquemas de opt-in y opt-out, que preserva la agilidad de las relaciones comerciales actuales (que requieren necesariamente la recolección y manejo de datos personales, especialmente en un mundo como el de hoy, en que la mayoría de los servicios son *"outsourceados"*), al tiempo que garantiza a los informantes, a los titulares de la información, a conocer con precisión el alcance del uso de su información, y sus derechos en relación con ella.

Más que una legislación restrictiva, de controles de tratamiento, de registros obligatorios, de supervisiones gubernamentales (que han probado su ineficacia), necesitamos una legislación de vanguardia, con un enfoque positivo pero firme, como puede ser el modelo basado en la existencia y regulación específica de los avisos de privacidad por parte de los particulares.