feature

Privacidad en era de la monitorización y la vigilancia

Un marco conceptual de protección de datos personales

Estamos en un momento de la humanidad donde las tensiones geopolíticas, establecen momentos de incertidumbre, de dudas y miedos. No es posible prever las acciones de los países ni establecer con claridad sus intenciones. El mundo vive momentos de paz tensa donde todos de alguna manera observan a los otros, como una forma de tratar de entender y anticipar que puede pasar y no estar desprevenido.

La necesidad de conocer y saber está desbordada como quiera que quien no tiene la capacidad de explorar y pronosticar los próximos pasos de su inmediato competidor clave, está en desventaja y será presa de los sistemas de inteligencia de otros y lo que es peor, será desnudado sobre sus estrategias y ventajas competitivas para su sector de negocio. En este escenario pensar en seguridad, control o privacidad de la información establece un paradigma contradictorio y sobre manera retador para dar respuesta a una realidad que busca revelar y comprometer.

Con este marco de actuación, la privacidad aparece amenazada por convivencia, por ser una aliada de las personas naturales y sobre manera un derecho que asiste a los individuos en medio de una sociedad del monitoreo y la vigilancia. Conforme más tecnología se adhiere e integra a los productos y servicios[1], mayor flujo de información tenemos y, por lo tanto, la probabilidad de que la información personal se vea comprometida cada vez es mayor. Frente a esta realidad, se hace necesario revisar con detalle algunos de los elementos que motivan escenarios adversos contra la privacidad y establecer un modelo de protección de la privacidad, que no solo consulte las prácticas de las naciones desde sus elementos jurídicos, sino que incluya prácticas vigentes de seguridad y control de las organizaciones, así como los comportamientos de las personas como una alternativa clave en medio de las tensiones internacionales.

Jeimy J. Cano, Ph.D, CFC, CFE, CMAS
Es profesor e investigador del Grupo de Estudios en Comercio Electrónico, Telecomunicaciones e Informática (GECTI) de la Facultad de Derecho de la Universidad de los Andes (Bogota, Colombia) y es candidato a su segundo título de doctor, ahora en educación de la Universidad Santo Tomás (Bogota, Colombia).

Elementos que generan tensión en la protección de datos personales

Dentro de los elementos claves a revisar tenemos la influencia y control de los países desarrollados, donde se concentra el mayor número de empresas multinacionales y adelantos tecnológicos que permean los diferentes negocios y necesidades de las personas. Estos países necesariamente buscan alternativas positivas y generosas para sus negocios, con el fin de consolidar sus actividades financieras y mantener los flujos de capital que, dicho sea de paso, igualmente nutren las economías emergentes.

Otro participante de esta realidad controversial es las regulaciones nacionales, las cuales generan tensiones y motivan acciones que resguardan las expectativas y realidades de sus propios países respecto de la protección de sus intereses, los cuales muchas veces deben ser negociados y asistidos de acuerdos económicos, que permitan el flujo de inversiones e información, que promuevan alianzas gana-gana donde los productos y servicios se alineen con estándares establecidos por entidades, muchas de ellas residentes en países desarrollados.

Un siguiente componente a revisar es el "entendimiento de la privacidad". Mientras en países anglosajones esta suele ser un servicio por el cual se paga y se confirma a través de acuerdos comerciales, en países eurocéntricos resulta ser un derecho cuya asistencia y capacidad de cumplimiento se delega al Estado. Las dos posiciones resultan de alguna manera enfrentadas, pues mientras la primera es una motivación de conexión comercial y de negocios, la segunda está centrada en la persona y sus connotaciones frente a un derecho de rango constitucional.

Si se ubican estos tres elementos en el escenario del mundo de la monitorización y la vigilancia, la pregunta que surge es ¿qué es lo que va a primar en el ejercicio de la protección de los datos personales, las necesidades nacionales, asistidas desde la natural protección del estado como bien superior, o las necesidades comerciales propias de un mundo

global o realmente la reinvindicación de la persona desde la dignidad que le asiste desde la realidad constitucional?

Cualquiera que sea la respuesta la tensión estará presente y el ejercicio de protección de la información personal será una temática donde habrá que hacer concesiones en cualquiera de las dimensiones analizadas. En este sentido, la pregunta para una persona natural sería ¿qué sería aquello (producto o servicio) por el cual estaría dispuesto a compartir sus datos personales? Es decir, ¿estaría dispuesto a renunciar a su privacidad, a su derecho de no revelar algo que es personal, que lo distingue y que lo identifica?

Nuevos normales que debemos entender en la protección de datos personales

Estamos viviendo en medio de una nueva revolución informática e industrial que interroga las condiciones actuales de las implementaciones tecnológicas vigentes. La necesidad cada vez más urgente de tener información para tomar decisiones y explorar hacia adelante de nuevas propuestas[2], establece un escenario donde la información debe ser instantánea (en redes sociales), estar en movimiento, en la nube, analizada y conectada a las cosas de la realidad.

En este contexto, tratar de contener o mantener la información que debe ser reservada, bien por condiciones de negocio o cumplimiento normativo, establece un reto cada vez más exigente, pues todo alrededor nos invita y nos sugiere una conexión o transmisión de información, decisión que al final queda en manos de los individuos que tiene acceso a ella, a su criterio de seguridad y control, así como a su entendimiento de la protección de los datos personales)[3].

En este sentido los académicos establecen una serie de consideraciones que se deben analizar respecto de la transparencia de las organizaciones en un mundo de información asimétrica[4], las cuales, leídas en el escenario de los datos personales, resultan de interés, dado el entendimiento de la realidad interconectada que consideran y la necesidad de conocer y compartir que demanda una sociedad de la información y el conocimiento.

> **“El ejercicio de protección de la información personal será una temática donde habrá que hacer concesiones en cualquiera de las dimensiones analizadas.”**

Las consideraciones mencionadas son:

- **Revise sus supuestos sobre cómo mantener resguardada la información**. Mantener secretos o establecer límites a la información cada día será más complicado y más exigente. Podrá tener éxito algunas veces y otras no. En el contexto de los datos personales, las prácticas de las personas sobre el acceso a este tipo de información, la validación permanente de las mismas y la apropiación de los riesgos que estos datos establece para las organizaciones, son elementos que deben ser parte del gobierno y gestión de la privacidad de las empresas en este nuevo milenio.
- **Revise su estrategia corporativa frente a revelaciones de información no deseadas**. Si la estrategia corporativa depende de la información y sus flujos en los procesos misionales, es decir, se usa de forma constante y tratada de manera permanente por personas en la empresa, deberá revisar sus esquemas de seguridad y control para disminuir la probabilidad de fugas de información clave no deseadas. En el escenario de los datos personales, la clasificación de la información y las medidas de seguridad y control asociadas con el nivel de sensibilidad, deberán ser la norma base

de la protección de dichos datos, como quiera que si bien, muchas de ellas son de consulta permanente, cualquier fuga inesperada puede comprometer la confiabilidad de la empresa en su entorno de negocio.

- **Revise sus operaciones y aquellos aspectos que pueden ser problemáticos si se revelan**. No es que las empresas estén ocultando cosas inadecuadas o temas semejantes, sino que deben ajustar sus procesos en toda la cadena de suministro, para establecer las mejores prácticas que aseguren el debido cuidado de la organización frente a la operación y la rendición de cuentas ante el equipo ejecutivo. Respecto de los datos personales, la cadena de suministro debe conocer muy bien los flujos de datos personales que tiene, las prácticas que debe aplicar, los registros que debe dejar y los reportes que deben hacer. Una brecha de datos personales, generalmente motiva acciones administrativas y jurídicas en contra de la empresa objeto de la falla de seguridad y control.
- **Asuma que las personas pueden revelar información sobre su organización por sus propias razones y usted no será capaz de impedirlo**. Este elemento habla del manejo y control de la imagen de las empresas, las cuales deben estar preparadas para responder rápidamente, especialmente cuando la información publicada es incorrecta. Es claro que no podrá detener falsedades intencionales a través de las redes sociales, pero lo que sí puede hacer es registrar información precisa en el ciberespacio, con personas responsables con hechos que se pueden verificar. Esta realidad sobre los datos personales, implica una apropiación de las personas a cargo de su tratamiento, de tal forma, que comprenda los riesgos e impactos que sus acciones pueden tener en el eventual caso que quiera alterar o modificar información personal a la cual tiene acceso sin autorización o con fines distintos a los establecidos por la empresa.
- **Reconozca que los nuevos flujos de información cambian aquello que las personas consideran justo**. Antes del uso masivo del ciberespacio, los flujos de información eran limitados y sometidos a controles propios de los procesos empresariales los cuales no tenían mucho debate. Con el acceso a la información de forma permanente y abierta, las personas sienten que mucho de lo que tienen o reciben debería estar igualmente en el dominio público. En este sentido el acceso a la información no debería ser una restricción sino una oportunidad para conocer mejor, lo cual en el contexto empresarial genera contradicciones y fuertes debates que se asisten de reglamentaciones y conceptos legales[5].

  En datos personales ocurre algo semejante, no es el control de acceso lo que cambia la forma de pensar de las personas, sino el uso que éstas le dan a la información a la que tiene acceso y allí es donde, la diferencia se presenta en las prácticas actuales de protección de estos datos: se debe pensar en un control de uso de la información personal, asistido por control de acceso y no al revés, lo que implica una responsabilidad individual sobre el "accountability" que la organización tiene con los datos de sus clientes, empleados o terceros involucrados[6].

Una propuesta de un marco de protección de la privacidad

Considerando los nuevos normales y las tensiones mencionadas previamente, el marco de actuación y acción para proteger la privacidad, deberá estar articulado al menos en el grado de vulneración de la privacidad y el grado de efectividad de las prácticas disponibles en el momento, dos variables que se concentran en el fundamento de la protección que son las personas y las fallas que se pueden generar frente a la custodia del dato personal, sin importar otros aspectos que generan tensión.

Si bien puede haber muchos otros criterios que se pueden usar para establecer un marco de acción sobre la protección de la privacidad, éste se debería fundar sobre la inevitabilidad de una violación de la privacidad, como quiera que el contexto que previamente se ha comentado está diseñado para que el flujo de información se materialice, bien de forma intencional o no intencional.

El marco conceptual propuesto a continuación, sobre consejos de seguridad (**figura 1**)[7], ofrece cuatro cuadrantes que buscan situar el ámbito de la protección de datos personales con acciones concretas que evolucionan con la exposición de los flujos de información y las nuevas amenazas a la privacidad, generalmente asociadas con nuevos vectores de ataque a la seguridad de la información y al surgimiento de servicios o productos que consultan o solicitan datos personales para configurar o entregar la promesa de valor que ofrecen.

El cuadrante inferior izquierdo—que denominaremos actual—indica las vulneraciones específicas que se tienen a la privacidad que son ampliamente mencionadas en las regulaciones internacionales y buenas prácticas de entidades y asociaciones de estándares multinacionales, las cuales por lo general están asociadas con inadecuadas prácticas en el tratamiento de la información: fallas en la disposición final de datos, limitadas prácticas de seguridad y control en equipos de cómputo (p.e contraseñas, cifrado, respaldos de información), extracción de información mediante engaños (ingeniería social)[8].

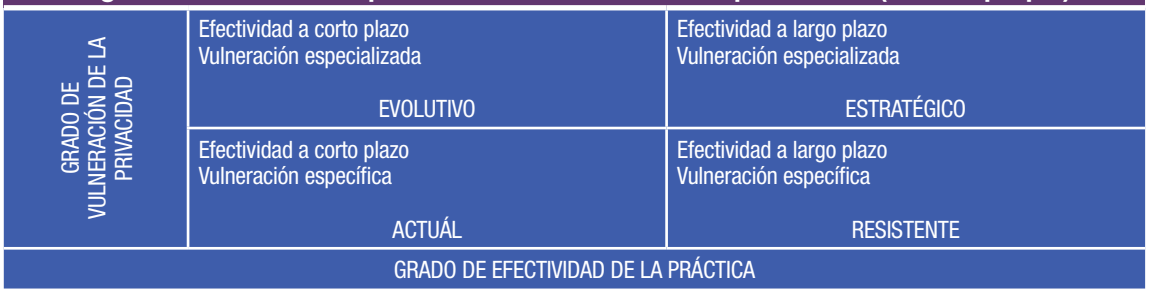
Para estos eventos, existen prácticas de seguridad y control que son de aplicación inmediata y de corto plazo, que permiten aumentar la resistencia de la organización frente a una fuga o pérdida de información personal, las cuales terminan siendo estándares para las personas que tiene a su cargo dicha información y de manera general para todos en una empresa, que reconocen en el dato personal un derecho del cual cada empleado se hace custodio y garante.

El cuadrante inferior derecho—que denominaremos resistente—es un área que nos ilustra las vulneraciones específicas a la privacidad, previamente mencionadas en el cuadrante anterior, en el cual las prácticas establecidas tienen el reto de incorporar en el imaginario colectivo de los individuos de una organización, una referencia permanente y formal de la protección de los datos personales, como una competencia genérica, propia de empresas que reconocen el valor de la información y el respeto por los derechos y garantías de los ciudadanos en el tratamiento de su información personal.

Para lograr lo anterior, se requiere desarrollar un trabajo de sensibilización, interiorización, apropiación y cumplimiento de las prácticas de protección de datos, como fundamento del comportamiento consentido y competente de las personas respecto de la privacidad. En este ejercicio, la alta gerencia asiste no solo como responsable último de las consecuencias de un inadecuado tratamiento de estos datos, sino como la primera interesada en la formación y configuración un imaginario que reconoce la privacidad como un derecho de los individuos y como un deber de cumplimiento en la empresa.

El cuadrante superior izquierdo—que denominaremos evolutivo—representa el reto que los nuevos vectores de ataque[9, 10] producen y donde las prácticas conocidas se quedan cortas para facilitar la protección de los datos personales. Ataques como las amenazas persistentes avanzadas, el secuestro de datos (en inglés ransomware), los códigos maliciosos (malware

Figura 1—Marco conceptual de Protección de datos personales (Autoría propia)



Source: Fuente: J. Cano. Reimpreso con autorización.

incluso en sistemas móviles), son ejemplos de realidades novedosas cuyos efectos en la privacidad comprometen las buenas prácticas que puedan tener algunas organizaciones, dadas las múltiples y variadas formas en que se pueden presentar las mismas.

Para este contexto, las prácticas conocidas en seguridad y control pueden tener una efectividad limitada, por lo cual se deben estudiar con detalle, estrategias extendidas de protección de datos tanto en los flujos como en las fuentes de los datos, que si bien no evitarán una vulneración a la privacidad, establecen acciones adicionales como cifrados de datos[11] y vistas particulares de acceso debidamente monitoreadas, direcciones IP y localizaciones autorizadas, dispositivos y aplicaciones previamente registrados y autorizados, dobles autorizaciones para el acceso, control de horarios y cifras de control, entre otras actividades, que hagan más resistentes los flujos de información a revelaciones o pérdidas no deseadas.

El cuadrante superior derecho—que denominaremos estratégico—configura el reto más alto para un responsable de la protección de datos en una organización, esto es, mantener una visión actualizada de las amenazas a la privacidad empresarial, configurando prácticas extendidas de protección como las mencionadas en el cuadrante evolutivo, asegurando una transformación permanente del imaginario colectivo sobre la privacidad, ajustado con las exigencias del entorno y los entes de supervisión, así como con las expectativas de los clientes y usuarios.

Para lograr esta condición, se requiere la aplicación de un análisis de impacto de privacidad extendido, que no solo considere los riesgos conocidos y reportados frente a la privacidad, sino que consulte amenazas y riesgos latentes, emergentes y de industria[12], con el fin de motivar acciones preventivas frente a este escenario y anticipe prácticas que aumenten la resistencia de la empresa frente a vulneraciones especializadas a la privacidad y así, fortalezca su marco de debido cuidado en la protección de datos personales frente a cada uno de sus grupos de interés.

Reflexiones finales

No hay duda que en un mundo interconectado y de tensiones geopolíticas, la información en general tiene una importancia fundamental que define las estrategias políticas, económicas, sociales y administrativas en una sociedad de la información y el conocimiento. El control y gestión de la información para la toma de decisiones establece el referente natural de la gerencia moderna, que entiende que los datos tienen un poder en potencia para quienes los tienen, y son sus intenciones y acceso legítimo los que determinan finalmente su uso.

> **“Cada vez se advierte una modificación digital de los productos y servicios a los que se tiene acceso, que los flujos de información que se generan permiten una mayor identificación de los individuos.”**

Bajo estos parámetros y conscientes de que cada vez se advierte una modificación digital de los productos y servicios a los que se tiene acceso, que los flujos de información que se generan permiten una mayor identificación de los individuos, es claro que la privacidad establece un reto para los individuos, las organizaciones y las naciones, como quiera que genera tensiones que construyen dilemas donde los beneficios de unos son desventajas para otros.

En este sentido, la propuesta del marco conceptual de protección presentada en este documento,

busca conciliar las prácticas internas de las organizaciones con las exigencias del entorno y la inevitabilidad de una vulneración de la privacidad, con el fin de fundar un esfuerzo inteligente, que consultando las tensiones que genera el tema y los nuevos normales que debemos entender en la protección de los datos personales, permita construir una estrategia de privacidad evolutiva que muestre la madurez del programa de protección de datos personales en una organización.

Indistintamente cambien las regulaciones, los comportamientos y hábitos de las personas y se tengan nuevos vectores de ataque a la seguridad de la información, el marco conceptual de privacidad sugerido deberá aprender y desaprender para poder madurar frente al entorno que se le imponga. Está en manos de la organización, cada uno de sus empleados y en particular del ejecutivo responsable de la protección de datos personales, darle forma a los cuadrante enumerados y detallados para construir una distinción de privacidad ajustada a la realidad de la empresa, que consolide el imaginario de respeto, compromiso y cumplimiento frente a la dignidad de las personas y su autodeterminación informática.

Referencias

1 Federal Trade Commission (FTC), *Internet of Things: Privacy & Security in a Connected World*, FTC Staff Report, USA, January 2015, *https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf*

2 Bodell, L.; "Five Steps to Formalizing Forward Thinking in Your Organization," *Strategy+Business Blogs*, 4 January 2016, *www.strategy-business.com/blog/Five-Steps-to-Formalizing-Forward-Thinking-in-Your-Organization*

3 Cano, J.; "Privacidad en las conversaciones electrónicas. Cuatro perfiles para analizar," IT-Insecurity blog, 25 October 2015, *http://insecurityit.blogspot.com.co/2015/10/la-privacidad-en-las-conversaciones.html*

4 Austin, R.; D. Upton; "Leading in the Age of Super-Transparency," *Sloan Management Review*, 14 December 2015, *http://sloanreview.mit.edu/article/leading-in-the-age-of-super-transparency/*

5 *Ibid*.

6 Smith, J.; "Demanding Accountability: The Need for Cyber Liability," *Help Net Security*, 4 January 2016, *www.net-security.org/article.php?id=2436*

7 Stewart, G.; "The Security Advice Magic Quadrant," *ISSA Journal*, February 2016, *www.bluetoad.com/publication/index.php?i=-286807&m=1336&l=1&p=7&pre=*

8 Krausz, M.; J. Walker; *The True Cost of Information Security Breaches and Cyber Crime*, IT Governance Publishing, UK, 2013

9 Goodman, M.; *Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It,* Doubleday, USA, 2015

10 Zetter, K; "The Biggest Security Threats We'll Face in 2016," *Wired*, 1 January 2016, *www.wired.com/2016/01/the-biggest-security-threats-well-face-in-2016*

11 Greenberg, A.; "The Father of Online Anonymity Has a Plan to End the Crypto War," *Wired*, 6 January 2016, *www.wired.com/2016/01/david-chaum-father-of-online-anonymity-plan-to-end-the-crypto-wars/*

12 Cano, J.; *La ventana de AREM. Una herramienta estratégica y táctica para visualizar la incertidumbre. Actas de la XIII Reunión Española de Criptología y Seguridad de la Información*, RECSI 2014, Alicante, Spain, 2-5 September 2014, *http://web.ua.es/es/recsi2014/documentos/papers/la-ventana-de-arem-una-herramienta-estrategica-y-tactica-para-visualizar-la-incertidumbre.pdf*