

# Seguridad vs. privacidad

*La ley sobre protección de datos personales obliga a que las organizaciones se preparen, a que la Academia forme sobre las nuevas necesidades, porque además de contemplar la tecnología es un binomio de seguridad-libertad, señalaron los expertos.*

Sara Gallardo M.

Los datos personales generan más de un dolor de cabeza en las organizaciones, porque muchas de ellas no los tienen clasificados y su protección es un derecho fundamental de los usuarios. De ahí la razón de este debate, en el que fue abordada la ley que está andando camino a ser sancionada y puesta en marcha.

El director de la revista Francisco Rueda dio la bienvenida a los invitados, enfatizando en la importancia de estos foros, en el sentido de suministrar a nuestros lectores una información de primera mano en las voces de especialistas de diferentes sectores, convocados con el propósito de tener un amplio cubrimiento de opiniones.

Estuvieron presentes María Fernanda Guerrero M., Gerente de Ilazió, Enlace al derecho; Javier Díaz Evans, director de Seguridad Informática de ATH; Jaime Eduardo Santos, vicepresidente Legal y de Gobierno del Grupo Colpatria; el Intendente César Villamizar Parada, investigador de la Dijín; y, María Consuelo Franky, docente de la Universidad Javeriana.

“Es un panel exquisito en todas las aristas de los temas que vamos a tratar, los cuales trascienden lo técnico y lo legal, para enfatizar en la persona”, señaló Jeimy J. Cano, moderador del foro, antes de dar inicio al debate.

“Hay un escenario que gira en torno a la evolución del tema de seguridad en el país y creo que este foro viene muy bien, en lo relacionado con la protección de datos, y de cara al Tratado de Libre Comercio, –agregó-. Así mismo, el temario está enmarcado dentro de un contexto que contempla lo que ya está aprobado en la legislación, el proyecto de Ley, su impacto en las organizaciones, y la claridad que estas tienen sobre el particular”, agregó Jeimy J. Cano para formular la primera pregunta:

***Si las empresas tienen clasificada la información personal que poseen ¿qué hacen para manejarla?***

**Javier Díaz Evans**  
Director Seguridad Informática  
ATH

Con relación a la privacidad y los datos personales, hace varios años algunas empresas comenzaron a tener cierto tipo de contacto con leyes encaminadas a su protección, sobre todo aquellas que tenían relación con filiales o casa matriz radicadas en Europa. En la actualidad, los más altos estándares de privacidad se implementan cuando se lleva a cabo una transferencia de datos hacia algún país de la Unión Europea, UE. Entre Estados Unidos y Europa se han generado conflictos, originados precisamente con tales regulaciones.

Posteriormente, llegó a Colombia la ley 1266 de 2008 “Hábeas Data” la cual fue motivo para apalancar a través de los consultores, el reconocimiento de que toda base de datos de información personal, no sólo las desarrolladas por empresas del sector financiero y bases de datos de reputación financiera, debían cumplir con los lineamientos establecidos en la ley. Esperamos que este año con la aprobación de la ley de protección de datos personales, esas compañías que tuvieron la asesoría de consultores y que profundizaron la ley 1266 de 2008, no se vean tan impactadas enfrentando el cumplimiento.

El sector financiero no se ha orientado a generar un modelo exclusivo de privacidad, sino que lo ha incluido en el mismo modelo de seguridad. En esa dirección, se establecen políticas de clasificación de información y, dentro de ellas, se involucra un conjunto de datos relacionados con personas, como: datos de identificación personal, información médica, hábitos y costumbre; los cuales hemos denominado datos privados y hemos identificado en qué momento nuestras organizaciones generan, procesan, transmiten y resguardan este tipo de datos o información. De los lineamientos o controles que se han establecido se encuentran en primera medida: determinar un responsable frente a dichos datos, toda vez que es fundamental determinar la responsabilidad. Puede responsabilizarse al oficial de seguridad garantizando controles frente a la protección de privacidad en actividades como investigación, monitoreo o forense que realice esta área. El segundo aspecto es el inventario de información, saber qué estamos

recolectando, en dónde está, y aunque es un tema técnico, es importante que las organizaciones apliquen los conceptos de ciclo de vida de la información; es decir, en dónde se crean y se resguardan los datos personales. Cómo se transmiten y en qué momento de los procesos y operaciones del negocio estamos manipulando la información personal. El tercer aspecto son las actividades operativas que involucran el contacto con las personas, para informarles cambios, usos o modificaciones a las políticas de privacidad o la información personal. Y, por último, todos los temas tecnológicos que conocemos relacionados con la seguridad de la información, entre ellos la criptografía, el acceso, la prevención de fuga, entre otros.

**Francisco Rueda**  
*Director Revista*

***Mi inquietud es si todos esos aspectos señalados de verdad se tienen en cuenta. Para una empresa del sector financiero, por ejemplo, lo prioritario es la seguridad para evitar robos y clonación de tarjetas y, de golpe por estar pensando en eso la privacidad se vuelve un tema que puede convertirse en secundario, en la medida en que no existan robos ni cosas por el estilo. Entonces si los procesos no están muy formalizados y no hay mucha conciencia sobre la necesidad de la privacidad de la información de las personas, esto quizás se vuelva secundario. Los empleados de las empresas no sienten que eso sea muy importante.***

**Javier Díaz Evans**

El sector financiero tiene clara la necesidad de proteger los datos personales por la gran cantidad de eventos de fraude y suplantación de identidad que han elevado el riesgo a niveles inaceptables para nuestras organizaciones. PCI, el estándar de las franquicias de tarjetas orientado a proteger la información personal de los tarjetahabientes, es un claro ejemplo de la necesidad de proteger los datos personales. El sector financiero sabe de su problemática y ha trabajado mucho en beneficio de su protección.



Francisco Rueda (centro) indaga sobre la privacidad en las empresas, cuando de investigaciones se trata.

### **María Consuelo Franky**

*Docente*

*Universidad Javeriana*

Como ciudadano colombiano uno se siente muy desprotegido, siente que a cada rato le están sacando información a través de encuestas, realizadas por el sector financiero y los proveedores de celulares, y uno no sabe qué hacen con dicha información. Me parece muy importante que se regule ese manejo, porque aquí se han cometido muchos delitos y es un tema muy preocupante. Esta ley me parece vital para obtener la protección de los datos del ciudadano.

### **César Villamizar**

*Investigador*

*Dijín*

El problema de la empresa con relación al manejo de datos personales es la desinformación que se genera para los procesos de investigación criminal, porque en la averiguación de hechos y conductas para identificar a los responsables de los mismos, la Policía Judicial como instrumento de la Fiscalía General de la Nación que tiene la titularidad de la acción penal en Colombia, delega la realización de actuaciones, en las cuales el insumo significativo es la información.

La problemática son las talanqueras legales para poder acceder a la información, necesarias por cierto. Pero esto pasa a un segundo plano cuando se solicita información a las empresas que se supone tienen el manejo y administración de la información de

acuerdo con la ley 1266 de 2008, norma que señala que para administrar datos personales es necesario tener un administrador, un usuario y demás elementos. Pero, cuando se solicita la información, pasando por las vicisitudes del juez de control de garantías y todo lo que conlleva esta situación se observa que la información que da la empresa, o está incompleta o es totalmente diferente a la que también maneja otra entidad. Entonces, surge el problema en darle esa categoría de especial dentro de la investigación. No se sabe si la administración de la empresa ayuda en las investigaciones o, por el contrario, frenan y dificultan el avance de las investigaciones. Creo entonces que ese es el mayor de los problemas desde el punto de vista de la investigación penal, es decir, la mala información que se deriva por la mala administración.

### **Francisco Rueda**

*Y cuando ustedes como autoridades visitan una empresa, ¿cuál es la situación que encuentran? ¿Hay informalidad en los procesos? En promedio sobre el número de investigaciones que ustedes hacen, ¿cuál es la sensación que tienen? ¿Sí estamos preparados? Porque el tema que más preocupa no es la seguridad como tal, que se da como un hecho, sino el tema de la privacidad que es más sutil.*

### **César Villamizar**

Hay empresas en las que uno pide el teléfono de alguna persona, pero en lugar de entregar

el número suministran otro tipo de información personal. Esa falta de administración por parte de las compañías que tienen acceso a información privada de sus clientes y/o usuarios. No se tienen unas mínimas normas sobre lo que se debe o no entregar de esa información. También estamos limitados por una norma constitucional de un juez, para poder ir a buscar los datos personales, pero eso no reduce en beneficio de la investigación, porque nos convertimos en unos formalistas. En ese ejercicio se puede llevar tres o cuatro horas y en los procesos penales, los anaqueles están llenos. Hay investigaciones de 2005 o 2006, en los que los datos personales ya no son reales o están desactualizados. No existe una política definida en la empresa frente a lo que debe tener, proteger y entregar. Muchas veces tampoco nos entregan lo que deben.

**María Fernanda Guerrero M.**

*Gerente de Ilazión. Enlace al derecho*

En la empresa comienza a darse toda una revolución frente al tema del dato personal y su protección. Con la frase: “La privacidad está muerta, viva la privacidad” el profesor Mauro Paissan, miembro de la entidad garante de los datos personales de Italia, afirma que en los actuales momentos la privacidad es otra y continúa aceleradamente evolucionando a estadios diversos e insospechados. La realidad demuestra que desde el momento en que pasamos de la modernidad a la postmodernidad, carac-

terizada por una sociedad cada vez más fragmentada, el mundo se convierte en altamente incierto e inseguro, confirmando una vez más que la seguridad continúa siendo el valor máspreciado; pero, igualmente las libertades, especialmente la libre expresión, que van adquiriendo un significado y sentido fundamental con miras a su real reconocimiento y protección. Son tiempos inéditos, desafiantes e innovadores en el que el binomio seguridad-privacidad se debate entre la protección de los datos como un derecho vital de las personas, pero también del Estado, de lo político y lo económico. Una de las consecuencias precisamente de la crisis financiera del 2008 es precisamente el déficit que se presenta en la función que realizan los legisladores. La falta de adecuación de la ley a las nuevas exigencias, así como también en las sanciones por su cumplimiento, no deja bien parados a los legisladores. Son en cambio los jueces los que en últimas están definiendo la tendencia y crean y dan forma a un derecho viviente que cada vez se adapta a las nuevas realidades. De hecho, la directiva 95/46 de la Comunidad Europea en materia de protección de datos personales está siendo objeto de actualización y de integración a las legislaciones nacionales, desde el 25 de enero de este año. La Comunidad Europea, entonces, replantea los esquemas que durante 17 años no fueron tocados y que aunque se mantienen los principios originales, la realidad de hoy es otra completamente distinta. Lo dinámico de lo “relacional” entre seres humanos, empresas y Estado nos lleva



De izquierda a derecha: César Villamizar (Dijín); Francisco Rueda (Sistemas); María Fernanda Guerrero (Ilazión); Jaime Eduardo Santos (Colpatria); Javier Díaz Evans (ATH); María Consuelo Franky (Javeriana); y, Jeimy J. Cano (moderador).

a entender que la gestión de los datos, la información y la comunicación, ya no “uno a uno”, es dinámica y que son las redes sociales las que imponen una comunicación generalizada. El tema se convirtió en algo global y las realidades nacionales ya son otras frente a lo global y las empresas frente a lo global muestran que las exigencias son otras. Entonces se trata de nuevos esquemas para las empresas, para los Estados y los ciudadanos.

Llegó el momento en que la seguridad y la privacidad se transformaron en una industria. Muestra de ello es la designación de oficiales de cumplimiento, el diseño de manuales, etc. Ahora vemos que las normas fueron insuficientes y que la tecnología entra a jugar su papel y eso obliga a mirar las cosas desde el diseño de la privacidad. La tecnología es la que ahora establece la forma de la seguridad de los datos y la protección de los datos se volvió una completa industria. Ha contribuido, además, a que la alta jerarquía de las empresas tenga que ver con la responsabilidad en el manejo de los datos personales, ya no es un asunto exclusivo de los técnicos. Colombia y la mayoría de países están enfrentados en este momento a un nuevo paradigma y es cómo gestionar –no manejar, porque manejar es manipular-, cómo gobernar, orientar y hacer una buena gestión del dato.

Ese es el gran desafío que tienen hoy las empresas porque si vemos el texto del reglamento, que ya ha sido aprobado en la Unión Europea, las exigencias son mayores. Sin embargo, en el caso nuestro, los problemas continúan presentes en la misma conceptualización del tema. ¿Cómo es que todavía confundimos Hábeas Data con Privacidad e intimidad? Son conceptos diferentes. Finalmente, cabe preguntarnos ¿hasta dónde queremos sacrificar nuestra libertad a cambio de mayor seguridad? Pero, igualmente el consumo y los límites que se requieren para que éste sea sensato será un reto para las empresas en era digital.

**Francisco Rueda**

*Y ¿qué tan bien manejan y entienden tales conceptos las personas del común, el ciudadano corriente?*

**María Fernanda Guerrero M.**

No es el mejor. Lo que se requiere es dar el paso a la alfabetización digital; hay que volver a lo elemental. Eso no se ha hecho. Le aseguro que el movimiento M-15 o de los Indignados y la Primavera árabe tenía muy claro qué pretendían con la revolución que finalmente lograron y que se difundió rápidamente en el mundo. Las convocatorias a través de las redes sociales fueron, sin duda un éxito, pero en la práctica un detenimiento sobre lo que significa el derecho fundamental a la libre expresión y los límites del ejercicio de ese derecho no sobran para darle forma a la ciudadanía digital. La ignorancia en estos asuntos no es sólo de las personas, sino también de los Estados.

Un hecho importante en Colombia es que no tenemos aún la reforma a la Ley 1266 y tampoco el fallo de control de constitucionalidad de la Corte Constitucional. Cuando la ley finalmente se firme quedará muy pronto obsoleta. Sobre el comunicado de prensa estoy muy de acuerdo con los salvamentos de voto, porque quedamos con una protección de datos estática de empresas y de personas que tienen datos almacenados. Pero, qué sucede en una realidad más dinámica y práctica en la que el dato viaja de un lado para otro, en donde la libertad de expresión debe permitirse, pero también la seguridad debe ser un límite porque los derechos no son absolutos y hay un bien común que salvaguardar. Internet es un espacio y un concepto de bien común. Todo eso está ausente de muchas leyes nacionales y hasta ahora estamos poniendo sobre la mesa tales asuntos.

Recientemente en el Japón se habló de la contextualización del dato personal; es decir, la persona ya no es un nombre o una dirección, sino todo un conjunto de información, sumado al tema de la verdad. Al unir tanta información ¿qué es lo que realmente tenemos? Las definiciones, procedimientos, nuevas metodologías, nuevos modelos de clasificación, todo esto está siendo replanteado. Y el reglamento de la Unión Europea está efectivamente dando la pauta ¿lo que indica que prevalecerá la norma transnacional? No se sabe, pero sí es un referente





*Jaime Eduardo Santos (izquierda) dice: "...en Colombia con respecto a la información, usando el lenguaje de los físicos, estamos en el gobierno del caos con su ley de entropía, pues tenemos el desorden más grande con su propio orden,...".*

importante para los países. En los actuales momentos se están abriendo caminos alternativos e inevitablemente hay una narrativa diferente frente a los derechos. Debo permitir la gestión de datos personales también para garantizar otros derechos y ¿cómo lo vamos a hacer?

### **Jeimy J. Cano**

*Uno de los aspectos que señala el documento al que se ha referido María Fernanda sobre la Unión Europea, específicamente con relación a la privacidad y el flujo de datos a través de las fronteras, dice: "incrementar inminente atención sobre la protección de la privacidad al más alto nivel de las organizaciones, particularmente haciendo sentido del significado del uso del dato personal". Es un llamado casi internacional, una declaración que busca motivar a nivel global atención sobre el tema del dato personal, no sólo sobre su protección, sino sobre el dato en sí.*

### **Francisco Rueda**

*¿Y qué tan real es ese asunto aquí? ¿En qué nos afecta que los europeos tengan una reglamentación si los colombianos no la usan, no la apropian ni la concientizan? Son dos mundos. Precisamente lo que tratamos de hacer en estos foros es mirar*

*qué sucede aquí, en la realidad colombiana. En mi opinión existe un vacío entre el marco y su aplicación. ¿Aquí estamos preparados? ¿La ley colombiana está lista? ¿Hay un abismo?*

### **María Consuelo Franky**

Ese es un objetivo global, pero hay que realmente llegar a algo mucho más concreto en la legislación.

### **Jaime Eduardo Santos**

*Vicepresidente Legal y de Gobierno  
Grupo Colpatria*

En mi labor diaria de abogado uso los planteamientos de María Fernanda como un norte magnético, como un deber ser regulatorio a escala global, que sirve cuando estamos entre el barro de los casos particulares, explorando nuestra realidad local. Podría decir que en Colombia, con respecto a la información, usando el lenguaje de los físicos, estamos en el gobierno del caos, con su ley de entropía, pues tenemos el desorden más grande con su propio orden, que no es necesariamente el esperado por las regulaciones, y a eso nos enfrentamos cada vez que vamos a realizar una investigación. En la realidad, todas las empresas tenemos una clasificación formal de la información, por lo menos en las del sector financiero y las del mercado público de valores, que tienen reglas y control prudencial.

Se trata de una respuesta formal de las empresas fundada en el Código de Gobierno o con una certificación tipo ISO 27001, es decir, a todo se responde afirmativamente. Pero, cuando se hace una investigación legal o forense, nada de eso pasa del libro a la cultura corporativa. Eso no va más allá de buenos deseos y buenas intenciones. Teníamos todos los libros escritos en el mundo corporativo y ocurrió la crisis de los mercados desarrollados, y tenemos las políticas de protección de la información y permanentemente ocurre pérdida de datos. Entonces es muy distinto el manejo diario del dato, a lo que debería ser en la realidad formal de las políticas y las reglas.

Cuando uno está en una investigación concreta y escucha o lee al académico, se dice a sí mismo: -Un día puedo llegar allá, voy a procurar hacerlo, pero mientras tanto existe una realidad aquí, realidad que está mediada por tres variables: La primera es el derecho. Todos dicen las reglas se están cocinando, ya van a salir, como por ejemplo el fallo de constitucionalidad de la Ley de *Hábeas Data*; La segunda es la economía. Los datos se negocian como cualquier otro bien, dentro de la demanda y la oferta del mercado; no podemos desconocer que ahí aplica la economía pura. Y dentro de la tercera variable, la empresa, ¿Cómo se maneja esto? Como un activo de información, pero no se valora como otro bien patrimonial, sabemos que ahí están las marcas, los inmuebles y los muebles, pero también hay datos de la clientela y cuando se mira en tal sentido no se encuentra una partida en el balance que les asigne un valor. La contabilidad en sí misma no los reconoce, pero en todas partes dice: “aquí la información es un activo”. Y eso da lugar a que se pongan denuncias porque yo perdí un activo y recibí un daño, pero cuando va a mirar ese activo en la contabilidad no está registrado generando un debate probatorio infinito.

Pero, si voy más atrás de ese concepto de activo de información, es que la misma banca ya no maneja realmente dinero, sino datos. Hace 10 años, una sucursal bancaria podía tener en la bóveda setecientos millones de pesos, hoy en día puede que tenga unos pocos pesos, porque el 30% o el 50% de las

transacciones son por Internet, es decir, datos. Toda la seguridad que era para los billetes se reenfoca hacia los datos.

Permítanme insistir en que cuando se hace una investigación sobre la pérdida de datos dentro de las compañías, ya se sabe que se va a proceder dentro del desorden, pero el desorden tiene orden, tiene entropías, y entonces uno también aprende a navegar dentro del desorden, y éste siempre va a superar las reglas y el deber ser de los equipos de abogados. En un momento concreto y por ocasiones, los jueces logran construir hipótesis de responsabilidad, y en este tema se han vuelto más importantes sus decisiones que las normas generales. Hacen derecho. Como se puede leer en la línea jurisprudencial de *Hábeas Data*. Esto es así porque el operador judicial también se mete en el caos y se encuentra con situaciones singulares como que la prueba estaba mal recaudada, que la cadena de custodia no se cumplió. Un ejemplo es el fallo inhibitorio en el proceso que se adelantó usando como prueba correos electrónicos del computador de Reyes, el guerrillero de las Farc. Es decir, toda esa es la realidad que vivimos en el día a día del litigio con pruebas en datos electrónicos y también la realidad del ciudadano pues le pasa lo mismo, él como titular del dato se siente inseguro y confundido con los derechos y obligaciones en un contexto de alta movilidad de su información, de tal manera que debemos adentrarnos en el uso real del dato y en la práctica diaria.

Para cerrar les doy un ejemplo: una empresa puede tener una regla en sus códigos de conducta que advierta: “los computadores de esta entidad sólo se pueden usar para fines de la empresa, y no se puede tener acceso a Internet”. Pero, cuando uno va a la empresa eso no es cierto, porque encuentra información en los computadores que dice: “mi amor nos vemos a las cinco para llevar al niño al odontólogo”, u otro: “le vendo un cachorrito que tuvo mi perrita este fin de semana”. Si uno observa esa telaraña de datos personales y empresariales en la intranet de una empresa cuando adelanta una investigación forense debe clasificar y descartar mucha data. Entonces ¿Qué muestra eso? Que la empresa no es un laboratorio en el que se pueda manejar de

forma séptica la información; indica que las empresas y el mundo están vivos y no puedo esperar que pueda controlar la temperatura, la humedad, nada de eso se controla, ocurre y lo que ocurre es que tengo que aprender a navegar para proteger los intereses que esté representando.

### Francisco Rueda

*Pero, ¿no se puede buscar una mejor organización? ¿Es un poco lo que va a pasar con las leyes?*

### Jaime Eduardo Santos

No, yo creo que la data aprendió a vivir y evolucionar en el caos. Al parecer sigue la tendencia de la entropía en física, que es pasar del orden (baja entropía) al caos (alta entropía). Por lo tanto, no hace falta adicionar la segunda ley de la termodinámica, pues es querer parar la naturaleza con mandatos sociales que caducan todos los días a manos de la ciencia. Por eso estoy en contra de la regulación intervencionista del universo virtual.

¿Qué logra el ciudadano con leyes diseñadas de un solo lado del río, que no se pueden

aplicar y cuando se emiten ya están caducas? En ese sentido puede ser más eficiente el caos; por ejemplo en el "Hay Festival" de Cartagena en enero de este año, en los conversatorios sobre el movimiento de los indignados, algunos escritores extranjeros decían que Brasil y Colombia se han vuelto objeto de observación de los sociólogos y los antropólogos, y ¿Por qué? Porque ¿cómo ha hecho América Latina para funcionar en el caos? Europa perdió la esperanza y Estados Unidos la ética corporativa en un ambiente altamente regulado. Y entonces un sociólogo dice: -Bueno y ¿cómo funciona un lugar como Ciudad Bolívar en Bogotá? ¿Cómo se gobierna un país en vía de desarrollo con un conflicto interno armado de más de 50 años? En este momento estamos siendo objeto de observación, así como la Amazonía ha sido históricamente objeto de observación para los farmacéuticos, hoy en día nuestra sociedad es objeto de observación. Algo hacemos y no sabemos qué es. Entonces no me molesta el caos como el modelo descrito por los físicos cuánticos y sobre el cual ya existen trabajos sociales como el de Arieh Ben-Nain titulado *La entropía desvelada*, el mito de la segunda ley de la termodinámica y el sentido común, que les invito a leer.



Los invitados analizaron el contexto colombiano y el impacto que tendrá la ley.



## Jeimy J. Cano

*A la luz del tema práctico, los impactos que eso va a tener en las empresas, toda vez que se trata de una ley estatutaria que habrá que cumplir o sugerir alguna manera para hacerlo.*

## Jaime Eduardo Santos

Los impactos de la Ley serán tomados como el calor en la termodinámica. Es decir, que está presente cuando hay trabajo que transforma energía. Lo sentimos, por ejemplo, cuando nuestro PC está procesando información, al tiempo está generando calor.

## Javier Díaz Evans

Creo que el desarrollo tecnológico y las organizaciones tienen la capacidad de enfrentarse a la protección de los datos, se debe trabajar en procesos operativos para su manejo. Tenemos muchas herramientas y soluciones, los controles de seguridad siguen siendo los mismos de hace varios años, tan solo han evolucionado frente a las nuevas tecnologías. El punto está, más que en la tecnología y los procesos, en lo que denominamos Gobierno. Si la organización no tiene la voluntad para proteger los datos, eso nunca se va a dar. El Gobierno está en que la cabeza de la organización establezca la directriz, las personas, los procesos y la tecnología se encaminen a cumplir y que de vez en cuando monitoreemos su cumplimiento.

En esa dirección, lo que falta a las organizaciones y a la comunidad es tener claro que proteger los datos personales es fundamental. Y ahí quiero referirme a cómo vivimos hoy en día. Al ir a cualquier organización, llámese banco, clínica, hasta un supermercado; lo primero que hace la organización es pedir información personal. Pueden pedir registro de nacimiento, número de cédula y muchas veces información que no tiene nada que ver con el servicio que nos van a prestar y ahí radica el problema. Ahí es donde las regulaciones empiezan a funcionar, cuando la persona no tiene la capacidad de enfrentarse a las organizaciones y cuando la pelea es difícil por temas de desequilibrio de

fuerza, las leyes sí funcionan. En ese momento es cuando el Estado debería entrar a tomar partido para equilibrar dichas fuerzas. Lo que está sucediendo es que la organización le dice al ciudadano: -qué pena con usted, pero yo necesito toda la información para poderle prestar el servicio. Entonces se le deben dar a la persona las herramientas para reclamar y exigir una explicación sobre el uso que se le dará a los datos y cómo serán protegidos. En ese momento es necesario y no se puede dejar el caos, más bien empecemos a implementar modelos cooperativistas y control social.

## Francisco Rueda

*Pero en estos países la intimidad es un asunto del que el ciudadano no se ocupa. Estoy tratando es de sobrevivir. Para la mayoría de las entidades el tema de la privacidad quizás no es importante. Que los pongan a hablar de seguridad de pronto sí, pero de intimidad no, ¿qué tan “exquisito” es ese tema para una empresa?*

## Javier Díaz Evans

Las empresas las hacen las personas y esto es una ley que a cada uno de nosotros nos interesa. Como miembro de junta directiva, alta dirección o líder de una organización, me preocuparía sobre qué van a hacer con mis datos, para qué los van a utilizar. Si soy consciente de eso y dirijo una organización, voy a hacer lo que sea para que mi empresa responda en ese sentido, porque presto un servicio a la comunidad. Esto es regulación bajo un modelo de control social.

## María consuelo Franky

A pesar de que vivimos en el caos es necesario regular, porque si no lo hacemos quedamos por fuera de la globalización. Entiendo que esto es importante para poder negociar con otros países como Estados Unidos y los países de Europa. Tener esa legislación significa atraer la inversión y poder tener más puestos de trabajo, por ejemplo, en el negocio de los call centers. Esa inversión no ha llegado todavía porque a Colombia lo han visto como muy inseguro al respecto del tema de



*Dentro del impacto de la ley en el país, en la mesa de debate fueron contemplados también los costos.*

protección de datos. Entonces sí debemos legislar. Sin embargo, el aspecto más importante es la cultura dentro de las empresas. Todos debemos tomar conciencia sobre cuáles son nuestros derechos y deberes sobre los datos personales, pero dentro de las empresas también. Porque muchos de los delitos informáticos son realizados por los mismos empleados de las organizaciones, quienes manejan las bases de datos. Y ahí debe haber un proceso de cultura, de pronto no son conscientes de que lo que están haciendo es un delito. Hay que escribir, manuales, guías, procedimientos técnicos de seguridad, teniendo en cuenta que en la parte técnica no hay una solución 100 por ciento completa. No creo que en términos técnicos el avance sea apreciable, a pesar de los desarrollos recientes. Siempre va a haber vacíos, hay posibilidades de fraudes de suplantación de la identidad. Mi trabajo se orienta mucho a la seguridad para aplicaciones web y lo que he visto en las interventorías a los sistemas en el país es que existen muchas deficiencias. Son conocidos los temas técnicos de protección por roles para determinar quién se puede autenticar ante un sistema. Pero lo que sucede es que frecuentemente se protegen las páginas web, pero no el resto del sistema que es lo realmente importante. Así que cualquier ha-

cker suplanta las páginas e ingresa a los componentes internos del sistema y por ahí entran fácilmente a la base de datos. Me he referido a la seguridad cuando trabajamos con servidores de aplicaciones. Es lo que hoy en día utilizamos para aplicaciones en la web. No hay protección en muchas aplicaciones; a pesar de que están los elementos para proteger los sistemas, apenas se protege el acceso a las páginas y el vacío es enorme. Ahora con los sistemas en la nube, a veces operan para muchas empresas a la vez y comparten una misma base de datos, así que desde el punto de vista técnico cualquier tipo de consulta que se haga debe llevar un filtro indicando cuál es la empresa que está haciendo la consulta para que ésta no pueda ver los datos de la otra empresa. Pero eso es difícil lograrlo. En resumen, desde el punto de vista técnico, existen elementos para proteger el acceso a los datos de los sistemas, pero, frecuentemente no se aplican y cuando se hace de todas formas no existe la posibilidad de evitar la trampa dentro de la empresa que administra tales sistemas.

**Jeimy J. Cano**

*Hay una tendencia hacia la privacidad por diseño, relacionada con el tema técnico para introducir estos aspectos dentro del*

**tema de seguridad. Ahora nos referiremos a los asuntos jurídicos, la ley en concreto. A la luz de la práctica de dicha ley ¿cuáles son los impactos que ustedes contemplan en su implantación, uno de ellos los costos? No sólo para el sector financiero, sino para todo el mundo, desde el edificio que administra una huella biométrica hasta el señor del supermercado que tiene n datos personales con la famosa tarjeta puntos. En opinión de ustedes ¿cuál sería la crítica constructiva, sumada a los impactos que pueda tener en los sistemas de información?**

**Francisco Rueda**

***Pero cómo hacer para que al ciudadano joven le interese su privacidad, cuando pone fotos, información de todo tipo sin ninguna preocupación. Por mucho que advierta la Comunidad Europea, para los jóvenes del mundo no es una preocupación.***

**María Fernanda Guerrero**

A la gente joven le interesa ser vista. Se preocupa muy poco por los riesgos, pero esa actitud puede originarse por simple desconocimiento. En todo caso, el cumplimiento de la ley depende de la motivación de querer cumplirla, porque se cree y se comparte sus postulados y mandatos.

**César Villamizar**

Por estos días llegó a mi oficina una amiga de vieja data, abogada, y me dijo: “soy penalista y convivir con la delincuencia de cerca no me asusta. Pero, hoy sí estoy asustada porque tocaron a mi hijo a quien le hicieron el paseo millonario.” Deberíamos preguntarnos, entonces ¿cuándo les va a preocupar a las personas el manejo de los datos personales? Ahí es cuando nuestra entidad como brazo de la administración de justicia en la recepción de denuncias -se está evolucionando al entorno de la denuncia no formal, a través de los medios tecnológicos como lo es el CAI virtual-, percibe que desde el más joven hasta el más anciano, pone en conocimiento hechos como

los siguientes: “-Me robaron los datos personales, me subieron un perfil en Facebook, etc.” A partir de ese momento sí aparecen las preocupaciones. Las causas generalmente corresponden a la mala práctica de diligenciar en la web cualquier formato o formulario, que aunque sea con datos falsos, se ha podido establecer que de 10 formularios, al menos 5 contienen información cierta. Entonces, esos datos se convierten en el insumo fundamental y de utilidad para la ciberdelincuencia. En ese momento sí existe la necesidad de la protección, investigación y acudo a la administración de justicia. A los usuarios no les importa cómo y quién los regule en la navegación, pero el día que pasa algo sí la buscan. Me parece muy importante el tema de los principios, sobre todo para garantizar la integridad, con qué política va a garantizar los datos personales. La problemática es la afectación que se da con el uso de los datos personales, pero insisto, mientras estos no estén en juego no pasa nada. En ese caos vivimos, para compartir la opinión del doctor Jaime Eduardo Santos. Vivamos así que está bien, el problema es cuando se pasa la barrera de los datos personales en su utilización sea para bien o para mal. Si publican algo bueno perfecto, pero si publican algo malo viene el problema. La crítica a la ley estatutaria es que ordena la creación de un organismo para administrar bases de datos, pero está ausente la de crear institución alguna que nos permita identificar dónde están, quien tiene datos personales. En todas partes los datos de cada uno de los aquí presentes están circulando. En ese sentido se quedó corto el legislador en decir, pongámonos en cintura y miremos a ver qué tantas personas tienen datos personales, no todo el mundo se va a someter a la Superintendencia de Industria y Comercio para matricular la base de datos, que es lo que el Gobierno tiene que entrar a reglamentar a partir de la sanción de esta ley.

**Jaime Eduardo Santos**

Yo sigo con la hipótesis del caos para responder a César. Usted dice que sí sabe cuándo importa en un caso específico que conoció, y yo le digo que si nos metemos en la física cuántica, que es inherente a los grandes números, no importa esa singularidad en el

caos. Eso lo tienen clarísimo los denominados *Numerati*, que a toda hora están procesando datos estadísticos para gobernar. Cuando estamos operando en el mundo de bases de datos se está trabajando con grandes números en el lenguaje estadístico, para poder hacer predicciones útiles en torno a asuntos como el diseño de perfiles de riesgo de un segmento de clientes. Entonces, es una forma dura de contestar un evento particular, pero las bases de datos funcionan dentro de los criterios de los grandes números y cuando a uno le sucede algo, claramente le pasa y eso para uno es severo, emocional y patrimonialmente. Eso no es marginal para un ciudadano, en concreto es su vida, es el ciento por ciento. Entonces ningún ciudadano se encuentra por fuera del caos, todos estamos en relación con el caos en un nivel distinto, que era la pregunta de Francisco en relación con los jóvenes. Ellos forman parte también de ese caos, pero en un nivel distinto. O cuando Francisco se refería a los conceptos que emitía María Fernanda como algo muy exquisito de tratar. Yo lo veo con el filtro de la pirámide de Maslov. Si tengo un país en el que la gente no tiene empleo, pues qué le va a importar dónde está su dato o venderlo o prestarlo para sobrevivir. Pero atendiendo directamente la pregunta, creo que el impacto de esta Ley no va a ser nada distinto a un dato más en el caos, y que para que podamos empezar a digerirla, tenemos que trabajar con algún sistema de los que ya están muy cimentados en la banca, como los Sistemas de Administración de Riesgo-SAR,

que tienen un apellido como SARC, SARM, SARO, etc.

### **César Villamizar**

Pero ese transporte debe tener unas condiciones mínimas de seguridad para poderse movilizar.

### **Jaime Eduardo Santos**

Si esas condiciones mínimas se desarrollan dentro del caos sin intervención de autoridad. Esa es la diferencia entre lo que desea la regulación y lo que ocurre en las vías. Por la carrera séptima unos circulan en bus, otros en carro, otros en bicicleta, pero todos dentro del mismo caos, uno muy cómodo, otro apretado y otro haciendo equilibrio.

### **Francisco Rueda**

*Cuáles son las debilidades en la ley actual. ¿Cómo la ven? ¿Qué opinan? ¿Se quedó con lo tradicional, sin tener en cuenta el nuevo entorno de las redes sociales, la comunicación móvil, entre otros aspectos? ¿Cuáles son en resumen las grandes críticas, los grandes aciertos de esa ley, desde el punto de vista jurídico?*

### **María Fernanda Guerrero**

De alguna manera la ley solucionó algunos asuntos que teníamos sin resolver de tiempo



María Fernanda Guerrero (izquierda) señala que la protección de los datos debe contemplar un concepto holístico.



atrás. Por ejemplo, que la protección de datos era exclusivamente para datos del sector financiero. Hay otros datos que ameritan ser protegidos. La mirada debe ser a partir de un concepto holístico, pues todo está relacionado finalmente con datos. Una debilidad muy grande es el tema de la autoridad garante de protección de datos, porque no son autoridades independientes dentro de la administración. Y aunque se han logrado avances el sesgo se mantiene, la ley se enfoca al dato económico almacenado en centrales de riesgos. Es algo así como un poder preferente. Y en el tema constitucional, es decir, el Hábeas Data como derecho constitucional nos quedamos cortos, especialmente frente al ámbito de aplicación de los artículos 15 y 20 de la Carta. Al parecer, quisimos hacerlo mejor, pero finalmente estamos en lo mismo. Pero, soy optimista y espero que pronto tengamos la sentencia de la Corte para salir de las dudas. La motivación de los salvamentos parece contundente y llevaría a pensar que lo mejor habría sido declararla de una buena vez inconstitucional; sin embargo, me embarga la esperanza de que tendremos un mejor marco regulatorio a futuro. Eso depende de nosotros.

### **Javier Díaz Evans**

En una reunión con el doctor Nelson Remolina le preguntaba sobre cuál es la definición

jurídica de datos personales, cuál va a ser el alcance y qué se va a controlar con la ley de protección de datos personales. El problema radica en que todos tengamos claridad de estas respuestas. No podemos decirle a las personas, a través de una ley, qué pueden o no hacer con sus datos personales. Vivimos en un periodo donde las personas exponen y comparten sus datos personales sin medir el impacto de sus acciones. Pero lo que sí está detrás y lo que sí debemos buscar con esta ley es controlar qué van a hacer las organizaciones (ej.: redes sociales) con dicha información. En las redes sociales y otros sitios en Internet lo complicado es que la información salió de nuestra jurisdicción y nuestras leyes no tienen la capacidad de protegernos, porque se trata de una empresa fuera de Colombia, regulada por leyes extranjeras. Es complejo regular las acciones de los ciudadanos, pero sí las acciones de las organizaciones que pueden afectar a las personas por el tratamiento, manipulación y comercialización de la información personal.

### **César Villamizar**

Vendría en ese entorno la tercerización de los servicios. Hemos tenido casos en los que la fuga de información no es endilgable a la empresa titular del dato personal, sino a una compañía tercera que vende servicios, seguros, productos, entre otros. Y es allí



*César Villamizar (primero, izquierda) se refiere a la tercerización de los servicios.*





María Consuelo Franky enfatizó en aspectos como la prevención y la penalización.

donde hemos visto que como ellos no comulgan con la filosofía de la empresa y no les interesa la administración del dato, entonces es allí donde se fuga la información personal para crear cuentas falsas, para enviar spam, etc. Tiene una gran incidencia la tercerización de los servicios.

### Francisco Rueda

*Pero eso se puede interpretar en dos sentidos. Por una parte, existe la experiencia y uno se arriesga a enviar su información. En una empresa como Google o Microsoft, ¿no será que son más seguros los datos allá que aquí en un centro de datos ubicado en el centro de la ciudad? Ahí puede pasar cualquier cosa. Entonces, desde el punto de vista de la tercerización ¿es positivo o negativo para los asuntos que estamos analizando?*

### César Villamizar

Para nosotros todos los servidores de correo electrónico no están en el país y son un problema, porque pedimos información y esas empresas nos entregan lo que quieren. Por ejemplo, Hotmail nos entrega datos, a pesar de que en la creación de las cuentas existe información que cada usuario pone, lo único real es la dirección IP, y eso. En torno a las

empresas, sobre todo algunas relacionadas con la banca, tercerizan la administración de los datos. Por ejemplo, algunos call center que administran información de empresas de telefonía celular y de la banca. Es allí donde hemos visto la falencia porque existe el riesgo de pérdida de los datos. No se trata de que los administren bien o no, sino el riesgo de que mi dato, el que le confío al banco X no me lo administre ese banco con quien yo hice el acuerdo, sino un tercero, con quien yo no tengo ningún tipo de contacto. Esa es la problemática, porque qué puedo exigirle a ese tercero si yo no lo autoricé.

### María Consuelo Franky

Pero precisamente ahí es donde el banco es el responsable y no el tercero. Por eso necesitamos también la ley. Me parece importante el aspecto de prevención, pero me parece que aquí lo fundamental es la penalización, en la medida en que no sabemos en dónde están los datos. Cuando ocurre un delito debe haber una legislación al respecto. En esos casos el banco debe ser el responsable. O en el caso de Facebook pues no podemos penalizar allá la empresa que está por fuera del país, pero sí al usuario que puso un perfil con datos falsos. Tiene que ser punitiva la ley en ese sentido, para evitar los fraudes.

## Javier Díaz Evans

El control de los proveedores y terceros que apoyan las actividades de las organizaciones es un frente de trabajo fundamental en los modelos de control. El acceso, manipulación y tratamiento de datos personales por terceros debe controlarse sin transferir en su totalidad la responsabilidad en ese proveedor. En la actualidad el eslabón más débil en el modelo de seguridad se ha convertido en el proveedor más débil de la cadena de valor de su organización. Con este entendimiento y preocupación en la industria, se está desarrollando la norma ISO 27036 para la protección de la cadena de suministro. Nuestras organizaciones deben garantizar que todo proceso operativo o cadena de valor esté seguro en cada una de las partes o elementos involucrados (sea una actividad, persona, proveedor, entre otros). Ejemplos de esta preocupación se han dado en los últimos meses. Una empresa de seguridad con mucha reputación dedicada al desarrollo de algoritmos criptográficos fue víctima de un ataque estructurado con el cual los atacantes obtuvieron información de propiedad intelectual lo que afectó a varios de sus clientes que quedaron vulnerables en Internet. Debemos tener cuidado con no diluir la responsabilidad de protección de datos aunque tercericemos la operación o entreguemos información sensible.

## Sara Gallardo M.

Editora Revista Sistemas

### *Y en la práctica, ¿eso sí se cumple?*

## Javier Díaz Evans

Realmente no. Las herramientas y servicios de Internet son utilizadas por muchas empresas medianas y pequeñas las cuales firman contratos estándar donde no es posible pedir al proveedor que se cumplan los requerimientos de seguridad propios de cada organización. Cada empresa tiene un nivel de riesgo aceptable, los contratos estándar para unos pueden ser beneficiosos y para otros no. Estandarizar los niveles de riesgo es difícil, porque esto impacta el P y G de las organizaciones. Así que cada empresa debe administrar sus proveedores, su cadena de

suministros. Si voy a estar en la nube, pues lo mínimo es solicitar que se cumplan mis requerimientos de seguridad.

## Jeimy J. Cano

*Esto ha sido un caos benéfico, han ido apareciendo elementos. Y, finalmente el hecho es que la ley viene y las empresas se tienen que preparar. Cuando entró en funcionamiento la circular 052 de 2007, todos los bancos revisaron e hicieron el estudio de cuánto iba a costar la puesta en marcha de la norma y, en ese momento, eso llegaba a dos millones de dólares. Entonces la pregunta es ¿eso va a tener impactos en las organizaciones y van a tener que acudir a las prácticas de seguridad de la información para comenzar a entender cuál es el requerimiento de la ley? Eso va a ser una reacción natural de todo el mercado. Igualmente, en la Academia también hay impacto, particularmente en el desarrollo de software, donde se deberá incluir el concepto de privacidad por diseño. Eso va a ser otro reto, será lo que va a exigir la ley, la protección del dato sensible. Y las personas que están detrás de la tecnología se preguntan ¿cómo esos asuntos se incluyen por diseño? El tema es que la norma va a tener muchos impactos. El primero, a nivel corporativo, porque según la norma quien responde es el que está en el más alto nivel organizacional. Dos, hay que tener un manual de protección de datos personales, oficial, declarado. Tres, los temas de investigaciones judiciales, van a tener otra exigencia que cursar, dado que se trata de un derecho constitucional vía ley estatutaria. Cuatro, el impacto en la Academia sobre cómo se hacen las aplicaciones y qué significa la seguridad por diseño. Y el impacto natural, como lo anota María Fernanda; la norma lo que va a generar es una industria como le ocurrió a España, en el año 1994. En ese entonces en ese país existían sólo dos o tres cursos de seguridad informática. Diez años después, más de 100 posgrados y doctorados, a raíz de la Ley Orgánica de Protección de Datos Personales –LOPD-. Estamos en un momento muy importante en el país, donde*

*va a haber muchos elementos que se van a conjugar; se van a alinear los planetas para que todos comencemos a hablar un único idioma sobre la protección del dato personal, como derecho fundamental del individuo, sea en investigación, empresa, Academia, o en cualquier ámbito. En ese contexto quisiera que dieran su conclusión sobre lo que hemos conversado, para darle cierre al foro.*

### **María Consuelo Franky**

Desde el punto de vista técnico y de la Academia hemos venido enseñando cómo hacer aplicaciones seguras; pero, otra cosa es que lo apliquen en la realidad profesional. Cuando por la nueva ley- se impone el diseño de seguridad desde el principio, las aplicaciones deben contemplar en primera instancia la seguridad. Por ejemplo, el módulo de seguridad es lo primero que debe construirse en una nueva aplicación, más cuando todo hoy en día está relacionado con la web. Pero, uno ve en la práctica que en muchas ocasiones la seguridad se aplica al final del desarrollo de una aplicación. Es decir, están haciendo las cosas al revés. Así que en la Academia tenemos que enfatizar mucho más sobre la manera de hacer estas aplicaciones para la web, y propender porque

los estudiantes una vez se gradúen, estén preparados para trabajar de esa manera.

### **Francisco Rueda**

*¿Qué tantas modificaciones requiere la circular 052, si se quiere introducir esta Ley en su totalidad?*

### **Javier Díaz Evans**

Esta discusión es muy interesante y hemos profundizado el tema en varios foros con expertos en seguridad. La conclusión es que no podemos continuar nuestro día a día y rol de oficiales de seguridad en las organizaciones, esperando a que llegue una nueva ley para desarrollar un nuevo proyecto de varios miles de dólares. Mi posición personal es que la publicación de nuevas leyes no puede seguir impactando a nuestras organizaciones. Los modelos de seguridad se han consolidado, las primeras regulaciones fueron un apoyo para organizarnos y desarrollar muchas iniciativas de la estrategia de seguridad que estaban detenidas por temas de presupuestos. En la actualidad, los proyectos de seguridad ya no se cumplen por norma o por ley, sino son temas transversales dentro de la organización, la alta dirección y junta directiva comprenden que la seguridad



*Javier Díaz Evans (derecha) advirtió sobre la necesidad de que las organizaciones, más allá de la ley, adopten la seguridad como un asunto transversal.*

puede generar valor dentro de las compañías y que una gestión adecuada y uso adecuado de los recursos son directrices claves de la administración y gobierno de seguridad. No nos debería afectar; un impacto mayor a la organización será porque no estaba haciendo la tarea de forma adecuada. La nueva versión de Cobit 5 nos presenta una visión de seguridad de la información más amplia: es un tema transversal, de gobierno, el nivel de seguridad debe tratarse más arriba que solo como un tema técnico u operativo. Creo que nuestra misión y labor como oficiales de seguridad es dejar un poco los temas técnicos, para llevar estos asuntos a un nivel de alta dirección y Junta Directiva en el marco de los objetivos de la organización. La información y los datos son los mismos, pero no existía la claridad sobre la clasificación de datos personales y su protección.

### **Jeimy J. Cano**

*A la fecha se tiene registro de tecnologías novedosas para asegurar datos clasificados, las cuales hablan de almacenamiento cifrado, control de acceso vía hardware con pin de autenticación para discos externos y USB, los cuales representan una oportunidad para el almacenamiento y transporte de información clasificada disminuyendo los riesgos propios de los datos en movimiento. Los proyectos de DLP – Data Lost Prevention-, son otra alter-nativa para el control de la información sensible en las empresas, la cual exige de la organización una práctica de clasificación informacion base claramente asegurada en sus procesos.*

### **Javier Díaz Evans**

Hace algunos años asesorando a un nuevo banco que iniciaba operaciones en Colombia, un auditor de la Superintendencia Financiera, realizando una revisión del cumplimiento de la Circular Externa 052, solicitaba protección de borrado seguro automático cuando se transportaban datos personales en dispositivos móviles, dicho control podía ser complejo debido a que en esa época, aproximadamente unos 5 años, los datos móviles y el control centralizado de dichos dispositivos no era una solución econó-micamente viable. El interés

de proteger los datos personales lleva varios años, esa protección requiere de recursos y de una directriz propia de la organización, la cual puede ser una iniciativa propia de la organización o reforzada con una ley como la que hemos discutido el día de hoy. Esperemos que las organizaciones entiendan que es un tema que nos interesa a todos.

### **María Fernanda Guerrero**

El binomio para mí es seguridad-libertad, el concepto de seguridad implica dos caras. La seguridad que impida la intromisión abusiva, pero también la libertad positiva, hacer las cosas. La fuerza del mercado y de las empresas debe tener de frente la fuerza de los derechos. En la medida en que conozcamos perfectamente tales conceptos, tal vez podamos vivir en una forma más armónica frente a los desarrollos tecnológicos y los demás asuntos relacionados.

### **César Villamizar**

El juego que damos nosotros desde el punto de vista de policía administrativa y de investigación o judicial es bastante significativo en los asuntos que entran a regir por el legislador. Debemos estar de parte de la seguridad como un principio fundamental de nuestra institución hacia los fines esenciales del Estado, pero también debemos garantizar esa privacidad como principio fundamental. Es decir, también nos tenemos que someter como empresa al tratamiento de los datos personales, porque de hecho nosotros somos administradores de los mismos. Así que lo importante es alinearnos con la ley y la jurisprudencia y, antes que todo, entender conceptos jurídicos como son el hábeas data, la intimidad y el derecho al buen nombre y a la información, puesto que son asuntos diferentes.

Son tres autopistas que no se tocan, pero las tres apuntan a lo mismo, hacia la buena administración de los datos personales. Entonces desde la visión de la Policía Judicial es muy importante que las empresas que estén quedadas se pongan al día muy rápido. Para nosotros sería una garantía, porque nos van a certificar los datos que requerimos en las investigaciones, ya no serán erróneos. El



*Jaime Eduardo Santos planteó nuevas formas de acercamiento a la problemática de la información y la seguridad.*

camino será más expedito y tendremos la confianza sobre los datos personales, desde el punto de vista de la acción penal, porque nos ayudan en esa persecución del que está administrando mal los datos personales, es decir los delincuentes. Lo que quiere decir que cerraremos esa brecha al delito.

### **Jaime Eduardo Santos**

Entiendo que para mis compañeros de foro el

concepto de caos de la termodinámica no es trasladable para el tratamiento del dato, pero asumí el riesgo de argumentarlo en un foro de ACIS que da el ambiente ideal para incluir nuevas formas de acercamiento a la problemática de la información y la seguridad. Sin embargo, como tesis alternativa propongo diseñar un sistema de riesgo de la información y dentro de ese SARI seguir el ISO 27001, Cobi u otro modelo similar, pues siempre contribuirán a conservar el orden deseado. 🏠

**Sara Gallardo M.** Periodista comunicadora, universidad Jorge Tadeo Lozano. Ha sido directora de las revistas “Uno y Cero”, “Gestión Gerencial” y “Acuc Noticias”. Editora de Aló Computadores del diario El Tiempo. Redactora en las revistas Cambio 16, Cambio y Clase Empresarial. Ha sido corresponsal de la revista Infochannel de México y de los diarios “La Prensa” de Panamá y “La Prensa Gráfica” de El Salvador. Autora del libro “Lo que cuesta el abuso del poder”. Investigadora en publicaciones culturales. Fue gerente de Comunicaciones y Servicio al Comensal en Andrés Carne de Res. Es corresponsal de la revista IN de Lanchile y editora de esta publicación.