**Ciudad de México, 30 de enero de 2020.**

**Versión estenográfica del Panel 1: “Cooperación Internacional y Protección de Datos en el Ámbito Judicial y Policial”.**

**Presentador:** Les informamos a los asistentes que a través del Código QR pueden tener acceso a las semblanzas y programas del Foro.

El Código QR se encuentra en los banners que se encuentran en la entrada del Auditorio y la mesa de registro.

Para iniciar, cedemos el uso del micrófono a la maestra Elsa Bibiana Peralta Hernández, Comisionada Ciudadana del INFO, quien moderará este Panel.

Cedemos el uso de la palabra a la maestra Elsa Bibiana Peralta Hernández, Comisionada Ciudadana del INFO, quien moderará este Panel.

**Mtra. Elsa Bibiana Peralta Hernández:** Se vale aplaudir.

Muchas gracias a todos.

Me da mucho gusto que permanezcan y que bueno, ahorita se van a ir incorporando las demás personas que ya saben ustedes, una disculpa, como siempre, porque el tema de la inauguración siempre desfasa un poco los tiempos, pero nos vamos a ir acoplando.

Doy nuevamente la bienvenida a todos los que se están incorporando. Muchas gracias por el interés mostrado para llevar a cabo este Panel.

Y vamos a iniciar con el Panel número 1, que se llama “Cooperación Internacional y Protección de Datos en el Ámbito Judicial”.

La dinámica es la siguiente: Expondrán quienes me acompañan y a quienes presento, que es Juan Pablo Olmedo, Director de la Fundación Pro Acceso, de Chile.

Bienvenido, Juan Pablo.

Al doctor Nelson Remolina Angarita, Director de la Delegatura de Protección de Datos, Superintendencia de Industria y Comercio de Colombia.

Bienvenido, Nelson. Muchas gracias.

Y a José Álvaro Quiroga León, experto en privacidad, Asesor del Defensor del Pueblo y ex Director de la Autoridad Nacional de Protección de Datos del Perú.

Muchas gracias, Álvaro.

Todos ellos, como bien dijo mi Presidente, ya viejos conocidos en el tema y me place mucho que estén nuevamente aquí en México con la experiencia y en las nuevas trincheras en las que se están desarrollando.

Muchas gracias, porque de todas maneras su experiencia los lleva por todos estos caminos en los que siguen recopilando experiencia para venir a compartirla con todos nosotros.

La dinámica será la siguiente: Yo pongo una alarma que les avisa del tiempo que ya acordamos que van a exponer y cuando suena esta alarmita quiere decir no cortan de inmediato, quiere decir que ya pueden ir cerrando, solamente les queda un minutito para concluir el tiempo establecido.

Al final, si nos permiten, si el tiempo lo permite, habrá un cierre de ideas, igual por uno o dos minutos cuando mucho.

Y para que ellos tengan el tiempo suficiente para exponer no vamos a leer sus reseñas, igual y aparecerán en la pantalla y también irán apareciendo las ponencias que ellos también prepararon para ustedes, pero les pedimos que todos, todos recibieron un gafete como éste, ¿verdad?

**Coro:** No.

**Mtra. Elsa Bibiana Peralta Hernández:** Entonces tienen que ir por él, porque qué creen, que si no se van a perder toda la información.

Con su teléfono celular ubican la cámara en este código QR y al ubicar la cámara ahí los millenials seguramente sí ya lo hicieron, todos los que no somos millennials decimos “y ese garabato para qué es”.

Entonces va a aparecer ahí una página, en el momento que la cámara lo detecta aparece una página, le pican en esa página y se despliega, se los voy a poner de ejemplo.

Cuando le pican, aparece esta página. Es una bienvenida y después de esa bienvenida tienen ustedes aquí un menú donde aparece el programa, a quién pueden contactar en caso de cualquier tema que quieran tratar, aparecen todas las reseñas curriculares de los ponentes y todo lo relativo al evento. Ahí le pican en cada uno.

Por ejemplo, en ponentes y aparecen las fichas de todos los ponentes. Y así ustedes pueden leerlas, conservarlas inclusive y el dato del contacto, por si alguien también desea contactarlos para cualquier tema, circunstancia o demás.

Así está funcionando para evitarnos papel y estamos hablando de tecnología, ¿no? Pues ocupémosla.

Entonces esto es algo muy sencillo, la verdad no es nada del otro mundo, pero aquí tienen todos ustedes la información relativa a todo el evento, ya está cargada en este portalito.

Y entonces por eso me tomé el tiempo para explicarlo, porque me estaban preguntando que dónde estaba el programa, que dónde estaban las fichas, que dónde estaba todo; está ahí.

Quienes no tienen su gafetito, pues ahorita que terminemos este Panel vayan por su gafete respectivo para que puedan desplegar toda la información.

Entonces esa será la dinámica en todas las mesas para que inmediatamente revisen los ponentes de la siguiente mesa y estén informados ustedes también.

En ese tenor voy a darles nuevamente la bienvenida a todos y voy a ceder el uso de la voz hasta por 15 minutos a quien inicia esta mañana, y me place mucho darle nuevamente la bienvenida a Juan Pablo Olmedo, Director de la Fundación Pro Acceso, de Chile, para que nos haga su exposición.

Un fuerte aplauso, por favor, y bienvenido, Juan Pablo.

No tenemos pantalla, ¿qué pasa? No tenemos luz, estamos muy oscuros aquí, por favor, tecnologías, logística.

Gracias.

**Mtro. Juan Pablo Olmedo:** Buenos días.

Esa va a ser la única lámina que vamos a plantear, espero que se vea durante el transcurso, pero es una noticia que salió el día de ayer en el diario El Mercurio, en Santiago, y que da cuenta de un caso, de una resolución del Consejo para la Transparencia de Chile del día 23 de enero reciente.

Por lo tanto, estamos hablando de contingencia y de un escenario que en materia de cooperación policial y rendición de cuentas que el foro o el foco de este Panel parece más que relevante.

Quisiera agradecer, primero que nada, por cierto, a la Unión Europea y al Instituto por la gentil invitación a poder estar con ustedes; a Elsa en particular, por su compromiso y por su iniciativa. Y con eso empezar.

Algunos de ustedes me imagino, por lo menos la mayoría hemos visto la película de Harry Potter, alguna de sus versiones, y en un tema como éste hay una imagen que me hace mucho sentido de sacarse un pelo del cabello, ponerlo en una bolsa de agua y poder ver la memoria y la historia, y reconstituirla.

En Derecho Internacional y en la evolución del cambio social, muchas veces sucede así. Hay que mezclar algunos pequeños puntos en distintas maneras, ponerlos en algunos espacios juntos y desde ahí evoluciona.

Y creo que estamos en la materia en que nos estamos desarrollando en ese tipo de escenarios, como continuaciones, pero planteándolo.

Esta idea obviamente recoge una experiencia acumulada ya durante bastante tiempo, como representante de la sociedad civil, a través de esta Fundación que presido, pero también como Primer Presidente del Consejo para la Transparencia en Chile, como asesor parlamentario y hasta hace pocos días, yo diría hasta el 31 de diciembre del año pasado, como miembro del Gabinete del Ministro de Justicia del gobierno del Presidente Sebastián Piñera, precisamente en la formulación de las políticas públicas del sector.

Y en particular también, en mi condición de abogado del señor Carlos Cardoen, que es esta noticia que aparece ahí, sobre quien pesa una alerta roja vigente desde año 1993, y que ha sido en marzo del año 2019 extendida nuevamente por la Secretaría General de INTERPOL hasta el año 2024.

Esta experiencia ya desde el año 2017 que estoy en un proceso contencioso como abogado defensor en contra de INTERPOL, me ha permitido un conocimiento de lo que son las instancias de autorregulación que dicha institución hoy día se ha dado.

Y tengo que desde aquí, ya desde este pódium, señalar que Latinoamérica tiene aún escasa experiencia en lo que significa la defensa de los derechos a los datos personales por parte de la comunidad policial.

El momento en que se desarrolla este Panel resulta muy oportuno y créanme que la alegría que me provoca poder conversar y compartir con ustedes en esta ocasión como hombre libre y no como funcionario público, me permite también desarrollar con mayor tranquilidad algunas cosas que veo, que miro con tristeza, con preocupación, pero también con esperanza.

Latinoamérica se encuentra sometida a una tensión institucional democrática, que tiene un alcance generacional y un incierto futuro.

La respuesta de las inquietudes de la transición democrática de la década de los 90 ya ha sido superada, es la década que a nosotros nos tocó trabajar.

El populismo acecha y nuestros gobiernos se enfrentan con una profunda desconfianza ciudadana, que se expande a toda la región y alcanza también a las organizaciones internacionales.

Entre los fenómenos que explican la fragilidad social, se reconoce por cierto la corrupción, las incumplidas promesas de equidad de ingreso y educación de nuestras poblaciones y décadas de postergación de respeto a derechos humanos de grupos sociales desprotegidos, como son las mujeres, los pueblos originarios, los migrantes, entre otros.

En este marco, los países de la OEA, a través de la Cumbre Iberoamericana de Presidentes, a través del Banco Interamericano de Desarrollo y recientemente a través de la Comisión Interamericana de Derechos Humanos, han ido dando cuenta de los desafíos de gobernabilidad que nuestro hemisferio requiere, particularmente en ámbitos de generación de información y rendición de cuentas.

No me voy a extender más sobre estos puntos, porque me parece que nos alejan del Panel, pero sí es un marco de referencia, de conocimiento de que hay interés en la región, hay preocupación, hay conocimiento, hay documentación, lo que nos falta ahora es capacidad de implementación y articulación.

Algo sobre INTERPOL y la alerta roja, que son los temas sobre los cuales me voy a referir en particular como espacios donde creo que se requiere intervención importante para la cooperación policial efectiva, coherente, con el respeto a los derechos humanos y a los principios que emanan de la protección de los datos personales.

La comunidad policial regional e internacional se ha visto sobrepasada, sino también comprometida y envuelta también en situaciones del uso abusivo de la fuerza y también de violación a los derechos humanos. Es un hecho de la causa.

En función de los cometidos de generar una reflexión sobre cómo superar y fortalecer la cooperación y la protección de los datos en el ámbito judicial y policial, me parece que una vía de entrada dentro de muchos es referirse a los mecanismos e instrumentos de cooperación policial de INTERPOL y particularmente uno, que se denomina alerta roja.

Me parece que el sentido con el que pretendo abordar este tema no es la del abogado defensor, por cierto, que este es un caso particular, sino más bien con un sentido constructivo, de formulación de política pública y de cooperación regional.

Acá lo primero que tenemos que recordar es que INTERPOL es, para aquellos que no lo conocen, es una comunidad internacional de policías, que nace en el año de 1946; INTERPOL es una comunidad de policías que se fundamenta en acuerdos nacionales para los efectos de cooperación policial.

Durante los años INTERPOL ha llegado a ser reconocida como una organización internacional per se y, por lo tanto, con todo el régimen de inmunidades, de jurisdicción y de alcance que se dan para ese tipo de organizaciones.

En particular en materia de protección de datos, INTERPOL ha revitalizado durante los últimos años los reglamentos sobre protección de datos personales y también un Estatuto de lo que se denomina la Comisión de Ficheros.

La Comisión de Ficheros es el órgano encargado de evaluar, es un mecanismo de autorregulación, de evaluar la idoneidad de los datos que están contenidos en el sistema de información de alerta roja de la institución.

La definición de alerta roja aquí resulta importante para poder guardar información, es una solicitud que hace un Estado miembro a la comunidad policial para buscar, identificar y arrestar a una persona que ha sido solicitada por la jurisdicción nacional o un tribunal internacional con miras a su extradición.

Su fundamento es la orden de arresto o una orden judicial estimada por las autoridades judiciales del país requirente.

El tratamiento que lleva a efecto INTERPOL se lleva en el marco de un sistema de información, que es administrado por la institución sin que esta base pertenezca al dominio de las oficinas nacionales.

INTERPOL básicamente lo que hace es: La policía tiene una unidad, que es la Unidad de INTERPOL. Esa unidad es la que presenta a la organización una solicitud de alerta roja y es puesta en circulación al interior de toda la comunidad policial.

Pero esa información no pertenece a ninguna de las oficinas locales, sino que pertenece como sistema a la organización en general.

INTERPOL ha sostenido y sostiene en tribunales y a nivel internacional la confidencialidad y la titularidad de los datos que están dentro de este sistema, porque en caso de divulgarse generaría un perjuicio a las relaciones internacionales de los países que intervienen a la organización internacional, pudiendo causarse incluso un daño a las relaciones internacionales y a los intereses generales de los países miembros, o sea, el estado del arte hoy día es que esta información que se entrega en este sistema de información de alertas rojas, primero no pertenece a los Estados, pertenece a INTERPOL y respecto del cual INTERPOL alega la confidencialidad del mismo.

¿Fundado en qué? Una causal de reserva más que legítima, por cierto, que es las relaciones internacionales entre los países miembros.

¿Cuál es la importancia de esto?

La práctica internacional hoy lleva a anotar un aumento sustantivo en el uso de la alerta roja, entre el año 2005 y 2015 el número anual de notificaciones de alerta roja aumentó casi cinco veces; de 2 mil 343 a 11 mil 492.

Sólo el año 2016 un total de 12 mil 787 alertas rojas fueron emitidas, o sea, la tendencia al alza es brutal.

La Oficina de Asuntos Jurídicos de INTERPOL, yo digo hoy día con claridad, pero llegar a saber qué es la Oficina de Asuntos Jurídicos de INTERPOL les aseguro que les va a llevar dos años, o sea, la página web de INTERPOL para los efectos del estudio profesional que permita identificar posiciones, cargo y procedimiento les diré que es un desafío mayor.

Pero yo me siento cómodo con INTERPOL, ya lo conozco y creo que ellos también, hemos ido estableciendo una relación a la distancia y silenciosa con ellos.

Pero la Oficina ha considerado que no se puede revelar ninguna correspondencia realizada a través de los canales de INTERPOL, toda vez que esa información o entrega supondría una brecha de las obligaciones de confidencialidad a las que están sujetas las Oficinas Centrales Nacionales de INTERPOL, que generalmente es la policía de cada uno de nuestros países, y señala existe la posibilidad sin coste alguno, o sea, gratuitamente, de concurrir a la Comisión de Ficheros, que es un organismo independiente que se ocupa de las solicitudes de acuerdo a las normativas de INTERPOL.

Yo he citado hace un momento atrás los dos documentos matrices, a eso se suma el Estatuto y otros más, pero yo me debería invitarlos a la lectura de ambos documentos, es decir, el Reglamento de Datos Personales y el Estatuto del Reglamento de la Comisión de Ficheros, y lo cierto es que más allá de las maestrías, los doctorados, la capacidad mental, es muy difícil entender lo que dice, es muy complejo.

Entonces realmente están hechos en su configuración para generar mayor burocracia y burocracia que no ayuda al ciudadano, sino burocracia que fortalece la política institucional.

Y de hecho sorprende la aseveración de la independencia del Comité de la Comisión de Ficheros, a la cual les tengo el mayor respeto, pero ellos no es tal, porque toda la decisión de gestión de INTERPOL hoy pasa por el Secretario General de INTERPOL. Esa es la autoridad final que decide respecto de lo que estamos planteando hoy día, el destino de un fichero determinado.

¿Cuál es la práctica de INTERPOL? Y aquí esto es bueno hacerlo en este Foro, porque por primera vez me permite hacer una denuncia pública.

El artículo 2º del Estatuto de INTERPOL establece que el mandato de INTERPOL es garantizar y promover la asistencia mutua más amplia posible entre todas las autoridades de la policía criminal dentro de los límites existentes en los diferentes países y en el espíritu de la Declaración Universal de Derechos Humanos. Ahí está, el marco de INTERPOL debe basarse en ese espíritu.

INTERPOL con todo, en su actual estructura carece de mecanismos efectivos para la revisión sustantiva de la justificación de las solicitudes de notificación roja, tanto en términos de su adecuación a las normas del debido proceso como también del escrutinio de motivación política de dicha solicitud.

Siendo una organización que convoca a las policías, ha estado fuera del alcance de las innovaciones de fortalecimiento democrático, de transparencia y de acceso a información pública que se ha desarrollado en nuestros países y en el hemisferio durante los últimos años.

¿Esa es la alarma? Ay, qué lástima.

Bien, con su respeto entonces, me voy a permitir, a propósito de una denuncia pública para no limitar al denunciante, su autorización para pedir dos minutos más en esta línea.

Pero lo que estoy señalando tiene ya a esta altura un piso de fortalecimiento y de información fidedigna.

La Asamblea Reglamentaria del Consejo de Europa, el Parlamento Europeo y el Senado de Chile durante los últimos dos años, han emitido sendos informes donde han constatado el uso abusivo del sistema de alerta roja por parte de INTERPOL. Y requiere rectificación.

Entonces dicho eso, esa es la denuncia, ¿cuál es la salida, cuál es el camino?

Aquí me gustaría proponer en ésta dos reflexiones, la primera de política pública y la segunda derechos fundamentales.

Latinoamérica hoy día cuenta con dos redes bastante interesantes y que están subdesarrolladas, desde el punto de vista del acceso a la información y la transparencia, este Instituto adhiere a la Red de Transparencia y Acceso a la Información en Latinoamérica, que aglutina a todos los órganos de acceso a información y transparencia.

Tuve el privilegio en mi Presidencia, hace varios años atrás, en el Consejo de la Transparencia de dar los primeros pasos de esa Red junto con -en esa época- el IFAI.

Y esa Red es una Red de intercambio interesante, pero que se mira hacia adentro, no es una Red que haya salido.

Por otra parte, el año 2006 INTERPOL instaló lo que se llama AMERIPOL. AMERIPOL es una organización de policías latinoamericanos que tienen también similares objetivos de cooperación e intercambios de información interna.

A mí me parece hoy día, a propósito de este Panel del interés del diagnóstico, que los institutos de transparencia latinoamericanos tienen algo que decir, tanto es así que si se pudiera leer esa noticia lo que aparecería ahí es que el Consejo de la Transparencia en Chile el 23 de enero ordenó de oficio, de oficio tomó la iniciativa para pedirle a la Oficina Nacional de Chile que, a su vez, le pidiera a la Secretaría Internacional de INTERPOL información respecto de la ficha que estamos hablando de este señor Carlos Cardoen, que se encuentra desde el año de 1993 con una alerta roja.

Eso es inédito, eso inédito en la región y me atrevería también inédito en Europa. La iniciativa de un órgano de transparencia de requerir información.

De modo tal que a mí me parece acá que hay una oportunidad, sobre todo teniendo presente los espacios de la Unión Europea, la Comisión Interamericana, el Banco Interamericano, todos los otros actores que están involucrados para efectivamente generar un diálogo que es denominado transparencia policial, que eso es además muy lindo, el cambio, a propósito de las tecnologías, transparencia policial de modo de utilizar una conversación entre la policía organizada en sus redes con las entidades de transparencia.

Bueno, ¿el objetivo cuál es? De generar mejoras en la rendición de cuenta institucional. Eso me parece que hoy día sería un aporte y me parece que a lo menos aquello hoy día que está en proceso o en posición de toma de decisiones, me atrevería respetuosamente a pedirles que lo consideraran.

Y, en segundo término, desde la perspectiva del derecho de acceso de los derechos fundamentales, rescatar también un reciente aporte de la OEA. La OEA tiene una Unidad de Estudio que se denomina el Comité Jurídico Interamericano.

El Comité Jurídico Interamericano hizo un análisis ahora reciente sobre la reactivación de las inmunidades diplomáticas y analizó todos los Estatutos de las organizaciones internacionales, incluida aquellas como INTERPOL que se fundan en el acuerdo sede.

Y da a entender de que efectivamente hoy día no tenemos una norma internacional que pueda obligar a los órganos internacionales a rendir cuentas o eventualmente a solicitudes de acceso a información, pero sí en sus conclusiones hay un paso adelante y dice “mire, no tendremos norma, pero hoy día a nivel internacional las organizaciones internacionales deben comparecer frente a demandas de acceso a la justicia en los territorios locales”, obligación de comparecer.

Y eso es lo interesante y eso es lo que está acá, porque el Consejo de la Transparencia lo que ha hecho mediante esta solicitud, a través de la FDI chilena, a INTERPOL es decirle a la Secretaría General “señores, ustedes tienen que comparecer, a dar cuenta de esos dichos”.

Y qué mejor espacio para comparecer en esta materia que precisamente a través de los órganos de acceso a la información y protección de datos personales, es decir, aquí, y aprovechando que viene mi colega de Protección de Datos Personales en Colombia le hago el punto, porque yo creo que hay que revisar los acuerdos sede de INTERPOL con cada uno de nuestros países para efectos de generar un adendum, una rectificatoria, algún mecanismo que permita en casos como los que estoy planteando, una alerta roja vigente por más de 26 años, pueda eventualmente colaborar con INTERPOL.

Y esa sí fue la señal de término para efecto de poder dar pronta solución.

Me quedó claro su mensaje y cómo vuela en la energía en este evento.

Yo con esto termino, espero que haya sido claro, muy contento de estar con ustedes y de poder presentar una denuncia pública ante toda la comunidad latinoamericana.

INTERPOL, por favor, tranquilos, mis datos están aquí.

Muchas gracias.

**Mtra. Elsa Bibiana Peralta Hernández:** No tengo tanto poder mental, ¿o sí?

No, la idea era “a ver, que tome agua”, pero bueno. Creo que se fue más allá.

Muchas gracias.

Como les decía, escucharlos de verdad el tiempo es poco y ellos tienen mucho qué decir.

Por eso yo también presentare inmediatamente al doctor Nelson Remolina Angarita, Director de la Delegatura de Protección de Datos, Superintendencia de Industria y Comercio de Colombia.

Muchas gracias, Nelson. Tienes la palabra.

Gracias.

¿Tienes presentación? A ver, pedimos a Tecnología si ya resolvieron sus problemas técnicos.

No se ve la pantalla, entonces a ver qué podemos hacer.

¿Ya, ya se ve?

Me encanta que paradójicamente que estamos hablando de tecnología, sea la tecnología la que precisamente falle.

Pero como atrás de la tecnología hay personas; bueno, ya sabemos quiénes son y a quiénes vamos a extrañar.

Gracias.

**Dr. Nelson Remolina Angarita:** Bueno, muy buenos días.

Me da mucho gusto estar acá y ustedes saben, para mí siempre ha sido un honor venir a México, de manera que agradezco la invitación.

Maestra Bibiano, desde luego mi reconocimiento por hacer no sólo este evento, sino por toda su gestión que ha hecho, liderando estos temas no sólo en México, sino fuera del país; de manera que la felicito por eso y a todo su equipo le agradezco por todo el esfuerzo que han hecho para que estemos acá, para compartir algunas ideas.

Yo voy a plantear este tema, ustedes lo ven en la presentación, pero voy a referirme a algunos temas que me parecen centrales.

Al final de la presentación van a encontrar como 10 o 12 referencias bibliográficas, y ahí está en mayor detalle de lo que quiero decirles, pero voy a centrarme quizá en lo que en mi opinión podrían ser los grandes mensajes o por lo menos los más importantes, no todos desde luego, pero vamos a ver.

Lo primero es que estamos hablando de cooperación internacional y hay que mirar el mundo en que estamos, porque hoy estamos y tenemos que hablar necesariamente del ciberespacio. Y en el ciberespacio, pues también hay ciberdelincuencia.

Las regulaciones de protección de datos, inicialmente, cuando uno mira los principios de la OCDE de los años 80, entre otras cosas se hicieron para permitir el flujo transfronterizo de información.

La información, como ustedes miraron o ya lo saben, hoy en día es determinante de muchas actividades. La economía se mueve en la información, la gestión pública se mueve a partir de información, pero los derechos humanos también depende de lo que se haga con nuestra información.

Entonces ahí hay muchos intereses legítimos, válidos, cruciales en cualquier sistema democrático que hay que mantener y respetar.

Este mapa que ustedes ven ahí es simplemente una referencia para algo que tengan presente. El mundo no siempre fue así, pero sí ha habido una exclusión normativa de normas sobre protección de datos que pone, entre otras del presente, la relevancia de lo que significa los datos en la sociedad, pero también cómo si esos datos no se tratan debidamente, pues cómo pueden afectar los derechos de las personas; derechos que van desde su buen nombre, pero también intimidad y en algunos casos su libertad e incluso hasta la vida misma.

Entonces en un sistema democrático, ustedes muy bien saben, un aspecto fundamental es el respeto de los derechos humanos, pero también lo es combatir la delincuencia, también lo es el sistema de justicia. Y la información allí es crucial, determinante.

Ustedes ven ya que básicamente el 62 por ciento de los países del mundo tienen normas generales de protección de datos, insisto, eso pone de antecedente lo que les planteo, la evidencia de este derecho que para mí es el derecho del siglo XXI, entre otros, por otro tema que ustedes ven ahí, ya en el mundo hay 84 autoridades de protección de datos.

Yo siempre pregunto: ¿Ustedes conocen otro derecho que desde su concepción se creó pensando en que para protegerlo es necesaria una autoridad especializada? ¿En los otros derechos existe?

Bueno, la respuesta, no es un quest, pero la dejo para que la estudien, pero ese es un derecho, insisto, que se crearon autoridades especiales sólo para ello. Y eso también pone de precedente lo que he tratado de mencionar, la relevancia de que la información de todos y cada uno de nosotros, de los que estamos acá y los que no están acá, se trate debidamente tanto en el sector privado como en el sector público, tanto por parte de las autoridades del Poder Judicial como la policía y demás partes u órganos del Estado.

Y otro tema aquí importante para tener y no perder de vista, por eso hago presente o pongo de precedente la realidad sociotecnológica de este siglo.

Fíjense, ya casi 60 por ciento de la población mundial tiene acceso a internet; digamos, somos los ciberciudadanos. Si a un Estado dentro de su territorio le es muy complejo poner las cosas en orden, que funcionen, el sistema de investigación, por ejemplo, el sistema de justicia, piénsese ahora en un territorio como el que estamos viviendo en el ciberespacio, que es global y transfronterizo y que habitan allí más de 4 mil 400 millones de personas.

Entonces los retos que tienen los Estados son enormes, porque muchos pensemos en el tema de la ciberdelincuencia, muchos delitos que pueden estar afectando a ciudadanos mexicanos seguramente se están haciendo no desde el territorio mexicano, sino desde otra parte del mundo.

Y por eso es necesaria la cooperación y el flujo de información, y creo que sobre eso no hay duda de la necesidad, el tema no es el qué se quiere, sino el cómo se hace. Y ahí es muy importante eso para tenerlo presente.

Y cuando uno mira este tema de cooperación en el ámbito judicial y policial, pues reitero, no creo que haya dudas de la necesidad, de la importancia, pero también de que no se haga de cualquier manera.

Si bien los ciberdelincuentes sí hacen las cosas de cualquier manera, las autoridades democráticas y legítimas no pueden hacerlo, eso es parte de las reglas de juego de una sociedad.

Y la idea, no quiere decir que lo estén haciendo, a mí no me consta, pero la idea es siempre hacer las cosas de manera correcta. Y esto va con algo de mi último slide cuando acabe, aquí finalmente estamos en un concepto no sólo de legitimidad jurídica, sino de confianza; confianza de los ciudadanos por sus instituciones, confianza de los ciudadanos por las organizaciones respecto el tratamiento de datos, y un buen tratamiento de datos genera confianza. No es lo único, pero genera confianza. Y ustedes saben que confianza es la percepción que tienen sobre una entidad.

Entonces el gran reto que tenemos ahí es hacer las cosas bien para que ello, pues la confianza se incremente y las cosas funcionen, me parece, mejor.

Ahora, cuando uno habla de las reglas de protección de datos, pues hay muchas, en el mundo ustedes ven 119 normas generales y además de las sectoriales, pero uno podría decir “eso se limita en últimas a unos grandes principios muy básicos”.

Primero, legalidad, o sea, simplemente no se pueden hacer las cosas como uno quiere, no se puede captar información de manera fraudulenta o engañosa; bueno, sin duda.

Pero hay uno, por ejemplo, que pongo a colación con casos y casos, el de la calidad de información. En Colombia un caso, Corte Constitucional T310 de 2003, ahí se pone de precedente cómo un ciudadano fue capturado 20 veces porque el sistema de información que tiene la policía no está actualizado; 20 veces, o sea, ya uno, ni la mamá le cree que uno no tiene un problema, que el problema es de la mala administración en ese caso, por favor, de la calidad de la información.

Por favor, es así de sencillo, aquí también en todas las organizaciones hay seres humanos y necesitamos personas que en esto sean muy diligentes, porque no actualizar simplemente un dato, implica detener a una persona, su libertad. Así de sencillo.

Y ahí hay que mirar algo muy importante también, si estamos hablando de información no es de cualquier calidad de información, sino información veraz, imparcial que esté actualizado.

Y ahí la gran diferencia es si tenemos grandes bases de datos o grandes basureros de datos. Y eso hay que tenerlo claro, porque si vamos a tomar decisiones en el sector de policía y judicial con información, insumos que no son de calidad, que no se actualicen, pues de pronto las decisiones no son las mejores y afectan los derechos de la gente.

Principio de finalidad y pasó muy rápidamente; claro, no podemos obtener la información de cualquier manera ni utilizarla para cualquier cosa. Todas las autoridades, yo soy un servidor público, pues tenemos que obedecer la Constitución y la ley, y entonces tenemos que mirar qué nos permite hacer la regulación en esos casos a las autoridades para “X” o “Y” cosas.

Entonces es muy importante no sólo la circulación de la información per se, sino para unos fines concretos y crear límites para que esa información no se use más allá de lo que inicialmente se informó o de lo que permite la ley. Y fíjense que todo detrás de esto va la conducta humana.

La doctora Bibiana mencionaba una palabra fundamental dentro de las tantas en su intervención: Ética.

Acá quien quiere hacer trampa sin que nadie se dé cuenta, lo puede hacer.

¿Quién controla la conducta humana, quién controla a las personas que tienen nuestra información?

Usted puede leerse las políticas de información perfectas, brillantes en el texto, pero hay que mirar en la práctica qué está sucediendo. Y es ahí donde están los grandes retos.

La debida protección de datos no es tanto en una excelente política, que muchas veces ya es copia, copy paste, sino realmente si eso en la práctica, eso que prometen decir se está haciendo. Eso es un tema también que tiene que ver mucho con ese aspecto.

La seguridad de la información, esos grandes sistemas de información realmente hay controles para evitar, por ejemplo, no sólo alteraciones, modificaciones o destrucción de la información, sino usos indebidos.

Los principios de seguridad normalmente en el mundo hablan de uso indebido. Y ahí estamos, porque el tema no es tener el tema de poder tener datos, sino de abusar de tener esos datos.

Y ahí es algo que por el momento es la preocupación, ¿qué están haciendo las autoridades con nuestros datos, efectivamente están haciendo sólo lo que permite la ley o no? Y ahí ya es un abuso del poder informático que se tiene.

Y vuelvo al tema, esto es ético, esto es humano. Y ahí es donde hay que trabajar mucho más en la gente como tal.

Acá paso a algo que seguramente; bueno, espero se vea mejor, ahí está, el mensaje es lo importante. Un principio de hace rato, pero que cada vez cobra mucha relevancia es accountability o responsabilidad demostrada o demostrable. Eso obliga a todas las entidades público-privadas a adoptar medidas, pero no cualquier medida, sino medidas útiles, oportunas, verificables y demostrables para hacer cumplir las normas, entre otras, de datos.

Y esa es una reflexión interna que debe mirar cada organización: ¿Lo que estamos haciendo es útil, es pertinente, eso sí sirve para cumplir la norma, estamos haciendo monitoreo de lo que estamos implementando para que en la práctica efectivamente eso funcione, sí o no?

Y eso es accountability o responsabilidad demostrada. Aquí no basta hacer las cosas, sino demostrar que las hicimos, pero no cualquier cosa. Entonces ahí es clave.

Yo insisto mucho en el factor humano, hay que entrenar, capacitar mucho a la gente. Si las personas no saben la importancia de la información que tienen y que si hacen cosas indebidas pueden afectar derechos humanos, seguramente no darán la relevancia que el tema merece. Y ahí hay que hacer grandes esfuerzos.

Y ya para esto simplemente voy acá terminando con lo siguiente: La vida es una sucesión de riesgos, uno hasta dormido asume riesgos, ¿sí o no? Y en tratamiento de datos siempre va a haber riesgos.

Yo creo que cualquier proyecto que se va a iniciar o gestión que se está realizando o que va a surgir, es siempre importante hacer este tema de establecer: ¿Cuáles son los posibles riesgos que genera nuestra actividad, medir qué tan factible es que pueda suceder o acontecer en la práctica, establecer cómo vamos a controlarlos y en caso en que se nos salga de las manos cómo vamos a actuar ahí?

Pero aquí en esto hay que trabajar netamente con un enfoque preventivo-proactivo, para evitar precisamente la violación de los derechos humanos por indebido tratamiento de datos.

Entonces estos sistemas de administración de riesgo en tratamiento de datos es un ejercicio permanente que deben de estar haciendo los responsables del tratamiento en el sector público y privado para precisamente, a partir de una gestión consciente de riesgos, pues adoptemos las mejores medidas para evitar que esos riesgos se vuelvan una realidad, se materialicen y afecten derechos de las personas. Ese es de pronto uno de los grandes mensajes que podría darse.

Y, finalmente, termino con éste que les comenté: Yo creo que a veces la gente se preocupa mucho por quién tiene nuestros datos, y creo que ahí hay una crisis de confianza. Y la confianza se gana haciendo bien las cosas. La confianza no es sólo decir que voy a hacer algo, sino hacerlo en la práctica.

Yo creo que ustedes como ciudadanos, y uno lo ve como autoridad, ve muchos textos en papel, pero a veces ve muchas cosas que no son consistentes en la práctica con esas promesas.

Entonces aquí no basta decir “voy a hacer”, sino efectivamente hacer las cosas correctamente.

Yo por ahora dejo esas ideas y muchas gracias a todos. Muy amables.

**Mtra. Elsa Bibiana Peralta Hernández:** Nos quitamos por lo menos para que vieran mejor la presentación, qué bueno, insisto, no sé qué esté pasando con la luz en este lugar.

Gracias.

Esperemos resolverlo en pocos momentos. Gracias.

Enseguida cedo el uso de la voz a José Álvaro Quiroga León. Él es experto en privacidad, Asesor del Defensor del Pueblo y ex Director de la Autoridad Nacional de Protección de Datos del Perú.

Muchísimas gracias, Álvaro. Adelante. Gracias.

**Abogado José Álvaro Quiroga León:** Buenas tardes. Muchas gracias.

Es un placer siempre venir a México. La protección de datos, entre otras cosas, me ha dado la posibilidad de conocer esta ciudad; no es la primera vez que estoy acá y siempre es un placer. Muchas gracias por considerarme en condiciones de decir algo sobre este tema.

Cuando me hablaron de este evento, me plantearon la posibilidad de venir a moderar un panel, yo me sentí muy contento porque me creyeran capaz de moderar un panel sobre esta materia y estaba tranquilo.

Luego me plantearon la posibilidad de exponer en este Panel y entonces ya me responsabilicé un poco más, porque sentía que no era un tema con el que yo hubiera tenido mucha cercanía. Eso creía yo.

Y le entré por el lado de la legislación y me di cuenta, hasta ahí, a las dos de la mañana que me levanté con otros ejemplos en la cabeza, de que estaban muy presentes muchas cosas que había tenido en mi experiencia en mi país y que es absolutamente importante.

Eso es lo que vengo a compartir con ustedes, algunas experiencias, algunas nociones básicas y trataré de transmitirlas con algunos ejemplos que me parecen bien interesantes.

Me da muchísimo gusto coincidir con Nelson, que es un maestro en esta materia, sobre una cosa que yo quería decir al principio para poder entendernos en este intercambio de ideas: ¿Qué entiendo yo por protección de datos personales?

Y cuando digo “qué entiendo yo”, me refiero a cómo funciona en mi cabeza como una cosa operativa. Sobre la teoría el maestro tiene los libros que ustedes necesitan leer, pero yo como un abogado que estaba en el litigio y se encontró con la protección de datos casi, casi por azar hace como ocho años, necesitaba una forma operativa de comprender la protección de datos.

Para mí la protección de datos no es otra cosa que una disciplina destinada a identificar y neutralizar los riesgos que ocurren como ocasión del manejo de nuestra información.

Identificar los riesgos e intentar neutralizarlos, eso explica por qué es tan transversal; porque nuestra información se maneja en internet, qué duda cabe; en nuestra tarjeta de crédito, qué duda cabe; en nuestra historia clínica. Y ahí pondría 50 ejemplos, ¿no es cierto?

Y en todos esos espacios hay manejo de información que genera riesgos, riesgos ciertos, reales y en algunos casos efectos reales sobre la vida de personas de carne y hueso, y en algunos casos efectos para toda su vida, gente que no puede volver a trabajar por alguna información inconveniente, gente que ve afectada su vida para siempre, porque no se identificaron los riesgos o no se neutralizaron los riesgos del manejo de esa información para otras finalidades que pueden ser buenas, naturales, usuales o lo que fuera, pero que nos afectaron.

Es importante tener esta mirada, porque por lo menos en mi país, y soy consciente de que estoy en el ámbito de una organización que junta transparencia y protección de datos, lo mismo ha ocurrido en mi país, lamentablemente la unión de ambas funciones, transparencia y protección de datos, ha dado como resultado casi, casi la sepultura de la protección de datos.

Pero digo, soy consciente de que estas dos funciones están juntas, pero estoy también un poco harto de escuchar una mirada superficial e infantil de la conexión de estos dos derechos.

Nos vienen diciendo que la protección de datos y la transparencia son dos caras de la misma moneda, dos caras, por supuesto que miran para lados diferentes.

Y nos vienen diciendo que la protección de datos nació y sirve para ponerle límites al derecho al acceso a la información, con lo cual es un enemigo de quienes son activistas por la transparencia. Y eso, desde mi humilde punto de vista, es una mentira que genera muchísimos problemas.

La protección de datos y la transparencia, como yo las concibo, forman parte de un inmenso poliedro, no de una moneda de dos caras. Y en ese poliedro está la transparencia, está el honor, está la reputación, está la imagen, está la libertad de expresión, está la libertad de prensa, está la privacidad, está la intimidad.

Es mucho más complejo que una moneda de dos caras, porque claro, desde esa mirada yo tiro la moneda y cae una cara y esa es la que protejo. No, debo, casi, casi como un cubo de Rubik, encontrar una fórmula para que todos estos derechos coexistan.

La ponderación entre ambos derechos no significa que yo pondere en abstracto, que yo diga “a mí me gusta, yo trabajo, soy activista, me pagan por la transparencia y entonces mi enemigo es la protección de datos”. Eso no es ponderar.

O del otro lado, yo trabajo, me dedico a la protección de datos y entonces mi enemigo es la transparencia, porque ya ponderé que uno es mejor que el otro”. La ponderación se realiza en el caso concreto, para que la persona de carne y hueso que tiene un problema encuentre una solución en la cual todos estos derechos involucrados se hagan un espacio, le permitan pasar al otro, se incomoden un poco, pero que el resultado sea un resultado en el cual el ciudadano encuentre que su sistema jurídico lo escucha y lo atiende.

Con esta mirada lo que tenemos en materia legislativa, y creo que el Perú no es único cuando señala cosas como las que voy a decir ahora, la ley peruana excluyó de su ámbito de aplicación los bancos de datos contenidos o destinados a ser contenidos… Perdón, exceptuó los datos de su ámbito de aplicación destinados a ser contenidos en bancos de datos de administración pública sólo en cuanto su tratamiento resulte necesario para el estricto cumplimiento de las competencias asignadas por ley a las respectivas entidades públicas para la defensa nacional, seguridad pública y para el desarrollo de las actividades en materia penal para la investigación y persecución del delito.

Entonces los datos con esa finalidad están exceptuados de la ley.

Y aquí hay otra pasión que yo quisiera pasarles, que es importantísima, porque hubiera sido mucho más fácil para quien hizo la ley peruana, para quienes hicimos el reglamento peruano y para quienes se acercan a este tema, comprender que lo que se protege son los datos personales, no los bancos de datos.

Los bancos de datos se protegen porque contienen datos personales. Si yo vendo bicicletas y tengo 25 almacenes de bicicletas, yo no me dedico a almacenes de bicicletas, yo me dedico a vender bicicletas y me ocupo de los almacenes porque ahí están las bicicletas.

Esa mirada así de simple permite evitar un montón de problemas. Uno bien simple, ¿quién es el encargado de la protección de datos en nuestra entidad público-privada? Los que ven bancos de datos.

¿Quién va a ver bancos de datos? Los informáticos. Ya está. ¿Es así o no es así?

Bueno, ese es un tema jurídico, es un tema del diseño, del proceso y del diseño del negocio.

No se protegen los bancos de datos porque son bancos de datos, se protegen porque tienen datos y entonces el centro de gravedad de este derecho es el tratamiento, aquello que se hace con los datos.

Si hubiéramos tenido eso presente en el Perú la ley no diría lo que dice, el reglamento no tendría que hacer malabares para encontrar, definir responsables y una cantidad de cosas que están muy complicadas de comprender y que podría haber sido muy fáciles de comprender.

Entonces los tratamientos destinados a la investigación y persecución del delito están por fuera de la ley peruana.

Y en otra parte la ley también dice, en materia de flujo transfronterizo, que el titular o encargado del banco de datos, no del tratamiento, ahí está un problema, deben realizar el flujo transfronterizo de datos personales sólo si el país destinatario mantiene niveles de protección adecuados.

Siguiente párrafo: En caso que el país destinatario no cuente con un nivel de protección adecuado, el emisor del flujo transfronterizo debe garantizar que el tratamiento de los datos personales se efectúe conforme a lo dispuesto por la presente ley, o sea, si va a puerto seguro no hay problema; si no va a puerto seguro toma las medidas contractuales o las que fueran para que llegue y sea tratado como un puerto seguro.

Y luego viene un párrafo que es muy similar a la norma española, pero con un defecto, dice: No se aplica lo dispuesto en el segundo párrafo en los siguientes casos:

Número dos, cooperación judicial internacional; número tres, cooperación internacional entre organismos de inteligencia para la lucha con el terrorismo, tráfico ilícito de drogas, lavado de activos, corrupción, trata de personas y otras formas de criminalidad organizada.

¿Cuál es la diferencia con la norma española? La norma española decía “no se aplica el párrafo anterior, el artículo anterior”, es decir, el que obliga a tener puerto seguro o tomar medidas para que lo traten como puerto seguro, sino que dice “no se aplica el segundo párrafo”.

Si no se aplica el segundo párrafo, quiere decir que no tengo obligación de tomar las medidas para que sea tratado como puerto seguro y se aplique el primero, sólo puedo enviarlo a aquel país que tiene el mismo nivel que yo.

Y eso no es así, porque además recuerden que las entidades dedicadas a la persecución del delito están por fuera de la ley.

¿Para qué decimos esto entonces si no están dentro de la ley? Tendríamos que pensar que aquí queda la cooperación o los flujos vinculados a la operación judicial en materia familiar, laboral, civil, pero la penal está por fuera.

Si además recordamos que los tratamientos que realizan las entidades públicas están exoneradas en hacer tratamiento en la ley peruana, entonces no había necesidad de decir nada, porque no necesito consentimiento, estoy fuera de la ley, hay un espacio en blanco. Y ese espacio en blanco no se puede mantener en blanco, porque hay necesidad de que los tratamientos que se hacen sobre los datos de las personas para estas materias tengan estándares y tengan reglas.

¿Qué reglas las rigen hoy? Las reglas internas, las que se han dado en las propias entidades. Y sería bueno saber si esas reglas están de acuerdo a los estándares constitucionales.

Hemos escuchado dos ponencias en las que todo indica que no y que no hay mucha posibilidad de hacer nada desde la autoridad administrativa porque están por fuera. Y ahí hay un espacio para trabajar bastante interesante.

Voy a aprovechar el tiempo para, antes del ejemplo, ¿qué espacio queda entonces? ¿Quiere decir que los tratamientos de datos personales en materia penal que no están dentro de la ley no tienen protección?

En ningún caso deberíamos tener esa respuesta, porque la protección de datos personales no viene de la ley, viene de la Constitución y la Constitución no hace distingos. Y además en mi país, como en muchos países, tenemos una acción de garantía constitucional, que es el habeas data, que permite a los ciudadanos ir al Poder Judicial y no a una sede administrativa que bajo obvia competencia no están esos tratamientos para conocer, actualizar, incluir, suprimir, rectificar la información, etcétera; es decir, sí hay protección en sede judicial.

¿Sobre qué parámetros hará el órgano jurisdiccional esa protección? ¿Ninguna, se la inventa, recurre a la doctrina de la privacidad del derecho civil o tendrá que mirar el desarrollo moderno de la protección de datos que está en la ley, aunque esté fuera de la ley por analogía?

Ahí también hay un espacio para trabajar, para conectar y dar la vuelta. Puede ser que estés por fuera de la ley, pero la forma en que resuelvas estas cosas tiene que tener algún correlato con lo que dicen las normas, que sí son constitucionales, que ya tienen garantía de ser constitucionales.

Lo que me queda lo voy a aprovechar para ponerles algunos ejemplos que son bien interesantes.

En mi trabajo tuve tres contactos con el servicio de inteligencia. El primero fue un señor que se acercó a preguntarme cómo podía hacer para proteger su dato personal de ser trabajador del servicio de inteligencia en el contexto siguiente:

Él iba a una clínica, lo ponía en espera para ser atendido por el médico y cuando lo llamaban, lo llamaban “señor tal, empleador del servicio de inteligencia”, porque el seguro tiene que saber quién es tu empleador. Me decía “y así no puedo”, me decía “no pueden hacer eso conmigo por el altavoz diciendo que trabajo en el servicio de inteligencia”.

Fíjense, en el Perú en los años 90 los policías y los militares estaban autorizados a quitarse la ropa de militar y ponerse chompas, casacas, para salir a la calle. Ahora lo puedo comentar sonriendo, pero en su momento era cuestión de vida o muerte, o sea, no podían salir uniformados.

Pero además no es de sentido común que a un miembro del servicio de inteligencia lo llamen a que se acerque identificándolo como miembro del servicio de inteligencia, parece esto Maxwell Smart.

Le contesté que este no era un tema de protección de datos y que más bien tendrían que ellos diseñar para que su empleador apareciera con un nombre que no sea identificable.

Y aquí voy a hacer algo que de repente no les va a gustar a mis amigos de la transparencia, porque los servicios de inteligencia no pueden ser transparentes, son opacos, tienen que ser opacos, tienen que mentir.

El segundo contacto fue una consulta que nos hicieron sobre si los bancos de datos del servicio de inteligencia debían ser inscritos en la autoridad.

La respuesta fue: Los bancos de datos destinados a las actividades de inteligencia no, los bancos de datos destinados a operaciones administrativas, de capacitación o lo que fuera, los que no tienen destino, pues sí.

Y la respuesta fue: Todos nuestros bancos de datos tienen finalmente función hacia los servicios de inteligencia y, por lo tanto, tendríamos que estar fuera.

Yo dije “bueno, sí, no vamos a discutir sobre eso”, para qué voy a discutir yo con el servicio de inteligencia. El día que haya una denuncia o haya una fiscalización -termino ahorita- tendrás que demostrar que eso es así y si lo demuestras, pues estarás por fuera de la norma, pero si no lo demuestras serás sancionado.

Fíjense, yo tengo unos ejemplos más, que los dejaré para una siguiente intervención si es posible, pero quiero comentarles esto:

Uno de los campos en los que la información personal de antecedentes judiciales o policiales se busca, es en el campo de las elecciones. Esto es el manual de verificación de datos de candidatos, publicado por una fundación vinculada a la libertad de prensa.

En su momento, cuando hubo una iniciativa de una cosa similar, desde la autoridad de protección de datos le dijimos “quien está legitimado para generar este concepto de elector informado es el Jurado Nacional de Elecciones”. Y el Jurado Nacional de Elecciones puede recopilar información que sea relevante para la toma de una decisión sobre por quién votar y ponerla en su web. Y eso hicieron.

No sé qué ha pasado luego que esta fundación, a partir de eso, expone sitios, vías y tutoriales de internet para encontrar la información de las personas que postulan.

Pero luego de cinco minutos mirando el manual uno se da cuenta que puedes encontrar unas personas que postulan y la de cualquier feligrés, no sólo la que postulan. Y la mirada es que el periodista tiene derecho a entrar.

Bueno, el periodista se hará cargo de para qué lo usa, pero de esto es potencialmente muy invasivo, o sea, el tutorial dice “ustedes pueden poner apellido, nombre, y proceso, denuncia, imputación, delito, fiscalía, procuraduría, contraloría, comisaría, testimonio, confesión y 15 palabras con las cuales van a poder acceder a los registros internos del Poder Judicial y Ministerio Público para encontrar no sólo condenas, sino también procesos, denuncias, iniciadas, por iniciar, la vida completa judicial de una persona accesible a quien pueda entrar por acá.

Y entonces en la protección de datos aparece dos alertas: Finalidad, proporcionalidad, una cosa que parece buena para efectos de conocer por quién voy a votar y tomar una decisión se convierte en una cosa un poco monstruosa en la que todos estamos expuestos a que nos averigüe quien sea y para lo que sea.

Y acá aparece otra moción que ustedes ya habrán escuchado que yo voy a repetir, porque te miran así como si fueras un loco y te dicen “pero si no tienes nada que esconder, para qué existe la protección de datos”.

Y la respuesta que todos hemos dado alguna vez: El hecho que tú no tengas nada que decir no significa que se puede eliminar la libertad de expresión. Esa es la diferencia de defender principios y de reconocer que esto nos puede afectar y afecta a muchas personas.

Comentaré luego otros ejemplos. Con esto termino. Gracias.

**Mtra. Elsa Bibiana Peralta Hernández:** Pues muchas gracias.

Creo que la oscuridad en la que dimos esta ponencia, estas ponencias, es reflejo precisamente de mucho del quehacer que desafortunadamente en estos temas se sigue realizando.

Pero por eso estamos aquí, para dar luz a todo lo que tiene que ver con crear estas políticas en la materia, crear estas normas, estas reglas en el tema de cooperación internacional y protección de datos personales en ámbitos como judicial, policial y el tema que tiene que ver también con procuración de justicia.

Y todas las experiencias que ellos han expuesto esta mañana, evidencian que tenemos que trabajar mucho de la mano en la parte de la protección de datos personales.

Con todo respeto, es cierto lo que dice Álvaro, las corporaciones que integran estos cuerpos: Seguridad, en el Poder Judicial y en el tema de procuración de justicia no siempre son tan abiertos o no siempre pueden ser tan abiertos; yo diría más bien eso, abiertos, no tanto opacos, no tanto oscuros.

Trabajé muchos años en el Poder Judicial y espero regresar ahora que ya me despidieron, voy a ir a tocar la puerta, pero la experiencia me enseñó en esos ámbitos, y también por el manejo de muchos expedientes, que sí se puede armonizar el tema de datos con el tema de transparencia.

Y lo que hay que aprender, como bien se dijo también aquí en este Panel, es a capacitar a todos los servidores públicos, hacer que entiendan cómo funciona esto, pero para que también ellos puedan ejercer su labor, tenemos que construir normativa eficiente y también construir las herramientas ahora con el uso de la tecnología, las herramientas tecnológicas que nos permitan lograrlo.

Un tema de ética, sí es cierto, atrás -como dije hace rato con el tema de la luz- de la tecnología hay personas, entonces para que la tecnología tenga un uso ético que funcione para construir esto, pues obviamente tenemos que trabajar en la ética de las personas y que las personas sean las que hagan eficiente todo esto para lograr una adecuada cooperación internacional y desde luego la protección de los datos personales en el ámbito judicial, policial, en las fuerzas de seguridad y en los órganos de fiscalización o de procuración de justicia.

La verdad es que lo que yo diga sale sobrando, porque lo dijeron mucho mejor ellos en su exposición, que aunque no lo crean y aunque esté al pendiente de la logística, sí escucho. Las mujeres tenemos un oído acá y otro acá, y me doy perfectamente cuenta de que este Panel estuvo maravillosamente iluminado, aunque físicamente no.

Muchísimas gracias. Espero que la luz haya llegado al entendimiento de todos en este primer Panel y que haya sido la provocación para que iniciemos estos trabajos y damos paso al siguiente Panel, con una mínima, mínima logística también para hacer el cambio de panelistas.

Quiero pedirles un gran aplauso para quienes nos acompañaron hoy aquí.

Y los invitamos, voy a hacerles también entrega de su respectivo reconocimiento.

Si me acompañan, por favor, de pie.

A José Álvaro Quiroga. José Álvaro, muchas gracias, bienvenido. Gracias.

A Juan Pablo Olmedo. Juan Pablo, gracias.

Y a Nelson Remolina, muchas gracias.

Viejos, viejos amigos que nos hemos encontrado aquí y gracias a ustedes.

Ah, unos obsequios que también les preparamos. Por favor, aquí a quienes me acompañan.

Gracias.

No, no es tequila. Muéstralo para que vean que no es tequila. Ese viene al rato y todos estamos invitados.

Muchas gracias por todo.

Y damos paso al siguiente Panel. Gracias por su permanencia y espero que haya sido la provocación para iniciar estos trabajos muy bien.

Gracias.