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

**Versión estenográfica del Panel 2: “La privacidad y el uso de los Datos por la Policía y Fuerzas de Seguridad”.**

**Presentador:** Se llevará a cabo el Panel 2: “La privacidad y el uso de Datos por la Policía y las Fuerzas de Seguridad”.

Agradecemos también la participación en este evento, de la licenciada Karime Yolanda Atié Ortiz, especialista anticorrupción.

A la doctora Eva Abaid Yapur, Comisionada del INFOEM. Y agradecemos a todos nuestros panelistas, que vienen de diferentes países, como Chile, España, Argentina, Costa Rica, Panamá, Uruguay, Columbia y Perú.

Agradecemos a todos ellos la participación en este Foro Internacional.

Y bueno, ahora a continuación, cedemos el uso del micrófono al maestro Samuel Montoya Álvarez, Comisionado Presidente del Instituto Zacatecano de Transparencia, Acceso a la Información y Protección de Datos Personales, quien moderará este Panel.

Adelante.

**Mtro. Samuel Montoya Álvarez:** Muchas gracias.

Muy buenos días, ya casi tardes.

La verdad es que me siento muy honrado en tener a dos excelentes panelistas.

Este Panel habla sobre la privacidad y el uso de los datos por la Policía y las Fuerzas de Seguridad.

Un tema muy polémico, muy complicado para poder establecer, toda vez que el tema de la policía, el trabajo que hace la policía, el trabajo que hacen las fuerzas de seguridad, pues desde el primer respondiente, desde la prevención, la persecución, la investigación, son totalmente torales y bases para que en su momento tenga que emitirse algún fallo por parte de las autoridades judiciales.

Y me permito presentar, vamos a tener, a razón de que tenemos dos panelistas, se les va a dar 15 minutos a cada uno, con la intención de que al final tengamos algunas dos o tres preguntas que sean preguntas que pudiéramos compartirlas con los panelistas y ellos nos puedan ayudar a sugerir alguna duda o dar alguna respuesta respecto a este trabajo.

Pues tenemos a la maestra, la doctora Cynthia. Es una compañera, es doctora en derecho privado en ciencias criminales, por la Universidad de París. Cuenta con maestría en derecho e innovación de técnicas de la Universidad de París. Con estudios en maestría en traducción del Colegio de México; maestría y doctorado, está muy joven para hacer tanto, pero creo que empezó desde primaria el tema de la preparación.

La verdad es que preferiría dar el espacio a la doctora Cynthia Gabriela Solís Arredondo, a razón de aprovechar la experiencia y los conocimientos en este Panel tan importante de qué hacen las corporaciones de seguridad, qué hacen las policías en el resguardo, en el manejo de los datos personales, hasta dónde pueden o no compartirlos, hasta dónde afecta o no afecta la investigación.

Puede en su momento ser importante o toral para que al momento de que la autoridad judicial emita algún fallo, esto afecte o no el tema de este derecho humano, que ese es el tema de los datos personales en su resguardo.

Doctora, muy buenas tardes, bienvenida, muchas gracias. Le dejamos el lugar.

**Dra. Cynthia Gabriela Solís Arredondo:** Muchísimas gracias, Comisionado.

Bueno, primero que nada, muchísimas gracias a todos ustedes por estar aquí.

Quiero agradecer profundamente a todo el Comité Organizador, principalmente a mi gran amiga, la Comisionada y maestra Dulce Bibiana Peralta, por la invitación, porque realmente es un honor estar en este evento internacional, de gran trascendencia, y pues aquí con mi colega, el ingeniero Joaquín y con el Comisionado.

A ver, empezaremos con una triste realidad. Sabemos que los índices de criminalidad, de violencia van a la alza en el mundo, no solamente en México, pero bueno, obviamente aquí nos toca vivirlo.

Simplemente en la Ciudad de México, todos los días, los ciudadanos, los habitantes de esta Ciudad y de la zona metropolitana, antes de salir de casa hacemos un análisis de riesgo.

Vamos a decir el día de hoy qué bien jurídico queremos poner en riesgo, si el patrimonio, la vida, la integridad física. Entonces, si nos vamos, por ejemplo, en transporte público, pues ponemos en riesgo, sobre todo si es microbús, la integridad física.

Y bueno, las mujeres, si nos vamos a ir en metro, ya sabemos que ese día no tenemos que ponernos ni minifalda, ni tacones, y si de plano salimos en nuestro coche, pues si no tenemos dónde estacionarlo, nos arriesgamos, o asumimos ese riesgo de que cuando regresemos ya no tenga llantas, autopartes, o simplemente ya no esté.

Y, bueno, esto también sucede en el ciberespacio, o sea, no es una cuestión que únicamente se limita al tema, digamos, físico, sino que todos los días salimos e interactuamos en el ciberespacio.

Entones, ante esta realidad, que no es para que caigamos en depresión, ni nada por el estilo, sino que, para poder transformar esta realidad en algo mejor, necesitamos asumirla, entenderla y actuar en consecuencia.

Entonces, ante esta realidad cada vez más preocupante, pues los organismos de investigación, de impartición de justicia, también se enfrentan a este tipo de retos, y de repente salen propuestas muy interesantes, de creación, de bases de datos que permitan obviamente tener información y monitoreo de la actividad, de hechos presuntamente delictivos, tanto dentro como fuera del ciberespacio.

Y a poco no, de repente sale una propuesta y dice: “Bueno, vamos a crear una base de datos única, que contenga datos biométricos”, y todo mundo entra en paro cardiaco.

Datos biométricos, como si no anduviéramos por la vida exhibiendo nuestros datos biométricos.

Pero aquí lo importante de la creación, es que sean bases de datos de calidad.

Lo sepamos o no, este tipo de información, este tipo de bases, se están creando día con día, sobre todo en el entorno privado.

Muchas empresas, como ustedes lo saben, ya no es un secreto para nadie pues están constantemente monitoreando nuestra actividad, y generando lo que, en mi tema de tesis doctoral, le llama como la identidad digital, que es justamente todo lo que se dice, lo que se habla de nosotros, y que no es como la identidad que conocíamos antes, que era estática, sino que ahora, realmente todo lo que se dice de nosotros, dónde estamos, con quién hablamos, con quién platicamos, a dónde vamos, se vuelve parte de esta identidad.

Entonces, si les soy honesta, ante una realidad en la cual obviamente ante los riesgos que estamos comentando, que ya no solamente son a nivel físico, sino a nivel también en el ciberespacio, solamente que en el ciberespacio lleguemos a ser un poco como más ingenuos, como que somos más ingenuos y creemos que en el ciberespacio no pasa nada.

Y, de hecho, ni otros organismos son reconocidos en el ciberespacio, como el quinto dominio de la guerra, o sea, donde se puede llevar a cabo la guerra.

Entonces, ante esta situación, si les soy honesta, yo utilizo este dispositivo, que es a través del cual la mayoría o todos nosotros estamos siendo monitoreados constantemente, yo tengo geolocalizadas a las personas más importantes de mi familia y ellas a mí, y es cierto, estoy cediendo un poco de mi privacidad, o estoy cediendo un poco de este control de mis actividades, y les estoy diciendo dónde estoy, pero la verdad si un día desaparezco, de preferencia me gustaría que me encontraran viva, si me encuentran viva en la mejor de las circunstancias y si no, que por lo menos encuentren mi cuerpo para que mi familia pueda seguir su vida adelante, porque hoy en día la realidad es que pues lo que vivimos aquí, y en muchas partes del mundo, es que las personas desaparecen y no sabemos dónde están.

Para esto, se ha propuesto en el mundo, la creación de diferentes bases de datos importantes; esto no es nada nuevo. Por ejemplo, tenemos las bases de datos del FBI, que contienen las huellas digitales y que son incluso consultables, obviamente bajo petición debidamente fundada y motivada, bases de datos europeas, que contienen pues todo este monitoreo. Incluso les invito a que ustedes hagan un récord, si alguna vez han viajado a Estados Unidos, ustedes pueden en una página web, consultar todas las entradas y salidas que han hecho a ese país, solamente poniendo su pasaporte y es una página gubernamental.

Entonces, hay un montón de bases de datos de consulta. El problema es que no se comunican entre sí, el problema es que no hay una cooperación entre todos esos organismos, y de nada sirve en un entorno en donde la delincuencia ya no conoce de fronteras, ya no conoce de jurisdicciones y como lo decía hace un minuto, en la inauguración el diputado Santillán, pues realmente ya no existen estas líneas divisorias.

Ahora bien, todo esto debe de llevarse a cabo correctamente. ¿Cómo? Estas bases de datos que como lo comentaba hace un momento, deben de ser de calidad, es decir, debe ser información confiable, porque también es cierto que hay muchas bases de datos que no son confiables, que no están unificadas, que hay duplicidades, etcétera, y para eso pues lo importante sería tener la posibilidad de correlacionar información con otras bases de datos, lo importante de esto es generarlas con una conciencia de finalidad, para qué voy a ocupar esa base de datos, porque creo que como ciudadanos mexicanos, lo que nos estresa mucho cuando hay este tipo de propuestas, es para qué otra base de datos, qué va a pasar con ella, la vamos a encontrar en el comercio ilegal a los meses, qué es lo que va a pasar.

Entonces, realmente lo que necesitamos es tener como esta conciencia de la finalidad, para qué se van a generar esas bases de datos, quién va a tener acceso a ellas, que se conciban desde este concepto de privacidad por defecto.

También la transparencia en cuanto al tratamiento de la información, qué se va a hacer con ella, exactamente para qué la quieren, quién va a tener acceso, etcétera, pero sobre todo también un marco jurídico adecuado que permita legalmente que obviamente jueces, policías de todo el país, e incluso transnacionales, puedan tener acceso a esta información para hacer un rastreo de las actividades delictivas y de las células delictivas.

Y también algo muy importante, esto no es un tema exclusivamente jurídico, es un tema que también debe de ser abordado desde el punto de vista tecnológico, contar con debidas medidas físicas, técnicas y administrativas, un sistema de gestión de seguridad de datos personales, para que nosotros como ciudadanos también tengamos esta o recuperemos esta confianza en que la información no va a caer en manos de la delincuencia organizada, o en personas que por alguna razón pues se desvíen en el camino y cooperen con la delincuencia.

Entonces, yo creo que aquí lo importante es tener en cuenta de que esas bases de datos que ya existen hoy en día y que ya existen en el ámbito gubernamental, pues de preferencia que estuvieran unificadas y que pudieran servir para esto, en pro de la sociedad; ninguno de nosotros aquí estamos peleados con nuestra seguridad, yo creo que todos queremos estar en un ámbito seguro, el debate realmente aquí no es el qué, sino el cómo y para eso obviamente aquí, Joaquín es experto en ese tema y con todo el backroom que tiene en la agencia española de protección de datos personales, nos puede decir cuál es su perspectiva.

Muchísimas gracias.

**Mtro. Samuel Montoya Álvarez:** Muchas gracias, doctora.

Temas muy importantes, torales, marcos jurídicos, la gestión de seguridad, el cómo que finalmente es la parte importante del cómo resguardar estos datos personales, de cómo ser cuidadosos, las corporaciones, sin que afecte el debido proceso; pero también en algún momento, cómo deben de actuar en ese resguardo que, a pesar de haber cometido algún delito, alguna falta, pues se tiene que resguardar este derecho humano.

Y la verdad es que nos sentimos muy honrados, muchas gracias, doctora. Asimismo, presentar a Joaquín Pérez Catalán.

Joaquín Pérez Catalán es ingeniero de telecomunicaciones e inspector de datos de la Agencia Española de Protección de Datos. Dispone de diversas certificaciones; ha desarrollado su carrera durante más de 20 años en los entornos de seguridad y protección de datos, tanto en España como en el extranjero.

Ha sido consejero de la Unión Europea en materia de protección de datos para Israel y Bulgaria.

Ha participado en diversos proyectos, actualmente desempeña su labor como maestro en diferentes universidades de España, y participa en el proceso de implementación y coordinación en un entorno de nuevo reglamento general y europeo de protección de datos personales.

Doctor, bienvenido, ingeniero y pues escucharemos atentamente la experiencia en todo lo que respecta a su experiencia profesional y práctica en el tema de datos personales.

Gracias.

**Ing. Joaquín Pérez Catalán:** Bueno, muchas gracias; gracias Cynthia también.

En primer lugar, quiero agradecer a todos ustedes por estar aquí, a la Organización, al Info de Ciudad de México, por invitarme, a la Unión Europea, que también ha hecho posible que esté hoy aquí, y también por supuesto a Bibiana, amiga también que me ha invitado personalmente a estar aquí con todos ustedes.

Bueno, me toca hablar del cómo.

Pues el cómo en mi caso se traduce, viene del contexto europeo, porque donde trabajo habitualmente, Europa, la Unión Europea es un ente, es menos que un estado, no llegamos a ser un estado la Unión Europea, sigue habiendo los distintos estados; tampoco somos una organización internacional, somos algo más que una organización internacional, estamos ahí a caballo, somos un ente un poco extraño, entre un estado y una organización internacional.

Ahí en medio, no es algo que se va construyendo día a día, yo me paso la vida prácticamente en Bruselas, la semana que viene estaré toda la semana ahí, y a mí me sorprende todavía cuando nos reunimos en el grupo de protección de datos y tomamos decisiones, pues una cosa que me sorprende es que votamos y Alemania es un voto y Luxemburgo es un voto.

España es un voto, Portugal un voto más. Eso es una sesión de generosidad por parte de algunos países tremenda.

No sé cuántos Luxemburgos tiene Alemania. Pues un voto cada uno.

Pues así funcionamos y funcionamos de forma dinámica.

De hecho, teníamos un marco en materia de protección de datos, derivado de la directiva, que funcionó en su momento. Una cosa que tiene buena la Unión Europea es que cada vez que saca normativas, la propia normativa incluye un período de revisión, para saber si esa normativa que se haga ahora con unos objetivos, los objetivos se han alcanzado en un 100 por ciento o en un 20 por ciento, a nosotros nos debía mucho y hay que tunear, hay que tocar la normativa.

Eso llevó a que la directiva en su momento se retocara y se cambiara totalmente de modelo. Cuando se hizo la directiva en el ’95, pues no existía Google, Facebook, ninguna de estas empresas, ni se las esperaba. Y eso permitía abordar los tratamientos que tenemos hoy en día y se cambió el modelo al reglamento de Europa de Protección de Datos que supongo, más o menos, todos han oído hablar de él.

Pero no solamente este cambio de la directiva al reglamento ha sido este cambio, sino que han aparecido también otra serie de instrumentos jurídicos, que han aparecido nuevos y que no existían antes, aparecen como versión cero; es una directiva justo en materia de protección de datos en el sector policial.

Y una directiva también para los sistemas de los PNR. Son directivas que obligan a los estados a laborar una serie de normas, de acuerdo a ese patrón, marca una directiva para regular esto.

La Unión Europea también, en ese proceso devolutivo, porque empezó siendo simplemente un entorno donde podían circular las mercancías, pero era curioso, las mercancías podían circular, pero no las personas.

Entonces, en un momento dado, se decidió y esto sí en un sentido de humanidad, porque no van a circular las personas, si somos más importantes que las mercancías, y determinados los países, firmaron el Convenio y esto permitió eliminar a las fronteras.

Y ahí hubo un primer fichero o gran base de datos o gran sistema, de intercambio policial, porque al desaparecer las fronteras, y aquí voy entrando un poco en el cómo, al desaparecer la frontera, significa que a mí me roban mi coche en España, en Madrid, donde yo vivo, yo lo denuncio, pero el que me ha robado el coche, se puede ir a Francia porque no hay frontera, no tiene que pasar ningún control de Francia a Alemania y el que me ha robado el coche, pudiese ir a Dinamarca y conducir ahí mi vehículo.

¿Y qué pasa si en un control de la policía en Dinamarca paran al que lleva mi coche? Si la policía de Dinamarca no sabe que mi coche ha sido robado, pues la persona circulará por ahí con mi coche.

La policía de Dinamarca, tiene que saber que mi coche ha sido robado; tiene que saber que mi coche ha sido robado, tiene que saber si mi pasaporte o mi documento nacional de identidad ha sido robado; tiene que saber si mi pasaporte o mi documento nacional de identidad ha sido robado; tiene que saber si una persona cercana a mí ha desaparecido y yo no he denunciado su desaparición, porque puede aparecer en Dinamarca o en Suecia o en cualquiera de estos países, porque no hay fronteras.

Eso, el de la desaparición de fronteras, implica constituir una gran base de datos, donde cada país vuelca la información de personas desaparecidas, de objetos robados, también, por ejemplo, cuando un juez decreta la búsqueda y captura de una persona en España, esa persona puede no estar en España, porque no hay frontera, puede estar en Italia.

Esa información también va a este sistema. Entonces, es un sistema de información que, como se puede imaginar, tiene información muy jugosa.

Cuando se constituyó en la primera versión, pues se hizo con un sistema informático, bastante limitado, tiene una serie de problemas, pero lo que sí se hizo ahí ya es cuando se diseñó este sistema, meter el concepto y eso que todavía no estaba en la Ley de Privacidad por Defecto y por diseño.

Se diseñó el sistema de forma que, como iba a haber datos personales, que las autoridades de control, las autoridades de supervisión, de protección de datos, tuvieran competencia sobre estos sistemas.

Y, de hecho, la han tenido desde el origen. Ha ido evolucionando porque es sabido bien por determinadas deficiencias, y se han ido mejorando, es un proceso constante, pero las agencias de protección de datos, tienen plena autoridad sobre ese sistema. Lo han tenido al comienzo y la tienen, y de hecho, puedo decirles una cosa, y es que si en España el origen de la primera Ley de Protección de Datos que tenemos en España y de la primera, la creación de la agencia de protección de datos española, en la cual yo trabajo, pues no fue un capricho del gobierno, de decir: “Vamos a sacar una ley, y vamos a sacar una autoridad independiente”, vino derivado de la necesidad del gobierno español, de incorporarse a este club de Schengen, de eliminación de fronteras.

La incorporación a este club implicaba, porque así estaba diseñado el sistema, que tenía que tener el país una Ley de Protección de Datos, y tenía que tener una autoridad independiente.

Y, de hecho, cuando España firmó el protocolo de adhesión, en el protocolo iba un compromiso de crear una Ley, de hecho, se creó al año siguiente, antes de la directiva, y tuvimos la Primera Ley de Protección de Datos y la primera vez que se estableció la agencia, como consecuencia de entrar en este Sistema de Información de Schengen.

Bueno, en este Sistema de Información de Schengen, se hacen auditorías por parte, porque esta voz es fundamental; es decir, las autoridades de protección de datos, tienen que monitorizar este sistema, tienen que controlar que los tratamientos que se hacen sobre esos datos, los accesos cumplen las reglas.

Esto lo engancho con lo que ha dicho antes el ponente chileno, con lo que está pasando en Interpol, donde quizá haya habido un fallo, porque en el diseño de Interpol, quizás es una organización mucho más antigua, no se previó para nada el tema del manejo de los datos y que pudo haber problemas en el sistema de control de datos, y que puede haber incluso excesos en los tratamientos sobre los datos y no existe una autoridad claramente definida.

En cambio, en los sistemas que se están creando en Europa y ya llevamos unos cuantos, de cooperación policial, en todos, desde el comienzo, está el papel de la protección de datos y las autoridades de protección de datos.

Y eso que estos sistemas están evolucionando y mucho. Se está favoreciendo la interoperabilidad, se está favoreciendo, porque por ejemplo, a raíz de los atentados que hubo en Bruselas, se detectó, se puso de manifiesto que quizás se podía haber evitado ese atentado.

Si se hubieran conectado a determinada base de datos, que eran estancas, que no tenían interoperabilidad entre ellas, porque hubo dos terroristas que salieron, eran ciudadanos europeos, salieron con su pasaporte europeo, legalmente de Europa se fueron a entrenar a donde no tenían que ir, y después volvieron, no haciendo uso de su pasaporte europeo, sino volvieron camuflados entre los migrantes de forma ilegal.

Al entrar de esa manera, los capturaron, les tomaron las huellas, fueron sus datos a un sistema de huellas, pero que estaba destinado a una finalidad muy concreta. Si ese sistema se hubiera chequeado contra los restos de los sistemas, lo hubiera hecho, y por qué hacen los ciudadanos que tiene pasaporte europeo entrando de forma ilegal en Europa.

Eso hubiera sido tremendamente sospechoso.

Eso ha activado alarmas y ahora la Unión Europea reacciona y está moviendo a todos sus sistemas de colaboración policial en los distintos sistemas que eran estancos, para crear una interoperabilidad entre ellos.

Pero siempre teniendo en cuenta las autoridades de protección de datos, y los principios de protección de datos.

Y de larga tradición, venimos haciendo auditorías sobre estos sistemas. Eso, como todo proceso, tiene su estado, digamos, infantil, inicial, donde las cosas funcionan o medio funcionan; las primeras auditorías, por ejemplo, que se hicieron sobre el sistema Schengen, pues lógicamente lo hizo gente que no tenía conocimientos en materia de tecnología, en materia de auditoría.

Entonces, lo digo así, porque era así claramente, las primeras auditorías iban al centro de proceso de datos, donde estaba la base de datos de Schengen, en Starburgo, el jefe del centro le pone una presentación de lo maravilloso que era aquello, los invitaba a comer, y se había terminado la auditoría.

Con el tiempo, eso se vio, aquí hay que hacer una auditoría en serio. De hecho, yo tuve la ocasión de participar en la primera auditoría que se hizo con parámetros de auditores sistemas, y tuvimos la presentación de todos los años, la invitación a comer, pero paramos, dijimos: “no, queremos esta serie de documentos, porque no nos vamos a ir hoy, vamos a estar aquí unos días y queremos mirar cosas”.

Y después de esto, no entiendo: “Sí, queremos esto”, pues estuvimos una semana mirando cosas, evidentemente encontramos cosas y nos expulsaron.

Pero bueno, ahora lo puedo contar como anécdota, porque ahora funciona muy bien.

De hecho, las primeras veces, claro, vas a auditar, auditamos a nuestras policías, las primeras que fueron a auditar a nuestra policía, pues notabas que trataban de ocultar cosas, contestaban sí, no, las típicas.

Ahora en cambio, casi están deseando que vayas a auditarle y te dicen lo que tienen mal. Y hasta dicen: “Pónmelo por favor en el informe de auditoría, así de grande”, a ver si mi responsable político cuando vea el informe, por fin me dota los recursos para tener esto.

Ahora tenemos en el sistema de Schengen tenemos auditorías cruzadas.

¿En qué consiste esto? Pues España tiene una serie, la policía española, el Ministerio de Asunto Exterior Español, que participa en este sistema, la agencia española tiene una serie de funciones, de obligaciones de acuerdo a la normativa, en materia de los policías, la gente de Ministerio de Exteriores, tiene que tratar los datos de determinada manera y la autoridad española tiene que controlar que eso sea así.

De vez en cuanto recibimos una auditoría formada por equipos de distintos países europeos, claro, no hay españoles ahí, porque vienen a auditar a España, nos vienen a auditar, nos sacan cosas, como todo el mundo, algunas incluso los policías están diciendo: “Ponlo, por favor. A ver si así me dotan dinero, porque quiero esto”.

Y hacen ese informe y ese informe luego se eleva, y evidentemente se intenta resolver. Y cuando se audita a otro país, pues españoles, tanto policías como funcionarios de la Agencia, participan.

Yo he participado en auditoría a Francia, y tuve que atender la auditoría que vino a España.

Es un proceso que claro, ha costado tiempo, porque si yo te audito en tu casa y luego tú vienes a auditar mi casa, suena muy fuerte, pero la verdad es que, pasando ese estado inicial de cierto rechazo, de cierto rechazo a mostrar tu casa, y tus deficiencias, al final lo conviertes en algo positivo, incluso sacas lo que tienes mal, porque es la forma de que te den los recursos para arreglarlo.

Creo que estoy un poco en el cómo y además de forma operativa.

Entonces, yo creo que esto es un camino que se va desarrollando y cada vez se va desarrollando más.

Ahora, en Europa se van a decidir toda una serie de nuevos sistemas en materia policial y van por esta vía, por esta vía, este mecanismo está funcionando razonablemente bien, es obviamente auditorías cruzadas y también de revisión de la normativa, porque hay que revisar la normativa cada cierto tiempo.

Los delincuentes, cada vez utilizan más las nuevas tecnologías y es lógico que la policía también.

Tradicionalmente la policía, como usted trata datos sin consentimiento, porque obviamente el denunciante, el delincuente no le va a dar consentimiento, a cambio de ese control pues usted solamente puede usar los datos para esa investigación concreta, que está haciendo sobre este delincuente.

Ahora, eso ha cambiado en la nueva directiva de protección de datos en materia policial, se amplía la base legal, se permite que se hagan tratamientos tipo big-data, cruzando datos, porque una de las cosas que uno descubre es que delitos que parecían que eran inconexos, están correlacionados.

Esto es una de las cosas que hace Europol.

Europol hace eso, Interpol permite pedir datos de un país a otro, pero datos de un delincuente concreto, de un delincuente concreto.

Y te hace la comunicación. Hoy, antes, una persona interesante, la ponencia del colega chileno, que Interpol considera que el dato es suyo, cuando Interpol no ha generado datos, lo ha generado la policía de un país.

En Europol esto no es así, en Europol que recibe los datos de distintos países, la normativa dice que el dato es del país que lo ha incluido.

Y, de hecho, si Europol quiere utilizar, hacer correlaciones, tiene que pedir permiso al país que ha metido el dato. Fíjense la diferencia, no tiene nada que ver.

Y de hecho está muy claro que hiciste una cosa que no está claro en Interpol.

Yo no sé si en España hubiera llegado este caso, un ciudadano español, con una alerta de 20 y tantos años, no sé qué pasaría, había que analizarlo jurídicamente.

Pero si eso pasara en Europol, estaría clarísimo que somos competentes, porque está en la norma, está claramente definido que hay unas autoridades de control y no un mecanismo para controlar eso, en el sistema Schengen, en el sistema Europol y en todos los sistemas que hay de intercambio policial.

Con esto, voy a cruzar el charco ahora y vengo aquí, donde estoy. Voy a hablarles de Ameripol, que era para lo que yo había venido.

¿Qué es Ameripol? Ameripol no es, no cuelga de Interpol, para nada. Ameripol pretende, tampoco cuelga de Europol, pero pretende ser algo parecido a Eorupol.

De hecho, ahorita mismo funciona una especie de prototipo, financiado por la Unión Europea, por Europol y en el que participan un conjunto pequeño de países de Latinoamérica.

¿Qué tiene Eorupol, Ameripol que no tiene Interpol? Interpol permite la comunicación de datos, digamos, de un delincuente concreto. Oye, este delincuente que sé que está en tu país, yo creo que está en tu país, por favor, te pongo una alerta y si lo encuentras, me avisas.

Europol permite hacer eso, pero permite mucho más, porque permite hacer estudios de correlación y te devuelve datos de inteligencia.

Hace poco en una conferencia en Ecuador, que ya están hablando con un alto cargo de la Policía Brasileña, en una cena, pues ya están usando, con datos agregados, y me comentaba que gracias a Ameripol, están viendo que incidentes, delitos que antes veían de forma aislada, al correlacionarlos, se dan cuenta de que forman parte de la misma mafia.

Y entonces permite tratarlos como delincuencia organizada, y ver esa relación.

Eso para la policía es fundamental, fundamental y las autoridades tenemos que permitir eso, porque eso va en nuestra seguridad.

Ameripol permite hacer eso. ¿Qué le falta a Ameripol? A Ameripol le falta ahora mismo que no tiene en personalidad jurídica propia. Ahora mismo es un convenio entre altos cargos policiales, de distintos países de Latinoamérica, con apoyo de la Unión Europea, a través de Europol, incluso les ha facilitado Europol, software, para que no tengan que comprar licencias, para que empiecen a funcionar, para que vean la utilidad de eso.

Pero la idea es que eso se constituya en un organismo internacional, por lo tanto, que sea vinculante, que tenga personalidad jurídica propia, ¿para qué? Pues en África hay una Africapol, en Asia hay un Asiapol, en Europa hay un Europol. Si tiene personalidad jurídica propia y participa en un conjunto importante de países, podrán firmar acuerdos de tú a tú con Europol, con Áfricapol, con Asiapol y poder intercambiar datos, porque los delincuentes no están en un país solo, se mueven por todo el mundo. Y si no tenemos esa colaboración y no dotamos de esto a mecanismos de colaboración, pues no vamos a ningún lado.

Ni siquiera Europol por sí misma, que agrupa a todo Europa, Europol necesita de algo, de un ente similar o parecido en América y aquí haría falta un ente similar, ya existe, pero hay que crearlo para que pueda relacionarse de tú a tú con estos organismos que existen equivalentes.

Por supuesto, es fundamental que las autoridades de protección de datos, estén ahí, ¿y cómo van a estar ahí? Pues miren, fácil. Esto también es una oportunidad, como lo fue en su día para la Agencia Española, que nació como consecuencia de entrar en un club, donde el núcleo era una base de datos policial, el espacio Schengen, ahora puede ser también para las autoridades de protección de datos de Latinoamérica, el estar en Ameripol, porque eso nos puede dar mayor estabilidad como institución, mayor independencia y les va a permitir también trabajar juntas, estas auditorías que yo les digo que hacemos en Europa, donde nos juntamos inspectores o auditores de distintos países, y vamos a auditar a un país, esto aquí también se tendría que dar.

Este sistema Ameripol, en su día, cuando se firme el tratado internacional, estará en algún sitio, en algún país de Iberoamérica, no sé, el que decidan, el que sea.

Pero ahí habrá que hacer auditorías, sobre esa base de datos, y obviamente no debería hacerla solo la autoridad de ese país. Imagino, por ejemplo, que se entiende que está en Brasil. Pues ahí están los datos de las policías de todos los países que participen, no sólo las de Brasil.

La auditoría sobre ese sistema, no debería hacerla la agencia de Brasil, debería hacerla representantes de todas las agencias, cuyos países meten datos ahí.

Luego, estos sistemas también tienen una parte nacional; es decir, no cualquier dato puede entrar al sistema, tiene que cumplir las normas que se definan.

Eso sí que sería competencia de cada autoridad nacional.

La autoridad de México, comprobaría que la policía de México, mete los datos debidamente, no mete a un señor 25 años ahí, sin causa.

La autoridad policía de Panamá, haría lo mismo respecto de la policía de Panamá, pero a la hora de auditar el sistema común, que tiene que estar en algún sitio, no vamos a poner en altamar, debería ser algo que podamos denominar, una autoridad de control común, que no es necesario crear burocracia y crear una agencia a nivel súper americano, simplemente que a la autoridad que forma parte de este sistema, designa una o dos personas, y ese conjunto de personas, son los que tienen la capacidad hacia el sistema Schengen y funcionó.

Por eso les cuento esto.

Puede haber otras soluciones, pero eso es una solución barata, de bajo coste, y funciona y efectiva, y permitiría coordinarse en dos agencias y funcionar.

Luego entonces, yo quiero promocionarles Ameripol, creo que sería estupendo para América contar con el proyecto Ameripol salga adelante, sería una oportunidad estupenda para las autoridades de protección de datos, está ahora pendiente de hacerse la parte de una negociación del tratado internacional, este tratado internacional va a tener un anexo dedicado a protección de datos, ahí habría que meter los controles de protección de datos, todas las políticas de protección de datos que tiene que cumplir Ameripol, y también cómo va a ser monitorizado ese cumplimiento por parte de las autoridades de protección de datos.

Y cómo tienen que coordinarse para verificar ese cumplimiento, que tiene que pasar por hacer auditorías, por hacer monitorizaciones, e incluso, por auditorías cruzadas.

Eso puede implicar una cierta sesión de soberanía, por eso de que el inspector de un país pueda ir a otro, se puede llegar a eso, pero créanme que, pasado el estadio inicial, este de abrir las puertas de tu casa y ver adentro, al final, lo agradeces y funciona y ayuda a que mejore.

Entonces, esto al final, digamos, como conclusión, lo que antes ha dicho otro ponente, que protección de datos y transparencia no son dos caras de un amoneda antagónica, sino que tienen que hablar, yo estoy totalmente de acuerdo con ello, protección de datos y transparencia hay que dialogar y mucho, porque se tienen que entender y lo mismo digo ahora, si metemos en esta ecuación a la policía.

La policía no es el enemigo de la protección de datos, ni la protección de datos es enemigo de la policía, tienen que hablar, porque seguramente llegan a un entendimiento. Los comienzos no son fáciles, no lo han sido, yo los he vivido, llevo trabajando en la Agencia Española desde su comienzo y he vivido de las primeras inspecciones hasta las que hacemos ahora.

Y simplemente como anécdota, esto que llevo aquí es un pin, hace poco la policía me condecoró con la medalla al mérito policial.

Y he sido el enemigo de ellos, les he hecho multitud de inspecciones, les he sacado multitud de defectos, pero de vez en cuando me llaman y me consulta, porque al final se dan cuenta de que tenemos que trabajar juntos.

Tenemos que trabajar juntos y ese es el camino.

Entonces, les quiero pedir, por favor, que piensen en el proyecto Ameripol, no como el Interpol, no tiene nada que ver. La idea es que los datos de Ameripol, sean de los países que lo introducen y los tratamientos de correlaciones de inteligencia, sean con el consentimiento de los países, el país que introduce el dato siempre tiene el control de los datos, y si tiene una autoridad de protección de datos detrás, que le dice si lo puede o no puede hacerlo, no van a pasar estas cosas, como las que han pasado con el ciudadano de Chile en Interpol.

De hecho, en Europa, esto no ha pasado, con los sistemas europeos, porque están las agencias ahí, desde el comienzo.

Bueno, con esto, muchas gracias por su atención.

**Mtro. Samuel Montoya Álvarez:** Muchas gracias, ingeniero Joaquín.

A razón de darle un poquito más de tiempo, y aprovechar a nuestros dos importantes panelistas, pudiéramos hacer dos o tres preguntas. Si gustan, serían dos o tres personas, que la pregunta sea muy concisa, para poder dar el tiempo y no exceder mucho el tiempo del panel y poder iniciar el otro panel.

Entonces, sería una, dos o tres preguntas y si alguien tiene alguna inquietud.

Si le pueden acercar algún micrófono.

¿Alguien más para después? Ok.

**Pregunta:** Buenas tardes.

En relación al tema de las policías y las fiscalías, quisiera saber qué tanto avance tienen en la implementación del sistema de seguridad de datos personales, de los propios policías.

**Mtro. Samuel Montoya Álvarez:** Aquí le damos el micrófono.

**Dra. Cynthia Gabriela Solís Arredondo:** Qué tal, buenos días.

El planteamiento es muy interesante, porque justamente aquí es donde entramos o no a otro tema, que es el tema de la transparencia.

Hay muchos casos, como bien lo comenta, donde justamente la información de muchos policías, también ha sido exhibida de forma irresponsable, sobre todo por medios de comunicación, donde también se pone en riesgo la seguridad física y la integridad, no solamente del policía, de los militares, de la familia. Y eso también es un tema que se ha tocado mucho, porque es un tema también, hay que decirlo, de falta de responsabilidad por parte de los propios medios de comunicación.

Recordamos que obviamente estos límites, ningún derecho fundamental es absoluto, y entonces este tipo de derechos que empiezan a ser, no le quiero decir, que colisionan, sino que tienen que convivir entre la protección de la transparencia a la protección de los datos personales y el tema también de la privacidad, mucho está como el tema de la conciencia y en el sentido, ahorita es muy reciente obviamente la creación de las fiscalías con organismos autónomos, y se está trabajando en ese tema, pero creo que también es muy importante la conciencia, como lo comentaba ahorita, de los ciudadanos y de los medios de comunicación.

Porque también como ciudadanos de repente exponemos y videograbamos a estas personas y las ponemos en riesgo de una forma irresponsable.

Entonces, bueno, pues se está trabajando en eso, evidentemente todo esto pues está justamente en la parte en la cual estos funcionarios obviamente sus datos personales, son en algún punto deben de ser carácter público, necesitamos saber eso, pero también hay un momento en el cual se excede, digamos, la finalidad para la cual son tratados esos datos y entonces, sí podemos caer en rebasar esta línea y utilizar esos datos para fines desproporcionales o cuya finalidad no es lícita.

¿No sé si respondí correctamente?

**Ing. Joaquín Pérez Catalán:** Yo simplemente quería añadir, no conozco la normativa aquí en México, pero sí quiero comentarle, no he tenido tiempo de explicarles la directiva de protección de datos policial, pero sí que una de las cosas que miramos en las auditorías, porque está la normativa, es que la gente, los funcionarios de policía tienen que recibir formación en materia de protección de datos.

Y, de hecho, vamos muchos funcionarios de la Agencia a los lugares policiales a dar cursos de protección de datos, porque los funcionarios tienen que saber qué pueden hacer, qué no pueden hacer con los datos.

El hecho de que uno tenga el dato ahí, no significa que pueda hacer con él lo que quiera, eso es fundamental, ese dato está con la finalidad y está para determinar las cosas.

Y hay cosas que, aunque el dato no esté adelante, no puede utilizarlo para determinadas finalidades, y eso tiene que saberlo y eso hay que formarlo.

Forma parte de ese diálogo, autoridad de protección de datos, fuerzas policiales.

**Mtro. Samuel Montoya Álvarez:** Muchas gracias.

Abriríamos el espacio a una pregunta más.

Si alguien puede acercar el micrófono.

**Pregunta:** Gracias.

En la experiencia de Europol, y particularmente, porque por desgracia no estamos de que nuestras policías, hablo no solamente de la de este país, sino en Latinoamérica en general como que no están tan preparadas o tan capacitadas, lo acaban de decir justo en esta materia de protección de datos personales, qué tan factible va a ser este proyecto en particular, en esta materia, esto que decías de Ameripol, y qué países están ya integrados.

Gracias.

**Ing. Joaquín Pérez Catalán:** A ver, ahora mismo ahí está firmado el protocolo del convenio de Buenos Aires, donde creo que hay ocho o nueve países, tendría que mirarlos ahora.

La idea, hubo una conferencia en Quito, a primeros del año pasado, donde auspiciado por el Ministerio del interior, se preparó por parte de tres redactores, un policía brasileño, un policía con conocimientos jurídicos, otro argentino y una inspectora de policía española, prepararon un borrador de Tratado Internacional, eso en Brasil creo que lo ha traducido y está ahora circulándolo por los países.

Aquí a México supongo que habrá llegado, porque ya no tienen que intervenir las cancillerías, la idea es que esto sea un tratado internacional, porque Ameripol, debería de tener personalidad jurídica propia, para poder firmar acuerdos de tú a tú con organismos similares, y no solamente la colaboración a nivel intra países del área, sino también poder intercambiar información con países de África, con países de Asia, y con países de Europa.

Entonces, esto está ahora en ese proceso, dentro de ese análisis está el documento principal que sería el Tratado Internacional y va a tener, está previsto que tenga tres anexos: uno, que está sacando esos anexos, porque son temas más políticos. Uno de ellos es el reglamento de sede, es decir, dónde va a estar Ameripol.

Al final tiene que estar, ahora mismo es un prototipo y está en una máquina de la policía colombiana, porque bueno, lo dejaron así y Europol puso un software, pero eso es para empezar a funcionar. Pero al final tendrán que tomar su decisión, y es una decisión política.

¿En qué país se va a situar eso?

Otro tema es cómo se va a financiar el sistema, eso es un tema que la policía tampoco quiere entrar, eso es un tema político, eso va a ser un anexo.

Y otro tema también que va a ser un anexo es el reglamento de protección de datos, que va a aplicar ahí.

Entonces, ahí se está trabajando en elaborar un borrador, lo ideal es que ese borrador se circule entre las autoridades, yo creo que un foro adecuado puede ser la Red Iberoamericana de Autoridades de Protección de Datos, entre las autoridades lo hagan, lo hagan suyo, lo discutan, que quiten lo que crean conveniente, y lo presenten como anexo al tratado y a partir de ahí, empezar a funcionar.

Los comienzos no son fáciles, esto es lento, pero en Europa también ha sido lento, pero las policías van viendo que eso les da juego, les da información y las autoridades deben estar ahí para evitar que pasen estas cosas como ha pasado el Interpol.

Entonces, es bueno aquí aplicar esto de privacidad por diseño. Ahora que se está diseñando el sistema, ahora que se está poniendo las bases en el Tratado Internacional, eso es de las autoridades, deben hacer la privacidad por diseño, que tenga estos controles, que tenga estas auditorías, que tenga estas monitorizaciones, que existan estos derechos, que existan estos mecanismos para que no pase como ha pasado con este ciudadano de Chile, donde no se sabe qué autoridad es la competente para saber qué ha pasado con él, por qué tiene una alerta roja y lleva 25 años ahí.

Eso no debe de ocurrir; eso, insisto, en los sistemas europeos, no pasa, porque desde el diseño están las autoridades de protección de datos, reconocidos en la norma como autoridades de control, y con capacidad para atender la denuncia y con capacidad para tomar decisiones.

Que, si no le gusta al sistema de turno policial, pues acudirá a los Tribunales, no recurrirá. Pero al final el Tribunal dará la palabra y dirá: “Pues este señor tiene que estar fuera o no tiene que estar”.

De ahí una serie de controles muy fuertes, que no impiden trabajar a estos sistemas en Europa, no les impide trabajar.

Pero hay controles muy fuertes en el sentido de que no existan fugas de información, hay unos blocks tremendos, blocks son ficheros informáticos donde se queda registrado quién accede a qué cosa, cuándo y qué ha mirado.

Entonces, hay luego análisis estadísticos, para ver por qué si unos policías que trabajan en la misma unidad, por qué uno de ellos tiene 50 accesos diarios y de repente aparece alguien que tiene 100.

Se sale del parámetro. No será que a este señor le están pagando para que acceda a información.

Hay toda una serie de controles, mecanismos de autoevaluación, blocks, protocolos de seguridad que tienen que estar definidos ahí, y que las autoridades tienen que controlar que se están verificando.

**Mtro. Samuel Montoya Álvarez:** Muchas gracias.

Pues respetando los tiempos, antes de cerrar, agradecer, doctora Cynthia, ingeniero Joaquín y agradecer mucho al INFO Ciudad de México, por estos importantes foros que vienen a generar muchas inquietudes que de eso se trata, se generan muchas dudas que también de eso se trata y nos dejan mucha tarea de estudio y de investigación para poder conformar, desarrollar, resguardar esta tarea tan importante que son el tema de datos personales, un foro muy importante.

Comisionada Bibi, muchas gracias; Comisionado, muchas gracias por la invitación. Saludo, con mucho gusto a la Comisionada del Estado de México y por aquí vi a los Comisionados de Baja California.

La verdad es que excelente Foro y si me permiten, alguien va a entregar o entrego unos reconocimientos, si me permiten.

Quisiera entregar un reconocimiento a la doctora Cynthia Gabriela Solís Arredondo por su participación en este Foro.

Doctora, muchas gracias, una excelente participación.

Asimismo, ingeniero Joaquín Pérez Catalán, muchas gracias por su participación, muy enriquecedora y nos deja muchas tareas y muchas dudas.

Muchas gracias.

Muchas gracias, muy buenas tardes, damos paso les entregan un presente. Dejamos el espacio para el siguiente Foro y más o menos ir a los tiempos que están marcados en el Programa.

Muy buenas tardes. Muchas gracias.

**--oo0oo--**