**Ciudad de México, 31 de enero de 2020.**

**Versión Estenográfica Panel 3. Privacidad y Gobierno Electrónico**

**dentro del Foro Internacional de Protección de Datos Personales: *Privacidad para la Persecución del Delito y la Rendición de Cuentas*.**

**Presentador:** Gobierno Electrónico.

Cedemos el uso de la voz a la maestra Marina Alicia San Martin Rebolloso, Comisionada Ciudadana del INFO, quien moderará este Panel.

**Mtra. Marina Alicia San Martín Rebolloso:** Pues muy buenas tardes a todos. Ya estamos casi cerrando actividades.

Muchas a los que siguen aquí presentes en el evento.

Mi reconocimiento, digamos, como Comisionada a mi compañera Bibiana, porque hizo posible también esto como coordinadora. La verdad es que es un placer trabajar con ese Pleno, y en particular, tengo que decirlo, de mayoría de mujeres.

Y encanta de estar aquí con este panel de expertos en esta mesa, que es Privacidad y Gobierno Electrónico el tema que nos toca abundar.

Les comento muy rápido la dinámica de la mesa. Vamos a dar 10 minutos a cada uno de ustedes, si nos hacen favor de hacer su explicación. Algunos de los ponentes traen presentaciones, como ustedes se sientan libres, si quieren pasar al pódium o aquí, empezamos a platicar.

Y luego por el tiempo, porque ya vamos encima, nos piden que no tengamos preguntas y respuestas. Pero para que no se queden ustedes con la inquietud, les pediríamos, por ahí hay papelitos que les pueden pasar, que quien tenga dudas anote sus datos y la pregunta, algún correo electrónico o algún medio donde se les pueda contestar, al ponente, al que les interesa mandárselo para que nosotros podamos también hacérselo llegar, si ustedes lo tienen así a bien, de que puedan ayudarnos a contestarla, si se hace así.

Empiezo, si les parece bien, tenemos aquí grandes expertos, no solo tenemos gente nacional que nos acompaña la Agencia Digital, sino también de fuera.

Y el orden en que haríamos nuestras inversiones, y así empiezo en la presentación, todo lo demás lo tienen, ya saben, al hacer esto tecnológico, ahí pueden ver la síntesis, que no son tan síntesis de nuestros ponentes, pero bueno, ahí pueden consultar todo, en fin, el material.

Empiezo con la doctora Laura Nahabetian, espero haberlo pronunciado bien, Brunet. Ella, que es nuestra representante de Uruguay, la Jefa de Despacho de la Unidad Reguladora y Control de Datos Personales de la Agencia justamente que trabaja la parte de gobierno electrónico en Uruguay, ella nos acompaña.

De una vez haré la presentación del resto.

Está también el maestro Pablo Corona Fraga, él que es el Vicepresidente para Ciberseguridad en la asociación de internet mexicana, que está aquí en la punta.

Está también el maestro Christian Hidalgo García, Director de la Cooperativa Sula Batsú, de Costa Rica también, que él nos hablará también de algún enfoque en casos particulares aplicados.

Y la licenciada Norma Solano Rodríguez, que ella es parte aquí de la Agencia Digital de la Ciudad de México, una nueva iniciativa que empezó del año pasado, que seguramente nos platicará. Es la Directora General del Centro de Normatividad Tecnológica.

Bueno, sin mayor preámbulo pediría yo a la doctora Laura que pudiera darnos una explicación de esto de gobierno electrónico.

Muchas gracias, Laura.

**Dra. Laura Nahabetian Brunet:** Muy buenas tardes para todos.

Muchas gracias por la invitación, en primer lugar. Un gusto compartir con mis compañeras de Panel y con todos ustedes.

Y además un agradecimiento enorme por permitirme una vez más estar aquí en México, un país que me encanta y en el que disfruto siempre que tengo la chance de venir.

Así que muchísimas gracias por la invitación.

Para empezar vamos a conversar precisamente unos minutitos sobre protección de datos y gobierno electrónico o gobierno electrónico y protección de datos.

Si ustedes ven ahí, puse gobierno electrónico entre signos de interrogación, porque en realidad a esta altura del partido yo me pregunto si lo correcto es que sigamos hablando todavía de gobierno electrónico.

Ustedes van a ver en el desarrollo de estos minutos por qué es que yo me hago este cuestionamiento, que de alguna manera se los traje ahora a ustedes.

Gobierno electrónico es mucho más que hacer portales, solemos decir, y lo identificamos con un iceberg, como ven ahí en la diapositiva. En tanto, cuando uno ve un iceberg lo que ve es la parte de arriba, la puntita que es la parte simpática, digamos.

Sin embargo, por atrás lo que lo sostiene, lo que está por debajo del agua generalmente es mucho más grande que lo que podemos ver a primera vista.

Y de esta manera, ahí no se ve la línea, pero en la parte de arriba tenemos desarrollo de sitios web y gestión de servicios online. Eso es lo que todos vemos en gobierno electrónico: las distintas prestaciones, los distintos trámites y servicios que podemos hacer con el estado, y que de alguna manera la tecnología nos ha ido posibilitando.

Sin embargo, en la parte de atrás o por debajo del agua, si fuera el caso del iceberg, tenemos también cuestiones muy importantes vinculadas con la interoperabilidad, vinculadas con la inclusión digital.

De qué nos sirve tener mucha tecnología si nuestros ciudadanos, las personas que viven en nuestros países no acceden a la tecnología; por tanto, la inclusión es muy importante.

Hay todo tipo de asimetrías técnicas y administrativas que de alguna manera necesitamos resolver para que el gobierno electrónico funcione. La infraestructura de red para que el país y su infraestructura tecnológica funcionen, la seguridad de la red es un elemento muy importante, la autenticidad, los documentos y las personas, y fundamentalmente la gestión del cambio.

Tradicionalmente cuando hablamos de estos temas decimos: la palabra la tienen los expertos, y los expertos no son quienes creen que son los expertos, sino que los expertos son los ciudadanos y los funcionarios que trabajan con este tema, que interactúan con la tecnología, porque en definitiva son ellos los que viven las buenas y las malas del intercambio con la tecnología, no quienes en definitiva hacen el planteo teórico y se sientan a esperar a ver como que en definitiva funcione.

Ahora, no se ve bien ahí, pero lo cierto es que ahí lo que decía es: eficacia, eficiencia, interoperabilidad, inteligencia, y todo bajo el tamiz democrático.

¿Qué es esto? Son los componentes esenciales de cualquier definición de gobierno electrónico. Necesitamos eficacia, necesitamos eficiencia, necesitamos interoperabilidad y necesitamos que esto se haga dentro de un marco democrático para defender derechos. Y ahí es donde nos vamos a empezar a embarcar en lo que tiene que ver con la protección de los datos.

Estas son las tradicionales prestaciones que nosotros le hemos exigido al gobierno electrónico: más transparencia, servicio 24 x 7, posibilidades de evitar lo que se llama *el costo cola*. Podemos hacer en nuestra casa cualquier trámite en cualquier momento del día, no tenemos por qué utilizar nuestro tiempo para estar haciendo trámites o consumiendo servicios del estado, sino que por el contrario, la tecnología nos permite que lo hagamos desde la comodidad de nuestra casa.

Le estamos exigiendo al estado mayor eficiencia, mayor eficacia y teóricamente la tecnología nos lo permite.

Ahora, ahí dice *digitalizar una administración obsoleta no produce una administración moderna*. No se trata de inventar, sino de reinventar. Este es un comic y aquí por el auditorio no corro el riesgo, como mis alumnos, que me pregunten quiénes son los que están en el comic, entonces por lo menos desde ese punto de vista me siento más en empatía con ustedes por edad.

Pero lo cierto es que los chicos preguntan: “¿Y esto por qué?”. ¿Por qué? Porque Picapiedra siempre estaba planteando hacer lo mismo con el tronco-móvil, mientras que del otro lado los supersónicos no, no se ve bien, por eso se los cuento, están planteando hacer una nave distinta, una forma de movilidad diferente.

Y de eso es de lo que se trata el gobierno electrónico de reinventar, no de colocarle una “e” de administración electrónico para decir: hacemos todo tecnológico, pero el *cesIto* que tradicionalmente ponía el funcionario ahora lo ponemos con la tecnología. Eso no sirve para absolutamente nada.

Entonces necesitamos empezar a cambiar, y para empezar a cambiar lo que tenemos que hacer es ponernos en una serie de premisas que nos impliquen, bueno, cómo hacemos para vincular esta tecnología y este gobierno electrónico con los derechos de las personas.

Y ahí es donde yo vuelvo a la diapositiva original que decía *gobierno electrónico* entre signos de interrogación. Realmente creo que tenemos que dejar de hablar de gobierno electrónico y empezar a hablar de gobierno de la información.

Lo que nosotros manejamos es información, información de personas, información pública, y necesitamos que además esa información sea segura.

Por tanto, nos tenemos que manejar en esta trilogía de derechos fundamentales, que son precisamente: la protección de datos personales, el acceso a la información pública y la seguridad a la información.

Y esta trilogía se maneja bajo la lógica de lo que hace ya varios años muchos académicos vienen hablando de gobierno de la información.

¿El gobierno, y ahí sí ya hablo desde el punto de vista político, cómo funciona? En base a flujos de información. Toda nuestra vida se maneja entorno a flujos de información.

Entonces, si eso es así, pues, señores, salgamos de la tecnología y vayamos a focalizar otra vez en lo importante. ¿Qué es lo importante? Las personas.

Entonces, nuestra primera premisa, la persona en el centro.

Cuando decimos que la persona está en el centro de lo que tenemos que hablar es de que la persona y el bien común son de esencias fundamentales para el desenvolvimiento de cualquier política pública. Esto parece de Perogrullo, pero también desde los tecnólogos nos siguen insistiendo, y no tengo nada contra los tecnólogos, en que lo importante es la tecnología. Eso no es cierto, lo importante somos nosotros, somos las personas.

Entonces, persona y bien común son conceptos que están presentes siempre y en todo lugar.

El profesor Nogueira Alcalá nos dice que la dignidad de la persona se constituye en el valor supremo y en el principio jurídico que constituye la columna vertebral básica de todo el ordenamiento constitucional y es fuente de todos los derechos fundamentales irradiando todo el sistema jurídico, el que debe interpretarse y aplicarse conforme a las condiciones en que dicha dignidad se realice de mejor forma.

La protección de datos entonces, y con ella la dignidad humana, está sometida a indudables riesgos e innumerables riesgos, entre los que es factible indicar por ejemplo: la libertad de expresión, la transparencia, el acceso a la información, aunque en estos casos es imprescindible instrumentar una adecuada ponderación para evitar las colisiones y fomentar la complementariedad.

Tampoco nos creamos esto de que los derechos siempre están en conflicto. Eso no es cierto, generalmente eso es un argumento para tratar de no cumplir con alguno de los derechos que tenemos que cumplir.

Los intereses la evolución del mercado, la imprescindible garantía de la seguridad ciudadana y la lucha contra el terrorismo, los procesos de globalización y la inexistencia de instrumentos adecuados que permiten otorgar garantías de eficacia al derecho frente a los diversos ataques que no tienen límites fronterizos y vienen en múltiples ocasiones de países que carecen de marcos jurídicos de protección de la privacidad, por lo que es prácticamente imposible poner en ejecución mecanismos eficaces de reacción y tutela.

La Ferriére ha indicado en este sentido, él es un profesor Argentino muy connotado, que el hecho de que el ser humano tenga las herramientas para penetrar hasta los secretos más precisos y concretos de la vida biológica no significa que la vida humana se reduzca a esos componentes materiales.

Justamente la expresión *dignidad humana* viene a expresar el reconocimiento de una excelencia en el ser de la persona humana, que abarca y accede a los componentes corporales, implicando una necesaria dimensión espiritual. Esta dimensión se expresa en las potencias espirituales, inteligencia y voluntad, capacidad de conocer y de amar.

Por eso es tan importante plantear sus dificultades frente a temas trascendentes, como la democracia, la ética mundial, los derechos humanos en tanto sustento y contenido de ambos, asumiendo liderazgos críticos que pongan la fuerza y el empuje en el cambio social, donde precisamente el centro sea una vez más la persona.

Nos vamos a la segunda premisa entonces. ¿Cuál es la segunda premisa? La tecnología es un medio. Nuevamente, dejemos a la tecnología afuera del centro del sistema, el centro del sistema somos las personas.

Y disculpen que insista tanto con esto. El tema es que yo trabajo rodeada de tecnólogos y de gente que está en la lógica de la racionalidad tecnológica. Si puede ser hecho que sea y después vemos. Y la realidad es que si puede ser hecho, enhorabuena, si no violenta y si no vulnera ningún derecho.

Entonces, lo importante es que tengamos en cuenta que la tecnología tiene que ser un medio para el desarrollo precisamente del bienestar, de la mejor posibilidad de desarrollo de la vida de las personas.

No nos confundamos que la información exista en poder del estado no significa que esta pueda circular indiscriminadamente, que se pueda trasladar de un organismo al otro sin problema, que cualquiera la pueda pedir para cualquier cosa; de ninguna manera.

Las competencias, el principio de especialidad de lograr de las administraciones públicas es fundamental si nosotros queremos poner andar a la tecnología en su vínculo con la protección de datos.

El hecho que el organismo de estadística tenga los datos de las personas no significa que hay que pasárselos al ministerio de salud. No, tal vez el ministerio de salud no necesita el tipo de datos que tiene el Instituto de Estadística, y viceversa.

Cada organismo tiene que manejarse en la lógica de su competencia y sus funciones específicas, lo demás va a vulnerar específicamente la protección de la información personal.

Las tecnologías tienen una serie de riesgos asociados, y esto lo tenemos en cuenta, todos lo sabemos, los derechos humanos se ven vulnerados en muchos casos precisamente por el malo uso de la tecnología.

El paradigma de la información tecnológica y su increíble velocidad en el tiempo y en el espacio se ha presentado como el gran cambio del mundo, así lo hemos comprado todos. Sin embargo esta transformación sin definir cómo, para qué, para quién y por qué no sirve para absolutamente nada.

No estoy en contra de la tecnología, muy por el contrario, estoy súper a favor de la tecnología razonablemente utilizada. La razonabilidad, la racionalidad, el equilibrio, como en tantas cosas en la vida, son fundamentales a la hora de interactuar tecnología y derechos humanos.

Tenemos que tener en cuenta además que es fundamental mantener el contenido esencial de estos derechos humanos, porque necesitamos, porque la política pública que estamos pretendiendo instrumentar hace que sea necesaria la utilidad, de la utilización de determinada información, eso no quiere decir que podamos vulnerar un determinado derecho humano, ni la privacidad, ni ningún otro derecho humano.

Por tanto, pensar siempre a la hora de la instrumentación de sistemas informáticos, que pueden tener que ver con gobierno electrónico o no, siempre pensar en el límite fundamental es el contenido esencial del derecho humano que se va a considerar.

Tercera premisa. Keep Calm y cuidemos nuestros datos. Definitivamente cuidemos nuestros datos. Esto es tremendamente importante. Y en esa línea nosotros tenemos un tiempo en esta parte, ya se ha hablado algo de esto, al reglamento general de protección de datos europeo, que directamente no se nos aplica, si bien la extraterritorialidad que plantea nos hace potencialmente, lo hace potencialmente aplicable a nosotros, con una serie de principios, de derechos ampliados con una serie de instrumentos, que lo que hacen es precisamente colaborarnos en la mejor utilización de la tecnología, porque tiene mucho de tecnológico el nuevo reglamento europeo, pero en combinación estricta y directa con la protección de la información personal.

En el caso de Uruguay, por ejemplo, nosotros hemos tomado algunos de los elementos sustantivos al reglamento europeo y hemos hecho una modificación normativa a nuestra Ley de Protección de Datos para que esta norma contenga algunos de estos elementos, en tanto consideramos que el reglamento europeo es un estándar internacional absolutamente válido, y que además Uruguay en la medida que tiene el estatus de adecuación con la normatividad europea, necesitamos adornar nuestra legislación para seguir manteniendo esa lógica de adecuación.

También tenemos, ya se habló algo básicamente aquí, el Convenio 108 y además el Convenio 108 PLAS. También Uruguay ha ratificado el Convenio 108 y ha adherido al Convenio 108 PLAS, y se encuentra en proceso de ratificación de este último, y también es otro instrumento internacional más que nos ayuda, que nos colabora en la protección de la información personal.

Ahora, despedidas complejas y bienvenidas saludas, ¿y esto qué es? Bueno, en la lógica de lo que les venía diciendo hoy y de que realmente considero que hay que abandonar al gobierno electrónico, hay que salirse de esa lógica que tecnólogos y economistas nos plantearon a finales de los 90 para instrumentar gobierno electrónico y decirnos que la eficiencia y la eficacia del estado era lo más importante, y lo que quede por el camino que quede. Y si lo que queda por el camino son los derechos de las personas, después vemos cómo lo arreglamos.

Definitivamente eso ya fue, eso ya no funciona más. Estamos en una lógica en la cual lo que funciona es una sociedad de redes. La sociedad está atrapada en redes de todo tipo y lo que necesitamos es que los derechos de las personas avancen positivamente.

En ese sentido, lo que tenemos que indicar es que hemos llegado definitivamente al fin de una era, ¿de qué era? Voy de vuelta, la era del gobierno electrónico.

El gobierno electrónico como concepto refleja definitivamente una época pasada, una conceptualización acuñada cuando la sociedad recién empezaba a dar sus primeros pasos en la transformación y en esa transición hacia la incorporación de automatización en el gobierno.

Y el enfoque en ese momento era el uso más efectivo de la herramienta que pudiera facilitar el trabajo de los funcionarios. Ahora en prácticamente en todas las oficinas públicas existen computadores, existen conexiones a internet, aunque tengamos en cuenta que solo la mitad de la población mundial se encuentra conectada a internet.

Entonces también tengamos cuidado con eso, los términos absolutos en estos temas nunca son buenos consejeros. Solo la mitad de la población mundial tiene acceso a la tecnología a estas características, por tanto, tenemos toda otra mitad que está absolutamente por fuera de lo que hemos dicho, son ventajas para nosotros ciudadanos conectados o ciudadanos iluminados, no por la luz del sol, claro, por la tecnología.

Luego, tenemos que hablar de una segunda razón, que es la obsolescencia, la mentalidad de las herramientas. Puede afirmarse en consecuencia entonces, a partir de lo dicho antes, que la era de las herramientas y la mentalidad de las herramientas a terminado.

En efecto, en la década de los 90, que podría catalogarse como el telón de fondo temporal del concepto de gobierno electrónico, se vivía aun en la sociedad de la información. Sin embargo, se trata de una época que ya pasó, ya fue, la transición a la sociedad en red en la que se vive hoy apenas empezaba.

Hoy vivimos definitivamente en la sociedad red y vivimos definitivamente en el marco del gobierno de la información, que es lo que nos permite darle garantía a nuestros derechos.

Tercera cuestión tremendamente importante es el desarrollo del moderno estado constitucional de derecho. Y digo a propósito constitucional de derecho, ya nos estamos saliendo por suerte del estado social de derecho, que es el que hemos transitado durante todo el siglo pasado y este siglo estamos arrancando a defender derechos humanos, y por eso focalizamos específicamente en el estado de derecho y en los derechos humanos, y hablamos precisamente de desarrollo del moderno estado constitucional de derecho.

La nueva gestión pública de los 90 y fines de los 90 ya fue. Si ustedes se fijan, cuando uno lee literatura de gobierno electrónico lo que lee siempre es: los ciudadanos y los usuarios. Los usuarios hacen esto, los usuarios hacen lo otro, los ciudadanos pueden, los ciudadanos no pueden, a tal punto que en el Uruguay en un minuto quisimos definir ciudadano para el gobierno electrónico y quienes hicieron la propuesta se olvidaron que la Constitución Nacional ya definía a los ciudadanos, pero esa es otra cuestión. Nuestros legisladores a veces son un poco particulares.

Entonces, lo cierto es que cuando se habla de gobierno electrónico se habla de esa manera. Sin embargo, cuando nosotros hablamos de gobierno de la información en la medida que focalizamos en derechos hablamos de personas, y esto hace que la diferencia sea sustantiva.

Otra cuestión, y ya para ir terminando rápidamente, tenemos que tener en cuenta el cuarto desarrollo, que es el cambio en la situación de la información en la sociedad. Las personas hablaban de la sociedad de la información, lo que tenían en mente era el crecimiento cuantitativo de la información, qué cantidad de información tenemos, cuánto se puede procesar, así como de los impactos que estos desarrollos tendrían en la sociedad.

Hoy las opiniones sobre la importancia creciente de la información tienen su base en un interés, en el derecho de las personas a saber y en el derecho al conocimiento que esto conlleva. El nuevo estado constitucional de derecho tiene ahí una importancia y una dimensión informativa tremendamente importante.

Quinto elemento, trabajo digital. La quinta razón es la transición que se está llevando a cabo a través del ambiente de trabajo digital en todos los ámbitos: las personas, las organizaciones y el sector público.

Este cambio permite diseñar sistemas interoperables en lo que la ruta de la información se puede optimizar tanto desde el punto de vista técnico como jurídico, con la finalidad, otra vez, de respetar los derechos de las personas.

Y por último, la valorización que ha tenido la seguridad de la información.

Antes cuando hablábamos de seguridad de la información o cuando le consultábamos a alguien sobre la seguridad de la información en muchos o nos miraba con los ojos desorbitados como preguntando: “¿y como para qué?”, o nos decían: “sí, tengo las cosas bajo llave” y parábamos de contar.

Ciertamente hoy en la medida en que estamos avanzando sustantivamente en lo que tiene que ver con proteger información personal y con proteger activos del estado, porque también tenemos que tener en cuenta que la información crítica del estado debe ser protegida, la seguridad de la información se ha transformado y se le ha dado un valor absolutamente superlativo, a tal punto que por ejemplo el profesor Sarenpa nos dice que el derecho a la seguridad a la información es un meta derecho constitucional en tanto precisamente garantiza tanto la protección de los datos personales cuanto el acceso a la información.

Para terminar, creo que para avanzar definitivamente en la conjunción de tecnología y derechos, ya como vieron, me salí de gobierno electrónico definitivamente, es necesario avanzar en una lógica de compromisos.

Y yo creo que aquí tenemos por lo pronto dos compromisos: el primero de ellos, lo que tiene que ver con lo que yo no denomino los equilibrios entre el conocimiento técnico, científico y los derechos humanos. Ha habido una nueva positivación de derechos, no quiere decir que los derechos no existieran, los derechos existían definitivamente, incluso nuestras Constituciones los tenían en algunos casos sugeridos por vía de su incorporación a través de las fórmulas personalidad humana o forma republicana de gobierno, como es el caso del Uruguay.

Sin embargo, ha habido un avance muy importante en términos de concretar la ejecución de esos derechos. Tenemos una cantidad, tenemos una cantidad de normas reglamentarias, tenemos normatividad internacional que nos facilita esta tutela.

La racionalidad tecnológica, y esto es parte de la vieja época, pero hay que tenerlo en cuenta a la hora de definir los compromisos vinculados con los equilibrios, nos habla de que la eficiencia, la utilidad son los valores fundamentales en términos de conocimiento científico. La innovación es tremendamente importante también; y, por tanto, en la medida en que así lo determinación, tenemos que el imperativo tecnológico nos dice: todo lo que puede ser hecho que se haga porque las posibilidades tecnológicas son irresistibles.

Y eso nos hace que se desarrollen además dos posturas contrapuestas, que además por antagónicas son negativas: la tecnofilia y la tecnofobia. La tecnofilia nos dice: vamos por la tecnología y que todo lo que la tecnología proponga que se haga, porque la tecnología es lo máximo. Y la tecnofobia nos dice: no quiero saber nada con la tecnología, fuera la tecnología.

Como todo en la vida, ni tanto, ni tampoco. Los equilibrios son lo más importante.

Entonces tenemos que avanzar en una lógica de equilibrios, equilibrios entre tecnología, desarrollo científico y también derechos.

El segundo compromiso tiene que ver con la construcción de puentes. Yo critico muchas veces a los tecnólogos, aquí lo hice un par de veces, pero si no colaboramos quienes nos dedicamos al derecho, quienes se dedican a la tecnología, quienes se dedican a la sociología y así sucesivamente a las distintas áreas del conocimiento, ciertamente vamos a seguir en problemas y no vamos a avanzar en términos de desarrollo propositivo.

Por tanto, es muy importante que se tiendan puentes en términos democráticos para poder funcionar efectivamente en el marco de la pluralidad de conocimiento.

Y para terminar, efectivamente vamos por la efectividad de los derechos. El profesor Germán Bidart Campos, de la Argentina, profesor constitucionalista, dice que en nuestros sistemas constitucionales los derechos no se constituyen en la norma positiva, sino que ella solo los asegura, los respeta, los garantiza y los promueve. Los derechos humanos emanan de la dignidad humana; y por tanto, ahí tenemos ciertamente el imperativo de la protección de los datos personales, porque tenemos el imperativo de la protección de la persona.

Muchas gracias.

**Mtra. Marina Alicia San Martín Rebolloso:** Muchas gracias, Laura.

Clarísimo, me parece que, sí, digamos, cambias el concepto, me gusta mucho, de gobierno electrónico a gobierno de la información. Pones en el centro a las personas.

Y ahora vamos contigo Norma para que nos platiques aquí en México un poco, y creo que esa parte de la trilogía que dices de datos, acceso y cómo la tecnología te ayuda en la parte de seguridad de la información es fundamental, y eso es una parte que ahora se está construyendo aquí.

No podemos tratar de hacer muchas cosas si no cuidamos los derechos, y este equilibrio me gustaría que nos lo compartas querida Norma, respecto de la experiencia mexicana.

**Lic. Norma Solano Rodríguez:** Muchas gracias a todos; muchas gracias al INFODF por la invitación a la Agencia Digital de Innovación Pública de la Ciudad de México, es un placer y un honor compartir con brillantes panelistas, expertos en la materia.

Bueno, la exposición de la doctora Laura fue muy clara, muy amplia, muy enriquecedora.

Yo les voy a hablar un poco, y además me da mucho gusto compartir con compañeros de Unidades de Transparencia, porque además de las funciones en materia estrictamente de normatividad tecnológica, también siempre compartimos los temas de transparencia.

Les voy a platicar qué se está haciendo en la Ciudad de México en temas de gobierno electrónico, gobierno digital.

La Agencia Digital de Innovación Pública es un órgano que se creó en la Ley de Operación del 31 de diciembre del año pasado, y es un órgano que nace en el 2019. Uno, tiene varios ejes, varias agendas importantes para la Ciudad de México, una de ellas es reducir las brechas digitales.

Hay una política de conectividad importante en la Ciudad de México sin la cual una parte del proceso de digitalización que tiene el Gobierno de la Ciudad carecería o no estaría suficientemente reforzado, es la conexión en puntos gratuitos wi-fi de la Ciudad de México.

Sabemos todos que los postes de las cámaras de videovigilancia aproximadamente 13 mil 600 tienen conexiones de puntos gratuitos de la Ciudad de México, este año habrá otros 3 mil más en otros programas de cámaras en las calles de la Ciudad de México.

Este es un eje del Gobierno de la Ciudad de México.

Otro eje es la racionalización y uso, adquisición de las tecnologías de la información. La Agencia Digital dictamina todas las adquisiciones que se llevan por parte de los entes públicos de la Ciudad de México.

¿Qué buscamos? Que las adquisiciones de tecnología primero tengan ciertos requisitos como códigos abiertos, que se cuiden costos y sobre todo que aquellos desarrollos que puedan ser hechos en casa no se erogue ningún recurso más a cargo de los entes públicos.

Y un tercer y gran eje de los trabajos de la Agencia es la digitalización. Existen hoy 996 trámites administrativos, de los cuales 21 están digitalizados. La verdad es que la Ciudad de México ha avanzado no tan rápidamente como quisiéramos, de esos 21 trámites digitalizados al día de hoy 12 fueron desarrollados el año pasado por la agencia, y tenemos un plan digital para este año muy ambicioso, básicamente la premisa es que se muevan los documentos, no las personas.

El 7 y 9 de enero de este año se publicaron dos ordenamientos legales, que a los sujetos obligados nos van a cambiar la dinámica y las obligaciones que tenemos en materia de digitalización y simplificación administrativa, que nos pone un reto mayor, que tiene que ver con el tema de la privacidad.

Uno de ellos es la Ley de Mejora Regulatoria, que establece en alguno de sus dispositivos la obligación de crear expediente electrónico. Y la Ley de Seguridad Digital, que es un ordenamiento que establece las bases que señalan la obligación de todos los entes públicos de simplificar todos aquellos trámites que tengan oportunidades de simplificación, estaremos obligados a identificarlos y a hacerlo, y además de pasarlos por un proceso de digitalización.

La idea es que la totalidad de los trámites y los servicios que se solicitan al Gobierno de la Ciudad de México pasen por un tema de digitalización de principio a fin.

Lo que queremos es que no vayamos entregando documentos ventanilla por ventanilla a cada ente público, que no sea el ciudadano el que mueva y vaya perdiendo y vaya entregando documentos si el Gobierno ya los tiene.

No teníamos este marco jurídico, la Ley de Seguridad Digital es un proyecto que se estará llevando a cabo este año, y que básicamente tiene algunos ejes: uno, la creación de una ficha electrónica, que tiene que ver con un catálogo de documentos que va a señalar en qué dependencia se encuentra cada documento, dónde está tu INE, dónde está tu Acta de Nacimiento, donde está tu licencia, de tal forma que identifique, el ciudadano pueda saber: uno, crear un expediente electrónico y saber identificar dónde está cada uno de los documentos, de tal forma que el Gobierno no le vuelva a pedir al ciudadano un documento más que ya obre en sus archivos.

Otro elemento es la creación de un expediente electrónico. No estamos pensando en un expediente electrónico único, la práctica internacional establece que una de las mejores prácticas es que no concentremos la información, los datos personales en una sola base de datos. Eso no solamente la hace más vulnerable, sino que en caso de que existiera algún riesgo el daño de la vulneración de esa información sería mucho mayor.

Entonces de lo que se trata es de que las bases estén separadas. Este tema de los desarrollos por diseño, desde un inicio el código fuente debe vivir y albergarse en una base de datos distinta de donde conviven las bases de datos, en donde se encuentran los datos personales que recaba cada ente público.

Y aun en las mismas bases de datos no nos podemos permitir integrar un solo expediente en donde obre toda nuestra información, datos patrimoniales, fiscales, de salud, familiares, aun el gobierno desde atrás, resolviendo los trámites, servicios de los ciudadanos, no podemos tener una sola base de datos.

Si hubiera una vulneración debiéramos tener los siguientes elementos para que no accedan a la totalidad de nuestra información. Pudiera ser un dato aislado, pero no nuestra vida fundamentalmente que tiene el gobierno en sus distintos entes administrativos.

Este expediente electrónico la única forma en que se va a poder hacer realidad es una serie de desarrollos tecnológicos que la ley establece como un riel de interoperabilidad, y es el gran reto que tiene la Agencia Digital de Innovación Pública para este año y que, desde luego, se requiere todo el apoyo y coordinación con todos los entes públicos de la administración pública.

Pasa por crear un sistema que me permita hacer consultas puntuales a cada uno de los registros y expedientes que tiene cada ente público. Cada ente público tiene un expediente integrado, SEMOVI tiene integrado un expediente por trámites, licencias; las Alcaldías tiene un expediente, SEDUVI tiene un expediente, de tal forma que a partir de que el ciudadano identifique con su ficha ciudadana dónde están los documentos y qué documentos tiene cada dependencia, yo puedo decir: “te autorizo para que tú SEDUVI hagas una consulta puntual con una Alcaldía”.

Por supuesto, y aquí ya es un tema no solamente de cumplimiento de la normatividad en materia de protección de datos personales, que tiene que ver con la recabación de datos, que sean los suficientes, no excedidos, los necesarios, para el cumplimiento de las funciones, tiene que ver con que sepan los ciudadanos con toda claridad para qué se va a tratar las posibles transmisiones que se hagan de los datos personales y de las remisiones, y desde atrás, los documentos jurídicos que necesitamos suscribir los entes públicos para que haya una certeza jurídica y seguridad hacia los particulares.

Hoy en la Agencia hay una preocupación permanente, somos una fábrica de software de la Ciudad de México y, como bien lo decía la doctora, hay un tema entre técnicos y abogados, que es muy complicado, los técnicos piensan permanentemente en la creación de soluciones tecnológicas, pero desde el inicio de la creación de la Agencia, y por supuesto con el acompañamiento del INFODF permanente no lo podríamos hacer, es hacer mesas de trabajo de diversas especialidades.

Debemos estar permanentemente los abogados de la mano con los tecnólogos para que haya no solamente la obligación, no solamente que entiendan que hay obligaciones normativas de protección de datos personales, que no solo desarrollan software y no hay bases de datos para que los hagan posibles, sino que en las bases de datos hay datos personales, datos fundamentales de las personas y que pueden ser vulnerables en algún momento, y el riesgo al que se podría poner a las personas es muy grande, y que tiene que ver con sus derechos fundamentales.

Yo entrego un dato personal a un ente público porque requiero un trámite específico, requiero un servicio, requiero una pensión, requiero una beca, y eso por supuesto que no autoriza a los desarrollos a acceder a esa información.

Entonces no solamente es que sepan y que haya consciencia del cumplimiento de la ley, sino un tema ético de los propios desarrolladores y de todo el personal, de todos los servidores públicos del cuidado de los datos y de la información a la que se tiene acceso.

Por eso además hay medidas de seguridad de la información que se han tomado desde la Agencia Digital para que, por supuesto, no cualquier servidor público puede acceder a toda la información. Si accede a datos personales solamente serán aquellos indispensables para una función. Las personas desarrolladoras que tienen el desarrollo no necesariamente acceden a bases.

Y el otro tema es que la Agencia Digital es un desarrollador de software, es como si ustedes contrataran a una empresa de desarrollo, pero los entes públicos son quienes tienen la atribución legal de recabar los datos personales, de tratar para las finalidades establecidas en sus sistemas, que no necesariamente acceden.

Hay una idea de que la Agencia Digital de Innovación Pública concentra las bases de datos de todos los ciudadanos y de todos los entes públicos, y eso es hoy un mito, la Agencia Digital lo que hace son desarrollos que pone a disposición de los entes públicos para eficientar el desarrollo de sus funciones.

Y, por otro lado, fundamental que sepamos que cada ciudadano que entra a una plataforma en la Ciudad de México tenga el aviso de privacidad, el largo, el corto, un aviso de privacidad muy robusto para que sepa exactamente qué datos estamos recabando y cuáles son las finalidades y a quién posiblemente vamos a transmitir.

Hay un elemento muy importante en la Ley de Seguridad Digital de la Ciudad de México, la Agencia, dada la naturaleza de sus funciones, debe, esta obligada por ley a solicitar cada dos años auditorías a la Contraloría General, a la Secretaría de la Contraloría General de la Ciudad de México y/o a Comités expertos en materia de ciberseguridad.

De tal forma que nosotros a diferencia de Uruguay, por ejemplo, son temas aun nuevos, 21 trámites digitalizados. Eso en términos macros es muy poco, y queremos un gobierno digital, que las personas puedan iniciar un trámite desde inicio a fin en un celular, en una plataforma única, en una ventana única, y que el gobierno tenga que hacer desde atrás lo que tengamos que hacer para resolverlo.

No pidamos más datos de los que no necesitamos, no podamos más documentos si ya obran en nuestros archivos, es un problema del gobierno organizar sus datos, por supuesto que pasa por retos en materia de archivos, de documentos digitales, pasa por un tema de cómo nos coordinamos los sujetos obligados para la creación de sistemas de datos personales, cuando la Agencia desarrolla un software también asumimos responsabilidad de seguridad al menos de la infraestructura de hardware.

Los servidores, mucha de la información de los entes públicos se aloja en los centros de datos de la Agencia, que no implica que accedamos a esa información, pero tenemos responsabilidades legales y técnicas que cumplir.

Entonces es un reto colaborativo de todos los sujetos obligados con la Agencia. Esta Ley que empieza a operar este año nos trae muchos retos y sobre todo con un tema de confianza.

Los ciudadanos dan datos por ejemplo biométricos a algunos clubes deportivos, pero tienen un temor a dar un dato personal y más de esa naturaleza al gobierno.

Entonces al ciudadano le debe quedar claro que el gobierno tiene pleno, para empezar está regulado, está todo el tiempo vigilado por los órganos garantes y por organizaciones de la sociedad civil, que hay un compromiso y una obligación de cumplir la ley, pero también hay un criterio ético del uso de la información e inclusive de elementos, políticas de seguridad de la información que se están estableciendo no solamente para la Agencia, sino para el gobierno, para las unidades administrativas en general.

Entonces los retos son muchos, el ciudadano debe saber que la tecnología está ahí, que es un facilitador, nos permite abrir otros derechos, exigir otros derechos fundamentales, como la rendición de cuentas, la transparencia no es un enemigo y tenemos que permear en la sociedad, uno, para que las usen, porque de nada nos sirve estar en una fábrica de software todo el tiempo desarrollando plataformas que no van a utilizarse y que se las apropian, que se las apropien, que las hagan suyas y que sepan que es un mecanismo, es un medio de exigir al gobierno trámites más eficientes, más ágiles, de verdad, el sufrir de una persona, una mamá que tiene que salir del trabajo y tiene que dar 10 vueltas a una unidad administrativa del gobierno, en términos cuantitativos, en términos económicos y personales es mayor.

Entonces los retos que tenemos como dependencias, como órganos de la administración es mucha, pero tendremos que caminar acompañados del INFODF para lograr y recuperar la confianza en la ciudadanía, y es una política además que está implementando la Jefa de Gobierno.

Esto es una realidad, no hay vuelta atrás y más bien tenemos que marchar por el camino de implementar todos los elementos que sean necesarios para la seguridad de la información, y para que los ciudadanos sepan que su información está segura y que no va a ser excesivo aquello que se recabe.

Muchas gracias.

**Mtra. Marina Alicia San Martín Rebolloso:** Muchas gracias, Norma.

Ya ella dejó muy claro el alcance de la Agencia Digital. Nosotros como INFO hemos trabajado luego en mesas, por eso retomo el enfoque, que me encantó, que diste tú, de decir: los derechos en el centro y las personas en el centro, porque sí, efectivamente, nos ha pasado, y lo sabe aquí Norma, en las discusiones, que luego ya: rápido, rápido, rápido, y más que correr hay que tener mucha seguridad en lo que estás dando.

Parte de la construcción de la confianza viene, y justamente metería un elemento adicional, en cómo comunican que efectivamente tienes las medidas de seguridad, que sí hay el aviso de privacidad.

En alguna discusión que tuvimos, que efectivamente ellos cuentan con las medidas de seguridad, como que da uno por sentado que está ahí y no lo ve uno atrás, y entonces les da medio igual, pero el ciudadano se siente más tranquilo si sabe si está segmentada su información, quién la ve, quién no la ve.

Entonces si logras comunicar eso, para qué es y efectivamente que tengas plena claridad en el aviso para qué la voy a ocupar, quiénes son los responsables, que esa claridad también en la articulación que hemos sugerido nosotros como INFO que tengan las distintas entidades, SEMOVI con ustedes, Consejería con ustedes, en fin, a los que les toca, eso creo que ayuda mucho en este pian pianito de construcción, digamos, efectivamente de un gobierno de información más que gobierno electrónico.

Y sí, la idea es súper buena, por supuesto que en eso estamos dando el pinino aquí en la Ciudad, y nosotros como INFO cuenten con eso, para eso están también las famosas, estas evaluaciones de impacto a la privacidad, también importante que se hagan.

Bueno, gracias por dar la primera introducción querida Norma.

Y vamos justo, como están viendo ustedes, la intervención de los panelistas que nos acordamos cómo es para que vayan teniendo de lo más general a lo particular con una muy buena idea.

Y ahora le pediría a Christian que nos puedas platicar un poco, que tú vas a entrar, entiendo, a temas también del Big Data por ahí que mencionaron y otros puntos.

Muchas gracias.

**Mtro. Christian Hidalgo García:** Bueno, muy buenas tardes a todas y todos.

De verdad agradecer la invitación a este evento y estar con estos compañeros que como los he oído, he oído sus presentaciones, creo que vamos en una misma línea de pensamiento.

Yo pertenezco a una organización de la sociedad civil y tenemos alrededor de 15 años de trabajar temas de sociedad y tecnología. Dentro de ese proceso con colaboración del estado hemos empezado a trabajar evaluaciones ex post, pero evaluaciones ciudadanas.

Esas evaluaciones ciudadanas son evaluaciones de tres, cuatro, cinco meses, dependiendo, donde lo que nos enfocamos es en ver cuáles son los efectos y los impactos que están generando los procesos de automatización, los procesos de protección de datos en la ciudadanía.

Yo no voy a entrar tanto en la parte de gobierno electrónico, gobierno digital, sobre todo porque creo que la compañera lo tocó bastante bien, y yo concuerdo con ella. Y tenemos un enfoque donde partimos que el ciudadano es el centro, es el que tenemos que cuidar y además no debemos cuidar solo los datos que tiene ese ciudadano, sino que debemos de cuidar al ciudadano en sí, debemos saber que todo el proceso que se esté realizando en realidad le esté generando un beneficio.

Entonces ese es el enfoque con el que nosotros hemos estado trabajando.

Y después de dos años de investigación en varias entidades de Costa Rica, algunas de Guatemala, otras del Salvador, lastimosamente tuvimos que sacar de la investigación al de Nicaragua, porque nos sacaron, no nos dejaron seguir con el proceso. Yo básicamente lo que les voy a exponer son resultados, o sea es lo que nosotros nos hemos encontrado en el día a día cuando los procesos se están aplicando.

En el caso de Costa Rica sí quiero ser, digamos, para que se entienda por dónde va el proceso, es que partiendo de una ley que se estableció en 1997, que se empezó a ejecutar en realidad en el 2008, se le obliga a las entidades del estado, literalmente se le obliga, a entrar en proceso de automatización.

Entonces dentro de esos procesos de automatización algunos van bastantes avanzados, algunas de las entidades con las que yo he trabajado están en un proceso comenzando, otras en un proceso medio, como el sistema judicial, y otros en un sistema muy alto, como el sistema de salud, que en este momento tiene automatizado todo su proceso de salud, al nivel de que cada ciudadano en su celular tiene acceso a todo su expediente electrónico y tiene acceso a todos los servicios, y ya se ha quitado todo el proceso de papel, donde van a sacar su cita, reciben sus medicamentos, ven su ruta quirúrgica, etcétera, todo lo ven en un proceso automatizado.

Eso, como ustedes se imaginarán, ha llevado gran cantidad de cambios.

Ese enfoque ciudadano, lo primero que quiero que recordemos es cuál es el ciudadano con el que estamos trabajando actualmente. Dentro del sistema digital todavía vamos a seguir con las diferentes problemáticas, como analfabetismo digital, como derecho digital, brechas de género, brechas de edad, nivel educativo, y seguimos manejando conceptos sumamente erróneos, como el de nativos digitales y pensar que la gente porque nació en esta época tan tecnológica ya viene aprendida, viene con chip de seguridad, que eso se da infinidad de veces, pero sí es un ciudadano que en los últimos años ha ido cambiando, ya no es un ciudadano, como decía la compañera, que no tiene un conocimiento de lo que está pasando y lo que pasa con sus datos, es un ciudadano que le es tan importante la divulgación de la información a la que tiene derecho, pero que ha empezado a entender que es necesaria la protección de aquella información a la que no se tiene derecho a acceder.

Es un ciudadano más involucrado, pero que no protege lo que no produce, con lo que no trabaja y con lo que no entiende. Es una ciudadanía que solicita el derecho al dato, eso es algo muy importante, lo empieza a pedir, y aunque todavía falta mucha expropiación sobre la cultura de protección de datos, sí, podemos decir que actualmente ha habido un cambio en los últimos cinco años de ese ciudadano con el que estamos interactuando.

Ahora, dentro de los procesos que hemos trabajado en este momento, trabajando con las instituciones nos hemos encontrado casi en todas las evaluaciones que yo he realizado y con todos los procesos que he trabajado en conjunto con las instituciones hay ciertas características que siempre he encontrado. La primera es el poco interés de las instituciones en la existencia de la responsabilidad demostrada más que por el cumplimiento a la norma.

Ahora, lo que sí es positivo es que ese es un proceso que ha venido cambiando. Como decía el compañero ayer con las auditorías, con el proceso de las auditorías y cuando nosotros hemos llegado a trabajar, la primera vez definitivamente no nos quieren ver, no quieren saber qué estamos haciendo ahí y no quieren tener ningún proceso de evaluación, ni saber qué está sucediendo, pero normalmente después, cuando empezamos a trabajar en conjunto, normalmente nos siguen buscando y más bien nos terminan pidiendo que les ayudemos a muchos de los procesos que están llevando.

Eso creo que es algo sumamente positivo, porque aunque las entidades tienen ese miedo a involucrarse y a entender cuáles son los efectos que está teniendo la ciudadanía sí están generando cambios.

El segundo es la necesidad de intentar hacer interpretaciones al principio de ecuación y el fin, sobre todo cuando reciben, cuando se dan cuenta que pueden utilizar los datos de sus bases para diversos fines, sobre todo justificando bajo el argumento que se convertirán en un beneficio hacia la población.

Y normalmente lo justifican bajo la lógica de la relevancia pública en la generación de política pública.

Básicamente cuando una entidad se da cuenta la cantidad de datos que tiene en su base y lo que puede generar con esa información normalmente olvida que esos datos se generaron por un fin, y siempre normalmente van a tratar de hacer más de lo que estaba ya estipulado.

Eso es casi una lógica, no digo que todos lo hagan, pero es una situación que normalmente se da.

Segundo, un conocimiento, del conocimiento informado, pero de poca claridad en el manejo del consentimiento en menores de edad y personas con alguna discapacidad. Eso nos llamó sumamente la atención, porque es increíble cómo a la hora de aplicar la normativa con menores de edad y con personas con discapacidad, aunque la normativa sea clara, no saben cómo llevarlo a la aplicación.

En el caso de Costa Rica por ejemplo hay una ventaja, que el trato de menores de edad es de 18 años, igual en la normativa, pero por ejemplo en el caso de Europa a la normativa para consentimiento informado ha ido variando, hay países que tienen consentimiento informado desde los 13 años en adelante, hay otros de los 14, eso es aplicado por cada país.

Y normalmente a la hora, aunque conozcan la normativa y tienen que aplicarla en ese sentido, no saben cómo hacerlo, y es donde hemos encontrado que se dan más vulnerabilidades.

Lo siguiente es dejar la responsabilidad de la protección de datos personales enteramente en el personal de informática, y como este en la mayoría de los casos tiene escaso o nulo conocimiento de la generación especifica de protección de datos.

Yo les podría contar una anécdota, que cada vez que yo llego a ver un proceso de cómo están trabajando, normalmente me sientan con todos los informáticos. Y para darles un ejemplo, cuando estaban sacando el App de Ledus, que es el App de Salud, yo vi el App, era 2.0 y me senté con todos los informáticos: “bueno, tienen que hacer un App 1 punto, algo, o tienen que cambiar esto, vamos a reunirnos con todas las personas, con grupos de personas con discapacidad para hacer pruebas, porque esto ni siquiera tiene accesibilidad, ni siquiera tiene medidas de seguridad”.

Entonces, lo pensaron muy bien técnicamente, pero no pensaron en la población que iba a trabajar. O sea, pensar una App para salud no contemplaba a personas con discapacidad, no tiene sentido.

Igual hay que cambiar, hemos notado que hay que cambiar a los profesionales que están trabajando, hay que generar un nuevo profesional que está entrando dentro de estos procesos en las instituciones, un profesional que tanto comprenda parte de la parte informática, pero que también conozca de la protección de datos.

Yo soy profesor universitario y a mis estudiantes de ciberseguridad, siempre que me toca trabajar con ellos, no me quieren, porque dicen que yo les pongo todas las restricciones de todo lo que técnicamente ellos hayan hecho también, y les digo: “pero es que no han pensando en la población a la que están trabajando”.

Y posterior a las evaluaciones prácticamente en todos los casos, una de las principales vulnerabilidades se encuentra en los funcionarios base de las instituciones y además instruyen inadecuadamente a la población con la que interactúan sobre la protección de sus datos personales.

Lastimosamente hemos olvidado que aquella persona que recibía al usuario o al ciudadano en la caja y que ahora la estamos pasando al proceso de automatización, esa persona tiene que entender, porque es a la primera persona que le van a preguntar. Es más, a la primera persona que le preguntan es al guarda y el guarda no sabe lo que está pasando, y normalmente eso nunca se hace.

Ahora bien, sí hay una gran ventaja que hemos encontrado para ver vulnerabilidades con los procesos de automatización, que es la trazabilidad del dato. Ahora es mucho más fácil encontrar esas vulnerabilidades con los procesos de automatización, porque encontramos específicamente en qué momento y quién incurrió.

Ejemplo, en los servicios de salud vimos un caso específico de un familiar que quiso, un familiar que era enfermero, y quiso averiguar algo de un familiar que tenía un problema de salud mental, pero al momento de hacer todo el proceso jurídico fue exacto el momento donde se pudo localizar donde había ingresado a revisar esa información, y además de que no debía haber ingresado a revisar esa información por las funciones que tiene.

Esto de los funcionarios me parece sumamente importante porque, por ejemplo trabajando con el Poder Judicial y trabajando con el sector salud, quienes son funcionarios que ya por su formación fuera de la automatización tiene un bagaje de cómo deben proteger la información, es increíble la cantidad de vulnerabilidades que generan.

En el sector salud las enfermeras dejaban los expedientes abiertos, se pasaban las claves. Los médicos eran los primeros que le decían al mismo usuario durante, perdón, al mismo ciudadano durante la atención: usted no debería de hacer esto o no haga esto, o hágalo de tal manera.

Entonces, si no trabajamos con esa población, por más normativa que tengamos, no vamos a poder generar un cambio en la población que queremos.

Esto nos lleva a solicitar siempre con las instituciones que hemos trabajado, aparte de todos los cambios técnicos que se puedan encontrar, que es indispensable la alfabetización del dato hacia la ciudadanía. Esto implica no solo saber qué datos se están tomando, quién los toma y para qué, sino también el derecho de saber leer e interpretar el dato para su propia toma de decisiones, y esto implica todo un proceso de formación ciudadana que las entidades deben empezar a tomar.

El segundo es un cambio completo, así como hemos buscado un cambio en la cultura de la ciudadanía, es necesario generar un cambio completo en una cultura organizacional de las entidades, donde en la mayoría de los casos proponemos procesos de gestión de cambio enfocados a la adaptación de los procesos de adopción de tecnologías digitales, pero incluyendo la protección de datos personales como un eje transversal.

Ciertamente les decía que al principio no nos querían ver, cuando llegábamos a trabajar a pedir los datos, pero sin embargo estas evaluaciones le han servido en muchos casos a las entidades para poder justificar y pedir recursos para poder generar esos procesos de gestión de cambio, que entiendo no son ni rápidos, ni de bajo costo.

Por ejemplo, el proceso de hacer el cambio en este caso para el sector salud que se ha planteado, que estamos hablando de 10 mil trabajadores, es un proceso de gestión de cambio que está planteado a mínimo tres años; o sea no es algo que se vaya a hacer de un día para otro.

Ahora bien, cuando me invitaron a este foro específicamente en el tema de delito y sobre organismos judiciales, yo sí voy a plantearles una perspectiva muy desde la sociedad civil, me atrevería a dar algunas sugerencias, no voy a profundizar en ellas excepto en la última, por sus características que aplica a todas las entidades, no solo a organismos judiciales.

En el proceso de organismos judiciales lo primero es generar una normativa específica para el tratamiento de datos personales por parte de las fuerzas de seguridad, algunas de las medidas que se podrían incluir serían: la inclusión de plazos para la supresión de los datos personales o para su revisión periódico a fin de evaluar la pertinencia de su almacenamiento, la distinción entre los datos personales recabados en base a hechos de aquellos que pueden derivarse de las apreciaciones personales, opiniones, juicios de valor propios de los agentes que realizan las tareas de seguridad.

Otra cosa que hemos encontrado en la práctica es que es necesario, en beneficio del ciudadano, es necesario eliminar o mínimo restringir al máximo la utilización de herramientas de hackeo estatal para la investigación y vigilancia.

Como tal, el hacking gubernamental es quizá la técnica de vigilancia más intrusiva, debido a la gran cantidad de datos íntimos que se almacenan en nuestros equipos y debería utilizarse solo cuando los medios alternativos de investigación se revelen notoriamente ineficaces y generando las máximas garantías posibles, estableciendo los requisitos de transparencia necesarios.

Proteger el cifrado de las comunicaciones. Hemos notado que no solo en mi país ha sido una tendencia, y creo que en muchos países se replica; la adopción del cifrado de punto, punto por parte de los servicios de mensajería constituye un elemento esencial para asegurar.

La privacidad de las comunicaciones. A pesar de estos beneficios distintos gobiernos del mundo están haciendo esfuerzos por lograr que las compañías permitan accesos exclusivos o puertas traseras a su sistema.

Una de las cosas que nosotros sugerimos desde la parte de ciudadanía, pensando en el beneficio del ciudadano, es que no se permita estas restricciones.

Lo otro también es buscar un equilibrio entre el estado y el ciudadano. Cuando nosotros le generamos ciertas características al estado para que pueda observar o ingresar en la privacidad de los ciudadanos, debemos empezar a trabajar en una réplica para que el ciudadano pueda equiparar esas fuerzas y no generar una fuerza superior de parte del estado.

Y finalmente que tal vez es un tema específico que quisiera tratar, es contemplar los peligros de los algoritmos, de los procesos de Big Data e inteligencia artificial en la generación de la política pública.

Esto no aplica solo en el caso de entes de seguridad, sino que aplica para cualquier ministerio que esté pensando en el manejo de datos a través de Big Data.

Nos hemos dado cuenta que cada vez que llegamos a una institución obviamente el informático lo primero que le dice es: estamos en una era donde ahora hay que trabajar, ahora se puede procesar, se puede hacer minería de datos, se puede hacer Big Data. Entonces debemos entrar en eso con las bases que tenemos.

Ahora, la inteligencia artificial está en el centro del interés debido al impacto político, económico y social que su desarrollo pueda tener para las poblaciones; sin embargo, si las condiciones de aplicabilidad de estas tecnologías son defectuosas las consecuencias pueden ser más negativas o positivas, inclusive generar procesos que aumenten la inequidad de las personas.

Debido a que en varios casos son los datos personales la fuente que permiten el funcionamiento de estos sistemas, urge adoptar una política pública respetuosa de los derechos de los individuos.

Si los datos personales se utilizan para tomar decisiones automatizadas sobre las personas se debe de poder explicar la lógica detrás de su proceso, y es importante empezar a normar la transparencia de los procesos.

Aquí tal vez quisiera explicar cómo funciona, no voy a entrar en un detalle técnico, pero quisiera explicar por qué nosotros pensamos que es importante empezar a normar esos procesos de Big Data, porque además es una tendencia en toda la política pública. Yo no conozco prácticamente a ningún político de ningún país que dentro de sus propuestas no sugiera que esto le va a generar un beneficio para hacer predicciones, lo cual es cierto, siempre que el dato se trate adecuadamente.

Ahí podemos ver un gráfico, donde se ve que la primera parte es la creación del dato. Para poder hacer un análisis algorítmico es importante entender cuál es la situación o la problemática que nosotros queremos solucionar. Eso quiere decir que nosotros no podemos agarrar datos de cualquier lado y extrapolarlos para trabajar otra solución.

Lo siguiente es que es indispensable para que el algoritmo y en los procesos de inteligencia artificial no creen sesgos, es la calidad del dato. Si el dato no tiene calidad per se va a crear sesgos.

Y normalmente lo que hemos detectado es que una vez que las bases de datos ya están en manos de las instituciones muchas veces no se está valorando la calidad del dato antes de entrar en un proceso de análisis de Big Data o de inteligencia artificial.

Una sugerencia que siempre hemos dado es desarrollar la infraestructura y experiencia local versus empresas privadas. Yo les podría varios casos donde lo que se hace es contratar empresa privada, normalmente Microsoft porque desarrolla estos procesos, pero en realidad esto debería desarrollarse con equipos internos de cada ministerio.

Definir y adoptar prácticas de transparencia, participación ciudadana y rendición de cuentas en esas etapas de desarrollo e implementación.

Ahora bien, tal vez para ser muy breve, para poder hacer un análisis se tiene que tener equis cantidad de datos y después tiene que entrenar el algoritmo, según lo que usted quiere averiguar, según la problemática, y después le ingresa esos datos.

Entonces, primero tenemos que tener calidad del dato y después tenemos que ver cómo estamos construyendo el algoritmo. Si el algoritmo no se construye adecuadamente, todos los sesgos que puedan existir, el algoritmo los va a mantener; o sea los algoritmos son productos culturales al fin y al cabo.

Entonces pensar equívocamente que al trabajar con un análisis de Big Data o con algoritmos estamos quitando todos los sesgos que se puedan tener al trabajar con personas, eso es incorrecto.

Después definir criterios para evaluar el riesgo de distintos modelos e implementaciones. Normalmente cualquier proceso en el momento que se está construyendo el algoritmo está blindado. Cualquier empresa privada que desarrolle para el estado un proceso de este tipo lo va a blindar, porque una entidad estatal lo que busca es un beneficio o una información, una entidad privada lo que busca es vender un servicio, y por lo tanto va a proteger ese proceso de información. Pero si nosotros no sabemos cómo se está trabajando ese proceso, vamos a generar sesgos muy fuertes.

Les puedo dar un ejemplo, en la Provincia de Salta, en Argentina, que hizo un acuerdo con Microsoft para trabajar con población de mujeres embarazadas, y lo que le dice Microsoft es: Okey. Él va a agarrar todos los datos y va a poder predecir para que se pueda tomar política pública para trabajar con mujeres jóvenes que quedan embarazadas.

Ahora bien, el resultado es que como se construyó el algoritmo era inadecuado, generando una serie de sesgos, que al final lo que estaba construyendo es que se estaba logrando llegar a ciertos grupos etarios específicos y se les estaba cambiando la política o el proceso de uso, partiendo de que ellas eran propensas a quedar embarazadas, lo cual era una violación directa a su privacidad.

Y también hay casos, por ejemplo, en Brasil donde se empezó a aplicar, que el 90 por ciento, se empezó a aplicar a través de reconocimiento facial para detectar focos de delincuencia, pero curiosamente como también estaba construido mal el algoritmo, generando ciertos sesgos, el 90 por ciento de las personas que detectaba eran personas afrodescendientes. ¿Por qué? Porque ya se había generado con un sesgo.

También tenemos el caso, que por tiempo no voy a entrar tanto, que es el del Software de Presspull, en Uruguay, que tal vez ahí Laura lo conozca, que también fue una situación que se llevaba en esa línea.

¿Qué sugerimos nosotros en esto? Realizarse la implementación legítima y además de procedimientos y resultados, y revisar la procedencia del dato, la creación de la base y la calidad del dato.

Los algoritmos y los modelos de IA se comparten de acuerdo a las reglas, bajo las cuales fueron programadas, y hay que tener claridad si el resultado deriva de una decisión automatizada o en una interpretación que genera información para la interpretación.

Bueno, aquí casi no se ve la imagen, pero lo que les estamos poniendo acá es que hay dos momentos: primero, hay que saber cómo se construye el dato; y, segundo, hay que saber cuál es el resultado que buscamos cuando manejamos inteligencia artificial. Si es un dato automatizado, o sea que tome decisiones automáticas, o si lo que me está generando es información para que las entidades puedan tomar decisiones.

Esa diferenciación sí debe estar muy clara, porque hay infinidad de peligros cuando nosotros, si no sabemos cómo se está construyendo y con qué datos se está trabajando esa inteligencia artificial y lo que estamos buscando son procesos de automatización, esos procesos de automatización pueden generar una serie de problemas y de sesgos, como que a una persona se le quite la pensión, como que a otra persona se le encarcele por equis tiempo, como un ejemplo que dieron ayer, etcétera, etcétera.

Y finalmente, mi sugerencia es que las agencias deben de empezar a revisar esto. O sea deben de empezar a tener pendiente toda esta tendencia, deben de empezar a normar cómo se está trabajando y deben de empezar a solicitar transparencia en cómo se está construyendo el algoritmo.

Ahora bien, en la presentación anterior hay casos en los que los algoritmos tienen que ser cerrados por las características de la información que está buscando, pero si en realidad estamos generando procesos de IA para política pública y para beneficio y mejora de las condiciones de los ciudadanos, no debe por qué estar cerrado cómo es la construcción de ese algoritmo, para estar claros que no estamos generando sesgos, que no estamos tratando mal el dato o que no estamos invadiendo datos personales durante el proceso.

Muchas gracias.

**Mtra. Marina Alicia San Martín Rebolloso:** Christian, muchas gracias.

Muchas, muchas gracias por los ejemplos prácticos.

Y sin mayor preámbulo pasaría contigo Pablo, si nos haces favor de explicar, ya sea ahí, aquí, donde quieras.

**Mtro. Pablo Corona Fraga:** Para no romper el orden armónico de cómo se dieron las presentaciones, desde acá, vamos uno y uno.

Muy bien, quisiera empezar con esta lámina, y van a darse cuenta que parece que nos pusimos de acuerdo todos, y la verdad es que no nos pusimos de acuerdo prácticamente para nada; es más, la última lámina de Christian prácticamente describía lo que quiero decir aquí.

La mayoría de las veces que la gente ve esta lámina lo ve así hasta con emoción y dice: sí, sí, me siento identificado, porque todo es relativo. Y a mí me cuesta un poco de trabajo, porque le falta la mitad de la información.

¿Y por qué? Porque nadie escribe un seis así pululando en el aire, todo mundo escribimos algo en un contexto, y en el momento en que los conceptos, las cosas o un seis lo disociamos y lo abstraemos de su contexto, pierde valor y significado por completo, y Christian lo ponía con palabras mucho más elegantes y el título de la lámina decía “No se puede disociar el procesamiento de los datos del contexto” o algo así.

Y creo que es bien importante entender el contexto, porque a veces perdemos la dimensión de qué estamos buscando, y lo decía en la mañana Carmen Quijano de una manera muy buena y decía: “no se puede tener una ponderación genérica que aplique a todos los casos para la aplicación del derecho.

Tenemos que hacer una contextualización de cada uno de los casos y tratar de generar, y ahora hablando de los algoritmos, de los que te referías Christian, necesitamos aprender a entender que los algoritmos tienen limitaciones, y creer que vamos a tener un algoritmo que contemple todos los casos, no sé si un día vamos a llegar a allá, y el día que lleguemos a lo mejor me preocuparé un poco más y los que hayan visto Skymet habrá que preocuparnos, pero tenemos que entender el contexto. Y por el momento necesitamos que esto quede en la decisión de una persona.

Y me gusta mucho cómo lo decía Laura, yo sueño con el día en que le quitemos a las cosas el electrónico o el digital, o ahora que le ponen ciber a todo, y entonces es gobierno electrónico, gobierno digital y luego van a salir con el cibergobierno, porque en realidad el gobierno no hace gobierno electrónico, el gobierno gobierna, y déjenme decir, el ciberespacio que trasciende a lo digital o a lo físico, sino es un solo espacio, una sola dimensión en la cual hoy vivimos, y no es o digital o físico, sino ya es una sola, y hay ejemplos muy claros en donde ya las afectaciones al mundo físico tienen impactos digitales, o las afectaciones en el mundo digital tienen un impacto físico.

Y me gusta usar un ejemplo extremo, pero que es ilustrativo. El año pasado por abril, una noticia que a mí se me hizo parteaguas en la historia, fue que por primera vez hubo un ataque físico, perdón, un ataque cibernético, un ataque de una secta terrorista, que se llama Hamás en Israel, que estaba atacando infraestructura del gobierno, y la respuesta del gobierno por primera vez en la historia del mundo fue ante un ataque cibernético, una bomba en el edificio donde estaban los hackers.

Entonces se pierde la frontera de lo que hay entre lo físico y lo digital, y creo que es el momento de voltear hacia allá, y me gusta cómo lo ve Laura, o sea ya no es físico-digital, sino es un solo concepto importante.

Y el siguiente es que cada vez deberíamos hablar menos, el foro, y así es, no es crítica, es algo que lo vemos todos los días, pero hablamos de protección de datos personales, por lo menos ya es un paso más. Hace 20 años hablábamos en estos temas de temas digitales de proteger las bases de datos, entonces por lo menos hoy ya no se habla de proteger las bases de datos, ya hablamos de proteger los datos personales.

Pero en realidad habría que recordar que no protegemos tampoco los datos personales, o sí los protegemos, pero en realidad lo que estamos buscando proteger al final es a las personas, no los datos personales.

Y ese cambio de paradigma es fundamental, porque mientras no entendamos que no estamos protegiendo un dato, sino a una persona, y que en el momento en el que ese dato se pueda mal utilizar, se pueda filtrar, se pueda llevar a un ente o ámbito que no fue la intención del ciudadano o no está en el marco jurídico, entonces el impacto no es en los datos, es en las personas.

Y entonces, a ver, ¿quién quiere la información, quién quiere los datos? Todo mundo. Hay un delicado equilibrio, y durante las presentaciones ayer y hoy hemos visto que alguien y varios han dicho: hay que buscar el equilibrio. Yo solo quisiera modificarlo un poco a decir: hay que mantener un equilibrio, porque como cualquier equilibrio, no se puede alcanzar y ya, sino hay que encontrarlo y después mantener ese balance; y mantener el balance a veces es más complicado que encontrar el equilibrio.

Entonces, ese balance, y déjenme hacer comparaciones muy sencillas, vayan no a la aplicación de la ley en los ámbitos federales o locales, sino vayan a la aplicación de las reglas en nuestras casas, porque en el momento en el que yo quiero saber dónde están mis hijas, voy a querer ser lo más invasivo y entonces poder decir: a ver, desde mi celular en dónde está su celular y poderlas tener rastreadas todo el tiempo.

Y ahora si nos vamos un poquito ya a la aplicación de la ley, en el momento en el que nosotros somos víctimas de la delincuencia es todo el tiempo tentador decir: “a ver por qué la ley no en ese momento intercepta las llamadas de los delincuentes y por qué no los localizan en tiempo real y por qué”. Pero cuando nosotros estamos del otro lado, nos cuestionamos: “a ver, ¿pero porqué van a interceptar mis llamadas?”.

Entonces, ese equilibrio es algo que no es permanente y hay que estarlo buscando constantemente.

Y algo que me parece importante señalar es que pensemos en la historia y en la historia las leyes no son perfectas, se han tenido que ir adaptando al entorno, y hay leyes que hoy leemos de hace, y ni siquiera tanto tiempo, de 40, 50, 60 años, y que hoy nos parecían irrisorias, diríamos: “era ridículo que hubiera una ley así”.

Pues habrá que pensar que hoy tenemos leyes que dentro de 30 años van a parecer ridículas, y por lo tanto hay que mantenernos en ese constante cuestionamiento del status quo. No puede ser una situación permanente en la que estamos.

Y entonces, a ver, todo mundo queremos información, y si yo quiero información de mi hija, pues obviamente voy a ponerme enfrente del fulano con el que sale y le voy a decir: mira, mis grandes capacidades de cazador, pero necesitamos entender que eso vive en un contexto, pero bueno, todo mundo tiene ganas de información de datos y ya hablamos de las marcas de las corporaciones, de los hackers, pero también de los países.

Y déjenme usar esto como un ejemplo actual. El año pasado se firmó un tratado que se llama *Cloud At* entre el Reino Unido y Estados Unidos. No sé qué tanto estén relacionados o lo conozcan, pero básicamente lo que dice es que la información que esté en servicios de nube alojados, ya sea en Estados Unidos o en el Reino Unido, habrá una cooperación entre las fuerzas del orden de ambos países para poder acceder a ellas sin orden judicial, lo cual puede ser bastante grave.

Y ahí empiezan esos temas, donde el equilibrio es delicado de mantener y las fronteras entre lo físico y lo digital empiezan a ser irrelevantes.

Y esta lámina no se ve mucho, pero me gusta hablar del caso de San Bernardino, un caso en donde el gobierno de Estados Unidos exigía a Apple romper el cifrado que tenía un teléfono porque lo veían como evidencia para un caso, pero entonces el gobierno está hasta enfrente de la fila, pero atrás están los hackers y atrás están gobiernos autoritarios, y atrás están delincuentes, y el momento en el que esto, se cede ante estas presiones de: a ver, vamos a crear un *Bagdor* en el cifrado, vamos a crear un *Bagdor* en el cifrado punto a punto para la mensajería, pues en el mundo perfecto en el cual solo las fuerzas del orden van a tener acceso a esto, pudiera ser más o menos razonable, pero desafortunadamente no vivimos en ese mundo perfecto y todos los gobiernos del tamaño que quieran, por más que han guardado secretos, siempre ha habido forma de que alguien se los robe.

Y entonces si este es uno de esos secretos, alguien se lo va a robar y habría que tener mucho cuidado con ello, y más ahora que todo está en la nube, y cuando yo pienso en mis datos en la nube, quiero pensar que están en un centro de datos, como los que están en la foto, con pasillos interminables de foquitos intermitentes.

Pero del otro lado de un AIP nunca sabes si la infraestructura que hay es esta, y entonces tenemos que aprender no solamente a entender cómo proteger, decíamos hace rato, no las bases de datos, no los datos personales, sino a las personas, pero al final las personas, la vida de las personas, sus datos dependen de una infraestructura, y la elección de esa infraestructura, la elección de un programador, de un lenguaje, de qué librería o no utilizar, se vuelve a veces de vida o muerte, y habrá que considerarlo en todos esos casos.

Bueno, déjenme usar esta otra lámina como un ejemplo también práctico. Un investigador en internet encontró una manera, mediante datos públicos, de hacer estas gráficas y las hizo para distintas ciudades, no sé si la ubican, pero esta es la Ciudad de México, y la Ciudad de México ni siquiera está pintada en el mapa, el mapa lo estamos viendo prácticamente pintado solamente por puntos localizados de donde había un celular encendido a cierta hora, y los rojos son IPhone y los azules son Androide, lo cual en este caso se revelan.

Lo que trato de decir es: todo el tiempo por donde nos movemos vamos dejando una huella digital, y todas las personas a las cuales ustedes les brindan un servicio como ciudadanos, van dejando una huella digital de lo que dimos como servicio, y a veces es tentadora esta situación de: entonces como estos datos ya los tiene la Agencia B, vamos a compartirlos. Y creo que deberíamos borrar esa imagen de poder compartir bases de datos, de poder transferir bases de datos, yo creo que sería inaceptable transferir una base de datos, para cambiar el paradigma de decir: mejor vamos a compartir o a colaborar en brindar datos específicos para la prestación de un servicio para el cumplimiento de un mandato o ley.

O sea, no compartimos bases de datos, lo que hacemos es compartir datos específicos en términos de un mandato. Y si seguimos pensando, entonces, en compartir bases de datos, estamos perdidos en ese sentido.

Bueno, déjenme seguir un poco el orden. Y quería poner esto, hace rato hablaban de compartir datos personales en materias de datos personales sensibles o no sensibles por ser un dato biométrico, y mencionaban en el panel anterior, no nos hemos terminado de poner de acuerdo si los datos personales biométricos son sensibles o no.

Y yo creo que ya el cuestionamiento creado afortunadamente ya pasó hace mucho, porque desde hace varios años en México el INAI emitió unas recomendaciones, en donde decía: los datos personales biométricos deben ser considerados sensibles.

Pero no solo eso, sino hay que tener mucho cuidado en su tratamiento, porque se hizo toda una polémica de: a ver, les vamos a dar datos personales, y déjenme quitar si es al gobierno o a un ente privado, pero en este caso a ustedes como gobierno, le vamos a dar los datos personales al gobierno, y es que eso es muy peligroso, pues habría que sensibilizar a la gente de qué procesamiento y qué recabación estamos haciendo en realidad de los datos.

Porque no es lo mismo yo recabar un biométrico completo, por ejemplo tener una imagen en alta resolución y tercera dimensión del rostro completo, lo cual puede hacer reproducible no solo la validación de que el rostro es el mismo, sino el uso de ese biométrico, o lo mismo de una huella digital en alta definición con tener patrones que ayuden a identificar si ese patrón, como se ve en la gráfica, los puntitos que miden la distancia entre la ceja, la distancia entre los ojos de la nariz, pero entonces nunca almacené por completo el dato biométrico del rostro completo, lo único que hice es guardé un patrón de cómo se ve ese dato biométrico de manera comparable, para después saber que eso lo puedo llevar a validar si esa persona, cuando llega nuevamente con su huella digital o cuando llega nuevamente con su rostro o con el iris, es la persona que dice ser.

Entonces, trato de aterrizarlo en ejemplos como esto de: a ver, no le tengamos miedo a procesar los datos biométricos mientras no los tengamos almacenados y los hagamos de una manera responsable y siguiendo los lineamientos, que ya aparte hay prácticas internacionales para ello.

Y en el panel anterior hablaban mucho sobre la privacidad de diseño y por defecto, y quise dejar un ejemplo, no quiero ahondar mucho, porque dieron muy buenos ejemplos, pero yo quisiera nada más darles este otro ejemplo, que algunos de ustedes ya conocen, porque en una serie de pláticas lo vimos, el gobierno de Estados Unidos hicieron, yo critico mucho luego a los gringos, y ahora me toca darles una cucharadita blanca por las negras, pero hicieron algo que le llaman “loggin.gob” o sea una página de gobierno electrónico, en donde lo que dicen es: almacenamos los datos, al momento de que un ciudadano se da de alta crea una llave digital, una firma electrónica con una contraseña, y esa contraseña es, bueno, no se ve nada la lámina, pero esa contraseña es la única llave que puede abrir el procesamiento de sus datos.

De tal manera que solo cuando el ciudadano introduce su llave podemos acceder a los datos.

De tal manera que en el momento en el que solamente los entes que necesitan acceder a los datos tienen la mitad de la lleva, o sea en este caso una dependencia del gobierno tiene la mitad de la llave, y la otra mitad la tiene el ciudadano, que cuando dice: quiero hacer un trámite, introduce su llave y ahora sí se puede acceder a los datos. Mientras no estén ambas llaves no podría accederse a los datos, lo cual me parece, otra vez, un mecanismo muy práctico de esta privacidad por diseño y por defecto para cómo llevar esta protección de los datos.

Bueno, y ahora déjenme, para terminar, hablando, hace rato que hablaba de la historia, hacer un poco de historia, que hay esta tentación, y Laura decía hace rato; hay que tener cuidado con esto de que todo lo que sea posible tecnológicamente debe hacerse, porque no sabemos cuándo va a ser el ejemplo de la máquina de vapor; o sea, la máquina de vapor fue una revolución y creó la revolución industrial, y dijeron: esto es lo que va a cambiar al mundo. Sí, sí cambió al mundo, pero quién usa vapor hoy.

O sea, no quiere decir que el que haya un cambio va a ser la tecnología permanente. Y puedo dar varios ejemplos, el primero que me viene a la mente es *Lowchen*, está la tentación de: “Ah, mandemos todo al BlogChen”.

Pues no sé, hay que tener cuidado, hay que tener prudencia de si lo necesito y necesito esas capacidades en ese momento, y ya que las evalúo, entonces ahora sí veremos si me voy a ellas o no.

Y en ese sentido vivimos en esta híperconvergencia, en donde hablaba de que se pierde la frontera entre lo físico y lo digital, y esa frontera regresa a la definición original.

Me gusta, un poquito en ese sentido las etimologías y la palabra cibernética viene de un libro por allá en los 40, que alguien decía que era el estudio científico del comportamiento y las funciones que realizan los seres vivos y cómo las máquinas pudieran reemplazarlos.

Pero entonces esto tomó distintas vertientes, y una de ellas, que me pareció interesante, y hace poquito encontré un libro al respecto, fue que veían la cibernética por ahí de los 60 como una manera de controlar la mente como procesos solamente mentales, y piensen en Cambridge Analytica, él basado en tus hábitos y en la forma de hacer cosas controlarte, pero lo mismo sucede en los gobiernos.

Hace rato dabas un buen ejemplo de cómo ciertas personas empezaron a ser segregadas, porque eran sujetas o propensas a estar embarazadas.

Entonces, este tipo de tomar datos y hacer minería de datos de manera irresponsable pudiera llevarnos a un descontrol grave y habrá que tener cuidado, lineamientos claros, y un cuestionamiento de la sociedad civil, del gobierno, de las empresas y de todos los entes de la sociedad para no creer que ya alcanzamos un equilibrio, y entonces encontramos la perfección.

Hay que cuestionar, hay que mantenernos y crear estos foros como estos me parece que es relevante siempre y mantenernos actuales.

Eso es todo, muchas gracias.

**Mtra. Marina Alicia San Martín Rebolloso:** Pues muchas gracias.

Voy a pasar, les reitero que quien tenga preguntas por favor anótelas y las hacemos llegar. En principio ahorita no ha llegado una, salvo que las tengan ahí.

Y agradecerles las intervenciones, y pasaría a entregarles sus constancias.

De verdad fue muy enriquecedor este panel, para ya pasar a la clausura.

Pablo, empiezo contigo.

Muchas gracias. Por favor, aplauso.

Doctora Laura, gracias, muchas gracias.

También un aplauso, por favor.

Querida Norma, a nombre de la Agencia Digital de parte del INFO.

Y querido Christian, muchísimas gracias también.

Aplauso, por favor.

**Presentador:** Invitamos a los panelistas tomarse la foto oficial.

Despidámoslos con un fuerte aplauso.