Ciudad de México, 19 de noviembre de 2020.

Versión estenográfica de la Conferencia Magistral: "La importancia de la Protección los de Datos Personales y el uso de las nuevas tecnologías en la nueva normalidad laboral y educativa, dentro de la Semana Nacional de Transparencia.

Presentadora: Buenos días. Damos inicio a la Conferencia Magistral: "La importancia de la protección de los datos personales y el uso de las nuevas tecnologías en la nueva normalidad laboral y educativa".

Tenemos el gusto de presentarles a nuestros distinguidos participantes. Álvaro Rae Fernández, Oficial Legal Asociado en la Organización de Estados Iberoamericanos para la Educación, la Ciencia y la Cultura.

Presenta la conferencia la investigadora y académica de la UNAM Jacqueline Peschard Mariscal, a quien le damos la bienvenida y cedemos el uso de la voz.

Dra. Jacqueline Peschard Mariscal: Muchas gracias, muy buenos días. Es un honor poder estar aquí en esta importante Semana de Transparencia y también de Protección de Datos Personales.

El día de hoy tenemos, como ya se dijo, vamos a presentar al doctor Álvaro Rae Fernández, quien es un doctor abogado y politólogo, y desde 2015 trabaja en la Organización de Estados Iberoamericanos para la Educación, la Cultura y la Ciencia.

Y actualmente no solo es Oficial Legal Asociado, sino que es el responsable de implementar el Reglamento General de Protección de Datos Personales de la Unión Europea en dicha organización.

Ciertamente la pandemia nos ha presentado el desafío de cómo atender las medidas para protegernos frente a la emergencia sanitaria y, al mismo tiempo, asegurar el ejercicio de nuestros derechos y de nuestras libertades.

Sabemos que el confinamiento nos ha limitado en el ejercicio de esos derechos, en el ejercicio del derecho de reunión, del derecho de tránsito, del derecho de movilidad.

Pero el hecho de que hoy buena parte de las actividades laborales y particularmente las actividades educativas, se realizan desde el hogar o desde algún lugar privado, desde espacios de convivencia personal, y esto nos enfrenta al reto de cómo proteger utilizando internet y todas las herramientas informáticas, cómo asegurar que se protegen nuestros derechos personales, particularmente aquellos que son más sensibles y más íntimos como es, efectivamente, los espacios de convivencia personal y familiar.

Creo que ese reto, la utilización de las nuevas herramientas informáticas y, por otro lado, la protección de nuestros datos personales y el ejercicio de nuestra privacidad, es un tema que nos ocupa el día de hoy.

Y le voy entonces a dar la palabra al doctor Rae Fernández, dándole la bienvenida a esta Semana Nacional de Transparencia.

Dr. Álvaro Rae Fernández: Muy buenas tardes a todos.

En primer lugar agradecerte, doctora Jacqueline, tus palabras, tu presentación.

No quiero comenzar sin antes también agradecer al INAI en nombre de nuestro Secretario General por la invitación que han hecho a la Organización de Estados Iberoamericanos para la Educación, la Ciencia y la Cultura a esta Conferencia Magistral sobre la Importancia de la Protección de los Datos Personales en esta situación, en esta nueva realidad que estamos todos viviendo.

También quisiera felicitar al INAI por las conferencias que se están realizando a lo largo de la Semana Nacional de la Transparencia y por la buena gestión que están realizando para realizar esta reunión en esta modalidad on line que nos ha tocado vivir este año y esperemos que el año que viene se pueda celebrar con relativa normalidad.

Antes de comenzar, un poco para que el público se encuentre de alguna forma familiarizado con lo que se hace en la Organización de Estados Iberoamericanos, somos un organismo internacional de carácter gubernamental que trabaja para la cooperación de los países de toda la región Iberoamericana en los ámbitos de la educación, la ciencia y la

cultura y siempre en el contexto del desarrollo integral y la integración regional.

Somos un organismo iberoamericano, además, con mayor trayectoria, organismo decano de la región con 71 años de experiencia y de alguna manera en nuestra propia composición, ya que contamos con 18 oficinas en toda la región Iberoamericana, más la Secretaría General que se encuentra aquí en España, aquí en Madrid, pues nos hace vivir esta situación de la protección de datos con especial protagonismo, sobre todo por la cantidad de normativa distinta con la que tenemos que trabajar en nuestro día a día y para eso, creo que es fundamental conocer el marco normativo en el que se desempeña, en este caso, el trabajo de nuestra organización.

Si bien es cierto que tuvo un gran impacto la normativa de protección de datos del Parlamento y del Consejo Europeo, el Reglamento 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales, en la libre tripulación de los mismos, la cual entró en vigor en mayo del año 2018 (falla de audio) un gran revuelo, no solamente en el espacio económico europeo, sino las consecuencias que tuvo en los ordenamientos jurídicos de los países que de alguna forma contaban con una mayor digitalización, pero sí es verdad que ya anteriormente había bastante normativa al respecto.

Sin embargo, digamos que se cumplía de forma bastante laxa, sobre todo, debido a que no había un régimen sancionador en estas normativas, que de alguna forma obligara a los estados a cumplir con las normativas de protección de datos.

Si bien es verdad, en esta normativa que ya digo que se hace extensible a la legislación que se puede aprobar prácticamente en cualquier Estado que al día de hoy apruebe normativa de protección de datos, bueno, parecen aspectos como puede ser el consentimiento expreso, ya no vale el consentimiento tácito, que de alguna forma todos los usuarios juran conocer con exactitud cuáles son los tratamientos que se van a hacer sobre sus datos personales, que de alguna forma ellos tengan que consentir de forma individualizada todos y cada uno de los tratamientos que se van a hacer.

Anteriormente, pues recibíamos un texto con una cantidad enorme de información que no podíamos distinguir cuáles eran realmente los tratamientos que se iban a hacer. Ahora, digamos que tenemos que ir punto por punto, aceptando todos y cada uno de estos tratamientos.

También es una normativa esta y las que se han aplicado, como consecuencia de la aprobación de esta normativa, que van siempre, que siempre van en dirección a proteger cada vez más a los menores y de esta manera, también ofrecer a los tutores, una mayor información sobre los tratamientos que se van a hacer de los datos de este colectivo, colectivo por otro lado vulnerable y sobre todo, ofrecer una mayor transparencia, hacer comprensible a los usuarios qué es lo que se va a hacer con sus datos, como venía diciendo.

Las consecuencias que ha tenido la aprobación de esta normativa, bueno, pues en el caso del espacio económico europeo, lógicamente, la acción de todas nuestras legislaciones nacionales a este nuevo esquema, incluso se han incluido en las leyes que han, de alguna forma traspuesto este reglamento, nuevos derechos a los ciudadanos, como puede ser el derecho a la seguridad, a las comunicaciones, a la educación digital, a la protección de los menores en internet o incluso a la propia desconexión digital en el ámbito laboral; es decir, cuestiones que de alguna forma estaban en el aire pero que ya se van plasmando en los ordenamientos jurídicos.

Y en América Latina vemos cómo también ha habido una creciente actualización de las normativas de protección de datos, pues lógicamente a raíz de la expansión y mercantilización de nuevas tecnologías. Al final los países tienen que adaptar sus esquemas y sus regulaciones a la protección de datos.

Vemos, por ejemplo, cómo el pasado mes de agosto en Brasil acaban de aprobar una nueva normativa de protección de datos, ya que anteriormente tenía hasta 40 regulaciones diferentes en todo el país. Entonces, la idea es uniformizar toda esta normativa para que a todos nos llegue por igual.

Pero, bueno, digamos que no solamente Brasil, muchísimos países ya tenían normativa sobre esto. Colombia desde el año 2012 ya tenía una normativa de protección de datos bastante potente. Ecuador y El

Salvador están avanzando también ante una integración de la privacidad. Chile, Uruguay y Argentina también cuentan con mecanismos desde el punto de vista técnico bastante actualizados, y también están actualizando esto en sus nuevos marcos regulatorios.

Es decir, que poco a poco todos van entrando en una dinámica de proteger cada vez más al ciudadano en lo que se refiere a sus datos personales.

Y claro cómo se puede explicar la nueva realidad si no tenemos en cuenta que nuestros datos están viajando día a día de unos países a otros. Pues básicamente es muy importante que todas las regulaciones sean muy precisas en lo que se refiere a las transferencias internacionales de datos. Esto nos afecta, ya no solamente en el ámbito laboral y educativo, sino básicamente en todos los sectores de nuestra vida, ya sea en nuestro ejercicio profesional o en nuestra vida privada.

Al final el hecho de que vivamos en una economía global hace que sea indispensable el flujo internacional de estos datos, y al final, como ya decía, en todos los sectores van apareciendo este tipo de tratamientos, por ejemplo.

Si hablamos de la OEI, nosotros que trabajamos con profesores, con docentes, con estudiantes, donde realizamos cursos, seminarios, programas de becas a nivel internacional pues al final estos tratamientos que se producen entre diferentes países, entre diferentes regiones pues han de tener de alguna forma las salvaguardas que ofrecen las normativas nacionales, y a su vez informar siempre a los interesados, en este caso a los ciudadanos, qué es lo que se va a hacer con sus datos personales, y en nuestro caso sí que es cierto que trabajamos con datos bastante básicos, datos identificativos, nombres, apellidos, correos electrónicos, nacionalidad.

Al final son datos que no revierten una especial sensibilidad. Como mucho tratamos datos de menores que se considera un colectivo vulnerable, pero nos ponemos a pensar en datos que puedan manejar muestras de salud, datos que tengan que ver con nuestra filiación política, sindical, datos religiosos, étnicos.

Al final estos datos de especial sensibilidad a la hora de transferirlos internacionalmente tienen que contar con las medidas de seguridad técnicas apropiadas.

Y para ello, es muy importante que los interesados conozcan y consientan estos tratamientos.

Es decir, bien sea ofreciéndoles toda la información posible, haciendo lo más comprensible al ciudadano, para que conozcan no solamente los tratamientos que se van a hacer de sus datos, sino también todos sus derechos, que eso es muy importante, poder conocerlos, para que posteriormente nosotros podamos, no solamente ejercer nuestro derecho de acceso, rectificación, cancelación o posición, eso al final vendrían a ser derechos ARCO, que de una forma u otra, ya venían reflejados en diferentes legislaciones anteriores.

Ahora aparecen nuevos derechos, derecho al olvido, aparece el derecho a la portabilidad de nuestros datos, como mencionaba antes, nuevos derechos del ámbito digital, como puede ser el derecho a la educación digital, el derecho a la desconexión digital en el ámbito laboral, es decir, los ciudadanos tienen que ir poco a poco familiarizándose con estas nuevas garantías y, sobre todo, que los estados las implementen de forma correcta, porque lógicamente una cosa es que aparenta las leyes de los ordenamientos jurídicos, pero otra cosa es la implementación efectiva de éstas, que poco a poco nos tendremos que ir adaptando a esta nueva realidad.

Y, como bien decía, al final, todo este flujo de datos que se da a nivel internacional, hace que los estados tengan que contar con mecanismos de seguridad, bastante potentes, desde el punto de vista técnico, para hacer posible la sesión de los datos entre el país emisor y el país receptor, con totales garantías.

Sí que es cierto que cada vez más vemos cómo los países van adoptando decisiones de adecuación, para que se puedan transferir datos de forma segura; encontramos como por ejemplo, en el reglamento de protección de datos de la Unión Europea, cómo Argentina y Uruguay, han sido considerados países desde el punto de vista técnico, que se consideran seguros para recibir datos del espacio económico europeo.

También encontramos acuerdos, como puede ser el TMEC, entre Estados Unidos, México y Canadá, es decir que cada vez más vamos viendo este tipo de acuerdos internacionales, donde los datos de los ciudadanos van viajando de un lugar a otro, de forma segura.

Y esto al final es una realidad cambiante. Como he comentado al final, se tiene que tener en cuenta, a la hora de realizar este tipo de transferencias, sobre todo garantizar que en el país receptor de los datos, hay un control verdaderamente independiente de la protección de datos, donde se establezcan mecanismos de cooperación con las autoridades de esos estados.

De tal manera que se puedan, de alguna forma, reconocer derechos efectivos, y exigibles a esas autoridades.

Ahora, por ejemplo, me gustaría hacer hincapié en un acuerdo, en el acuerdo de privacidad, que era el acuerdo que había entre la Unión Europea y Estados Unidos para la transferencia internacional de datos; la Unión Europea, en este caso, el Tribunal de Justicia de la Unión Europea, ha declarado inválido este acuerdo; precisamente, porque en Estados Unidos, no existía un organismo, una institución ante la que recurrió nuestros derechos en caso de que se vieran afectados.

De tal manera que tiene que haber cierto paralelismo entre lo que se exige, en este caso, al espacio económico europeo que contamos con mecanismos siempre para poder ejercer nuestros derechos, y en el otro lado, que también sea eso exigible.

No existía eso. Además, no se garantizaba el principio de proporcionalidad, en la medida en que los programas de vigilancia estadounidenses, no se limitaban a revisar lo que era estrictamente necesario, sino que iban mucho más allá.

Por ese motivo, el Tribunal de Justicia de la Unión Europea, y esto venia a raíz de una demanda de un irlandés, contra Facebook, como tumbó este acuerdo, precisamente porque no se encontraba con mecanismos de protección verdaderamente eficaces para la salvaguarda de los derechos de los ciudadanos.

Y ahora digamos que es importante recalcar cómo todo esto ha tenido impacto mayor a raíz de la COVID y de los confinamientos.

Y nos hemos preguntado, ya sea los ciudadanos o desde los medios de comunicación, cómo era posible el tratamiento de datos de todos nosotros en esta situación tan excepcional.

Es importante recalcar, y esto es verdad que lo han mencionado así las diversas autoridades de control, cuando hablo de autoridades de control hablo de instituciones independientes que se encargan de velar por el verdadero funcionamiento de la normativa de protección de datos dentro de los Estados, que las diferentes normativas de protección de datos que había, independientemente del país, en la medida que salvaguardan un derecho fundamental se aplica en su integridad a la situación actual.

Es decir, las propias normativas contaban con este tipo de circunstancias tan extraordinarias excepcionales para poder tratar los datos personales de los ciudadanos.

Y ya de alguna forma vienen a desarrollar las salvaguardas y reglas necesarias para permitir legalmente los tratamientos de los datos personales en este tipo de situaciones.

De hecho, este es un ejemplo bastante significativo, cómo la normativa, por ejemplo, de protección de datos de la Unión Europea reconocía situaciones como podía ser una epidemia.

En el considerando 46 de la normativa establecía que la base jurídica de los tratamientos en situaciones extraordinarias, como la que estamos viviendo, podían estar basadas en el interés público, como está ocurriendo; es decir, están tratando nuestros datos de salud para de alguna forma realizar estadísticas sobre la evolución de la pandemia sin contar directamente con nuestro consentimiento, como suele ocurrir.

Sino que se están amparando en otra base legítima de tratamiento como es el interés público o el propio interés vital del interesado para poder tratar nuestros datos.

En el ámbito laboral, ya yendo un poquito más a lo que puede ser más específico en la vida de cada uno de nosotros, por ejemplo, esa base legítima de tratamiento puede ser el cumplimiento de una obligación legal.

Por ejemplo, la situación en la que el empleador tenga que tratar los datos de los empleados para prevenir riesgos laborales, es decir, que de alguna forma todo esto estaba ya contemplado en las normativas.

Si bien es cierto que alguna están más actualizadas que otras, pero es importante recalcar como todas de alguna forma van navegando en la misma dirección; eso es lo más curioso de todos.

Al final podemos emplear la normativa que se acaba de aprobar en Brasil y la normativa de protección de datos de la Unión Europea, y vemos que al fin y al cabo son bastante similares, lógicamente con sus particularidades, sobre todo atendiendo las transferencias internacionales de datos que son bien diferentes en una región y en otra.

Y el nivel laboral que esto puede ser muy interesante para los ciudadanos. Al final, si bien es cierto que partimos de la premisa de que al igual que en nuestra vida, en nuestro día a día, en nuestro ocio, la digitalización es una absoluta realidad, ya sea a través de las redes sociales, de los teléfonos móviles, a la hora de descargar cualquier tipo de aplicación gratuita que de alguna forma nos dice que la forma de contraprestar ese servicio es prestando nuestros datos personales, pues lógicamente esto va a ocurrir también en el ámbito laboral.

Y hemos experimentado durante los diferentes confinamientos cómo en nuestro trabajo, en nuestro día a día tenemos áreas que se venían desarrollando. En las oficinas las podíamos hacer desde nuestras casas con total “normalidad” y nunca podíamos pensar que podíamos haber hecho eso con la facilidad que lo hemos estado desarrollando durante todo este tiempo.

Pero claro, si bien es cierto que podíamos acceder desde cualquier dispositivo a un servidor online, a una intranet, a través del cual podíamos desarrollar nuestro trabajo, también es verdad que tenemos que tener muy en cuenta la implicación y los riesgos que puede mantener, bueno, que puede conllevar este tipo de situaciones.

Pero, para eso es necesario establecer una serie de pautas que son bastantes lógicas, de sentido común, pero que tienen que ser empleadas, sobre todo, explicaré también las situaciones de trabajadores por cuenta propia, pero sobre en relaciones por cuenta ajena donde está una relación empleador-empleado, donde se tiene que seguir una serie de pautas, que al final son tan sencillas, como puede ser definir una política de protección de datos para situaciones de trabajo o situaciones extraordinarias, como puede ser una nueva pandemia en un futuro.

De alguna forma se tiene que quedar establecido, marcado, cómo tienen que ser las formas de acceso, hasta el tipo de dispositivos válidos, desde los cuales podemos acceder a nuestra actividad profesional y siempre importante definir las responsabilidades y obligaciones que hay, tanto por el lado del empleador, como por el lado del empleado.

Por eso, es muy importante la formación a los trabajadores, que de alguna forma estén concienzados, en su trabajo, en su día a día, qué es el tratamiento de datos personales, en qué momento ellos tienen que trabajar con datos de terceros y tratarlos según lo que establecen sus normativas nacionales.

Es decir, tiene que haber una labor de concienciación y de predisposición por parte de las empresas e instituciones para que los empleados tengan esa concienciación colectiva, cuando tengan que trabajar con datos personales.

De esa manera, se tienen que trabajar siempre con prestadores de servicios confiables, al final las empresas, instituciones, empleadores en definitiva tienen que trabajar o tienen que ofrecer garantías desde el punto de vista técnico a sus empleados. De tal manera que haya la mayor seguridad posible en los datos personales, pues que se trabajen.

Y luego, también es importante seguir siempre ese tipo de instrucciones que están en las políticas de protección de datos, como pueden ser, pues no descargar aplicativos que no estén autorizados, ni otras herramientas de software, sino que se trabaje siempre con herramientas seguras.

Pero bueno, como lo hemos hablado, también el empleado tiene que tener su parte en esta, tiene que poner de su parte en esta tarea, de alguna forma protegiendo el dispositivo que utiliza, ya no solamente si trabaja por cuenta ajena, sino trabaja por cuenta propia, estableciendo mecanismos de protección, a través de contraseñas robustas, utilizando herramientas seguras desde el punto de vista técnico, trabajar con herramientas que han sido previamente autorizadas, guardar la información en espacios habilitados de toda esta información, que de alguna forma le quede clara también al empleado para que él también conozca las obligaciones que puede mantener desde el punto de vista laboral.

Y bueno, si nos vamos al ámbito educativo, que creo que también es bastante interesante, sobre todo desde nuestra experiencia en la OEI, ya sea pos, prepandemia o pospandemia, pues es interesante analizar cómo se tiene que implementar la normativa de forma, no decir diferente, pero se tiene que tener una conciencia distinta si hablamos de centros educativos, cuando hablamos de actividad presencial a diferencia de cuando hablamos de centros que ofrecen formación online.

En los centros educativos con actividad presencial debe ser una prioridad del centro en cuestión garantizar y demostrar que el tratamiento es conforme a la normativa de protección de datos del país en cuestión. Pero siempre atendiendo las características que tenga el propio centro, es decir, las medidas de seguridad, las medidas técnicas que tiene que emplear un centro educativo de dos mil estudiantes es bien distinto a uno que trabaja con 100. Ya solamente por la cantidad de estudiantes que maneja ese centro.

Entonces, de alguna forma las medidas tienen que corresponder en función a los riesgos existentes que haya dentro de los centros. Y siempre teniendo en cuenta la vulnerabilidad que tienen los datos y sobre todo si hablamos de menores.

Como ya comentaba anteriormente hablamos de un colectivo considerado vulnerable por los ordenamientos jurídicos, y al final es que las consecuencias que pueden derivarse de un inadecuado tratamiento que se haga, pues pueden generar situaciones bastante difíciles, sobre

todo porque en un centro educativo se pueden dar datos que van más allá de meros datos identificativos, se pueden tratar datos de alergias, de alumnos, datos de salud, datos familiares, es decir, que de alguna forma los centros educativos tienen que estar siempre actualizándose con este tipo de datos que facilitan, en este caso, o bien los propios estudiantes, si son mayores de edad, o los tutores de los menores.

Por eso es tan importante informar siempre a los ciudadanos, en este caso, desde los centros educativos con total transparencia de la información que se va a tratar, así como de todos los derechos con los que cuentan, de tal manera que todos ellos puedan tener pleno conocimiento del tratamiento que se está haciendo de sus datos personales.

Y si pasamos a la educación con line, y sobre todo en época de pandemia, que ha sido bastante común que muchos centros educativos han continuado con sus clases de manera on line, pues nos hemos hecho muchas preguntas como si se podía grabar a menores cuando están realizando un examen, o si se podían usar técnicas de reconocimiento fácil para verificar la identidad de un estudiante. Pues claro, al final todas estas cuestiones, que de alguna forma forman parte de la protección de datos, en este caso de los estudiantes, pues es muy importante que en este tipo de circunstancias el grupo docente se encuentre formado.

Es muy, muy importante que se encuentre de alguna forma familiarizado con toda la materia de protección de datos, para que de alguna forma pueda implementar de forma correcta las medidas para llevar a cabo ya sea para controlar un examen, ya sea para controlar la asistencia a clase, y sobre todo manejando siempre un juicio de proporcionalidad.

Es decir, si de alguna forma yo con esta medida consigo el objetivo que pretendo, o si de alguna forma está medida es necesaria o no existe otra que sea más moderada o si ofrece más desventajas que ventajas. Es decir, no decimos que no sea posible, sino simplemente tienes que de alguna forma justificar que es la única medida posible para poder conseguir el objetivo que tú quieres, en este caso, por ejemplo, controlar un examen.

Es decir, el juicio de proporcionalidad ha de estar siempre presente, y de alguna forma, como hablábamos, siempre con el consentimiento de los, en este caso, de los alumnos, a través de sus tutores, para que de alguna forma, sepan qué se está haciendo con sus datos personales.

Y, bueno, hasta le podría pasar igual, por ejemplo, con el tema de las calificaciones, que no se tienen que publicar en espacios abiertos, que se tienen que publicar, si tenemos aulas virtuales o Intranet, que se puedan comunicar directamente a los interesados, sin que sea necesario informarlo públicamente a todo el público.

Entonces, de esta manera, lo que tenemos que trabajar siempre es con la minimización de dato, y ya hablando en genérico, intentar de alguna forma, que tratemos el menor número de datos posibles, y en el caso de que sea estrictamente indispensable hacerlo, bajo los límites que marca la normativa, el consentimiento, porque se tiene una obligación legal, y porque estás cumpliendo un interés público, etcétera.

Y de alguna forma, tratar, como ya decía, el menor número de datos posibles, en la medida que no sea estrictamente indispensable. Y ya como conclusión, quizás, al final hemos visto como en muchos de nuestros países, con independencia de la gravedad que haya tenido la pandemia en todos y cada uno de ellos, al experimentar circunstancias nunca vividas, hemos avanzado más en digitalización en estos meses, de lo que hemos hecho en muchos años.

Al final, por ejemplo, si pongo el caso de mi país, durante el confinamiento, hubo picos de tráfico en Internet que llegaron a crecer hasta en un 80 por ciento de lo que es habitual.

Al final, todo esto hace que tú te tengas que adaptar a esta nueva circunstancia. Por ejemplo, en España, sí es cierto que contamos con unas buenas redes de fibra óptica, y como muchos, lo que tuvieron que hacer los servidores, fue adaptarse. Por ejemplo, las plataformas que servían servicios en streaming, que todos conocemos, pues bajaban la calidad de sus reproducciones.

Y, bueno, al final, nos hemos tenido que adaptar, al final hemos tenido que hacer de la necesidad una virtud, y por ejemplo, en el caso de pequeñas empresas, y en el comercio y proximidad, se tiene uno que

digitalizar a la fuerza, y se han transformado en pocos meses, como no lo habían podido conseguir en años, porque básicamente si no podían adaptarse a esta nueva realidad, pues no podían ejercer su actividad profesional, pues ya sea permitiendo pagos telemáticos, incorporar redes sociales para de alguna forma solicitar más sus contenidos y sus trabajos, estableciendo también herramientas de DIDICOMERS, todo siempre con unos criterios técnicos que han tenido que ir cumpliendo.

Pero bueno, aún así, siguen habiendo muchos retos pendientes; por ejemplo, en el ámbito educativo, hemos visto grandes carencias; que bueno que exigen una mayor inversión por parte de los estados, pues en equipamiento, en formación del profesorado, en nuevas metodologías de aprendizaje, que de alguna forma, nos hagan entender que hemos podido, de alguna forma, poner un parche a la situación que hemos vivido, pero una vez que hayamos vivido esta situación, actuar con diligencia en situaciones futuras y, sobre todo, sabiendo la inversión que hay que hacer en el ámbito educativo para que se pueda garantizar, por ejemplo, el derecho a la educación digital, como hablaba anteriormente.

Y que, sobre todo, puede servirnos para otros ámbitos de la vida. Es decir, estas cosas se han vuelto tan complejas en el ámbito laboral, en el ámbito educativo, pues también se pueden emplear ciertos esfuerzos que hemos hecho, para otros ámbitos, como por ejemplo el cambio climático.

Al final, hemos aprendido que un problema global nos puede afectar a todos individualmente. Por tanto, esta es una enseñanza que nos sirve, no solamente para estos dos campos, sino para todos los sectores y a partir de aquí, amoldarnos a una nueva situación en la que cada vez más vamos a estar más digitalizados, donde los tratamientos automatizados van a formar parte de nuestra vida de aquí en adelante, y la protección de datos personales, sobre todo han venido para quedarse. Y la seguridad que se tiene que mantener sobre nuestros datos ha de primar, ya que bueno, al final el derecho de protección de datos no deja de ser un derecho fundamental.

Básicamente esto es lo que quería comentar y agradecer al INAI por ofrecernos esta plataforma para contar un poco la labor que hacemos en la OEI y también esta nueva realidad que estamos viviendo.

Dr. Jacqueline Peschard Mariscal: Muchas gracias, doctor Rae, por esta presentación que usted ha logrado compactar realmente en muy poco tiempo, cuáles son, no solamente, los grandes avances y cómo se ha ido uniformando las normativas en materia de protección de datos, en general, no solamente en Iberoamérica, sino en buena parte del mundo.

Pero cómo tenemos retos enormes, sobre todo con la protección de los menores, creo, en la parte educativa; la seguridad informática, cómo asegurar que las empresas y los estados puedan tener esas medidas de seguridad y junto a esto cómo la pandemia nos ha obligado a extender nuestro conocimiento y nuestras habilidades digitales, pero también estas habilidades digitales nos exponen a una serie de posibles riesgos para la protección de nuestros datos.

Tenemos algunas preguntas que le quiero plantear. Pero yo quisiera decirle, ¿qué tanto realmente se ha avanzado en el mundo en un conocimiento de lo que es la protección de los datos personales?

En Europa ya tienen más de 30 años con regulación en esta materia, en los países latinoamericanos tenemos menos años; pero sí creo que todavía, particularmente entre los jóvenes que son los más entrenados en la utilización de todas las redes digitales, qué tanto realmente se ha ido desarrollando una cultura de protección de datos personales.

Pero quiero aprovechar para plantearle algunas preguntas que nos llegan del auditorio.

Si usted considera que los Estados Iberoamericanos deben invertir en inteligencia artificial para la protección de datos personales.

Y ante este uso de la tecnología, si la protección de datos es vulnerable ante posibles hackeos o venta de datos.

¿Y qué tanto el avance en el uso de la tecnología informática ha llevado a las mafias internacionales a traficar con datos en todo el mundo, sobre todo en relación a las normas que existen en Europa, si sería necesario diseñar un mecanismo único común?

Usted dice que estamos caminando hacia una uniformación de criterios de regulación, pero qué tanto podríamos tener una regulación que pudiera ser coordinada desde la ONU.

Y sobre el carácter laboral, el tema laboral, en distintas empresas y en organismos internacionales para ocupar una vacante, además del currículum, se pide a veces una prueba PCR, el resultado negativo del SARS-CoV-2 de la COVID-19.

¿Qué tanto se estaría vulnerando los datos personales sensibles en este tipo de contratación?

Dr. Álvaro Rae Fernández: Quizá como las dos primeras preguntas están más vinculadas, voy a empezar por esta última que amablemente me ha planteado.

En este tipo de circunstancias sí que es cierto que si se está informando al candidato qué es lo que se va a hacer con el tratamiento de sus datos, en este caso los datos de salud, y en este caso el interesado, el aplicante, consciente con este tratamiento, el tratamiento sería lícito. Al final, tenemos que entender que una de las bases legítimas de tratamiento es el consentimiento de los interesados.

Por tanto, si de alguna forma en la política de privacidad de la empresa, de alguna forma justifica y explican de forma bastante explícita cuál va a ser el tratamiento que se va a dar, cuál es la finalidad, cuál va a ser el plazo de conservación de esos datos, ante quién puede recurrir sus derechos, entre todo ese tipo de circunstancias que se encuentra normalmente en cualquier formulario de protección de datos, sin duda se podría hacer este tipo de tratamiento.

¿Hasta qué punto la empresa empleadora puede tratar estos datos o si esta medida es proporcional a la contratación? Bueno, esa ya es una pregunta para la empresa, porque dependerá, también en gran medida de cómo esté conformada, si dentro de la propia empresa, si son las mismas circunstancias y puede ser que haya dentro colectivos vulnerables, la propia edad que pueda tener, la medida edad que puede haber dentro de la empresa.

Entonces, al final son circunstancias que tienen que amoldarse a cada situación.

Eso respecto a la última pregunta. La primera que usted me planteaba, doctora, al final, creo que la población cada vez se está concienciando más sobre la protección de datos. Es decir, si bien es cierto que en prácticamente un porcentaje muy amplio de las empresas, la protección de datos era un tema bastante baladí y poco conocido, creo que los últimos, sobre todo dos, tres años, comienza a hacer una materia que, al menos, está en boca de todas las empresas, pero sobre todo, viene a ser un poco triste, pero no deja de ser el régimen sancionador de las normativas el que ha hecho que las entidades, que las empresas, que los ciudadanos empecemos a cumplir con esta normativa.

Y para ello, bueno, existen autoridades de control que, de alguna forma, vienen a velar por el cumplimiento de estas normativas, ya sea bien asesorando a los propios ciudadanos, bien imponiendo las multas correspondientes, bien realizando las auditorías que correspondan con los tratamientos de datos de determinada naturaleza.

Entonces, bueno, creo que estamos caminando en la buena dirección, lógicamente con un camino bastante amplio por recorrer, porque lógicamente está todavía prácticamente en la génesis de nosotros el comenzar con esta interiorización de los datos personales, si bien es cierto que bueno, al final no deja de ser una cosa que viene dándose desde que comienza a haber datos, sobre todo desde que comienza a haber datos automatizados a gran escala.

Y la siguiente pregunta, que de alguna forma están correlacionadas sobre hasta qué punto se debe invertir en inteligencia artificial por parte de los Estados y si de alguna forma tendría que haber acuerdos internacionales para que no haya hackeo o mafias internacionales que trabajen en este sentido, pues bueno, como venía diciendo anteriormente, al final, en el espacio económico europeo, por ejemplo, que contamos con una autoridad de control, digamos, común, a todos los Estados, que de alguna forma vela por el cumplimiento del reglamento y de alguna forma establece una serie de medidas, ya sea, por ejemplo, para la Interpol, para poder realizar investigaciones cuando se cedan datos internacionalmente, datos que sufren hackeos, datos

que sufren, empresas de seguridad por el tipo de transferencias que se realiza.

Entonces, al final, lógicamente tiene que entrar la cooperación entre los Estados para poder realizar este tipo de seguimiento. Al final, la inversión que se tiene que hacer en esta materia es muy amplia, pero no solamente por el tipo de derechos que se vulneran, que al final no dejan de ser derechos fundamentales, sino también por la magnitud del negocio que tiene también este tipo de sesiones y el tratamiento de los datos personales.

Digamos, que antes de que hubiera normativas que de alguna forma vinieran a regular las circunstancias de cómo se tenía que tratar los datos de las personas esto era, entre comillas, “un bufete libre de cesión de datos”. Es decir, donde al final unas empresas se los podían pasar a otras con fines totalmente diferentes sin que el ciudadano supiera por qué de respeten recibía una llama de una empresa que es cliente de otra, y a raíz de ahí se ha producido la cesión.

Al día de hoy eso no se puede hacer, es decir, si yo recibo una llamada de una empresa que me está llamando y me dice que me lo ha pasado un cliente suyo, pues lógicamente ese tratamiento no está legitimado.

Pues lógicamente si nos ponemos a pensar en grandes transferencias de datos para usos, se puede hablar de usos políticos, de usos bancarios, farmacéuticos, pues lógicamente aquí es cuando los estados se han dado cuenta de la necesidad de cooperar entre sí para poder resolver este tipo de situaciones, por tanto tiene que haber un mecanismo de regulación común, ya sea a nivel internacional, a nivel regional, para que de alguna forma exista coordinación en la materia, y me consta que existe coordinación entre los diferentes estados, porque, por ejemplo, en el caso, por ejemplo, de la Unión Europea está siempre estableciendo un listado actualizado de aquellos países con los que es seguro realizar transferencia internacionales de datos.

Por tanto es una materia, que como lo digo, está en absoluta actualización y la inversión de los estados es bastante potente en este año.

Dra. Jacqueline Peschard Mariscal: Pues muchas gracias por sus respuestas para todos pues esto que actualmente podrá consultarse su ponencia y la discusión que ha tenido.

Para mí es un honor haber estado con usted y haber podido acompañarlo en esta presentación que nos ayuda a países que vamos con una regulación no tan avanzada como en países europeos, pero que sí tenemos este referente que nos puede ayudar a mejorar nuestros marcos normativos y, sobre todo, al propósito último que es ofrecerles a las poblaciones, sobre todo a las más vulnerables herramientas para que puedan proteger adecuadamente sus datos personales.

Pues le agradezco mucho que haya estado aquí con nosotros, y muchas gracias al INAI por este espacio que nos ha ofrecido.

Muy buenas tardes para usted, buenos días.

Presentadora: De esta manera concluye la Conferencia Magistral *La importancia de la protección de los datos personales y el uso de las nuevas tecnologías en la nueva normalidad laboral y educativa.*

Agradecemos la participación del conferencista y de la presentadora Jacqueline Peschard Mariscal.

--oo0oo--