2017

Instituto de Acceso a la Información Pública

INFORME DE RESULTADOS

ACTIVIDAD: SEMINARIO "PRIVACIDAD Y COMUNICACIONES ELECTRÓNICAS" (MONTEVIDEO, 22 AL 23 DE NOVIEMBRE DE 2017) Y VISITA TÉCNICA A LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES (URCDP) (24 DE NOVIEMBRE DE 2017)

RENE EDUARDO CÁRCAMO/COMISIONADO

CARLOS HUMBERTO CALDERON MÓNCHEZ/UNIDAD DE PROTECCIÓN DE DATOS PERSONALES

Aprobación

Elaboró: Rene Eduardo Cárcamo Cargo: Comisionado Carlos Humberto Calderón Mónchez Cargo: Jefe de Unidad de Protección de Datos Personales. Fecha: 4 de diciembre 2017	**Revisó:** José Juan Marroquín Director Ejecutivo en funciones Fecha: 5 de diciembre de 2017	**Aprobó:** Carlos Ortega Comisionado Presidente Fecha:

I. Objetivo del informe

Realizar una sistematización de la experiencia del Seminario "Privacidad y comunicaciones electrónicas¨, que tuvo como objetivo debatir cuestiones relativas a las comunicaciones electrónicas que suscitan una mayor inquietud desde la perspectiva de la normativa de protección de datos, y en especial del Reglamento General de Protección de Datos aprobado por el Parlamento de Europa y su Consejo, dado que, en general se considera que los datos de una comunicación electrónica en que interviene una persona física constituyen datos personales.

En ese contexto, se realizó una visita técnica a la Unidad Reguladora y de Control de Datos Personales de la República Oriental de Uruguay, que tuvo como objetivo intercambiar experiencias en el control y la regulación de la normativa de protección de datos, así como de temas y actividades estratégicas para la promoción y garantía del derecho.

Estas actividades internacionales forman parte de las actividades enmarcadas en el Plan Estratégico del IAIP de cara a ejecutar en los próximos cinco años, específicamente en lo relacionado a "*Participar en las redes con instituciones homólogas, para el intercambio de experiencias y fortalecer la gestión estratégica institucional*" y como específica "*Participar en actividades con instituciones homologas*".

II. Antecedentes de la actividad

El Instituto a través de la Unidad de Protección de Datos Personales ha planteado como acciones estratégicas para estos cinco años, implementar un proceso eficaz de resolución para los casos de protección de los datos personales; asimismo, coadyuvar en la formación de aspectos básicos a los servidores públicos en esta materia, y en temas especializados dependiendo al tipo de datos que recopilan los entes obligados.

En esta lógica, parte de las actividades del plan operativo de la Unidad, se encuentra el gestionar con instituciones homólogas, el intercambio de experiencias para contribuir a las acciones antes mencionadas. En ese sentido, el Pleno recibió una invitación para designar dos representantes para asistir al Seminario "Privacidad y comunicaciones electrónicas", donde se abordarían temas como: a) Modelo de regulación de la privacidad en la comunicaciones electrónicas; b) Las comunicaciones electrónicas no deseadas; c) Las quiebras de seguridad; d) Las evaluaciones de impacto en protección de datos (EIPD) en el ámbito de las telecomunicaciones; e) El perfilado y las decisiones automatizadas; La Protección de la información almacenada en equipos terminales y relativa a los equipos; f)

El derecho a la portabilidad; g) La monitorización en el ámbito laboral; y, h) Inteligencia artificial, especialmente en relación con machine learning y big data. Transparencia de algoritmos.

En ese contexto, el Pleno designó a la Unidad de Protección de Datos Personales y al Comisionado Cárcamo para asistir a dicho evento, debido a que los temas son de un importante contenido académico y técnico, que coadyuva a las actividades y esfuerzos que se están realizando para la promoción y garantía de la Protección de Datos Personales en entes públicos, en específico, las actividades de normalización del expediente clínico, antecedentes policiales y penales, y el proyecto de Ley de Protección de Datos Personales.

Esto plantea la necesidad de capacitación y formación técnica, particularmente desde aquellos espacios académicos donde se aborden temáticas de vanguardia en temas de la protección de datos personales, en especial en las comunicaciones electrónicas.

III. Resultados obtenidos

Los principales resultados académicos y estratégicos del seminario, fueron los siguientes:

- La normativa que busque regular la privacidad en las comunicaciones electrónicas, deber ser amplia y neutra, debido a que convergen varias situaciones, tales como: la socioeconómica, tecnológica e institucional. Asimismo, se debe determinar si lo datos son confidenciales, aplicando el test del daño, es decir, el análisis si dicha información puede afectar el derecho al honor, a la intimidad personal y familiar y a la propia imagen.
- El Reglamento General de Protección de Datos aprobado por el Parlamento Europeo y su Consejo, es un marco de referencia para normar el derecho a la protección de datos personales en las comunicaciones electrónicas en nuestro país, ya que reconoce que un metadato es un dato personal, y regula lo relativo a las comunicaciones comerciales y publicitarias donde el consentimiento del usuario es primordial y que puede ser revocado en cualquier momento.
- Se conoció de la problemática que existe en el ámbito de las telecomunicaciones entre la seguridad y la innovación. La importancia que en las normativas se señale que los puntos de intercambio de tráfico de datos, se encuentren dentro del país, ya que eso permite aumentar los controles y por lo tanto la seguridad, generando confianza en los usuarios. También se deben establecer reglas claras en la utilización de los metadatos y las direcciones IP para casos legales, salvaguardando el derecho a la privacidad.
- Se conoció sobre los nuevos métodos que utilizan los agentes del mercado, para realizar comunicaciones no deseadas (como el spam). Existe el derecho de estos

agentes a comunicar, pero deben evitar el abuso, es por ello que debe normarse este tipo de situaciones, y contemplar reglas como la identificación del número, correo donde se efectúa la comunicación, establecer horarios protegidos y listas de opt-out (baja de usuarios). También un sistema de sanciones efectivo. En Iberoamérica Argentina y Chile tienen normativa sobre ello.

- La necesidad de que en la normativa pertinente, se defina que es un incidente de seguridad, que dichos incidentes deben ser comunicados a las autoridades y usuarios afectados. Los agentes del mercado e instituciones que recopilan datos deben monitorear sus sistemas de protección, deben priorizar la información, inspeccionar las situaciones que pueden acarrear una quiebra de seguridad y efectuar acciones de corrección, y sobre todo deben establecer acciones preventivas.
- Existen diferentes formas de la explotación de datos robados, como el "in the Shell keyloggers" (mide las pulsaciones de los teclados, sin conocimiento del usuario), "phishins kits" (robo de identidad a través de la recopilación de datos útiles por medio correo electrónicos falsos) y la comercialización de datos.
- La conveniencia de implementar en las organizaciones en específico en sus telecomunicaciones, sistema de evaluaciones de impacto en protección de datos, ya que permite crear confianza y resiliencia, evitando así la precepción negativa de la organización. Esto acompañado de la sensibilización y educación en el tema.
- Que debe existir normativa que regule el perfilado y las decisiones automatizadas, sobre todo la posibilidad de que las personas cuestionen esas decisiones, pedir explicaciones y a solicitar a no ser objeto de esas decisiones, basados en la premisa que esos perfiles son personas. Hay que tomar en cuenta que este tipo de actividades permite la vigilancia masiva, indiscriminada de forma automatizada de los individuos que conformamos la sociedad, vulnerando nuestro derecho a la privacidad y otras libertades.
- Los sistemas de telecomunicaciones de los países, deben garantizar que el registro de comunicaciones electrónicas de todos los usuarios, en poder de los agentes del mercado, debe permanecer almacenado en un plazo determinado por la ley, y que su consulta debe ser excepcional por orden judicial e investigaciones especificas realizadas por el Ministerio Público.
- Debe existir interoperabilidad entre los sistemas, para garantizar el derecho a la portabilidad de los datos, que es la potestad de mover mis datos a donde quiera. También regulación que indique que tipos de datos puedo trasladar, la forma de trasladarlos y los formatos.
- Que el empleador antes de efectuar la monitorización laboral debe cumplir el principio de transparencia de los datos personales, es decir, que debe informar sus

trabajadores que tipo de datos recopila y para qué. Asimismo, debe atender a un test de proporcionalidad y razonabilidad para decidir qué datos recopilará mediante la vigilancia y fiscalización, buscar sobre todo los métodos menos invasivos que pueden lesionar la privacidad e intimida de los trabajadores.

- También se obtuvo conocimientos sobre los principales desafíos del desarrollo de inteligencia artificial, los cuales son: 1) una concepción errada: 2) información engañosa sobre su desarrollo; 3) la conducta humana (utilización para propósitos ilícitos); 4) utilización para segmentar población (discriminación), es por ello que debe existir la transparencia en los algoritmos utilizados para efectuar alguna función.

Respecto a la visita a la URCDP, los resultados fueron los siguientes:

- La experiencia de la URCDP sobre el registro de sistemas de datos, merece para ellos dos opiniones, la primera que ayuda para la promoción del derecho, y la otra que dichos registros no abonan a la promoción y garantía, ya que deslegitiman el trabajo al no tener un objetivo claro en la protección de datos.
- El establecimiento de sectores de priorización del tema, esto permite promocionar el tema estratégicamente, y causa un efecto domino, ya que otros sectores al constatar beneficios buscan sumarse al esfuerzo.
- El compromiso de ambas instituciones de brindarse cooperación técnica relativa a asesorías en normativa, intercambio de expertos y funcionarios, capacitación del recurso humano, eventos de información y difusión, intercambio de información tecnológica y científicas de manera gratuita y las investigaciones conjuntas o paralelas en la relación a posibles contravenciones que requieran cooperación entre ambas instituciones en materia de datos personales.

IV. Proyectos / actividades propuestas como resultado de la actividad

- Firma de un Acuerdo de cooperación entre el IAIP y la URCDP en donde se establezca cooperación técnica relativa a asesorías en normativa, intercambio de expertos y funcionarios, capacitación del recurso humano, eventos de información y difusión, intercambio de información tecnológica y científicas de manera gratuita y las investigaciones conjuntas o paralelas en la relación a posibles contravenciones que requieran cooperación entre ambas instituciones en materia de datos personales.
- Realizar charlas sobre el tema de protección de datos personales en comunicaciones electrónicas a los servidores públicos del Instituto de Acceso a la Información Pública, en especial con la Unidad de Informática y Recursos Humanos.

- Analizar la Incorporación al proyecto de Ley de Protección de Datos Personales, lo pertinente a las medidas que garanticen la protección de datos en las comunicaciones electrónicas o la posible reforma a Ley de Telecomunicaciones en lo relativo a los registros que las empresas de comunicación almacenan de sus usuarios.
- Incorporar en el proyecto de ley de Protección de Datos Personales, el derecho a la portabilidad de los datos, que permitirá contar con un marco legal, cuando una persona quiere trasladar sus datos a otro responsable. Asimismo, analizar el aspecto de la interoperatividad para garantizar este derecho.
- Analizar la pertinencia del registro de sistemas de datos, en la Ley de Protección de Datos Personales

V. Conclusiones y/o recomendaciones

- Para la Unidad de Protección de Datos Personales, la experiencia fue fundamental en términos académicos, en los temas que se señalaron anteriormente.
- Reforzar la Unidad de Protección de Datos Personales con el personal técnico altamente capacitado para el tema, una complejidad y diversidad jurídica. Asimismo, promover una regulación legal de Protección de Datos Personales.
- La necesidad en impulsar en el Instituto, las facultades que la ley le otorga sobre la protección de datos personales, reflejándolo desde sus presupuestos, organización y compromiso tanto del personal de apoyo y operativo con el tema.
- Identificar sectores claves (salud, telecomunicaciones) para la promoción y garantía de la protección de datos personales, con el fin de que sea efecto multiplicador y coadyuven a que otros se sumen al esfuerzo.
- La necesidad de incorporar en la normativa nacional los avances en materia de datos personales que el Reglamento General de Protección de Datos y el Reglamento europeo de Privacidad y Comunicaciones Electrónicas ("E-Privacy") señalan, para que un futuro El Salvador pueda solicitar una Declaración de adecuación de su legislación con el marco europeo de protección de datos, con lo que supondría un aumento significativo de los intercambios comerciales con ese continente, como ha ocurrido con los dos países que hasta la fecha la han obtenido (Argentina y Uruguay).

VI. Anexos

a. Lecciones aprendidas.

- La necesidad de la aprobación de la Ley de Protección de Datos Personales, que permita la protección no jurisdiccional del derecho a la autodeterminación

informativa, para ello se debe concientizar a la población, tanques de pensamiento y clase política sobre la importancia del tema.

- La búsqueda de socios estratégicos nacionales e internacionales que se comprometan con el tema, tanto del sector público como del privado.

b. Otros relevantes

i. Documentos

Todos los documentos que fueron entregados están en formato electrónico, los cuales se enviarán a la gerencia ejecutiva de este Instituto.

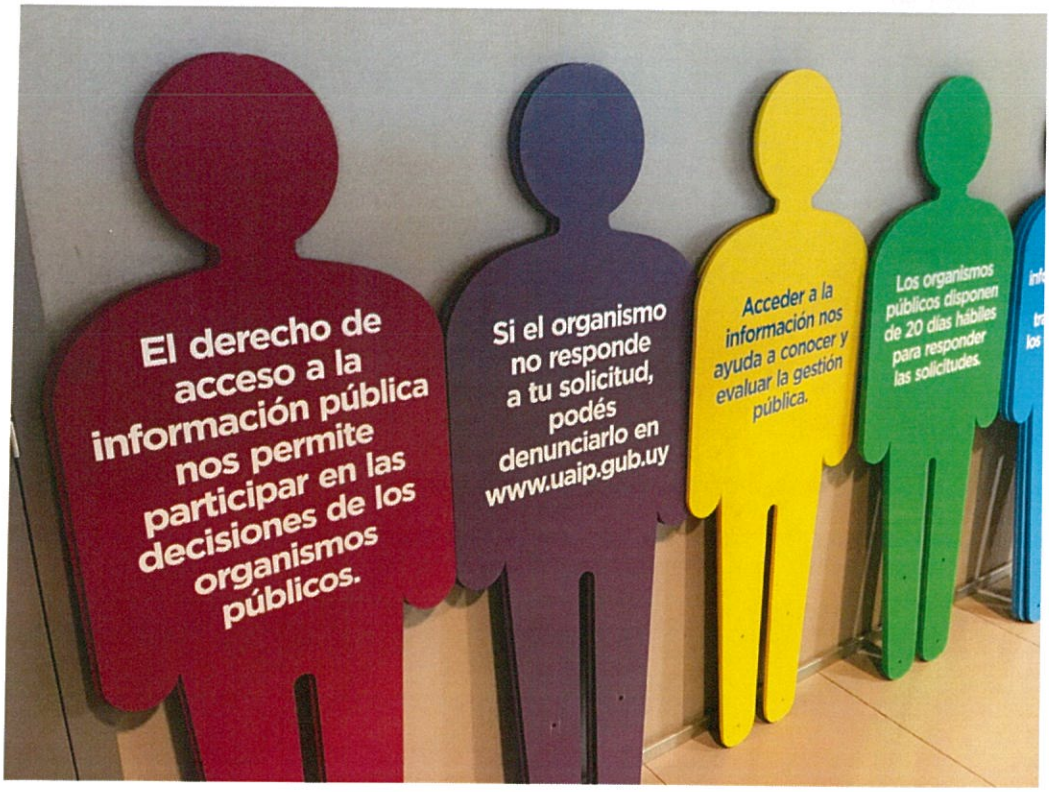
1. PRESENTACIONES

- El perfilado y las decisiones automatizadas (2 presentaciones).
- El nuevo ecosistema digital y la evaluación de impacto en protección de datos.
- Llamadas no deseadas.
- Monitorización en el ámbito laboral.
- Modelo de Regulación de la Privacidad en las Comunicaciones Electrónicas (3 presentaciones).
- Protección de Datos Personales en el marco de las Telecomunicaciones.
- Todo lo que siempre quisiste saber sobre Inteligencia Artificial/Big Data.
- Presentación de la Superintendencia de Industria y Comercio de Colombia.
- Derecho a la Portabilidad
- Comunicaciones Electrónicas no deseadas.
- La Protección de la información Almacenada en equipos terminales y relativa a los equipos (dos presentaciones).

2. BORRADOR DE ACUERDO DE COOPERACIÓN ENTRE EL IAIP EL SALVADOR Y LA URCDP

3. FOTOGRAFIAS


cooperación
española


El derecho de acceso a la información pública nos permite participar en las decisiones de los organismos públicos.
Si el organismo no responde a tu solicitud, podés denunciarlo en www.uaip.gub.uy
Acceder a la información nos ayuda a conocer y evaluar la gestión pública.
Los organismos públicos disponen de 20 días hábiles para responder las solicitudes.

Anexo: Formato de Lecciones aprendidas.

Actividad	Valoración (favorable o desfavorable)	Evaluación (+ o -)	Recomendación para futuras actividades
Participación en el Seminario "Pivacidad y comunicaciones electrónicas".	• El conocimiento sobre: a) Modelo de regulación de la privacidad en la comunicaciones electrónicas; b) Las comunicaciones electrónicas no deseadas; c) Las quiebras de seguridad; d) Las evaluaciones de impacto en protección de datos (EIPD) en el ámbito de las telecomunicaciones; e) El perfilado y las decisiones automatizadas; La Protección de la información almacenada en equipos terminales y	+	Es necesario establecer mesas de dialogo con la Institución Pública que fiscaliza las telecomunicaciones, para revisar si la normativa se adecua con los estándares europeos en protección de datos en comunicaciones electrónicas.

relativa a los equipos; f) El derecho a la portabilidad; g) La monitorización en el ámbito laboral; y, h) Inteligencia artificial, especialmente en relación con machine learning y big data. Transparencia de algoritmos.		
• La necesidad de promocionar y sensibilizar académicamente a la población sobre la protección de datos personales.	+	Es necesario adecuar el anteproyecto de la Ley de Protección de Datos Personales se establezca la inclusión en los programas educativos sobre la protección de datos.

Nota aclaratoria:

Actividad: Acción realizada para el cumplimiento de la meta programada

Valoración: Breve descripción de la lección aprendida

Evaluación: Colocar signo:

(+) Si es positiva yetirse.

(-) Si es negativa y debe evitar que ocurra.

Recomendaciones:

Acciones y/o condiciones que deban ser tomadas en cuenta en próximos eventos.

Instituto de Acceso
a la Información Pública