Asunto: A/RES/68/167
"El derecho a la privacidad en la era digital"

Documento preparado por la Unidad Reguladora y de Control de Datos Personales de la República Oriental del Uruguay en respuesta a la solicitud realizada por la Oficina del Alto Comisionado para los Derechos Humanos con relación a la implementación de la Resolución 68/167.

1. **¿Qué medidas se han tomado a nivel nacional para asegurar el respeto y la protección del derecho a la privacidad, incluido en el contexto de la comunicación digital?**

En Uruguay, el derecho a la protección de datos personales se encuentra reconocido en el artículo 72 de la Constitución de la República como un derecho inherente a la persona humana.

De acuerdo a ello, en el año 2008 se aprobó la Ley Nº 18.331 de 11 de agosto de 2008 que regula la protección de datos personales y la acción de habeas data, la cual fue posteriormente reglamentada por el decreto Nº 414/009. El artículo 1º de la Ley expresa que la protección de datos personales es un derecho humano y se encuentra comprendido dentro del artículo constitucional mencionado anteriormente.

La Ley crea en el artículo 31 el órgano de control encargado de vigilar el cumplimiento de la normativa en la materia, denominado Unidad Reguladora y de Control de Datos Personales. Dicha Unidad está dotada de amplia autonomía técnica con competencia en todo el país. Se crea como un órgano desconcentrado de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y Sociedad de la Información y del Conocimiento (Agesic). La Unidad está dirigida por un Consejo integrado por tres miembros, uno de ellos es el Director Ejecutivo de Agesic, y dos designados por el Poder Ejecutivo.

La creación de un órgano de control en la materia ha sido de gran importancia para el desarrollo del derecho a la protección de datos personales. Ha significado la puesta en marcha de diversas actividades tendientes a concientizar a la población en el conocimiento y la importancia de la protección de sus datos, así como en el fortalecimiento del ejercicio de los derechos con los cuales son empoderados en la normativa. Asimismo, se ha trabajado en el posicionamiento del país en el contexto internacional a través de la vinculación con otras autoridades de control y redes de cooperación en la materia.

Desde sus comienzos, la Unidad ha desarrollado importantes tareas de capacitación y sensibilización dirigidas a diferentes sectores de la sociedad incluyendo a las personas, empresas y organismos del Estado. Además ha hecho énfasis en la capacitación de niños, adolescentes y sus familias a través de campañas dirigidas a las escuelas públicas y privadas del país.

Dentro de las competencias de la Unidad, se destaca la de asistir y asesorar a las personas acerca del alcance de la Ley, y de los medios de los que disponen para garantizar sus derechos, así como controlar la observancia del régimen legal. En este marco recibe consultas y denuncias sobre las cuales emite resoluciones y dictámenes. De esta manera resuelve la aplicación de la normativa a las situaciones concretas.

En este marco, se destacan resoluciones relativas a la incorporación de políticas de privacidad en todo sitio web que efectué tratamiento de datos personales en el Uruguay, en adecuación a lo dispuesto por la Ley 18.331. También se emitió resolución recomendando a los responsables de publicar contenidos en los sitios web de los organismos públicos, la adopción de algún criterio técnico para evitar la indexación de la información por los motores de búsqueda. Las resoluciones de la Unidad pueden ser consultadas en www.datospersonales.gub.uy.

2. ¿Qué medidas fueron adoptadas para prevenir violaciones al derecho a la privacidad, incluidas las que aseguran que la legislación nacional relevante cumpla con las obligaciones de los Estados Miembros bajo la legislación internacional?

Como punto de partida, el marco normativo vigente establece una serie de principios rectores en la materia que rigen el tratamiento lícito de los datos personales, destacándose los principios de previo consentimiento informado y el de finalidad del tratamiento.

También la norma reconoce a las personas, dentro del marco del derecho a la protección de datos personales, una serie de derechos derivados que los empoderan con el objetivo de tutelar sus datos personales y ejercer un control efectivo sobre éstos. Estos son: el derecho a la información frente a la recolección de datos, el derecho de acceso y los derechos de rectificación, actualización, inclusión o supresión. Conforme con la normativa, estos derechos son ejercidos directamente por el titular ante el responsable del tratamiento, quien en un plazo de 5 días hábiles deberá dar respuesta. En caso de no hacerlo, la legislación prevé dos garantías adicionales. Por un lado, la posibilidad de ejercer la acción de habeas data en la vía judicial, y por otro, presentar una denuncia ante la Unidad Reguladora y de Control de Protección de Datos Personales.

Otra medida de control prevista en la Ley es la aplicada a las bases de datos personales tanto públicas como privadas cualquiera sea el soporte en el cual se encuentre la información. La Ley condiciona la legalidad de estas bases a su inscripción en el Registro que a estos efectos lleva la Unidad. A ello se agrega que el principio de legalidad establece que las bases de datos no pueden tener finalidades violatorias de derechos humanos, ser contrarias a las leyes o a la moral pública.

Otras garantías que establece la ley y que resultan de gran relevancia son las asociadas a las potestades de la Unidad respecto a los responsables de bases de datos, entre ellas, las relativas a la posibilidad de solicitar información y a la realización de inspecciones y auditorías.

3. ¿Qué medidas específicas fueron tomadas para asegurar que los procedimientos, prácticas y legislación sobre la vigilancia de las comunicaciones, su intercepción y recolección de datos personales, son coherentes con las obligaciones de los Estados Miembros bajo la legislación internacional?

En el ordenamiento jurídico uruguayo se cuenta con la regulación del delito de atentado contra la irregularidad de las telecomunicaciones, el cual fue incorporado por la Ley Nº 18.383, de 17 de octubre de 2008, modificando el Código Penal. A través de este delito, se penaliza al que, de cualquier manera, atente contra la regularidad de las telecomunicaciones alámbricas o inalámbricas, previendo una pena de tres meses de prisión a tres años de penitenciaría. Se considera agravante especial de este delito, la sustracción, el daño o la destrucción de instalaciones destinadas a las prestaciones del servicio de telecomunicaciones.

No se cuenta actualmente con delitos específicos en materia de datos personales. Igualmente son aplicables las disposiciones relativas a la revelación de secreto profesional previsto en el Código Penal (artículo 302), siendo éste el criterio seguido por la jurisprudencia nacional.

Asimismo, la Ley Nº 18.331 prevé la posibilidad de aplicar sanciones administrativas a los responsables de bases de datos, encargados de tratamiento y demás sujetos alcanzados por el régimen legal en caso de violación a la normativa vigente. Estas sanciones van desde la observación, el apercibimiento, la multa de hasta 500.000 UI (unidad indexada), la suspensión de la base de datos por 5 días, hasta la clausura de la base de datos respectiva.

4. ¿Qué medidas han sido adoptadas para establecer y mantener la independencia de los mecanismos efectivos capaces de asegurar la transparencia y rendición de cuentas de las comunicaciones vigiladas o interceptadas por los Estados y la recolección de datos personales?

En el marco de la protección de datos personales, las bases de datos de titularidad pública se encuentran alcanzadas por la normativa, debiéndose cumplir con todos los extremos que ella establece. De acuerdo a ello, quedan sujetas a la supervisión del órgano de control que cuenta con amplia autonomía técnica.

En la definición de su ámbito objetivo de aplicación, la Ley Nº 18.331 excluye expresamente las bases de datos que tengan por objeto la seguridad pública, la defensa, la seguridad el Estado y sus actividades en materia penal, investigación y represión del delito. Además, se incluye un capítulo que se encarga de regular en forma específica las bases de datos de titularidad pública.

Específicamente en materia de datos relativos a las telecomunicaciones, el artículo 20 de la referida Ley dispone que los operadores que exploten redes públicas o que presten servicios de comunicaciones electrónicas disponibles al público deberán garantizar, en el ejercicio de su actividad, la protección de los datos personales conforme a la ley.

Asimismo, deberán adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad en la explotación de su red o en la prestación de sus servicios, con el fin de garantizar sus niveles de protección de los datos personales. En caso de que exista un riesgo particular de violación de la seguridad de la red pública de comunicaciones electrónicas, el operador que explote dicha red o preste el servicio de comunicaciones electrónicas deberá informar a los abonados sobre dicho riesgo y sobre las medidas a adoptar.

La regulación contenida en esta ley se entiende sin perjuicio de lo previsto en la normativa específica sobre telecomunicaciones relacionadas con la seguridad pública y la defensa nacional.

Cabe destacar que la Ley establece una garantía adicional al consagrar la acción de habeas data como una acción judicial efectiva para tomar conocimiento de los datos referidos a la persona y de su finalidad y uso, que consten en bases de datos públicas o privadas, y exigir la rectificación, inclusión o supresión de los datos que se entienda corresponder. Además, establece que cuando se trate de datos personales cuyo registro este amparado por una norma legal que consagre el secreto a su respecto, el Juez apreciará el levantamiento del mismo en atención a las circunstancias del caso.

5. Cualquier otra información sobre la protección y promoción del derecho a la privacidad en el contexto de la vigilancia doméstica y extraterritorial y en la intercepción de las comunicaciones personales, así como en la recolección de datos personales.

A efectos de promover la protección de datos personales en el ámbito internacional, la Unidad ha trabajado fuertemente en desarrollar la cooperación internacional. Es así que ha establecido convenios de cooperación en materia de protección de datos personales con diversos países. También ha pasado a formar parte de la Red Iberoamericana de Protección de Datos así como del Comité Organizador de la Conferencia Internacional de Protección de Datos.

Además, el país ha sido declarado país adecuado a los estándares de la Unión Europea de conformidad con la "Directiva 95/46/CE". Se trata de un reconocimiento a Uruguay como país en condiciones de asumir el desafío de cumplir con los controles que exige la Unión Europea en el uso de los datos personales y a la tarea realizada por la Unidad Reguladora y de Control de Datos Personales. Su importancia radica en que favorece el flujo de datos y la transferencia de información. Esto es posible porque nuestro país garantiza la debida salvaguarda o tutela de los datos personales. A partir de ahora, las transferencias de datos personales entre países adecuados podrán realizarse sin necesidad de autorización de la Autoridad de Control.

También fue el primer país no europeo en adherir al Convenio Nº 108 ante el Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y su Protocolo Adicional a las autoridades de control y a los flujos transfronterizos de datos

Montevideo, 24 de marzo de 2014