Título Otros aspectos legales de la privacidad

Tipo de Producto Material Didáctico

Autores Galmarini, Luciano

Seminario Interno, materias Derecho Informático y de la Propiedad Intelectual, Carrera de Abogacía, y Derecho Informático, Carreras de Ingeniería en Informática y Licenciatura en Gestión Ambiental de Tecnología de la Información

Código del Proyecto y Título del Proyecto

P17S06 - La protección de los datos en la era del Big Data, y el acceso a la información en el "Estado Recolector"

Responsable del Proyecto

Toscano, Silvia

Línea

Derecho Empresarial

Área Temática

Derecho

Fecha

Octubre 2017

INSOD
Instituto de Ciencias Sociales y Disciplinas Proyectuales

FUNDACIÓN UADE

Otros Aspectos Legales de la Privacidad

La Privacidad en la Internet de las Cosas

- IoT (Internet of Things): interconexión digital de objetos cotidianos con Internet.
- Productos equipados con conectividad inalámbrica a Internet, que generan una gran cantidad de información que es enviada en tiempo real a la web.
- Para 2020 se estima que habrá 2.400 millones de productos con IoT.
- ¿Pueden afectar la privacidad y seguridad de nuestra información? No hay una regulación legal específica.

La Privacidad en la Internet de las Cosas

- El volumen de información que generan estos objetos “inteligentes” es difícil de controlar.
- Existen tantas direcciones IP, sensores, teléfonos, relojes, alarmas, cámaras, electrodomésticos y automóviles conectados a Internet, que no somos conscientes de las aplicaciones con las que interactuamos y cuyo funcionamiento no autorizamos expresamente; y en las que dejamos un rastro.

La Privacidad en la Internet de las Cosas

- Un celular conectado con un producto IoT: permite conocer patrones de conducta del usuario, como sus estados de ánimo, hábitos, nivel de stress, tipo de personalidad, progresión de una enfermedad).
- Un producto hogareño con IoT: permite saber cuando la casa está vacía, o ocupada por niños o personas ancianas.

La Privacidad en la Internet de las Cosas

- Por medio de un sistema IoT del automóvil: se pueden conocer los hábitos de manejo del usuario, a qué lugares suele ir, en qué horario, con qué clima y en que compañía. Una aseguradora puede calcular la prima gracias a estos datos.
- La aplicación de fitness: permite que una prepaga sepa cuantas veces nos ejercitamos al día, donde y con qué intensidad. De allí a medir el riesgo cardíaco (y la prima) hay un solo paso.

La Seguridad en la Internet de las Cosas

- La vulnerabilidad de la IoT pone en riesgo la privacidad del usuario: una cuestión tecnológica, como la arquitectura de seguridad de los productos con IoT, trae consecuencias sobre derechos reconocidos en la CN.
- Cualquiera de estos productos puede ser fácilmente "hackeado": se puede acceder a ellos desde muchos puntos, y sus programas son lo suficientemente conocidos para un "hacker". Una vez vulneradas las defensas de uno de estos productos, puede replicarse su acción en todos los que sean similares.

La Seguridad en la Internet de las Cosas

- ¿Existe en el mercado quien garantice la seguridad y privacidad de la información que los IoT trasladan a la nube?
- ¿Quién es el responsable de tener al día las actualizaciones en materia de seguridad en routers y cualquier medio de acceso a la nube?
- ¿Qué ocurre cuando el vendedor del producto IoT descontinúa la fabricación y ya no da soporte al usuario?
- ¿Quién es el propietario de los datos recolectados y generados por los productos con IoT?
- ¿Qué ocurre cuando los productos IoT actúan independientemente de la voluntad o el conocimiento del usuario?

La Seguridad en la Internet de las Cosas

- La velocidad con que se desarrollan y lanzan al mercado estos productos, provoca que en muchos casos no haya protocolos de seguridad generalmente aceptados.
- En contados casos, se encriptan los datos que se recolectan y transmiten.
- En general, las contraseñas que usan son muy simples.

La Seguridad en la Internet de las Cosas

- La seguridad no solo debe concentrarse en cada aparato con IoT, sino en cada app de software y redes que se conectan con los productos.
- Algunos desarrollos ofrecen la posibilidad de clickear un link y ver que datos tiene el fabricante sobre ellos, para ejercer su derecho a la privacidad, suprimiendo la información de modo permanente, o tornándola confidencial.
- En la práctica, se terminan consintiendo términos de uso, que permiten compartir información privada con el fabricante.

Drones y Cámaras de Videovigilancia

- El avance de la tecnología permite realizar actividades de tratamiento de datos personales a través de nuevos dispositivos y sistemas, que por sus particularidades y eventual peligrosidad, en cuanto a la preservación de los derechos de las personas, requieren una normativa particular.

Drones y Cámaras de Videovigilancia

- Una imagen, un registro fílmico o sonoro, constituyen un dato personal, en tanto se refiere a una persona determinada o determinable
- Su tratamiento a través de sistemas informáticos, constituye una base de datos en tanto conforma un sistema organizado de fácil consulta.

Drones y Cámaras de Videovigilancia

- **Drones**: todo vehículo no tripulado terrestre, subterráneo, marino, submarino y aéreo. Estos dispositivos pueden desplazarse, lo que encierra una afectación particular a la privacidad.
- **VANTs**: todo dispositivo que se desplaza por el aire sin una persona a bordo (en algunos casos no detectable).
- **Actividades de video vigilancia**: el tratamiento de imágenes digitales de personas con fines de seguridad mediante cámaras que se encuentran en una posición fija.

La utilización de Drones y la privacidad

- **VANTs**: vehículos aéreos no tripulados, capaces de mantener un nivel de vuelo controlado y sostenido, que pueden ser piloteados a distancia o en forma remota, desde uno o varios puntos de control, e incluso, ser programados para su vuelo en forma autónoma con un software específico.
- **ANAC**: Reglamento Provisional de los Vehículos Aéreos No Tripulados (materia aeronáutica).
- **DNPDP**: Condiciones de Licitud para la captura de datos personales mediante VANTs o Drones.

DISPOSICIÓN 20/2015 DNPDP

- Art 1: aprueba las “Condiciones de Licitud para la Recolección de Datos Personales a través de VANTs o drones” (Anexo I).
- Art. 3: aprueba las “Recomendaciones Relativas a la Privacidad en el Uso de VANTs o drones” (Anexo II).

Anexo I: Requisitos de Licitud

- La recolección de datos personales (fotográficos, fílmicos, sonoros o de cualquier otra naturaleza) en formato digital, a través de dispositivos colocados en VANTs o drones, para su posterior almacenamiento o tratamiento, será lícita en la medida que se realice con el consentimiento del titular del dato según lo previsto en los arts. 5 y 6 de la Ley N° 25.326.

Anexo I: Requisitos de Licitud - Excepciones

- No se requerirá el consentimiento (en la medida que los VANTs o drones no impliquen una intromisión desproporcionada en la privacidad del titular del dato), cuando los datos se recolecten con motivo de:
- a) la realización de un acto público o hecho sobre el que pueda presumirse la existencia de un interés general para su conocimiento y difusión al público;
- b) la realización de un evento privado por parte del organizador o responsable del evento, que respondan a usos y costumbres (casamientos, fiestas, etc.);

Anexo I: Requisitos de Licitud - Excepciones

- c) la atención a personas en situaciones de emergencia o siniestros;
- d) los datos se recolecten dentro de un predio de uso propio y/o su perímetro sin invadir el espacio de uso público o de terceros, salvo en aquello que resulte una consecuencia inevitable, debiendo restringirlo al mínimo necesario.
- e) la recolección de los datos la realice el ESTADO NACIONAL en el ejercicio de sus funciones;

Anexo I: Obligaciones

- El Responsable del tratamiento debe:
- usar medios técnicos de recolección proporcionados, pertinentes y no excesivos respecto de la finalidad que motiva dicha recolección, verificando que no afecten el derecho a la intimidad del titular del dato.
- cumplir con los mecanismos técnicos de seguridad y confidencialidad.
- inscribirse en el Registro de la DNPDP.
- contar con un Manual o Política de tratamiento de datos personales y privacidad.

Anexo I: Obligaciones

- El Manual debe contener:
- la finalidad de la recolección,
- referencia de los lugares, fechas y horarios en los que se prevé que operarán los VANTs o drones,
- el plazo de conservación de los datos,
- las tecnologías a utilizar para la disociación de los datos (indicando si es reversible o no),
- los mecanismos técnicos de seguridad y confidencialidad previstos,
- las medidas dispuestas para el ejercicio de los derechos del titular del dato.

Anexo I: Fines Científicos

- Las recolecciones de datos a través de VANTs o drones que tengan por finalidad la realización de estudios científicos, cartográficos, sobre recursos naturales, medio ambiente o actividades análogas, que no tengan por objeto la recolección de datos personales.

Anexo I: Fines Científicos

- En el caso que por razones técnicas no pueda evitarse la recolección de datos personales, se deberá aplicar sobre dichos datos, en el más breve lapso que las reglas del arte lo permitan, una técnica de disociación definitiva (difuminación de la imagen), de modo que no permita identificar a persona alguna mediante su tratamiento.

Anexo II: Drones con Fines Recreativos

- Cuando se utilicen VANTs o drones con fines exclusivamente recreativos y sin la finalidad de capturar datos personales de terceros, se deberán observar las RECOMENDACIONES RELATIVAS A LA PRIVACIDAD EN EL USO DE VANTs O DRONES (Anexo II).
- Principio: las personas mantienen el derecho a la privacidad y a su imagen aún en espacios públicos.

Anexo II: Drones con Fines Recreativos

- a) El uso recreativo de VANTs o drones debe hacerse teniendo en consideración las implicancias que tiene sobre la privacidad de las personas, debiendo dar un uso prudencial al mismo, evitando la observación, entrometimiento o molestia en la vida y actividades de terceros.
- b) No podrá considerarse uso recreativo si se utiliza el VANT o dron con la finalidad expresa de recolectar datos personales de terceros.

Anexo II: Drones con Fines Recreativos

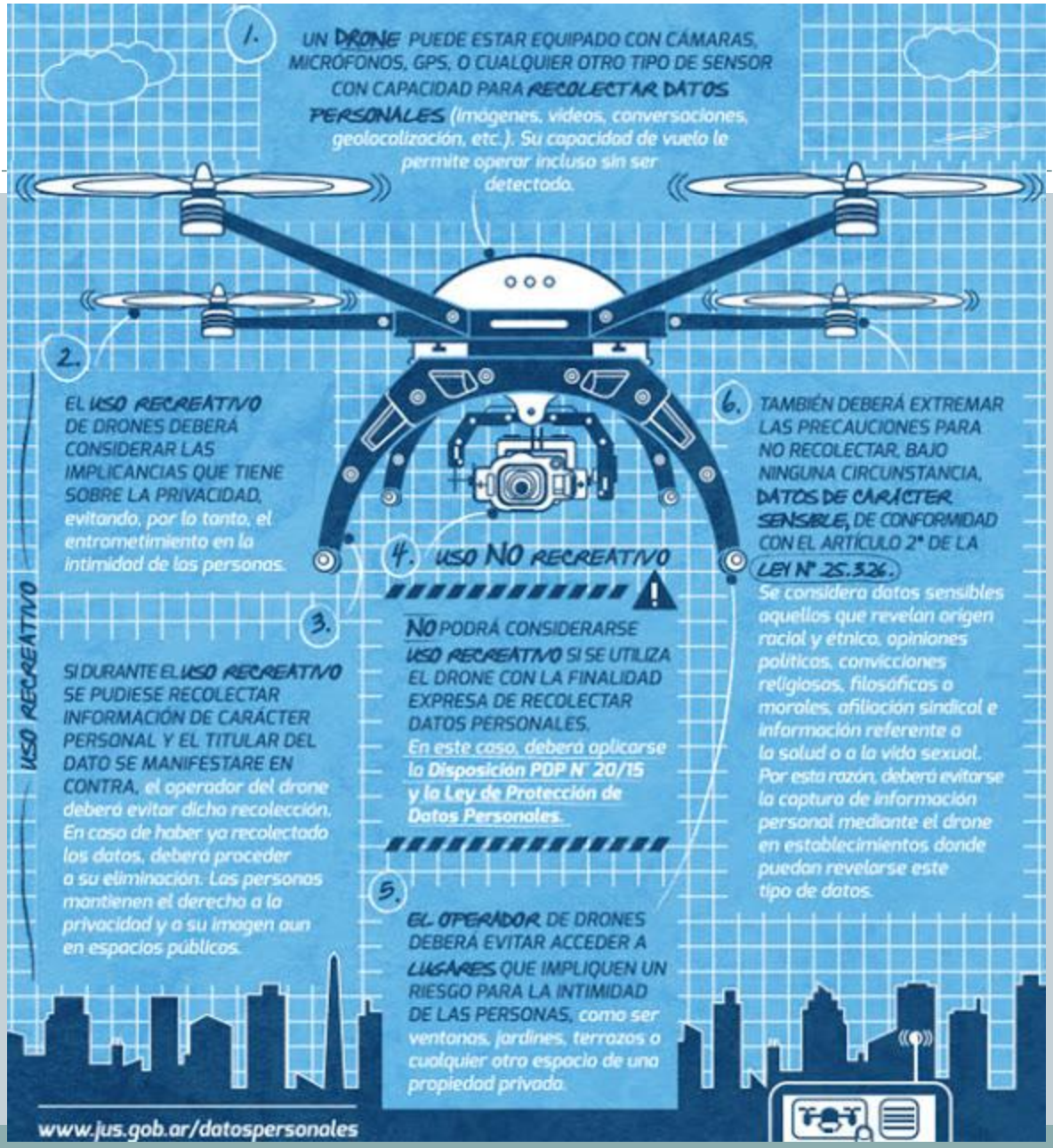
- c) La utilización de VANTs o drones en espacios públicos con alta conglomeración de personas tendrá mayores posibilidades de una recolección incidental, por lo que el operador deberá extremar las precauciones para resguardar la privacidad de terceros.
- d) Si incidentalmente se pudiese recolectar información de carácter personal y el titular del dato se opone, el operador del VANT o dron debe evitar dicha recolección, y en caso de haberla recolectado, proceder a su eliminación.

Anexo II: Drones con Fines Recreativos

- e) El operador de VANTs o drones debe evitar acceder a lugares que impliquen un riesgo para la intimidad de las personas (ventanas, jardines, terrazas o cualquier otro espacio de una propiedad privada cuyo acceso no le fuere previamente autorizado).

Anexo II: Drones con Fines Recreativos

- f) El operador de VANTs o drones debe extremar las precauciones para no recolectar bajo ninguna circunstancia datos íntimos o de carácter sensible de conformidad al art. 2 de la Ley N° 25.326.
- Debe evitarse la captura de información personal en establecimientos de salud, lugares de culto, manifestaciones políticas o sindicales, y en aquellos lugares donde se pueda presumir la preferencia sexual de las personas, entre otros.


1.
UN DRONE PUEDE ESTAR EQUIPADO CON CÁMARAS, MICRÓFONOS, GPS, O CUALQUIER OTRO TIPO DE SENSOR CON CAPACIDAD PARA RECOLECTAR DATOS PERSONALES (imágenes, videos, conversaciones, geolocalización, etc.). Su capacidad de vuelo le permite operar incluso sin ser detectado.
2.
EL USO RECREATIVO DE DRONES DEBERÁ CONSIDERAR LAS IMPLICANCIAS QUE TIENE SOBRE LA PRIVACIDAD, evitando, por lo tanto, el entrometimiento en la intimidad de las personas.
3.
SI DURANTE EL USO RECREATIVO SE PUDIESE RECOLECTAR INFORMACIÓN DE CARÁCTER PERSONAL Y EL TITULAR DEL DATO SE MANIFESTARE EN CONTRA, el operador del drone deberá evitar dicha recolección. En caso de haber ya recolectado los datos, deberá proceder a su eliminación. Las personas mantienen el derecho a la privacidad y a su imagen aun en espacios públicos.
USO RECREATIVO
4. USO NO RECREATIVO
NO PODRÁ CONSIDERARSE USO RECREATIVO SI SE UTILIZA EL DRONE CON LA FINALIDAD EXPRESA DE RECOLECTAR DATOS PERSONALES. En este caso, deberá aplicarse la Disposición PDP N° 20/15 y la Ley de Protección de Datos Personales.
5.
EL OPERADOR DE DRONES DEBERÁ EVITAR ACCEDER A LUGARES QUE IMPLIQUEN UN RIESGO PARA LA INTIMIDAD DE LAS PERSONAS, como ser ventanas, jardines, terrazos o cualquier otro espacio de una propiedad privada.
6.
TAMBIÉN DEBERÁ EXTREMAR LAS PRECAUCIONES PARA NO RECOLECTAR, BAJO NINGUNA CIRCUNSTANCIA, DATOS DE CARÁCTER SENSIBLE, DE CONFORMIDAD CON EL ARTÍCULO 2° DE LA LEY N° 25.326.
Se considera datos sensibles aquellos que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual. Por esta razón, deberá evitarse la captura de información personal mediante el drone en establecimientos donde puedan revelarse este tipo de datos.
www.jus.gob.ar/datospersonales

Disposición 10/2015 DNPDP

- Art. 1: aprueba las condiciones de licitud para las actividades de recolección y posterior tratamiento de imágenes digitales de personas, con fines de seguridad (Anexo I).
- Art. 2°: aprueba el modelo de diseño de cartel que podrá ser utilizado en el caso de recolección de imágenes digitales, en cumplimiento del requisito de información previa al titular del dato (Anexo II).

Anexo I: Requisitos de licitud

- La recolección de imágenes digitales de las personas a través de cámaras de seguridad será lícita en la medida que cuente con el consentimiento previo e informado del titular del dato en los términos de los arts. 5 y 6 de la Ley N° 25.326.

Anexo I: Requisitos de licitud

- El cumplimiento del requisito de información previa debe realizarse a través de carteles que en forma clara indiquen:
- - la existencia de dichos dispositivos de seguridad (sin que sea necesario precisar su emplazamiento puntual),
- - los fines de la captación de las imágenes, y
- - el responsable del tratamiento con su domicilio y datos de contacto para el correcto ejercicio de los derechos por parte del titular del dato.

Anexo I: Requisitos de licitud - Excepciones

- No será necesario requerir el consentimiento previo del titular del dato, siempre y cuando la recolección de las imágenes personales no impliquen una intromisión desproporcionada en su privacidad, cuando los datos se recolecten:
- a) con motivo de la realización de un evento privado en el que la recolección de los datos sea efectuada por parte del organizador o responsable del evento;

Anexo I: Requisitos de licitud - Excepciones

- b) dentro de un predio de uso propio y/o su perímetro, sin invadir el espacio de uso público o de terceros, salvo en aquello que resulte una consecuencia inevitable, debiendo restringirlo al mínimo necesario.
- c) la realice el Estado en ejercicio de sus funciones; sin perjuicio de ello, en las oficinas y/o establecimientos públicos deberá hacerse saber dicha recolección;

Anexo I: Calidad del dato

- Las imágenes registradas no podrán ser utilizadas para una finalidad distinta o incompatible a la que motivó su captación.
- El Estado sólo podrá disponer su difusión al público cuando se encuentre autorizado por ley o por decisión de funcionario competente y medie un interés general que lo justifique.

Anexo I: Calidad del dato

- La información que se recabe debe ser adecuada, pertinente y no excesiva en relación a la finalidad para la que se hubiera obtenido.
- Debe cuidarse que las imágenes obtenidas se relacionen estrictamente con los fines perseguidos evitándose la captación de detalles que no sean relevantes para la consecución de los objetivos que justifican la recolección del material fotográfico o fílmico.

Anexo I: Calidad del dato

- Debe evitarse cualquier afectación del derecho a la privacidad, cuidando de no instalar dispositivos de captación de imágenes en ámbitos inapropiados que no permitan verificar la debida proporcionalidad entre las razones de seguridad que motivan la toma de las imágenes y la intromisión efectuada en la intimidad de las personas.

Anexo I: Calidad del dato

- Las imágenes registradas que sean atentatorias de los derechos de las personas (ej. intimidad) deben ser eliminadas en cuanto ello fuera constatado por el responsable o a pedido del titular del dato, lo que resulte primero.
- Debe determinarse el tiempo por el cual resultará de utilidad el registro de las imágenes, y eliminarse las mismas una vez vencido el plazo.

Anexo I: Derechos del titular del dato

- El responsable del tratamiento de datos debe prever la entrega de la información personal que soliciten los titulares a través del derecho de acceso y su rectificación o supresión en caso que sea procedente.

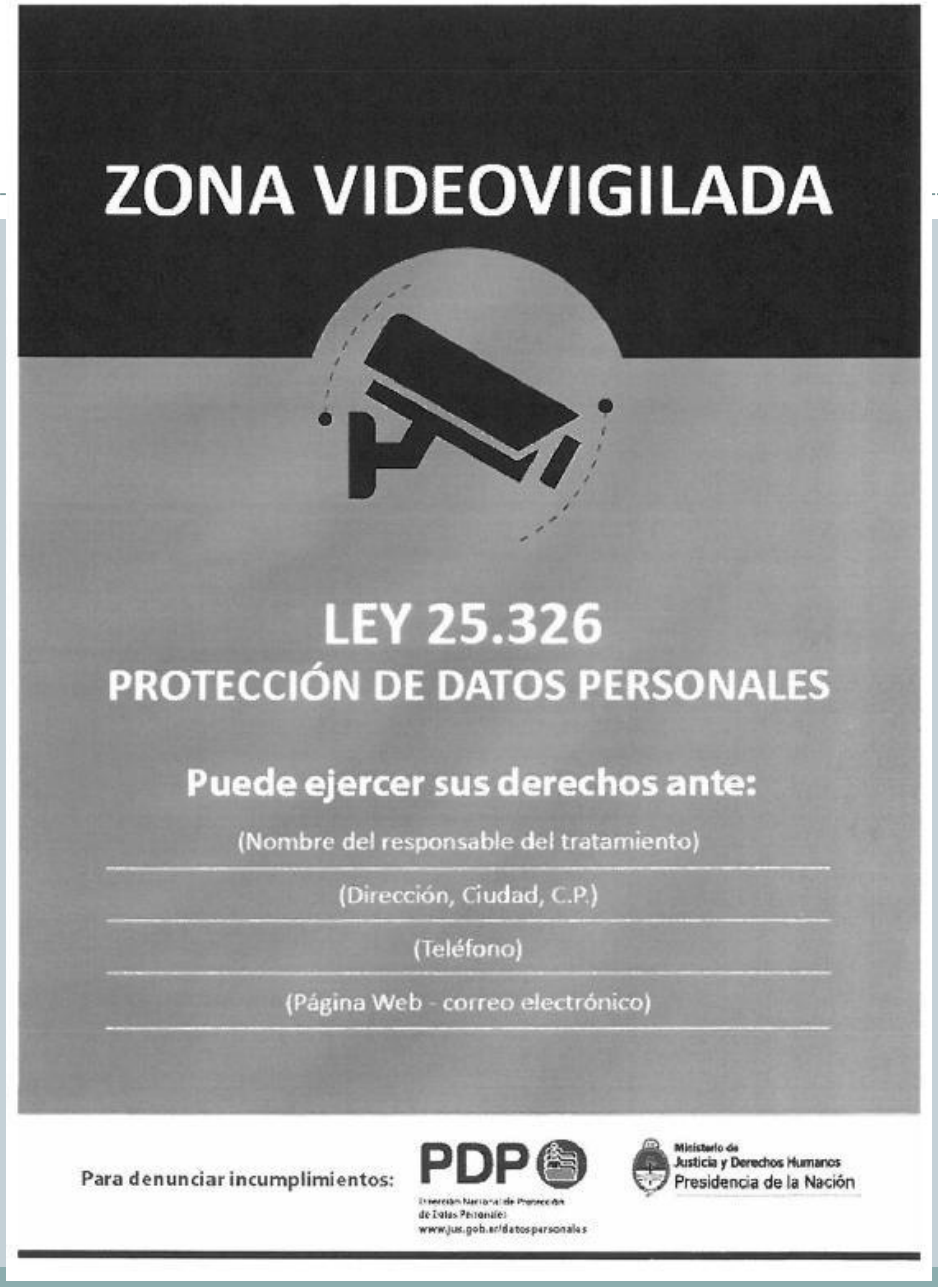
Anexo I: Obligaciones

- El responsable de la bases de datos debe:
- - adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales.
- - inscribirse en el Registro de la DNPDP.
- - contar con un Manual o Política de tratamiento de datos personales y privacidad, que ponga en práctica las condiciones de licitud previstas en la Ley N° 25.326.

Anexo I: Obligaciones

- El Manual debe contener:
- forma de recolección;
- referencia de los lugares, fechas y horarios en los que se prevé que operarán;
- plazo de conservación de los datos;
- mecanismos técnicos de seguridad y confidencialidad previstos;
- medidas dispuestas para el cumplimiento de los derechos del titular del dato;
- los argumentos que justifiquen la toma de fotografías para el ingreso al predio, en caso de disponerse dicha medida de seguridad.

Anexo II:


ZONA VIDEOVIGILADA
LEY 25.326
PROTECCIÓN DE DATOS PERSONALES
Puede ejercer sus derechos ante:
(Nombre del responsable del tratamiento)
(Dirección, Ciudad, C.P.)
(Teléfono)
(Página Web - correo electrónico)
Para denunciar incumplimientos:
PDP
www.jus.gob.ar/datospersonales
Ministerio de Justicia y Derechos Humanos
Presidencia de la Nación