Protección de datos personales

Abregú Lucas Gonzalo - Guerra Jésica Marinés - Ledesma Rubén Darío
Estudiantes de Licenciatura en Análisis de Sistemas
Departamento de Informática - Universidad Nacional de Salta
Avenida Bolivia 5150 CP 4440, Argentina
lgabregu@gmail.com.ar; jesica92.guerra@gmail.com;
rdledesma1995@gmail.com

Tutor: Abgª. Royano, Griselda Liliana
Docente Responsable de Cátedra de Derecho de la Informática
Departamento de Informática - Universidad Nacional de Salta
Avenida Bolivia 5150 CP 4440, Argentina
groyano@di.unsa.edu.ar

Abstract. El presente trabajo es una investigación sobre la legislación vigente con respecto a la protección de datos personales cuando se realizan actividades de video vigilancia, se destacan los lineamientos principales para llevar a cabo la correcta instalación de un sistema de video vigilancia en una institución de educación de nivel superior como una universidad.

1 Introducción

Con el avance de la tecnología, al día de la fecha, no se puede pasar por alto el aporte de la misma a las incumbencias relacionadas con la seguridad para el bienestar de la sociedad.

Particularmente la tecnología aplicada en el uso de sistemas de video-vigilancia, pertenecientes a distintas entidades como ser el estado, empresas de seguridad, universidades, comercios, propiedades privadas, etc. Ha demostrado que dicha vinculación permite identificar de una manera relativamente certera a personas que tienen pedido de captura o que por dictamen jurídico no pueden acceder a algunos recintos tanto públicos como privados, así también ha permitido a estas organizaciones reconocer tanto a las personas como a los hechos ilícitos que se cometen.

Los sistemas de video-vigilancia se implementan instalando cámaras de video cuyas grabaciones digitales pueden almacenarse o ser vistas en un monitor central. Estos son muy sencillos de utilizar ya que en el fondo se trata solamente de videos tradicionales.

2 Aplicaciones

Un sistema de video-vigilancia permite grabar las imágenes de las cámaras mientras el usuario no está presente, así también permite ver en tiempo real lo que se está grabando y controlar las diferentes dependencias y rincones, ofreciendo una visión global de todas las instalaciones.

Por otro lado, las cámaras de video-vigilancia tienen un "*efecto disuasorio*" contra los robos y el vandalismo. En caso de robo funciona tanto en personas ajenas al lugar, como en el mismo personal. Por ende, la principal ventaja de las cámaras, es que se pueden tener grabaciones de todo lo que sucede y sucedió, sin ser necesario tener que estar físicamente en el lugar.

3 La video vigilancia en la vía pública

La aplicación de la video vigilancia en espacios públicos, como ser escuelas, universidades, hospitales, transportes públicos, etc. resulta ser una excelente herramienta para la prevención de robos, vandalismos, asaltos, y otros crímenes en zonas públicas. Sin embargo, este sistema puede ser percibido por el ciudadano como un recurso demasiado invasivo a su rutina diaria.

En espacios públicos donde concurren muchas personas es importante mantener la situación siempre bajo control, para poder coordinar de forma efectiva las medidas a tomar ante situaciones potencialmente peligrosas, la video-vigilancia, además de prevenir actos violentos, robos o asaltos, permite vigilar el comportamiento de las personas. La presencia de las cámaras, obliga a ladrones, vándalos e incluso a espectadores a comportarse debidamente.

Cada vez son más los establecimientos educativos los que optan por la implementación de este tipo de sistemas, para brindar mayor seguridad a las personas que concurren. La video-vigilancia permite tener un mayor control ante situaciones que representen ciertos peligros, como ser, robo, vandalismo, posesión de armas, venta y consumo de estupefacientes, personas vinculadas a un delito anterior, situaciones de violencia, etc.

Además de ofrecerse como una herramienta para la detección de posibles situaciones que pongan en riesgos a las personas que concurren a los establecimientos, estos sistemas, son también una herramienta adicional para las tareas de controles administrativos que se realizan.

4 Ámbito de estudio

Desde hace más de 4 años, en la Universidad Nacional de Salta, se implementa, el uso de cámaras de seguridad, con el fin de identificar amenazas que atenten contra la

integridad de profesionales, estudiantes y demás personas que trabajan en dicho establecimiento, amenazas como por ejemplo robo, violencia física, ingreso de personas con pedidos de captura o que tienen prohibido el ingreso a el establecimiento, vandalismo.

El control de dichas cámaras depende de cada facultad, más precisamente de cada departamento, lo que permite un mejor y mayor control. Sin embargo, esta actividad es realizada de forma esporádica, y poco eficiente, debido a la falta de personal asignado y a la poca capacitación para realizar dicha tarea.

En la actualidad esta labor es realizada de forma manual, por pedido de alguna autoridad, por auditorías o en caso de robo o algún otro problema.

En una primera instancia, se recuperan las grabaciones, luego de identificar dicha grabación se procede al estudio de la misma para tomar las medidas correspondientes.

4.1 Fortalezas

La disposición de las cámaras de video-vigilancia en los recintos de la universidad implica que las personas que concurren a la misma, pongan en consideración la vigilancia de la cámara, por sobre la idea de cometer cualquier hecho ilícito.

Al concebirse la operatividad del sistema dividida en secciones asociadas a cada facultad, y dentro de cada una de estas, divididas en departamentos, se obtiene una mayor capacidad de control y se facilita el mantenimiento del mismo.

4.2 Debilidades

La ubicación de las cámaras utilizadas por el sistema no es, en todos los casos, la más óptima para obtener un eficiente uso del mismo. Esto sumado a que la tecnología que se emplea no es considerada la más avanzada, lo cual supone que el sistema no puede operar de la mejor manera.

4.3 Oportunidades

El interés de la comunidad universitaria por colaborar en la mejora del sistema de video-vigilancia, implicaría una mejora en la monitorización de las cámaras, lo que permitirá tener un rápido accionar.

La necesidad de incrementar la sensación de seguridad y tranquilidad por parte de las personas que concurren a dicho establecimiento, fomentan el interés en la adquisición de mejores recursos de tecnología, necesarios para el funcionamiento del sistema.

4.4 Amenazas

El cambio en las disposiciones legislativas podría significar cambios en los requerimientos para poner en producción el sistema, estos cambios van desde simples modificaciones sobre la operatividad del sistema hasta dejarlo en un estado de desuso, posiblemente.

5 Marco Legislativo

5.1 Principios generales relativos a la protección de datos personales.

La ley 25.326 trata concretamente la protección de datos personales. En ella se especifica su objetivo como la protección de datos personales que se encuentren en archivos, registros, bancos de datos o medios técnicos para el tratamiento de datos ya sean públicos o privados.(Art.1)

Además la ley especifica definiciones de conceptos y categorías de datos como:

Datos personales: Información de cualquier tipo referida a personas físicas o de existencia ideal.

Datos Sensibles: Datos personales que revelan origen racial, étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o vida sexual.(Art.2)

También especifica en qué casos los archivos de datos serán lícitos, es decir, cuando el usuario posea una registro de datos que cumpla con todas las condiciones establecidas por ésta ley.(Art.3) También trata sobre la calidad y tipo de datos(Art.4, Art.7), el modo en que se obtiene el consentimiento para registro de los datos, los casos en que este consentimiento se toma de forma implícita o en los que no es necesario dicho consentimiento. (Art.5, Art.6)

Las obligaciones de los usuarios de datos con respecto a las medidas técnicas y organizativas para garantizar la seguridad y confidencialidad evitando filtración, alteración, pérdida o consulta no autorizada (Art.9, Art.10). También en cuanto al debido registro o inscripción del banco de datos en la autoridad pertinente (Art.21)

El derecho de los titulares a acceder al contenido de su información, su finalidad, su corrección o eliminación, los casos excepcionales en que los usuarios pueden denegar el uso de tal derecho. (Artículos 13, 14,15,16 y 17)

La existencia y reglamentación para archivos públicos (Art.22) , con fines publicitarios (Art.27) y los generados a partir de encuestas (Art.28)

La existencia, función y reglamentos del órgano de control que se encarga del cumplimiento de ésta ley (Art.29)

Actualmente Es la dirección nacional de protección de datos personales que depende del ministerio de justicia y derechos humanos.

Las sanciones administrativas como clausura del banco de datos o multas económicas por incumplimiento de la ley y también sobre las sanciones penales (Art.31, Art.32)

La legitimación de las acciones legales que se pueden llevar a cabo por protección de datos o habeas data y los requisitos, trámites y reglamentos que se deben considerar para el uso de esta ley en dichas acciones. (Art.33 a Art. 43).

Por último remarca que la ley se aplica en todo el territorio nacional.(Art.44)

5.2 Condiciones de licitud para las actividades de video vigilancia. (Año 2015)

Desde la dirección nacional de datos personales se crea la “Disposición 10/2015” en la cual se tiene en cuenta que:

- ➔ Una imagen o video donde una persona pueda ser determinada, constituye un dato personal.
- ➔ Un conjunto de material fotográfico donde una persona pueda ser determinada, constituye una base de datos (tiene protección de ley 25.326)
- ➔ El tratamiento de imágenes con fines de seguridad, constituye una actividad de video vigilancia y se encuentra en la categoría de base de datos.

Y por lo cual establece un Artículo en el cual se indican cuales son las condiciones necesarias para llevar a cabo actividades de video vigilancia de forma lícita.

Remarcando las condiciones principales y a modo de resumen, se indica que es posible el cumplimiento de información del titular de datos (Ley 25.326,Art.6) por medio de carteles que indiquen la existencia de dispositivos de seguridad, también indica que **no es necesario el consentimiento previo en los casos en que los datos se recolectan con motivo de realización de un evento privado, lo realice el estado en el ejercicio de sus funciones y/o los datos se recolectan dentro de un predio de uso propio como ser propiedad privada, alquilado o de concesión pública.**

Por último indica la obligatoriedad de la inscripción en el registro nacional de bases de datos de la dirección nacional de protección de datos personales junto a los requisitos para dicha inscripción, en los cuales se solicita un manual de tratamiento de datos donde se especifique quienes son los responsables o usuarios de los datos, el modo de recolección, lugares fecha y hora donde operarán, plazo de conservación de los datos, los mecanismos técnicos de seguridad y confidencialidad y los argumentos que justifiquen esta necesidad.

También se incluye un modelo de cartel para informar sobre la video vigilancia en el lugar.

5.3 En cuanto al almacén de datos biométricos en Argentina

En la argentina existen varios entes gubernamentales y privados que realizan registro y almacenamiento de información biométrica en diferentes bancos de datos. Teniendo en cuenta que los datos biométricos incluyen; firma, fotografía, huellas dactilares, registros odontológicos y ADN no codificante.

SALUD: La ley 26.812 que sustituye al art. 15 de la ley 26.529; en su inciso f indica que las historias clínicas odontológicas deben contener registros que permitan la identificación del paciente.

ANSES (Administración Nacional de la Seguridad Social): en la resolución 648/2014 art. 10º indica que los datos biométricos recolectados por ANSES serán resguardados

en una base de datos perteneciente a la Dirección General de Diseño de Normas y Procesos (DGDNyP)
RENAPER: La LEY 13.482 que trata su creación, indica en Capítulo III art 6º sobre la identificación de las personas dice: " La identificación se cumplirá ante la dependencia del registro correspondiente al lugar donde viva el causante mediante fotografías, impresiones dactiloscópicas, descripción de señas físicas y datos individuales".
AFIP: en la resolución general 2811 se aprueba el "Sistema Registral" para la realización de trámites mediante transferencia electrónica de datos el cual requiere el registro de datos biométricos a través de la digitalización de la fotografía, la firma, la huella dactilar y la imagen reproducida del documento nacional de identidad.
SID: El Sistema de Identidad Digital (SID) es una plataforma desarrollada íntegramente por el Estado que permite validar la identidad a distancia y en tiempo real con Renaper mediante factores de autenticación biométrica.
En su página explicita que: La biometría del rostro es un modo de identificación legalmente válido y adaptado a las nuevas tecnologías, tal como se propugna en los términos de los artículos 9 y 11 de la Ley 17.671 y su reglamentación en el Art. 1 del Decreto 1501/09
SIBIOS: El ministerio de seguridad, por decreto 1766/2011 crea el Sistema Federal de Identificación Biométrica para la Seguridad

6 Conclusión

La inseguridad se ha incrementado en todo el mundo en estos últimos años, esto acrecentó la necesidad tanto de los gobiernos como de los particulares de buscar nuevas tecnologías que garanticen su seguridad, siendo la video-vigilancia la más utilizada.

Se debe destacar también que, la tecnología evoluciona a un ritmo mucho más acelerado que la legislación, al menos ocurre esto en los países que no están al frente del apogeo tecnológico.

Antes de hacer mención a las recomendaciones siguientes, entiéndase que al referirse a la provincia de Salta se debe tener en mente por supuesto a la Universidad Nacional de Salta, definida como el objeto de estudio de este trabajo.

En Salta se han alcanzado niveles de aplicación tecnológica para los que su legislación no está del todo preparada, porque si bien existe la ley 25.326, no se ha procurado en Salta una ley que regule el sistema de video-vigilancia como las hay en otras provincias, lo que lleva a condiciones de licitud establecidas para los sistemas de video-vigilancia dispares en las leyes provinciales, por lo que, si bien no existiera una vulneración directa a los derechos de las personas, no se puede asegurar que haya una completa armonía entre los sistemas de video-vigilancia y su fin de brindar seguridad, con los derechos a la imagen, privacidad e intimidad.

Este problema, ha llevado a numerosas discusiones y divulgaciones de proyectos a favor y en contra de la aplicación de dicho sistema. Si bien una postura destaca como

principal aspecto positivo de la video-vigilancia, la seguridad y productividad que se logra con ella, otros aluden a su aspecto negativo, fundamentalmente basado en la invasión de la privacidad de aquellas personas que son vigiladas a través de estas cámaras.

Por lo anteriormente expuesto se considera que para qué el sistema de video-vigilancia sea eficiente, mínimamente se deben dar las siguientes condiciones:

1. que los ciudadanos cedan parte de su privacidad y se involucren en el proceso de formulación de las leyes que inciden sobre ella,
2. que se tome como una realidad que el sistema de video-vigilancia de la provincia se encuentra en constante evolución, y que es necesario que sea reglamentado
3. que se respeten las normativas existentes en materia de protección de datos, manteniendo la confianza de la ciudadanía.
4. Que se unifiquen los bancos de datos y se administren por una única entidad permitiendo una auditoría general de las actividades realizadas

Estas recomendaciones no tienen intenciones de expresar que se dé prioridad a la seguridad pública por sobre el derecho a la privacidad.

Sin embargo, se especula que, sería fundamental, la procuración de una ley que regule la video-vigilanica en la provincia, que contemple el uso de los medios de grabación, el tiempo de conservación de las grabaciones, el momento de su destrucción, y defina los procedimientos a realizarse durante la utilización del sistema, teniéndose en cuenta las opiniones de ONGs, instituciones y otras organizaciones que podrían verse afectadas.

7 Bibliografía

https://www.argentina.gob.ar/aaip/datospersonales

https://privacyinternational.org/state-privacy/57/state-privacy-argentina

https://www.eltribuno.com/jujuy/nota/2018-3-1-0-0-0-proponen-instalar-alarmas-y-camaras-en-las-escuelas

https://www.elesquiu.com/policiales/2017/9/20/esta-prohibido-que-los-chicos-sean-filmados-con-camaras-en-las-escuelas-261136.html

https://www.ambitojuridico.com/noticias/general/administrativo-y-contratacion/vigilancia-en-aulas-de-clase-traves-de-camaras-viola

http://www.elsindical.com.ar/notas/la-video-vigilancia-llega-a-las-escuelas-contra-inseguridad/

https://elpais.com/elpais/2017/01/13/mamas_papas/1484295654_015542.html

http://44jaiio.sadio.org.ar/sites/default/files/sid174-184.pdf

https://viapais.com.ar/salta/985495-camaras-de-seguridad-permitieron-el-arresto-de-un-traficante-en-salta/

https://viapais.com.ar/salta/840666-desde-abril-habra-nuevas-camaras-de-videovigilancia-en-salta/

https://www.legalisconsultores.es/2013/08/camaras-de-videovigilancia-en-la-ley-de-proteccion-de-datos-parte-ii/

https://seti.afip.gob.ar/sistema-registral-internet-help/Registro_y_Aceptacion_de_Datos_Biometricos.htm

http://servicios.infoleg.gob.ar/infolegInternet/anexos/240000-244999/240220/norma.htm

http://servicios.infoleg.gob.ar/infolegInternet/anexos/295000-299999/295928/texact.htm

https://www.argentina.gob.ar/sid-sistema-de-identidad-digital;

http://servicios.infoleg.gob.ar/infolegInternet/anexos/185000-189999/189382/norma.htm

https://www.argentina.gob.ar/noticias/identificacion-biometrica-para-la-seguridad

https://blog.smaldone.com.ar/2012/04/24/sobre-el-sibios-identificacion-biometrica-en-la-argentina/