lavits ****** 2017
5to Simposio Internacional LAVITS
Vigilancia, Democracia y Privacidad
en América Latina: Vulnerabilidades y resistencias

ISSN 2175-9596

TRANSPORTE PÚBLICO, PROTECCIÓN DE DATOS PERSONALES Y RESGUARDO DE LA PRIVACIDAD: TRANSANTIAGO COMO EJEMPLO DE LOS PELIGROS ASOCIADOS A LA IMPLEMENTEACIÓN DE MEDIDAS TECNOLÓGICAS EN EL TRANSPORTE URBANO

Transporte público, proteção de dados pessoais e proteção da privacidade: Transantiago como um exemplo dos perigos associados à implementação de medidas tecnológicas no transporte urbano

Public transport, protection of personal data and protection of privacy: Transantiago as an example of the dangers associated with the implementation of technological measures in urban transportation

Pablo Viollier[a]
Patricio Velasco[b]

[(a)] Investigador del área "*Research & Policy*", Derechos Digitales y América Latina. E-mail: pablo@derechosdigitales.org.
[(a)] Abogado – Investigador del área "*Research & Policy*", Derechos Digitales y América Latina. E-mail: patricio@derechosdigitales.org.

Resumen

La ponencia busca exponer cómo la promoción e instalación de tecnologías en contextos urbanos puede llevar a consecuencias indeseadas desde el punto de vista de la protección de los derechos fundamentales y, especialmente, del debido resguardo a la privacidad de las personas. En particular, se discutirá la aplicación de soluciones tecnológicas que sientan las bases para la vulneración de derechos en el contexto del sistema de transporte público de Santiago de Chile (Transantiago); luego se indagará en el rol de la institucionalidad y sus falencias a la hora de proteger los derechos de la ciudadanía y, aún más, al momento de aplicar penas infamantes -tal como el Registro de evasores del Transantiago. La ponencia advierte sobre la inexistencia de una institucionalidad adecuada para el resguardo de los derechos humanos ante la emergencia de políticas y prácticas comprendidas bajo el concepto de "ciudades inteligentes". Todavía más, se expone el caso de las políticas vinculadas a Transantiago como un ejemplo negativo de

tratamiento de datos y establecimiento de medidas que busquen corregir defectos en el sistema de transporte.
Palabras clave: Privacidad; Protección de datos; Transporte público.

Resumo

O artigo procura mostrar como a promoção e instalação de tecnologias em contextos urbanos pode levar a conseqüências indesejáveis do ponto de vista da proteção dos direitos fundamentais e, principalmente, da devida proteção à privacidade das pessoas. Em particular, será discutida a aplicação de soluções tecnológicas que estabelecem as bases para a violação de direitos no contexto do sistema de transporte público de Santiago do Chile (Transantiago); então investigaremos o papel das instituições e suas deficiências quando se trata de proteger os direitos dos cidadãos e, mais ainda, quando se aplicam penalidades infames - como o Registro Transantiago Evaders. O documento adverte sobre a falta de um quadro institucional adequado para a proteção dos direitos humanos em face do surgimento de políticas e práticas incluídas sob o conceito de "cidades inteligentes". Ainda mais, o caso das políticas vinculadas ao Transantiago é exposto como um exemplo negativo de processamento de dados e estabelecimento de medidas que buscam corrigir defeitos no sistema de transporte.
Palavras-chave: *Privacidade; Proteção de dados; Transporte público.*

Abstract

The paper seeks to show how the promotion and installation of technologies in urban contexts can lead to undesirable consequences from the point of view of the protection of fundamental rights and, especially, of the due protection of the privacy of people. In particular, the application of technological solutions that lay the foundations for the violation of rights in the context of the public transport system of Santiago de Chile (Transantiago) will be discussed; then we will investigate the role of institutions and their shortcomings when it comes to protecting the rights of citizens and, even more, when applying infamous penalties -such as the Transantiago Evaders Registry. The paper warns about the lack of an adequate institutional framework for the protection of human rights in the face of the emergence of policies and practices included under the concept of "smart cities". Still more, the case of the policies linked to Transantiago is exposed as a negative example of data processing and establishment of measures that seek to correct defects in the transport system.
Keywords: *Privacy; Data Protection; Public transport.*

INTRODUCCIÓN

Esta ponencia tiene como objetivo exponer el caso de Transantiago bajo el prisma de una política pública que ha buscado modernizar el transporte público mediante la aplicación de tecnologías capaces de amenazar derechos fundamentales de la ciudadanía. En particular, la indagación expondrá la forma en que la aplicación de medidas tecnológicas ha amenazado – y amenaza – la privacidad de las personas. Se sostiene que buena parte de las decisiones que articularon el plan de modernización del transporte asumen un prejuicio positivo en relación al rol de las tecnologías, lo que ha resultado

especialmente problemático a la hora de orientar prácticas destinadas a disminuir la evasión de pago.

Es así como, bajo la premisa que los problemas tecnológicos tendrían soluciones del mismo carácter, problemas como el de la evasión – en un sistema de transporte altamente tecnificado – ha implicado el desarrollo y aplicación de prácticas de registro y vigilancia que atentan contra la privacidad de las personas. Incluso buscando la aplicación de penas infamantes que refuerzan los principios de un régimen de vigilancia que busca provocar cambios en el comportamiento de la ciudadanía mediante la instalación de la vergüenza como dispositivo de control social (Foucault, 1979).

EL ROL DE LAS TECNOLOGIAS EN EL DISEÑO DE TRANSANTIAGO

Investigaciones recientes (Ureta, 2017) han destacado la relevancia de la instalación de procesos tecnológicos en la narrativa que conformó el proyecto Transantiago. Bajo una premisa que inspiraba la necesidad de elevar el estándar del transporte público santiaguino hasta niveles de país desarrollado, el

diseño del nuevo sistema de transporte público implicó el desarrollo y aplicación de una serie de herramientas tecnológicas: desde aquellas que permitían el control de la flota de buses en las calles hasta el nuevo sistema de mecanismo integrado de pago. A partir de lo anterior, no resulta extraño que, a la hora de afrontar la evasión en el pago, también se haya pensado en la aplicación de tecnologías que buscasen limitarla y promover la configuración de un usuario ejemplar: que respondiese de forma eficiente a los requerimientos de un sistema moderno.

Desde su implementación en el año 2007, el sistema de transporte público metropolitano ha adoptado como método preferente de pago, y método exclusivo en el caso de buses, la utilización de una tarjeta inteligente, capaz de ser cargada con dinero y que descuenta el valor del pasaje en cada transacción. Esta tarjeta funciona de forma similar a otras utilizadas en el transporte público de grandes ciudades en el mundo, y permite almacenar en tiempo real la información de su utilización.

En la discusión sobre el diseño del sistema de pago un punto álgido resultó aquel destinado a evitar la evasión. La discusión abordó diversas posibilidades técnicas y su aplicabilidad en los buses para favorecer el pago del pasaje, en un contexto donde anteriormente eran los conductores los encargados de recaudar el dinero. La duplicación de funciones que recaía en conductor era una de las

preocupaciones de quienes diseñaron el sistema: en el modelo previsto el conductor sólo debía encargarse de la dirección del bus, dejando el problema del cobro en responsabilidad de los nuevos sistemas y dispositivos de Transantiago.

Las falencias observadas en la implementación del plan de transporte, entre las que se cuenta la fallida instalación del sistema de conteo automático de pasajeros, impidió conocer la proporción efectiva de pasajeros que pagaban su pasaje versus el total de pasajeros transportados. Este y otros cambios en el diseño original en relación a la ejecución del proyecto llevaron a tratar el problema de la evasión desde una lógica particular: la de promover la vergüenza entre los usuarios que evadían. Tal como señala Ureta, "la mejor manera de mantener la evasión de tarifas bajo control parecía ser el exponer a los posibles evasores de la forma más pública posible, frente a los conductores y otros viajeros, de manera que se sintieran avergonzados y renunciaran a esta práctica, [donde] la visibilidad se identifica directamente como la manera más válida de disciplinar a este vergonzoso chileno para que pague." (Ureta, 2017, p. 174).

La importancia de la vergüenza en pos de la corrección de comportamientos sociales ha sido ampliamente estudiada[1]. Lo novedoso en el caso de Transantiago es cómo se produjo la integración de tales principios a nivel tecnológico y la manera en que se han desplegado esfuerzos sistemáticos para proseguir en el uso de la vergüenza como mecanismo de coacción. Incluso a costa de los datos sensibles de los usuarios, ya sea por falta de resguardo en el cuidado de tal información o activamente en busca del escarnio público.

DATOS PERSONALES Y TRANSANTIAGO: DEL DESCUIDO A LA VERGÜENZA PÚBLICA

A continuación se exponen tres casos relacionados con Transantiago y la aplicación de tecnologías que vulneran o pueden vulnerar derechos fundamentales. En primer lugar, se exponen los peligros asociados a la base de datos de la tarjeta Bip!, luego se discuten las intenciones de aplicar tecnologías de biometría para la validación del pasaje y, finalmente, se expone el caso del registro de evasores. En la totalidad de los casos se aprecia que se opera bajo el principio de que nuevas tecnologías darán resolución a problemas que, incluso, pueden no haber existido previa implementación del nuevo

[1] Véase "The Civilizing Process: Sociogenetic and Psychogenetic Investigations" (2000) y Powers of Freedom (1999).

sistema de transporte. Así, se exponen estos casos como elementos a favor de la crítica sostenida en torno al solucionismo tecnológico (Morozov, 2013).

LA BASE DE DATOS DE LA TARJETA BIP!

Un buen ejemplo de una política pública que, al no tener en consideración la protección de datos de las personas, termina por exponer de forma negligente los datos sensibles de los ciudadanos es la base de datos de la tarjeta Bip! El sistema permite a cualquier portador de una tarjeta, acceder a través de una plataforma web al historial de utilización y carga de la misma. Este sistema denominado "Bip en línea"[2], solo exige el número de la tarjeta para su acceso.

Si bien la información contenida en el sistema Bip! en línea solo entrega el dato de la validación al momento de la entrada al transporte público, un estudio muestra que al analizar la información de los usuarios contenida en dicha base de datos es posible estimar con más de un 60% de exactitud que la estación de bajada del usuario se encuentra a menos de 700 metros de su hogar (Bahamonde, Font, Bustos-Jimenez, & Montero, 2014)[3]. La misma investigación también da cuenta que los usuarios no están conscientes que el número ID de su tarjeta puede permitir el acceso a información sensible, ya que no encontraron ninguna objeción al momento de pedirle esa información a los participantes de la encuesta realizada (Bahamonde, Font, Bustos-Jimenez, & Montero, 2014). Por otro lado, esta información no cuenta con ningún tipo de resguardo, ya que se encuentra visible en el dorso de cada tarjeta.

Del mismo modo, la tecnología utilizada para resguardar los datos de dichas tarjetas se encuentra obsoleta y sus vulnerabilidades informáticas han sido reportadas hace años. Esto permite a terceros inhabilitar tarjetas de usuarios, obtener información privada de ellos e incluso realizar viajes gratis emulando transbordo (Quezada & Yazim, 2016). Al utilizar el MIFARE Classic 4K, la tarjta BIP utilizada un algoritmo que ya fue "quebrado" y puede ser explotado de varias formas documentadas, que permiten acceder y modificar los datos contenidos en la tarjeta[4].

[2] Disponible en: http://pocae.tstgo.cl/PortalCAE-WAR-MODULE. Recuperado el 30 de octubre de 2017.
[3] La estimación alcanza un 87,5% de acierto cuando se trata de ubicar el hogar de la persona a menos de 3.000 metros de la estación de bajada (Bahamonde, Font, Bustos-Jimenez, & Montero, 2014).
[4] Como realizar esto puede incluso encontrarse en tutoriales de YouTube: www.youtube.com/watch?v=VUvSpyNg9OI. Recuperado el 30 de octubre de 2017.

Más grave aún, es la forma en que se almacena la información de la Tarjeta Nacional Estudiantil (TNE), método de pago que constituye un beneficio social entregado por el Estado y es utilizado por la totalidad de los estudiantes de enseñanza básica, media y superior de Chile. El sitio web www.tne.cl permitía, hasta hace poco, acceder al historial de saldo, validación y recarga de cualquier tarjeta TNE. Esto pues el número de tarjeta TNE está vinculado al número RUT de cada estudiante, que se encuentra disponible a través de múltiples fuentes accesibles al público conociendo su nombre[5]. En la práctica, lo anterior permitía a cualquier persona acceder al historial de navegación de los últimos tres meses de cualquier estudiante chileno, así como tener acceso a información sensible del titular, como nombre, apellido, RUT, nivel de estudios, número de tarjeta TNE, código de referencia de la institución educacional, región de Chile y estado de la tarjeta.

El nivel de resguardo informático es tan precario, que el sistema permitía realizar *data-mining* de la totalidad de la base de datos utilizando un simple código de programación. Esta vulnerabilidad fue parchada, sólo parcialmente, luego de que una investigación expusiera públicamente las fallas del sistema (Grubi, 2016). Sin embargo, la solución solo impide realizar *data-mining* masivo de la base de datos, pero todavía permite el acceso a la información de la TNE de estudiantes individuales.

IMPLEMENTACIÓN DE BIOMETRÍA EN EL TRANSPORTE PÚBLICO

Con el objetivo de disminuir la evasión del sistema de transporte público, El Ministerio de Transportes ha anunciado que se encuentra estudiando implementar un sistema de reconocimiento facial que le permita identificar a quienes no paguen al momento de abordar los buses del Transantiago (Grubi, 2016).

Si bien los detalles de cómo operaría este sistema no han sido revelados, lo cierto es que el solo hecho de crear una base de datos con los rasgos faciales de la totalidad de usuarios del transporte público resulta en sí misma una idea peligrosa, desproporcionada y atentatoria contra los derecho fundamentales.

Esto se debe a que, por su naturaleza, la identificación a través de datos biométricos es esencialmente

[5] Por ejemplo, en el sitio web http://prontuario.cl se puede conocer el RUT de una persona ingresando su nombre, y viceversa.

imperfecta (Iglesias & Castellaro, 2017). Esto puede dar pie a un porcentaje importante de falsos positivos y de personas injustamente identificadas como infractores, especialmente considerando que no existe claridad respecto a qué base de datos se utilizará para contrastar dichos datos recolectados.

Por otro lado, la eventual filtración o robo por parte de terceros de la base de datos puede dar pie a un uso discriminatorio de la misma, permitiendo que la información recolectada por el Estado sea utilizada por terceros para crear diversos modelos de perfilamiento individual (ADC, 2017).

Por otro lado, la implementación de este tipo de medidas también manifiesta una intención de control por parte de la autoridad, la que puede generar efectos adversos en el ejercicio de derechos fundamentales. El hecho de que un porcentaje importante de la población se sienta bajo vigilancia genera el denominado "efecto inhibitorio", o *chilling effect*, en el cual las personas se abstienen de actuar como lo harían normalmente, por miedo a ser individualizados o vigilados, restringiéndose de esta forma no solo su libertad de expresión, sino también su derecho a reunión, petición, entre otros (Unión Europea, 2014).

REGISTRO DE INFRACTORES DEL TRANSANTIAGO

En otros casos, no ha sido la negligencia de los organismos públicos lo que ha expuesto los datos personales sensibles de los ciudadanos. Por el contrario, la exposición pública de los mismos ha sido el fin perseguido por políticas públicas que buscan utilizar la vergüenza pública y la humillación como forma castigo ante ciertas conductas.

Este es el caso del denominado "DICOM del Transantiago", un proyecto de ley que se encuentra en su última etapa de tramitación[6], y que busca crear un registro público de personas que tengan multas impagas por no pago de la tarifa del transporte público.

Distintas organizaciones de la sociedad civil, así como el Consejo de Transparencia[7] han advertido

[6] Boletín 10125-15, disponible en: https://www.camara.cl/pley/pley_detalle.aspx?prmID=10545&prmBoletin=10125-15. Recuperado el 30 de octubre de 2017.

[7] Las objeciones del Consejo para la Transparencia al contenido del proyecto se encuentran disponibles en: http://olt.consejotransparencia.cl/Paginas/DetalleLey.aspx?ID=52. Recuperado el 30 de octubre de 2017.

que de acuerdo a la legislación, esta base de datos constituiría una fuente accesible al público[8]. Lo anterior abre la puerta para la creación de bases de datos paralelas o "listas negras" que pueden ser utilizadas de forma discriminatoria, impidiendo el acceso al trabajo y al crédito de los infractores, incluso después de haber cancelado su deuda y haber sido eliminados del registro original.

Esta no es una consecuencia indeseada o secundaria de la publicidad del registro, sino su objetivo principal. Si bien el gobierno no se hizo totalmente responsable de su justificación original, lo cierto es que cuando fue anunciado el proyecto, personeros del gobierno explícitamente dijeron que el objetivo del proyecto era que quienes tengan deudas del transporte público sean discriminados al momento de postular a puestos de trabajo[9].

Esta política pública representa un precedente particularmente peligroso. La creación, administración y acceso a bases de datos, especialmente aquellas administradas por organismos públicos y que contienen información sensible, deben cumplir un objetivo de política pública legítimo y determinado. Del mismo modo, deben cumplir con los principios que orientan la protección de datos personales, entre ellos los de finalidad y minimización de datos.

CONCLUSIONES

Basta tomar el último de los casos referidos para señalar que resulta sumamente preocupante que un organismo público pretenda que la creación de una base de datos no cumpla una finalidad, sino que su existencia misma sea utilizada como forma de sanción a través de la generación de un sentimiento de vergüenza y humillación en el individuo condenado ante la sociedad. Este tipo de penas de vergüenza o penas infamantes, comunes durante la edad media (García-Molina, 1999), no solo han sido denunciadas por vulnerar los derechos fundamentales de los afectados, sino que por su dificultad para ser justificadas jurídicamente a través de las teorías modernas sobre la función de la pena (Javier, 2007).

[8] Un análisis más detallado de lo que implica jurídicamente que un dato personal se encuentre en una fuente accesible al público puede encontrarse en: Alvarado, Francisco (2014). Las fuentes de acceso público a datos personales. Revista chilena de derecho y tecnología Vol. 3, No 2. Disponible en: http://www.rchdt.uchile.cl/index.php/RCHDT/article/viewFile/33276/37869. Recuperado el 30 de octubre de 2017.

[9] Así lo reconoció jefa del programa nacional de fiscalización, Paula Flores en una entrevista en televisión abierta: http://www.dailymotion.com/video/x5ezz8r. Recuperado el 30 de octubre de 2017.

De esta forma, el Estado no solo incumple su deber de proteger los datos personales de sus ciudadanos, sino que activamente los expone como forma de castigo social. Tal como se ha señalado: "Dada la resistencia de los conductores de los buses a censurar a los evasores, todo el sistema descansaba ahora sobre la vergüenza que los propios usuarios podían llegar a sentir ante otros pasajeros y […] no parecía ser lo suficientemente fuerte como para impedir que lo hicieran. Por lo tanto, en la práctica, en vez de controlar efectivamente la evasión, los dispositivos simplemente terminaron enactando dos tipos de dispositivos humanos: el pagador y el malvado evasor" (Ureta, 2017, p. 178).

El "malvado evasor" se configura en Transantiago mediante la exposición pública, que se encuentra tecnológicamente facilitada e, incluso, es políticamente buscada. Así, las y los usuarios del transporte público de Santiago se enfrentan a grandes falencias institucionales referidas a la protección de datos personales. La accesibilidad de las bases de datos, la orientación hacia medidas biométricas y la instalación del registro de evasores son todas medidas que suponen la integración de dispositivos tecnológicos capaces de exponer a las y los usuarios del transporte público de formas altamente riesgosas.

Todo lo anterior se vuelve crecientemente peligroso en un contexto en que la aplicación de medidas *inteligentes* para la gestión urbana – regularmente bajo la etiqueta de programas que fomenten el desarrollo de Smart cities – hallan creciente apoyo en diversas agencias estatales y empresas privadas. En otros contextos, se ha evaluado la percepción del resguardo a los datos personales en el desarrollo de Smart cities, encontrándose evidencia sobre una evaluación dispar de la ciudadanía según cómo son resguardados los datos personales para la gestión del espacio urbano (Zoonen, 2016).

Es de esperar que, en el futuro, el descuido y exposición de los datos personales dejen de ser la norma en el marco de las políticas de transporte metropolitano. Toda vez que, hasta ahora, la extrema confianza en las tecnologías y su eficacia permite apoyar el diagnóstico de Morozov, para quien "El principal problema con el solucionismo es que se niega a aceptar que al esforzarse por la perfección, independientemente de si se manifiesta en demandas para que los políticos sean completamente honestos y transparentes o en esfuerzos reales por trascender las supuestas limitaciones del partidismo, podría estar ejerciendo una influencia negativa en nuestra cultura política. La perfección no debe buscarse como fin en sí mismo; la democracia es un asunto complejo en el que, en ausencia de desilusiones, nunca habrá ningún logro" (Morozov, 2016, p. 116, traducción libre).

REFERENCIAS

ADC (2017). *Si nos conocemos más, nos cuidamos mejor:* Informe sobre políticas de biometría en la Argentina. Recuperado el 30 de octubre de http://www.adc.org.ar/wp-content/uploads/2015/05/InformeBiometriaADC2015.pdf.

Alvarado, F. (2014). Las fuentes de acceso público a datos personales. *Revista Chilena de Derecho y Tecnología, 3*(2). Recuperado el 30 de octubre de http://www.rchdt.uchile.cl/index.php/RCHDT/article/viewFile/33276/37869.

Contesse, J. (2007). Consideraciones acerca de la relación entre reproche penal y pena: el caso del "shaming punishment" en la práctica punitiva norteamericana. *Revista de Estudios de la Justicia, 9*, 241-274. Recuperado el 30 de octubre de http://web.derecho.uchile.cl/cej/rej9/Pena.pdf.

Elias, N. (2000). *The Civilizing Process:* Sociogenetic and Psychogenetic Investigations. Londres: Wiley-Blackwell.

Foucault, M. (1979). *Microfísica del Poder*. Buenos Aires: Ediciones de La Piqueta.

García-Molina, A. (1999). El régimen de penas y penitencias en el tribunal de la inquisición de México. *Serie Doctrina Jurídica, n. 17* [capítulo octavo]. Recuperado el 30 de octubre de 2017 de https://archivos.juridicas.unam.mx/www/bjv/libros/7/3476/11.pdf.

Iglesias, R. G., & Castellaro, S. B. (2017). La biometría en Chile y sus riesgos. *Revista chilena de derecho y tecnología, 6*(1), 67-91.

Gubri, M. (2016). La recolección de datos en el sistema de transporte público de Santiago: el caso de la tarjeta nacional estudiantil. *Derechos Digitales*. Recuperado el 30 de octubre de https://derechosdigitales.org/wp-content/uploads/V3-la-recoleccion-de-datos-en-el-transporte-pu%CC%81blico-chileno.pdf.

Bahamonde, A. H. J., Font, G., Bustos-Jimenez, J., & Montero, C. (2014, abril). Mining Private Information from Public Data: The Transantiago Case. *IEEE Pervasive Computing*, *13*(1), 37-43.

Zoonen, L. van (2016, junio 30). Privacy Concerns in Smart Cities. *Government Information Quarterly 33*(3), 1-9.

Morozov, E (2013). *To Save Everything, Click Here:* The Folly of Technological Solutionism. Nueva Iorque: Public Affairs.

Quezada, R., & Yazim, B. A. (2016). Análisis de seguridad de la Tarjeta Bip! chilena como medio de pago. Tesis para optar al grado de magíster en ciencias mención computación, Universidad de Chile, Santiago, Chile. Recuperado el 30 de octubre de 2017 de http://repositorio.uchile.cl/handle/2250/139911.

Rose, N. (1999). *Powers of Freedom*, Reframing political thought. Cambridge: Cambridge University Press.

Unión Europea (2014). *Opinion 01/2014 on privacy and data protection issues relating to the utilization of drones* [01673/15/EN]. Recuperado el 30 de octubre de 2017 de http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp231_en.pdf.

Ureta, S. (2017). *Transantiago o el fallido ensamblaje de una sociedad de clase mundial*. Santiago: Ediciones Universidad Alberto Hurtado Santiago.