Avances en seguridad privada

rev.relac.int.estrateg.segur.13(2):247-272,2018

Digitalización, automatización y empresas transnacionales de seguridad privada en áreas con capacidad estatal limitada*

Maximiliano Vila Seoane**

Fecha de recepción: 10 de febrero de 2018
Fecha de evaluación: 19 de abril de 2018
Fecha de aprobación: 5 de mayo de 2018

Artículo de reflexión

Referencia: Vila Seoane, M. F. (2018). Digitalización, automatización y empresas transnacionales de seguridad privada en áreas con capacidad estatal limitada. *Revista de Relaciones Internacionales, Estrategia y Seguridad, 13*(2), 247-272. **DOI:** https://doi.org/10.18359/ries.3300

Resumen

El estudio del aumento de empresas militares y de seguridad privada, junto con los estudios sobre prácticas de vigilancia electrónica, son dos temas de creciente debate en el campo de las relaciones internacionales. Por un lado, la privatización de la seguridad tiene efectos en la seguridad internacional y en la soberanía estatal. Por otro, la expansión de las prácticas de vigilancia electrónica es un nuevo riesgo para los derechos humanos, como la privacidad. En este contexto, el artículo indaga sobre un tema poco investigado en áreas con capacidad estatal limitada: las implicancias del continuo proceso de digitalización y automatización en la industria de la seguridad privada

* Resultado del proyecto de posdoctorado titulado "*Big data* y vigilancia: derechos humanos bajo presión", financiado por la Escuela de Política y Gobierno (EPyG) de la Universidad Nacional de San Martín (Unsam), en el marco de la Licenciatura en Relaciones Internacionales.

** Doctor en Ciencias Sociales, Universidad de Bremen; magíster en Gestión de la Ciencia, la Tecnología y la Innovación, Universidad Nacional de General Sarmiento; Licenciado en Ciencias Físicas, Universidad de Buenos Aires. Becario posdoctoral de la EPyG de la Unsam, Buenos Aires, Argentina. Correo electrónico: mvila@unsam.edu.ar

y la vigilancia electrónica. El artículo se basa en un análisis de los discursos de las empresas transnacionales de seguridad privada y vigilancia electrónica que operan en Argentina, y de los problemas asociados a estas prácticas. Específicamente, se detallan las consecuencias de la digitalización y automatización, como lo son el incremento de la dependencia tecnológica, la oferta de falsas soluciones tecnológicas que no resuelven los complejos problemas sociales que provocan la inseguridad, la creciente susceptibilidad a fallas tecnológicas de los equipos de vigilancia electrónica, y su amenaza a los derechos humanos. Finalmente, se concluye con una síntesis de los principales puntos y recomendaciones de política pública para contrabalancear las asimetrías en favor de estas empresas transnacionales.

Palabras clave: dependencia tecnológica; derechos humanos; empresas transnacionales; seguridad privada; vigilancia electrónica.

Digitization, Automation and Transnational Private Security Companies in Areas of Limited Statehood

Abstract

The study of the increase in military and private security companies and electronic surveillance practices are two topics of growing debate in international relations. On the one hand, the privatization of security has effects on international security and state sovereignty. On the other hand, the expansion of electronic surveillance practices poses new risks to human rights, such as privacy. In this context, this article explores a subject that has been little researched in areas of limited statehood: the implications of the continuous process of digitization and automation in the private security and electronic surveillance industry. The article analyzes the discourses of transnational private security and electronic surveillance companies operating in Argentina and the problems associated with these practices. Specifically, it lists the consequences of digitization and automation, such as increased technological dependence, offer of false technological solutions that do not tackle complex social problems causing insecurity, increasing vulnerability of electronic surveillance equipment to technological failures, and the new threats to human rights. Finally, the main points and recommendations for public policy to counterbalance asymmetries in favor of these transnational companies are summarized.

Keywords: electronic surveillance; human rights; private security; technological dependence; transnational companies.

Digitalização, automatização e empresas transnacionais de segurança privada em áreas com capacidade estatal limitada

Resumo

O estudo do aumento de empresas militares e de segurança privada, junto com os estudos sobre práticas de vigilância eletrônica, são dois temas de crescente debate no campo das relações internacionais. Por um lado, a privatização da segurança tem efeitos na segurança internacional e na soberania estatal. Por outro, a expansão das práticas de vigilância eletrônica é um novo risco para os direitos humanos, como a privacidade. Neste contexto, o artigo indaga sobre um tema pouco pesquisado em áreas com capacidade estatal limitada: as implicâncias do contínuo processo de digitalização e automatização na indústria da segurança privada e a vigilância eletrônica. O artigo se baseia em uma análise dos discursos das empresas transnacionais de segurança privada e vigilância eletrônica que operam na Argentina, e dos problemas associados a estas práticas. Especificamente, se detalham as consequências da digitalização e automatização, como são o aumento da dependência tecnológica, a oferta de falsas soluções tecnológicas que não resolvem os complexos problemas sociais que provocam a insegurança, a crescente susceptibilidade a falhas tecnológicas dos equipamentos de vigilância eletrônica, e sua ameaça aos direitos humanos. Finalmente, conclui-se com uma síntese dos principais pontos e recomendações de política pública para contrabalançar as assimetrias favoráveis a estas empresas transnacionais.

Palavras-chave: dependência tecnológica; direitos humanos; empresas transnacionais; segurança privada; vigilância eletrônica.

Introducción

El estudio del aumento de empresas militares y de seguridad privada, junto con los estudios sobre prácticas de vigilancia electrónica son dos temas de creciente debate en el campo de las relaciones internacionales. Por un lado, el crecimiento de estas empresas influye en la seguridad internacional y la soberanía estatal (Avant, 2005; Gómez del Prado, 2009). Según los críticos, la privatización de la seguridad debilita la capacidad del Estado de garantizarla como un bien público (Zedner, 2006). Por el contrario, los adherentes a estas prácticas sostienen que estamos viviendo una transición de la provisión centralizada por parte del Estado de los servicios de seguridad, a una red de múltiples actores, también denominada *gobernanza nodal*, donde nuevos actores privados participan activamente, pero donde el Estado aún retiene la preponderancia (White, 2011). Por otro lado, es inne-

gable que las empresas proveedoras de tecnologías juegan un rol central para facilitar el nivel minucioso de vigilancia electrónica al que está sometida la población en nuestras sociedades contemporáneas (Ball, Haggerty y Lyon, 2012; Bauman et ál., 2014). La principal consecuencia de la expansión de estas prácticas de vigilancia son los nuevos riesgos para los derechos humanos en la era digital, como la privacidad. Estas tendencias son evidentes en países de América Latina, donde la privatización de la seguridad también crece a la par de altos niveles de criminalidad, sumados a la desconfianza en las fuerzas policiales (Arias, 2009; Fleitas Ortiz de Rosas y Quevedo, 2011). Ante este problema, varias figuras políticas emplean discursos de mano dura y proponen el uso de tecnologías para reducir la inseguridad, como la expansión indiscriminada de cámaras de vigilancia, sin intentar resolver explícitamente sus causas. Esto describe un escenario propicio para la expansión de empresas de seguridad privada y vigilancia electrónica en la región, que ofrecen productos y servicios para atender los problemas de inseguridad de empresas y ciudadanos, que el Estado no llega a resolver.

En este contexto, el presente artículo indaga sobre un tema poco investigado en áreas con capacidad estatal limitada como las de América Latina: las implicancias del continuo proceso de digitalización y automatización en la industria de seguridad privada y de vigilancia electrónica. Por digitalización se entiende la recolección de todo tipo de datos sobre las interacciones entre humano y máquina o máquinas en formato digital (p. ej., audios, textos, videos, etc.), tendencia denominada *datafication* en la literatura anglófona (Mayer-Schönberger y Cukier, 2013, p. 21). En cambio, la automatización alude al progresivo reemplazo de humanos por robots en los procesos de trabajo de diferentes industrias (Brynjolfsson y Mcafee, 2016), tales como los autos que se manejan solos o los brazos robóticos automatizados empleados en líneas de producción. Cabe remarcar que estos procesos no son independientes. Al contrario, el avance significativo de la automatización depende de la digitalización, ya que mientras más datos se tengan de los procesos de trabajo por automatizar, más fácil será diseñar e implementar robots que reemplacen a los seres humanos con base en técnicas de aprendizaje automático. En el artículo se argumenta que, si bien la digitalización y la automatización evidentemente ofrecen algunos beneficios para los clientes de las empresas de seguridad privada y vigilancia electrónica, el avance de estos procesos genera nuevos desafíos para la seguridad de los países con áreas de capacidad estatal limitada. Específicamente, se detallan las siguientes consecuencias de la digitalización y automatización: el incremento de la dependencia tecnológica, la oferta de falsas soluciones tecnológicas que no resuelven los complejos problemas sociales que provocan la inseguridad, la creciente susceptibilidad a fallas tecnológicas de los equipos de vigilancia

electrónica y su amenaza a los derechos humanos.

La próxima sección describe el marco conceptual empleado en el artículo, seguido de una descripción de la metodología utilizada. Luego, se analizan las principales características del discurso global y de las prácticas de empresas transnacionales de seguridad privada y de vigilancia electrónica que operan en Argentina. En seguida, se examinan cuatro serias tensiones del proceso de digitalización y automatización de las empresas de seguridad privada y vigilancia electrónica en áreas con capacidad estatal limitada. Finalmente, el artículo concluye con una síntesis de los principales puntos y recomendaciones de política pública para contrabalancear las asimetrías en favor de estas empresas.

Marco conceptual

Para comprender los impactos de la digitalización y automatización en empresas de seguridad privada y vigilancia electrónica, el artículo emplea un marco conceptual compuesto por los siguientes tres pilares. Primero, se acepta la tesis de que estas empresas son productos de la globalización neoliberal de las últimas décadas. Segundo, se propone un enfoque de seguritización modificado, a fin de comprender la manera como estas empresas hablan de seguridad. Finalmente, se utiliza ideas de los estudios sociales de la ciencia y tecnología, a fin de considerar el creciente rol de redes de dispositivos electrónicos y humanos en la seguridad.

Varios autores coinciden en señalar que el factor detonante del proceso de expansión de empresas de seguridad privada es la difusión de ideas neoliberales a nivel mundial (Gill, 2008; Kruck, 2014), que, como parte de una globalización timoneada por EE. UU. en un contexto de posguerra fría, redujeron la capacidad de intervención de los Estados en la economía. Una de las consecuencias de la ideología neoliberal ha sido el incremento de la desigualdad mundial, lo cual ha provocado que los ciudadanos más acaudalados crecientemente incorporen servicios y productos de estas empresas privadas de seguridad, a fin de complementar o de reemplazar los servicios de las fuerzas de seguridad públicas. Asimismo, la expansión de empresas transnacionales de seguridad es central para reducir los riesgos en los procesos de acumulación de capital de las empresas, en general, y de las transnacionales, en particular.

Si bien la relación entre empresas privadas de seguridad y los Estados tiene tanto dimensiones de complementariedad como de competencia, las áreas con capacidades estatales limitadas son las que enfrentan mayores desafíos en este vínculo. Siguiendo a Börzel y Risse (2010, p. 119), el concepto de área con capacidad estatal limitada alude a áreas donde las autoridades gubernamentales no tienen la habilidad de implementar ni de hacer

cumplir reglas y decisiones, o donde el monopolio legítimo sobre el uso de la violencia se encuentra ausente o es restringido tanto en algunas partes de su territorio, como hacia determinados grupos sociales. Por ejemplo, en los casos donde grupos terroristas u organizaciones de crimen organizado disputan la autoridad estatal. En otras palabras, este concepto intenta caracterizar la situación contemporánea de la globalización, que creó serias limitaciones en varios Estados *vis-à-vis* con actores no estatales, como las empresas transnacionales. Es importante destacar que el concepto no es dicotómico, sino más bien un gradiente, que contiene en un extremo a los denominados Estados fallidos, y en el otro a Estados consolidados como EE. UU.; ahora, en el medio, abarca una variedad de países con áreas de capacidades estatales limitadas (Risse, 2011), por ejemplo, zonas controladas por guerrillas o sectores industriales donde las decisiones de política son fuertemente influenciadas por empresas. Este último caso es el de mayor interés de este artículo, ya que el sector de la seguridad privada justamente le disputa a los Estados su privilegio del monopolio de la violencia, que en los casos extremos donde los Estados no cuentan con capacidad ni recursos, dejan un vacío de gobernanza que queda bajo la autoridad íntegra de las empresas transnacionales. En cambio, los Estados consolidados, con economías fuertes, suelen ser huéspedes de las empresas transnacionales, y, por ende, cuentan con mayores capacidades regulatorias que, en parte, limitan las consecuencias más negativas de sus acciones, como la violación de distintos derechos humanos.

La principal consecuencia de la creciente influencia económica y política de las empresas transnacionales de seguridad privada y vigilancia electrónica es su mayor influencia en la agenda de lo que es un problema de *seguridad*. Para comprender esto, es importante considerar el concepto de *seguritización* de la escuela de Copenhague, que fue desarrollado tras la guerra fría para conceptualizar las nuevas amenazas a la seguridad internacional, más allá de las militares. Se trata de un enfoque posestructuralista, que entiende que la seguridad no es algo que puede ser definido de forma objetiva. Al contrario, se propone entenderla como el proceso en el cual determinados actores declaran (*speech-act*) que algo o a alguien (objeto referencial en la literatura) está amenazado en su existencia (Buzan, Waever y Wilde, 1998), y, por lo tanto, se requiere que el Estado tome medidas excepcionales y urgentes para protegerlo. Es decir que, desde tal óptica, la seguridad es una construcción intersubjetiva, y de esta forma puede abarcar las diferentes expansiones del concepto, más allá de las amenazas militares, como por ejemplo seguridad ambiental, económica, ciberseguridad, etc. Sin embargo, los autores de la escuela de Copenhague consideran que la seguritización es un proceso problemático, ya que evita que las decisiones se tomen de forma abierta y transparente a la luz de las reglas del

sistema político, evadiendo las posteriores responsabilidades (Buzan, Waever y Wilde, 1998, p. 29).

Por tal motivo, la escuela remarca la importancia de los procesos de *desecuritización* para devolver estos asuntos problemáticos a la esfera de la discusión política, de tal forma que no sean fruto de decisiones de excepción (Taureck, 2006; Waever, 1995). Si bien esta perspectiva es muy productiva para extender el alcance de los análisis sobre seguridad, el concepto de seguritización es deficiente para comprender las formas en que actores no estatales, tales como las organizaciones no gubernamentales o las empresas transnacionales, hablan y actúan en términos de seguridad. Según Avant (2007, p. 144), el problema se encuentra en el concepto de *lo político* que la escuela de Copenhague utiliza, y que está inspirado en la perspectiva de Carl Schmitt. Este autor alemán lo definió como una relación intensa que genera una división entre amigo y enemigo, donde el Estado soberano juega un rol central para tomar las decisiones en los estados de excepción, que ocurren cuando el sistema político no puede llegar a un acuerdo. De hecho, en los escritos de la escuela de Copenhague, los actores estatales juegan el rol central en los procesos de seguritización. En cambio, con base en su investigación sobre las ONG y empresas transnacionales en África, Avant (2007) argumenta que estos actores hablan de seguridad aunque de una forma discordante con el proceso de seguritización, ya que su sustentabilidad operativa, en gran parte, depende del hecho de mantener relaciones apolíticas con diferentes tipos de actores. A pesar de esto, Avant rescata el enfoque posestructuralista, pues es útil para estudiar la forma como los actores no estatales hablan y actúan sobre lo que entienden por seguridad. Este es el enfoque utilizado en el artículo para analizar a las empresas transnacionales de seguridad privada y vigilancia electrónica.

No obstante, dado el creciente proceso de digitalización y de automatización, no es suficiente estudiar la manera como las empresas transnacionales hablan de seguridad, pues también se requiere observar cómo influyen en las prácticas de seguridad por intermedio del diseño de dispositivos electrónicos. Esto va en línea con las investigaciones de frontera de seguridad internacional, que están adaptando conceptos de los estudios sociales de la ciencia y la tecnología para investigar las redes de dispositivos electrónicos (p. ej., *smartphones*, drones, algoritmos, etc.) y a humanos como nuevas formas delegadas de implementar la seguridad (Amicelle, Aradau y Jeandesboz, 2015; Balzacq y Dunn, 2016; Bueger, 2015). Así, se intenta comprender cómo influye el diseño de artefactos y sistemas tecnológicos en las prácticas de seguridad, y cuáles son sus consecuencias, para corregir la ceguera tecnológica en los estudios de relaciones internacionales, que generalmente tratan a la tecnología como algo externo y dado (Mayer, Carpes y Knoblich, 2014).

Método

El artículo se basa en un análisis tanto de los discursos de las empresas transnacionales de seguridad privada y vigilancia electrónica que operan en Argentina, como de los problemas asociados a estas prácticas. Se realizó un estudio de las empresas transnacionales de seguridad privada presentes en Argentina, por tratarse de un país donde la seguridad privada creció considerablemente en las últimas décadas como respuesta a una limitada capacidad Estatal de lidiar con los problemas de inseguridad que enfrentan los ciudadanos. Asimismo, la selección de este caso buscó comprender las implicancias de la digitalización y la automatización de las empresas transnacionales de seguridad privada en un país de América del Latina expuesto a niveles de desigualdad económica; también, buscó comprender limitaciones tecnológicas que no están presentes en las discusiones de académicos de Europa o EE. UU. Si bien hay varios tipos de actores que proveen productos y servicios de seguridad privada y vigilancia electrónica, como el Estado u organizaciones comunitarias o vecinales, el foco del artículo son las empresas transnacionales, porque en distintas regiones, tal como ocurre en la Unión Europea, se experimenta un proceso de concentración del mercado en pocas de esas empresas, que tienen un poder económico y político mayor que el resto de los actores del sector (Steden y Waard, 2013).

Por ende, la hipótesis subyacente al estudio del discurso de empresas transnacionales de seguridad privada consiste en que son pocas las empresas muy influyentes en las tendencias generales del sector. Para estudiarlas, se consideraron las siguientes fuentes de información: 1) los reportes anuales de las empresas, donde se justifica su modelo de negocio, su perspectiva sobre la industria actual y a futuro; 2) información detallada de sus productos y servicios, extraída de sus páginas internacionales (generalmente en inglés), con su respectiva versión en español; 3) datos recolectados mediante la observación participante en eventos del sector y sobre la operación de estas empresas en la ciudad de Buenos Aires, y 4) artículos de periódicos en internet, foros y organizaciones relacionadas con el sector de la seguridad y la vigilancia (principalmente cámaras empresariales y sindicatos). El análisis cualitativo de los datos se realizó con el *software* Atlas.TI, y consistió en la asignación de códigos a las distintas empresas para sistematizar la información recabada por empresa, a fin de detectar patrones en común y diferencias entre ellas, que se analizan a lo largo del artículo.

En cuanto a las empresas transnacionales de seguridad y vigilancia electrónica estudiadas, se seleccionaron aquellas con mayor presencia en Argentina, divididas en dos grupos: 1) empresas que ofrecen varios servicios de seguridad además de productos de video-vigilancia, en particular las siguientes: ADT (EE. UU.), G4S (Reino Unido), Prosegur (Es-

paña) y Securitas (Suecia); y 2) empresas que se especializan en el diseño, la construcción y la comercialización de distintos productos para la vigilancia electrónica, como cámaras, *software* de identificación de imágenes, robots, etc., específicamente las que se mencionan a continuación: Bosch Security (Alemania), Dahua (China) y Hikvision (China). Esta división tiene que ver con los cambios que están ocurriendo en la industria, debido al proceso de digitalización y automatización, el cual permitió el crecimiento de las empresas de vigilancia electrónica. Estas amenazan el liderazgo de las empresas tradicionales de seguridad privada que operan desde hace años prestando servicios con base en recursos humanos, por ejemplo: guardias de seguridad o transporte de caudales. Asimismo, en el sector de empresas de vigilancia electrónica se observa un liderazgo de empresas chinas, como Dahua o Hikvision (*A&S Magazine*, 2017), que, al ofrecer productos de menor costo y con una cada vez mayor sofisticación tecnológica, desplazaron a empresas occidentales. Este hecho se tiene que entender como parte de una competencia geoeconómica y geopolítica de mayor alcance entre empresas de Occidente y China.

Empresas transnacionales de seguridad privada y vigilancia electrónica

A pesar de sus diferencias, las empresas de seguridad privada y vigilancia electrónica tienen algunas características comunes relacionadas a su discurso global, las cuales se detallan a continuación. Entre ellas, se observan las siguientes: la forma arbitraria de hablar sobre "seguridad", aunque sin caer en un proceso de seguritización; la financialización de sus operaciones, y la propuesta de soluciones tecnológicas a los problemas de inseguridad. No obstante, también hay diferencias, en particular en cuanto a sus posturas sobre el respeto a los derechos humanos.

En primer lugar, en todos los reportes de las empresas de seguridad privada se usa frecuentemente la palabra *seguridad*, y se posiciona a las empresas como garantes de tal concepto. Por ejemplo, la presidenta de Prosegur afirma: "La seguridad es un pilar básico para el normal desarrollo de la sociedad y nosotros jugamos un papel relevante en la consecución de un entorno más seguro y, por tanto, de más libertad" (Prosegur, 2015, p. 7). Es decir, se entiende la seguridad como un valor central, pero sin detallar sus características. El resto de las empresas que ofrecen servicios de seguridad tampoco presentan una definición precisa del concepto, pero sí suelen identificar una serie de factores que generan inseguridad, que sus productos y servicios logran prevenir. Por ejemplo, G4S (2015, p. 14) identifica el terrorismo, las migraciones masivas, la inestabilidad económica, las pandemias, el cambio climático y la ciberseguridad como motores del crecimiento de su industria. Del mismo modo, Securitas (2015, p. 2) considera que el terrorismo, los refugiados, los conflictos y la inestabilidad política son fuentes de

inseguridad. En cambio, ADT (2016, p. 77) pone el foco en disparadores más bien locales, como en un aumento de la percepción y las tendencias reales del aumento del crimen, o en eventos en la vida personal que llevan al potencial consumidor a adquirir estos dispositivos (p. ej., compra de una mascota, mudanza a un nuevo hogar, cambio de trabajo, etc.).

En general, estas prioridades se corresponden con asuntos de interés en las regiones de mayor peso económico y político del mundo, como el tema de los refugiados para Europa o el terrorismo y la ciberseguridad para EE. UU. Esta observación es coherente con el hecho de que Europa y EE. UU. son los mercados más lucrativos para estas empresas. Si bien las soluciones desarrolladas para estos problemas pueden adaptarse en otros contextos, los problemas causados por la desigualdad económica, que es tal vez la mayor causa de casos de inseguridad en América Latina, no tienen la prioridad que uno esperaría. Esto es problemático, pues si entendemos a estas empresas no solo como actores económicos, sino también políticos (White, 2011), su creciente influencia a nivel internacional implica que tienen mayores chances de influenciar el rumbo las agendas de las fuerzas de seguridad de países con áreas de capacidad estatal limitada hacia direcciones que no necesariamente contribuyen a la solución de los problemas locales. En cuanto a las empresas transnacionales dedicadas a la elaboración de productos de seguridad electrónica, también se emplea frecuentemente el concepto de *seguridad*, pero en los casos estudiados no se enumeran factores de riesgo o amenazas, ni se ofrece una definición precisa del término (Dahua, 2017; Hikvision, 2017).

En efecto, se emplea el término de seguridad en frases abiertas a interpretación, como: "Bosch te empodera para construir un mundo más seguro" (Bosch Security, 2017). Esta práctica es comprensible, pues al ofrecer solamente los productos que las empresas y otras organizaciones utilizarán, les es conveniente dejar en abstracto el concepto de *seguridad* para que cada usuario emplee sus equipos tecnológicos según sus necesidades, en vez de estar previamente estructurado como pasa en las empresas proveedoras de servicios de seguridad.

En segundo lugar, la operación de las empresas transnacionales en general está bajo la influencia del creciente proceso de *financialización* de la economía mundial, que alude al creciente poder del sector financiero y la expansión de sus prácticas en múltiples niveles (p. ej., empresarial, gubernamental, individual) (French, Leyshon y Wainwright, 2011). Entre los varios cambios que este proceso está produciendo, es importante destacar la creciente presión que los gerentes de las empresas transnacionales tienen para mostrar un continuo aumento del valor de sus acciones en las bolsas donde cotizan. Tal presión para devolverle un mayor valor a sus accionistas es algo evidente en los reportes anuales y en

todos los sitios de las empresas de servicios estudiadas, donde se tiene acceso directo a información detallada de la cotización de sus acciones. En cambio, esto no se muestra en las páginas de empresas de productos, aunque sí en sus reportes anuales. Por un lado, este proceso de financialización obliga a las empresas a respetar un conjunto de prácticas, que aseguran la transparencia de sus operaciones, y a enviar señales de performance a los accionistas para que inviertan recursos de forma eficiente. Por otro lado, esta dependencia de los mercados financieros somete a las empresas a una intensa presión para reducir sus costos y diferenciarse de sus competidores, lo que, en parte, incentiva la introducción de continuas innovaciones tecnológicas para distinguirse de sus competidores (G4S, 2015, p. 13).

En tercer lugar, las empresas transnacionales de productos y servicios de seguridad privada y vigilancia electrónica convergen en la identificación de la tecnología como el factor principal que está transformando la industria y que puede ofrecer soluciones a los problemas de inseguridad que las sociedades contemporáneas enfrentan. A continuación, trazo las principales tendencias plasmadas en los reportes y las páginas web de las empresas de servicios y productos estudiadas.

La principal tecnología de las empresas de seguridad privada y vigilancia electrónica es la video-vigilancia, que explica su oferta de productos y servicios tecnológicos para ofrecerles a sus clientes la posibilidad de realizar vigilancia a distancia. De hecho, Hikvision basa su estrategia de *marketing* en vender formas superiores de percepción, que permitan tomar mejores decisiones. De forma similar, empresas como Prosegur y ADT presentan la video-vigilancia como una forma de disuasión de posibles hechos delictivos. El éxito comercial de esta tecnología tanto en empresas de servicios como de productos de seguridad electrónica es indudable. En pocos años, todo tipo de organizaciones (p. ej., empresas, Estados y hogares) han incorporado productos y servicios asociados a la video-vigilancia. Una de las tendencias más recientes en servicios de vigilancia está representada por el denominado Ojo del Halcón, de Prosegur, que consiste en un tótem, con pantalla, cámara y parlantes, que le permite al guardia de una empresa controlar al mismo tiempo, desde la distancia, varias organizaciones que lo tengan instalado. De esta forma, la empresa baja los costos de operación, ya que un mismo video-guardia puede observar más de un lugar a la vez desde el centro de monitoreo de la empresa, y actuar sin presencia física en el lugar.

La vigilancia móvil es otra de las tecnologías que creció considerablemente en la oferta de las transnacionales. Esto se debe a la expansión del uso de *smartphones* y *tablets* en la población, que permiten descargar *apps* desarrolladas por las empresas para controlar cámaras a distancia, llevar un registro de la ubicación de personas queridas por intermedio de tecnologías de

georreferenciamiento, etc. Por ejemplo, ADT ofrece la herramienta FIND U ('encontrarte'), que facilita las prácticas de *sousveillance* (o vigilancia desde abajo) de sus clientes, dado que pueden saber, en tiempo real, la ubicación geográfica de otras personas de su círculo cercano que usen el servicio, y en caso de emergencias pueden enviar con sus celulares señales de pánico al centro de seguridad de la empresa.

Impulsada gracias a los avances en inteligencia artificial y a la recolección masiva de datos (*big data*), la automatización es otra de las tendencias emergentes en algunas de estas empresas. En efecto, las empresas de productos están incursionando en el desarrollo de distintos tipos de robots para la vigilancia, tales como drones y robots móviles terrestres que puedan reemplazar a los guardias de seguridad humanos. Hay varias nuevas PyME innovando en esta área, que compiten con las transnacionales, como Knightscope en EE. UU., que ofrece toda una gama de robots que actúan como guardias de seguridad. En general, estas empresas argumentan que los robots son más convenientes porque no sufren el desgaste que padecen los guardias de seguridad privada, y porque son de menor costo; también, suelen destacar que son complementarios al accionar de los guardias humanos. Debido a esta tendencia, no es de extrañar que las empresas de servicios de seguridad privada también estén invirtiendo de forma estratégica en robots (Securitas, 2015, p. 4), ya que su negocio está amenazado por la automatización. Por ejemplo, Prosegur (2015, p. 23) ya ofrece servicios de drones especialmente diseñados para tareas de vigilancia.

Debido a la creciente digitalización y automatización, todas las empresas de vigilancia electrónica se están especializando en la Internet de las Cosas, dado que su objetivo es ofrecer todo tipo de artefactos para la vigilancia conectados a internet. Esto explica su provisión de dispositivos de vigilancia para las denominadas *ciudades inteligentes* y *casas inteligentes*. Si bien el adjetivo 'inteligente' puede parecer hiperbólico, la reciente incorporación de técnicas de aprendizaje profundo (*deep learning*) (Hikvision, 2017, p. 17) están revolucionando la industria de seguridad privada, pues permiten reconocer automáticamente de forma muy eficiente y en tiempo real todo tipo de sujetos y objetos en videos. Por lo tanto, con respecto a los vehículos, cada vez es más sencillo identificar las patentes, el color, el tipo e, incluso, si el conductor está empleando o no cinturón de seguridad (Hikvision, 2017, p. 20). De igual modo, se puede individualizar a cualquier sujeto en los circuitos de cámaras de una empresa o ciudad en pocos minutos con tan solo una foto de aquel (BBC, 2017). Es evidente que estas tecnologías aumentan considerablemente las posibilidades de vigilancia de sus usuarios, y su adopción, desde el punto de vista técnico, seguramente irá en aumento.

Una de las diferencias entre las empresas de servicios y las de productos es

que las primeras apuntan a vender *soluciones integrales* de seguridad (G4S, 2015, p. 41), es decir, no solamente los nuevos y sofisticados equipos de vigilancia electrónica, sino que ofrecen diseños adaptados a las necesidades de los clientes, que contemplen personal de seguridad de la empresa utilizando sofisticadas tecnologías. Por ejemplo, Zacarías Erimias, consejero delegado de Securitas España, declaró:

> El sector se transforma, y el vigilante evoluciona hacia un especialista de seguridad con más herramientas. Hoy lleva un *smartphone* con las aplicaciones de control, pronto llevará *wearables*, y el terminal de gestión de los drones que vigilarán espacios inaccesibles para él. Hemos desarrollado sofisticados sistemas basados en la tecnología para aumentar la seguridad, pero por sí solos no suplantarán a las personas. (Blázquez, 2015)

Es decir, las empresas de servicios de seguridad, como Prosegur o G4S, están progresivamente incorporando sistemas de vigilancia electrónica en su oferta, pero estos quedan bajo la administración y el control del personal de sus propias empresas. En cambio, las empresas transnacionales de productos de vigilancia electrónica, como Dahua o Bosch Security, se destacan por vender los productos y sistemas de vigilancia que pasan a ser administrados por sus propios sus clientes. El aspecto que tienen en común ambos casos es que las empresas transnacionales propician la expansión de plataformas tecnológicas de vigilancia, que son complejas redes de dispositivos electrónicos y humanos para realizar un control de forma personal, a distancia y en tiempo real, que crecen a la par de las redes estatales de vigilancia.

En último lugar, la mayoría de las multinacionales de servicios de seguridad privada y vigilancia electrónica occidentales intentan proyectar una identidad de actor sensible, transparente y responsable, que respeta los derechos humanos y contribuye de forma "positiva" a la sociedad por intermedio de diferentes mecanismos. Por ejemplo, elaboran reportes periódicos de Responsabilidad Social Empresaria (RSE), donde detallan sus aportes sociales y explican los diferentes mecanismos para denunciar el comportamiento inapropiado de sus empleados; también, algunas empresas tienen sus propios códigos de conducta y de buenas prácticas.

Siguiendo a Börzel y Risse (2010), estas iniciativas se pueden entender como una estrategia conveniente para estas empresas, al operar en países con áreas de capacidad estatal limitada, ya que legitiman sus operaciones tanto en sus países de origen como en el exterior, y, si son efectivamente puestas en práctica, vuelven sus negocios más sustentables en el tiempo. No obstante, este tipo de compromisos de buena conducta brillan por su ausencia en la mayoría de las empresas transnacionales que se especializan en el diseño y la comercialización de equipos de video-vigilancia, en particular las chinas.

En parte, se puede argumentar que el uso que se le dé a sus tecnologías es algo que escapa al control de las empresas de productos de vigilancia electrónica. No obstante, argumentaré en la sección siguiente que la ausencia de compromisos con el respeto de los derechos humanos es un problema.

En síntesis, la seguridad es un concepto que no tiene una esencia estable en estas empresas transnacionales, y que se construye a partir de sus declaraciones discursivas y prácticas. Estas observaciones concuerdan con Avant (2007), ya que las empresas de seguridad transnacionales continuamente están realizando actos de habla (*speech-acts*) sobre seguridad, definiendo qué es un problema y cómo resolverlo, pero de formas que no se ajustan completamente a la lógica de securitización de la escuela de Copenhague. Esto se debe a que las formas de intervención no terminan en decisiones fuera de lo normal, como ocurre en el caso de securitización, sino más bien en la adquisición de productos o servicios que pueden pasar por procesos apolíticos.

Al hablar de *seguridad*, el discurso de las empresas transnacionales combina un conjunto dispar de causas de la inseguridad, un interés por obtener mayores réditos económicos por intermedio de soluciones tecnológicas a los problemas percibidos de inseguridad, y, en el caso de las empresas occidentales, la promesa de actuar de forma ética, respetando los derechos humanos. Si bien hay una evidente indeterminación en términos de lo que se entiende por seguridad, que es una decisión posiblemente estratégica de las empresas transnacionales para operar en contextos variados, no hay que perder de vista que el creciente poder económico de estas empresas en varios países conlleva la intervención de aquellas en la agenda de seguridad por intermedio del diseño de servicios y productos de vigilancia humana y electrónica, que normalizan nuevas prácticas de vigilancia. Efectivamente, el creciente poder económico, político y tecnológico de estos actores puede ser problemático para los ciudadanos y las fuerzas de seguridad de países con áreas de capacidad estatal limitada, por diversos motivos que se detallan en la sección siguiente.

La inseguridad de la vigilancia electrónica

Si bien las empresas transnacionales de seguridad privada y vigilancia electrónica se presentan como genios que resolverán los principales problemas de seguridad que sus potenciales clientes enfrentan, sus operaciones de *marketing* soslayan varios de los inconvenientes que aquellos enfrentan en la práctica. En esta sección examino las implicancias de la digitalización y automatización de la industria de la seguridad privada y vigilancia electrónica desde la perspectiva de países con áreas de capacidades estatales limitadas. En particular, exploro: 1) el problema de la dependencia tecnológica; 2) la oferta de falsas soluciones tecnológicas para complejos proble-

mas sociales; 3) la susceptibilidad a fallas tecnológicas, y 4) la amenaza a los derechos humanos.

Dependencia tecnológica

La producción de tecnologías militares y de seguridad se globalizó en las últimas décadas, razón por la cual ni siquiera las grandes potencias pueden aspirar a una producción cien por ciento autónoma de tecnologías militares y de seguridad. Según Brooks (2005), lo anterior es un factor de estabilidad en el sistema mundial, pues no se alcanza un desequilibrio en términos de estas tecnologías, aunque Brooks también advierte que los efectos de la globalización de la producción de tecnologías de seguridad son desiguales geográficamente, y esto sí puede acrecentar conflictos en países periféricos en las redes de producción de tecnologías y servicios de seguridad. De hecho, la competencia entre las transnacionales para ofrecer las mejores tecnologías que resuelvan los problemas de inseguridad las impulsa a utilizar estrategias de protección de su propiedad intelectual, por ejemplo, mediante patentes. Esto les permite demandar a sus competidores, y hacerles pagar un elevado costo si quieren entrar en su nicho tecnológico, lo cual es un riesgo, ya que "legaliza" el proceso de innovación tecnológica (ADT, 2016, p. 95) y propicia la concentración de conocimiento no solo en las empresas con mayores condiciones para desarrollar tecnologías, sino en aquellas con la estructura suficiente para mantener costosos litigios. A su vez, esta tendencia limita el desarrollo de empresas de tecnologías de seguridad en países con áreas de capacidad estatal limitada, que van a ver restringida su capacidad de competir, al menos durante el periodo que dure la patente.

De igual modo, tales Estados verán reducida su posibilidad de incidir en el diseño de las tecnologías de seguridad bajo el monopolio temporal de las empresas transnacionales. Consiguientemente, la digitalización y la automatización tienden a reforzar la concentración de capacidades tecnológicas en empresas trasnacionales, lo cual incrementa la asimetría del poder económico, político y tecnológico con respecto a los países con áreas de capacidad estatal limitada, y profundiza la influencia de las transnacionales en la agenda de las fuerzas de seguridad estatales (Steden y Waard, 2013). Esto, sin duda, puede entenderse bajo el concepto de dependencia tecnológica, que emana de la literatura de dependencia latinoamericana y alude a las asimetrías entre países en el desarrollo y aplicación de tecnologías en la economía mundial (Castells y Laserna, 1989). No obstante, también se puede argumentar que, gracias a sus capacidades tecnológicas y financieras, las transnacionales pueden desarrollar tecnologías adaptadas a las necesidades locales. De hecho, ya lo están haciendo, por ejemplo: la sede de Prosegur en Argentina diseñó el Ojo del Halcón, y presentó la solicitud de la patente para esta invención. Es decir, se trata de un desarrollo local, ajustado a las necesidades de bajar el

costo y, a la vez, de disuadir a posibles criminales, el cual se puede expandir a todas las unidades de negocio de la empresa en otros países. En este caso, otras jurisdicciones tendrán que padecer el problema que se detecta con respecto a tecnologías generadas en el exterior. Sin embargo, esto no niega sino que confirma la existencia de un proceso de concentración tecnológica en transnacionales, así como de la redistribución del poder entre los actores dedicados a la seguridad, especialmente a favor de estas transnacionales, en desmedro de las fuerzas locales de seguridad.

Si bien la dependencia tecnológica es un problema histórico y común entre varias industrias de los países de América Latina, las mismas preocupaciones ya están presentes en el debate público de países occidentales, donde las empresas chinas lograron una alta penetración en el mercado. No obstante, hay una diferencia, pues el uso histórico del concepto en los países de América Latina se asocia con la falta de capacidades tecnológicas para el desarrollo de tecnologías, mientras que el debate en países como EE. UU. o de Europa tiene que ver más con el riesgo a su seguridad nacional causado por el uso de productos de origen chino de menor costo. Por ejemplo, la prensa británica explica que Hikvision está bajo el control del gobierno chino, algo que teóricamente le permitiría introducir *puertas traseras* (*backdoors*) en los equipos que venden en el exterior para operaciones de espionaje (Knowles, 2016). Por ende, agentes del servicio secreto del Reino Unido (MI6) proponen limitar el ingreso de estos equipos a sus mercados o, al menos, realizar revisiones de seguridad más estrictas, en particular para las aplicaciones gubernamentales de los mismos.

De forma similar, EE. UU., por miedo al espionaje de China (Honovich, 2016), prohibió la compra de equipos de Hikvision para ser usados en sus embajadas. Si bien no hay pruebas de espionaje, las sospechas de los artículos no son descabelladas, pero se puede agregar que las empresas occidentales encargadas de vender productos y servicios similares de vigilancia están en las mismas condiciones de realizar tal tipo de operaciones en otros países. Sin embargo, estas preocupaciones están ausentes en el debate público de los países de América Latina, donde la dependencia con proveedores extranjeros es considerable.

Falsas soluciones tecnológicas para complejos problemas sociales

El proceso de financialización empuja a las empresas de seguridad privada y vigilancia electrónica por senderos de desarrollo tecnológico que les permita ofrecer soluciones diferenciadas con respecto a sus competidores. Ahora bien, una crítica que se puede hacer es que esta presión financiera necesita que el problema de la inseguridad continúe, pues, si no, la industria se volvería insustentable e innecesaria. Esto también explicaría por qué la industria se inclina, como tantas otras,

por soluciones tecnológicas simples en respuesta a problemas sociales complejos, las cuales muchas veces son totalmente inadecuadas para resolverlos (Morozov, 2011, p. 305). En efecto, si bien la cantidad de dispositivos de vigilancia electrónica está en aumento, no hay evidencia contundente sobre su capacidad de disuadir actividades criminales.

De hecho, su existencia no evita que los perpetradores puedan encontrar formas de sobrepasar estas medidas, al cubrir sus rostros durante los hechos delictivos o al atacar las cámaras de seguridad. Indudablemente, la tecnología por sí sola no resolverá el problema de la inseguridad ciudadana, que se trata de un fenómeno de múltiples causas, siendo una de las principales, en América Latina, la gran desigualdad de ingresos y oportunidades entre la población. Sin embargo, la desigualdad como causa de la inseguridad está prácticamente ausente de los reportes y sitios web de estas empresas. Por lo tanto, no es arriesgado pensar que estamos ante soluciones tecnológicas simples, que en la práctica son ineficaces por soslayar las complejas causas de los problemas de inseguridad.

Pero si esto es así, ¿por qué el mercado de empresas de seguridad privada y de tecnologías de seguridad y vigilancia continúa creciendo? Para responder a esta pregunta, sin duda se requiere de un estudio detallado de las prácticas de consumo de productos y servicios de seguridad (Goold, Loader y Thumala, 2010), pero hay dos hipótesis que no pueden ser ignoradas en tal iniciativa. Primero, la creciente desigualdad económica genera un aumento de la percepción de inseguridad por parte de los sectores de mayores recursos, que son los principales consumidores de los sofisticados productos y servicios de vigilancia electrónica, a pesar de ser en muchos casos los que menos sufren los hechos de inseguridad (Kessler, 2013). Segundo, las soluciones tecnológicas son funcionales para la difusión de discursos conservadores, de "mano dura" y que promueven el castigo a criminales, por parte de varios políticos y sectores de la población en la región, que, en vez de intervenir para reducir los determinantes sociales del crimen, prefieren apoyar las soluciones tecnológicas que las empresas de seguridad les ofrecen, sin cuestionar su efectividad.

Fallas tecnológicas

Las empresas de seguridad prometen que sus soluciones son eficaces para resolver la inseguridad de sus clientes, pero en la práctica estas promesas no siempre se cumplen, debido a distintos tipos de fallas que todo sistema sociotécnico puede llegar a sufrir. Por ejemplo, las alarmas de seguridad pueden y suelen fallar seguido. Por tal motivo, empresas como ADT consideran a las falsas alarmas como un riesgo para su negocio en países como EE. UU. y Canadá, porque el Estado las penaliza si envían señales falsas a los servicios de seguridad estatal. Otro argumento común a favor de la video vigilancia es que esta permite registrar

los movimientos de sospechosos, tanto como forma de disuasión o como elemento de prueba para un juicio posterior. No obstante, los datos grabados no siempre son fidedignos. Ya hay casos de personas que han sido injusta y erróneamente condenadas por culpa de errores de interpretación de las imágenes grabadas por cámaras de vigilancia (Kofman, 2016a), que también ponen seriamente en duda la precisión de los sistemas de identificación automática de rostros.

Finalmente, la expansión de los dispositivos de vigilancia electrónica puede reducir algunos problemas de inseguridad, pero a la vez genera nuevos en términos de ciberseguridad, ya que tales dispositivos son susceptibles de ciberataques por parte de atacantes malignos, que los pueden dañar, utilizar de forma indebida o usar para el robo de datos personales de sus usuarios. Por ejemplo, recientemente usuarios malintencionados explotaron vulnerabilidades en el software de miles de cámaras de vigilancia de Dahua para controlarlas a la distancia y así montar un ataque de denegación de servicio (DDoS) a reconocidos sitios como AirBnB, Twitter, *The New York Times*, entre otros; bloquearon el acceso a estas páginas por varias horas (Fox-Brewster, 2017; Sanger y Perlroth, 2016), algo que causó pérdidas económicas significativas a estas empresas.

Si bien estas vulnerabilidades explican parcialmente el creciente interés e inversión en el área de "ciberseguridad" por parte de las empresas transnacionales de seguridad y vigilancia electrónica —tanto en términos de oferta de servicios para otras empresas como para garantizar la seguridad de la operación de sus artefactos y servicios— no deja de ser evidente que la creciente digitalización y automatización de sus productos y servicios son susceptibles de ser víctimas de diversas fallas tecnológicas que aumentan su inseguridad.

Violación de derechos humanos

La digitalización de las empresas de seguridad privada, dedicadas tanto a servicios de vigilancia electrónica como a proveer de productos para estas actividades, propician nuevas prácticas que ponen en riesgo los derechos humanos, principalmente el derecho a la privacidad. En efecto, los servicios de las empresas transnacionales de seguridad dependen de la colección masiva de datos, como de videos o información sobre geoposicionamiento, que se resguardan y analizan en sus centros de datos en tiempo real. Sin duda toda esta información es muy sensible, ya que revela patrones confidenciales e íntimos de los perfiles de los clientes de estas empresas. De hecho, empresas como ADT (2016, p. 90) reconocen que es un riesgo para su negocio no poder asegurar tales datos ante ataques informáticos.

Pero no solo sus clientes se exponen a estos nuevos riesgos, sino también todos aquellos que por diversos motivos quedan en algún momento bajo ob-

servación de los sistemas de vigilancia de estas empresas, y que pueden sufrir de las decisiones poco transparentes de estas. Este tipo de preguntas son de suma importancia, dada la velocidad de la innovación tecnológica en el área de reconocimiento facial y sonoro, que está revolucionando los sistemas de vigilancia privados y estatales. No se trata de dudas meramente teóricas; al contrario, en EE. UU., varias organizaciones que defienden los derechos civiles exigieron información a la policía sobre cómo aplican la tecnología de reconocimiento facial para identificar sospechosos, ya que se teme que la usan de forma indiscriminada, sin ningún tipo de procedimiento legal, y sin sopesar las discriminaciones en el sistema que padecen los afroamericanos y otras comunidades étnicas (Kofman, 2016b).

En cuanto a las empresas proveedoras de equipos de vigilancia electrónica, el problema radica en que el creciente control del mercado de estas empresas les permite popularizar diseños de sistemas tecnológicos que no necesariamente respetan los derechos humanos. En particular, la cobertura en los diarios occidentales muestra preocupación por la ventaja que tomó China en esta área, dado que sus menores restricciones legales para la recolección y análisis de los datos de los ciudadanos le permite a sus empresas innovar en sus sistemas de vigilancia en una forma en que las empresas occidentales no lo pueden hacer. Como se mencionó previamente, el uso de cámaras de seguridad con tecnología de inteligencia artificial incorporada ya es la norma en China, donde es fácil reconocer personas y estimar atributos, como género, edad, con gran precisión. Efectivamente, las autoridades afirman que pueden reconocer y estudiar los patrones de interacción social de las personas simplemente con base en un documento de identidad (Human Rights Watch, 2017) y, a su vez, se sospecha que estas buscan extender considerablemente sus capacidades de identificación de sujetos mediante técnicas de identificación de voz.

Por supuesto, la expansión de este tipo de tecnologías biométricas en China genera crítica y oposición por parte de organismos que defienden los derechos políticos y civiles en Occidente, ya que tales tecnologías pueden ser fácilmente utilizadas para acallar a las voces críticas del gobierno. Si bien la descripción de los periodistas que critican a China puede ser precisa, no hay que olvidar que las empresas occidentales hacen algo similar en donde operan, pero con las capacidades de vigilancia concentradas en empresas transnacionales, que, tal como divulgaron las revelaciones de Snowden, bajo presión suelen colaborar con los Estados donde tienen su casa matriz para operaciones de espionaje y vigilancia.

Asimismo, la creciente automatización de las actividades de seguridad privada, debido tanto al uso de robots físicos como de sofisticados algoritmos que reemplazan las tareas de vigilancia visuales, posiblemente tendrá

un impacto negativo en términos de derechos laborales. Ya son múltiples los conflictos sindicales en el sector, debido a las precarias condiciones de trabajo actuales, en empresas nacionales y transnacionales y, por ende, no es exagerado estimar que la automatización los exacerbará. Si bien es cierto que estas innovaciones tecnológicas crearán nuevos puestos, estos probablemente serán para personal técnicamente calificado, mientras que el personal sin el entrenamiento adecuado quedará desempleado. Por lo tanto, hay un riesgo de que se incremente la conflictividad en el sector en términos laborales.

En fin, como las transnacionales probablemente estarán a la vanguardia en el uso y la venta de tecnologías de seguridad privada y de vigilancia electrónica en países con escasas o medianas capacidades de desarrollo tecnológico autóctono, cabe preguntarse si aquellas tendrán recaudos en estos países donde la sociedad civil no está tan informada sobre estas nuevas formas digitales de violar los derechos humanos, y donde la legislación al respecto suele estar rezagada o ser inexistente (Cejas y González, 2014).

Conclusión

Las empresas transnacionales son un vector clave en la privatización de la seguridad y en el aumento de prácticas de vigilancia electrónica en las sociedades contemporáneas. Tal como observó Avant (2007), estas transnacionales hablan de *seguridad* de formas que no encuadran con todos los supuestos del marco teórico de la escuela de Copenhague. De hecho, en los casos considerados se observaron discursos que mezclan con diferente intensidad temas relacionados con la seguridad pública, la innovación tecnológica (como si se tratara de empresas de Silicon Valley) y, en el caso de las empresas occidentales, con expresiones de interés por el respeto a los derechos humanos. Si bien en el contexto de países con Estados fuertes se habla de *gobernanza nodal*, donde se redistribuye el poder entre actores públicos y privados, en países con áreas de capacidad estatal limitada estas imágenes de equilibrio entre actores son engañosas.

En efecto, en tales casos, las asimetrías de poder entre ellos son pronunciadas, ya que tales países no siempre pueden regular adecuadamente las empresas transnacionales de seguridad y de vigilancia electrónica. No es nuevo afirmar que el poder corporativo saca ventajas en países con gran desigualdad social, donde las instituciones no funcionan como deberían, y donde las empresas pueden fácilmente utilizar sus recursos económicos para influenciar a los decisores de la política pública, con el fin de alcanzar sus objetivos y de imponer sus agendas, excluyendo la participación de la sociedad civil. Vale la pena preguntarse si esto es algo siempre negativo o no, aunque se trate de una duda empírica, pues es innegable que la privatización de la seguridad y la vigilancia pone bajo presión la idea de seguridad como un bien público que provee únicamente el Estado.

A la par de liderar el proceso de privatización de la seguridad, las empresas transnacionales de seguridad privada y vigilancia electrónica son pioneras en la digitalización y automatización de los productos y servicios ofrecidos en esta industria. Estos procesos se explican por la acentuación de la globalización neoliberal de las últimas décadas, cuya lógica financiera impulsó a estas transnacionales a una intensa competencia por conquistar mercados a través de soluciones tecnológicas avanzadas que responden a los problemas de inseguridad. Es indudable que la digitalización y automatización en los productos y servicios ofrecidos por estas empresas satisfacen algunas de las demandas de sus clientes, pero, tal como se argumentó en el artículo, estos procesos generan nuevos desafíos para la seguridad de los países con áreas de capacidad estatal limitada.

En primer lugar, pueden reforzar dependencias tecnológicas, ya que la especialización y concentración de productos y servicios tecnológicos en pocas empresas transnacionales aumenta la subordinación tecnológica de las fuerzas de seguridad estatales a estas transnacionales. En segundo lugar, la tendencia a ofrecer soluciones tecnológicas para complejos problemas sociales de inseguridad suelen ser ineficaces, ya que no intentan atacar las causas de los problemas de inseguridad, sino que apenas ofrecen herramientas para evitar sus consecuencias. En tercer lugar, la utopía de un mundo mejor y seguro con base en la compra de soluciones tecnológicas ofrecidas por estas trasnacionales dista mucho de la realidad, ya que en muchos casos estos sistemas crean nuevas vulnerabilidades, por ejemplo, a ciberataques o al robo de información sensible, que ponen en duda la contribución de la industria a la seguridad ciudadana y estatal.

Por último, el diseño de sistemas de vigilancia por parte de estas empresas transnacionales es algo que no está abierto a la sociedad civil, que podría intervenir en los procesos de construcción de tales tecnologías con el fin de asegurar, en su funcionamiento, el respeto de los derechos humanos. Por ende, se trata de un nuevo déficit democrático causado por el incremento de complejos sistemas tecnológicos diseñados por pocas empresas transnacionales, puesto que se reduce el espacio en el que la seguridad es un bien público y no uno privado. A partir de las implicaciones exploradas en el artículo, se deriva un conjunto de propuestas de política pública para los países con áreas de capacidades estatales limitadas, como los de América Latina.

Primero, es indispensable implementar políticas económicas y sociales que ataquen la raíz de los problemas de inseguridad en la región, que en general emanan de los altos niveles de desigualdad.

Segundo, dado que gran parte de los problemas asociados a la digitalización y automatización tienen que ver con la pérdida de capacidades tecnoló-

gicas ante la creciente influencia de empresas transnacionales, es indispensable aumentar las capacidades nacionales en ciencia y tecnología, y en tecnologías estratégicas de seguridad. Esto puede realizarse mediante el aumento de la inversión destinada a la investigación y el desarrollo en áreas de seguridad, así como a través de programas estratégicos que fomenten la transferencia de tecnologías de tales empresas transnacionales a empresas nacionales.

Tercero, en términos de estrategia nacional de ciberseguridad, es preciso contemplar las nuevas vulnerabilidades generadas por la expansión de la Internet de las Cosas en el sector. Esto implica tener que considerar los sistemas paralelos de vigilancia electrónica, administrados por empresas privadas de servicios de seguridad, como infraestructuras críticas, pues así será posible establecer estándares y procedimientos que minimicen sus vulnerabilidades. También, para dificultar potenciales intromisiones de potencias extranjeras, sería aconsejable evaluar o usar equipos de vigilancia de diseño nacional en otras infraestructuras críticas (p. ej., bancos centrales, datos de seguridad social, plantas de energía, etc.).

Cuarto, no es inevitable la reducción de empleos en el sector de la seguridad privada a causa del creciente proceso de automatización, pues, como en otras industrias, los Estados pueden y deben generar incentivos para que las empresas capaciten a sus empleados en estas nuevas tecnologías, a fin de adaptar las tareas que ya realizan, en vez de despedirlos (Eichengreen, 2017), por ejemplo: al propiciar programas de capacitación financiados con mecanismos de inversión público-privados. Este tipo de programas de aprendizaje continuo son imprescindibles para mantener un balance entre capital y trabajo en una época de acelerado cambio tecnológico.

Quinto, hay al menos dos iniciativas que necesitan ser profundizadas para proteger los derechos humanos. Por un lado, dada la creciente expansión de empresas chinas, será necesario demandar una mayor responsabilidad por parte de estas, ya que exportan equipos y prácticas de vigilancia aceptadas en su país de origen, donde la protección de derechos civiles y políticos es diferente de las prácticas legalmente aceptadas en la región. Por otro lado, si bien los niveles de regulación en términos de protección de datos varían en los distintos países de América Latina, el foco de la legislación suele estar en la limitación de los potenciales malos usos de los datos por parte del Estado.

Es importante actualizar y extender tales regulaciones, a fin de limitar el potencial abuso de los datos recabados por parte de los sistemas de vigilancia privados y de asegurar que los sistemas implementados operen de forma transparente. Por último, estoy de acuerdo con los representantes de estas transnacionales cuando demandan mayores regulaciones para el

sector. Sin embargo, pienso que estas no tienen que hacerse a la medida de los intereses corporativos, sino deben incluir las indispensables perspectivas de representantes de la sociedad civil, junto con adecuados mecanismos de control y legislación vinculante de las actividades empresariales, a fin de implementar políticas progresistas en el área de seguridad ciudadana y en la vigilancia, respetando un debido proceso legal dentro del Estado de derecho.

Referencias

ADT Inc. (2016). *The ADT Corporation 2015 Annual Report*. Boca Ratón, FL: ADT Inc. Recuperado de http://www.annualreports.com/HostedData/AnnualReportArchive/a/NYSE_ADT_2015.pdf

Amicelle, A., Aradau, C. y Jeandesboz, J. (2015). Questioning security devices: performativity, resistance, politics. *Security Dialogue*, *46*(4), 293-306.

Arias, P. (2009). *Seguridad privada en América Latina: el lucro y los dilemas de una regulación*. Santiago: Flacso.

Avant, D. (2005). *The Market for Force. The Consequences of Privatizing Security*. Cambridge: Cambridge University Press.

Avant, D. (2007). NGOs, corporations and security transformation in Africa. *International Relations*, *21*(2), 143-161.

A&S Magazine. (6 de diciembre de 2017). Security 50 rankings confirm Chinese industry dominance. *Asmag.com*. Recuperado de https://www.asmag.com/showpost/24137.aspx

Ball, K., Haggerty, K. y Lyon, D. (eds.). (2012). *Routledge Handbook of Surveillance Studies*. Nueva York: Routledge.

Balzacq, T. y Cavelty, M. (2016). A theory of actor-network for cybersecurity. *European Journal of International Security, 1*(2), 176-198. doi:10.1017/eis.2016.8

Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D. y Walker, R. B. J. (2014). After Snowden: Rethinking the Impact of Surveillance. *International Political Sociology*, *8*(2), 121-144. https://doi.org/10.1111/ips.12048

BBC. (10 de diciembre de 2017). In Your Face: China's all-seeing state. [Archivo de video]. *BBC*. Recuperado de http://www.bbc.com/news/av/world-asia-china-42248056/in-your-face-china-s-all-seeing-state

Blázquez, S. (31 de octubre de 2015). Laboratorios contra el crimen: Prosegur y Securitas diseñan el futuro de la seguridad privada en sus centros de innovación. *El País*. Recuperado de https://elpais.com/economia/2015/10/29/actualidad/1446141257_470484.html

Börzel, T. A. y Risse, T. (2010). Governance without a state: can it work? *Regulation & Governance*, *4*(2), 113-134.

Bosch Security. (2017). *About us*. Recuperado de https://www.boschsecurity.com/xc/en/about-us/

Brewster, T. (23 de octubre de 2017). A Massive Number of IoT Cameras Are Hackable – And Now The Next Web Crisis Looms. *Forbes* Recuperado de https://www.forbes.com/sites/thomasbrewster/2017/10/23/reaper-botnet-hacking-iot-cctv-iot-cctv-cameras

Brooks, S. (2005). *Producing Security: Multinational Corporations, Globalization, and the Changing Calculus of Conflict*. Princeton, NJ: Princeton University Press.

Brynjolfsson, E. y McAfee, A. (2016). *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies*. Nueva York: W.W. Norton & Company.

Bueger, C. (2015). Making Things Known: Epistemic Practices, the United Nations, and the Translation of Piracy. *International Political Sociology*, *9*(1), 1-18.

Buzan, B., Wæver, O. y Wilde, J. de. (1998). *Security: A New Framework for Analysis*. Londres: Lynne Rienner.

Castells, M. y Laserna, R. (1989). The New Dependency: Technological Change and Socioeconomic Restructuring in Latin America. *Sociological Forum*, *4*(4), 535-560.

Cejas, E. y González, C. (2015). Estado de la normativa sobre video vigilancia en Argentina y su relación con la protección de datos personales. En *15º Simposio Argentino de Informática y Derecho* (pp. 174-184). Rosario: Sociedad Argentina de Informática e Investigación Operativa.

Dahua Technology. (2017). *Dahua Technology 2016 Annual Report*. Zhejiang: Dahua.

Eichengreen, B. (12 de diciembre de 2017). Two Myths About Automation. *Project Syndicate*. Recuperado de https://www.project-syndicate.org/commentary/two-myths-about-automation-by-barry-eichengreen-2017-12

Fleitas, D. y Quevedo, M. V. (2011). *La seguridad privada en Argentina* [documento de trabajo]. Fundación Arias para la Paz y el Progreso Humano.

French, S., Leyshon, A. y Wainwright, T. (2011). Financializing space, spacing financialization. *Progress in Human Geography*, *35*(6), 1-22.

Gill, S. (2008). *Power and Resistance in the New World Order* (2.ª ed.). Nueva York: Palgrave Macmillan.

Gómez, J. (2008). Private Military and Security Companies and the UN Working Group on the Use of Mercenaries. *Journal of Conflict and Security Law, 13*(3), 429-450.

Goold, B., Loader, I. y Thumala, A. (2010). Consuming security? Tools for a sociology of security consumption. *Theoretical Criminology*, *14*(1), 3-30.

Hikvision. (2017). *2016 Annual Report*. Hangzhou: Hangzhou Hikvision Digital Technology.

Honovich, J. (22 de noviembre de 2016). Hikvision Removed from US Embassy Afghanistan. *IPVM*. Recuperado de https://ipvm.com/reports/hik-removed-embassy

Human Rights Watch. (22 de octubre de 2017). China: Voice Biometric Collection Threatens Privacy: Police, AI Giant Collaboration in Legal Gray Area. Recuperado de https://www.hrw.org/news/2017/10/22/china-voice-biometric-collection-threatens-privacy

Kessler, G. (2013). Algunas hipótesis sobre la extensión del sentimiento de inseguridad en América Latina. *Cuadernos de Antropología Social*, *37*, 25-42.

Knowles, G. (1 de octubre de 2016). Inside China's Big Brother HQ: Its cameras monitor millions of Britons. Now undercover MoS reporters infiltrate the nerve centre of a CCTV giant that spies on its own people to root out dissidents. *Daily Mail*. Recuperado de http://www.dailymail.co.uk/news/article-3817204/Inside-China-s-Big-Brother-HQ-cameras-monitor-millions-Britons-undercover-MoS-reporters-infiltrate-nerve-centre-CCTV-giant-spies-people-root-dissidents.html

Kofman, A. (13 de octubre de 2016a). Losing Face: How a Facial Recognition Mismatch Can Ruin Your Life. *The Intercept*. Recuperado de https://theintercept.com/2016/10/13/how-a-facial-recognition-mismatch-can-ruin-your-life/

Kofman, A. (18 de octubre de 2016b). Study: Face Recognition Systems Threaten the Privacy of Millions. *The Intercept*. Recuperado de https://theintercept.com/2016/10/18/study-lack-of-face-recognition-oversight-threatens-privacy-of-millions/

Kruck, A. (2014). Theorising the use of private military and security companies: a synthetic perspective. *Journal of International Relations and Development*, *17*(1), 112-141.

Mayer, M., Carpes, M. y Knoblich, R. (2014). The Global Politics of Science and Technology: An Introduction. En M. Mayer, M. Carpes y R. Knoblich (eds.), *The Global Politics of Science and Technology* (vol. 1, pp. 1-35). Berlín: Springer-Verlag.

Mayer-Schönberger, V. y Cukier, K. (2013). *Big Data: A Revolution that Will Transform How We Live, Work, and Think*. Nueva York: Houghton Mifflin Hartcourt.

Morozov, E. (2011). *The Net Delusion: The Dark Side of Internet Freedom*. Nueva York: Public Affairs.

Prosegur. (2015). *Informe anual*. Madrid: Prosegur.

Risse, T. (ed.). (2011). *Governance Without a State?: Policies and Politics in Areas of Limited Statehood*. Nueva York: Columbia University Press.

Sanger, D. y Perlroth, N. (22 de octubre de 2016). A New Era of Internet Attacks Powered by Everyday Devices. *New York Times*. Recuperado de https://www.nytimes.

com/2016/10/23/us/politics/a-new-era-of-internet-attacks-powered-by-everyday-devices.html?_r=0

Securitas. (2015). *Annual Report*. Estocolmo: Securitas.

Taureck, R. (2006). Securitization theory and securitization studies. *Journal of International Relations and Development*, *9*(1), 53-61.

Steden, R. van. y Waard, J. de (2013). "Acting like chameleons": On the McDonaldization of private security. *Security Journal*, *26*(3), 294-309.

Wæver, O. (1995). Securitization and Desecuritization. En R. D. Lipschutz (ed.), *On Security* (pp. 46-87). Nueva York: Columbia University Press.

White, A. (2011). The new political economy of private security. *Theoretical Criminology*, *16*(1), 85-101.

Zedner, L. (2006). Liquid security: managing the market for crime control. *Criminology & Criminal Justice*, *6*(3), 267-288.