Chile frente a la vigilancia digital

RENÉ PERALTA ARCAYA

Criptógrafo del Instituto Nacional de Normalización y Tecnología (NIST) de Estados Unidos. Doctor en Computación por la Universidad de California, Berkeley. Ha sido profesor de varias universidades, incluyendo la Universidad Católica de Chile y Yale. Actualmente trabaja en las áreas de aleatoriedad pública, criptografía postcuántica, criptografía de mejora de la privacidad, y complejidad de circuitos.

rene@peralta.one

Este documento fue preparado por René Peralta Arcaya a título personal. Las opiniones aquí vertidas son de exclusiva responsabilidad de su autor, y no reflejan puntos de vista ni de NIST, ni del Departamento de Comercio, ni del Gobierno de Estados Unidos.

Una nueva Constitución chilena sería una oportunidad para enfrentar la vigilancia digital. Estas palabras tienen como objetivo denunciar el fenómeno y llamar a expertos a articular derechos constitucionales que reviertan la precaria situación actual de los ciudadanos chilenos frente al capitalismo de vigilancia.

La vigilancia digital

Mientras camino con mi pareja por el parque, es normal sentirnos dueños de nuestro entorno. En la actualidad, sin embargo, el simple hecho de tener un teléfono con nosotros pone gran parte de este entorno a disposición de intereses ajenos. Nuestra posición geográfica, lo que nos decimos, si nuestros corazones laten lenta o apresuradamente, si nos encontramos con unos amigos, si nos paramos a mirar un árbol o una estatua, si nos abrazamos en el césped... Todo esto es ahora la materia prima de un modelo de despojo y comercialización de nuestras vidas en beneficio de otros.

El rumbo actual de nuestra sociedad es hacia un mundo lleno de sensores. No solo nuestro teléfono, sino nuestro reloj, nuestra ropa, nuestros lentes, y un sinfín de lugares otrora privados son ahora considerados oportunidades de mercado para el capitalismo de vigilancia. Pero no solo nuestros cuerpos. También lo son nuestra casa, nuestros colegios, nuestras calles y parques. En resumen, nuestras vidas. El capitalismo de vigilancia nos despoja de nuestro comportamiento, lo transfiere al mundo digital, y luego trafica esta información en mercados digitales. En estos mercados se lucra, en primera instancia, mediante la predicción algorítmica de nuestro comportamiento futuro en el mercado de bienes y servicios. En segunda instancia el modelo de lucro apunta no solo a predecir, sino que a determinar. Este modelo de intervención en nuestras vidas adopta las técnicas del conductismo de Skinner, expandidas y adaptadas al mundo digital por gurús académicos financiados por el capitalismo de vigilancia. El modelo conductista reduce la persona a su conducta, negando la relevancia de un mundo personal interno que dé sentido a la vida humana. Desde esa perspectiva, no hay un problema ético en el uso de técnicas que modifiquen nuestro comportamiento sin nuestro conocimiento ni permiso. Ni siquiera los más vulnerables entre nosotros, nuestros niños y adolescentes, tienen derecho a santuario. En el libro "The Age of Surveillance Capitalism" [7], Zuboff usa un concepto de Sartre, "la voluntad de ejercer la voluntad", como una condición necesaria de las personas. Si se extingue la voluntad de ejercer la voluntad, se extinguen nuestras vidas. Pero esto es precisamente la meta del conductismo digital. Los dueños del aparato de vigilancia digital nos venden en la medida que nos predicen o determinan. Seres autónomos que reclaman el derecho a ser impredecibles son un obstáculo en los mercados de predicción del comportamiento.

La vida efectiva

Vivir en sociedad es condición necesaria para la vida humana. En la era moderna, esto requiere del acceso a las comunicaciones, al transporte, a la educación, a la información, a la asamblea, al *"chat room"*... Con respecto a esto, es mucho lo que nos ha dado la revolución digital de las últimas décadas.[1] Sin embargo, el capitalismo de vigilancia condiciona el acceso a todo esto a la renuncia de nuestra autonomía y de nuestra privacidad. Vivir sometidos a un régimen de vigilancia corporativa, y acosados por un sinfín de pequeños estímulos conductuales para el lucro de otros, es ahora lo que entregamos en un pacto faustiano para obtener derecho a la vida efectiva. Esta situación global es producto de contingencias históricas (tecnología digital, hegemonía de Estado en el caso de China, globalización, hegemonía del capital consagrada por el neoliberalismo en el caso de Estados Unidos). Distintas contingencias hubieran podido dar otros resultados. En particular, el modelo de negocios basado en la vigilancia no es la única manera de hacer realidad las maravillas de la era digital. La rentabilidad de la vigilancia supera largamente lo necesario para pagar los servicios de información y conectividad de los cuales hemos llegado a depender. El Estado tiene la capacidad de financiar la infraestructura digital y de fomentar un modelo de negocios alternativo, en el cual se respeten los derechos humanos.

A modo de ejemplo, y sin intentar ser exhaustivo, enumero algunos de los principios y derechos que están en juego:

- Acceso a telefonía, y a Internet y sus servicios, sin vigilancia de las corporaciones. La intervención del Estado en estos medios debe ser acorde con derechos humanos y en beneficio de la sociedad y las personas.
- En el hogar y en los lugares sociales, así como en otros entornos del individuo moderno (en la calle, en los buses y autos, en los aviones, en el trabajo), debe ser posible vivir sin vigilancia electrónica.
- La conexión digital de los objetos cotidianos, ya sea entre ellos o con el exterior, no puede ser por defecto. Una vez conectados, la conexión debe ser fácil

1 | Una importante excepción a esta evaluación de lo positivo de la revolución digital, es la deterioración de la información necesaria a los procesos democráticos (ver [3], https://www.newyorker.com/magazine/2019/09/30/the-dark-side-of-techno-utopianism).

de terminar apretando un botón. No es aceptable que tengamos que andar construyendo cajas de Faraday para evitar que los objetos en nuestras casas reporten nuestras conversaciones a terceros.

- Los datos de salud de las personas no pueden ser traficados con fines de lucro.
- Los niños tienen derecho a que sus juguetes no estén conectados a Internet con fines de lucro.
- Los colegios deben ser santuarios adonde no llegue la vigilancia digital ni los estímulos conductuales con fines de lucro. Los modelos en los cuales se le "regala" a un colegio computadores, a cambio de pasarles avisos comerciales y monitorear las comunicaciones de los niños, no tienen lugar en nuestros colegios.
- El uso de técnicas de modificación de la conducta no puede ser en beneficio de intereses comerciales ni políticos. Tampoco pueden tener como objetivo la homogeneidad ni de nuestras conductas ni de nuestro fuero interno. Todo aquello que apunte a extinguir la voluntad de ejercer la voluntad, es un atentado a la persona.
- Estos derechos deben ser inalienables, de manera que el renunciar a ellos no pueda ser condición de acceso a los servicios digitales.

El modelo de negocios del capitalismo de vigilancia

Si compramos un bien de mercado es natural suponer que el dinero que pagamos corresponde al costo de producción y comercialización más un porcentaje de ganancia para el inversor. Pero éste no es el modelo de negocios del capitalismo de vigilancia. Lo ganancia que obtiene Google cuando compramos un Android, se deriva en gran parte del poder de despojarnos de nuestras experiencias de vida para venderlas en un mercado de predicción del comportamiento.[2]

Ahora, ya estamos acostumbrados a la vigilancia. Ésta ya no nos indigna, aunque debiera.

Esta situación es tan inédita que es natural que la persona no comprenda la naturaleza de la transacción. Si hace veinte años nos hubieran dicho que nos dan un teléfono a cambio de grabar nuestras conversaciones privadas y luego lucrar con las inferencias derivables sobre nuestro comportamiento, muchos de nosotros hubiéramos dicho que no. Ahora, ya estamos acostumbrados a la vigilancia. Ésta ya no nos indigna, aunque debiera. Y el individuo ya no puede decir que no, porque ahora esto implicaría renunciar a la vida en sociedad. La única manera de decir que no ahora es a nivel de sociedad y Estado.

También es importante comprender que, habiéndose establecido el modelo de negocios del capitalismo de vigilancia, las corporaciones son ahora prisioneras del modelo. Una empresa como Google no puede, unilateralmente, empezar a respetar los derechos humanos, sin hacerse no-viable comercialmente. La única salida que tenemos, tanto ciudadanos como corporaciones, es establecer la ilegalidad del modelo de vigilancia. Entidades con más poder que el Estado de Chile, por ejemplo la Comunidad Europea, están en eso. Pero las protecciones que los europeos logren establecer no se extenderán automáticamente a los chilenos. La disyuntiva chilena actual ofrece la oportunidad de mejorar la correlación de fuerzas en favor de los derechos humanos de los ciudadanos.

La predicción algorítmica

Hasta hace pocas décadas, la predicción de riesgos, por ejemplo para un seguro de vida, se basaba en no más de unas decenas de datos. El individuo, y las autoridades fiscalizantes correspondientes, tenían acceso a la ecuación que calculaba el riesgo. El capitalismo de vigilancia digital apunta a usar no unas decenas sino miles de datos sobre el individuo. Estos datos, en su mayoría, no son aportados voluntariamente. Ellos incluyen fotos, grabaciones de voz, el entorno del hogar, el historial de localización geográfica, y todo aquello detectable y capturable por el régimen de vigilancia. Los datos ni siquiera son accesibles para el individuo afectado. Además, el cómputo que arroja una medida de riesgo basada en estos datos es usualmente opaco, no solo para el individuo sino también para los mismos dueños de los algoritmos (éste es el caso cuando se usan redes neuronales u otras técnicas de inteligencia artificial [6]). No es posible una fiscalización del cómputo, por ejemplo para hacer respetar principios de equidad. Peor aún, estos algoritmos perpetúan y magnifican sesgos e inequidades [1, 2].

La predicción algorítmica también se usa para "optimizar" sistemas y entornos. Por ejemplo, un colegio "inteligente" del futuro (y también del presente) usaría estas técnicas para "optimizar" la educación de los alumnos. Pero ¿qué es lo que se optimiza? Solo aquello que es factible de expresarse en un número, en una función matemática sobre datos medibles por el régimen de vigilancia. No se puede reducir el bienestar de los individuos ni la salud o efectividad de las instituciones, a lo medible y calculable. Es necesario medir y calcular, pero

2 | Las ganancias de Apple con el iPhone son más complicadas de explicar aquí. Éstas dependen en menor medida, y en forma indirecta (mediante contratos con Google y Facebook), de la vigilancia digital.

sobre aquello es necesario una evaluación no por computadoras sino por personas e instituciones. Tal evaluación debe, además, contextualizarse en una realidad y un marco de valores locales. El capitalismo de vigilancia promueve aplicar la optimización algorítmica a todos los entornos e instituciones sociales, a los colegios, los parques, las ciudades, las comunicaciones, los hospitales... Esto necesariamente lleva a emascular principios y conceptos como equidad, solidaridad, amistad, salud, felicidad. Y, convenientemente para los dueños de los capitales, a elevar la vigilancia como condición necesaria al bienestar humano y social.

Soberanía del Estado sobre la red de Internet

Querámoslo o no, la visión de mundo y sociedad de gran parte de la población está hoy mediada por Internet. La hegemonía de unas pocas corporaciones sobre este medio les otorga un poder inédito sobre el público. Esta asimetría de poder no solo se establece en la relación corporaciones-ciudadanía sino también en la relación corporaciones-Estado. Como lo demostró el caso de Cambridge Analytica (ahora Emerdata), el capitalismo de vigilancia también trafica en influencias sobre los procesos democráticos. No podemos aceptar que una corporación pueda vender al mejor postor un porcentaje posiblemente determinante de votos. El Estado debe tener las atribuciones necesarias para ejercer la soberanía digital en nombre de la ciudadanía. Esto es tanto para proteger la libertad de expresión como para combatir las asimetrías de poder que atenten contra los derechos humanos y los procesos democráticos. Estas asimetrías son enormes. La capitalización de mercado de Alphabet (conglomerado dueño de Google) es varias veces el valor agregado de todas las compañías chilenas. Los estados hacen lo que pueden en defensa de los derechos humanos de sus ciudadanos. Debemos estudiar y aprender de los esfuerzos de instituciones internacionales, como la ONU y la Unión Europea, así como de las denuncias de las organizaciones internacionales de derechos humanos como Amnistía Internacional.[4]

Las redes sociales

La persona moderna requiere de un espacio psíquico privado en el cual forjamos y alojamos nuestra identidad. Este espacio es particularmente vulnerable en la niñez y en la adolescencia, cuando aún no se ha desarrollado la conciencia que una persona tiene de ser ella misma y distinta a las demás. El capitalismo de vigilancia toma por asalto este espacio. El modelo que Facebook ha instalado en las redes sociales apunta a eliminar el espacio privado y sustituirlo por una cara pública (una cara mucho más lucrativa, por cierto). Es en este espacio público donde el adolescente busca la legitimación de su identidad. Los daños que esto causa están ampliamente documentados por psicólogos, sociólogos y filósofos. El poder de quienes controlan este espacio es enorme. ¿De verdad debemos aceptar, por ejemplo, que una corporación trasnacional decida qué nivel de depresión en los jóvenes chilenos es aceptable y compatible con sus ganancias?

Santuario para el hogar

Entre los planes del capital de vigilancia está llenarnos la casa de sensores conectados a sus algoritmos de captura y comercialización de datos. La cocina y el baño son particularmente atractivos para quienes quieren saberlo todo sobre nosotros. Si en un futuro no muy lejano, sentado en el baño de tu casa, el parlante "Google home" te anuncia que, según la taza del baño, tu presión arterial está algo elevada [5], y te recomienda que vayas a tal o cual doctor, ¿cuál será tu reacción? Cuando te expliquen que los sensores del baño tienen como finalidad la protección de tu salud ¿qué pensarás? Es mi esperanza que sientas indignación. Que te preguntes qué cara te habrán visto... Y si tu indignación les resulta incomprensible a tus hijos, ¿qué harás? ■

REFERENCIAS

[1] S. Barocas and A. D. Selbst. Big data's disparate impact. *California Law Review*, 104:671–732, 2016.

[2] F. Z. Borgesius. Discrimination, artificial intelligence and algorithmic decision-making. 2019. Documento del Consejo de Europa.

[3] A. Marantz. The dark side of techno-utopianism. *The New Yorker*.

[4] Amnistía Internacional. Gigantes de la vigilancia: La amenaza que el modelo de negocios de Google y Facebook representa para los derechos humanos. 2019.

[5] US Patent Office. Patente US 10064582 B2, de Google: Noninvasive determination of cardiac health and other functional states and trends for human physiological systems. 2018.

[6] A. Selbst and S. Barocas. The intuitive appeal of explainable machines. *FORDHAM L. REV.*, 87:1085–1139, 2018.

[7] S. Zuboff. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. 1st edition, 2018.