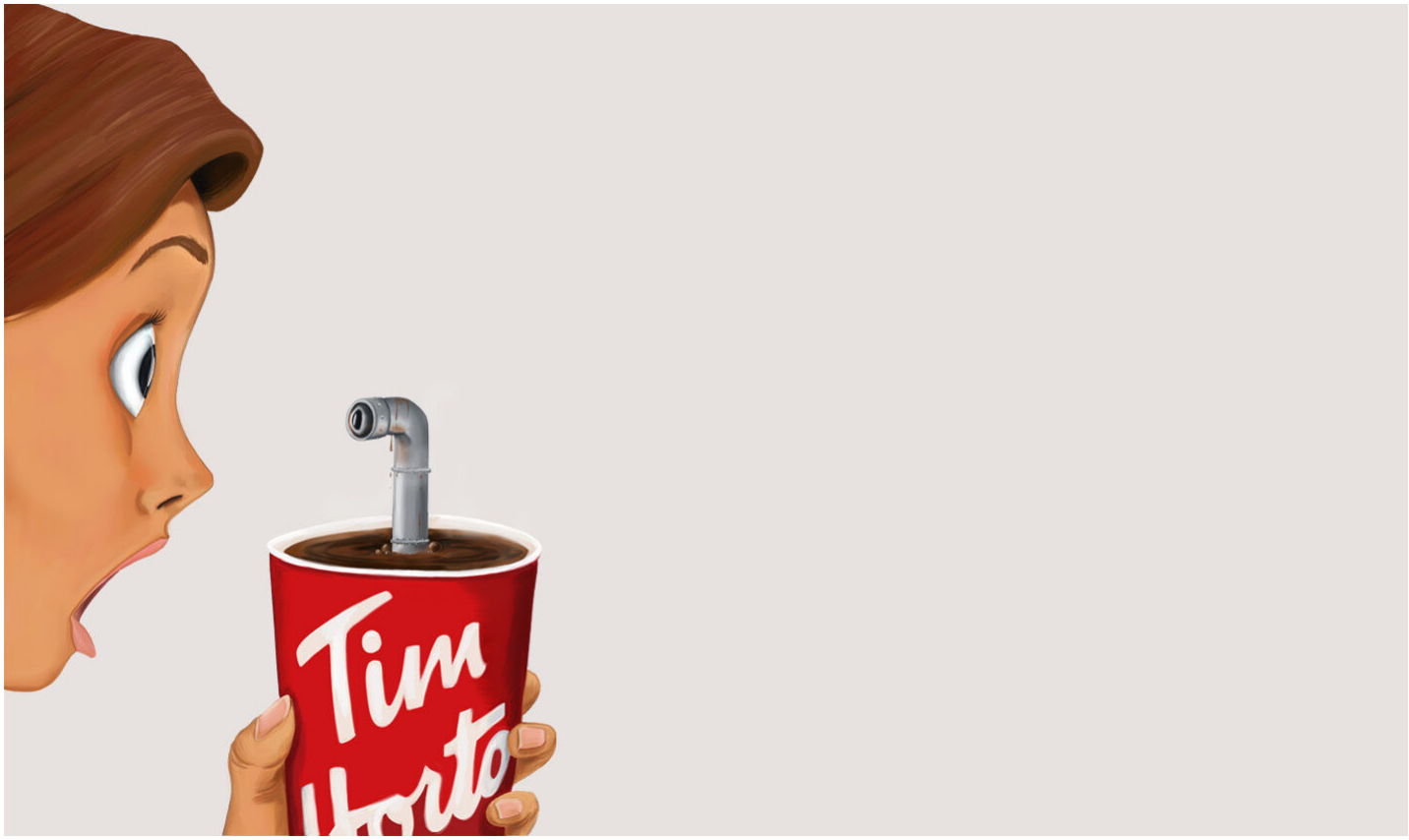

EMMA MOORE/TROMPETA

¿Está su café espiándole?

Los peligros de una sociedad en la que todo está observando.

- Richard Palmer
- 25/7/2022

En Canadá, [la cadena internacional de cafeterías] Tim Hortons está en todas partes. Con 4.300 sucursales, es casi tres veces más numeroso que McDonalds. El 80% de los canadienses pasan por allí al menos una vez al mes.

Y Tim Hortons está vigilando.

Seis millones de canadienses, de una población adulta de 31 millones, usan la aplicación de Tim Hortons para pedir sus bebidas. Uno de ellos es James McLeod, del *Financial Post*, quien se dio cuenta que la aplicación rastreaba su ubicación y presentó una solicitud de libertad de información para saber más. “Desde mi casa hasta mi oficina, pasando por un partido de los Blue Jays en el Rogers Centre, e incluso hasta Marruecos, donde viajé de vacaciones en junio pasado, la aplicación de la empresa registró silenciosamente mis coordenadas y las transmitió a sus servidores corporativos”, escribió McLeod. Basándose en estos datos, Tim Hortons averiguó dónde vivía McLeod.

Si le preocupa la privacidad, está claro lo que tiene que hacer: haga su propio café.

Pero incluso eso podría no ser suficiente. Christopher Balding, de New Kite Data Labs, descubrió unas máquinas de café inteligentes fabricadas en China que enviaban datos a Pekín. Las máquinas Kalerm recopilaban información sobre quiénes las usaban, dónde vivían, si se utilizaban comercialmente y datos de pago.

Es fácil desestimar estos “escándalos”. Usted podría pensar, *¿y qué? El Partido Comunista Chino sabe cómo me gusta el café*

Pero esto es sobre mucho más que un café. Es un ejemplo de lo común e incluso rutinaria que se ha vuelto la vigilancia de alta tecnología.

En venta: usted

La combinación de teléfonos inteligentes y hogares inteligentes significa que una cantidad sin precedentes de datos privados está ahora al descubierto. A menudo, la información de su ubicación está disponible para que la compre el mejor postor.

Muchos de los compradores quieren tener la posibilidad de comercializar su producto exactamente con el consumidor adecuado, en el momento y lugar correctos para maximizar sus posibilidades de conseguir una venta. Esto se ha vuelto tan común y automatizado que estamos insensibilizados a ello. Por eso, cuando usted busca unos zapatos en Amazon, los anuncios de exactamente esa talla y tipo de zapato lo siguen por Internet durante semanas.

Ahora también ocurre estando desconectado. Descargue la aplicación de una tienda o centro comercial, y probablemente le harán ofertas exclusivas. La aplicación también puede registrar en qué parte de la tienda usted pasó más tiempo y qué artículos probablemente miró. Ahora los productos que miró fuera de línea también lo acecharán en la web.

Estos datos se combinan y se venden, tal vez para fines comerciales, tal vez para algo peor. Es difícil imaginar un uso inocente para una lista de datos de víctimas de violaciones o de abusos domésticos. Pero todo está disponible: con 79 dólares se obtienen los datos personales de 1.000 mujeres violadas.

Algunos de los principales clientes de este tipo de datos son los gobiernos. En Estados Unidos, el Servicio de Impuestos Internos, el Departamento de Seguridad Nacional y otras agencias federales compran datos a empresas como X-Mode y Venntel. X-Mode recopila datos de más de 100 aplicaciones diferentes. El senador demócrata Ron Wyden acusó al gobierno de usar “su tarjeta de crédito para burlar la Constitución y comprar información sensible sin una orden judicial”. Los abogados del gobierno alegan que, dado que los consumidores ceden voluntariamente sus datos a estas aplicaciones, el gobierno puede ignorar las restricciones constitucionales a la intromisión gubernamental.

En Canadá, no sólo las cafeterías usan estos datos. En diciembre de 2021, la Agencia de Salud Pública admitió haber rastreado 33 millones de teléfonos móviles durante la pandemia. Contrataron a BlueDot para que rastreara cuánto cumplían los canadienses las restricciones de los cierres, registrando cuándo salía la gente de sus casas, qué distancia recorrían y durante cuánto tiempo.

Quizá el ejemplo más preocupante sea el de las protestas del 6 de enero de 2021 en el Capitolio de Estados Unidos. El fbi usó los datos de Google para rastrear a los asistentes y luego emitió más de 10.000 órdenes judiciales. En este caso, la administración está castigando a los que asistieron a una protesta que no le gustó, y usó los datos de los teléfonos inteligentes para ello.

Quién escucha en casa

Estas prácticas se están trasladando al hogar. Al igual que los datos de los teléfonos inteligentes, los datos del hogar inteligente también están a la venta. “El compromiso continuo con el cliente y la entrega de una experiencia superior es mucho más fácil cuando se sabe lo que está sucediendo en la vida de su cliente en un momento dado”, presume un intermediario de datos.

¿Qué tipo de datos puede incluir? “Qué hacen los consumidores a primera hora de la mañana, cómo interactúan con su dispositivo, dónde les gusta pasar el fin de semana, etcétera”, afirma el sitio web. “Puede utilizarse para entender mejor el comportamiento de sus consumidores”.

La seguridad de los dispositivos inteligentes es notoriamente mala, así que puede que no sean sólo los intermediarios de datos los que lo vigilen. Por ejemplo, los televisores inteligentes con cámara incorporada. La oficina de campo del fbi en Portland advirtió: “Más allá del riesgo de que el fabricante de su televisor y los desarrolladores de aplicaciones puedan estar escuchándole y observándole,

ese televisor también puede ser una puerta de acceso para que los *hackers* entren en su casa".

Las agencias de inteligencia son algunas de las que se introducen en estos dispositivos. WikiLeaks publicó detalles de una herramienta llamada Weeping Angel, desarrollada por la Agencia Central de Inteligencia y el MI5, que convertía los televisores inteligentes de Samsung en infiltrados. Daba a estas agencias acceso al micrófono, a las credenciales del wifi y al historial del navegador.

Los fabricantes de altavoces inteligentes y dispositivos de cámaras domésticas suelen facilitar los datos al gobierno cuando reciben una orden judicial. Algunos fabricantes son muy poco claros sobre su relación con el gobierno, por lo que es difícil saber cuánto entregan. Pero, al menos estas relaciones están restringidas por órdenes judiciales, aunque, como demuestran las protestas del 6 de enero, también se puede abusar de esta notificación legal.

En el extranjero, es fácil imaginar resultados peores. Escocia ha extendido recientemente las leyes de "incitación al odio" al ámbito doméstico. Ciertas opiniones están prohibidas por ley incluso en un entorno privado. ¿Cuánto tiempo pasará antes de que alguien sea procesado por comentarios escuchados por su altavoz inteligente?

Los vínculos con China son aún más preocupantes. Las cafeteras de Kalerm no son los únicos dispositivos inteligentes fabricados por empresas vinculadas al Partido Comunista Chino. "China realmente está recopilando datos sobre cualquier cosa", dijo Christopher Balding. "Como centro de fabricación del mundo, pueden poner esta capacidad en todo tipo de dispositivos que salen a todo el mundo" (*Washington Post*, 14 de junio).

Los micrófonos aparecen cada vez en más dispositivos. No es sólo el altavoz inteligente de Amazon. También es la aspiradora inteligente o el hervidor de agua de alguna marca china poco conocida.

Uno de los mayores actores del mercado del hogar inteligente es Tuya; más de 5.000 marcas incluyen los dispositivos de Tuya en sus productos. Venden más de 1.000 tipos diferentes de dispositivos inteligentes y han vendido más de 100 millones de productos. Como todas las empresas chinas, están obligadas a entregar todos los datos que el gobierno chino les exija. Tuya podría "desviar las masas de datos, incluidos los datos clasificados del gobierno, creados y compartidos en sus redes, y ponerlos a disposición del gobierno chino", escribió *Hill*. "Tuya bien podría estar canalizando la información recogida en las cámaras de seguridad del hogar y en los dispositivos de salud conectados, sólo por nombrar dos ejemplos, hacia Pekín" (30 de julio de 2021).

El año pasado, la empresa de seguridad tecnológica Dark Cubed seleccionó 10 dispositivos inteligentes vendidos en EE UU. Cada uno de ellos "tenía una conexión comercial con China y se observó que cada producto se comunicaba con la infraestructura en China, sin nuestro permiso", escribió.

Sonámbulos en la vigilancia

En junio, China nos dio un ejemplo alarmante de lo que permite esta tecnología.

Algunos bancos chinos se estaban quedando sin efectivo y empezaron a bloquear a algunos depositantes para que no pudieran retirar dinero. Los depositantes enfadados planearon una protesta en la provincia de Henan. Su plan fracasó.

China exige un pasaporte de covid para viajar. Los que planeaban protestar vieron de repente cómo sus códigos sanitarios se ponían en rojo, bloqueándolos. Otros que planeaban viajar a Henan pero no a protestar no se vieron afectados. *El gobierno sabía quiénes iban probablemente a protestar y los bloqueó electrónicamente* "Nos están poniendo unas esposas digitales", se quejó un manifestante que no pudo protestar. Otro dijo: "No puedo hacer nada; no puedo ir a ninguna parte. Te tratan como si fueras un criminal".

El gobierno de EE UU ya está deteniendo a quienes asistieron a una protesta que no le gustó. No es difícil imaginar que tome medidas similares.

Sin embargo, en general, estamos notablemente despreocupados por toda esta vigilancia. O más bien, muchos están preocupados pero no lo suficiente como para hacer algo al respecto. No nos gusta que las empresas nos rastreen y vendan nuestros datos, pero no lo suficiente como para cambiar nuestro comportamiento u obligar a esas empresas a cambiar. La tecnología inteligente es demasiado conveniente.

Pero esta tecnología le está dando a los gobiernos de todo el mundo un alcance sin precedentes en nuestras vidas. Y eso les da un poder sin precedentes.

"La tiranía gubernamental es rutinaria en la historia de la humanidad", escribe Gerald Flurry en su nuevo libro *Estados Unidos bajo ataque*. "No seamos ingenuos y pensemos que algo así nunca podría ocurrir aquí. Nuestros antepasados no eran estúpidos. Querían garantizar la libertad de los estadounidenses. Sabían que Dios es un Dios de libertad; Él quiere que seamos libres. Eso es un regalo de Dios, ¡y ellos lo entendieron!".

La difusión de esta tecnología y su uso por parte del gobierno se produjo en gran medida mientras Barack Obama era presidente. Desde entonces, instituciones clave como la cia y el fbi han permanecido bajo el control de la izquierda radical. Durante el mandato de Obama, Robert Morley escribió en *la Trompeta*: "Tal vez muchas o incluso la mayoría de las personas que son el blanco de agentes de la nsa [Agencia de Seguridad Nacional] y otras agencias policiales de hacer cumplir la ley, *son* en realidad unas amenazas para EE UU. ¡Pero el problema mayor es que *estas agencias oficiales se están expandiendo rápidamente bajo una Administración que en realidad desdeña la ley que juró defender*!" (julio-agosto de 2014).

La Biblia describe este tiempo como uno de aflicción "muy amarga" para las naciones modernas de Israel: Gran Bretaña y Estados Unidos. No había "siervo ni libre, ni quien diese ayuda a Israel" (2 Reyes 14:26).

Si el gobierno está en su casa y en su bolsillo, es difícil mantener una sociedad libre. Y los peligros del abuso de los gobiernos en casa o en el extranjero son enormes.

La izquierda radical está trabajando para que EE UU deje de ser una república constitucional, y están usando el poder proporcionado por dicha vigilancia como un arma. Como muestra *Estados Unidos bajo ataque*, la Biblia advierte que Dios Mismo tendrá que salvar a EE UU de este tipo de tiranía.

Pero la Biblia también advierte que, a menos que cambiemos, EE UU volverá a caer en la tiranía, esta vez impuesta desde el extranjero. Sin el compromiso de EE UU con la libertad, otros países se están levantando. Se profetiza que impondrán su gobierno por la fuerza y podrían aprovecharse fácilmente de este tipo de tecnología.

Sin embargo, como escribió el Sr. Flurry, Dios es un Dios de libertad. Todo esto es parte de Su plan para traer la libertad al mundo, libertad de la tiranía, y libertad de las dolorosas adicciones y pecados que mantienen a este mundo esclavizado.

NO HAY LIBERTAD SIN LEY

En todas partes, la gente lucha y se esfuerza por obtener mayor libertad. Al mismo tiempo, luchan contra la ley. Esto demuestra una peligrosa incomprensión de la naturaleza de la libertad verdadera y de la necesidad de una ley justa. El hecho es que sin ley no hay libertad verdadera. ¿Tiene usted la actitud hacia la ley que conduce a la libertad verdadera?