

To Track Coronavirus, Israel Moves to Tap Secret Trove of Cellphone Data

Enviado por Esmirna Lorena ... en Mié, 03/18/2020 - 17:46

Cita:

Halbfinger, David, Isabel Kershner y Ronen Bergman [2020], "To Track Coronavirus, Israel Moves to Tap Secret Trove of Cellphone Data", *The New York Times*, New York, 16 de marzo, <https://www.nytimes.com/2020/03/16/world/middleeast/israel-coronavirus-c...> [1]

Fuente:

Otra

Fecha de publicación:

Lunes, Marzo 16, 2020

Revista descriptores:

Combate y adaptación frente a la destrucción del ambiente

Corporaciones militares - corporaciones civiles que participan en la producción militar o en actividades militares [3]

Formas de la guerra [4]

Relaciones entre empresas estados y sociedad [5]

Sujetos de la guerra [6]

Tecnologías militares - tecnologías de uso dual [7]

Tema:

Israel acumula datos provenientes de teléfonos celulares para enfrentar la crisis del coronavirus.

Idea principal:

Benjamin Netanyahu, el primer ministro israelí, autorizó el acceso a la agencia de seguridad interna del país a una gran cantidad de datos de teléfonos celulares previamente no revelados. Lo anterior tiene como fin seguir el movimiento de las personas que han contraído coronavirus e identificar a otras que deberían ser puestas en cuarentena. El gabinete de Netanyahu autorizó el movimiento sin precedentes para utilizar datos que se recopilan en secreto para combatir el terrorismo, pero aún debe ser aprobado por el Subcomité de Servicios Secretos del Parlamento.

Las autoridades israelíes no habían informado sobre la existencia de ese conjunto de datos ni del marco legislativo bajo el cual éstos se acumulan y utilizan. El plan para usar los datos en la lucha contra el coronavirus, aún no ha sido debatido por los legisladores ni revelado al público. La idea es examinar cuidadosamente los datos de geolocalización recopilados por los proveedores de teléfonos celulares israelíes sobre millones de sus clientes en Israel y Cisjordania, y así, encontrar personas que hayan estado en contacto cercano con portadores de virus y enviarles mensajes de texto para que se aíslen de inmediato.

La divulgación del plan generó alarmas entre los defensores de la privacidad y los críticos de

Netanyahu, quien está luchando por retener el poder e imponiendo medidas autoritarias en respuesta a la crisis.

Además del rastreo, el gobierno israelí autorizó sentencias de prisión de hasta seis meses para cualquiera que viole las órdenes de aislamiento; también permitió que la policía disuelva las reuniones de más de 10 personas por medio de "uso de fuerza razonable". Según la nota, la mayor prueba a la democracia israelí en este momento de extrema fragilidad es la existencia del conjunto de datos de teléfonos celulares y su uso para rastrear pacientes o portadores de coronavirus.

Malkiel Blass, quien fue fiscal general entre 2004 y 2012, dijo que debido a la disolución del parlamento en diciembre de 2019, el gabinete de Netanyahu ha estado funcionando sin supervisión legislativa y que incluso en la crisis del coronavirus, el núcleo de los derechos civiles en una democracia debe ser preservado.

Como respuesta a estas preocupaciones, los funcionarios del gobierno israelí insistieron en que el uso de datos de teléfonos celulares por parte de la Agencia de Seguridad Interna (Shin Bet, por sus siglas en hebreo), sería limitado, argumentando que el uso de tecnologías avanzadas tiene como propósito salvar vidas.

El Shin Bet ha estado recolectando datos de los celulares desde 2002. Sin embargo, nunca ha revelado detalles sobre qué información recopila, cómo se protegen esos datos, si alguno de ellos se destruye o elimina, quién tiene acceso a ellos y en qué condiciones, o cómo se usa. Dos leyes y una serie de reglamentos secretos y órdenes administrativas rigen el esfuerzo de recopilación de datos y su uso por parte del Shin Bet, dijeron las autoridades.

La Ley de Telecomunicaciones israelí de 1995, otorga al primer ministro amplios poderes para ordenar a los operadores que permitan el acceso a sus instalaciones y bases de datos según sea necesario para realizar las funciones de las fuerzas de seguridad. Además, el artículo 11 de la Ley de la Agencia de seguridad de Israel, de 2002, permite al primer ministro determinar qué tipo de información sobre los suscriptores de teléfonos celulares es requerida por el servicio para cumplir su propósito, y señala que las compañías deben transferir información de este tipo al Shin Bet.

Según esa ley, depende de Shin Bet determinar cómo se utilizan los datos recopilados de teléfonos celulares. Si bien, la ley autoriza su uso durante solo seis meses, el director de Shin Bet es capaz de volver a autorizarlo. Un ex alto funcionario del Ministerio de Justicia dijo que desde 2002, los primeros ministros han requerido que las compañías de teléfonos celulares transfieran a la agencia una amplia gama de datos sobre sus suscriptores. Aunque el funcionario se negó a decir qué categorías de datos se proporcionaron o retuvieron, los datos incluyen la identidad de cada suscriptor, destinatarios o iniciadores de cada llamada, los pagos realizados en la cuenta, así como la información de geolocalización recopilada cuando los teléfonos se comunican con las torres de transmisión celular.

El uso de datos de teléfonos celulares para combatir el coronavirus requiere la aprobación del gobierno porque la Ley de la Agencia de seguridad limita el papel del Shin Bet para proteger a Israel contra amenazas de terrorismo, sabotaje, subversión, espionaje y exposición de secretos de estado. Sin embargo, está permitido actuar de otras maneras "vitales para la seguridad

nacional", pero solo con la aprobación del gabinete y del Subcomité de Servicios Secretos.

Contrariamente a algunos informes israelíes, no hay ningún plan para hackear los teléfonos celulares de los ciudadanos israelíes porque el gobierno ya recibe suficientes datos de los operadores de teléfonos celulares para monitorear el paradero de casi cualquier persona.

Finalmente, Lior Akerman, un ex oficial de Shin Bet, dijo que la agencia tenía buena práctica para distinguir entre objetivos apropiados, aquellos sospechosos de dañar la seguridad nacional y civiles inocentes. Sin embargo, se trata de utilizar las tecnologías existentes para identificar y localizar personas enfermas y portadores que podrían infectar a miles.

Nexo con el tema que estudiamos:

Esta nota señala las medidas que el estado israelí está tomando ante la crisis de coronavirus. Caso interesante, ya que en este país la recolección de datos y el espionaje están legitimados por la ley bajo la narrativa de la seguridad nacional y el combate al terrorismo; además que la coyuntura política está en un punto importante ya que el primer ministro plantea mantenerse en el poder mientras que cada vez toma decisiones más autoritarias. Lo que debe analizarse son las relaciones de poder que hacen plausible el espionaje.

Source URL (modified on 20 Marzo 2020 - 1:07am): <http://let.iiec.unam.mx/node/2743>

Links

[1] <https://www.nytimes.com/2020/03/16/world/middleeast/israel-coronavirus-cellphone-tracking.html>

[2] <http://let.iiec.unam.mx/taxonomy/term/76>

[3] <http://let.iiec.unam.mx/taxonomy/term/72>

[4] <http://let.iiec.unam.mx/descriptores-let/formas-de-la-guerra>

[5] <http://let.iiec.unam.mx/taxonomy/term/20>

[6] <http://let.iiec.unam.mx/descriptores-let/sujetos-de-la-guerra>

[7] <http://let.iiec.unam.mx/descriptores-let/tecnolog%C3%ADas-militares-tecnolog%C3%ADas-de-uso-dual>