Las aplicaciones de rastreo del COVID-19 no deben interferir con los derechos humanos

14 de mayo de 2020- MIENTRAS LOS GOBIERNOS BUSCAN MANERAS DE MONITOREAR Y CONTROLAR LOS CASOS DE COVID-19, EN GLOBAL WITNESS ANALIZAMOS UNA APLICACIÓN GUATEMALTECA PARA DEMOSTRAR CÓMO LAS SOLUCIONES TECNOLÓGICAS APRESURADAS PODRÍAN PONER EN RIESGO A LOS CIUDADANOS.

Hablando sobre música estimulante en un video promocional, Yossi Abadi dice con tono inspirador: "Es en tiempos de crisis y dificultades que se miden las amistades." Abadi es el CEO de Tenlot Group, la compañía multinacional que gestiona la lotería guatemalteca. En conjunto con el presidente de Guatemala, Alejandro Giammattei, anunció el lanzamiento de Alerta Guate, una nueva app proyectada para ayudar al país centroamericano en la lucha contra el coronavirus.

Alerta Guate fue desarrollada por una empresa estadounidense y financiada por Tenlot. Ahora, la compañía de Abadi, que forma parte de un conglomerado con sede en Londres y Tel Aviv, quería "donar" la aplicación al gobierno guatemalteco. Presentándose en varias estaciones televisivas locales, Abadi valoró la contribución en 10 miliones de dólares. Sin embargo una nueva investigación actuada por Global Witness sugiere que la donación de Tenlot podría no haber sido tan caritativa como parece.

LA CARRERA ARMAMENTISTA EN TIEMPOS DE CORONAVIRUS

Los gobiernos y los ciudadanos de todo el mundo están desesperadamente intentando encontrar formas seguras de aliviar las condiciones de cierre que el COVID-19 ha requerido. Las empresas de tecnología han desarrollado aplicaciones y otros software que ofrecen potenciales soluciones para el seguimiento de los contactos, de los síntomas e incluso para la gestión de la cuarentena. Sin embargo, sin las garantías adecuadas, algunas de estas aplicaciones pueden allanar el camino para que los gobiernos autoritarios violen los derechos civiles y repriman a las poblaciones marginadas.

Este no es un fenómeno nuevo: antes de la crisis del COVID-19, el mundo se hacía testigo de estos riesgos causados por la app de vigilancia masiva utilizada por la policía en la ciudad de Xinjiang en China para monitorear y controlar a millones de uigures y otros grupos musulmanes. Pero en este momento particular los gobiernos tienen una razón aparentemente legítima para recopilar información que podría ser usada más allá de la crisis actual para monitorear y reprimir a las comunidades.

Alerta Guate es una nueva aplicación para el COVID-19 que ilustra los riesgos. Lanzada el 24 de marzo, la aplicación se promocionó como un servicio de alerta de emergencias, que proporciona a sus usuarios información crítica por parte del gobierno. Pese a cumplir

con esta función, el análisis realizado por Global Witness de la versión Android de la aplicación, muestra que dicha app también envía la ubicación exacta del usuario a su desarrollador, In-telligent LLC, en intervalos regulares, incluso cuando la aplicación no esté en uso.

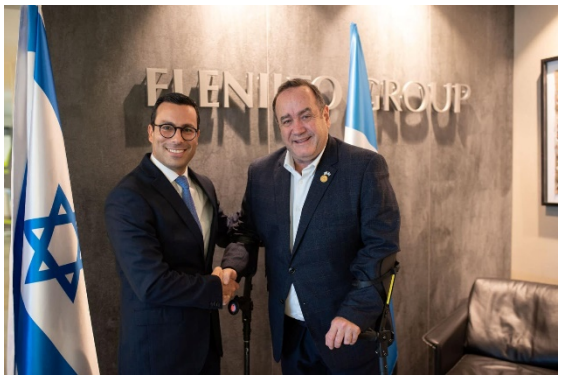
La política de privacidad de In-telligent define vagamente cómo podrían compartirse los datos con terceros, como cuando "la compañía razonablemente crea que es necesario proteger [la] seguridad de In-telligent, de nuestros usuarios u otras personas". También sugiere que In-telligent planea utilizar los datos recopilados por medio de sus aplicaciones para facilitar la publicidad dirigida, aprovechando efectivamente de la crisis del COVID-19 para sacar oportunidades de marketing. Tenlot ya ha usado la aplicación para promocionar sus tarjetas rasca y gana. Los críticos sugieren que existe un riesgo real de que los datos personales, como la ubicación, puedan ser compartidos con el gobierno.

En respuesta a la solicitud de comentarios por parte de Global Witness, el CEO de In-telligent, Allan Sutherland, dijo que la compañía no comparte los datos de la aplicación con el gobierno guatemalteco ni con Tenlot y que la información recopilada es "propiedad de In-telligent y se mantiene ... estrictamente confidencial." Abadi también niega que su empresa o el gobierno guatemalteco tengan acceso a los datos recopilados a través de la aplicación.

Alerta Guate fue eliminada de las tiendas de aplicaciones iOS y Android a mediados de abril, aparentemente después de que algunos blogueros en Guatemala y en el extranjero se dieron cuenta de que la app planteaba unos problemas de privacidad, pero es probable que las versiones de la aplicación ya instaladas en los teléfonos de los usuarios sigan funcionando. Menos de una semana después de su lanzamiento, la televisión guatemalteca informó que Alerta Guate había sido descargada más de 100.000 veces.

AMPLIACIÓN DE ACTIVIDADES?

Mientras las empresas tecnológicas se esfuerzan por producir software que puedan ayudar a los gobiernos a aliviar las medidas de cierre, los grupos de derechos humanos y los activistas de la privacidad han señalado el riesgo de que ocurra una ampliación de actividades. Los respaldos del presidente Giammattei sugieren que Alerta Guate podría tener un grupo más amplio de aplicaciones en el futuro, y una finalidad que vaya más allá de la lucha contra la pandemia actual. El presidente ha dicho explícitamente que espera que la aplicación evolucione para cubrir "problemas de seguridad", sin dar más detalles.



Presidente electo Giammattei visita las oficinas de Tenlot en Tel Aviv, Diciembre 2019 Yossi Abadi/Facebook

Tenlot, que financió la aplicación, parece tener una relación cercana con Giammattei, quien fue fotografiado (arriba) visitando las oficinas de la compañía en Israel como presidente electo en diciembre del año pasado. La permisiva política de privacidad de la aplicación, que permite a su desarrollador retener información personal durante una década, también genera señales de alerta sobre el uso futuro de los datos que recopila.

En los últimos dos meses, ha habido tres diferentes versiones de la política de privacidad de In-telligent, generando preocupación sobre que la política pueda cambiar regularmente en el futuro. En respuesta al lanzamiento de Alerta Guate, el defensor del pueblo de Guatemala urgió al gobierno a restringir el uso de la aplicación al período de crisis actual, describiéndola como " de extremo riesgo para el bienestar de la democracia y de las libertades civiles".

El hecho de que la aplicación y los datos personales que recopila puedan utilizarse para diferentes usos que vayan más allá de la crisis es causa de especial preocupación en Guatemala. En 2018, el periódico Nuestro Diaro publicó evidencia que sugería que el gobierno guatemalteco bajo los predecesores de Giammattei había autorizado una operación de vigilancia cibernética a gran escala contra "empresarios, políticos, periodistas, diplomáticos y líderes sociales". La campaña supuestamente se llevó a cabo utilizando tecnología que incluía el software de pirateo Pegasus de NSO Group, cuya adquisición fue facilitada por un ex traficante de armas y veterano de las fuerzas especiales israelíes.

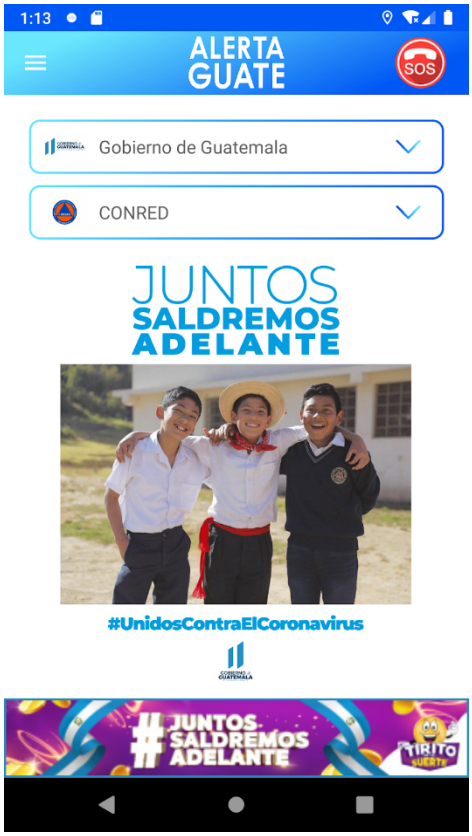
En un país donde los niveles de impunidad del gobierno son altos y los ataques contra los defensores de los derechos humanos están en aumento, hay un mayor riesgo de que la infraestructura de vigilancia se pueda usar para violar los derechos humanos. Según los datos de Global Witness de 2018, 16 activistas ambientales fueron asesinados en el país ese año, convirtiéndolo en uno de los lugares más peligrosos en el mundo para los defensores de la tierra y el medio ambiente.

Giammattei fue elegido en 2019 y asumió el cargo en enero. Tiene un enfoque de gobierno altamente ilitarista y prometió recuperar la pena de muerte a lo largo de su campaña presidencial. Anteriormente fue acusado de ejecuciones extrajudiciales mientras dirigía las cárceles del país; El cargo se retiró más tarde debido a la falta de pruebas, pero las organizaciones locales de la sociedad civil siguen estando preocupadas.

LAS EMPRESAS DETRÁS DE ALERTA GUATE

Alerta Guate fue desarrollada por In-telligent LLC, una empresa de software registrada en Chicago. La empresa produce software de alerta de emergencias listos para usar que se han personalizado para el uso en varios países del mundo. En respuesta a las preguntas formuladas por Global Witness, el CEO de In-telligent dijo que empezó a trabajar con Tenlot en marzo de 2019 y que tenía la intención de producir aplicaciones de alerta para varios "clientes gubernamentales" de Tenlot, entre las cuales Alerta Guate es la primera. In-telligent también declaró que los datos relativos a la ubicación solo se utilizarían para crear publicidad dirigida.

Los banners que publicitaban las tarjetas de lotería de Tenlot eran claramente visibles en la versión Android de la app que Global Witness analizó, lo que generó dudas sobre los motivos por los cuales Tenlot financió el proyecto. En acuerdo con la política de privacidad de In-telligent, los datos pueden compartirse con terceros anunciantes, lo que aumenta la posibilidad de que Tenlot pueda recibir información sobre los usuarios de la aplicación. En su respuesta a Global Witness, el CEO de In-telligent, Allan Sutherland, negó enérgicamente que se compartiera información con dichos anunciantes.



Captura de pantalla de Alerta Guate, 29 Abril 2020

Las conexiones de Tenlot con dos empresas de cibervigilancia y defensa, Cytrox e Inpedio, generan más preocupaciones sobre su posibilidad de acceder a datos personales. La compañía hermana de Tenlot, Elenilto Group, es una empresa de inversión global. Ambas son propiedad del multimillonario israelí Jacob Engel, y el CEO de Tenlot, Yossi Abadi, forma parte del equipo directivo a nivel global de Elenilto. En 2017, Elenilto tomó una participación en Cytrox e Inpedio a través de su Fondo Atooro. Cytrox e Inpedio venden servicios de ciberinteligencia a los gobiernos. Elenilto aún mantiene una participación en Inpedio, pero desde entonces ha vendido su participación en Cytrox.

El brote de COVID-19 representa una nueva oportunidad comercial para las empresas de cibervigilancia. Un reciente informe por Reuters pone en evidencia el riesgo de que las soluciones tecnológicas en respuesta a la pandemia puedan servir como medio para que dichas empresas ganen contratos para ejecutar formas de vigilancia gubernamental más controvertidas. Esto se ilustra con el ejemplo de Intellexa, una alianza de empresas de software espías que incluye Cytrox, y que ahora comercializa "soluciones pandémicas" para los gobiernos. El CEO de Intellexa ha expresado el deseo de "actualizar" los gobiernos a la tecnología de seguridad y espionaje de su compañía en el futuro. La proximidad de Tenlot a las empresas de inteligencia cibernética plantea preguntas similares sobre cómo las conexiones gubernamentales adquiridas a través de las medidas adoptadas en respuesta a la pandemia podrían usarse para vender otras formas de vigilancia.

Tenlot no respondió a las solicitudes de comentarios por parte Global Witness. El CEO de In-telligent negó firmemente que la compañía comparta información con el gobierno guatemalteco y dijo que Tenlot estaba "haciendo una donación muy generosa al pueblo de Guatemala" pagando el desarrollo y el mantenimiento de Alerta Guate.

Dado el potencial para que los gobiernos hagan un mal uso de las infraestructuras técnicas desplegadas para combatir las pandemias, se debe aplicar un nivel de control mucho más alto hacia las empresas que desarrollan estas aplicaciones, particularmente cuando estas empresas estén conectadas, directa o indirectamente, con el negocio de proporcionar inteligencia a los gobiernos en tiempos normales. Todos los datos recopilados deben mantenerse al mínimo necesario, y debe haber límites con respecto a cuánto tiempo se pueden usar los datos para contribuir a contrarrestar el riesgo de ampliación de actividades.

CÓMO INVESTIGAMOS LA APLICACIÓN

Global Witness descargó la versión Android de la aplicación Alerta Guate y la instaló en un emulador, un teléfono Android virtual que se ejecuta en un ordenador portátil, y configuró su ubicación en una sección de una carretera principal en Ciudad de Guatemala. La información enviada por el teléfono a través de Internet se monitoreó luego utilizando un software forense de seguridad cibernética.

Cuando se inició por primera vez, la aplicación solicitó el permiso del usuario para acceder a su ubicación. Una vez otorgado, la app enviaría dicha ubicación regularmente a un servidor controlado por los desarrolladores de la aplicación, incluso cuando la aplicación se cierre o se reinicie el teléfono. El análisis del tráfico de la red nos enseñó que durante una hora el teléfono virtual había enviado su exacta ubicación cinco veces.

Cada vez que el teléfono enviaba su ubicación, la respuesta del servidor mostraba estar vinculado directamente a una cuenta de usuario en una base de datos centralizada. Para nuestro usuario de prueba, solo incluimos el correo electrónico, pero también estaban presentes los campos para el nombre, edad, sexo, código postal e idioma del usuario.

www.globalwitness.org