La controversia de TikTok: su impacto en la seguridad internacional

Gloria Sicilia Lozano | Master en Máster en Estudios de Seguridad de la Universidad de Georgetown, Beca Fullbright.

Tema

El potencial impacto de TikTok en la seguridad occidental ha generado preocupación en relación a la recopilación de datos, el control algorítmico y la posible interferencia por parte del gobierno chino. Aunque ByteDance, la empresa matriz de TikTok, ha propuesto la instalación de centros de datos locales, estas medidas no abordan de manera efectiva los riesgos fundamentales que exponen a la sociedad europea a posibles influencias chinas. Ante este nuevo panorama tecnológico y geopolítico, la UE debe mantenerse firme en la protección de sus ciudadanos y sus intereses.

Resumen

TikTok, la popular aplicación de redes sociales, ha suscitado preocupación debido a su potencial para comprometer la seguridad occidental. Se teme que el gobierno chino pueda utilizar la aplicación para recopilar datos, ejercer control algorítmico e interferir en dispositivos personales. Ante estas preocupaciones, ByteDance ha propuesto almacenar los datos de los usuarios en suelo europeo.

Si bien este proyecto busca crear un cortafuego con China, no aborda las vulnerabilidades clave que exponen a los usuarios de TikTok a posibles interferencias por parte del Partido Comunista Chino (PCCh). Tanto desde una perspectiva tecnológica como legal, el gobierno chino podría seguir teniendo acceso a la información de los usuarios, así como al contenido al que están expuestos. Esta situación podría tener serias implicaciones para la soberanía de los países de la UE.

Hasta la fecha, 12 países han prohibido en su totalidad o parcialmente el uso de esta aplicación. Los principales motivos expuestos han sido el riesgo para la seguridad nacional, el espionaje, la violación de la protección de datos de las administraciones y la privacidad de sus ciudadanos.

TikTok representa una nueva forma de amenaza digital en un contexto de creciente interferencia extranjera, desinformación y tensiones geopolíticas, con la posibilidad de ser utilizada como arma para fines estratégicos. Como establecen la Brújula Estratégica para la Seguridad y Defensa (2022) y la Estrategia de Seguridad Económica Europea (2023), la UE debe adaptarse para hacer frente a las nuevas realidades tecnológicas y geopolíticas. Para ello, es fundamental mantenerse líder en la regulación de protección de datos, defendiendo la privacidad y seguridad de sus Estados miembros.

Análisis

Introducción

El éxito de TikTok y, en consecuencia, su gran alcance, sitúan a la aplicación como pieza clave en la llamada era de la información. TikTok no sólo posee la capacidad de recopilar una cantidad creciente de datos que pueden proporcionar información sumamente útil y generar un valor significativo para entidades y naciones, sino que también cuenta con la habilidad de influir en el contenido al que sus usuarios están expuestos. Del mismo modo, han surgido interrogantes acerca de la capacidad de esta aplicación para comprometer los dispositivos de sus usuarios. Por consiguiente, existe una creciente preocupación sobre el posible uso de TikTok por parte del PCCh. Por un lado, Afganistán, la India y Pakistán han prohibido la aplicación a nivel nacional, mientras que países como Bélgica, Canadá, Dinamarca, EEUU, Francia, Noruega, Nueva Zelanda, Suecia y Taiwán han restringido su uso para funcionarios gubernamentales.

En respuesta a estas preocupaciones, ByteDance, la empresa matriz de TikTok, ha propuesto el establecimiento de centros de datos locales, conocidos como *Proyecto Clover* en Europa y *Proyecto Texas* en EEUU. Estos centros de datos, ubicados en Irlanda y Noruega para el almacenamiento de datos procedentes de Europa, y en Texas para EEUU, tendrán un coste de 1.200 millones y 1.500 millones de euros respectivamente. Además, la compañía de *software* Oracle operará esta infraestructura con el objetivo de añadir una capa adicional de control y mejorar la seguridad.

Sin embargo, estas instalaciones almacenarán exclusivamente los "datos protegidos" legalmente, dejando expuesta el resto de la información de los usuarios. En consecuencia, volúmenes de datos cada vez más elevados podrían continuar siendo recopilados y explotados de acuerdo con los intereses del gobierno chino. La escasa separación entre el sector privado y el PCCh, así como la Ley de Protección de la Información Personal de la República Popular de China (RPC) de 2021, que otorga al gobierno chino acceso a los datos personales y no personales de las empresas nacionales bajo los principios de seguridad nacional, seguirían obligando a ByteDance a responder ante este si fuese requerido, presentando una amenaza significativa para los usuarios de TikTok. Por otro lado, persiste el riesgo de interferencia por parte de la RPC en relación con el contenido al que los usuarios están expuestos, lo que podría influir en su comportamiento. Por ejemplo, ya existen numerosos estudios que recogen el impacto negativo en la salud mental, especialmente en los adolescentes, se han registrado numerosos casos de intoxicaciones, actos de violencia y comportamientos imprudentes como resultado de retos virales y tendencias, y se ha demostrado un incremento en la propagación de discursos de odio, impactando así en la sociedad.

Posicionamiento de EEUU

EEUU, alegando que estas medidas no abordan adecuadamente la potencial amenaza a su integridad nacional, sigue ejerciendo presión sobre ByteDance para que desinvierta en TikTok o se enfrente a una posible prohibición a nivel nacional. Es la segunda vez que TikTok se encuentra ante una amenaza por parte del gobierno federal de prohibir el uso de esta aplicación que cuenta con 113 millones de usuarios estadounidenses. En 2020 el entonces presidente Trump intentó tomar medidas similares, pero sus esfuerzos

fueron bloqueados por los tribunales federales. Sin embargo, en la actualidad, el gobierno cuenta con una cooperación bipartidista en este aspecto y con el consenso de los legisladores estadounidenses, quienes comparten su preocupación acerca de los posibles usos de la aplicación por parte del PCCh. De hecho, en esta ocasión, la Casa Blanca cuenta además con el respaldo del FBI. Christopher Wray, director de esta agencia, ha declarado ante el Comité de Seguridad Nacional de la Cámara de Representantes que el gobierno chino podría utilizar los datos recopilados, y ejercer control sobre el algoritmo de recomendaciones y el *software* de los dispositivos. Asimismo, el director de Ciberseguridad de la Agencia de Seguridad Nacional (NSA), Rob Joyce, ha expresado su preocupación acerca de la capacidad de la aplicación de influir en la sociedad a gran escala. En marzo de 2023 tuvo lugar una audiencia en el Congreso sobre TikTok con la participación del CEO, Show Zi Chew, cuyo testimonio no logró convencer al Comité sobre la seguridad e independencia de la aplicación.

Los críticos más fervientes sostienen que no existen pruebas que respalden la afirmación de que el PCCh haya utilizado TikTok para espiar a sus usuarios. Además, argumentan que una prohibición a nivel nacional constituiría una clara violación de la primera enmienda de la Constitución de EEUU. Cabe mencionar que hay numerosas aplicaciones, como Meta y Google, que también recopilan grandes cantidades de datos, y, en 2013, Edward Snowden expuso la colaboración entre las grandes empresas tecnológicas y el gobierno estadounidense para acceder a información personal de los ciudadanos. Asimismo, señalan que TikTok genera una cantidad excesiva de datos, lo que dificulta su procesamiento. Además, resaltan que la principal preocupación radica en que TikTok es la primera aplicación que no pertenece a Meta en alcanzar una prominencia tan significativa, siendo además de una nación considerada adversaria.

Aunque la aplicación todavía se encuentra lejos de una prohibición nacional, se han presentado numerosas propuestas de ley con el objetivo de dotar al ejecutivo de nuevos poderes para prohibir tecnología extranjera con vínculos a países considerados adversarios que representen una amenaza para la seguridad nacional. La propuesta más significativa ha sido el Acta de Restricción de Amenazas Emergentes que Representan Riesgos para la Tecnología de Información y Comunicaciones (RESTRICT Act), respaldada por un grupo bipartidista de senadores y que ha recibido el apoyo de la Casa Blanca. Esta ley permitiría al Departamento de Comercio revisar cualquier tecnología extranjera que se considere un riesgo para la seguridad nacional. Las reacciones ante esta propuesta han variado desde el apoyo hasta la preocupación por el exceso de poder que esta ley otorgaría al ejecutivo. En cualquier caso, este acontecimiento evidencia una nueva fase de mayor determinación en la política exterior hacia China.

En este sentido, resulta evidente que tanto el partido Demócrata como el Republicano han alineado su postura. Este creciente consenso se debe a que la visión del partido Republicano, que considera a China un claro adversario, cada vez coincide más con la del partido Demócrata que, a pesar de sus divisiones internas, reconoce a China como un competidor y un desafío para el orden internacional. Así lo expuso el secretario de Estado, Antony J. Blinken, en un comunicado del Departamento de Estado en 2022, además de reflejarse en la nueva estrategia del gobierno de Biden denominada “invertir,

alinear y competir", que adopta un tono crecientemente agresivo en los ámbitos económico, militar, diplomático y tecnológico.

No obstante, todavía se desconocen las consecuencias económicas que pueden derivarse de las medidas adoptadas por la Administración Biden, algunas de las cuales son una continuación de las políticas del gobierno anterior. Por un lado, la Fundación de Impuestos estima que el PIB de EEUU se reducirá en 55.700 millones de dólares y se perderán 173,000 puestos de trabajo como resultado de un desacoplamiento de las economías estadounidense y china. Por otro lado, la Casa Blanca ha reiterado, tanto a través de su consejero de Seguridad Nacional, Jake Sullivan, como en el Comunicado del G7 en Hiroshima, que su objetivo es reducir riesgos y diversificar, con el fin de aumentar la seguridad y la resiliencia, apuntando a un desacoplamiento sólo en un conjunto específico de sectores críticos para la seguridad nacional.

Posicionamiento de la UE

En febrero de 2023 la UE siguió los pasos norteamericanos y prohibió así el uso de TikTok, que cuenta con 150 millones de usuarios en Europa, en los dispositivos registrados en los servicios de las instituciones europeas, como la Comisión Europea, el Consejo de la UE, el Parlamento Europeo, el Servicio Europeo de Acción Exterior y el Tribunal de Cuentas Europeo. Esta medida, que se describió como necesaria para la protección de datos aún sin hacer referencia explícita al PCCh, afecta tanto a los dispositivos profesionales como a los personales que alberguen aplicaciones de la UE. Más allá de esto, la UE no ha anunciado ninguna medida adicional que conduzca a una prohibición total de la aplicación.

EEUU ha estado exigiendo a la UE que establezca una estrategia coherente con respecto a China. Mientras algunos Estados miembros y funcionarios de la UE han adoptado una postura más firme contra China, otros se han mantenido neutrales, distanciándose del discurso estadounidense como demostró el presidente de Francia, Emmanuel Macron, en su última visita oficial a la RPC.

No obstante, en los últimos años, la UE ha establecido diversos mecanismos para regular la protección de datos, la desinformación y las amenazas planteadas por las nuevas tecnologías emergentes.

Actualmente, la UE cuenta con un marco regulatorio establecido por el Reglamento General de Protección de Datos (RGPD) adoptado en 2016, que ya prevé normas y mecanismos para abordar el tratamiento de datos de organizaciones tanto dentro como fuera de la UE. Especialmente relevantes para TikTok son los requisitos específicos para usuarios menores de edad –una base importante de sus usuarios– transparencia en el procesamiento de datos, la realización de una Evaluación de Impacto de Protección de Datos (EIPD) y requisitos estrictos en el caso de transferencias internacionales de datos europeos. El RGDP exige transparencia acerca de los tipos de datos recopilados, la finalidad del procesamiento, los destinatarios de los datos y cualquier transferencia internacional de datos que pueda tener lugar, exigiendo que los países receptores ofrezcan un nivel adecuado de protección o que se implementen salvaguardias adecuadas.

La Ley de Servicios Digitales (DSA) publicada en 2022 tiene como objetivo garantizar un espacio digital seguro y establece la realización de evaluaciones anuales de riesgos para plataformas de gran tamaño, que superen los 45 millones de usuarios como es el caso de TikTok. En abril de 2023 la UE publicó bajo la DSA una lista con 19 plataformas digitales, incluyendo TikTok, que deben someterse a mayores controles y auditorías anuales a partir de agosto de este año cuando la ley entre en vigor.

Además, el Código de Buenas Prácticas sobre Desinformación de la UE de 2022 busca actuar como herramienta para combatir la desinformación y establecer estándares, incluyendo 44 compromisos y 128 medidas específicas. TikTok ha sido acusada de bloquear contenido sobre derechos humanos en China –campos de internamiento de Xinjiang, genocidio uigur... – y su motor de búsqueda de difundir reiteradamente información errónea, según un informe publicado por NewsGuard en 2022, lo que va en contra de las prácticas establecidas en este código.

En mayo de 2023 se mantuvo la cuarta reunión ministerial del Consejo de Comercio y Tecnología UE-EEUU (TTC), cuya atención se centró en la regulación de las tecnologías emergentes, la defensa de los derechos humanos y los valores democráticos en un entorno digital cambiante. De esta manera, el TTC ha dedicado secciones específicas a resaltar la importancia de plataformas digitales transparentes y responsables, con un foco en la protección de menores, y la amenaza que supone la Manipulación de la información e injerencia por parte de agentes extranjeros (FIMI) para los principios europeos. La UE y EEUU buscan así avanzar hacia la creación de una estructura común para la identificación y respuesta de FIMI.

Por último, la Estrategia de Seguridad Económica Europea, presentada en junio de 2023, busca reforzar la seguridad económica de la UE frente a los nuevos desafíos geopolíticos y tecnológicos. Esta estrategia incluye medidas para proteger la infraestructura crítica (física y ciber), tecnologías de doble uso, evitar la coerción económica por parte de terceros países y fortalecer la Capacidad Única de Análisis de Inteligencia (SIAC) de la UE para la detección de amenazas. Asimismo, se está desarrollando la plataforma STEP para la prevención de dependencias estratégicas en el ámbito tecnológico.

Recomendaciones

Ante una creciente tensión del panorama político, la UE se encuentra recalibrando su postura con respecto a China. A pesar de las discrepancias todavía existentes entre los Estados miembros, es posible observar, a la luz de las últimas actuaciones de la UE, una mayor unidad y cohesión su estrategia en materia de política exterior y de seguridad común. Las diferencias en cuanto a cómo abordar al PCCh parecen radicar en matices, como afirmó el alto representante de la UE, Josep Borrell, lo que permite una actualización de su política al respecto. Por un lado, la UE publicó la Brújula Estratégica para la Seguridad y Defensa en marzo de 2022, en la que se califica a China como un "socio para la cooperación, competidor económico y rival sistémico", reconociendo así el potencial de China para desestabilizar el orden internacional, nuestros intereses y nuestros valores. Por otro lado, las medidas adoptadas por la UE en los últimos años, enumeradas en el apartado anterior, se dirigen hacia Rusia y China, aunque no se

mencionen explícitamente, según lo señalado por la presidenta de la Comisión Europea, Ursula von der Leyen.

En lo que respecta a TikTok y no obstante el proyecto Clover, es fundamental que se haga cumplir nuestra legislación. Para mitigar los riegos asociados con la penetración de nuevas tecnologías, especialmente las provenientes de rivales sistémicos, la UE debería seguir tres líneas principales de acción.

En primer lugar, es necesaria la realización de un análisis exhaustivo de la aplicación y sus posibles puertas traseras. Este análisis debería ser realizado por una institución pública o privada de reconocido prestigio e independencia que incluya un informe desclasificado que serviría como herramienta de negociación con ByteDance. Además, un informe concluyente permitiría al Comité Europeo de Protección de Datos (CEPD) evaluar si TikTok cumple con el RGPD y la DSA, así como con los principios establecidos en los documentos estratégicos publicados el año en curso y el año anterior. Es importante aplicar estas medidas para garantizar que TikTok cumpla con los estándares de seguridad y protección de los usuarios. Además, se pueden considerar medidas adicionales, como auditorías periódicas o mecanismos de supervisión más estrictos, para asegurar el cumplimiento continuo de las normas, y si fuese necesario explorar posibles actualizaciones o enmiendas para abordar específicamente los desafíos planteados por TikTok y otras aplicaciones similares.

En segundo lugar, sería necesario, aunque sea reiterativo, que TikTok firmase con las autoridades de la UE el reconocimiento de que la legislación europea prevalezca para los ciudadanos y las instituciones europeas sobre cualquier otro compromiso firmado por TikTok, incluidos los firmados con el gobierno de China; y que en ningún caso transmitirá los datos protegidos o no protegidos de ciudadanos europeos a terceros.

En tercer lugar, dado el potencial impacto en la seguridad occidental, se recomienda que la UE establezca colaboraciones con agencias de inteligencia y seguridad para obtener información y asesoramiento sobre posibles amenazas relacionadas con TikTok en este ámbito. Estas agencias, como Europol, la Agencia de la Unión Europea para la Ciberseguridad (ENISA) y el Centro de Inteligencia y de Situación de la UE (EU INTCEN), podrían tener un papel más importante y decisivo en la monitorización de las actividades de TikTok y la identificación de posibles riesgos.

Conclusiones

La UE debe ser plenamente consciente de su actual dependencia de EEUU y China, dado que todas las principales empresas tecnológicas tienen su sede en estos países. Europa, debido a su destacado peso económico, demográfico y tecnológico-industrial, se encuentra en una situación crítica en la que es imperativo que pueda contar en su territorio con líderes tecnológicos globales, aunque sea a costa de atemperar sus políticas de competencia que hasta la fecha han primado, impidiendo el desarrollo y asentamiento de este tipo de empresas líderes. Por el contrario, la UE debería fomentar la diversificación y aumentar el apoyo a empresas europeas siendo estas alternativas más seguras en consonancia con su estrategia. Ignorar esta necesidad supondría descuidar nuestro propio futuro y caer en la irrelevancia. Por tanto, resulta de vital

importancia que la UE adopte medidas concretas para promover y atraer la instalación de alguna de estas empresas en su territorio, lo que contribuirá a su crecimiento y a la consecución de una autonomía tecnológica sólida en el escenario global, además de reducir la dependencia de plataformas extranjeras y mitigar así los riesgos asociados.