ARI 40/2019
9 de abril de 2019

El papel del sector privado en la lucha contra la desinformación

Carlos Galán Cordero | Abogado especialista en derecho TIC, Máster en Relaciones Internacionales y Comunicación.

Tema

Los Gobiernos precisan de la colaboración de los actores privados para proteger las infraestructuras críticas y los servicios públicos esenciales, pero, sobre todo, para hacer frente a la desinformación.

Resumen

El secretario de Estado director del Centro Nacional de Inteligencia, Félix Sanz, en su comparecencia ante la Comisión Mixta de Seguridad Nacional de febrero de 2019, diferenció la capacidad gubernamental para garantizar la seguridad informática de las elecciones de 2019 y las dificultades para hacer lo mismo con las fake news o acciones de influencia. Estas acciones se llevan a cabo a través del ciberespacio, pero se dirigen hacia la opinión pública para condicionar sus reacciones. Para incrementar la resiliencia de las sociedades, los Gobiernos llevan a cabo campañas de sensibilización dirigidas a los ciudadanos y de colaboración con las compañías que proporcionan servicios digitales para moderar el impacto de la desinformación. Este ARI analiza el papel que puede desempeñar el sector privado –muy especialmente, las redes sociales– en el esfuerzo para combatir las campañas de desinformación y cómo este esfuerzo debería reflejarse en la nueva Estrategia de Ciberseguridad Nacional, actualmente en proceso de redacción.

Análisis

Tras la mencionada comparecencia del director del Centro Nacional de Inteligencia[1], el Centro Criptológico Nacional, dependiente del anterior, publicó un informe de buenas prácticas sobre "Desinformación en el ciberespacio" en el que alertaba de que cerca del 90% de la población española de entre 16 y 65 años puede ser víctima de un ataque de desinformación[2]. En marzo se hizo público el Informe Anual de Seguridad Nacional[3], del Departamento de Seguridad Nacional, órgano adscrito al Gabinete de la Presidencia del Gobierno, que señaló un año más las campañas de desinformación como uno de los

[1] Diario de Sesiones 131, de 14 de febrero de 2019, p. 20, http://www.congreso.es/public_oficiales/L12/CORT/DS/CM/DSCG-12-CM-131.PDF.

[2] Informe de Buenas Prácticas BP/13 Desinformación en el ciberespacio, febrero de 2019, p. 9, https://www.ccn-cert.cni.es/comunicacion-eventos/comunicados-ccn-cert/7680-como-actuar-frente-a-las-campanas-de-desinformacion-en-el-ciberespacio-uno-de-los-mayores-retos-de-seguridad-del-pais.html.

[3] Informe Anual de Seguridad Nacional 2018, https://www.dsn.gob.es/documento/informe-anual-seguridad-nacional-2018.

peligros y amenazas más significativos para la seguridad de nuestro país. Este informe, haciendo referencia a la Estrategia de Seguridad Nacional de 2017, reconoce las denominadas *fake news* y la desinformación como un problema de ciberseguridad, aunque diferenciándolo de aquellas actividades maliciosas que tienen como objetivo manipular redes y sistemas de información.

Empecemos definiendo el objeto de estudio. Hemos de entender como *campaña de desinformación* todo aquel contenido falso o no completamente cierto divulgado a través de medios de comunicación y, especialmente, redes sociales y creado y distribuido con la finalidad de dañar la reputación de una persona, colectivo o institución o de influir en la opinión pública.

Mucho se ha hablado del papel que pueden desempeñar las organizaciones del sector privado como elementos activos de colaboración con las entidades públicas en la lucha contra las ciberamenazas, muy especialmente respecto a los ataques de denegación de servicio o la protección de infraestructuras, entre otros. Sin embargo, no se ha mencionado apenas el papel que podrían tener esas mismas empresas del sector privado a hora de combatir las campañas de desinformación, sobre todo las plataformas digitales y empresas de comunicación que utilizan las redes sociales para combatir las campañas de desinformación (el informe del CNI también incluye a la comunidad académica para investigar el fenómeno y sus efectos). Esta colaboración debería reflejarse en la nueva Estrategia de Ciberseguridad Nacional, actualmente en proceso de redacción.

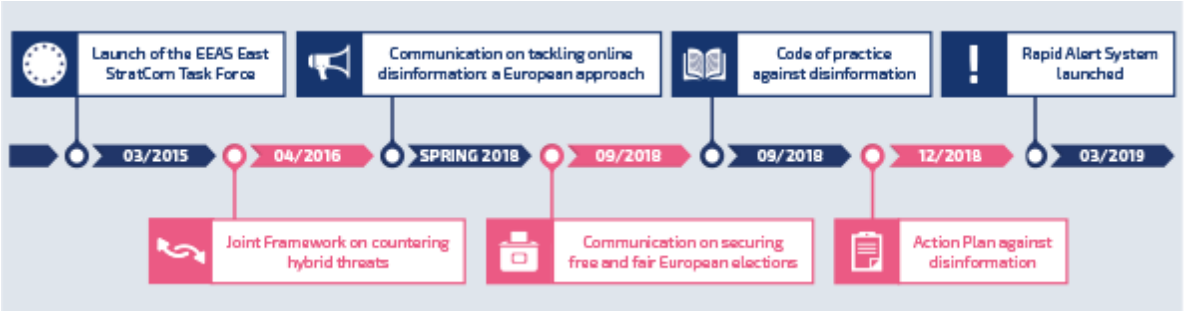
Las medidas gubernamentales

El Gobierno español no es el primero en alertar sobre los riesgos de la desinformación. Como muchos otros Gobiernos europeos, ha seguido las recomendaciones de la Unión Europea para prevenir los efectos de la desinformación y la propaganda[4]. Como refleja la Figura 1, la Comisión Europea ha tenido que evaluar el impacto de las campañas de desinformación sobre las elecciones y la estabilidad de los Estados miembros antes de elaborar las comunicaciones, códigos de conducta y planes de actuación contra ellas. Las medidas se dirigían a los Estados para que establezcan mecanismos y responsables de intercambio de información, a los expertos para que investiguen y desarrollen tecnologías de detección y a todos ellos para que creen mecanismos de alerta temprana, según el Plan de Acción contra la Desinformación de 2018[5].

[4] Informe del Parlamento Europeo 608.864, sobre desinformación y propaganda en la UE y sus Estados miembros, febrero de 2019, http://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU(2019)608864_EN.pdf.

[5] Action Plan Against Disinformation JOIN (2018), de 5 de diciembre, https://eeas.europa.eu/sites/eeas/files/action_plan_against_disinformation.pdf.

Figura 1. Cronograma de la movilización europea contra la desinformación



Fuente: EUvsDisinfo, diciembre de 2018, https://eeas.europa.eu/headquarters/headquarters-homepage/54831/action-plan-against-disinformation_en.

De acuerdo con el Plan, la Comisión Europea anunció este pasado marzo de 2019 la creación de la plataforma tecnológica Rapid Alert System para reaccionar inmediatamente ante campañas de desinformación mediante una vigilancia permanente (24/7) de los contenidos publicados a través de los medios de comunicación y las redes sociales y favoreciendo el intercambio de información, así como una respuesta o solución coordinada a los bulos.

La respuesta del Gobierno español debe ser proporcional al nivel de preocupación social. Según el Eurobarómetro Flash de abril de 2018, los españoles son los que menos confían en las noticias por televisión (57% frente al 86% de los primeros, Suecia y Países Bajos). También son los que más noticias falsas encuentran a diario (78% frente al 53% de Estonia y Malta, los que menos) y los menos confiados en poder detectarlas (55% frente al 87% de Dinamarca)[6].

En diciembre de 2017, tras la aprobación de la nueva Estrategia de Seguridad Nacional y la constatación de acciones de desinformación en Cataluña, el Gobierno anunció la creación de un centro de operaciones que protegería de los ciberataques a la Administración General del Estado y de la desinformación al conjunto de la sociedad. La preocupación continuó en los meses posteriores, pero hasta marzo de 2019 no se creó una unidad especializada en la desinformación dentro de las medidas de ciberseguridad adoptadas para proteger los procesos electorales nacionales, regionales y europeos en ciernes[7]. La unidad se coordina desde la Secretaría de Estado de Comunicación, apoyada por un grupo de expertos del Departamento de Seguridad Nacional y de otras agencias de ciberseguridad.

En julio de 2018, el Consejo de Seguridad Nacional acordó el procedimiento para la elaboración de un nuevo marco que sustituirá a la todavía vigente Estrategia de Ciberseguridad Nacional de 2013, que, pese a contemplar la necesidad de involucrar al sector privado en la lucha contra las ciberamenazas, no incluía el tratamiento de las *fake news*, puesto que en aquel momento las campañas de desinformación no constituían

[6] "Flash Eurobarometer 464: Fake News and Disinformation Online", abril de 2018, pp. 6-12, http://data.europa.eu/euodp/en/data/dataset/S2183_464_ENG.

[7] Lucía Abellán (2019), "El Gobierno activa una unidad contra la desinformación ante las elecciones", *El País*, 11/3/2019, https://elpais.com/politica/2019/03/10/actualidad/1552243571_703630.html.

un riesgo consolidado. Por el contrario, en la actualidad, la nueva Estrategia de Ciberseguridad Nacional debería señalar el papel del sector privado y asentar las bases de actuación a la hora de combatir este nuevo tipo de amenazas, sin limitar el conjunto de acciones a aquellas que pueda desarrollar aisladamente el sector público en un escenario —tantas veces señalado— de incapacidad de las instituciones públicas para lograr y mantener el talento en el ámbito de las nuevas tecnologías, lo que también viene a alentar una colaboración más estrecha con el sector privado, más ágil en esta pretensión.

La cooperación privada

Las medidas adoptadas por la Comisión preveían la movilización del sector privado para poner en práctica el Código de Conducta (*Code of Practice on Disinformation*), conseguir la cooperación de la sociedad civil en la detección de las acciones de desinformación, apoyar a quienes verifican la veracidad de los hechos (*fact-checkers*) y conseguir la participación de las grandes compañías, como Google, Twitter, Facebook o Mozilla, que suscribieron el Código de Conducta propuesto por la Comisión.

El propósito del Código de Conducta es identificar las acciones que, de forma constante, han de poner en marcha estas compañías para combatir las *fake news*, incluyendo la publicación de un informe periódico en relación con las medidas de seguridad adoptadas y los recursos empleados para garantizar, entre otras cosas, la transparencia de la publicidad política. Facebook, a raíz de adoptar el código, anunció el pasado 28 de marzo que bloqueará los anuncios electorales de páginas no autorizadas, de forma que todos los partidos políticos que deseen hacer cualquier clase de anuncio electoral en la plataforma (y en Instagram) deberán registrarse y acreditarse con la herramienta facilitada a tal fin, una herramienta ya utilizada en Brasil y Estados Unidos. La participación de estas compañías en la lucha contra las noticias falsas que circulan por las redes sociales revela su responsabilidad y compromiso con la lucha frente a la desinformación al reconocer este problema como uno de los desafíos más importantes para Europa[8].

Algunos países, como Alemania y Francia, han desarrollado leyes específicas para luchar contra la desinformación[9], pero en España el Informe de Buenas Prácticas mencionado recuerda a las empresas privadas su obligación de evitar que se utilicen sus plataformas digitales en acciones de influencia contra los ciudadanos, las instituciones y los Gobiernos y pide a la comunidad tecnológica e industrial que desarrollen metodologías de prevención. Para los ciudadanos, el informe ofrece un decálogo con medidas de concienciación como desconfiar de las noticias que circulan, verificar sus fuentes o tomar precauciones para no facilitar el proceso de desinformación.

[8] Las medidas puestas en marcha por las compañías privadas se recogen en el Anexo de Buenas Prácticas al Código de Conducta.

[9] Ley de Supervisión de las Redes alemana de octubre de 2017 y Ley contra la Manipulación de la Información francesa de diciembre de 2018.

Lo anterior justifica la necesidad de que la nueva Estrategia de Ciberseguridad Nacional no deba limitarse a señalar la importancia de la colaboración público-privada para combatir las campañas de desinformación, sino además exigir responsabilidades y constituir el marco de actuación de aquellos sectores industriales y organizaciones que juegan un papel esencial en la defensa de nuestra democracia, todo ello desde una perspectiva más proactiva e inclusiva. Este marco debería dar lugar al establecimiento de las bases legales que favorecerían la cohesión normativa a nivel nacional y comunitario y la coordinación entre los sectores público y privado.

Es por todo ello por lo que esta nueva Estrategia debería establecer ciertas obligaciones para entidades grandes, como Facebook o Twitter, y fomentar ejercicios y simulaciones a nivel nacional en materia de ciberdefensa frente a la desinformación en el sector privado, así como la creación y compartición de capacidades y herramientas adecuadas para integrar e interconectar satisfactoriamente los datos que aquellas entidades puedan generar con las instituciones de referencia en España en materia de ciberseguridad, como el Instituto Nacional de Ciberseguridad (Incibe) o el Centro Criptológico Nacional (CCN), entre otros. También se debería fomentar la colaboración público-privada para la investigación y desarrollo de tecnologías capaces de contrarrestar la desinformación aprovechando los futuros programas del Horizonte Europa que apoyan el I+D+i de las empresas, especialmente de las pequeñas y medianas (pymes).

Esas nuevas bases legales deberían no sólo exigir nuevas obligaciones a las grandes empresas aludidas, sino favorecer con incentivos a aquellas empresas que colaboraran activamente en la lucha contra estas amenazas, tomando como ejemplo el documento informativo del Tribunal de Cuentas Europeo de marzo de 2019 sobre “Desafíos de una política eficaz de ciberseguridad en la UE”, en el que los poderes públicos asumen la financiación de determinadas líneas de investigación tecnológica y exigen la adopción de ciertas normas o estándares técnicos para proceder a la contratación pública, como el protocolo IPv6 para contribuir a la lucha contra la ciberdelincuencia[10].

Aunque esta plataforma supone un importante avance en la protección frente a la desinformación, sería conveniente desarrollar una plataforma semejante a nivel nacional en la que, al margen de las instituciones públicas correspondientes, se integraran aquellas entidades privadas cuya presencia se considerara conveniente. Involucrar en esa identificación al sector privado es un elemento esencial; integrar a la empresa que constituye el origen o el medio de difusión de la noticia se configura como elemento indispensable para asegurar un tratamiento eficaz de las campañas de desinformación.

Por último, en relación con el papel que deberían jugar las empresas del sector privado en esta nueva Estrategia de Ciberseguridad Nacional, no se debería olvidar a las organizaciones de *fact-checking* político, aquellas organizaciones de ámbito periodístico que persiguen detectar falsedades, errores o contradicciones en las noticias cuyo contenido se refiere a figuras o instituciones políticas. En España, como señala el Informe del Centro Criptológico Nacional, existen algunos organismos, medios de

[10] “Desafíos de una política eficaz de ciberseguridad en la UE”, marzo de 2019, https://www.eca.europa.eu/es/Pages/DocItem.aspx?did=49416.

comunicación y portales web que confirman o desmienten datos, como Maldito Bulo –miembro del grupo de expertos de Alto Nivel de la Comisión Europea–, BSDetector, Snopes o FactCheck, entre otras. Estas organizaciones no han tenido mucha trascendencia, no así en otros países, como Estados Unidos, donde gozan de mayor repercusión y relevancia pública (por ejemplo, Politifact). El establecimiento de un canal de comunicación rápido y eficiente entre las empresas de *fact-checking* y las respectivas redes sociales resulta imprescindible para combatir de manera adecuada las campañas de desinformación.

Conclusiones

De todo lo anterior podemos extraer las siguientes conclusiones. En primer lugar, aunque las denominadas *fake news* puedan usar el ciberespacio como canal de difusión, no conviene identificar desinformación con ciberataques que tienen por objeto los sistemas y redes de información. Aunque en algún caso puedan perseguir propósitos similares (crear confusión, desestabilizar, alterar el normal funcionamiento de las organizaciones o de la sociedad, en definitiva), responden a vectores de ataque distintos que no pueden abordarse con las mismas herramientas.

Uno de los instrumentos más significativos en la propagación de campañas de desinformación son las redes sociales, que acaparan la atención prioritaria de una parte importante de la población, especialmente de los más jóvenes, para los que constituyen, en buena medida, el medio más importante para la recepción de información. Por ello son las propias redes sociales las que deben incrementar sus esfuerzos para eliminar o minimizar la presencia de noticias falsas en sus plataformas, sobre todo cuando se trate de informaciones que, por su relevancia pública, puedan causar un impacto significativo en la sociedad.

Para ello, siguiendo el camino emprendido por las instituciones europeas, los Gobiernos nacionales deben impulsar la creación y adhesión a códigos de conducta de aquellos proveedores de servicios digitales de amplia penetración en el mercado. También deben impulsar, de manera rotunda y decidida, campañas de sensibilización para los ciudadanos respecto al fenómeno de las campañas de desinformación y sus características que estimulen el espíritu crítico de los destinatarios de las noticias y fomenten una cultura de respeto por la información veraz. Los Gobiernos, además, están en la obligación de fomentar la colaboración público-privada para la investigación y desarrollo de tecnologías capaces de contrarrestar la desinformación, aprovechando los futuros programas del Horizonte Europa que apoyan el I+D+i de las empresas, especialmente de las pequeñas y medianas (pymes).

Puesto que la mayor parte de las campañas de desinformación se desarrollan en el ciberespacio, parece necesario que la nueva Estrategia de Ciberseguridad Nacional contemple entre sus previsiones acciones específicas para luchar contra esta nueva amenaza. Estas acciones habrán de pasar, entre otras, por reforzar el papel de los órganos creados al efecto y profundizar en la necesaria colaboración público-privada.