Por unas elecciones libres y justas al Parlamento Europeo (y nacionales)

Félix Arteaga | Investigador principal, Real Instituto Elcano | @rielcano

La Comisión Europea continúa preocupada por el efecto de los ciberataques y la desinformación sobre las elecciones en los países miembros y, en particular, por las que tendrán lugar en mayo de 2019 al Parlamento Europeo. Por si no fueran suficientes los precedentes de la interferencia rusa en las elecciones de Estados Unidos de 2016 y el miedo a su repetición en las de Países Bajos y Francia, las últimas revelaciones sobre Facebook/Cambridge Analytica muestran la vulnerabilidad de los procesos y datos electorales en las sociedades democráticas. Según el Flash Eurobarometer 464, de abril de 2018, dedicado a las noticias falsas y a la desinformación, el 85% de los europeos encuestados cree que las dos anteriores son un problema en su país (el 83%, que son un problema para la democracia en general). Consideran que las informaciones en línea son menos fiables que los medios de comunicación tradicionales (el 70% se fía de la radio, el 66% de la televisión y el 63% de los periódicos, mientras que baja al 47% en los medios digitales y al 26% en las redes sociales).

En consecuencia, la Comisión ha adoptado un conjunto de iniciativas de las que *CIBER elcano* viene informando puntualmente, incluida la actualización de Javier Alonso Lecuit en este número de noviembre de 2018, que tratan de fortalecer la resiliencia europea frente a los ciberataques y la mejor protección de los datos personales de los ciudadanos. Para asegurar, en la medida de lo posible, unas elecciones libres y justas en mayo de 2019, la Comisión ha elaborado en septiembre de 2018 una recomendación sobre las redes de cooperación electoral, la trasparencia en línea y la protección contra ciberataques y desinformación. La recomendación emplaza a los Estados miembros para adoptar medidas de protección adecuadas, estar alertas y participar en las redes de cooperación electoral, supervisar la trasparencia de la propaganda electoral en línea y sancionar los incumplimientos.

La **protección de los datos** personales de los electores es otro objetivo de la Comisión. El Reglamento General de Protección de Datos, que entró en vigor en mayo de 2018, ya incluyó normas que debían tener en cuenta los Estados miembros, los partidos políticos, las empresas dedicadas al análisis de datos, las autoridades nacionales y las plataformas de redes sociales. No se podrán utilizar datos personales cedidos para fines no electorales, se impedirá el acceso de personal no autorizado a los datos, se informará a las personas que den sus datos sobre los fines del análisis y no se podrán trasferir datos sin el consentimiento expreso de los electores.

La **desinformación** es otro elemento perturbador de la trasparencia electoral, aunque sus efectos no se limitan únicamente a los procesos electorales. En mayo de 2018, la Comisión convocó a un grupo amplio de representantes de las plataformas en línea, empresas de publicidad y expertos para elaborar un Código de Prácticas sobre

Desinformación que se acaba de publicar en septiembre de 2018[1]. El código no se ha diseñado para proteger específicamente las elecciones, aunque la experiencia europea muestra cómo se han utilizado estas para desarrollar campañas de desinformación. Las partes se comprometen a clausurar sitios web y cuentas desde las que se desinforme, sean falsas o utilicen bots y a fomentar la trasparencia permitiendo la denuncia de los ciudadanos, facilitando el acceso a datos de las plataformas para investigar y ofreciendo más información sobre la propaganda electoral en línea.

Las iniciativas de la Comisión y el Parlamento deberían servir de referencia para la adopción de medidas de ciberseguridad en las **elecciones españolas**, pero no agotan todas las medidas posibles. Por un lado, España deberá tener en cuenta las recomendaciones mencionadas para aplicarlas a su ámbito nacional. Son medidas técnicas y legislativas que refuerzan la protección y resiliencia de los sistemas electorales, pero que no solucionan todas las vulnerabilidades detectadas. En consecuencia, el Gobierno debería poner en marcha medidas de **concienciación** política y social que reduzcan el impacto potencial de los ciberataques y la desinformación sobre las elecciones, medidas que ni la Comisión ni el Parlamento Europeo pueden tomar por nosotros, porque tienen que diseñarse a medida de cada sociedad, de sus sistemas electorales y de su experiencia democrática. En particular, se echa en falta alguna campaña de concienciación similar a las que se han observado en Estados Unidos de cara a las elecciones de noviembre de 2018 o en la UE respecto a las de mayo de 2019.

A pesar del *revuelo* causado por el fenómeno de la desinformación y los ciberataques desde 2017, del que se han hecho eco todas las comparecencias de los últimos meses ante la Comisión Mixta de Seguridad Nacional, la respuesta gubernamental se ha limitado a asignar la lucha contra la desinformación y la ciberpropaganda al Centro de Operaciones de Seguridad del Centro Criptológico Nacional (CCN-CERT). Una asignación, no obstante, que sigue pendiente de respaldo presupuestario y, sobre todo, de una estrategia de comunicación que ayude a la concienciación ciudadana. No se trata de exagerar el riesgo (no está probado en qué medida la desinformación influye en la decisión de voto) ni de minusvalorarlo (la desconfianza señalada sobre las redes sociales y los medios digitales así lo revela), pero los ciudadanos tienen que estar responsablemente prevenidos por sus autoridades. Es probable que la futura **Estrategia Nacional de Ciberseguridad** que se está elaborando incluya medidas al respecto, pero probablemente no llegarán a tiempo para las elecciones autonómicas andaluzas de diciembre de 2018 o las municipales y autonómicas de 2019.

[1] La Comisión entiende por desinformación la "información verificablemente falsa o engañosa que se crea, presenta y divulga con fines lucrativos o para engañar deliberadamente a la población, y que puede causar un perjuicio público. El perjuicio público comprende amenazas contra los procesos democráticos políticos y de elaboración de políticas, así como contra los bienes públicos, como la protección de la salud, el medio ambiente o la seguridad de los ciudadanos de la UE. La desinformación no incluye los errores de información, la sátira y la parodia ni las noticias y los comentarios claramente identificados como partidistas". Comunicación de la Comisión COM(2018) 236, de 26 de abril: "La lucha contra la desinformación en línea: un enfoque europeo".