TECNOLOGÍA, DATOS Y ELECCIONES:
Una lista del ciclo electoral

Junio de 2019

privacyinternational.org

ABOUT PRIVACY INTERNATIONAL

Governments and corporations are using technology to exploit us. Their abuses of power threaten our freedoms and the very things that make us human. That’s why Privacy International campaigns for the progress we all deserve. We’re here to protect democracy, defend people’s dignity, and demand accountability from the powerful institutions who breach public trust. After all, privacy is precious to every one of us, whether you’re seeking asylum, fighting corruption, or searching for health advice.

So, join our global movement today and fight for what really matters: our freedom to be human.

Privacy International
62 Britton Street, London EC1M 5UY, United Kingdom
Phone +44 (0)20 3422 4321
privacyinternational.org

Privacy International is a registered charity (1147471), and a company limited by guarantee registered in England and Wales (04354366).

Tecnología, datos y elecciones: Una “lista” del ciclo electoral

Junio de 2019

Tabla de contenido

Introducción

Cada vez más, la participación democrática es mediada por la tecnología digital. Ya sea a través del uso de las plataformas de redes sociales para hacer campaña política, el registro biométrico de los votantes, el voto electrónico, el uso del reconocimiento facial y otros métodos de vigilancia para el monitoreo policial de mitines, la tecnología ya es parte del proceso político.

Como señala el Manual de Observación Electoral de la Unión Europea:

“El rápido desarrollo de las tecnologías de la información y la comunicación (TIC) también ha influido en las elecciones, ofreciendo nuevas compromisos y retos tanto a administradores electorales como a votantes y observadores. Las TIC están cambiando no solo la manera en la que se gestionan aspectos clave de los procesos electorales —como la elaboración del censo electoral y los procedimientos de voto— sino también el entorno democrático en su conjunto en un contexto en el que los medios de comunicación digitales brindan nuevas oportunidades para el intercambio de opiniones e información entre las personas.” [1]

El funcionamiento de estas tecnologías se basa en la recolección, el almacenamiento y el análisis de datos personales.[2] Gran parte de los debates recientes en torno a las elecciones se enfocan en el contenido de las comunicaciones digitales, como, por ejemplo, las “noticias falsas” y la desinformación. Pero el sistema oculto para la explotación de datos del que dependen muchas de estas tecnologías también entraña graves amenazas para la celebración de elecciones libres y limpias.

En las elecciones democráticas, los partidos políticos y quienes hacen campaña utilizan estas tecnologías —basadas en datos personales— para llegar a los posibles votantes. Además, los organismos de administración electoral (OAE) de todo el mundo dependen cada vez más del registro de datos biométricos.

Del mismo modo, depender de tecnologías digitales en todos los aspectos de las campañas y los procesos electorales hace que las elecciones sean más vulnerables a los ciberataques. La consecuencia más significativa de la digitalización es que las medidas adoptadas para proteger contra ataques cibernéticos deben considerarse para todas las fases de las campañas y los procesos electorales, desde la creación del padrón electoral hasta el voto electrónico, desde las bases de datos de votantes y partidarios que manejan los partidos políticos hasta los datos

[1] Ver https://eeas.europa.eu/sites/eeas/files/handbook_for_eu_eom_2016.pdf
[2] Ver https://privacyinternational.org/topics/data-and-elections

recopilados y utilizados por otros actores tales como las plataformas de redes sociales, los corredores de datos o data brokers y el sector de la tecnología de publicidad.[3]

Ante este panorama, es cada vez más fuerte el llamado a los observadores electorales internacionales para que consideren el papel de los datos personales y las tecnologías digitales que emplean todos los actores principales de las elecciones democráticas. No es una tarea fácil. Demandará la actualización de las metodologías que hoy día utilizan los observadores electorales y el aprendizaje de nuevas competencias técnicas.

A pesar de estos retos, Privacy International considera que los observadores electorales internacionales están bien situados para enfrentarlos y pueden, además, desempeñar un papel importante a la hora de asegurar que los datos personales y las tecnologías digitales se usen para apoyar, y no para debilitar, la participación en los procesos democráticos y la celebración de elecciones libres y justas.

En las secciones que siguen, Privacy International identifica las principales áreas en las que la tecnología y el tratamiento de datos personales desempeñan un papel clave en el proceso electoral. La información se organiza de acuerdo con las metodologías desarrolladas por las organizaciones de observadores electorales.[4] Cada sección ofrece una breve descripción del asunto en juego, recomendaciones de políticas y preguntas claves que los observadores podrían utilizar para evaluar si el marco nacional es adecuado para salvaguardar contra la explotación de los datos en el proceso electoral.

La primera parte abarca el marco jurídico general y las normas relevantes relacionadas con la administración de las elecciones (el registro de votantes, la votación y el papel del Organismo de Administración Electoral). La segunda parte examina la regulación de los partidos políticos y otros actores políticos (incluidos el financiamiento y las campañas políticas). La tercera parte se enfoca en el rol de la empresa privada, especialmente las plataformas de redes sociales, en el contexto de las elecciones (con énfasis particular en la transparencia en la publicidad política).

[3] Ver Stiftung Neue Verantwortung, Securing Democracy in Cyberspace - An Approach to Protecting Data-Driven Elections, octubre de 2018, https://www.stiftung- nv.de/sites/default/files/securing_democracy_in_cyberspace.pdf

[4] Ver Promoting Legal Frameworks for Democratic Elections (https://www.ndi.org/sites/default/files/2404_ww_elect_legalframeworks_093008.pdf); Tercera edición de Handbook for European Union Election Observation (https://eeas.europa.eu/sites/eeas/files/handbook_for_eu_eom_2016.pdf); OSCE/ODIHR manual de observación electoral (6ª edición, https://www.osce.org/odihr/elections/68439?download=true)

Parte 1 — Administración de elecciones

1.1 Marco jurídico — protección del derecho a la privacidad

El derecho a la privacidad (Artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, PIDCP) es un derecho humano fundamental que cada día cobra mayor importancia y relevancia en el contexto de las elecciones.

La protección de la información personal está unida intrínsecamente al derecho a la privacidad.[5] Conforme lo ha señalado la Comisión Europea, la protección de datos es necesaria para la resiliencia democrática,[6] y la normativa de protección de datos provee algunas de las herramientas que se necesitan para hacer frente al uso ilícito de datos personales en el contexto electoral.

Haciendo eco del derecho a la privacidad consagrado en el derecho internacional, 134 países de todo el mundo han promulgado leyes de protección de datos.[7] Sin embargo, es común que estas normas están desactualizadas, no abarquen todos los temas (en particular, a menudo excluyen el tratamiento de datos personales por parte de las autoridades públicas) y no prevean mecanismos independientes de vigilancia y reparación.[8] A veces las normas de protección de datos también prevén exenciones para los partidos políticos que podrían llegar a facilitar la explotación de los datos.[9] Estas normas deben ser evaluadas y actualizadas en lo pertinente.

El derecho a la privacidad también es un derecho habilitador que permite el goce de otros derechos humanos, en particular, en el contexto de las elecciones y las campañas políticas, del derecho a la libertad de expresión (Artículo 19 del PIDCP) y el derecho a la participación política (Artículo 25 del PIDCP). El derecho a la privacidad permite que las personas puedan formar opiniones, incluidas opiniones políticas, sin injerencias indebidas.
Según la interpretación que hace el Comité de Derechos Humanos de la ONU del derecho a la participación política consagrado en el Artículo 25 del PIDCP, los “electores [...] deberán poder

[5] Por ejemplo, de acuerdo con el Relator Especial de la ONU sobre sobre la promoción y protección del derecho a la libertad de opinión y de expresión, “el derecho a la privacidad” incluye “la capacidad de las personas para determinar quién posee información acerca de ellos y cómo se utiliza dicha información”. U.N. Doc. A/HRC/23/40, para 22, 17 de abril de 2013. Ver también el informe del Alto Comisionado de las Naciones Unidas para los Derechos Humanos acerca del derecho a la privacidad en la era digital, U.N. Doc. A/HRC/39/29, 3 de agosto de 2018.
[6] Ver https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-data-protection-law- electoral-guidance-638_en.pdf
[7] A abril de 2019, ver https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3386510.
[8] Privacy International desarrolló una guía sobre las leyes de protección de datos, que identifica las normas internacionales y regionales pertinentes y las mejores prácticas: https://privacyinternational.org/type-resource/data-protection-guide
[9] Ver https://privacyinternational.org/news-analysis/2836/gdpr-loopholes-facilitate-data-exploitation- political-parties

formarse una opinión de manera independiente, libres de toda violencia, amenaza de violencia, presión o manipulación de cualquier tipo”.[10] Algunas de las técnicas basadas en enormes cantidades de datos que se utilizan en el contexto de las elecciones y las campañas políticas (la elaboración de perfiles o profiling, la microfocalización o micro-targeting, etc., detalladas en la sección 2.2) pueden constituir una injerencia manipuladora e ilícita en el derecho a formarse una opinión y a ser informado.

Recomendaciones:

- La normativa nacional, idealmente la constitución, debe reconocer el derecho a la privacidad (incluida la protección de datos).
- Debe existir una ley moderna y completa de protección de datos, con una autoridad de protección de datos independiente y dotada de los suficientes recursos. Tal norma debe revisarse periódicamente, para garantizar que sus disposiciones estén actualizadas y sean eficaces para hacer frente a los retos que plantea la aplicación de las nuevas tecnologías, incluido en el contexto electoral.[11]
- La autoridad nacional de protección de datos debe expedir un código de buenas prácticas, o su equivalente, o por lo menos directrices sobre el uso de los datos personales en el proceso electoral, incluidas las campañas políticas.

Preguntas:

- ¿El derecho a la privacidad es protegido por la constitución o alguna otra norma?
- ¿Existe una normativa moderna y completa sobre la protección de datos?
    - ¿Cubre el tratamiento de datos personales por parte de las autoridades públicas?
    - ¿Prevé exenciones para los partidos políticos u otros actores de las campañas?
    - ¿Establece una autoridad nacional independiente para la protección de datos?
- Si existe una autoridad nacional de protección de datos, ¿ha dictado directrices sobre el uso de datos personales en el proceso electoral?
    - La directriz o el marco de protección de datos que aplica a las actividades políticas:
        - ¿Incluye una definición amplia de campaña política?

[10] Ver Comité de Derechos Humanos, observación general 25.
[11] Para más información sobre lo que debería incluir una normativa de protección de datos exhaustiva, ver https://privacyinternational.org/report/2255/data-protection-guide-complete

- ¿Aplica no solamente a los partidos políticos sino también a otros actores importantes, como las plataformas y los corredores de datos?
- ¿Consagra una interpretación amplia de los datos personales, que incluye lo que se deriva, se infiere y se predice (como resultado de la elaboración de perfiles)?

1.2 Inscripción de votantes

La inscripción de los votantes es necesaria para que las elecciones funcionen eficazmente. Su propósito es garantizar y permitir que solamente voten las personas elegibles para votar. Por lo tanto, requiere que de alguna manera se verifique la identidad de las personas del padrón electoral. Solo se deben registrar los datos personales que sean necesarios para identificar al votante y determinar que cumple los requisitos para votar. Del mismo modo, es necesario que los actores que monitorean las elecciones (y los partidos y las organizaciones políticas) tengan acceso al padrón electoral, para salvaguardar la imparcialidad del proceso electoral, pero esto no debe llevar al acceso ilimitado. Por último, incluso en los casos en que los datos personales que figuran en el registro personal se hagan públicos, el uso de tales datos debe estar sujeto a salvaguardas de protección de datos.

Aunque la forma en que se elabora el padrón electoral varía de un país a otro, es cada vez más frecuente que los gobiernos generen bases de datos centralizadas que almacena una gran variedad de datos personales de los votantes, incluidos, a veces, datos biométricos. Actualmente es común que los datos de los votantes que se registran se almacenen en una base de datos electrónica central. Si bien esto tiene ventajas, especialmente en relación con la mejora de la transparencia y el acceso y la divulgación responsables de los datos, los registros electrónicos centralizados generan inquietudes en cuanto a la seguridad de los datos personales almacenados y la posible utilización indebida de los mismos.

De hecho, si no son regulados adecuadamente, estos padrones electorales pueden perjudicar los procesos democráticos a los que aparentemente apoyan.

En primer lugar, los datos almacenados en estas bases de datos podrían combinarse con otros datos y ser usados para crear perfiles de los posibles votantes con el propósito de manipular sus opiniones. Este tema se aborda en la sección 2.2.

En Kenia, durante las elecciones presidenciales de 2017, hubo informes de que kenianos recibieron mensajes de texto no solicitados de candidatos políticos, que le pedían al destinatario

que votara por el candidato.[12] Estos mensajes mencionaban información personalizada del votante, como el distrito electoral y la mesa de votación, que había sido extraída del registro biométrico de votantes de Kenia. Existen inquietudes sobre si la comisión electoral de Kenia (IEBC, por sus siglas en inglés) compartió esta base de datos con terceros, sin el consentimiento de los votantes, y sobre si las empresas de telecomunicaciones compartieron la información de los suscriptores, también sin su consentimiento, para que se pudiera llevar a cabo esta microfocalización. No es claro con quién se compartió la base de datos de votantes y, por lo tanto, qué empresa, si la hubo, es la responsable de la microfocalización. La organización aliada de Privacy International, el Centro para el Derecho de Propiedad Intelectual y Tecnología (CPIT, por sus siglas en inglés) de la Universidad de Strathmore, en Kenia, investigó si el registro de votantes de 2017 fue compartido con terceros y, si lo fue, con quién. Sin embargo, el CPIT encontró más preguntas que respuestas.[13]

En segundo lugar, aunque los partidos políticos tienen un interés legítimo en acceder a los datos personales consignados en el padrón electoral, esto no puede conducir al acceso y el uso irrestricto de estos datos. La normativa debe definir quién puede acceder a estos datos y con qué fines.

En algunos países existirán dos padrones, un padrón general (cuyo acceso estaría limitado por ley) y un padrón abierto o editado (al que cualquiera podría comprar acceso). En el Reino Unido,[14] por ejemplo, el padrón general (completo) está a disposición de las personas previstas en la ley, como los funcionarios del padrón electoral, los partidos políticos registrados, los candidatos, las autoridades locales y las entidades que prestan servicios de información crediticia. Solo deben poder usar los datos para fines específicos, también prescritos en la ley. El padrón editado/abierto (que opera sobre la base de la exclusión voluntaria) puede ser comprado por cualquiera y a menudo es utilizado para fines de mercadeo. Por lo tanto, las entidades que tengan acceso al padrón completo no podrán compartirlo sin un fundamento lícito. Por ejemplo, una entidad que preste servicios de información crediticia no podrá compartir estos datos con otros corredores de datos para fines de mercadeo.

[12] Ver https://sur.conectas.org/en/a-very-secret-ballot/
[13] https://privacyinternational.org/report/2066/investigating-privacy-implications-biometric-voter- registration-kenyas-2017-election
[14] Ver https://ico.org.uk/your-data-matters/electoral-register/

En tercer lugar, si el padrón electoral carece de seguridad adecuada, pueden producirse filtraciones o fugas de datos personales, lo que podría llevar a que los votantes simplemente decidan no inscribirse en el padrón y podría causar otros perjuicios, como el robo de identidad.

En marzo de 2016, los datos personales de más de 55 millones de votantes registrados en Filipinas fueron filtrados, después de que se vulneró la base de datos de la Comisión Electoral (COMELEC).[15] La investigación adelantada por la autoridad nacional de protección de datos concluyó que se vulneró la seguridad de la base de datos de COMELEC, la cual almacenaba datos personales y confidenciales y otros datos, como información de pasaportes y números de identificación tributaria. El informe identificó como causas principales de la vulneración, la ausencia de una política clara de gobierno de datos, las vulnerabilidades del sitio web y la falta de control regular de las violaciones a la seguridad.

- **Registro biométrico de votantes (BVR, por sus siglas en inglés)[16]**

Quienes abogan por el BVR argumentan que es efectivo contra los fraudes electorales, como la suplantación de votantes y el voto múltiple. Sin embargo, el BVR no alcanza a reemplazar totalmente a los demás mecanismos utilizados para asegurar que el padrón esté actualizado (por ejemplo, reportar a los votantes fallecidos y eliminarlos del padrón). Además, el BVR plantea problemas concretos en relación con los costos de la tecnología, su mantenimiento y su soporte (lo que, a su vez, podría incrementar el riesgo de corrupción o, para los países en desarrollo, de depender de donantes).[17]

El BVR puede utilizarse para deduplicar el padrón electoral y/o para verificar la identidad de los votantes cuando acuden a la mesa de votación. La consecuencia de usar la biometría para deduplicar es que ello resulta en una base de datos centralizada que contiene información biométrica de toda la población inscrita en el padrón. El BVR debe incorporar la privacidad por diseño y por defecto. Por ejemplo, un sistema de autenticación diseñado exclusivamente para la deduplicación no tiene ninguna necesidad que vincular los datos biométricos con la persona; todo lo que necesita saber es si ya había visto esos datos biométricos específicos (es decir, responde a la pregunta, “¿este votante cumple los requisitos?”).

Desde el punto de vista de la protección y seguridad de datos, recopilar y almacenar datos biométricos para registrar votantes genera inquietudes adicionales. Los datos biométricos son

[15] https://www.privacyinternational.org/state-privacy/1009/state-privacy-philippines

[16] Con los registros biométricos de votantes, una o más características físicas del votante, tales como la foto, su huella dactilar o el escaneado de la retina, entre otras características, se registran en el momento de la inscripción. Dicha información puede usarse para identificar al votante en la mesa de votación.

[17] Para una lista de tales inquietudes, ver el Manual de la EU --EU Handbook--, https://eeas.europa.eu/sites/eeas/files/handbook_for_eu_eom_2016.pdf

especialmente sensibles y reveladores en cuanto a las características y la identidad de una persona. Por lo tanto, es posible abusar gravemente de ellos.[18] Muchas normativas de protección de datos ubican a los datos biométricos en una categoría especial de datos personales, que conlleva salvaguardas y límites adicionales para su recopilación y uso. Del mismo modo, los sistemas de identificación basados en datos biométricos también son vulnerables a las violaciones de seguridad, las cuales tienen consecuencias gravísimas para las personas afectadas y para la seguridad en general de la sociedad.[19]

Recomendaciones:

- La normativa debe estipular con claridad los procedimientos de registro de votantes.
- El padrón electoral no debe incluir datos personales distintos de los que se necesitan para acreditar la satisfacción de los requisitos para votar.
- La ley debe estipular las normas de seguridad mínimas para proteger el padrón electoral de accesos no autorizados; también debe definir las condiciones y los límites para acceder a los datos contenidos el padrón electoral.
- Por defecto, los datos personales del padrón electoral no deben ser publicados. Si el padrón electoral es abierto y cualquiera puede comprar acceso al mismo para cualquier fin, debe operar con fundamento en la inclusión voluntario (opt-in) y no la exclusión voluntaria (opt-out).
- La normativa y las directrices relevantes deben estipular con claridad que los datos personales del padrón electoral a que se permite acceder continúan estando protegidos y sujetos a la legislación sobre protección de datos, incluido su tratamiento futuro.
- El acceso y el uso de los datos personales almacenados en un padrón electoral deben ser regulados. La ley debe estipular claramente quién tiene derecho al acceso y para qué fines, debe limitarse a lo necesario para el proceso electoral, con prohibiciones claras de usar tales datos para cualquier otro fin.

[18] Informe del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, 3 de agosto de 2018, A/HRC/39/29, disponible en https://undocs.org/A/HRC/39/29

[19] Para ejemplos de violaciones de bases de datos biométricos, ver Privacy International, Briefing to the UN Counter-Terrorism Executive Directorate on the responsible use and sharing of biometric data in counter-terrorism, junio de 2019.

Registro biométrico de votantes:

- Dado que los datos biométricos son especialmente sensibles, su uso requiere las normas consagren fuertes salvaguardas, incluido que todas las normas de protección de datos reconozcan el carácter delicado de estos datos.
- Los datos biométricos (incluidas las fotografías) únicamente pueden usarse para los fines previstos en la ley (deduplicación y/o la autenticación de la identidad del votante).
- Se deben desarrollar protecciones adicionales contra el acceso no autorizado y otras violaciones de los datos personales, lo que incluye almacenar los datos biométricos de por separado de otros datos.
- Ningún tercero (aparte de la autoridad pública que administra el proceso de registro de votantes) debe tener acceso a los datos biométricos.
- Los contratos con los proveedores deben ser transparentes, y deben existir salvaguardas para el envío internacional de datos.
- Debe aplicarse una privacidad robusta, por diseño y por defecto. Por ejemplo, los sistemas deben diseñarse para usos y casos específicos y solamente deben usarse para la autenticación (1 respecto a 1) y no la identificación (1 respecto a muchos).

Preguntas:

- ¿La ley regula el registro de los votantes y la administración del padrón electoral?
- ¿Quién tiene acceso al padrón electoral completo y cuáles son las condiciones para acceder al mismo?
- ¿Cuáles son los datos personales de acceso abierto, quién puede acceder a ellos, con base en qué fundamento y en qué condiciones (por ejemplo, el consentimiento del votante)?
- ¿Cuáles son las medidas de seguridad adoptadas para garantizar que los datos personales contenidos en el padrón electoral ¿Cuáles son las medidas de seguridad adoptadas para garantizar que los datos personales contenidos en el registro de votantes estén protegidos del acceso no autorizado? ¿Con qué frecuencia se revisan estas medidas? ¿Y cómo se evalúan?
- ¿Se consulta a la autoridad nacional de protección de datos sobre la administración y las actualizaciones relacionadas con el padrón electoral?
- ¿Si se usa un registro biométrico, está sujeto a salvaguardas reforzadas en razón a la sensibilidad de los datos?
- Si se utiliza el registro biométrico, ¿se ha diseñado con miras a la privacidad y limitando su uso a situaciones específicas y relevantes?

1.3 Votación

Las reglas relacionadas con la votación buscan “asegurar que todos los votantes que reúnan las condiciones tengan una oportunidad real de depositar libremente su voto secreto, prevenir la votación ilegal, que se registre la voluntad de los votantes, evitar el fraude y que la transparencia sea la base de la confianza pública en el proceso electoral”.[20]

En este contexto, surgen consideraciones similares a las planteadas en relación con el padrón electoral, en particular, sobre la necesidad de limitar la recopilación de la información personal de los votantes a lo estrictamente necesario para completar el proceso (ver la sección 1.2). Por ejemplo, los datos compartidos en la mesa de votación deben limitarse a los datos necesarios para identificar al votante y completar el proceso de votación.

Asimismo, una mayor dependencia de soluciones técnicas, como, por ejemplo, el voto electrónico, plantea riesgos adicionales de abuso y, además, de desafíos específicos relacionados con la ciberseguridad y la protección del anonimato de los votantes. Estas inquietudes han sido articuladas por algunas organizaciones de observadores electorales, al señalar, por ejemplo, que “los sistemas de voto electrónico vinculados a Internet u otras redes de ordenadores pueden ser susceptibles de piratería informática o manipulación exterior”.[21] En un informe exhaustivo, Security Democracy in Cyberspace, la organización alemana Stiftung Neue Verantwortung detalla una serie de medidas relativas a la ciberseguridad y las elecciones.[22] Algunas de las recomendaciones relevantes contenidas en ese informe se recogen a continuación. Adicionalmente, en el contexto estadounidense, el Centro para la Democracia y la Tecnología desarrolló unas guías muy útiles para concienciar sobre los riesgos de seguridad que conlleva el uso de las tecnologías de voto electrónico.[23]

En la práctica, incluso los países con experiencia significativa en la organización de elecciones y referendos son vulnerables a estos riesgos. Por ejemplo, en Suiza, investigadores encontraron fallas técnicas en el sistema de voto electrónico que podrían permitir que intrusos sustituyeran los votos legítimos por votos fraudulentos.[24]

[20] Ver Promoting Legal Frameworks for Democratic Elections (https://www.ndi.org/sites/default/files/2404_ww_elect_legalframeworks_093008.pdf)
[21] Ver la tercera edición de Handbook for European Union Election Observation (https://eeas.europa.eu/sites/eeas/files/handbook_for_eu_eom_2016.pdf)
[22] Ver Stiftung Neue Verantwortung, Securing Democracy in Cyberspace - An Approach to Protecting Data-Driven Elections, octubre de 2018, https://www.stiftung-nv.de/sites/default/files/securing_democracy_in_cyberspace.pdf
[23] Ver https://cdt.org/insight/election-cybersecurity-101-field-guide-ddos-attack-mitigation/
[24] Ver https://www.cyberscoop.com/swiss-voting-system-flaw-encryption/

Recomendaciones:

- Solamente deben recopilarse los datos personales mínimos necesarios para garantizar la integridad del proceso de votación.
- Deben incorporarse salvaguardas específicas para proteger el anonimato, minimizar el riesgo de que los datos sean objeto de accesos no autorizados y la piratería informática, en el caso de la votación electrónica.
- Deben destinarse recursos a la seguridad de las elecciones, incluidas la elaboración y la realización de evaluaciones de riesgo de las tecnologías utilizadas en las elecciones.
- Deben establecerse mecanismos para monitorear, detectar y alertar sobre ataques cibernéticos contra la infraestructura electoral y, además, estos mecanismos deben integrarse a las respuestas de seguridad cibernética.
- Las personas que administran o participan en la votación electrónica deben recibir capacitación técnica y de sensibilización ante los riesgos de ciberseguridad que implica dicho sistema.

Preguntas:

- ¿Cuáles son los datos personales solicitados en el momento de la votación (es decir, para la verificación)?
- ¿Cuáles son los datos personales que se almacenan, cómo se transfieren y a quién?
- ¿Qué salvaguardas específicas existen en relación con la votación electrónica para proteger el anonimato de los votantes?
- ¿Qué salvaguardas específicas existen para proteger el voto electrónico en conexión con Internet u otras redes informáticas del acceso no autorizados y la piratería electrónica?
- ¿La ciberseguridad de las elecciones es parte de la estrategia nacional de ciberseguridad?
- ¿Qué mecanismos existen para monitorear, detectar y responder a los ciberataques relacionados con el voto electrónico?
- ¿Las personas involucradas en las elecciones reciben capacitación sobre ciberseguridad?

1.4 Papel del Organismo de Administración Electoral

El Organismo de Administración Electoral (EMB, por sus siglas en inglés), es el organismo (o los organismos) encargado de garantizar la imparcialidad, eficacia y transparencia de las elecciones.

En razón del importante papel que desempeñan los datos y las tecnologías digitales en el proceso electoral, es imperativo que los EMB cuenten con el conocimiento técnico que les permita evaluar la forma en que se usan en el proceso electoral la información personal y las tecnologías digitales para el tratamiento de dicha información. Necesitan conocimientos especializados en materia de protección de datos y de ciberseguridad.

Más allá del fortalecimiento de sus capacidades propias, se reconoce cada vez más la necesidad de coordinar con otros entidades gubernamentales y organismos reguladores independientes. Las amenazas a la integridad de las elecciones surgen de diferentes actores y precisan la participación de diferentes autoridades, así como la coordinación entre ellas.

Como ha señalado el Supervisor Europeo de Protección de Datos, “la legislación de protección de datos, la legislación electoral y la legislación audiovisual comparten principios comunes, como la transparencia y la equidad, y la cooperación entre los respectivos reguladores, especialmente en el período electoral, podría mejorar su aplicación coherente y reforzar la protección de las personas ante prácticas de microfocalización potencialmente injustas”. Hasta el momento, esta cooperación no ha sido suficiente.[25]

Para las elecciones al Parlamento Europeo de 2019, se adoptaron normas que permiten que las autoridades nacionales de protección de datos (APD) informen a la Autoridad para los Partidos Políticos Europeos y las Fundaciones Políticas Europeas de cualquier decisión que concluya que se infringieron las normas de protección de datos, cuando la infracción se relaciona con actividades políticas dirigidas a influir las elecciones para el Parlamento Europeo.[26]

Es poco probable que, por su cuenta, las distintas autoridades cooperen sistemáticamente. En cambio, los gobiernos deberían considerar la posibilidad de establecer un mecanismo de coordinación, especialmente en períodos de campañas y elecciones, para garantizar el intercambio de información y de conocimientos especializados entre las diferentes autoridades responsables de la celebración y el seguimiento de las elecciones.

[25] Supervisor Europeo de Protección de Datos, Opinion 3/2018 on online manipulation and personal data, 19 de marzo de 2018, https://edps.europa.eu/sites/edp/files/publication/18-03- 19_online_manipulation_en.pdf
[26] Ver https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-cybersecurity-elections-recommendation-5949_en.pdf

Recomendaciones:

- Los EMB deben desarrollar su pericia en materia de protección de datos y ciberseguridad.
- Los EMB deben cooperar oportuna y eficazmente con autoridades de ámbitos conexos (como las autoridades de protección de datos, los reguladores de los medios de comunicación, las autoridades de seguridad cibernética, los comisarios biométricos, etc.).

Preguntas:

- ¿Los EMB tienen conocimientos especializados en materia de protección de datos y ciberseguridad?
- ¿El EMB está consultando y cooperando con otras autoridades (protección de datos, reguladores de medios de comunicación, ciberseguridad)?
- ¿El gobierno ha establecido un mecanismo de coordinación de las autoridades encargadas de los distintos aspectos de la administración y el control de las elecciones?

1.5 Reclamaciones y reparación

Es necesario establecer un mecanismo independiente de reclamaciones para garantizar que los procesos electorales sean libres y justos y que todos los actores involucrados rindan cuentas sobre sus actos. Dado que las elecciones y los procesos democráticos (como la participación en campañas políticas) son manifestaciones del goce de derechos humanos fundamentales, los gobiernos tienen una obligación jurídicamente vinculante de garantizar que las personas tengan un derecho eficaz a la reparación de cualquier violación de sus derechos en este contexto.

Los mecanismos de reclamación y reparación pueden variar de un país a otro, pero, en el marco de la protección de datos, existe una marcada preferencia por el establecimiento de autoridades independientes de protección de datos que tengan la capacidad de recibir reclamaciones. Como mínimo, estas autoridades deberían tener el mandato de recibir cualquier reclamación relacionada con el abuso de información personal en el contexto electoral. Por ejemplo, en Italia, la APD investigó la plataforma “Rousseau” del Movimiento 5 Estrellas,[27] y en el Reino Unido, la APD multó al grupo de campaña Vote Leave Limited por enviar miles de mensajes de texto no solicitados en el período previo al referéndum relacionado con la Unión Europea celebrado en 2016.

[27] https://privacyinternational.org/examples/2843/failures-five-star-movements-rousseau

Las autoridades reguladoras electorales independientes también deberían estar facultadas para recibir quejas, en particular, en relación con el uso indebido de datos por parte de los partidos y otros agentes políticos.

Del mismo modo, las personas y las organizaciones, incluidos los grupos de observadores ciudadanos, deberían poder presentar reclamaciones por el abuso de información personal en el proceso electoral ante el EMB nacional u otro organismo nacional independiente que monitoree el desarrollo de las elecciones.

Recomendaciones:

- Las autoridades de protección de datos independientes deben estar facultadas para aceptar y tramitar las reclamaciones de personas y organizaciones que denuncien el abuso de datos personales en el contexto de las elecciones y las campañas políticas.
- Del mismo modo, las personas y las organizaciones deben poder presentar reclamaciones ante los EMB u otras autoridades reguladoras electorales independientes.
- Los EMB u otras autoridades reguladoras electorales independientes deben estar facultadas para recomendar y/o implementar reformas cuando las reclamaciones evidencien problemas sistémicos.
- Las personas y las organizaciones también deben tener derecho a interponer recursos judiciales por supuestas violaciones de la protección de datos durante las elecciones, ya sea directamente o apelando las decisiones de los órganos reguladores.

Preguntas:

- ¿Cuáles son los mecanismos de reparación a disposición de las personas y organizaciones que denuncian el abuso de datos personales en el contexto de las elecciones y las campañas políticas?
- ¿El EMB acepta quejas de personas y organizaciones?
- ¿Cuáles son los diferentes tipos de reparación disponibles (multas, imposición de condiciones o restricciones en el tratamiento de datos personales, etc.)?

Parte 2 — Partidos políticos y otros actores políticos

Cada vez más, las organizaciones de observación electoral reconocen que las normas que regulan la conducta de los partidos políticos y los demás actores en las elecciones deben evaluarse a la luz de una mayor dependencia de las tecnologías y los datos personales. Asimismo, es cada vez más evidente que las normas que regulan las campañas políticas no se han adaptado a los medios que hoy día utilizan las campañas, en particular, a la creciente dependencia de las comunicaciones digitales y las redes sociales.

Como la Comisión Europea señaló claramente en 2018: “Las actividades en línea, incluso durante los procesos electorales, se están desarrollando rápidamente y, por consiguiente, más seguridad y unas condiciones políticas equitativas son fundamentales. Las salvaguardas electorales convencionales (off-line o fuera de línea), tal como las reglas que aplican a las comunicaciones políticas durante los períodos electorales, la transparencia y los límites del gasto electoral, el respeto de los períodos de silencio y el trato igualitario para los candidatos, también deben aplicar en línea. [...] Esto no es lo que sucede ahora, y hay que remediarlo [...]”.[28]

2.1 Regulación del uso de datos personales por las campañas políticas

Los partidos y otros actores políticos están empleando cada vez más una gran variedad de técnicas que requieren grandes cantidades de datos para llegar a los posibles votantes. Estas técnicas se basan en la recopilación y el análisis de información personal. La información personal se considera un activo político (cuando los partidos generan sus propios conjuntos de datos o datasets), inteligencia política (que contribuye a formular las estrategias de la campaña y a ensayar y adaptar sus mensajes) y, por último, influencia política.[29]

Aplicar salvaguardas de protección de datos a la información personal que utilizan los partidos políticos es fundamental para evitar abusos que podrían, posiblemente, debilitar la democracia y la celebración de elecciones libres y justas.[30]

Los datos personales que revelan opiniones políticas son una categoría especial de datos, de acuerdo con las leyes modernas de protección de datos, como el Reglamento General de Protección de Datos de la Unión Europea. Por regla general, se prohíbe el tratamiento de estos datos, con algunas excepciones estrictamente interpretadas, como el consentimiento explícito, específico, plenamente informado y libremente otorgado de las personas afectadas.

[28] Ver https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-free-fair-elections- communication-637_en.pdf
[29] Ver Information Commissioner’s Office, Democracy Disrupted?, 11 de julio de 2018, https://ico.org.uk/media/2259369/democracy-disrupted-110718.pdf
[30] Ver https://privacyinternational.org/long-read/2850/data-exploitation-and-democratic-societies

Del mismo modo, los datos personales que hayan sido revelados públicamente o, que, de cualquier otra manera, hayan sido compartidos por votantes individuales con partidos políticos, incluso los datos que no revelan opiniones políticas, continúan estando sujetos a la ley de protección de datos y siendo protegidos por la misma. Por ejemplo, los datos personales recopilados a través de las redes sociales no pueden usarse sin cumplir las obligaciones relacionadas con la transparencia, el principio de finalidad y la legalidad.

El riesgo de que el abuso de los datos personales pueda afectar las elecciones democráticas motivó a la Unión Europea a introducir medidas, incluido un régimen de sanciones, para las elecciones al Parlamento Europeo celebradas en mayo de 2019. Como señala la Comisión Europea, “debería ser posible imponer sanciones a los partidos políticos o las fundaciones políticas que se beneficien de la violación de las normas de protección de datos para influir intencionalmente en el resultado de las elecciones al Parlamento Europeo”.[31]

Pese a estos riesgos, las leyes de protección de datos recientes a veces incluyen exenciones para los partidos políticos en relación con las obligaciones de protección de datos. Estas exenciones ponen en peligro los esfuerzos para hacer frente al riesgo de la explotación de los datos en las elecciones.[32]

Por ejemplo, en España, una disposición de la ley española de protección de datos establecía una exención para los partidos políticos.[33] La APD española abogó por una interpretación restrictiva y el Defensor del Pueblo interpuso una demanda judicial, tras la cual, en mayo de 2019, el Tribunal Constitucional declaró que la disposición era inconstitucional.[34]

[31] https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-cybersecurity-elections- recommendation-5949_en.pdf
[32] Ver https://www.gdprtoday.org/gdpr-loopholes-facilitate-data-exploitation-by-political-parties/
[33] Ver https://privacyinternational.org/long-read/2821/spanish-elections-under-new-data-protection-law-use-personal-data-political-parties
[34] Ver https://www.tribunalconstitucional.es/NotasDePrensaDocumentos/NP_2019_074/Press%20Release%20No.%2074.2019.pdf y https://www.tribunalconstitucional.es/NotasDePrensaDocumentos/NP_2019_076/Press%20Release%20No.%2076.2019.pdf

Recomendaciones:

- La normativa de protección de datos debe aplicarse en su totalidad al tratamiento de datos por parte de los partidos políticos y otros actores políticos.
- Los partidos y otros actores políticos deben
    - ser transparentes sobre las actividades de tratamiento de datos que realizan, incluso identificando los mecanismos que emplean para llegar a los votantes (por ejemplo, las redes sociales, sitios web, mensajes directos a través de plataformas como WhatsApp);
    - adoptar y publicar políticas de protección de datos;
    - realizar auditorías de protección de datos y evaluaciones de impacto;
    - cerciorarse de que cada vez existe tienen un fundamento jurídico cada vez que usan datos personales (incluidos los datos sensibles, como los que reflejan opiniones políticas);
    - facilitar que las personas ejerzan sus derechos sobre datos (incluso brindando información sobre la manera en que ocurre el tratamiento de sus datos y facilitar acceso al mismo);
    - garantizar que los terceros a los que recurren para sus actividades de campaña también cumplan la normatividad de protección de datos.

Preguntas:

- ¿La normativa nacional sobre protección de datos aplica a los datos recopilados y usados (tratados) por los partidos y otros actores políticos?
- ¿Los partidos y otros actores políticos cuentan con políticas de protección de datos?
- ¿Revelan dónde obtienen los datos personales y qué hacen con ellos?
- ¿Efectúan evaluaciones de impacto sobre protección de datos en relación con el tratamiento que hacen de los datos personales?
- ¿Obtuvieron el consentimiento de las personas o de qué otra manera justifican la posesión de los datos?

2.2 Campañas políticas

En todo el mundo, las campañas políticas se han convertido en sofisticadas operaciones de datos. El escándalo de Cambridge Analytica, aunque no fue un hecho aislado, sensibilizó sobre los posibles efectos en los procesos electorales de combinar la elaboración de microperfiles con poderosas herramientas de aprendizaje automático o machine learning.[35]

El Comité Europeo de Protección de Datos resumió con precisión el rol de los datos personales en las campañas políticas modernas: “Los partidos políticos, las coaliciones políticas y los candidatos dependen cada vez más de los datos personales y de sofisticadas técnicas de elaboración de perfiles para monitorear y dirigirse a los votantes y los líderes de opinión. En la práctica, los individuos reciben mensajes e información altamente personalizados, especialmente en plataformas de redes sociales, de acuerdo con sus intereses personales, hábitos de vida y valores”.[36]

Las técnicas de elaboración de perfiles y de personalización basadas en datos que utiliza el sector de la publicidad digital general son usadas cada vez más en el contexto de las campañas políticas.[37] Diferentes empresas ofrecen servicios específicos que adaptan al contexto electoral.[38]

- **Elaboración de perfiles**

La elaboración de perfiles es una forma de recopilar, derivar, inferir o predecir información sobre personas y grupos, preferencias personales, intereses, situación económica, etc.[39] Tal

[35] Cambridge Analytica era una empresa que operaba como un consultor político con sede en el Reino Unido. Uno de los principales servicios que ofrecía era un perfil “psicográfico” único de los votantes. Se utilizó en varias campañas en Estados Unidos y posiblemente en la campaña Leave EU en el Reino Unido. Ver, entre otras, European Parliament Resolution on the Use of Facebook Users’ Data by Cambridge Analytica and the Impact on Data Protection, 2018/2855(RSP), 25 de octubre de 2018.

[36] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-03-13-statement-on-elections_en.pdf

[37] Como dice Alexander Nix, director ejecutivo de Cambridge Analytica: “Lo que estamos haciendo no es diferente de lo que la industria publicitaria general está haciendo en el espacio comercial”. Testigo I: Alexander Nix, director ejecutivo, Cambridge Analytica, Comité Digital, de Cultura, Medios de Comunicación y Deporte Pruebas Orales: Fake News (HC 363), 27 de febrero de 2018. Disponible en: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media- and-sport-committee/disinformation-and-fake-news/oral/79388.pdf (última visita 7 de abril de 2019].

[38] Oracle Data Cloud Data Directory; Experian Marketing Services, A Reference Guide to All the Ways Experian Can Help Your Marketing Efforts, Libro Blanco. Ver, en particular, uno de los servicios de mercadeo ofrecidos por Experian que, en apariencia, puede influir en el comportamiento de los votantes: OmniActivation Strategic Services, Data, Targeting and Measurement: Full-Service Digital Display Campaigns Run by the Experts, ficha técnica, Experian.

[39] El RGPD define la elaboración de perfiles como “toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física;” Artículo 4(4), Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el

conocimiento puede usarse para tomar o informar decisiones, asignar puntajes, clasificar, evaluar y valorar a las personas, y para tomar o informar decisiones que personalizan el entorno de un individuo.[40] Los datos personales —independientemente de si han sido suministrados, recopilados automáticamente, derivados, inferidos o pronosticados— se utilizan para elaborar perfiles detallados de individuos y grupos. Múltiples actores compran, acumulan y comparten entre sí los datos que alimentan estos perfiles,[41] a menudo, sin el conocimiento de las personas implicadas, se elaboró un perfil de ellas. Los perfiles pueden correlacionarse y usarse para inferir datos no solo de los individuos sino de otras personas “como ellos”, por ejemplo, mediante públicos similares o lookalike.[42] Adicionalmente, los corredores de datos y las empresas de tecnologías publicitarias frecuentemente ofrecen soluciones probabilísticas, en las que establecen “coincidencias entre conjuntos de datos que aprovechan supuestos inferidos, modelados o variables proxy.”[43]

- **Técnicas de personalización basadas en datos**

La elaboración de perfiles potencia y mejora una serie de técnicas de personalización basadas en datos, entre las que se incluyen las descritas a continuación. La microfocalización de votantes individuales permite que los actores políticos les envíen mensajes personalizados, basados en sus preferencias —suministradas o inferidas—, a través de servicios en línea como las plataformas de redes sociales.[44] Otro método de personalización es el geoperimetraje, que permite enfocarse sobre un individuo con base en su ubicación.[45] La influencia sobre las búsquedas, también, permite que los partidos políticos y otros actores optimicen y aumenten su posicionamiento en los resultados de las búsquedas en línea, en particular, en los resultados de las búsquedas locales. Todas estas son técnicas de personalización basadas en datos, que se emplean cada vez más para llegar a los votantes e influir sus acciones. El uso de estas técnicas facilita la creación de burbujas

que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), 27 de abril de 2016.

[40] Kaltheuner y Bietti, 'Data Is Power: Towards Additional Guidance on Profiling and Automated Decision-Making in the GDPR', 2 Journal of Information Rights, Policy and Practice (2018), disponible en https://jirpp.winchesteruniversitypress.org/article/10.21039/irpandp.v2i2.45/ (última visita 4 de abril 2019).

[41] Privacy International, A Snapshot of Corporate Profiling, 9 April 2018, disponible en http://privacyinternational.org/feature/1721/snapshot-corporate-profiling (last visited 4 April 2019]. Our Complaints against Acxiom, Criteo, Equifax, Experian, Oracle, Quantcast, Tapad, 8 de noviembre de 2018, Privacy International, disponible en http://privacyinternational.org/advocacy-briefing/2426/our- complaints-against-acxiom-criteo-equifax-experian-oracle-quantcast-tapad (última visita el 7 de abril de 2019).

[42] Democracy Disrupted? Personal Information and Political Influence, Information Commissioner’s Office, 11 de julio de 2018, p. 36.

[43] Informe de Winterberry Group “Know Your Audience: The Evolution of Identity in a Consumer-Centric Marketplace”, agosto de 2018 https://www.winterberrygroup.com/our-insights/know-your-audience- evolution-identity-consumer-centric-marketplace

[44] D. Ghosh, What Is Microtargeting and What Is It Doing in Our Politics?, 4 de octubre de 2018, Internet Citizen, disponible en https://blog.mozilla.org/internetcitizen/2018/10/04/microtargeting-dipayan-ghosh.

[45]En general, sobre la geofocalización ver, “Geotargeting: The Political Value of Your Location”, Tactical Tech, disponible en https://ourdataourselves.tacticaltech.org/posts/geotargeting/.

de filtro o filter bubbles de información sobre intereses que se utilizan para hacer campaña y que, además, sirven para propagar desinformación con el fin de agudizar las divisiones sociales y manipular las acciones de personas y grupos específicos.[46]

***

Es importante reconocer que el uso de estas técnicas de personalización (sin importar si las aplican partidos políticos u otros actores políticos) no se limita a la campaña electoral. Los datos personales son utilizados indebidamente para la manipulación política y la desinformación en todo momento, no sólo en la época electoral.[47] Privacy International considera que la reglamentación del uso de los datos en las campañas políticas no debe limitarse al periodo electoral.

Adicionalmente, hay una plétora de empresas y otros actores, además de los partidos políticos y candidatos oficiales, que usan (u ofrecen) estas técnicas de personalización, las cuales requieren grandes cantidades de datos y atentan contra la privacidad. Circunscribirse únicamente a la campaña electoral y a los partidos políticos y candidatos oficiales podría llevar a que se ignore un fenómeno importante y cada vez más amplio, que influye directamente en la democracia.

Recomendaciones:

- Las leyes y los reglamentos deberían exigir que se revele la información sobre todos los criterios de selección que usan los partidos y otros actores políticos en la divulgación de las comunicaciones políticas.
- En el caso de técnicas de personalización basadas en datos, debe brindarse a los votantes información adecuada que explique porqué reciben un mensaje específico, quién es responsable del mismo y cómo pueden ejercer sus derechos para proteger sus datos y evitar que sean objeto de estas técnicas.
- Los partidos y los demás actores políticos deben asegurarse de que el público pueda reconocer fácilmente los mensajes y las comunicaciones políticas y el partido, la fundación o la organización detrás de estos mensajes y comunicaciones. En sus sitios web y como parte de la comunicación, deben suministrar acceso a la información sobre los criterios de selección usados para la difusión de dichas comunicaciones.

[46] Ver https://ourdataourselves.tacticaltech.org/projects/data-and-politics/
[47] Por ejemplo, en el contexto del Reino Unido: https://www.politico.eu/article/britain-nationalist-dark-web-populism-tommy- robinson y https://www.theguardian.com/politics/2019/apr/03/grassroots-facebook-brexit-ads-secretly-run-by-staff-of-lynton-crosby-firm.

- Los partidos y los otros actores políticos deben garantizar que el uso de datos para tales técnicas (por ellos mismos y por aquellos con los que trabajan para obtener datos) cumple todos los requisitos de la normatividad de protección de datos, incluidos principios como la transparencia, la imparcialidad y el principio de finalidad; el requisito de la existencia de fundamentación jurídica; derechos como el derecho a la información; y obligaciones como la de efectuar evaluaciones de impacto de la protección de los datos.
- Las campañas políticas deben ser transparentes sobre los terceros que contratan en la campaña para obtener datos y continuar el tratamiento de datos —incluidas la elaboración de perfiles y la personalización—, tales como los corredores de datos y las compañías de publicidad política.

Preguntas:

- ¿La normatividad exigen que los partidos políticos y otros actores divulguen sus conexiones con las organizaciones y los personas que desarrollan publicidad o campañas políticas, incluidas actividades en línea?
- ¿La normatividad exigen que los partidos políticos u otros actores proporcionen a los individuos y los reguladores información sobre su uso de técnicas de personalización, incluidos los criterios de personalización que aplican, y con qué terceros están trabajando?
- ¿Los partidos y otros actores políticos asumen suficiente responsabilidad por los datos que pueden usar los terceros con el que contraten? ¿Saben cuáles son los datos que utilizan esos terceros? ¿Han celebrado contratos con los terceros? ¿Estos contratos contemplan suficientes cláusulas sobre la protección y la seguridad de los datos?

2.3 Financiamiento de campañas

El financiamiento de campañas se refiere al financiamiento proporcionado a los partidos políticos o candidatos para los fines de la campaña electoral (ya sea a través de donaciones privadas o de financiamiento público) y los gastos de los partidos o los candidatos en los costos de la campaña electoral.

Los partidos políticos y los otros actores recurren cada vez más a las plataformas de redes sociales y otros medios de comunicación digitales, tanto para llegar a las personas naturales que son posibles donantes (especialmente en el caso de las pequeñas donaciones) como para gastar en publicidad política.

Es bien sabido que el financiamiento de las campañas es notoriamente difícil de monitorear. Más aún, investigaciones recientes y en curso ponen de manifiesto que las normas tradicionales de financiamiento de campañas son insuficientes para regular y revelar estas nuevas maneras de recaudar fondos y gastar en línea.

En el Reino Unido, por ejemplo, la Comisión Electoral investigó a la campaña Vote Leave.[48] En julio de 2018, la Comisión Electoral determinó que cinco pagos realizados por varios grupos de la campaña Vote Leave a una empresa canadiense de análisis de datos, AggregateIQ, violaban las normas de financiamiento y gastos de campañas. La Comisión Electoral multó a Vote Leave y remitió a la campaña a la policía por haber violado las leyes de elecciones. La Comisión Electoral ha hecho un llamado para que se modifiquen las leyes, para que las campañas digitales sean más transparentes frente a los votantes, incluso en relación con los gastos.[49]

En su informe de 2018 sobre la manipulación en línea y los datos personales, el Supervisor Europeo de Protección de Datos señaló que “es posible que los gastos en materiales de la campaña que fueron reportados no suministren suficientes detalles sobre lo gastado en publicidad digital y servicios asociados, por ejemplo, anuncios personalizados en las redes sociales, servicios analíticos, la creación de bases de datos de votantes, la utilización de corredores de datos”.[50]

Recomendaciones:

- La normativa de financiamiento de campañas debe exigir la presentación oportuna de informes sobre las sumas gastadas para hacer campaña en línea y los fondos recaudados través de Internet. La información debe ser lo suficientemente minuciosa y detallada como para promover la transparencia y la rendición de cuentas.
- Los partidos políticos y otros actores políticos deben poner a disposición del público (por ejemplo, en un lugar destacado en sus sitios web) información sobre lo gastado en actividades en línea, incluidos los anuncios y comunicaciones políticas en línea que pagaron. Esto debería incluir información sobre qué terceros, si los hay, han asistido a los actores políticos en sus actividades en línea, incluido el monto que se gastó en los servicios de cada uno de ellos.

[48] https://www.electoralcommission.org.uk/i-am-a/journalist/electoral-commission-media-centre/party-and-election-finance-to-keep/leave.eu-fined-for-multiple-breaches-of-electoral-law-following-investigation
[49] https://www.electoralcommission.org.uk/data/assets/pdf_file/0010/244594/Digital-campaigning- improving-transparency-for-voters.pdf
[50] Supervisor Europeo de Protección de Datos, Opinion 3/2018 on online manipulation and personal data, 19 de marzo de 2018, https://edps.europa.eu/sites/edp/files/publication/18-03- 19_online_manipulation_en.pdf

- La información divulgada sobre los gastos de la campaña debe clasificarse en categorías significativas, como el monto gastado en los distintos tipos de contenido en cada una de las plataformas de redes sociales, información sobre el público destinatario al que se dirigió la campaña e información sobre el público al que efectivamente logró llegar la campaña.
- Las normas y los reglamentos nacionales (por ejemplo, el código de prácticas) deben exigir la divulgación de información sobre grupos que apoyan a las campañas políticas pero no están vinculados oficialmente con la misma, y la divulgación de los gastos de la campaña en actividades en línea, incluidos los anuncios y comunicaciones políticas por Internet que pagaron.

Preguntas:

- ¿Las normas de financiación de campañas exigen la presentación de informes sobre las sumas gastadas en campañas en línea? ¿A quién fueron pagadas? ¿Qué tan detalladas son las exigencias de estas obligaciones? ¿Cuáles son los plazos? ¿cuáles son las sanciones por incumplimiento?
- ¿Existen leyes o regulaciones que exijan a los partidos políticos (y otros actores políticos) que revelen el monto pagado por los anuncios políticos en línea? ¿Cuáles son los detalles de la información presentada (por ejemplo, desglosada por plataformas digitales, etc.)?
- ¿Los partidos y los actores políticos están divulgando sus gastos de campaña en línea con el suficiente grado de detalle?

Parte 3 — Papel de Internet y las redes sociales en las elecciones y las campañas políticas

Internet y los medios sociales han contribuido a que muchos se organicen políticamente, participen en debates públicos, expresen sus opiniones —incluida la disidencia— en línea y reciban información, incluso durante las campañas electorales.

Paralelamente, las actuales tecnologías de comunicación digital cuestionan la eficacia de algunas de las salvaguardas adoptadas para garantizar que las elecciones sean libres y justas. En particular, ha sido objeto de especial atención la difusión de la desinformación y el riesgo de que sean manipuladas las opiniones políticas de las personas. Estas preocupaciones se agudizan en los períodos cercanos a las elecciones, pero son relevantes en cualquier momento, dado que incluso contextos en línea que aparentemente son apolíticos pueden resultar en la movilización política de la gente.

3.1 El supuesto de “escasez”

Una de las salvaguardas de campaña fundamentales es asegurar que el acceso de los partidos políticos y los demás concursantes a los medios de comunicación tradicionales sea equitativo y justo, y que el reportaje por parte de los medios de comunicación públicos sea justo e imparcial.

La razón de ser de estas obligaciones (de imparcialidad, equidad, equilibrio e igualdad durante las elecciones) es el “supuesto de escasez”, es decir, el hecho de que existen pocas oportunidades de acceder a los medios de comunicación tradicionales. Se asume que esta “escasez” no aplicaría a los medios de comunicación en línea, teniendo en cuenta la facilidad y la variedad de las fuentes de opinión y el acceso a las mismas.

Sin embargo, este supuesto no tiene en cuenta la concentración del mercado en el campo de las comunicaciones digitales y la forma como la información se distribuye y se comparte en las plataformas digitales (en especial, los motores de búsqueda y las plataformas de redes sociales, incluidas las aplicaciones de mensajería)

Un pequeño grupo de grandes empresas de tecnología actúa como guardianes del contenido digital al que la mayoría de las personas tiene acceso en línea. Tal como señala el Supervisor Europeo de Protección de Datos, “el análisis de datos podría contribuir a que las personas naveguen un entorno informativo cada vez más ruidoso”, pero, “en efecto, el foro de discurso público y el espacio para la libertad de expresión hoy día son circunscritos por el afán de lucro de poderosas empresas privadas”.[51]

En particular, los motores de búsqueda y las plataformas de medios sociales filtran de acuerdo a perfiles las noticias y opiniones que los usuarios pueden acceder. La elaboración de perfiles se basa en el tratamiento de la información con el fin de evaluar, analizar y predecir datos personales, frecuentemente de maneras que los usuarios no comprenden (ver la sección 2.2.). Esto no se limita a la publicidad personalizada pagada y a la promoción de contenidos,[52] sino que incluye también la forma en que se muestran y recomiendan todos los contenidos.[53]

Estas técnicas de personalización basadas en datos hacen que las personas solo estén expuestas a ciertos mensajes políticos y a cierta información política, lo que contradice directamente el

[51] Supervisor Europeo de Protección de Datos, Opinion 3/2018 on online manipulation and personal data, 19 de marzo de 2018, https://edps.europa.eu/sites/edp/files/publication/18-03- 19_online_manipulation_en.pdf
[52] Ver, por ejemplo, la crítica del control que ejerce Facebook en la promoción de contenidos políticos en Hungría https://www.theguardian.com/world/2019/may/18/hungary-crucible-facebook- attempt-banish-fake-news
[53] Por ejemplo, la personalización de los resultados de búsquedas en Google https://www.google.com/search/howsearchworks/algorithms/; el feed de noticias de Facebook https://www.facebook.com/help/1155510281178725 o las recomendaciones de YouTube https://www.nytimes.com/2018/03/10/opinion/sunday/youtube-politics-radical.html

supuesto de que cualquier persona puede acceder fácilmente a un amplio espectro de opiniones y contenidos en los medios de comunicación en línea. Los efectos como las burbujas de filtro, etc. son consecuencias directas de la elaboración de perfiles y tienen consecuencias importantes en la formación de opiniones políticas y, en última instancia, en las elecciones.

Recomendaciones:

- Las plataformas de Internet y las redes sociales deben ser transparentes sobre sus actividades de elaboración de perfiles, incluso respecto a la personalización de lo que la gente ve. Esto es especialmente importante durante los periodos electorales.
- El uso de datos personales en la elaboración de perfiles, incluida la personalización del contenido, debe cumplir las normas de protección de datos.

Preguntas:

- ¿Las plataformas de redes sociales han adoptado compromisos concretos o cualquier medida en relación con la visualización de los contenidos en las próximas elecciones, como, por ejemplo, la transparencia en la publicidad?
- ¿Cuáles son las maneras en las que los actores políticos pueden llegar a los usuarios de su plataforma? ¿Cómo funcionan sus servicios de publicidad, elaboración de perfiles y personalización? ¿Quién tiene acceso a estos servicios?
- ¿Las plataformas cumplen la legislación nacional de protección de datos o alguna norma regional (por ejemplo, el RGPD)?
- ¿Las principales plataformas tienen una persona de contacto en el país? ¿Cuáles son los mecanismos disponibles para denunciar los abusos y atender las quejas?

3.2 Transparencia de la publicidad política en línea y la publicidad temática

Los partidos políticos y otros actores se enfocan en los votantes utilizando no solo los datos que ellos mismos recolectan (ver arriba, sección 2), sino también las herramientas que proporcionan las plataformas de redes sociales, para inferir más datos y expandir su alcance y enfocarse en otros individuos, por ejemplo, a través de públicos lookalike.[54] La plataformas de redes sociales, los partidos políticos y otros actores comparten la responsabilidad por la forma como se utilizan los datos personales para enfocarse en las personas.

La falta de transparencia y, en general, la falta de regulación adecuada de la publicidad política en línea se ha tornado en una de las principales preocupaciones en las elecciones.

Algunas iniciativas recientes de la Unión Europea[55] y de algunos Estados (por ejemplo, Canadá,[56] EE.UU.[57] e Irlanda[58]) han tratado de remediar esta falta de regulación imponiendo —o, tratándose del Código de Buenas Prácticas contra la Desinformación de la Comisión Europea, fomentando— obligaciones en materia de transparencia a los motores de búsqueda, los medios de comunicación social y otras empresas.

Aunque imperfectas, estas medidas de transparencia pueden mejorar la capacidad de los investigadores independientes y las organizaciones de la sociedad civil de monitorear el impacto de la publicidad política y la publicidad temática (issue ads) en las campañas electorales.[59] Los observadores electorales también podrían beneficiarse de esta transparencia cuando evalúen la participación en línea antes y durante las elecciones.

---

[54] En Alemania, el partido de extrema derecha AfD usó esta herramienta (https://www.bloomberg.com/news/articles/2017-09- 29/the-german-far-right-finds- friends-through-facebook)., lo que se explica más detalladamente en (https://policyreview.info/articles/analysis/role-digital-marketing-political-campaigns).

[55] Ver https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation

[56] Ver https://policyoptions.irpp.org/magazines/april-2019/learned-googles-political-ad-pullout/

[57] Ver la propuesta Honest Ads Act [Ley de Publicidad Honesta] https://www.congress.gov/bill/115th-congress/senate-bill/1989

[58] Ver Private Member's Bill, Online Advertising and Social Media (Transparency) Bill 2017, https://www.oireachtas.ie/en/bills/bill/2017/150/?tab=bill-text

[59] Ver, por ejemplo, https://newsroom.fb.com/news/2019/04/election-research-grants/, https://blog.mozilla.org/blog/2019/03/27/facebook-and-google-this-is-what-an-effective-ad-archive-api- looks-like/, https://blog.mozilla.org/blog/2019/04/29/facebooks-ad-archive-api-is-inadeq

Recomendaciones:

- Las leyes y normativas nacionales (por ejemplo, el código de prácticas) deben exigir que las empresas sean transparentes en relación con la publicidad y las comunicaciones políticas pagadas en línea.
- Las plataformas de Internet, incluidos los motores de búsqueda y las plataformas de redes sociales, debe deben revelar públicamente toda la publicidad, incluida la publicidad política y la publicidad temática política. La información debe incluir por lo menos los parámetros de personalización (audiencia destinataria, audiencia real, perfiles) y quién pagó por los anuncios.
- Las plataformas deben crear bibliotecas de publicidad política a las que puedan acceder los investigadores que cumplan los requisitos de privacidad, para que puedan rastrear y comprender mejor la propagación y el impacto de estos anuncios políticos y de la personalización utilizada.

Preguntas:

- ¿Cómo se definen y regulan en la ley la publicidad política en línea y la publicidad temática?
- ¿Las principales plataformas de Internet que operan en el país han desarrollado políticas de transparencia para los anuncios políticos y las otras comunicaciones políticas? ¿Y para la personalización?
- ¿Las principales plataformas de Internet que operan en el país han permitido que los investigadores de interés público puedan monitorear y revisar la publicidad en el período preelectoral?

Conclusiones

Las tecnologías digitales están cambiando la manera de celebrar elecciones y realizar campañas políticas. Ofrecen nuevas oportunidades para interactuar con los votantes y apoyar su participación en las elecciones y en los procesos democráticos. También plantean nuevas situaciones y desafíos para todos los actores electorales.

En particular, exigen la modificación de normas y prácticas para garantizar que las elecciones sean libres, justas y transparentes y que los actores que intervienen rindan cuentas. Debido al papel que desempeñan los datos en el entorno digital, la privacidad y la protección de datos, incluida la seguridad cibernética de los procesos electorales, son fundamentales para estas reformas.

Las organizaciones de observadores electorales han de desempeñar un papel fundamental a la hora de garantizar que las tecnologías digitales se utilicen de maneras que protejan y promuevan los derechos de los votantes y que, a la larga, apoyen la celebración de elecciones libres y justas. Para poder desempeñar su función con eficacia, deben revisar y actualizar las metodologías que utilizan para observar las elecciones, de modo que puedan detectar las inquietudes derivadas del uso de las tecnologías digitales y formular recomendaciones correctivas.

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

+44 (0)20 3422 4321

privacyinternational.org