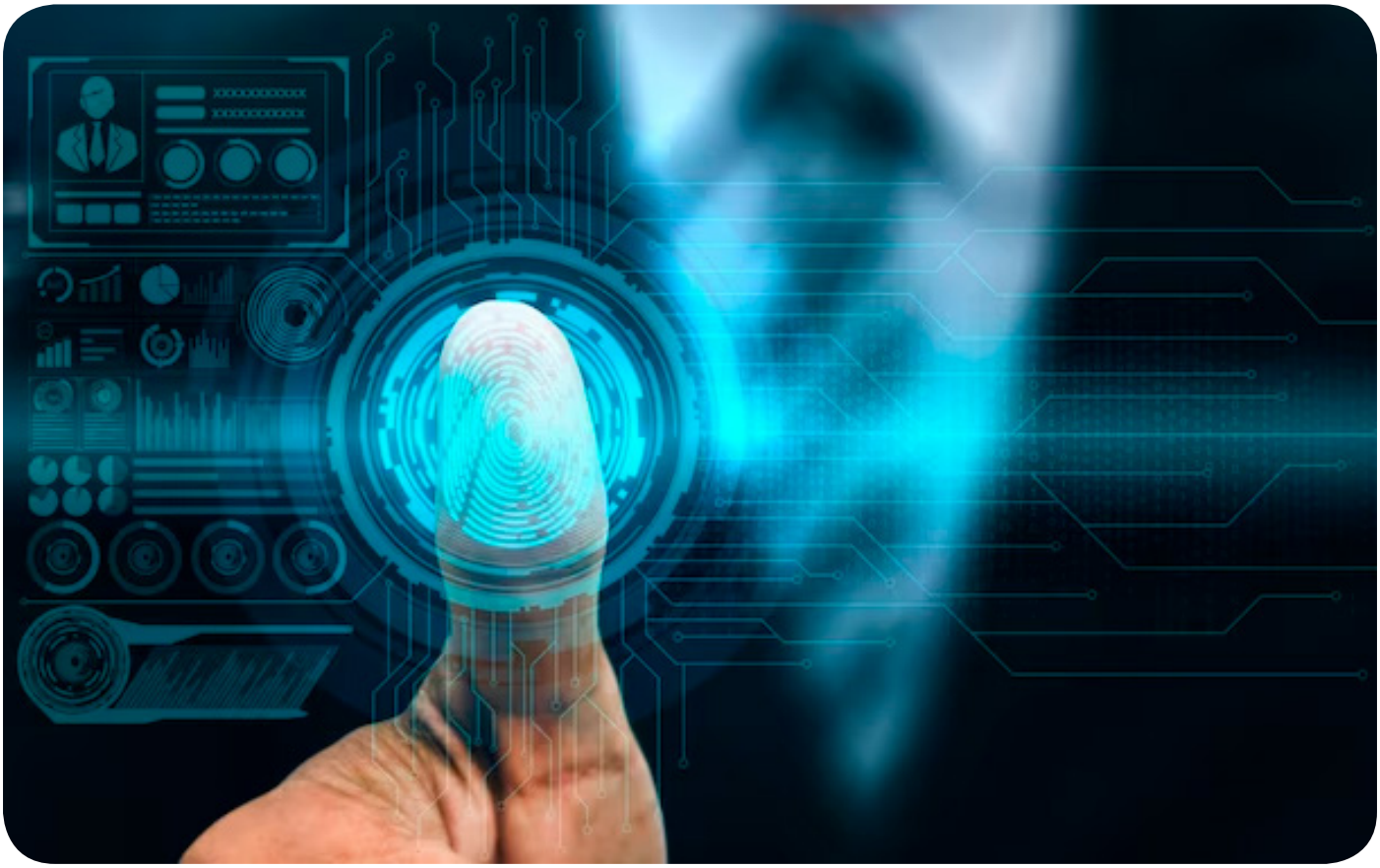

# El papel de la tecnología en las elecciones y la lucha por defender el derecho a la privacidad

## *Resumen del informe de la lista del ciclo electoral de Privacy International*



*Josie Thum*

Advocacy Officer en Privacy Internacional (PI). PI es una ONG con sede en Londres que trabaja a nivel mundial con socios para abogar por soluciones legales y tecnológicas para proteger a las personas y sus datos de la explotación por parte de gobiernos y empresas. Trabaja en proyectos que protegen el ciclo electoral, contrarrestando el autoritarismo y fiscalizando la vigilancia en las fronteras. Antes de unirse a PI, Josie fue investigadora senior en el Bahrain Institute for Rights and Democracy (BIRD), donde se centró en los derechos humanos en el Golfo, a saber, la pena de muerte, presos políticos y responsabilidad estatal y corporativa.

*Laura Lazaro Cabrera*

Senior Legal Officer en Privacy Internacional (PI). PI es una ONG con sede en Londres que trabaja a nivel mundial con socios para abogar por soluciones legales y tecnológicas para proteger a las personas y sus datos de la explotación por parte de gobiernos y empresas. Laura lidera el trabajo de PI en el ámbito electoral, además de investigar y litigar el uso opresivo de la tecnología por parte de actores estatales y privados. Antes de unirse a PI, Laura fue Litigation Fellow en la Open Society Justice Initiative, y fue Profesional Visitante en la Corte

La tecnología desempeña un papel central en el ecosistema democrático mundial, ya que los electores están cada vez más sujetos a las tecnologías digitales y de la información en cada etapa del proceso electoral. Nuestra creciente dependencia de la tecnología en el contexto de las elecciones plantea una serie de riesgos y desafíos únicos para la democracia moderna y la preservación de los derechos humanos y libertades fundamentales.

Muchas tecnologías que median el compromiso democrático hoy en día se basan en sistemas de explotación de datos ocultos que recopilan, almacenan y analizan información personal, y que plantean amenazas significativas para las elecciones libres y justas así como para los derechos humanos, incluido el derecho a la privacidad (Artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, PIDCP). Aunque pueden aportar beneficios innegables, el uso continuo y en expansión de las tecnologías digitales y de la información también aumenta los riesgos a los que se enfrenta una elección particular, incluida su vulnerabilidad a la manipulación y los ataques cibernéticos. Desde la publicidad política y las campañas electorales hasta la inscripción de los votantes, la tecnología se ha vuelto crucial para la celebración de elecciones en todo el mundo, lo que exige que los observadores electorales desarrollen nuevas metodologías y pericias para adaptarse al nuevo terreno democrático.

En respuesta a las preocupaciones planteadas por el uso de la tecnología en los procesos electorales, en 2019 Privacy International (PI) desarrolló una lista de verificación sobre tecnología,

*"En Argentina, tras las elecciones presidenciales en 2013, hubo una importante brecha de seguridad en el padrón electoral biométrico cuando se hizo disponible en línea, a pesar de avisos anteriores de vulnerabilidades en el sistema, que violaban el derecho a la privacidad de miles de personas cuyas fotos podrían haber sido descargadas. Eso fue todo sin que la gente siquiera supiera que sus fotos estaban en la base de datos, debido a que fueron subidas sin el conocimiento ni el consentimiento de los individuos."*

datos y elecciones para el uso de la sociedad civil y los observadores electorales, con el fin de asistir su labor y facilitar su evaluación del marco nacional y su idoneidad para proteger contra la explotación de los datos en el contexto electoral. Este artículo proporcionará un resumen general de la lista de verificación de PI, titulada "TECNOLOGÍA, DATOS Y ELECCIONES: Una lista del ciclo electoral", así como ciertos puntos claves a tener en consideración para identificar los principales riesgos que plantean el uso de datos y tecnología durante las elecciones y una serie de recomendaciones para ayudar a mitigar esos riesgos.[1]

**1. El derecho a la privacidad, el derecho a la libertad de expresión y opinión, y el derecho a la participación política: derechos intímamente vinculados**

Aunque el derecho a la privacidad es un derecho humano fundamental que está consagrado y protegido por una gran cantidad de disposiciones jurídicas internacionales vinculantes, los marcos jurídicos nacionales suelen estar desfasados y pobremente equipados para hacer frente a los problemas de protección de datos que plantea la evolución de los usos de los datos y la tecnología en las elecciones. La importancia del derecho a la privacidad se refleja a nivel nacional en 137 países que han adoptado leyes de protección de datos, y a nivel regional en las Américas donde el 74% de los países han hecho lo mismo.[2] Sin embargo, esas normas suelen verse rápidamente desactualizadas frente al avance de la tecnología, no abarcan todos los temas o carecen de mecanismos independientes de monitoreo y reparación.

Además, el derecho a la privacidad es un derecho habilitador que permite el goce de otros derechos humanos, en particular del derecho a la libertad de expresión y de opinión (Artículo 19 del PIDCP) y el derecho a la participación política (Artículo 25 del PIDCP), y un marco legal sólido que refleje esto es fundamental.

De hecho, el derecho a la participación política ha sido interpretado por el Comité de Derechos Humanos de las ONU acuerdo con el Artículo 25 del PIDCP, cuando declara que los "electores [...] deberán poder formarse una opinión de manera independiente, libres de toda violencia, amenaza de violencia, presión o manipulación de cualquier tipo".[3] Algunas de las técnicas basadas en enormes cantidades de datos desplegadas durante las campañas políticas en torno a las elecciones, como la elaboración de perfiles o profiling, y la microfocalización, o micro-targeting, pueden amenazar nuestro derecho a formar una opinión y a ser informado.

PI observó tal amenaza en las elecciones presidenciales de Kenia de 2017, donde surgieron informes que los votantes recibieron mensajes de texto no solicitados de candidatos políticos, los cuales hacían referencia a información personal, como el distrito electoral y la mesa de votación, dando lugar a serias preocupaciones de que la base de datos biométrica nacional de votantes se compartiera con terceros sin el consentimiento de las personas.[4] En 2019, Kenia aprobó una Ley de Protección de Datos, mejorando la legislación para proteger los datos personales y el derecho a la privacidad de sus electores. Otro ejemplo de este tipo de amenaza surgió en las elecciones presidenciales de Estados Unidos de 2016, donde la campaña de Trump colocó a 3,5 millones de ciudadanos afroamericanos en categorías digitales de disuasión, para luego someterlos a una microfocalización a través de publicidades políticas altamente personalizadas con el fin de disuadirlos de votar en estados claves, donde finalmente, Trump ganó con mayorías ínfimas.[5]

**2. Los retos relacionados a la inscripción de votantes y el uso de datos biométricos en padrones electorales**

El registro biométrico de votantes (BVR, por sus siglas en inglés) involucra la recolección de datos biométricos de individuos para alimentar la base de datos nacional de registro de votantes, o padrón electoral. El BVR puede ser utilizado para deduplicar la lista de votantes y/o verificar la identidad de un votante cuando acude a la mesa de votación. Los datos biométricos,[6] al ser datos basados en características fisiológicas únicas permitiendo identificar a una persona, son especialmente sensibles y por ende su tratamiento requiere salvaguardias complementarias por ley.[7]

Los BVR conllevan riesgos inherentes a la seguridad y privacidad en la medida que se apoyan en una base de datos electrónica centralizada que concentra la información biométrica de toda la población inscripta en el padrón electoral.

Por ejemplo, en Argentina, tras las elecciones presidenciales en 2013, hubo una importante brecha de seguridad en el padrón electoral biométrico cuando se hizo disponible en línea, a pesar de avisos anteriores de vulnerabilidades en el sistema, que violaban el derecho a la privacidad de miles de personas cuyas fotos podrían haber sido descargadas. Eso fue todo sin que la gente siquiera supiera que sus fotos estaban en la base de datos, debido a que fueron subidas sin el conocimiento ni el consentimiento de los individuos.[8] Otro ejemplo tuvo lugar en Filipinas, cuando los datos de más de 55 millones de votantes registrados se filtraron tras una brecha de seguridad que permitió el acceso a la base de datos de la Comisión Electoral en marzo de 2016.[9] Los datos personales y sensibles de la población se vieron comprometidos debido a lo que la autoridad nacional de protección de datos identificó como "falta de una política clara de gobernanza de datos, en particular en la recopilación y posterior procesamiento de datos personales [...] vulnerabilidades en el sitio web, y la falta de un seguimiento regular de la seguridad".[10]

Para evitar la filtración o uso indebido de datos sensibles, el procesamiento y acceso a la información contenida en un BVR debe gozar de sólidas salvaguardias jurídicas que impidan su utilización para cualquier otro fin que no sea el estipulado por la ley. En las elecciones presidenciales de Kenia en 2022, el órgano de gestión electoral anunció que el registro de votantes estaría a la venta por un precio mínimo.[11] PI recomienda que ningún tercero tenga acceso a los datos biométricos contenidos

1 Privacy International (2019) *TECNOLOGÍA, DATOS Y ELECCIONES: Una lista del ciclo electoral*, disponible en: <https://www.privacyinternational.org/sites/default/files/2022-12/PI%20Tecnologia%2C%20datos%20y%20elecciones%20lista%2032%20page%20June%202019%20SPANISH.pdf>.
2 Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (2021) *Data Protection and Privacy Legislation Worldwide*, disponible en: <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>.
3 Ver Comité de Derechos Humanos, observación general 25.
4 Privacy International (2019) *TECNOLOGÍA, DATOS Y ELECCIONES: Una lista del ciclo electoral*, disponible en: <https://www.privacyinternational.org/sites/default/files/2022-12/PI%20Tecnologia%2C%20datos%20y%20elecciones%20lista%2032%20page%20June%202019%20SPANISH.pdf>.
5 Channel 4 News (2020) *Revealed: Trump campaign strategy to deter millions of Black Americans from voting in 2016*, disponible en: <https://www.channel4.com/news/revealed-trump-campaign-strategy-to-deter-millions-of-black-americans-from-voting-in-2016>.
6 Los datos biométricos incluyen huellas dactilares, y características permitiendo el reconocimiento facial, por ejemplo la configuración del rostro, la retina y el iris.
7 Alto Comisionado de las Naciones Unidas para los Derechos Humanos (3 August 2018) *Informe A/HRC/39/29*, disponible en: <https://undocs.org/A/HRC/39/29>.
8 Privacy International (2013) *Ignoring repeated warnings, Argentina biometrics database leaks personal data*, disponible en: <https://privacyinternational.org/news-analysis/1566/ignoring-repeated-warnings-argentina-biometrics-database-leaks-personal-data>.
9 Privacy International (2019) State of Privacy in the Philipppines, disponible en: <https://www.privacyinternational.org/state-privacy/1009/state-privacy-philippines>.
10 Foundation for Media Alternatives (2016) *National Privacy Commission to issue findings on Comelec breach*, disponible en: <https://fma.ph/2016/09/08/national-privacy-commission-to-issue-findings-on-comelec-breach/>.
11 Privacy International (2023) *Our final report on Kenya's 2022 election in collaboration with The Carter Center Election Expert Mission*, disponible en: <https://privacyinternational.org/long-read/5053/our-final-report-kenyas-2022-election-collaboration-carter-center-election-expert>.

en los registros de votantes y que los procesos de registro de votantes se estipulen en la ley. Asimismo, el padrón electoral no debe incluir datos personales más allá de los que se necesiten para acreditar la satisfacción de los requisitos para votar.

Aún cuando el manejo del padrón electoral está en manos del órgano de gestión electoral, existen riegos de uso indebido y manipulación. La inscripción de los votantes, biométrico o de otro modo, se basa en una forma de verificación de la identidad de una persona contra un registro de las personas con derecho a voto. una vez más observó las elecciones en Kenia en 2022 junto con The Carter Centre, y encontró que una auditoría del padrón electoral biométrico identificó una serie de vulnerabilidades en el padrón, incluida una tendencia de transferencias de votantes "anormal", cambios tardíos e inesperados de la mesa electoral asignada a algunos votantes, sin su conocimiento o consentimiento. Tres funcionarios del órgano de gestión electoral de Kenia fueron detenidos y luego suspendidos en relación con la transferencia ilegal de votos.[12]

### 3. Los desafíos de la microfocalización política y 'profiling' en línea

Un ámbito clave que requiere una regulación sólida es la conducta de los partidos políticos y otros actores políticos, ya que el rápido desarrollo de las campañas políticas en línea significa que sobrepasan los marcos normativos actuales. El creciente uso de las comunicaciones digitales y las redes sociales en las campañas políticas, así como de una amplia gama de técnicas de uso intensivo de datos, facilita la elaboración de perfiles individuales y microfocalizar a los votantes potenciales, a su vez amenazando sus derechos a la privacidad y la libertad de opinión, un riesgo que se materializó a través del escándalo de Cambridge Analytica.

Las campañas políticas se basan cada vez más en el uso de datos personales para elaborar perfiles a las personas en línea y dirigirlas con información y mensajería altamente personalizadas, lo que representa una amenaza al derecho humano fundamental a la libertad de opinión como ha sido reconocido por la Relatora Especial sobre la libertad de expresión y opinión de la ONU.[13] Esta técnica de personalización es posible mediante la amplia recopilación de datos personales, cuyo análisis convierte a esos datos en inteligencia política. Esta inteligencia se amalgama entonces en bases de datos que sirven para alimentar las estrategias de campaña y sus objetivos finales de exigir influencia política. La elaboración de perfiles permite inferir o predecir información sobre un individuo o grupos de individuos, incluidos sus intereses, preferencias personales, situación económica, creencias políticas o religiosas, etc. Esta información puede utilizarse para elaborar perfiles detallados que sirvan de base a las decisiones de personalizar el entorno en línea de una persona, y estos perfiles pueden ser compartidos y vendidos entre múltiples actores sin el conocimiento ni el consentimiento del individuo. A su vez, la elaboración de perfiles reforza las técnicas de personalización basadas en datos que pueden utilizarse durante las campañas políticas en el contexto de las elecciones, como la microfocalización (que permite a las personas recibir información personalizada basada en su perfil) o el geoperimetraje (cuando los individuos son atacados en base a su ubicación). Por ejemplo, en 2021 se presentaron más de 200 quejas a la Oficina del Comisionado de Protección de Datos de Kenia después de que personas fueron registrados como miembros de partidos políticos sin su conocimiento o consentimiento, con un incidente parecido habiendo ocurrido en el país en 2017. Las quejas dieron lugar a la aplicación de salvaguardias y mecanismos de consentimiento adicionales.[14]

Estas sofisticadas técnicas de personalización basadas en datos tienen como objetivo influenciar las opiniones y acciones de los votantes, así como las de los donantes potenciales. Con el fin de evitar el abuso de datos personales, que puede socavar gravemente el proceso democrático y violar los derechos humanos de los votantes, es crucial que las leyes de protección de datos se apliquen al procesamiento de datos personales por los actores políticos. A su vez, los propios partidos políticos deben ser transparentes sobre sus actividades de procesamiento de datos, tener políticas de protección de datos y llevar a cabo auditorías de protección de datos y evaluaciones de impacto. De hecho, en 2020 el Relator Especial de las Naciones Unidas para la Libertad de Opinión y de Expresión y el Relator Especial para la Libertad de Expresión de la Organización de los Estados Americanos firmaron una declaración conjunta que llamó a actores privados digitales a adoptar medidas de transparencia con respecto a herramientas automizadas, "*sobre todo aquellos relacionados con elecciones*". La declaración también expresó alarma "*por el uso indebido de las redes sociales, por parte de actores estatales y privados, para subvertir los procesos electorales, incluso a través de diversas formas de comportamiento no auténtico y el uso de "propaganda computacional" (emplear herramientas automatizadas para influir sobre el comportamiento)*" y estipuló que "*Los medios y las plataformas digitales deberían hacer esfuerzos suficientes para adoptar medidas que posibiliten a los usuarios acceder a diversas ideas y perspectivas políticas. En particular, deberían cerciorarse de que las herramientas automáticas, como los algoritmos de clasificación, no obstaculicen indebidamente —sea o no de manera intencional— el acceso a contenidos relacionados con elecciones y la disponibilidad de diversos puntos de vista para los usuarios".*[15]

El Consejo de Europa ha declarado en sus directrices de 2022 sobre comunicación electoral y cobertura de los medios de comunicación que: "*Los Estados deben considerar las implicaciones de la publicidad política dirigida o microdirigida para el comportamiento electoral de los ciudadanos y, en este contexto, su acceso a la información y su exposición a puntos de vista políticamente diversos y su derecho a expresar libremente sus opiniones y elecciones políticas*" y que los estados deben exigir a las plataformas en línea que creen herramientas de exclusión para la publicidad política.[16]

Para ayudar a mitigar algunos de los riesgos significativos asociados con las técnicas de personalización basadas en datos empleadas por los partidos políticos (y otros actores políticos), la transparencia es esencial. El informe de PI recomienda que se informe a los votantes sobre por qué reciben un mensaje en línea y quién es responsable de él, mientras que los partidos políticos deben garantizar que el público pueda reconocer fácilmente las comunicaciones que vienen de ellos. Deben publicar información sobre cualquier criterio de personalización utilizado y hacer transparente lo que se contrata a terceros para procesar datos y participar en la elaboración de perfiles, tales como

> *"El supuesto de 'escasez' es la base de una salvaguarda tradicional de campaña política que asegura que los partidos tengan acceso equitativo y justo a los medios de comunicación, y que el reportaje por los medios de comunicación pública sea imparcial. Sin embargo, el supuesto de escasez no tiene en cuenta las formas en que la información se distribuye y comparte en las plataformas digitales, donde los motores de búsqueda y las plataformas de medios sociales median a qué contenido están expuestos los individuos, que conduce a las burbujas de filtro, como mensajes políticos seleccionados e información es favorecida por ciertas audiencias."*

12 Ibid.
13 Privacy International (2021) *The UN Report on Disinformation: a role for privacy,* disponible en: <https://privacyinternational.org/news-analysis/4515/un-report-disinformation-role-privacy>.
14 Privacy International (2023) *Our final report on Kenya's 2022 election in collaboration with The Carter Center Election Expert Mission*, disponible en: <https://privacyinternational.org/long-read/5053/our-final-report-kenyas-2022-election-collaboration-carter-center-election-expert>.
15 Relator Especial de las Naciones Unidas para la Libertad de Opinión y de Expresión, el Representante para la Libertad de los Medios de Comunicación de la Organización para la Seguridad y la Cooperación en Europa y el Relator Especial para la Libertad de Expresión de la Organización de los Estados Americanos (2020) *Declaración conjunta sobre libertad de expresión y elecciones en la era digital*, disponible en: < https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=1174&lID=2>.
16 Consejo de Europa (2022) *Recommendation CM/Rec(2022)12 of the Committee of Ministers to member States on electoral communication and media coverage of election campaigns,* disponible en: <https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a6172e>.

corredores de datos y las compañías de publicidad política, así como proporcionar desgloses transparentes de los gastos de campaña.

**4. La escasa información y monitoreo de la publicidad política en línea**

La difusión de la desinformación y su potencial para socavar la democracia ha recibido especial atención en los últimos años. El supuesto de 'escasez' es la base de una salvaguarda tradicional de campaña política que asegura que los partidos tengan acceso equitativo y justo a los medios de comunicación, y que el reportaje por los medios de comunicación pública sea imparcial. Sin embargo, el supuesto de escasez no tiene en cuenta las formas en que la información se distribuye y comparte en las plataformas digitales, donde los motores de búsqueda y las plataformas de medios sociales median a qué contenido están expuestos los individuos, que conduce a las burbujas de filtro, como mensajes políticos seleccionados e información es favorecida por ciertas audiencias. Esto puede conducir a la manipulación, la propagación de la desinformación y la amplificación de la polarización política y otras divisiones sociales.

Está claro que la publicidad política en línea durante las elecciones necesita urgentemente de regulaciones más fuertes y una mayor transparencia, y tanto las plataformas de redes sociales así como los actores políticos y entes reguladores comparten esta responsabilidad. Algunos estados como Canadá,[17] los Estados Unidos[18] e Irlanda[19] han reconocido formalmente esta responsabilidad y han adoptado medidas para imponer obligaciones de transparencia a los motores de búsqueda y las empresas de redes sociales. Además, las directrices del Consejo de Europa de 2022 sobre comunicación electoral y cobertura de los medios de comunicación de las elecciones, establecen que: "*la publicidad política en línea, incluida la publicidad basada en temas específicos, debe ser transparente*" y los anuncios políticos deben estar "*claramente marcados*".[20] Esas medidas de transparencia pueden permitir que investigadores independientes, la sociedad civil y los observadores electorales monitoreen mejor el impacto de la publicidad política. PI recomienda que las leyes y normas nacionales deben exigir que las empresas sean transparentes en relación con la publicidad y las comunicaciones políticas en línea, y que las plataformas de Internet - incluidos los motores de búsqueda y las plataformas de redes sociales - deben divulgar públicamente toda la publicidad, así como establecer bibliotecas de publicidad política.

**5. El papel de los reguladores en el manejo de las violaciones de datos**

La participación de las personas en procesos democráticos como las elecciones es un vector del ejercicio de sus derechos humanos fundamentales a la participación política y la libertad de opinión, y, por lo tanto, los estados están obligados a proporcionarles un recurso efectivo frente a potenciales vulneraciones. Al transformarse el paisaje electoral a través de una mayor digitalización, es esencial potenciar las facultades de órganos reguladores para que puedan identificar, prevenir y mitigar riesgos.

*Capacitación de órganos de administración electoral*
Cuando se trata de emitir un voto en las urnas, o remotamente, la creciente dependencia de las tecnologías digitales en este momento clave de la participación democrática presenta riesgos de que se abuse de las tecnologías implicadas. Esto incluye los sistemas de voto electrónico, que pueden conectarse al internet u otras redes informáticas. Es esencial que los Órganos de Administración Electoral (EMB, por sus siglas en inglés) cuenten con el conocimiento técnico necesario para evaluar estas tecnologías y cómo procesan la información, a fin de garantizar la imparcialidad, eficacia y transparencia de las elecciones. Todos los países son susceptibles a los riesgos planteados por las tecnologías incorporadas en los mecanismos democráticos. En Suiza, por ejemplo, el despliegue del voto electrónico fue interrumpido después que investigadores encontrasen fallas técnicas en el sistema de voto electrónico que podrían permitir que intrusos sustituyeran los votos legítimos por votos fraudulentos.[21]

*Cooperación entre órganos reguladores*
Es importante aumentar la cooperación entre los reguladores electorales, ya que les permite identificar y responder mejor a las violaciones de datos y a las leyes de protección de datos; algo reconocido por el Parlamento Europeo en 2018, cuando se introdujeron nuevas normas para proporcionar un mecanismo para que las Autoridades de Protección de Datos (APD) cooperen mejor con otras autoridades frente a las violaciones de datos.[22] Por lo tanto, el informe de PI recomienda que los EMB deben desarrollar su pericia en materia de protección de datos y ciberseguridad y colaboren eficazmente con las autoridades de ámbitos conexos, como las APD. El informe aclara además que estos reguladores electorales y de datos deben establecer mecanismos independientes de reclamaciones para tratar los casos de supuestas violaciones de datos y garantizar la rendición de cuentas. Lo ideal sería establecer una APD independiente a nivel nacional con capacidad de recibir quejas sobre el uso indebido de datos personales durante las elecciones.

*Facultad de recibir y responder a quejas relativas a las elecciones, los datos y tecnología*
Los EMB o las autoridades reguladoras independientes también deben estar facultadas para recibir quejas de individuos y organizaciones y aplicar reformas basadas en dichas quejas. Esos mecanismos de reclamación deberían proporcionar una vía de recurso judicial para las presuntas violaciones de la protección de datos durante las elecciones. Al evaluar un marco nacional determinado, los observadores electorales pueden tener en cuenta los mecanismos de reparación disponibles y las soluciones que ofrecen cuando se trata de violaciones de la protección de datos. Un ejemplo de tal mecanismo en acción es en el Reino Unido, donde 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 del 'Brexit' de la Unión Europea celebrado en 2016.[23]

PI cree que los observadores electorales internacionales están idealmente situados para abordar algunos de los desafíos más importantes que la tecnología presenta para la defensa de los principios democráticos en los procesos electorales mundiales. Para ello, los observadores electorales deben tener cada vez más en cuenta el papel de los datos personales, lo que requiere metodologías actualizadas y la adquisición de nuevos conocimientos; su papel será importante para garantizar que la digitalización apoye, en lugar de socavar, elecciones libres, transparentes y justas.

17 Dubois, McKelvey y Owen (2019) *What have we learned from Google's political ad pullout?,* Institute for Research on Public Policy, disponible en: <https://policyoptions.irpp.org/magazines/april-2019/learned-googles-political-ad-pullout/>.
18 Congreso de los Estados Unidos (2017) *S.1989 - Honest Ads Act,* disponible en: <https://www.congress.gov/bill/115th-congress/senate-bill/1989>
19 Houses of the Oíreachtais (2017) *Online Advertising and Social Media (Transparency) Bill 2017*, disponible en: <https://www.oireachtas.ie/en/bills/bill/2017/150/?tab=bill-text>.
20 Consejo de Europa (2022) *Recommendation CM/Rec(2022)12 of the Committee of Ministers to member States on electoral communication and media coverage of election campaigns,* disponible en: <https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a6172e>.
21 Privacy International (2019) *TECNOLOGÍA, DATOS Y ELECCIONES: Una lista del ciclo electoral,* disponible en: <https://www.privacyinternational.org/sites/default/files/2022-12/PI%20Tecnologia%2C%20datos%20y%20elecciones%20lista%2032%20page%20June%202019%20SPANISH.pdf>.
22 Comisión Europeo (2018) "What has the European Commission done?" en *Democracy and electoral rights*, disponible en: <https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/eu-citizenship/democracy-and-electoral-rights_en
23 Privacy International (2019) *TECNOLOGÍA, DATOS Y ELECCIONES: Una lista del ciclo electoral,* disponible en: <https://www.privacyinternational.org/sites/default/files/2022-12/PI%20Tecnologia%2C%20datos%20y%20elecciones%20lista%2032%20page%20June%202019%20SPANISH.pdf>.