TECNOLOGÍA, DATOS Y ELECCIONES:
Lista de verificación del ciclo electoral

Noviembre de 2023

privacyinternational.org

ACERCA DE PRIVACY INTERNATIONAL

Los gobiernos y las empresas están usando la tecnología para explotarnos. Sus abusos de poder amenazan nuestras libertades y aquello que nos hace humanos. Esta es la razón por la que Privacy International promueve el progreso que todos nos merecemos. Actuamos para proteger la democracia, defender la dignidad de las personas y exigir la responsabilidad y la rendición de cuentas de cuentas de las poderosas instituciones que violan la confianza pública. Al fin y al cabo, la privacidad es sumamente valiosa para cada uno de nosotros, sin importar si estamos pidiendo asilo, luchando contra la corrupción o buscando orientación médica.
Así que únase a nuestro movimiento mundial y luche por lo que realmente importa: nuestra libertad de ser humanos.

Privacy International

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

Privacy International es una organización benéfica registrada (1147471) y una asociación de responsabilidad limitada registrada en Inglaterra y Gales (04354366).

Imagen de la portada: Foto de Kvistholt Photography en Unsplash

Introducción

Desde hace algunos años, el tema de los datos en las elecciones ha cobrado mayor visibilidad e importancia. Hoy más que nunca, se ha tomado conciencia del papel crucial que pueden llegar a desempeñar los datos en los procesos electorales y de la gran variedad de actores que intervienen en las actividades de tratamiento de datos.

La capacidad de aprovechar y analizar inmensas cantidades de datos personales ha replanteado las campañas políticas y ha hecho posible la proliferación de publicidad política diseñada específicamente para públicos que comparten características concretas o para una única persona. Estas nuevas prácticas, sumadas a las plataformas que las hacen posibles, crean un entorno que facilita manipular la opinión y, en algunos casos, excluir a los votantes.

Al mismo tiempo, varios Estados están recurriendo a la tecnología biométrica para registrar y verificar a los votantes, con el objetivo de reducir el fraude y la manipulación de votos. A raíz de la modernización de la infraestructura electoral, es frecuente que surjan bases de datos de alcance nacional que albergan enormes cantidades de información personal y sensible, la cual requiere mayores salvaguardas y protección. Es común que la creciente dependencia del uso de tecnologías para registrar y verificar a los votantes vaya de la mano de la participación de la empresa privada, una costosa inversión que no está exenta de riesgos.

Este nuevo panorama electoral trae muchos retos que deben enfrentarse para proteger la libertad y la imparcialidad de las elecciones: un hecho que reconocen cada vez más los responsables políticos y los organismos reguladores. En los últimos años, esto ha generado una oleada de iniciativas de regulación que buscan garantizar la transparencia, la rendición de cuentas y el uso ético de los datos en las actividades electorales. Tales iniciativas abarcan desde investigaciones y la publicación de directrices por organismos internacionales y nacionales hasta la adopción de nuevas normas destinadas a limitar el uso de datos con fines de campaña política. A pesar de estas iniciativas, todavía existen muchas jurisdicciones donde aún no ha sido regulado el uso de datos en el contexto electoral.

Este entorno tan complejo y cambiante exige que expertos y observadores examinen la relación entre los datos, la tecnología y las elecciones. Los observadores electorales pueden cumplir un rol fundamental a la hora de reducir la brecha de conocimiento que a menudo existe entre el público y los funcionarios del gobierno de cara a esta relación, fortaleciendo así la confianza de los votantes en el proceso electoral al brindar una valoración independiente, imparcial y experta de todos los aspectos relevantes del mismo. Al incorporar metodologías que tienen en cuenta el papel de las tecnologías y los datos en las elecciones, los observadores pueden ofrecer recomendaciones sobre cómo respetar y proteger con eficacia la privacidad a lo largo de todo el ciclo electoral.

La finalidad de la actualización de la lista de verificación sobre datos y elecciones es ofrecer a los observadores electorales y a cualquier integrante de la sociedad civil interesado las herramientas necesarias para examinar y abordar algunos de los aspectos más complejos y problemáticos del proceso electoral en cuanto a los datos y la tecnología.

Mediante esta lista de verificación, Privacy International identifica las principales áreas en las que la tecnología y el tratamiento de datos personales convergen y cumplen un papel clave en el proceso electoral. El documento está estructurado siguiendo las metodologías desarrolladas por las organizaciones de observadores electorales. Cada sección ofrece una breve descripción del asunto en cuestión, recomendaciones de políticas y preguntas claves que podrían servir a los observadores para evaluar si el marco nacional es adecuado para salvaguardar contra la explotación de los datos en el proceso electoral. Estas preguntas han sido concebidas como un punto de partida para el análisis.

La primera parte se ocupa del marco jurídico general y de la normativa relacionada tanto con la gestión de las elecciones como con el rol que desempeñan terceros en el suministro o la gestión de la tecnología electoral (padrón electoral, votación, función de la entidad responsable de la gestión electoral y de las empresas privadas). La segunda parte examina la regulación de los partidos y otros actores políticos (incluida la financiación y las campañas políticas). La tercera parte se centra en el papel de las plataformas en línea, especialmente los motores de búsqueda y las plataformas de medios sociales, en el contexto de las elecciones (con especial atención a la transparencia de la publicidad política).

Parte 1 - Gestión de las elecciones

1.1 Marco jurídico – protección del derecho a la privacidad en el proceso electoral

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.

Como ha señalado el Consejo de Europa, la protección de la privacidad en las campañas políticas es fundamental para la celebración de elecciones imparciales y libres.[1] En este contexto, se entiende que el derecho a la privacidad garantiza la libre expresión de la ciudadanía, la representatividad adecuada de los representantes electos y la legitimidad de los órganos legislativos y ejecutivos, al tiempo que fortalece la confianza de la población en las instituciones.[2]

La protección de la información personal está indisolublemente ligada al derecho a la privacidad, como señaló el Consejo de Derechos Humanos de la ONU en octubre de 2023.[3] Las directrices sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales por y para las campañas políticas, adoptadas por el Consejo de Europa en noviembre de 2021, observan que "dado que en la mayoría de los países las elecciones están cada vez más 'basadas en datos', es fundamental que todas las organizaciones que participen en las campañas políticas traten los datos personales de los votantes de acuerdo con principios de protección de datos firmemente establecidos".[4]

[1] Introducción, Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns.
[2] Ibid.
[3] U.N. Doc. A/HRC/54/L.12/Rev.1, 9 de octubre de 2023.
[4] Introducción, Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns

La Comisión Europea y el Consejo de Europa señalan, respectivamente, que la protección de datos es necesaria para la resiliencia democrática[5] y que la aplicación de principios sólidos de protección de datos contribuye a fortalecer la integridad de las elecciones y a conservar la confianza en la democracia en la era digital.[6]

A la fecha, 137 países en el mundo han promulgado leyes de protección de datos.[7] Sin embargo, a menudo estas normas están desactualizadas, no son exhaustivas (en particular, suelen excluir el tratamiento de datos personales por parte de las autoridades públicas) y carecen de mecanismos independientes de monitoreo y reparación.[8] La normativa de protección de datos también puede incluir exenciones para los partidos políticos que podrían facilitar la explotación de datos durante las campañas políticas.[9] Estas normas deben examinarse y actualizarse en la medida de lo necesario.

El derecho a la privacidad es también 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 interferencias indebidas.

De acuerdo con la interpretación del Comité de Derechos Humanos de la ONU del derecho a la participación política según el artículo 25 del PIDCP, los "electores... deberán poder formarse una opinión de manera independiente, libres de toda violencia, amenaza de violencia, presión o manipulación de cualquier tipo". La Relatora Especial de la ONU sobre la promoción y protección del derecho a la libertad de opinión y de expresión ha ido un paso más allá, señalando que hay una preocupación realista de que la recopilación sistemática de datos sobre las actividades que desarrollan los usuarios en línea y la publicidad personalizada puedan violar su derecho a la libertad de opinión conforme el artículo 19 del PIDCP.[10] En particular, afirma que técnicas como la moderación de contenidos y la microfocalizacion cumplen un papel importante en la propagación de la desinformación y, al manipular de forma involuntaria o no consentida los procesos de pensamiento, contravienen el derecho a la libertad de opinión.[11]

Recomendaciones

- La legislación nacional, idealmente la constitución, debe reconocer el derecho a la privacidad (incluida la protección de datos personales);

[5] Veáse https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0638
[6] Introducción, Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns
[7] A fecha de octubre de 2020, véase Data Protection and Privacy Legislation Worldwide, disponible en: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide
[8] Privacy International tiene una guía sobre legislación en materia de protección de datos, en la que se recogen las normas internacionales y regionales pertinentes, así como las mejores prácticas: https://privacyinternational.org/data-protection-guide
[9] Véase https://privacyinternational.org/news-analysis/2836/gdpr-loopholes-facilitate-data-exploitation-political-parties
[10] U.N. Doc. A/HRC/47/25, párr. 66, 13 de abril de 2021. Disponible en: https://www.ohchr.org/en/calls-for-input/report-disinformation
[11] Ibid., párr. 36.

- Debe existir una ley de protección de datos moderna y completa, que contemple una autoridad de protección de datos independiente y dotada de recursos suficientes, con competencias para investigar, recibir denuncias e imponer sanciones. La ley debe ser examinada 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.
- La autoridad nacional de protección de datos debe publicar un código de prácticas o su equivalente, o al menos unas directrices sobre el uso de datos personales en el proceso electoral, subrayando las obligaciones en materia de protección de datos de todos los actores implicados en el proceso electoral, incluidas las campañas políticas.

Preguntas

- ¿La constitución u otra normativa protege el derecho a la privacidad, incluida la protección de datos personales?
- ¿Existe una normativa moderna y completa sobre la protección de datos? ¿Contempla el tratamiento de datos personales por parte de las autoridades públicas?
    - ¿Tiene excepciones para los partidos políticos u otros actores de la campaña?
    - ¿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?
    - Las directrices o el marco de protección de datos que aplica a las actividades políticas:
        - ¿Incluye una definición amplia de campaña política?
        - ¿Aplica no solo a los partidos políticos, sino también a otros actores importantes, como la entidad de gestión electoral, las plataformas y los agentes de datos?
        - ¿Interpreta los datos personales en sentido amplio, para incluir lo que se deriva, se infiere y se predice (como resultado de la elaboración de perfiles)?

1.2. Padrón electoral

Los registros de votantes son necesarios para que las elecciones funcionen eficazmente. Su propósito es garantizar y permitir que únicamente voten las personas con derecho a voto. Por consiguiente, se sustentan en verificar de alguna manera la identidad de una persona al cotejarla en un censo o un padrón electoral. Únicamente se deben registrar los datos personales 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 políticos puedan acceder al padrón electoral para garantizar la imparcialidad del proceso electoral y para contactar a posibles votantes, pero esto no debe derivar en un acceso sin restricciones. Por último, incluso en los casos en que los datos personales contenidos en el registro individual sean publicados, el uso de tales datos personales debe estar sujeto a salvaguardas de protección de datos.

Aunque la manera en que se elabora el padrón electoral varía de un país a otro, es cada vez más común que los gobiernos generen bases de datos centralizadas que almacenan una gran variedad de datos personales sobre los votantes, incluidos, a veces, datos biométricos. Hoy día es común que los datos de la inscripción de votantes sean almacenados en una base de datos electrónica central. Aunque esto presenta ventajas, especialmente en relación con una mayor transparencia y el acceso y la divulgación responsables de los datos, los padrones 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 socavar los procesos democráticos que pretenden apoyar.

En primer lugar, los datos personales 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. Esta problemática también es tratada en el la sección 2.2.

En Kenia, durante las elecciones presidenciales de 2017, hubo reportes de que kenianos recibieron mensajes de texto no solicitados de candidatos políticos que pedían al destinatario que votara por su candidatura.[12] Los mensajes mencionaban información personalizada del votante, como el distrito electoral y el centro de votación, que había sido obtenida del padrón electoral biométrico de Kenia. Persisten dudas de si la comisión electoral de Kenia (IEBC, por sus siglas en inglés) compartió la base de datos con terceros sin el consentimiento de los votantes y de si las empresas de telecomunicaciones compartieron la información de los suscriptores, también sin su consentimiento, para permitir esta microfocalización.

No queda claro con quién se compartió la base de datos de votantes y, por lo tanto, qué empresa, si la hubo, es responsable de la microfocalización. Estas mismas preocupaciones afloraron nuevamente en los comicios de 2022, cuando el IEBC anunció la venta del padrón electoral a cambio de una "tarifa".[13]

En segundo lugar, aunque los partidos políticos tienen un interés legítimo en acceder a los datos personales almacenados 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 para qué finalidad.[14]

En algunos países hay dos padrones, un padrón general (cuyo acceso es restringido por ley) y un padrón abierto o editado (al que cualquiera puede comprar acceso). En el Reino Unido,[15] por ejemplo, el padrón general (completo) está a disposición de las personas que establezca la

[12] Véase https://sur.conectas.org/en/a-very-secret-ballot

[13] Privacy International, Our final report on Kenya's 2022 election in collaboration with The Carter Center Election Expert Mission, 21 de marzo de 2023. Disponible en: https://privacyinternational.org/long-read/5053/our-final-report-kenyas-2022-election-collaboration-carter-center-election-expert

[14] Como señala el CdE en sus directrices para la protección de las personas en lo que respecta al tratamiento de datos personales: "Cuando los organizadores de campañas políticas obtienen el padrón electoral oficial de manera legal del organismo regulador de las elecciones con el fin de ayudar a sus campañas, la ley debe estipular quién tiene derecho a acceder a estos datos, y con qué fines, restringiendo dicho acceso a lo que resulte necesario para establecer contacto con el electorado, con prohibiciones claras y sanciones apropiadas para el uso de los datos con cualquier otro fin".

[15] Véase https://ico.org.uk/your-data-matters/electoral-register/

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 pueden utilizar los datos para ciertos fines, también prescritos por ley. El padrón editado/abierto (que permite darse de baja voluntariamente) puede ser comprado por cualquiera y utilizado para una gran variedad de fines. Por lo tanto, las entidades que tengan acceso al padrón completo no podrán compartirlo sin un fundamento legal. Por ejemplo, una entidad que preste servicios de información crediticia no podrá compartir estos datos con otros agentes de datos para fines de mercadeo.

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

La falta de seguridad adecuada ha permitido que se acceda sin autorización a los datos de millones de personas en diferentes países del mundo. En marzo de 2016, en Filipinas, se filtraron los datos personales de más de 55 millones de votantes registrados tras una vulneración de la base de datos de la Comisión Electoral (COMELEC)[16] que permitió acceder a datos personales y sensibles, según concluyó la autoridad nacional de protección de datos. En agosto de 2023, se supo que un ciberataque contra la totalidad del padrón electoral del Reino Unido ocasionó el acceso no autorizado a los datos de 40 millones de votantes, incluidos sus nombres y direcciones.[17] Después se supo que la Comisión Electoral había fallado una prueba de seguridad básica en la misma época en que sus registros fueron hackeados, lo que puso en tela de juicio la eficacia de las salvaguardias que existían en ese momento.

Registro biométrico de votantes (BVR, por sus siglas en inglés)[18]

Quienes abogan por el BVR argumentan que es efectivo contra el fraude electoral, como, por ejemplo, la suplantación de votantes y la votación múltiple. Sin embargo, el BVR no alcanza a sustituir completamente a otros mecanismos que buscan 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 el soporte (lo que, a su vez, podría incrementar el riesgo de corrupción o, para los países en desarrollo, de dependencia de los donantes).[19]

El BVR puede utilizarse para deduplicar el padrón electoral y/o para verificar la identidad de los votantes cuando acuden al punto de votación. La consecuencia de utilizar los datos biométricos con estos fines es una base de datos centralizada con los datos biométricos de toda la población empadronada. El BVR debe incorporar la privacidad por defecto y por diseño. Por ejemplo, un sistema de autenticación diseñado exclusivamente para la deduplicación no tiene necesidad de conectar los datos biométricos con una persona, todo lo que el sistema necesita

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

[17] Véase https://www.electoralcommission.org.uk/privacy-policy/public-notification-cyber-attack-electoral-commission-systems

[18] Con los padrones electorales biométricos, una o más características físicas del votante, tales como la foto, su huella dactilar o el escaneado de la retina, entre otras características, son registradas en el momento de la inscripción. Dicha información puede usarse para identificar al votante en el centro de votación.

[19] Para consultar un listado de estas inquitudes véase EU Handbook, https://www.eods.eu/library/EUEOM_Handbook_2016.pdf

saber es si ya había visto esos datos biométricos específicos (es decir, responde a la pregunta "¿este votante cumple los requisitos?" y no a "¿quién es esta persona?").

A la fecha de redacción de este informe, 54 países recogen algún tipo de dato biométrico para el padrón electoral.[20] De ellos, más de dos tercios se basan en huellas dactilares y fotografías, combinando tecnologías para cotejar de huellas dactilares con el reconocimiento facial.

Desde el punto de vista de la protección y seguridad de datos, recopilar y almacenar datos biométricos para registrar a los votantes genera inquietudes importantes. Los datos biométricos son especialmente sensibles y revelan las características y la identidad de las personas, lo que puede dar lugar a abusos graves.[21] Tal como reconocen cada vez más las agencias de protección de datos en todo el mundo,[22] a menudo los datos biométricos son considerados una categoría especial de datos personales que requieren 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, que tienen consecuencias gravísimas para las personas afectadas y para la seguridad en general de la sociedad.[23]

Recomendaciones

- Los procedimientos para empadronar a los votantes deben ser estipulados claramente en la ley.
- El padrón electoral no debe incluir datos personales más allá de los que necesarios para acreditar la satisfacción de los requisitos de votación.
- La normativa debe exigir la adopción de las mejores prácticas internacionales concertadas en materia de seguridad para proteger el padrón electoral de accesos no autorizados; también debe definir las condiciones y los límites para acceder a los datos del padrón electoral.
- Los datos personales del padrón electoral no deben ser publicados por defecto. Si el padrón electoral es abierto y cualquiera puede comprar acceso al mismo para cualquier fin, el padrón debe operar con base en la inclusión voluntaria (*opt-in*) y no la baja voluntaria (*opt-out*).
- La legislación y las directrices relevantes deben establecer con claridad que los datos personales del padrón electoral a los que está permitido el acceso siguen rigiéndose y están protegidos por las normas sobre protección de datos, incluso para el tratamiento

[20] IDEA, ICTs in Elections Database – Voter registration and identification; question "If the EMB uses technology to collect voter registration data, is biometric data captured and used during registration?"; disponible en: https://www.idea.int/data-tools/data/icts-elections-database
[21] 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
[22] ICO, Guidance on Biometric Data. Disponible en: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/guidance-on-biometric-data/key-data-protection-concepts/#special. AEPD, Empleo de datos biométricos: Evaluación desde la perspectiva de protección de datos, disponible en: https://www.aepd.es/prensa-y-comunicacion/blog/datos-biometricos-evaluacion-perspectiva-proteccion-datos
[23] Para información adicional sobre las violaciones a la base de datos del DNI de Argentina, puede consultar la presentación conjunta de Privacy International y la Asociación por los Derechos Civiles en el contexto del Examen Periódico Universal de Argentina, párr. 23. Disponible en: https://adc.org.ar/wp-content/uploads/2022/07/Adjunto-3-ADC-PI-UPR-Joint-Contribution.pdf

futuro. En particular, los datos personales del padrón electoral no deben combinarse con otras fuentes de datos personales para crear perfiles de los votantes.

- Debe regularse el acceso y el uso de los datos personales contenidos en un padrón electoral. La ley debe estipular claramente quién tiene derecho al acceso y para qué fines, se debe limitar a lo que sea necesario para el proceso electoral, con prohibiciones claras de usar tales datos para cualquier otro fin.

Padrón electoral biométrico

- Debido a que los datos biométricos son especialmente sensibles, su uso requiere la adopción de fuertes salvaguardas plasmadas en normas. Todas las normas de protección de datos deben reconocer esta sensibilidad.
- La ley debe estipular que ningún tercero salvo el organismo de gestión electoral debe tener acceso a los datos biométricos y que los datos biométricos (incluidas las fotografías) no deben ser utilizados para fines diferentes de la deduplicación y/o la autenticación de la identidad de los votantes.
- Se deben desarrollar protecciones adicionales contra el acceso no autorizado y otras violaciones de los datos personales, lo que incluye almacenar los datos biométricos con independencia de otros datos.
- Los padrones abiertos a los que se puede comprar acceso no deben contener datos sensibles, incluidos los datos biométricos.
- Cualquier sistema relacionado con la votación debe proteger fuertemente la privacidad por diseño y por defecto. Por ejemplo, los sistemas deben diseñarse para usos y casos específicos y solamente deben usarse para la autenticación (1-1) y no la identificación (1 a muchos).

Preguntas

- ¿La normativa regula la inscripción de los votantes y la gestión del padrón electoral?
- ¿Qué categorías de datos incluye el padrón electoral? (por ejemplo, nombre, dirección, número de identificación nacional, origen étnico, etc.)
- ¿Quién tiene acceso a la totalidad del padrón electoral y cuáles son las condiciones para acceder al mismo?
- ¿Existe un registro de las entidades que han tenido acceso a una parte o a la totalidad del padrón electoral y, en caso afirmativo, quién es responsable de dicho registro? ¿Este registro es auditado regularmente/monitoreado activamente para detectar accesos anómalos o no previstos?
- ¿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)?
- ¿Qué medidas de seguridad son adoptadas para garantizar que los datos personales contenidos en el padrón electoral estén protegidos de accesos no autorizados? ¿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 padrón biométrico, está sujeto a salvaguardas reforzadas en razón a la sensibilidad de los datos?

- En caso de usarse un padrón biométrico, ¿su diseño tuvo en cuenta la privacidad y limitó su uso a casos específicos de deduplicación y/o autenticación de la identidad de los votantes?

1.3 Votaciones

Como señala la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, la forma en que un país desarrolla sus operaciones de votación y su grado de transparencia son fundamentales para garantizar el disfrute de los derechos humanos pertinentes, además de aumentar la confianza pública en el proceso y los resultados.[24]

La verificación de los votantes es un elemento clave del proceso de votación. En este contexto, surgen consideraciones similares a las planteadas frente al 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 (véase la sección 1.2). Por ejemplo, los datos compartidos en el puesto de votación deben limitarse a los datos necesarios para identificar al votante y completar el proceso de votación. Además, los Estados deben adoptar medidas eficaces para garantizar que todas las personas que tengan derecho a voto puedan ejercerlo.[25] Esta obligación debe incluir la eliminación de obstáculos onerosos para la verificación de los votantes, como únicamente aceptar un solo tipo de documento de identidad oficial para poder votar.[26]

Como ha señalado la ACNUDH, la digitalización de los procesos electorales y, en particular, el voto electrónico son motivo de preocupación.[27] En este mismo sentido, la Asamblea General de la ONU ha observado el "uso de tecnología en línea en las votaciones" y ha reafirmado el derecho a la privacidad en ese contexto,[28] mientras que el Secretario General de la ONU ha recomendado que todas las tecnologías nuevas que se introduzcan en el contexto electoral sean sometidas a prueba antes de su despliegue, y que las pruebas tengan en cuenta "las crecientes preocupaciones por la vulnerabilidad de las infraestructuras electorales nacionales a los ataques cibernéticos".[29]

En los últimos años, quienes investigan las iniciativas de voto electrónico han identificado una serie de retos. En dos análisis diferentes sobre iniciativas de voto electrónico usadas en Estados Unidos, el MIT descubrió problemas de privacidad y vulnerabilidades de seguridad que

[24] ACNUDH, Human Rights and Elections: Manual sobre las Normas Internacionales de Derechos Humanos en materia de Elecciones, 2021, párr. 125. Disponible en: https://www.ohchr.org/sites/default/files/2022-02/Human-Rights-and-Elections.pdf
[25] Observación general No.25, CCPR/C/21/Rev.1/Add.7, párr. 11.
[26] Véase https://privacyinternational.org/news-analysis/4590/uk-government-should-drop-plans-compulsory-id-presentation-polling-station
[27] ACNUDH, Human Rights and Elections: Manual sobre las Normas Internacionales de Derechos Humanos en materia de Elecciones, 2021, párr. 125. Disponible en: https://www.ohchr.org/sites/default/files/2022-02/Human-Rights-and-Elections.pdf
[28] Resolución de la Asamblea General de la ONU sobre el Fortalecimiento de la función de las Naciones Unidas para promover la democratización y mejorar las elecciones periódicas y auténticas, U.N. Doc A/RES/76/176, 11 de enero de 2022.
[29] Secretario General de las Naciones Unidas, Fortalecimiento de la función de las Naciones Unidas para aumentar la eficacia del principio de elecciones periódicas y genuinas y la promoción de la democratización, U.N. Doc A/74/285, 6 de agosto de 2019, párr. 38. Disponible en: https://undocs.org/Home/Mobile?FinalSymbol=A%2F74%2F285&Language=E&DeviceType=Desktop&LangR

permitían manipular los votos.[30] Se han detectado fallas similares en los sistemas de voto electrónico de Suiza y Australia.[31]

Recomendaciones

- No restringir el derecho al voto únicamente a las personas que tengan un documento nacional de identidad y permitir que la identidad de los votantes se pueda acreditar de muchas formas distintas para evitar la discriminación y la exclusión.
- Solo deben exigirse el mínimo de datos personales necesarios para garantizar la integridad del proceso de votación.
- Deben incorporarse salvaguardas específicas para proteger el anonimato, minimizar el riesgo de accesos no autorizados a los datos y de *hacking* en la votación electrónica
- Deben dedicarse recursos a la seguridad de las elecciones, lo que incluye establecer y realizar evaluaciones de riesgos para las tecnologías utilizadas en las elecciones.
- Deben establecerse mecanismos para monitorear, detectar y alertar sobre ataques cibernéticos a la infraestructura electoral y, además, estos mecanismos deben integrarse a las respuestas de seguridad cibernética.
- Las personas que gestionan o intervienen en la votación electrónica deben recibir capacitación técnica y sensibilización ante los riesgos de ciberseguridad que implica este sistema.

Preguntas

- ¿Cuál es la principal forma de verificar la identidad de los votantes? Si la verificación de los votantes se basa en la presentación de un documento de identidad oficial, ¿se aceptan documentos/procedimientos alternativos si la persona carece de documento de identidad?
- Cuando la verificación de los votantes depende de la tecnología, ¿existen métodos alternativos de verificación si llegan a fallar las máquinas?
- ¿Cuáles son los datos personales exigidos en el momento de la votación (es decir, para la verificación)?
- De los datos personales exigidos en el momento de la votación: (i) ¿qué se registra, (ii) ¿cómo se registra, almacena y transfiere, y (iii) ¿a quién?
- ¿Qué salvaguardas concretas existen para proteger el anonimato de los votantes en cuanto a la votación electrónica?
- Si el proceso de votación se basa en el voto electrónico, la transmisión electrónica de resultados o tecnologías similares, ¿existen métodos alternativos para depositar el voto en caso de producirse cortes de electricidad, caídas de la red u otras fallas del equipo?

---

[30] Specter, Koppel y Weitzner, The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S. Federal Elections. Disponible en: https://internetpolicy.mit.edu/wp-content/uploads/2020/02/SecurityAnalysisOfVoatz_Public.pdf; Specter and Halderman, Security Analysis of the Democracy Live Online Voting System. Disponible en: https://internetpolicy.mit.edu/wp-content/uploads/2020/06/OmniBallot-1.pdf

[31] Jee, A major flaw has been found in Switzerland's online voting system, 12 de marzo de 2019. Disponible en: https://www.technologyreview.com/2019/03/12/136676/a-major-flaw-has-been-found-in-switzerlands-online-voting-system/; Halderman y Teague, The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election. Disponible en: https://arxiv.org/abs/1504.05646

- ¿Qué salvaguardas concretas protegen una votación electrónica enlazada con el internet u otras redes informáticas del acceso no autorizado y el hackeo?
- ¿La ciberseguridad de las elecciones está incluida en la estrategia nacional de ciberseguridad?
- ¿Qué mecanismos existen para monitorear, detectar y responder a los ciberataques vinculados al voto electrónico?
- ¿Las personas que intervienen en las elecciones reciben capacitación sobre seguridad cibernética?

1.4. Papel del organismo electoral y otras entidades claves en el proceso electoral

El organismo electoral (OE), 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 OE cuenten con conocimientos técnicos que les permita evaluar la forma en que se utilizan en el proceso electoral la información personal y las tecnologías digitales para el tratamiento de dicha información. De lo contrario, se exponen a poner en peligro la integridad y seguridad del padrón electoral, que suele estar bajo su responsabilidad. Una auditoría realizada en 2022 sobre el padrón electoral en Kenia reveló que los controles de acceso aplicados a las bases de datos que albergan el padrón eran ineficaces y que los procedimientos de autorización adecuados no se aplicaban sistemáticamente.[32]

Más allá del desarrollo de sus competencias internas, sigue reconociéndose la necesidad de coordinación entre otros organismos gubernamentales y organismos regulatorios independientes.[33] Las amenazas a la integridad de las elecciones surgen de diferentes actores y precisan tanto de la participación de diferentes autoridades como de la coordinación entre ellas.

Un ejemplo *ad hoc* de este tipo de colaboración se produjo en las elecciones kenianas de 2022, cuando la Oficina del Comisionado de Protección de Datos, que recibió más de 200 quejas de personas afectadas que habían sido inscritas erradamente como miembros de partidos políticos, colaboró con la Oficina del Registro de Partidos Políticos para corregir el problema.[34] Esta colaboración también puede ser reconocida formalmente. Por ejemplo, el organismo electoral de México establece en su reglamento interno la obligación de informar a la agencia de protección de datos.[35]

A pesar de lo anterior, siguen siendo escasos los casos de cooperación entre autoridades. Por este motivo, los gobiernos deberían examinar la posibilidad de crear un mecanismo coordinador, sobre todo en periodos de campaña y elecciones, para garantizar el intercambio

[32] Véase https://privacyinternational.org/long-read/5053/our-final-report-kenyas-2022-election-collaboration-carter-center-election-expert
[33] UNESCO, Elections in digital times: a guide for electoral practitioners, 2022, p.114. Disponible en: https://unesdoc.unesco.org/ark:/48223/pf0000382102
[34] Véase https://privacyinternational.org/long-read/5053/our-final-report-kenyas-2022-election-collaboration-carter-center-election-expert
[35] Veáse Reglamento del Instituto Nacional Electoral en Materia de Protección de Datos Personales, artículo 30. Disponible en: https://www.ine.mx/transparencia/protecciondp/marco-normativo/

de información y conocimientos entre las distintas autoridades responsables de gestionar y monitorear las elecciones.

Recomendaciones

- Los OE deben desarrollar sus competencias en materia de protección de datos y ciberseguridad.
- Los OE deben cooperar de manera oportuna y eficaz con las autoridades de áreas conexas (como las autoridades de protección de datos, los reguladores de los medios de comunicación, las autoridades de seguridad cibernética, los comisionados biométricos, etc.).
- Los OE deben regular el acceso interno al padrón electoral, es decir, definir qué funcionarios del OE tendrán acceso, y solamente los funcionarios autorizados podrán acceder al padrón, con sujeción a controles de acceso y mecanismos de monitoreo estrictos. A fin de identificar y combatir las actividades sospechosas, los OE deben llevar un registro de accesos del personal interno al padrón y este debe ser revisado periódicamente.
- Cuando los organismos que regulan los partidos políticos son independientes del OE, los organismos reguladores deben promover y facilitar que los partidos políticos y los candidatos cumplan las normas de protección de datos, incluso conectando a los partidos y los candidatos con las entidades de protección de datos.

Preguntas

- ¿Los OE tienen conocimientos especializados en materia de protección de datos y ciberseguridad?
- ¿Cuáles son los controles de acceso establecidos para garantizar que el acceso de los funcionarios del OE al padrón electoral es controlado y monitoreado y el nivel de acceso es acorde al papel/función/tarea de la persona que lo solicita?
- ¿El OE lleva un registro de acceso al padrón electoral? En caso afirmativo, ¿el registro es auditado, con qué frecuencia y qué tan eficaz es esta auditoría?
- ¿El OE está consultando y cooperando con otras autoridades (autoridad de protección de datos, reguladores de medios de comunicación, ciberseguridad)?
- ¿El gobierno ha establecido un mecanismo de coordinación para las autoridades encargadas de los distintos aspectos de la gestión y el control de las elecciones?

1.5. La empresa privada y los procesos de contratación

Los procesos electorales incorporan cada vez más nuevas tecnologías y procesos digitales, como el empadronamiento y la verificación biométricos de los votantes[36] o la transmisión digital de los resultados electorales. Algunas veces estos servicios son prestados por la empresa privada, que suelen participar en la celebración de elecciones después de una licitación iniciada

[36]A finales de 2023, casi el 20% de los países de todo el mundo utilizaban tecnología para identificar a los votantes en los colegios electorales. Véase IDEA, ICTs in Elections Database – Voter registration and identification; question "Is technology used for identifying voters at polling stations?". Disponible en: https://www.idea.int/data-tools/data/icts-elections-database

por el gobierno en la que se establecen los requisitos técnicos exigidos para cualquier producto o servicio que vaya a utilizarse para el proceso electoral.

En general, la privatización de las tareas y las funciones públicas puede ser muy problemática si no se aplican las salvaguardias necesarias.[37] Los riesgos son mucho más elevados en el contexto electoral, sobre todo cuando el uso de los productos técnicos o los servicios prestados por una empresa son esenciales para ejercer el voto.

Una vez adoptadas, este tipo de tecnologías pueden generar una relación de dependencia por parte de los gobiernos, entre otras cosas porque su sustitución es costosa y/o porque las compañías privadas conservan el control de los conocimientos técnicos necesarios para operar y actualizar las tecnologías. Las disputas contractuales pueden afectar significativamente al desarrollo de un proceso electoral, como, por ejemplo, si dan lugar al aplazamiento de unas elecciones o a la retención de bases de datos de ámbito nacional.[38] Es de vital importancia que el diseño y el funcionamiento de una tecnología integrada en el proceso electoral puedan ser cuestionados incluso después de las elecciones y puedan ser un elemento determinante para los actores judiciales a la hora de emprender una acción legal contra un resultado electoral.[39]

Es esencial que el vínculo entre la empresa privada contratada para proveer un producto o una tecnología para el proceso electoral y el organismo electoral sean examinado minuciosamente desde el inicio de las primeras etapas.

Recomendaciones

- Los organismos electorales y la empresa privada deben garantizar la aplicación de procesos rigurosos de diligencia debida en materia de derechos humanos, que abarquen tanto las fases iniciales de diseño y desarrollo como las fases de despliegue y uso de las tecnologías.
- Toda la documentación relacionada con el proceso de contratación de una empresa para la provisión de tecnología electoral debe estar a disposición del público.
- Las empresas que pretendan proporcionar tecnología electoral deben renunciar a la confidencialidad comercial y permitir que sus tecnologías puedan ser auditadas íntegramente a fin de permitir comprender cómo funcionan.
- En los casos en que se prevea que la tecnología electoral en cuestión tratará datos personales, la documentación provisional o definitiva deberá incluir información detallada acerca de las actividades de tratamiento de datos potenciales y actuales.
- Los contratos para el suministro de tecnología electoral deben detallar explícitamente la forma en que la empresa accederá a los datos y, además, deben prever las

[37] Privacy International, Safeguards for Public-Private Partnerships, diciembre de 2021. Véase https://privacyinternational.org/our-demands/safeguards-public-private-surveillance-partnerships

[38] Mali y Nigeria son ejemplos recientes de aplazamientos de las elecciones, véase https://www.aljazeera.com/news/2023/9/25/mali-postpones-february-presidential-election-due-to-technical-issues; and https://www.theguardian.com/world/2023/mar/09/nigeria-postpones-state-elections-dispute-presidential-vote. En Kenia, un proveedor de tecnología electoral retuvo una base de datos biométricos por incumplimiento en los pagos - https://privacyinternational.org/long-read/5053/our-final-report-kenyas-2022-election-collaboration-carter-center-election-expert

[39] En 2017, la Corte Suprema de Kenia anuló el resultado de las elecciones generales debido a una serie de factores, entre ellos que el organismo electoral no transmitió los resultados con credibilidad. Puede consultar la sentencia completa aquí: http://kenyalaw.org/caselaw/cases/view/140716/

salvaguardias correspondientes para garantizar la seguridad y el tratamiento adecuado de los datos, especialmente cuando los mismos sean transmitidos internacionalmente.

Preguntas

- ¿Cuáles son las tecnologías de empresas privadas en las que se basa la gestión de las elecciones? (por ejemplo, kits de registro/verificación biométricos)
- ¿Se ha publicado la suficiente información sobre el proceso de contratación y la tecnología en uso como para permitir el escrutinio público y reglamentario del proceso y la tecnología?
- ¿Cuáles son los datos personales a los que tiene acceso la empresa privada que provee la tecnología?
- ¿Qué argumentos se presentan para justificar el tratamiento de los datos?
- ¿Qué salvaguardias o límites, si los hay, se le exigen al proveedor de tecnología privado para el tratamiento de datos?
- ¿Existen condiciones claras que establezcan quién es el propietario del conjunto de datos que genera o mantiene la empresa?

1.6 Reclamaciones y reparación

Es necesario que exista un mecanismo de reclamaciones independiente a fin de garantizar que los procesos electorales sean libres e imparciales y que todos los actores involucrados rindan cuentas sobre sus actos. Para que los electores tengan confianza en el proceso electoral, la normativa debe prever el acceso a procesos para presentar reclamaciones o recursos y a procedimientos de auditoría.[40]

Los mecanismos de reclamación y reparación varían de un país a otro, pero en el marco de la protección de datos existe una marcada preferencia por establecer autoridades de protección de datos autónomas y con capacidad de recibir reclamaciones aunado al derecho de las personas a un recurso judicial efectivo contra las decisiones de la autoridad de protección de datos.[41] Como mínimo, tales autoridades deben tener competencia para recibir e investigar cualquier denuncia relacionada con el uso indebido de información personal en el contexto electoral. En 2021, tras recibir 51 denuncias, la Oficina del Comisionado de Información del Reino Unido multó al partido conservador por enviar correos electrónicos de marketing ilegales en julio de 2019.[42] En 2022, la Oficina del Comisionado de Protección de Datos de Kenia recibió más de 200 denuncias originadas en mensajes de texto no solicitados que fueron recibidos por votantes potenciales en los que se les señalaba de manera errónea como miembros de partidos políticos.[43] Más recientemente, la Autoridad Nacional de Protección de Datos de Brasil multó

[40] ACNUDH, Human Rights and Elections: A Handbook on International Human Rights Standards on Elections, 2021, párr. 128. Disponible en: https://www.ohchr.org/sites/default/files/2022-02/Human-Rights-and-Elections.pdf

[41] Véase, por ejemplo, el artículo 12 del Convenio 108 del Consejo de Europa, https://rm.coe.int/convention-108convention-for-the-protection-of-individuals-with-regar/16808b36f1 y el artículo 77 del Reglamento General de Protección de Datos de la UE.

[42] Véase https://ico.org.uk/media/action-weve-taken/mpns/2619896/conservative-party-mpn-20210601.pdf

[43] Véase https://privacyinternational.org/long-read/5053/our-final-report-kenyas-2022-election-collaboration-carter-center-election-expert

a una pequeña empresa de telecomunicaciones que fue investigada por ofrecerle a los políticos servicios de mensajería masiva a través de WhatsApp.[44]

Asimismo, las autoridades de protección de datos deben tener la facultad de iniciar investigaciones discrecionalmente. En 2019, por ejemplo, el Supervisor Europeo de Protección de Datos (SEPD) realizó una investigación del uso por el Parlamento Europeo de la empresa estadounidense de campañas políticas NationBuilder para el tratamiento de datos personales, que condujo a la primera amonestación de una institución de la UE.[45]

Las autoridades de regulación electoral independientes también deben tener competencia para recibir reclamaciones, en particular, frente al uso indebido de los datos por parte de los partidos políticos y otros agentes políticos.

Del mismo modo, las personas y las organizaciones, incluidos los grupos de observadores ciudadanos, deben tener la posibilidad de presentar reclamaciones por el uso indebido de información personal en el proceso electoral ante el organismo electoral nacional o ante algún otro organismo nacional independiente encargado de monitorear la celebración de las elecciones.

Recomendaciones

- Las autoridades de protección de datos autónomas deben tener competencia para iniciar investigaciones discrecionalmente y recibir y responder a las reclamaciones de personas y organizaciones que denuncien el uso indebido de datos personales en el contexto de elecciones y campañas políticas;
- Del mismo modo, las personas y las organizaciones deben poder presentar reclamaciones ante los organismos electorales u otras autoridades de regulación electoral independientes;
- Los OE u otras autoridades reguladoras electorales autónomas deben tener competencia para recomendar y/o implementar reformas cuando las reclamaciones revelen 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 mediante la apelación de las decisiones de los órganos reguladores.

Preguntas

- ¿Cuáles son mecanismos de reparación a los que pueden acudir las personas y las organizaciones que denuncian el abuso de datos personales en el contexto de las elecciones y las campañas políticas?
- ¿El OE acepta reclamaciones de individuos y organizaciones?

[44] Véase https://www.dataguidance.com/news/brazil-anpd-imposes-fines-and-warning-telekall

[45] Véase el comunicado del Supervisor Europeo de Protección de Datos sobre la investigación de las actividades electorales del Parlamento Europeo en 2019: https://edps.europa.eu/press-publications/press-news/press-releases/2019/edps-investigates-european-parliaments-2019_en; and their announcement closing the investigation: https://edps.europa.eu/press-publications/press-news/press-releases/2020/edps-closes-investigation-european-parliaments_en

- ¿Cuáles son los diferentes tipos de reparación disponibles (multas, imposición de condiciones o restricciones en el tratamiento de datos personales, etc.)?
- ¿La autoridad de protección de datos puede iniciar investigaciones discrecionalmente?

Parte 2 – Los partidos políticos y otros actores políticos

Las organizaciones de observación electoral reconocen cada vez más que las normas que regulan la conducta de los partidos políticos y los demás actores en las elecciones deben evaluarse a la luz de la creciente dependencia de las tecnologías y los datos personales.

El Consejo de Europa reconoce en sus directrices de 2021 que, puesto que las elecciones son cada vez más "basadas en datos", es crucial que todas las organizaciones que actúan en las campañas políticas traten los datos personales de los votantes de conformidad con principios de protección de datos firmemente establecidos.[46]

2.1. Regulación del uso que dan partidos políticos a la información personal

Los partidos y otros actores políticos están empleando cada vez más una gran variedad técnicas que requieren enormes 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 es vista como un activo político que puede utilizarse para focalizar con eficacia a diferentes grupos con el propósito de incentivar su apoyo o dificultar su participación en los procesos políticos, a partir de características individuales o compartidas.[47]

Los datos personales que indiquen opiniones políticas son una categoría especial de datos de acuerdo con la legislación moderna de protección de datos. Su tratamiento está sujeto a estrictas salvaguardias y generalmente está prohibido salvo excepciones de interpretación restrictiva, tales como una autorización expresa, específica, plenamente informada y libremente otorgada por las personas afectadas.[48] El Consejo de Europa ha señalado que el tratamiento de los datos personales entraña serios riesgos de discriminación contra los votantes–lo que puede desembocar en la supresión e intimidación de los votantes–y puede llegar a afectar la prestación de servicios gubernamentales.[49] Por estas razones, el tratamiento de datos pertenecientes a categorías especiales debe ir acompañado de salvaguardas adecuadas frente a los riesgos planteados.[50]

---

[46] Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns, noviembre de 2021, p.5. Disponible en: https://rm.coe.int/guidelines-on-data-proetction-and-electioncampaigns-en/1680a5ae72

[47] Una investigación de Channel 4 descubrió que el objetivo de una estrategia de campaña desplegada por Donald Trump en las elecciones de 2016 era disuadir a millones de afroamericanos de votar. Véase https://www.channel4.com/news/revealed-trump-campaign-strategy-to-deter-millions-of-black-americans-from-voting-in-2016

[48] Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns, noviembre de 2021, párr. 4.2.1 – 4.2.4. Disponible en: https://rm.coe.int/guidelines-on-data-proetction-and-election-campaigns-en/1680a5ae72

[49] Consejo de Europa, Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns, noviembre de 2021, párr. 4.2.4. Disponible en: https://rm.coe.int/guidelines-on-data-proetction-and-election-campaigns-en/1680a5ae72

[50] Ibid.

Sin embargo, es cada vez más frecuente que las opiniones políticas puedan ser descubiertas o inferidas mediante la aplicación de herramientas para el análisis predictivo y la elaboración de perfiles a partir de diferentes fuentes de información, incluidas fuentes públicas como la lectura de revistas y periódicos y la afiliación a grupos de interés, entre otras.[51] Ante el auge de las tecnologías que permiten hacer tales inferencias, algunos reguladores y organismos de supervisión han recortado los límites dentro de los que se permite el tratamiento. Por ejemplo, la autoridad española de protección de datos prohibió expresamente el tratamiento de datos personales a partir de los cuales se pueda inferir las opiniones políticas mediante la aplicación de tecnologías como la inteligencia artificial.[52]

A pesar de estos riesgos, las normas de protección de datos pueden contemplar excepciones a los requisitos de protección de datos para los partidos políticos.[53] Dichas excepciones podrían socavar las iniciativas que buscan hacer frente a la explotación de los datos personales durante las elecciones.

Los organismos de regulación de protección de datos adoptan cada vez más medidas para investigar el uso que hacen los partidos políticos de los datos de los votantes. En 2020, la Oficina del Comisionado de Información del Reino Unido realizó una auditoría sobre el uso de datos personales por parte de los partidos políticos a raíz de las preocupaciones expresadas con anterioridad sobre el uso de datos personales en campañas políticas.[54] En 2021, la Comisión Irlandesa de Protección de Datos auditó las prácticas de los partidos políticos en Irlanda ante la preocupación pública que suscitó que un partido almacenara la información de millones de votantes en una base de datos interna.[55]

Recomendaciones

- La normativa de protección de datos debe ser aplicada íntegramente al tratamiento de datos que realicen los partidos políticos y otros actores políticos.
- Los partidos políticos y los otros actores políticos deben:
    - ser transparentes en sus actividades de tratamiento de datos, indicando, entre otros, los mecanismos que utilizan para interactuar con los votantes (por ejemplo, redes sociales, sitios web, mensajería directa y métodos de campaña y segmentación) y qué datos personales tratan;
    - ser transparentes sobre cómo recopilan los datos de las personas y las fuentes de los mismos;
    - ser transparentes en cuanto a sus prácticas de elaboración de perfiles, incluidas las prácticas de los encargados o los corresponsables del tratamiento de datos,

[51] Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns, noviembre de 2021, párr. 4.22. Disponible en: https://rm.coe.int/guidelines-on-data-proetction-and-election-campaigns-en/1680a5ae72
[52] AEPD, https://www.boe.es/buscar/doc.php?id=BOE-A-2019-3423
[53] Véase https://privacyinternational.org/news-analysis/2836/gdpr-loopholes-facilitate-data-exploitation-political-parties
[54] ICO, UK Political Parties, 11 de noviembre de 2020. Disponible en: https://ico.org.uk/action-weve-taken/audits-and-overview-reports/uk-political-parties/
[55] Irish Data Protection Commission, Data Protection Audit of Political Parties in Ireland, diciembre de 2021. Disponible en: https://www.dataprotection.ie/en/news-media/latest-news/data-protection-commission-publishes-report-data-protection-audit-political-parties-ireland

incluyendo la realización de inferencias, y también explicando las decisiones automatizadas;
- ser transparentes en su publicidad y mensajes políticos, garantizando que el público pueda reconocer fácilmente los mensajes y comunicados políticos y la organización que tras ellos. Deben proporcionar información sobre los criterios de selección empleados en la difusión de dichos mensajes políticos;
- publicar una lista completa, de fácil acceso y comprensión, de todos los grupos de presión con los que tengan relaciones financieras o informales como colaboradores en las campañas, incluidos todos los terceros y con quienes desarrollen campañas conjuntas;
- ser transparentes respecto a las empresas con las que contratan en el marco de sus campañas para la recolección y el tratamiento de datos, incluidas la elaboración de perfiles y la segmentación, y también respecto a las empresas que suministran herramientas y software de campaña y los productos que utilizan;
- adoptar y divulgar políticas de protección de datos;
- realizar auditorías de protección de datos y evaluaciones de impacto;
- cerciorarse de que cuentan con un fundamento jurídico cada vez que utilicen datos personales (incluidos los datos sensibles, como los que reflejan opiniones políticas);
- antes de utilizar datos personales suministrados por un tercero, verificar que los datos se obtuvieron legalmente y que el tercero cumple la legislación sobre protección de datos;
- facilitar que las personas ejerzan sus derechos en materia de datos (informando cómo serán tratados los datos, facilitando el acceso a los mismos y permitiendo su actualización y eliminación, por ejemplo), y publicar mecanismos y procedimientos para plantear inquietudes y darles respuesta; y
- adoptar medidas de seguridad adecuadas para impedir el acceso y la divulgación no autorizados de datos personales. Tales medidas deben tener en cuenta las comunicaciones y tecnologías utilizadas, e incluir capacitación en privacidad y seguridad, controles de acceso, acuerdos de confidencialidad y controles de acceso físico a los lugares y los equipos donde se almacenan los datos personales.

Preguntas

- ¿La normativa nacional sobre protección de datos aplica a los datos recogidos y usados (tratados) por los partidos políticos y otros actores políticos?
- ¿Los partidos políticos y otros actores políticos cuentan con políticas de protección de datos?
- ¿Las políticas ofrecen información clara, accesible y comprensible sobre cómo se pueden ejercer los derechos sobre los datos?
- ¿Informan cuál es el origen de los datos personales que obtienen los partidos políticos y otros actores políticos y qué hacen con ellos?
- ¿Los partidos políticos y otros actores políticos efectúan evaluaciones de impacto de protección de datos en relación con su tratamiento de datos personales?

- ¿Obtuvieron el consentimiento de las personas o de qué otra manera se justifica la posesión de los datos?
- ¿Los partidos políticos y otros actores políticos evalúan si los terceros a los que recurren para sus actividades de campaña cumplen las normas de protección de datos y actúan conforme a la ley?
- ¿Qué medidas de seguridad adoptan para prevenir el acceso no autorizado o la divulgación de datos personales?
- ¿Capacitan a todas las personas que colaboran en sus campañas políticas sobre las medidas de privacidad y seguridad de los datos?

2.2. Regulación de las campañas políticas basadas en datos

Las campañas políticas en todo el mundo se han transformado en sofisticadas operaciones de datos que utilizan cada vez más los datos personales de los ciudadanos para hacerles llegar publicidad personalizada.

Tras el estallido del escándalo de Cambridge Analytica,[56] han seguido presentándose ejemplos de campañas políticas sustentadas en datos personales. Human Rights Watch denunció que las elecciones húngaras de 2022 se caracterizaron por campañas basadas en datos, y hay indicios de que el partido gobernante recicló los datos recopilados por el Estado para gestionar los servicios públicos para difundir sus propios mensajes de campaña.[57]

La microfocalización y otras técnicas de focalización basadas en datos empleadas por el sector de la publicidad digital se aplican cada vez más en el contexto de las campañas políticas.[58] Varias empresas, conocidas como *data brokers* o agentes de datos, venden a las campañas políticas datos que permiten segmentar mejor a los votantes. Una investigación de The Markup reveló que los datos ofrecidos por los agentes de datos incluían desde las posibles opiniones de los votantes sobre el aborto o el control de armas, hasta los datos de la ubicación de cada elector.[59]

Algunos de los riesgos identificados en torno a la elaboración masiva de perfiles y la microfocalización son la creación de burbujas de filtros o cámaras de eco, la discriminación de

[56] 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" personalizado para cada votante. Se utilizó en varias campañas en Estados Unidos y posiblemente en la campaña Leave.EU en el Reino Unido. Véase, 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.
[57] Human Rights Watch, Trapped in a Web – The Exploitation of Personal Data in Hungary's 2022 Elections, diciembre de 2022. Disponible en: https://www.hrw.org/report/2022/12/01/trapped-web/exploitation-personal-data-hungarys-2022-elections
[58] Como dice Alexander Nix, director ejecutivo de Cambridge Analytica: "Lo que estamos haciendo no es diferente de lo que la industria publicitaria en general está haciendo en el espacio comercial". Witness I: Alexander Nix, Chied Executive, Cambridge Analytica, Digital, Culture, Media and Sport Committee. Oral Evidence: 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: 30 de octubre 2023).
[59] The Markup, How Political Campaigns Use Your Phone's Location to Target You, 8 de noviembre de 2022. Disponible en: https://themarkup.org/privacy/2022/11/08/how-political-campaigns-use-your-phones-location-to-target-you

los votantes, la privación del derecho de voto, el potencial de desincentivar la participación política, el aumento de la polarización, la erosión de la solidez de los debates democráticos y el debilitamiento de la integridad electoral.[60]

Los riesgos que entraña utilizar datos personales para fines de publicidad política han suscitado un gran rechazo y también iniciativas de regulación. Los relatores especiales de la ONU y la OEA sobre la libertad de expresión han llamado a que se prohíba la focalización de la publicidad política a partir de datos personales cuando la persona no ha autorizado el uso de sus datos para este fin.[61] A la fecha de redacción de este informe, el proyecto de Reglamento de la Unión Europea sobre transparencia y segmentación de la publicidad política se encuentra en las últimas etapas del proceso legislativo, y los legisladores aún no han decidido si se debe permitir el uso de categorías especiales de datos en la publicidad política en línea.[62] Otras normas, como la Ley de Servicios Digitales de la UE, prohíben claramente la publicidad basada en la elaboración de perfiles a partir de categorías especiales de datos personales.[63]

A continuación, se describen algunas de las principales prácticas que continúan ganando importancia y se utilizan cada vez más en el contexto de las campañas políticas.

- Elaboración de perfiles

La elaboración de perfiles se refiere a "cualquier forma de tratamiento automatizado de datos personales, incluido el uso de sistemas de aprendizaje automático, que implique el uso de datos para evaluar ciertos aspectos personales en relación con un individuo, en particular para analizar o predecir aspectos relativos a su rendimiento en el trabajo, su situación económica, su salud, sus preferencias personales, sus intereses, su fiabilidad, su comportamiento, su ubicación o sus desplazamientos".[64] 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. A menudo, varios actores compran, acumulan y comparten entre sí los datos que alimentan estos perfiles[65] sin que las personas implicadas se enteren que se elaboró un perfil de ellas. Los perfiles pueden ser cotejados y utilizados para inferir datos no solo de una persona sino de otras personas "como ella", por ejemplo, mediante "Lookalike Audiences" (audiencias similares).[66]. Adicionalmente, con

[60] Consejo de Europa, Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns, noviembre de 2021, párr. 2.10.
[61] ONU, OEA y OSCE, Joint Declaration on Freedom of Expression and Elections in the Digital Age, abril de 2020. Disponible en: https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/JointDeclarationDigitalAge_30April2020_EN.pdf
[62] Véase https://edri.org/our-work/political-negotiations-continue-eu-lawmakers-fail-to-agree-on-strong-rules-for-regulating-political-advertising/
[63] Véase Ley de Servicios Digitales, considerando 69; artículo 26(3).
[64] Consejo de Europa, Recomendación CM/Rec(2021)8 del Comité de Ministros a los Estados miembros relativa a la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal en el contexto de la elaboración de perfiles, 3 de noviembre de 2021, párr. 1(c).
[65] Privacy International, Our Complaints against Acxiom, Criteo, Equifax, Experian, Oracle, Quantcast, Tapad, 8 de noviembre de 2018, disponible en https://privacyinternational.org/advocacy/2426/our-complaints-against-acxiom-criteo-equifax-experian-oracle-quantcast-tapad
[66] Oficina del Comisionado de Información, Democracy Disrupted? Personal Information and Political Influence, 11 de julio de 2018. p. 36. Disponible en: https://ico.org.uk/media/2259369/democracy-disrupted-110718.pdf

frecuencia los agentes de datos y las empresas de tecnologías de publicidad ofrecen soluciones probabilísticas que establecen "correspondencias entre conjuntos de datos que aprovechan supuestos inferidos, modelados o variables proxy."[67]

- Técnicas basadas en datos

Microfocalización

La práctica denominada microfocalización se comprende mejor si se considera como un proceso en cuatro etapas basado en (i) la recopilación de datos; (ii) la elaboración de perfiles, dividiendo a los individuos en pequeños grupos o "segmentos" en función de características, intereses o preferencias reales o percibidas; (iii) la personalización de contenidos en función de dichas características; y (iv) la focalización y la entrega de estos contenidos, a menudo a través de plataformas en línea.[68] Por su propia naturaleza, es probable que la microfocalización implique a numerosos actores, que comprenden desde los agentes de datos que proporcionan datos personales hasta las campañas políticas que elaboran los mensajes y las plataformas en línea que facilitan su difusión. Un ejemplo del papel complementario que las plataformas de medios sociales pueden desempeñar en la microfocalización es el uso de categorías de anuncios que pueden actuar como datos indirectos para características específicas como "pseudociencia" o "teoría conspirativa".[69]

A pesar de las preocupaciones que suscita, la microfocalización ha sido poco regulada. Una investigación de 2021 de la Universidad de Edimburgo que exploraba el panorama regulatorio de las campañas políticas en seis países descubrió que ni uno solo de ellos definía o regulaba de forma exhaustiva la microfocalización.[70] No obstante, los organismos reguladores están presionando para que se adopte una normativa rigurosa. En su opinión sobre el proyecto de Reglamento de la UE sobre publicidad política, el Supervisor Europeo de Protección de Datos propuso prohibir totalmente la microfocalización con fines políticos.[71]

Geofencing

El *geofencing* permite la focalización dinámica de las personas en función de su ubicación. Esta práctica puede revelar datos sensibles y presenta riesgos significativos para las personas.[72] Por

[67] Winterberry Group, "Know Your Audience: The Evolution of Identity in a Consumer-Centric Marketplace", agosto de 2018. Disponible en: https://marketing.acxiom.com/US-Parent-Winterberry-KnowYourAudience-REP-Main.html?&utm_source=website&utm_medium=owned&utm_campaign=identityresolution

[68] Véase https://privacyinternational.org/learn/micro-targeting

[69] Facebook utilizaba estas dos categorías de segmentación publicitaria y posteriormente las eliminó. Véase https://www.reuters.com/article/us-health-coronavirus-facebook-ads-idUSKCN2253CC

[70] Véase Privacy International y la Universidad de Edinburgh, Micro-targeting in political campaigns: a comparative analysis of legal frameworks, enero de 2021. Disponible en: https://privacyinternational.org/report/4364/microtargeting-political-campaigns-comparative-analysis-legal-frameworks

[71] Supervisor Europeo de Protección de Datos, EDPS Opinion on the Proposal for Regulation on the Transparency and Targeting of Political Advertising, 20 de enero de 2022, párr. 26-34. Disponible en: https://edps.europa.eu/data-protection/our-work/publications/opinions/edps-opinion-proposal-regulation-transparency-and_en

[72] Consejo de Europa, Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns, noviembre de 2021,

ejemplo, existen informes de que grupos religiosos han utilizado este tipo de tecnología para focalizar a personas que asisten a lugares religiosos.[73]

***

Es importante tener en cuenta que el uso de las técnicas de focalización (ya sea por los partidos políticos u otros actores políticos) no se limita al periodo de campaña electoral. El uso indebido de datos personales con fines de manipulación y desinformación, como ocurrió durante la pandemia de Covid-19 y en el periodo posterior, es un fenómeno constante que ha sido objeto de diversos informes y resoluciones de organismos de derechos humanos de la ONU, incluida una Resolución del Consejo de Derechos Humanos de la ONU.[74] A juicio de Privacy International, y en línea con el carácter incesante del intercambio de información y la recopilación de datos, la regulación del uso de datos para campañas políticas no debería limitarse al periodo electoral.

Existe un gran número de empresas y otros actores, además de los partidos políticos y los candidatos, que utilizan (u ofrecen) técnicas de focalización que requieren un uso intensivo de datos e invaden la privacidad. Centrarse únicamente en el periodo de campaña electoral y en los partidos políticos o candidatos oficiales entraña el riesgo de pasar por alto una parte importante del panorama.

Recomendaciones

- La normativa debería exigir que se revele información sobre todos los criterios de selección que utilizan los partidos y otros actores políticos en la divulgación de sus comunicaciones políticas.
- Cuando se utilicen técnicas de focalización basadas en datos, debe brindarse a los votantes información apropiada que explique por qué reciben un mensaje específico, quién es responsable del mismo y cómo pueden ejercer sus derechos para proteger sus datos y evitar que sea objeto de focalización.
- 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 tales mensajes y comunicaciones. Deben publicar en sus sitios web y como parte de la comunicación, información sobre cualquier criterio de selección utilizado en la difusión de estas comunicaciones.
- Los partidos y demás actores políticos no deben compartir datos personales con empresas de medios sociales para fines de publicidad digital sin antes notificar debidamente a los interesados.
- Los partidos y demás actores políticos deben garantizar que el uso de datos mediante estas técnicas (por ellos mismos y por quienes trabajan con ellos para obtener datos) cumpla todos los requisitos de las normas de protección de datos, incluidos principios como la transparencia, la imparcialidad y la limitación de la finalidad, la exigencia de tener una fundamento jurídico, derechos como el derecho a la información y a la supresión y obligaciones como la realización de una evaluación de impacto de la protección de datos.

[73] Véase https://www.npr.org/2020/02/06/803508851/how-political-campaigns-are-using-geofencing-technology-to-target-catholics-at-m

[74] Véase Resolución del Consejo de Derechos Humanos de la ONU A/HRC/RES/49/21. Disponible en: https://digitallibrary.un.org/record/3971994

- Las campañas políticas deben ser transparentes respecto a los terceros que contratan como parte de sus campañas para obtener datos y continuar el tratamiento de datos, incluidas la elaboración de perfiles y la personalización, tales como los agentes de datos y las compañías de publicidad política.

Preguntas

- ¿La normativa exige que los partidos y los demás actores políticos divulguen sus vínculos con las organizaciones y las personas que desarrollan publicidad o campañas políticas, incluidas las que se desarrollan en línea?
- ¿La normativa exige que los partidos y los demás actores políticos faciliten información a las personas y los reguladores sobre las técnicas de focalización que utilizan, incluidos los criterios de focalización y los terceros que les colaboran?
- ¿El marco normativo existente permite que el público o el regulador identifiquen a todos los terceros vinculados al partido político (por ejemplo, incluye a los subcontratistas)?
- ¿Los partidos políticos y los demás actores políticos asumen suficiente responsabilidad por los datos que puede utilizar cualquier tercero con el que contraten? ¿Saben qué datos utilizan esos terceros? ¿Qué contratos celebraron con los terceros? ¿Tales contratos contemplan suficientes cláusulas sobre la protección y la seguridad de los datos?

2.3. Financiación de campañas

La financiación de las campañas se refiere tanto a la financiación aportada a los partidos políticos o candidatos para la campaña electoral (ya sea mediante donaciones privadas o financiación pública) como el gasto los partidos o candidatos en los costos de la campaña.

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

Es muy difícil monitorear la financiación de las campañas. Una investigación realizada en Colombia por Dejusticia encontró que la herramienta de monitoreo en línea operada por el Consejo Nacional Electoral para suministrar información sobre los gastos de campaña no logró garantizar la transparencia en la contratación de servicios de marketing digital y comunicación política.[75] Un estudio reciente llevado a cabo en el Reino Unido reveló que no se habían rendido cuentas de casi el 15% del gasto de los partidos políticos durante los comicios generales británicos de 2019, en tanto que gastaron 10 millones de libras en publicidad, de los cuales el 73% fue en línea; y que las categorías de gasto que actualmente existen para las campañas políticas no reflejan la realidad de una campaña moderna.[76]

Como señala el Supervisor Europeo de Protección de Datos en su informe de 2018 sobre manipulación en línea y datos personales, los gastos en artículos de campaña reportados no

[75] Dejusticia, Digital Technologies and Political Campaigns: A Risk for the 2022 Elections?, 30 de noviembre de 2021. Disponible en: https://www.dejusticia.org/en/digital-technologies-and-political-campaigns-a-risk-for-the-2022-elections/

[76] IDEA, Regulating the Business of Election Campaigns, 20 de mayo de 2022. Disponible en: https://www.idea.int/publications/catalogue/regulating-business-election-campaigns

ofrecen información lo suficientemente detallada sobre el gasto en publicidad digital y servicios asociados.[77]

Recomendaciones

- La normativa sobre financiación de campañas debe exigir que se reporten oportunamente los gastos de las campañas en línea y la financiación que se obtenga en línea. La información debe ser lo suficientemente precisa y detallada como para fomentar la transparencia y la rendición de cuentas.
- La normativa debe exigir que los candidatos y los partidos políticos revelen públicamente los gastos de campaña relacionados con la captación y el tratamiento de datos personales, sobre todo los contratos con terceros como, por ejemplo, agentes de datos y empresas de publicidad política.
- 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. Esto debería incluir información sobre qué terceros, si los hay, han apoyado a los actores políticos en sus actividades en línea, incluido el monto pagado por los servicios de cada uno de ellos.
- La información publicada sobre los gastos de la campaña debe clasificarse en categorías relevantes, como la suma gastada en diferentes tipos de contenidos en cada plataforma de medios sociales, información sobre la audiencia destinataria en las plataformas, así como la audiencia concreta a la que efectivamente se llegó.
- La normativa nacional (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 en línea.

Preguntas

- ¿Las normas de financiación de campañas exigen la presentación de informes sobre los montos gastados en campañas en línea? ¿Ante quién deben presentarse? ¿Qué tan detalladas son las exigencias de esta obligación? ¿Cuáles son los plazos? ¿Cuáles son las sanciones por incumplimiento?
- ¿Las normas exigen a los partidos políticos (y a otros actores políticos) que divulguen las cantidades pagadas por anuncios políticos en internet? ¿Cuáles son los detalles de la información presentada (por ejemplo, desglosada por plataformas digitales, etc.)?

- ¿Los partidos políticos y los actores políticos están divulgando sus gastos de campaña en línea con el suficiente grado de detalle?

[77] Supervisor Europeo de Protección de Datos, Opinion 3/2018 on online manipulation and personal data, 19 March 2018, https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf.

Parte 3 – El papel del internet y los medios sociales en las elecciones y las campañas políticas

El internet y los medios sociales han contribuido a que muchas personas se organicen políticamente, participen en debates públicos, expresen sus opiniones (incluida la disidencia) en línea y reciban información, incluso durante las campañas electorales.

Al mismo tiempo, las tecnologías de comunicación digital actuales ponen en tela de juicio la eficacia de algunas de las salvaguardas adoptadas para garantizar que las elecciones sean libres e imparciales. En particular, se ha prestado gran atención a la difusión de la desinformación y el riesgo de que sean manipuladas las opiniones políticas de las personas. La mayoría de los análisis y los avances de las políticas o normas en este ámbito se han centrado en el contenido de las comunicaciones digitales, incluidos los esfuerzos por moderar o retirar contenidos, especialmente por parte de las empresas de internet y medios sociales. Se ha prestado relativamente menos atención a los datos personales recogidos y procesados con el fin de permitir que dichos contenidos lleguen a las audiencias deseadas, a pesar de las inquietudes que existen sobre los efectos negativos en los votantes de la explotación de los datos personales. Estas preocupaciones se intensifican cuando se acercan los periodos electorales, pero son pertinentes en cualquier momento, ya que incluso contenidos en línea que en apariencia no tienen carácter político pueden movilizar políticamente a la gente.

3.1. La presunción de "escasez"

Una salvaguarda crucial durante las campañas es garantizar que los partidos políticos y demás candidatos gocen de acceso igualitario y justo a los medios de comunicación tradicionales, y que la información ofrecida por los medios públicos sea imparcial y no partidista.

La razón de ser de estas obligaciones (de imparcialidad, equidad, equilibrio e igualdad durante las elecciones) es la "presunción de escasez", es decir, el hecho de que las oportunidades para acceder a los medios de comunicación tradicionales son limitadas. Tradicionalmente se ha asumido que esta "escasez" no afecta a los medios de comunicación en línea, debido a la facilidad y variedad de las fuentes de opinión y el libre acceso a las mismas.

Sin embargo, esta hipótesis no tiene en cuenta la concentración del mercado y los modelos de negocio en el ámbito de las comunicaciones digitales, ni la forma en que se distribuye y comparte la información a través de las plataformas digitales (en particular, los motores de búsqueda y las plataformas de medios sociales, incluidas las aplicaciones de mensajería).[78]

En concreto, los motores de búsqueda y las plataformas de medios sociales filtran las noticias y opiniones a las que pueden acceder los usuarios basándose en la elaboración de perfiles, que suele depender fuertemente de la explotación de datos. Esto va más allá de la compra de anuncios personalizados y de pagar por promover contenidos, y llega a afectar la forma en que

[78] Un ejemplo es que Google pagó 26.300 millones de dólares para ser el principal motor de búsqueda en todo el mundo, lo cual conduce a que los consumidores vean esencialmente los resultados de búsqueda de Google, y no los de otros motores de búsqueda. Véase https://www.theverge.com/2023/10/27/23934961/google-antitrust-trial-defaults-search-deal-26-3-billion

se muestran y recomiendan los contenidos.[79] Reflexionando sobre los retos que plantea el panorama actual de las comunicaciones digitales, la Relatora Especial de la ONU sobre la libertad de expresión señaló que "al diseñar sus productos con contenidos altamente personalizados para fomentar la consulta adictiva de contenidos, las empresas promueven un sistema que socava significativamente la capacidad de acción del individuo y sus decisiones en relación con la información que consume".[80]

Estas técnicas de focalización basadas en datos hacen que las personas únicamente estén expuestas a ciertos mensajes políticos y a cierta información política, lo que contradice directamente la suposición 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. Como recomendó la Relatora Especial de la ONU, "las empresas deberían proporcionar información clara y significativa sobre los parámetros de sus algoritmos o sistemas de recomendación y asegurarse de que esos sistemas permiten a los usuarios recibir por defecto una diversidad de puntos de vista, aunque permitiéndoles elegir las variables que afecten a sus actividades en línea".[81]

Recomendaciones

- Las plataformas de internet y los medios sociales deben ser transparentes acerca de sus actividades de elaboración de perfiles, incluso en cuanto a la personalización del contenido que la gente ve.
- Las empresas deben proporcionar información clara y significativa sobre los parámetros de sus algoritmos o sistemas de recomendación y asegurarse de que esos sistemas permitan que los usuarios reciban por defecto diversos puntos de vista, al tiempo que les permitan elegir las variables que conforman su experiencia en línea.
- 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 medios sociales han asumido compromisos concretos o adoptado 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 formas en las que los actores políticos pueden llegar a los usuarios de su plataforma? ¿Cómo funcionan sus servicios de publicidad, elaboración de perfiles, focalización y recomendación? ¿Quién tiene acceso a estos servicios?

[79] Por ejemplo, la personalización de los resultados de búsqueda de Google https://www.google.com/search/howsearchworks/algorithms/; el *feed* 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

[80] Informe de la Relatora Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, párr 66, U.N. Doc. A/HRC/47/2.

[81] Informe de la Relatora Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, párr 99, U.N. Doc. A/HRC/47/2.

- ¿Las plataformas cumplen la legislación nacional sobre protección de datos?
- ¿Las principales plataformas tienen una persona de contacto en el país? ¿Cuáles son los mecanismos disponibles para denunciar los abusos y responder a las quejas?
- ¿Existen normas que faculten a los organismos electorales para solicitar información específica sobre los usuarios a las plataformas de medios sociales?

3.2. Transparencia de la publicidad política y por temas

Una característica clave de la publicidad política moderna es que los partidos y otros actores políticos pueden dirigirse a los votantes utilizando numerosas fuentes de datos y/o mecanismos, algunos suministrados por terceros, como plataformas de medios sociales o agentes de datos. En sus directrices de 2020, el Consejo Europeo de Protección de Datos (integrado por las autoridades de protección de datos de los 27 Estados miembros de la UE) reconoció la diversidad de actores y fuentes de datos implicados, señalando que los criterios utilizados para dirigirse a los individuos "pueden haberse elaborado sobre la base de datos personales que los usuarios han proporcionado o compartido de forma activa [...] datos personales que han sido observados o inferidos, ya sea por el proveedor de medios sociales o por terceros, y recogidos (agregados) por la plataforma o por otros actores (por ejemplo, los agentes de datos) para apoyar las opciones de publicidad dirigida."[82]

En sus directrices, el Consejo de Europa ha subrayado la necesidad de que las organizaciones de campañas políticas proporcionen a los votantes "información adecuada sobre por qué ven un mensaje específico, quién responde por el mismo y cómo pueden ejercer sus derechos para evitar que ser objeto de focalización; e información sobre los criterios de focalización utilizados en la difusión de dichas comunicaciones [...] el votante debe tener derecho a saber "por qué estoy viendo este anuncio".[83]

La reciente evolución legislativa en la Unión Europea ha impuesto obligaciones adicionales para hacer cumplir la transparencia en la publicidad política. Partiendo de la base de los requisitos impuestos por el reciente Reglamento de Servicios Digitales[84] de la Unión Europea, la propuesta de reglamento sobre publicidad política amplía las categorías de información que deben ser reveladas en el contexto de la publicidad política cuando los anunciantes utilicen técnicas de segmentación o amplificación. Tal información incluye los grupos de destinatarios específicos a los que se dirige la publicidad, incluidos los parámetros utilizados para determinar los destinatarios entre los que se distribuyen los anuncios, las categorías de datos personales utilizados para la segmentación y la amplificación; cuando proceda, información que indique si los datos personales fueron derivados, deducidos o se obtuvieron de un tercero, así como la identidad del tercero y un enlace que permita acceder al aviso de protección de datos de dicho

[82] Directrices 8/2020 sobre la focalización de los usuarios de medios sociales, 2 de septiembre de 2020. Disponible en: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-82020-targeting-social-media-users_en

[83] Consejo de Europa, Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns, noviembre de 2021, párr. 4.4.5.

[84] El Reglamento de Servicios Digitales impone a determinadas plataformas en línea–las plataformas en línea de gran tamaño ("VLOP", por sus siglas en inglés) y los motores de búsqueda en línea de gran tamaño ("VLOSE", por sus siglas en inglés)–la obligación de crear repositorios de los anuncios presentados en su interfaz en línea que incluyan información sobre quién pagó por el anuncio y/o su entrega, los datos del anunciante y los criterios de focalización y entrega. Véase el considerando 95 y el artículo 39.

tercero para el tratamiento correspondiente; así como un enlace a un medio eficaz que sirva para apoyar que las personas ejerzan sus derechos de protección de datos.[85]

Aunque aún está por verse el alcance y la eficacia de estas iniciativas para mejorar la transparencia, hay un mayor reconocimiento de que la transparencia en la publicidad política puede beneficiar a la sociedad civil, a los investigadores y a los observadores electorales cuando realicen evaluaciones de la participación en línea antes y durante las elecciones.

Recomendaciones

- Las normativas nacionales (por ejemplo, los códigos de buenas prácticas) deben exigir a las empresas que sean transparentes respecto a la publicidad y las comunicaciones políticas en línea por las que pagan brindando a los usuarios información adecuada sobre por qué ven un mensaje concreto, quién es responsable de ese mensaje y cómo pueden ejercer sus derechos para evitar ser objeto de ese tipo de publicidad.
- Las plataformas de internet, incluidos los motores de búsqueda y las plataformas de medios sociales, debe deben revelar públicamente toda la publicidad, incluida la publicidad política y la publicidad basada en temas políticos. La información debe incluir como mínimo los parámetros de focalización (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, con cumplimiento de los requisitos de privacidad, para rastrear y comprender mejor la propagación y el efecto de estos anuncios políticos y de la focalización desplegada.

Preguntas

- ¿Cómo se definen y regulan jurídicamente la publicidad política en línea y la publicidad por temas?
- ¿Las principales plataformas de internet que operan en el país han formulado políticas de transparencia para los anuncios y otras formas de comunicación política, así como para la focalización?
- ¿Las principales plataformas de internet que operan en el país han permitido que los investigadores de interés público puedan monitorear y revisar la publicidad durante el período preelectoral?

Conclusión

A nivel internacional se reconocen cada vez más las numerosas formas en que se utilizan los datos personales en relación con los procesos electorales, así como los riesgos que suponen para la integridad, la imparcialidad y la libertad de las elecciones algunos tipos de tratamiento de datos.

[85] Propuesta de reglamento sobre la transparencia y la segmentación de la publicidad política, artículo 12 y Anexo II.

Las organizaciones de observadores electorales ocupan un lugar especial que les permite–en virtud de su conocimiento y comprensión del contexto local y, en algunos casos, de la práctica electoral internacional–asimilar y comentar sobre los aspectos tecnológicos y de datos del proceso electoral en cuestión.

Por ello, las organizaciones de observadores electorales cumplen un papel fundamental a la hora de garantizar que las tecnologías digitales se desplieguen de formas que protejan y promuevan los derechos de los votantes y, a la postre, fomenten unas elecciones libres e imparciales. A fin de ejercer su labor con eficacia, es necesario que revisen y actualicen sus metodologías de observación electoral de manera que puedan detectar problemas relacionados con el uso de datos y tecnologías digitales y, además, ofrecer recomendaciones para remediarlos.

Privacy International
62 Britton Street
London EC1M 5UY
Reino Unido

+44 (0)20 3422 4321

privacyinternational.org