Datos personales en padrones electorales: por qué y cómo limitarlos

Guillaume Hoffmann[0009−0001−8196−8819]

CONICET - Universidad Nacional de Córdoba, Argentina
guillaume.hoffmann@conicet.gov.ar

Abstract. En los últimos años, se ha observado un aumento notable de la publicación en línea de grandes cantidades de datos personales en forma de padrones electorales, accesibles con una simple búsqueda por la web. Esta práctica ha comprometido la privacidad de millones de argentinos. Se examinan algunas de estas filtraciones y se propone aplicar el principio de minimización de datos para salvaguardar la privacidad de los ciudadanos. En particular, se propone eliminar del padrón electoral la información referente al domicilio. En efecto, el domicilio es un dato sensible, pero no esencial para acreditar la identidad del votante. Esta propuesta busca preservar la privacidad de los ciudadanos, sin comprometer la integridad del proceso electoral.

Keywords: datos personales, bases de datos públicas, big data, doxing

1 Introducción

1.1 Principios generales del sistema electoral argentino

El sistema electoral argentino se rige por varios principios que buscan garantizar la participación democrática y el ejercicio efectivo del derecho al voto. Uno de los pilares es el voto obligatorio, donde todos los ciudadanos mayores de 18 años están legalmente obligados a emitir su voto en las elecciones nacionales, provinciales y municipales. Otro principio fundamental es el secreto del voto, que garantiza la libertad y la confidencialidad de la elección ciudadana.

Para votar, un elector debe acreditar su identidad. Para la mayoría de las personas, se trata de presentar su documento nacional de identidad (DNI). Este documento, contiene un número único a nivel nacional que identifica el elector [10]. Esto garantiza la integridad del proceso, dado que el Registro Nacional de Votantes utiliza los datos del Registro Nacional de Personas para mantener actualizado el listado de votantes habilitados.

Desde el punto de vista de las bases de datos involucradas, se debe diferenciar el Registro Nacional de Votantes del Padrón Electoral. El Registro Nacional de Votantes se encarga de mantener actualizada la lista de ciudadanos habilitados para votar en elecciones nacionales, utilizando como fuente de información el Registro Nacional de Personas. Mientras tanto, el padrón electoral es el listado

específico de votantes asignados a cada mesa de votación en una elección particular, que se extrae del Registro Nacional de Votantes y se utiliza para organizar y administrar el proceso de votación en el día de la elección. En cada mesa de votación, puede haber entre 300 y 400 ciudadanos habilitados a emitir su voto. Por lo cual es necesario un sistema automatizado que genere el listado de todas las mesas de votación, es decir el Padrón Electoral, a partir del Registro Nacional de Votantes. Las mesas de votación se distribuyen de acuerdo con la localidad de residencia de los electores, reflejado en el documento de identidad.

Por consecuente, los votantes son familiarizados con el padrón electoral. Además de interactuar con el padrón para buscar su mesa de votación, ven que el presidente de la mesa de votación maneja un documento impreso, que el votante firma después de emitir su voto. De ese documento se desprende un troquel que es la constancia de emisión de voto de cada votante. Este formato de padrón para presidente de mesa, con foto del votante y troquel, se implementó en el 2013 [3]. Incluye, además del nombre y DNI del votante, el año de nacimiento y el domicilio:

Los fiscales de los partidos políticos suelen ser equipados de una copia del padrón electoral de la mesa de votación, lo que les permite, al igual que el presidente de mesa, impugnar la identidad de una persona que pretende votar en esta mesa. La impugnación de la identidad sucede en el caso de que los datos del DNI no coinciden con los datos del padrón electoral, o que los datos del DNI no coinciden con la persona que se presenta a votar. Esos padrones no contienen ni la foto ni los troqueles, pero sí es resto de los datos de los votantes:

1.2 Marco legal del sistema electoral

La República Argentina se rige por un sistema federal donde existe una ley electoral nacional, y, en cada provincia, una ley electoral provincial. El Registro

Nacional de Votantes es único y los padrones usados en elecciones nacionales, provinciales y municipales de todo el país se desprenden de ese registro único.

Recorriendo los artículos de las leyes relevantes, podemos ver qué datos llegan desde el Registro Nacional de Votantes hasta los Padrones electorales entregados a autoridades de mesa y fiscales partidarios.

Según el Código Electoral Nacional (Ley N° 19.945) el registro nacional de electores "debe contener, por cada elector los siguientes datos: apellidos y nombres, sexo, lugar y fecha de nacimiento, domicilio, profesión, tipo y número de documento cívico, especificando de qué ejemplar se trata, fecha de identificación y datos filiatorios" (art. 16).

De este registro, se constituyen los padrones provisionales que contienen: "número y clase de documento cívico, apellido, nombre y domicilio de los inscritos" (art. 25). Son estos padrones los que sirven para que los electores verifiquen si sus datos son correctos, usualmente a través de una interfaz web. Luego, "Los padrones provisorios depurados constituirán el padrón electoral definitivo [...] que tendrá que hallarse impreso treinta (30) días antes de la fecha de la elección [...] Compondrán el padrón de mesa definitivo destinado al comicio, el número de orden del elector, un código de individualización que permita la lectura automatizada de cada uno de los electores, *los datos que para los padrones provisionales requiere la presente ley* y un espacio para la firma" (art. 29).

Luego, "la Cámara Nacional Electoral dispondrá la impresión y distribución de los ejemplares del padrón y copias en soporte magnético de los mismos [...] en los que se incluirán, *además los datos requeridos por el artículo 25*, para los padrones provisionales, el número de orden del elector dentro de cada mesa, y una columna para la firma del elector" (art. 30).

Finalmente, "el padrón de electores se entregará: [...] A las Juntas Electorales, [...] Al Ministerio del Interior [...] A los Partidos Políticos que los soliciten [...] A los Tribunales y Juntas Electorales de las Provincias" (art. 32).

Los códigos electorales provinciales siguen una estructura parecida. A continuación, veamos el caso de la provincia de Córdoba, codificado en la Ley N°9.571.

En su artículo 26, describe los datos del padrón provisorio: "a) Tipo y número de documento de identidad; b) Apellidos y nombres; c) Grado de instrucción; d) Profesión; e) Domicilio; [...]". En el artículo 33, se dispone la impresión del padrón definitivo "en los que se incluyen, *además de los datos requeridos por el artículo 26 de la presente Ley* [...] una columna para anotar la emisión del voto.".

Notablemente, no todos los datos del Registro Nacional de Electores pasan a ser parte del padrón. Por ejemplo, no se transfieren los datos de filiación, el lugar y la fecha de nacimiento. En cambio, en la provincia de Córdoba, la ley estipula que los padrones contengan el grado de instrucción del votante, pero no se encuentra en el Registro Nacional de Electores; puede ser que la ley nacional se haya actualizado más rápidamente que la normativa provincial.

1.3 Ley de protección de datos, presente y futuro

En Argentina, la ley N° 25.326 de protección de los datos personales, pretende "garantizar el derecho al honor y a la intimidad de las personas" y define los conceptos de datos personales, datos sensibles y bases de datos. Según esta ley, cualquier conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, se considera como una base de datos y es protegido por las disposiciones de la ley. Entonces, el registro nacional de votantes y cualquier padrón electoral, en sus formas electrónica o impresa, son bases de datos.

En su artículo 5, la ley N° 25.326 precisa que ciertos datos no requieren consentimiento previo del titular para su tratamiento. Entre ellos, los datos de nombre, documento nacional de identidad, ocupación, fecha de nacimiento y domicilio son explícitamente listados.

La Agencia de Acceso a la Información Pública (AAIP) fue creada en 2017 por la Ley 27.275 de Derecho de Acceso a la Información Pública. En su Resolución 86/2019, propone una guía sobre el tratamiento de datos personales con fines electorales, donde define los principios fundamentales de protección de datos personales, dos de ellos siendo particularmente relevantes en este trabajo:

- Finalidad. Los datos deben ser tratados conforme a la finalidad que se haya declarado al momento de obtenerlos. Se podrán emplear los datos para otros fines que sean compatibles con la finalidad principal, si y sólo si estos pudieran haber sido razonablemente previstos por el titular de datos.
- Proporcionalidad. Los datos recolectados deben ser proporcionales y no excesivos en relación con la finalidad que se hubiese declarado para su obtención.

Si bien la guía mencionada trata principalmente de datos a fines electorales recogidos por encuestas, páginas web y aplicaciones, estos dos principios nos ayudan a identificar el problema con algunos datos embedidos en los padrones electorales. De hecho, estos principios son la traducción del artículo 4 de la ley 25.326, según el cual "los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido".

¿Qué pasará en el futuro en cuanto a esta normativa? En el año 2018, y luego en el 2023, se presentó en el Congreso de la Nación un proyecto de reforma integral de la ley de protección de los datos personales. Ese proyecto incluye el *principio de minimización de datos*: "Los datos personales deben ser tratados de manera que sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que fueron recolectados".

A continuación, vamos a revisar recientes casos de filtraciones de padrones electorales por vía de páginas web en libre acceso. En su mayoría, se tratan de padrones electorales provenientes del Registro Nacional de Electores, pero también relevamos padrones de otras fuentes, como partidos políticos. Luego, vamos a considerar distintos riesgos de daños que son consecuencia de la difusión de esas bases de datos: la política computacional y microsegmentación electoral; las potenciales amenazas físicas consecuencia de la revelación del domicilio del

votante; y las estafas y extorsiones. Este artículo concluye con la propuesta de restringir la información contenida en los padrones electorales, con el objetivo de limitar estos riesgos.

2 Padrones encontrados en la web

En esta sección, describimos un conjunto de padrones encontrados en el año 2020 con simples búsquedas por la web. Esos padrones estaban disponibles en formato PDF, sin necesidad de identificarse para acceder a ellos. Esos padrones fueron denunciados por red social por el autor de este artículo, a través de una cuenta con un alcance de unos 300 seguidores. Esos archivos habían estado disponibles en la web abierta durante por lo menos seis meses, en caso de los padrones correspondientes a elecciones del año 2019, y mucho más para otros. Las motivaciones de esas denuncias fueron visibilizar la problemática y lograr que se retiren esos padrones de la web abierta. De hecho, la mayoría de esos padrones fue retirada en cuestión de días luego de esas denuncias, y la gran mayoría de los actores que difundieron esos padrones, no volvieron a hacerlo para las elecciones del año 2023.

Provincia de Córdoba El padrón definitivo de electores para las elecciones nacionales del 27 de octubre del 2019, para todos los circuitos de la provincia de Córdoba, se encontró subido a la web del partido político Hacemos por Córdoba desde octubre del 2019, hasta mayo del 2020, fecha en la cual el hecho fue denunciado por redes sociales y los archivos fueron retirados al día siguiente. Esos archivos PDF eran destinados a fiscales de ese partido político. En ellos se encuentran los datos de los 2.231.859 electores de la provincia de Córdoba: nombre, DNI, domicilio y año de nacimiento.

Provincia de Salta En este caso, se trata del mismo Tribunal Electoral de la Provincia de Salta que ponía a disposición del público, a través de su página web, los padrones definitivos de las elecciones primarias y generales 2019, hasta mayo del 2020. Se proveía un archivo para toda la provincia, además de un PDF para cada municipio. Esos padrones incluyen domicilio, edad y profesión, acerca de los 1.027.208 electores argentinos y 7.089 extranjeros de la provincia de Salta.

Municipios de Córdoba, Santa Fe y Neuquén Siguiendo con ese relevamiento, se encontraron padrones conteniendo los datos de unos casi 170.000 votantes de 12 localidades de la provincia de Córdoba (Alcira Gigena, Bell Ville, Colonia Caroya, Corral de Bustos Ifflinger, Hernando, Mendiolaza, Morteros, Río Ceballos, Salsipuedes, San Antonio de Arredondo, San Pedro Norte y Villa Dolores), incluyendo el domicilio. Los padrones mencionados referían a elecciones del 2015 y 2019. Los medios de difusión de esos padrones son distintos de los casos anteriores: en la mayoría de los casos, los padrones se encontraban subidos a la propia página web de los municipios o de sus concejos deliberantes (con dominio en `.gob.ar`). Pero también, en algunos casos, los padrones se encontraban en

páginas de medios de comunicación locales. También, encontramos el padrón 2019 de los 1.183 votantes de la comuna de Cafferata (Santa Fe), con domicilio y año de nacimiento de los votantes; y el padrón 2015 de Zapala (Neuquén), con 27.612 habitantes, incluyendo domicilio, profesión y año de nacimiento.

Padrones de partidos políticos Según la Ley Orgánica de Partidos Políticos (N° 23.298), el registro de afiliados y el padrón partidario son públicos (art. 26 y 27). Si bien el artículo 23 precisa que para afiliarse, es necesario dar su "nombre y domicilio, matrícula, clase, estado civil, profesión u oficio y la firma o impresión digital", la ley no indica qué datos deben estar en el registro de afiliados y los padrones.

A continuación, unos ejemplos donde los padrones se publicaron como archivos PDF por las páginas web de los propios partidos, conteniendo nombre, número de DNI, año de nacimiento y domicilio:

- la Unión Cívica Radical de Córdoba, más de 100.000 afiliados de la provincia de Córdoba, del 2021 y 2023
- la Unión Cívica Radical de Chubut, un padrón de afiliados del 2016 (25.145 personas) y otro del 2018 (29.471 personas)
- el Partido Justicialista de la Provincia de Buenos Aires, 1.343.234 afiliados, del 2015.
- el Partido Justicialista de la Provincia de Salta, 98.931 afiliados, del 2022.

Finalmente, el Partido Justicialista nacional publicó el padrón de todos sus afiliados en el país en su página web en el 2020, por cada provincia, incluyendo el nombre y DNI de 3.173.622 personas; pero sin domicilio, ni año de nacimiento.

Otros casos Se encontraron varios padrones con nombre, número de DNI y domicilio, para elecciones internas de universidades y de colegios profesionales.

2.1 Permanencia, difusión y valor de estos datos

Si bien la mayoría de esos padrones fue retirada de sus correspondientes páginas web, en algunos casos los archivos siguen disponibles en la plataforma en línea "The Wayback Machine", que se dedica a la preservación de contenido web a lo largo del tiempo. Generalmente, estamos conscientes que a nivel mundial, es probable que estos datos estén todavía en poder de estados, empresas y privados que los hayan compilado [15]. Las herramientas legales para solicitar la remoción de esos archivos parecen limitadas [18], esencialmente porque a los ojos de la ley 25.326, se trata de datos públicos.

En los términos de la inteligencia de fuentes abiertas (*Open Source Intelligence*), un padrón electoral es una fuente de datos estructurada [11]; a diferencia de, por ejemplo, una página web con texto libre. El valor de un padrón electoral como fuente de información es no solamente la cantidad de información que contiene, sino que se encuentra convenientemente presentada, incluso para procesamientos de datos de bajo presupuesto. Todos los archivos mencionados en esta sección se presentaban como archivos PDF cuyo texto puede ser extraído sin necesidad de reconocimiento óptico de caracteres.

3 Riesgos de daño

3.1 Microsegmentación electoral

La microsegmentación o microtargeting electoral se refiere a la estrategia de segmentar el electorado en grupos específicos con el fin de dirigir mensajes políticos personalizados y adaptados a sus intereses y preferencias, utilizando datos demográficos, comportamentales y de preferencias para influir en sus decisiones electorales [19]. En Argentina, informes reportan que la microsegmentación se empezó a usar en las elecciones del 2015 [9].

En [1], se reportan las actividades de varias empresas en Estados Unidos especializadas en la elaboración de bases de datos de votantes. En efecto, se estima que el fenómeno de la microsegmentación tuvo su auge en el 2008, más temprano que en Argentina. Desde entonces, las campañas electorales están interactuando cada vez más con los votantes basándose en datos, una práctica conocida como política computacional. Esta estrategia implica el uso de métodos computacionales para analizar grandes conjuntos de datos provenientes de fuentes en línea y fuera de línea.

Ciertas empresas gestionan extensas bases de datos que incluyen datos de cientos de millones de votantes y consumidores, ofreciendo a las campañas cientos de puntos de datos para identificar y movilizar a los votantes que probablemente apoyen a su candidato. Esas empresas combinan datos de consumidores con padrones electorales para permitir búsquedas basadas en criterios como precio de compra de vivienda, calificación crediticia o propiedad de mascotas [1].

La riqueza de los datos disponibles en el padrón electoral permite inferir con cierta probabilidad la religión o identidades sociales a partir del nombre [6]. Asimismo, mapas del valor inmobiliario pueden ayudar a predecir, a partir del domicilio de un votante, sus ingresos [14, 5]. Todo ello, junto con puntos de datos obtenidos desde otras bases de datos, permite inferir con cierta probabilidad las preferencias de voto de los electores [24]. Si bien el pronóstico del voto, no constituye estrictamente una violación del secreto del voto, una vez combinado con un ataque de abstención forzada [13] podría ser una manera de influenciar en el resultado una elección.

3.2 Doxeo y domicilio

El estudio pormenorizado del doxeo (o doxing) en la academia es relativamente reciente [2]. La mayoría de los artículos que se publicaron sobre el asunto son de la mitad de los años 2010. Eso indica que la toma de consciencia del problema del doxeo es relativamente reciente, y que por eso hay muy pocas campañas de prevención. Tampoco existe figura legal para calificarlo como delito.

Si buscamos una definición del doxeo desde organismos estatales argentinos, encontramos un documento en la web del Ministerio de Justicia dedicado exclusivamente al tema. El documento define el doxeo como la recopilación y publicación de información personal de alguien o de un grupo, sin su consentimiento, con el objetivo de dañar su trayectoria pública y profesional. Entre la

información personal sensible, se mencionan la dirección física de la persona y su lugar de trabajo.

Notamos que según esta definición, el problema con el doxeo tiene que ver exclusivamente con el el "doxeo de desanonimización" (revelar la identidad de alguien) y el "doxeo de deslegitimación" (dañar la reputación de una persona). Pero existe un tercer tipo de doxeo, no mencionado ahí: el doxeo "targeting", es decir tomar a alguien como blanco, apuntar a una persona [8].

El "targeting" crea la posibilidad de que el hostigamiento futuro se presente de forma física, con la incertidumbre y el riesgo que ello trae. El domicilio es una información personal que es usualmente difícil de encontrar y que revela detalles específicos de un individuo. Una vez divulgada la dirección de una persona a terceros, esos pueden hacerse presentes, observar sus movimientos, sus costumbres, su apariencia física y sus características [8].

El concepto de localizabilidad permite entender mejor la percepción del riesgo cuando uno sabe que su domicilio fue revelado. Las motivaciones por las cuales proteger el dato de su domicilio consisten en proteger su tiempo, espacio y persona, es decir prevenir todo tipo de hostigamiento, y proteger sus bienes [16].

En este aspecto, los Lineamientos para la Gobernanza de Datos de la Ciudad de Buenos Aires, publicados en el 2023, reconocen esta amenaza física. Mencionan que "el domicilio en algunas circunstancias debería ser considerado como un dato sensible. Por ejemplo: Casos de violencia de género, personas expuestas públicamente, etc. Su posible divulgación sugiere un riesgo en la persona: vulnera su intimidad y privacidad." Por ello, el acto de revelar datos personales de una persona es una forma de acoso en línea.

3.3 Estafas y extorsiones

Finalmente, las consecuencias de la nueva accesibilidad del dato de domicilio de millones de votantes favorecen ciertas acciones dañinas, algunas de ellas volviéndose más eficientes cuando se realizan a gran escala.

Primero, la suplantación de identidad [4], permite hacer fraudes financieros, adquirir deudas en nombre de la víctima, y acceder a información confidencial de empresas. Requiere la posesión de datos personales de la persona suplantada.

Otro tipo de estafa es el secuestro virtual [23], caracterizado por un formato de extorsión telefónica, donde el atacante intenta convencer a una persona que ha secuestrado un miembro de su familia y reclama una suma de dinero para "liberar" a esa persona. Esta práctica delictiva se desarrolló en los últimos años. En Argentina, es conocida por vía de prensa desde los años 2000. Un informe del Banco Interamericano de Desarrollo del 2017 señala que el 70% de las extorsiones en América latina se gestionan desde las cárceles [12]. Este modo de estafa o extorsión se beneficia con la disponibilidad de grandes bases de datos personales, no solo porque proporcionan más información acerca de cada persona, sino también porque amplían el universo de personas objetivo, generando oportunidades de manera oportunista.

3.4 Percepción del riesgo de daño

Cuando la información pública se convierte en datos más accesibles, compartibles y buscables, esto tiene profundas implicaciones en la privacidad. La preocupación de los ciudadanos, al saberse potencialmente vigilados, tiene consecuencias en su comportamiento. Una encuesta del 2005 encontró que el 23% de los votantes de California no se registraron para votar porque quieren que sus datos permanezcan privados. Este tipo de efecto inhibidor se puede manifestar también en el comportamiento de los votantes en cuanto a expresar sus opiniones, afiliarse o actuar políticamente [20].

En México, una encuesta del 2020 encontró que más del 60% de los participantes contestaron "sí" a la pregunta "Si en este momento te ofrecieran ocultar tus datos personales en tu credencial para votar, ¿lo harías?". A los que contestaron "sí", se les preguntó "Si decidiste ocultar tus datos, ¿cuál fue el motivo general para hacerlo?", y más del 80% contestó "por seguridad" [17].

En un estudio comparando distintas formas de acoso en línea, se midió la percepción del daño potencial desde el punto de vista psicológico, físico y sexual [21]. El doxeo fue la forma de acoso que conlleva más daño físico percibido, además de altos niveles de daño psicológico y sexual percibido, siendo solo superado por la divulgación no autorizada de imágenes íntimas.

Podemos concluir que la puesta a disposición y difusión de padrones electorales conteniendo datos personales genera riesgos de daños que son comprendidos por la ciudadanía, y que esta podría apoyar medidas preventivas que resguarden su seguridad.

4 Propuestas

4.1 Eliminación de datos personales

Por las razones expuestas anteriormente, proponemos eliminar en prioridad el dato del domicilio de los padrones electorales. De esa manera, Argentina se sumaría a otros países de la región, como Chile, Bolivia, Paraguay y Perú, que tampoco incluyen ese dato en el padrón de mesa.

Debemos aclarar que cierta inferencia puede todavía operarse en cuanto a la ubicación geográfica de los votantes. En efecto, que un votante aparezca en el padrón de una mesa de votación da cierta indicación sobre su domicilio, usualmente se puede inferir la localidad en la cual se encuentra, y si es una localidad grande, en qué zona de ella. Pero igualmente se reduciría drásticamente la localizabilidad de los votantes con respecto a la situación actual.

Proponemos además eliminar datos que puedan ayudar a inferir la edad de los votantes. El objetivo es dificultar la inferencia de estructuras familiares desde padrones electorales. Por ello, es obvio el beneficio de eliminar el año de nacimiento.

Sin embargo, el dato del DNI completo permite también inferir la edad de la persona, dado que los números de DNI son asignados de manera cronológica dentro de determinados rangos de valores. Es decir que hay aproximaciones posibles de la forma $EDAD = (DNI \times x) + y$.

U de la
Univ yó el
nomb
A :

REGISTRO NACIONAL DE ELECTORES
CÁMARA NACIONAL ELECTORAL
ELECCIONES NACIONALES 2019

SECCIÓN ELECTORAL
DISTRITO: 01 - PROVINCIA
SECCIÓN: 0001 - DEPARTAMENTO
CIRCUITO: 001 - LOCALIDAD
MESA: 1234

PADRÓN DEFINITIVO DE ELECTORES INSCRIPTOS AL 30 DE ABRIL DE 2019

NRO. ORDEN	APELLIDO_1, NOMBRE_1				NRO. ORDEN	APELLIDO_17, NOMBRE_17			
1	DOC. xx.xxx.111	DNI-EA		VOTÓ ☐	17	DOC. xx.xxx.717	DNI-EA		VOTÓ ☐
NRO. ORDEN	APELLIDO_2, NOMBRE_2				NRO. ORDEN	APELLIDO_18, NOMBRE_18			
2	DOC. xx.xxx.222	DNI-EB		VOTÓ ☐	18	DOC. xx.xxx.818	DNI-EB		VOTÓ ☐
NRO. ORDEN	APELLIDO_3, NOMBRE_3				NRO. ORDEN	APELLIDO_19, NOMBRE_19			
3	DOC. xx.xxx.333	DNI-EC		VOTÓ ☐	19	DOC. xx.xxx.919	DNI-EC		VOTÓ ☐

Señalamos que el número de DNI truncado deja de ser único, y es posible, aunque poco probable, que existan conjuntos de personas con el mismo nombre completo y los mismos últimos tres dígitos de DNI. Si eso sucede en una misma mesa de votación, se debe arreglar incluyendo más dígitos hasta que la ambigüedad se resuelva. En el caso de personas en distintas mesas, este sistema implica un riesgo de doble votación que debe ser considerado.

4.2 Trazabilidad de la información

No obstante las propuestas anteriores, se debe desalentar la difusión de los padrones electorales por la web. Sería fundamental acompañar los padrones dados a los partidos políticos, con instrucciones sobre los riesgos de su difusión. Esas instrucciones podrían ser un simple mensaje en la tapa del documento.

Además, se puede incorporar una marca de agua transaccional en los archivos [7]. Esta marca de agua permitiría asegurar la trazabilidad de la información, una idea que tiene sus orígenes en la aplicación del derecho de autor. El objetivo es responsabilizar al partido político correspondiente en caso de que se filtre alguno de estos archivos.

5 Conclusiones

En Argentina, a partir de los años 2010, aumentó la gestión de padrones electorales como archivos electrónicos. Esto hizo que se empezaran a encontrar padrones electorales en libre acceso por la web, algunos de ellos permaneciendo disponibles mucho tiempo después de la fecha de la elección en cuestión. Estos datos antes existían solo en forma impresa y tenían poca difusión. Este cambio de accesibilidad tiene un impacto sobre la privacidad de los ciudadanos. La privacidad no se define solamente por la difusión o no de datos personales, sino que se ve afectada por la modificación de la accesibilidad de esos datos [22].

Hemos identificado distintos riesgos de daño, con adversarios que pueden hacer un uso pernicioso de esos datos. Uno es un adversario computacionalmente dotado, trabajando con grandes conjuntos de datos, cuyos intereses pueden incluir la microsegmentación electoral, la vigilancia poblacional en general y la

venta de bases de datos. Otro es un adversario humano, que puede alcanzar físicamente a una persona de interés para infligir algún tipo de molestia, hostigamiento o daño físico. Existe en efecto una alta percepción del daño potencial por la difusión de datos personales, en particular del domicilio, que es el dato que más se relaciona con la potencialidad de un daño físico. Además, la disposición de estos datos facilita varias modalidades de estafa y de extorsión.

Reducir o incluso eliminar por completo la difusión de esos padrones en la web, obteniendo la remoción de los archivos, es insuficiente ya que estos archivos siguen en circulación entre los partidos políticos y otras autoridades a cargo de gestionar las elecciones. Por lo tanto, la propuesta acá es además la eliminación de datos en los padrones.

El texto del Código Electoral Nacional está en falta con respecto al principio de finalidad de datos del artículo 4.3 de la Ley 25.326. El dato de domicilio de los votantes es necesario para confeccionar los padrones electorales, clasificados según la jerarquía de distrito, sección, circuito y mesa. Por eso figura necesariamente en el Registro Nacional de Electores. Pero es un error incluirlo *dentro* de los padrones electorales, ya que no se usa para identificar a los votantes. Por un lado porque otros datos más pertinentes sí se usan para identificar a los votantes y son suficientes: el nombre y número del DNI. Y por otro lado, el domicilio indicado en el DNI es un dato que, para muchos de nuestros conciudadanos, no se corresponde con su residencia actual. Además, planteamos eliminar otros datos que permiten inferir información sensible, como es el año de nacimiento.

Para corregir esta situación, una posibilidad obvia es la emisión de una nueva norma por parte del Poder Legislativo de la Nación, que actualizaría el Código Electoral Nacional. Otra opción sería una acción de amparo, siguiendo el precedente de la Asociación por los Derechos Civiles en el caso de las fotos de identidad agregadas a los padrones de presidentes de mesa en el 2013 [3].

Cabe destacar que las sugerencias planteadas en este artículo no pretenden ser soluciones definitivas a la problemática de la difusión de datos personales en padrones electorales, sino que son propuestas basadas en la experiencia previa y en el análisis de riesgos identificados. La implementación de estas medidas requiere un análisis más profundo y un consenso entre las partes interesadas para garantizar su efectividad y aceptación. En Argentina, la protección de los datos personales demanda una reforma integral, con la modificación de varias leyes además de un cambio de paradigma en la sociedad toda. Solo en este 2024, las masivas filtraciones de datos como las del Registro Nacional de Personas y de las licencias de conducir, nos recuerdan la urgencia de la situación actual. Es fundamental que, junto con el Estado nacional, los Estados provinciales y municipales, además del sector privado, adopten una nueva mentalidad respecto a la creación y manejo de bases de datos, asegurando que se priorice la privacidad y la seguridad de los ciudadanos.

References

1. Akosah, K.N.: Cracking the one-way mirror: How computational politics harms voter privacy, and proposed regulatory solutions. Fordham Intell. Prop. Media &

Ent. LJ (2014)
2. Anderson, B., Wood, M.A.: Doxxing: A scoping review and typology. The Emerald international handbook of technology-facilitated violence and abuse (2021)
3. Asociación por los Derechos Civiles (ADC): El Estado recolector. Un estudio sobre la Argentina y los datos personales de los ciudadanos (2014)
4. Borghello, C., Temperini, M.G.: Suplantación de identidad digital como delito informático en argentina. In: X Simposio Argentino de Informática y Derecho (2012)
5. Carranza, J.P., Piumetto, M.A., Lucca, C.M., Da Silva, E.: Mass appraisal as affordable public policy: Open data and machine learning for mapping urban land values. Land Use Policy (2022)
6. Chaturvedi, R., Chaturvedi, S.: It's all in the name: A character-based approach to infer religion. Political Analysis **32**(1), 34–49 (2024)
7. Cox, I.J., Miller, M.L., Bloom, J.A.: Watermarking applications and their properties. In: Proceedings international conference on information technology: coding and computing. IEEE (2000)
8. Douglas, D.M.: Doxing: a conceptual analysis. Ethics and information technology **18**(3), 199–210 (2016)
9. Ferreyra, E.: Democracia segmentada: Acerca de la explotación de datos personales con fines electorales. Informe, Asociación por los Derechos Civiles (2019)
10. Fundación Vía Libre: Gestión de datos personales por parte del Estado (2024)
11. Gibson, H.: Acquisition and preparation of data for OSINT investigations. Open source intelligence investigation: From strategy to implementation (2016)
12. Jaitman, L., Caprirolo, D.: Los costos del crimen y de la violencia: nueva evidencia y hallazgos en américa latina y el caribe. Informe, Banco Interamericano de Desarrollo (2017)
13. Juels, A., Catalano, D., Jakobsson, M.: Coercion-resistant electronic elections. In: Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society (2005)
14. Lu, J., Zhou, S., Liu, L., Li, Q.: You are where you go: Inferring residents' income level through daily activity and geographic exposure. Cities (2021)
15. Lyon, D.: Surveillance, Snowden, and big data: Capacities, consequences, critique. Big data & society **1**(2), 2053951714541861 (2014)
16. Marx, G.T.: What's in a name? Some reflections on the sociology of anonymity. The information society **15**(2), 99–112 (1999)
17. Morales, V.H.S.: Protección de datos personales en credencial para votar, a examen de la información pública. derecho a la privacidad vs. principios rectores de la función electoral. Estudios en derecho a la información (2020)
18. Puccinelli, O.: El derecho al olvido digital. La nueva cara de un derecho tan viejo como polémico. Revista Derecho Constitucional (2019)
19. Romero Fierro, S.: El desafío regulatorio de las nuevas tecnologías: análisis del uso de datos personales e inteligencia artificial en el contexto de campañas electorales. Una mirada nacional y comparada. Tesis de pregrado, Universidad de Chile (2023)
20. Rubinstein, I.S.: Voter privacy in the age of big data. Wis. L. Rev. (2014)
21. Schoenebeck, S., Lampe, C., Trieu, P.: Online harassment: Assessing harms and remedies. Social Media+ Society **9**(1), 20563051231157297 (2023)
22. Solove, D.J.: Access and aggregation: Public records, privacy and the constitution. Minn. L. Rev. **86**, 1137 (2002)
23. Uriel, D.G.: Los secuestros virtuales. Revista Penal México **11**(21), 167–190 (2022)
24. Vercelli, A.H.: El extractivismo de grandes datos (personales) y las tensiones jurídico-políticas y tecnológicas vinculadas al voto secreto. THEMIS: Revista de Derecho (2021)