Efectos individuales y colectivos de la difusión de padrones electorales en Argentina
Guillaume Hoffmann
SADIO Electronic Journal of Informatics and Operations Research (EJS) Vol. 24 No. 2 (2025) e-ISSN 1514-6774
https://doi.org/10.24215/15146774e079 | https://revistas.unlp.edu.ar/ejs
Sociedad Argentina de Informática e Investigación Operativa | Universidad Nacional de La Plata | Buenos Aires | Argentina

Efectos individuales y colectivos de la difusión de padrones electorales en Argentina

Individual and Collective Effects of the Dissemination of Electoral Rolls in Argentina

Guillaume Hoffmann[0009−0001−8196−8819]

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

Abstract. En Argentina, la publicación de padrones electorales en la web abierta ha generado un impacto significativo en la privacidad individual y en el equilibrio del debate democrático. La exposición de datos personales, en particular el domicilio, ha facilitado diversas formas de hostigamiento digital y de fraude, afectando tanto a ciudadanos comunes como a figuras públicas. Este artículo analiza casos concretos de filtraciones de padrones y examina los riesgos asociados a la accesibilidad masiva de estos datos. Se plantea la necesidad de limitar la publicación de padrones, eliminar datos innecesarios y establecer mecanismos de monitoreo para su remoción en la web.

Keywords: datos personales, doxing, libertad de expresión, participación ciudadana

Abstract. In Argentina, the publication of electoral rolls on the open web has had a significant impact on individual privacy and the balance of democratic debate. The exposure of personal data, especially home addresses, has facilitated various forms of digital harassment and fraud, affecting both ordinary citizens and public figures. This article analyzes specific cases of electoral roll leaks and examines the risks associated with the mass accessibility of this data. We argue for restricting the publication of electoral rolls, eliminating non-essential data, and implementing monitoring mechanisms to ensure their removal from the web.

Keywords: personal data, doxing, free speech, citizen participation

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,

Received May 2025; Accepted June 2025; Published July 2025

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 [15]. 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 administrar el proceso de votación. En cada mesa de votación, puede haber entre 300 y 400 ciudadanos habilitados a emitir su voto. Por lo cual se utiliza un sistema automatizado que genera 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. En cada mesa de votación, el presidente de la mesa maneja el padrón impreso de dicha mesa, 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 [6]. Incluye, además del nombre y DNI del votante, el año de nacimiento y el domicilio:

Los fiscales de los partidos políticos suelen tener una copia del padrón 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:

REPÚBLICA ARGENTINA

REGISTRO NACIONAL DE ELECTORES

CÁMARA NACIONAL ELECTORAL

ELECCIONES GENERALES 2023

PADRÓN DEFINITIVO DE ELECTORES INSCRIPTOS AL 25 DE ABRIL DE 2023

SECCIÓN ELECTORAL
DISTRITO: 02 - BUENOS AIRES
SECCIÓN: 3
CIRCUITO: 12 - SAN VICENTE
MESA: 0123

NRO. ORDEN	APELLIDO NOMBRE				NRO. ORDEN	APELLIDO NOMBRE			
001	PALERMO 320				017	SARMIENTO 743			
	DOC. 111.111.111	DNI-EA	1954	VOTÓ ☐		DOC. 111.111.111	DNI-EB	1993	VOTÓ ☐

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 esos 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 y su 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.".

En la práctica, 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 provincial.

1.3 Ley de protección de los datos personales

En Argentina, la ley N° 25.326 de protección de los datos personales, del año 2000, 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. Entonces, el registro nacional de votantes y cualquier padrón electoral, en sus formas electrónica o impresa, son bases de datos protegidas por esa ley.

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 otras fuentes, como listas de afiliados a partidos políticos. Luego, vamos a hacer un repaso sobre análisis anteriores de riesgos de daños asociados con 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. Luego de este repaso, hacemos un análisis cualitativo a partir del caso de los legisladores de la provincia de Córdoba y de los datos que se pueden encontrar e inferir desde el padrón electoral difundido en el 2019. Seguimos con los impactos colectivos de la difusión de estos datos personales a gran escala en la participación ciudadana y la libre expresión. Este artículo concluye con la propuesta de restringir la información contenida en los padrones electorales y remediar a la difusión de ellos en la web abierta, con el objetivo de limitar todos estos riesgos.

2 Padrones encontrados en la web

En esta sección, describimos un conjunto de padrones encontrados con simples búsquedas por la web, principalmente en el año 2020. 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 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 departamentos de la provincia de Córdoba salvo uno (Sobremonte), se encontró subido a la web del partido político Hacemos por Córdoba desde octubre del 2019, hasta mayo del 2020, fecha en la cual los archivos fueron retirados. Esos archivos PDF eran destinados a fiscales de ese partido político. En ellos se encuentran los datos de 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. En el 2023, los municipios de Bell Ville, Oliva, Villa Allende y Villa Carlos Paz publicaron sus padrones hasta por lo menos principios del 2025. 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`). 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 toda la provincia, 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 y del 2023.

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 Aparecen periódicamente padrones con nombre y número de DNI para elecciones en colegios profesionales y universidades. Por ejemplo, buscando en el dominio `uba.ar` (Universidad de Buenos Aires), encontramos alrededor de 40 archivos PDF de padrones electorales correspondiendo al mes de agosto del 2024; para el dominio `unc.edu.ar` (Universidad Nacional de Córdoba), el número se eleva a 50 padrones disponibles desde mayo del 2024. Estos archivos siguen disponibles a la fecha de enero del 2025, y contienen nombre completo y DNI, aunque en el caso de la UNC la mayoría de los padrones solo revela los últimos tres dígitos del DNI.

Permanencia 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. Además, esos datos estan probablemente en poder de estados, empresas y privados que los hayan compilado y conservado [21].

En los términos de la inteligencia de fuentes abiertas (*Open Source Intelligence*), un padrón electoral es una fuente de datos estructurada [16]; 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 [29]. En Argentina, se reporta que la microsegmentación se empezó a usar en las elecciones del 2015 [14].

En los Estados Unidos, varias empresas se especializan en la elaboración de bases de datos de votantes. Se estima que el fenómeno de la microsegmentación tuvo su auge en el 2008. Desde entonces, las campañas electorales están interactuando cada vez más con los votantes basándose en datos, una práctica conocida como política computacional. Dichas empresas gestionan extensas bases de datos acerca de cientos de millones de votantes y consumidores, ofreciendo a sus clientes cientos de puntos de datos para identificar y movilizar a votantes. 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 [2].

Los datos disponibles en el padrón electoral permiten inferir con cierta probabilidad algunas informaciones concretas. Por ejemplo, con tan solo el nombre de una persona, se puede inferir la religión o identidades sociales [12]. Asimismo, el domicilio permite estimar los ingresos de un votante [20, 10]. 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 [35]. Si bien el pronóstico del voto no constituye estrictamente una violación del secreto del voto, una vez combinado con un ataque de abstención forzada [19] puede ser una manera de influenciar el resultado una elección.

3.2 Doxeo y domicilio

El estudio pormenorizado del doxeo (o doxing) en la academia es relativamente reciente [4]. La mayoría de los artículos que se publicaron sobre el asunto son de la mitad de los años 2010, indicando que la toma de consciencia del problema es relativamente reciente.

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 [13].

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 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 [13].

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 [22].

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

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 [8] permite hacer fraudes financieros como adquirir deudas en nombre de la víctima o acceder a información confidencial de empresas. Requiere la posesión de datos personales de la persona suplantada.

Otro tipo de estafa es el secuestro virtual [34], 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 [18]. 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.

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 del estado 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 [30].

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" [23].

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 [31]. 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 Análisis de caso: legisladores de Córdoba

4.1 Presentación del análisis

En la sección anterior, detallamos los riesgos de daños asociados con la difusión de padrones electorales, y en la sección que la precede, reportamos casos concretos de padrones filtrados. Si bien estas dos informaciones son en teoría suficientes para generar consciencia del problema, es útil e incluso necesario poner el foco en casos particulares suficientemente evocadores.

A continuación, confrontamos el listado de los 70 legisladores provinciales de Córdoba, electos en el 2019, con el padrón electoral difundido ese mismo año. Por ley, los legisladores deben ser domiciliados en la provincia de Córdoba, por lo cual sus datos deben estar en esa base de datos. Los 70 legisladores provinciales se componen de 26 legisladores departamentales y 44 legisladores del distrito único. Se toma la lista de los legisladores electos, no incluyendo a sus reemplazos durante el período 2019-2023.

Desde ya, este conjunto de personas no constituye una muestra representativa del total de las personas en el padrón de la provincia de Córdoba, y se trata de un enfoque más bien cualitativo que involucra a personas ya expuestas públicamente. Todos esos legisladores tienen una declaración jurada patrimonial pública disponible en la web de la legislatura; de ahí se pueden conseguir algunos datos presentes en el padrón electoral, como su DNI. Las búsquedas a continuación se hacen con el nombre completo sin DNI.

Los padrones difundidos por Hacemos por Córdoba incluyeron a 25 de los 26 departamentos por lo cual de los 70 legisladores, una no tiene ocurrencia en esta base de datos, presuntamente por tener domicilio en el departamento faltante. Cada departamento tiene un PDF asociado, salvo el departamento Capital, que es dividido en catorce archivos. La base de datos se compone entonces de 38 archivos PDF, que se pueden fácilmente convertir a texto bruto con el programa `pdftotext` para ser luego buscados con el programa `grep`.

4.2 Datos inferidos: co-ocurrencias de domicilios

Los nombres completos de 64 legisladores tienen una ocurrencia única en la base de datos. Además de la legisladora no listada, otros cinco nombres completos de legisladores tienen entre 2 y 67 ocurrencias. Es decir, existen más de una persona en el padrón con el mismo nombre completo.

En el caso de ocurrencia única del nombre, se puede encontrar el correspondiente dato del domicilio del legislador; cabe recordar que ese dato es el domicilio indicado en el documento de identidad, y puede ser distinto del actual paradero o lugar de residencia de la persona.

Una búsqueda con `grep` o con la función "buscar" de cualquier editor de texto es una búsqueda exacta que no toma en cuenta las variaciones y errores de ortografía, por lo cual los resultados siguientes son conservadores y podrían ser extendidos aplicando alguna normalización sobre las direcciones.

De los 64 legisladores, seis tienen más de diez co-ocurrencias en su domicilio. En dos casos, porque su dirección es "[Calle] Pública 0", una práctica común en localidades pequeñas donde las calles no tienen una designación oficial. En un caso porque su dirección es "[Nombre de Calle] 0", que también sucede cuando alguna calle tiene nombre pero no una numeración oficial. En los últimos tres casos, la dirección es completa y, como lo vamos a confirmas más adelante, se tratan de direcciones con varias unidades habitacionales.

Entre los 58 legisladores que quedan, 18 son ocurrencia única en su domicilio; 12 tienen dos co-ocurrencias; 5 tienen tres co-ocurrencias; 7 tienen 4 co-ocurrencias; 7 tienen 5 co-ocurrencias; 4 tienen 6 co-ocurrencias; 2 tienen 7 co-ocurrencias y 3 tienen 8 co-ocurrencias.

Una co-ocurrencia en el padrón tiene como consecuencia el acceso al nombre completo de una persona viviendo en el mismo domicilio, con su DNI y su año de nacimiento. El apellido en común puede indicar una relación familiar con la persona de interés. Además, el nombre indica, en casi todos los casos, el sexo de la persona relacionada. Tomando en conjunto el apellido, año de nacimiento y sexo, se puede inferir alguna estructura familiar. Con sexos opuestos, apellidos distintos y años de nacimientos cercanos, se puede suponer una relación de pareja. Sumándole el mismo apellido del padre a personas con nacimientos unos 20 a 40 años después del padre, se puede concluir a una relación de padre-hijos.

Las inferencias tienen límites ya que también se puede explicar que varias personas tengan el mismo domicilio en el caso de haber sido inquilinas o sucesivas dueñas de una propiedad. Si bien la página web del gobierno nacional argentino indica que cualquier cambio de domicilio implica tramitar un nuevo ejemplar de DNI, en la práctica esta obligación no se hace cumplir y muchas personas – no se sabe en qué proporción – tienen un domicilio en el DNI que discrepa con su domicilio actual.

4.3 Uso de Google Maps y Google Street View

Para dar cuenta del mayor riesgo asociado con el doxeo, que tiene que ver con la posibilidad de apersonarse en el domicilio de alguien, usamos la aplicación Google Maps que es de uso muy común en Argentina. Google Maps ofrece para esta tarea la practicidad de corregir automáticamente direcciones que tengan aproximaciones ortográficas. Además, propone la función Street View, que permite, en algunos casos, confirmar el tipo de domicilio buscado, ya sea una casa o un edificio.

Omitiendo los legisladores con más de una ocurrencia en el padrón, y los legisladores cuya dirección es "Pública 0", quedan 62 legisladores. Dado que para 5 de ellos, la dirección no permite identificar una calle, los casos más interesantes son 57.

Para 41 de ellos, es muy fácil identificar la vivienda o la cuadra de su domicilio en el padrón; estos casos se dividen en 19 donde la vivienda es claramente identificable en Street View (en algunos casos se trata de un edificio con departamentos) y 22 donde se puede encontrar la cuadra pero no determinar la vivienda por problemas de visibilidad.

Finalmente, para 14 casos más, se consigue la ubicación de la calle, extendiéndose sobre varias cuadras, y para 2 de ellos solo se puede inferir el barrio sin indicación de la calle.

En los casos donde se identifica una vivienda particular, Street View permite conseguir información adicional sobre ella y su entorno. Las vistas interactivas de la plataforma revelan el estado de la vivienda y sus accesos, además del nivel socioeconómico del barrio y su aparente seguridad. Sin dudas, Street View potencia el riesgo de daño asociado al doxeo. También, aumento el riesgo de estafas debido a la información que se puede recoger a partir de fotografías de viviendas y de su entorno.

4.4 Antecedentes

La organización Open Data Córdoba hizo un análisis geográfico del padrón de Villa Allende del 2015, usando la herramiendo OpenRefine para convertir el padrón en forma tabular y limpiar los datos. Los resultados anonimizados de co-ocurrencias en una misma dirección fueron visualizados en un mapa interactivo. El análisis arrojó ciertas direcciones con altas cantidades de votantes. Cuatro direcciones tienen más de 40 votantes, entre ellas hogares de jóvenes y de ancianos [25]. Para un análisis periodístico sobre el crecimiento de padrones en localidades cordobesas entre 2007 y 2017 y la detección de grupos de votantes identificados por DNI, mudándose de un padrón municipal a otro entre distintas elecciones, referirse también a [17].

Estos trabajos generan la sospecha de que para fines electorales, grandes cantidades de electores hayan sido desplazados de un municipio a otro, y que en esos casos, las direcciones con muchas co-ocurrencias serían domicilios ficticios.

Si bien el objetivo de este trabajo no es corroborar esta hipótesis, creemos que se refuerza el argumento de que en muchos casos, el domicilio no es dato confiable. Como lo menciona la nota periodística citada, "hay millones de errores en el padrón de Buenos Aires". Al constatar que estos datos erróneos no impiden el desarrollo de las votaciones, entendemos que el domicilio puede ser removido del padrón de mesa sin inconvenientes.

5 Efectos colectivos de la difusión de datos personales

Como lo señala Solove [33], no siempre se puede explicitar un vínculo entre daños a la privacidad y personas en particular, pero se pueden generar desequilibrios de poder que afecten concretamente a las vidas de las personas al generar efectos inhibidores colectivos, moldeando así el ambiente político y social de una localidad, una provincia o un país entero. A continuación, dos perspectivas concretas sobre esta cuestión: el efecto del miedo a las represalias en los mecanismos de democracia directa y el hostigamiento disciplinador por redes sociales. La dinámica en juego en estas dos situaciones se puede entender desde la teoría del comportamiento planificado [9].

5.1 Democracia participativa a nivel local

En Argentina, existen en casi todas las provincias mecanismos de democracia directa, o democracia participativa, que se pueden activar a nivel municipal. En el caso de la provincia de Córdoba, el electorado tiene acceso a tres herramientas: la iniciativa popular (ingresar un proyecto de ordenanza al concejo deliberante), convocar a referéndum de veto de ordenanza, y convocar a referéndum de revocatoria popular, usualmente dirigido al intendente municipal [5].

Estos derechos formales convierten los electores en actores políticos y se activan una vez que una cantidad suficiente de electores empadronados se identifican a través de una junta de firmas. En el caso de la revocatoria popular, se interpreta que este derecho es una forma de poner límites a gestiones municipales impopulares. En efecto, el sistema de elección con mayoría simple suele generar casos donde el ganador alcanza no más de 40% de los votos expresados [11].

Pero constatamos que en la realidad, este objetivo puede no cumplirse según lo previsto. Una búsqueda de publicaciones académicas y periodísticas desde el año 2000 indica que a través de los 427 municipios de la provincia, los casos que hayan llegado a la instancia de la votación se cuentan con los dedos de la mano. Es decir, menos de diez casos para 2562 períodos de gestiones municipales acumuladas en los últimos 24 años.

Lo parámetros que contribuyen a este resultado son difíciles de desenredar y probablemente la falta de educación cívica tiene un rol importante. Otro parámetro, bien definido, es el umbral de votantes necesario para promover el referéndum de revocatoria, que es del 10% del padrón en los municipios de Córdoba sin carta orgánica. Pero se suma el parámetro informal del temor a las represalias. Al firmar y dar sus datos personales, una persona se sabe identificada y ubicada, exponiéndose a posibles abusos de poder de parte de funcionarios municipales y a actos de hostigamiento [24]. En efecto, la constitución nacional argentina establece la autonomía municipal; por lo cual la gestión de los mecanismos de democracia directa está a cargo del mismo municipio. Es una diferencia clave con, por ejemplo, Perú, donde las revocatorias a nivel municipal son gestionadas por un ente nacional [32].

Al mejorar la protección de los datos personales en padrones electorales y limitar el acceso de los partidos políticos a esos datos, se puede reducir la percepción de los riesgos de parte de los ciudadanos y así hacer que los mecanismos de democracia directa cumplan con su objetivo de equilibrio institucional.

5.2 Libertad de expresión en redes sociales

En el contexto digital actual, el ejercicio de la libertad de expresión está condicionado por la protección de los datos personales. La exposición indebida de información sensible, como el domicilio posiblemente obtenido a partir de padrones electorales, ha sido utilizada como herramienta de hostigamiento, apuntando a generar un efecto disciplinador e inhibidor en la esfera pública.

En el caso de Argentina, el hostigamiento disciplinador on-line tomó relevancia en la agenda pública desde el 2019, con el debate sobre la ley nacional de

legalización del aborto, y se intensificó con la campaña a elecciones presidenciales del 2023.

El informe de Amnistía Internacional *"Corazones Verdes"* documenta cómo el abuso en línea y la exposición de datos personales afectan de manera desproporcionada a mujeres con voz pública, incitándolas a retirarse de debates políticos o sociales, además de generar daño psicológico [3]. Otro relevamiento de casos de hostigamiento on-line en distintos países de América Latina y Caribe expone las consecuencias en la autocensura de las víctimas [7].

En el 2023 se sancionó la ley nacional 27.736 "Olimpia", que reconoce la violencia digital como un tipo de violencia de género, incluyendo entre sus modalidades la "difusión no consentida de datos personales" [1]. Pero la misma ley limita esta definición aclarando "en la medida en que no sean conductas permitidas por la ley 25.326 (de protección de datos personales)"; y precisamente esta última ley indica que la difusión de listados conteniendo el domicilio de una persona no requiere consentimiento ninguno.

El año 2024 vio numerosos casos de hostigamiento dirigidos a mujeres y hombres por razones políticas, atribuibles a grupos organizados paraestatales [28]. En algunos casos, el hostigamiento virtual ha derivado en agresiones físicas o persecución a familiares de las víctimas en sus domicilios.

Proteger los datos personales de las personas puede garantizar que ejerçan su libertad de expresión y de asociación [33], pero este vínculo entre privacidad y libertad de expresión rara vez es reconocido explícitamente en la normativa sobre protección de datos personales. La ley 25.326 de protección de los datos personales solo hace referencia a "garantizar el derecho al honor y a la intimidad de las personas", pero no a la libertad de expresión.

Recientemente, algunas plataformas de redes sociales decidieron reducir la moderación bajo el argumento de defender la libertad de expresión [26]. Este argumento es conveniente para los dueños de esas plataformas pero es simplista y no resuelve el problema de fondo para la sociedad en su conjunto. Al contrario, los casos de hostigamiento y de exposición de datos personales aumentaron. A la luz de las tendencias recientes, quedó claro que la libertad de expresión también requiere proteger a las personas de toda forma de violencia que las obligan a callar. En este sentido, frenar la publicación de datos personales en la web abierta es un paso necesario para asegurar un debate público realmente libre.

6 Propuestas

6.1 Eliminación de datos personales

En prioridad, se propone eliminar 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.

Cabe 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.

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. Una solución a este problema consiste en inspirarse de las elecciones internas de la Universidad Nacional de Córdoba del 2024. En esos padrones, solo se incluyó el nombre completo y los últimos tres dígitos del DNI de los votantes.

Aplicando estas propuestas, un padrón quedaría de la siguiente manera:

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

El número de DNI truncado deja de ser único y es posible que existan conjuntos de personas con el mismo nombre completo y los mismos últimos tres dígitos de DNI. Si eso sucede en una mesa de votación, el sistema que genera el padrón debe incluir más dígitos hasta que la ambigüedad se resuelva; alternativamente, se puede determinar el número de orden mediante una consulta on-line al padrón con el DNI completo. En el caso de personas en distintas mesas, este sistema implica un riesgo de doble votación que debe ser tomado en cuenta.

6.2 Desmalezamiento virtual

Se propone implementar la vigilancia activa de la web abierta por parte de una agencia estatal, por ejemplo la Agencia de Acceso a la Información Pública de dependencia nacional, con el fin de detectar y eliminar padrones electorales y otros listados de datos personales. Esta estrategia implicaría un monitoreo permanente de la web buscable para identificar la presencia de padrones electorales accesibles sin restricciones. Una vez detectados, la agencia responsable contactaría a los administradores del sitio para solicitar la eliminación del archivo. Además, se encargaría solicitar la supresión de estos contenidos de los cachés de motores de búsqueda y repositorios de historial web.

Esta tarea sería una forma proactiva y desindividualizada del principio del derecho al olvido o derecho a la supresión [27]. Si bien este derecho no tiene entidad legislativa actualmente en Argentina, se puede entender según los términos de la ley 25.326 de protección de los datos personales: "Los datos deben

ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados". En el caso de padrones electorales, el órgano de monitoreo tendría plena legitimidad para solicitar el retiro de los padrones inmediatamente luego del acto electoral.

7 Conclusiones

En Argentina, desde los años 2010, aumentó la gestión de padrones electorales como archivos electrónicos. Esto hizo que se empezaran a difundir padrones electorales por la web abierta, algunos de ellos permaneciendo disponibles por mucho tiempo. 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 [33].

Esta creciente accesibilidad de padrones electorales tiene consecuencias tangibles tanto individuales como colectivas. A nivel personal, la exposición de datos sensibles ha facilitado el hostigamiento digital y el uso indebido de la información con fines delictivos. A nivel colectivo, genera efectos inhibidores en la participación ciudadana, particularmente en mecanismos de democracia directa y en el ejercicio de la libertad de expresión. 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.

El 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 no por eso es necesario incluirlo dentro de los padrones electorales.

Como respuesta a los problemas mencionados anteriormente, se propone seguir el principio de minimización de datos y eliminar el domicilio de toda base de datos que no lo necesite, incluyendo los padrones electorales. Esta medida alcanzaría a todo tipo de formato de los padrones, incluyendo el formato papel. Además, se propone implementar un mecanismo de desmalezamiento virtual para detectar y eliminar padrones expuestos en la web abierta.

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. 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. 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 seguridad de los ciudadanos.

References

1. Abiuso, M., López, J.: Acoso y violencia digital. herramientas de acción para periodistas. (2024), UNICEF; UNFPA, PNUD; ONU Mujeres; Red de Editoras de Género
2. 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)
3. Amnistía Internacional: Corazones verdes. violencia online contra las mujeres durante el debate por la legalización del aborto en Argentina (2024)
4. Anderson, B., Wood, M.A.: Doxxing: A scoping review and typology. In: The Emerald international handbook of technology-facilitated violence and abuse, pp. 205–226. Emerald Publishing Limited (2021)
5. Arques, F.: Argentina: una herramienta de los gobernados en manos de los gobernantes. In: La dosis hace el veneno: análisis de la revocatoria del mandato en América Latina, Estados Unidos y Suiza, pp. 159–186. Instituto de la Democracia (2014)
6. Asociación por los Derechos Civiles (ADC): El Estado recolector. Un estudio sobre la Argentina y los datos personales de los ciudadanos (2014)
7. Beck, I., Alcaraz, F., Rodríguez, P.: Violencia de género en línea hacia mujeres con voz pública. Impacto en la libertad de expresión (2022), Alianza Regional por la Libre Expresión e Información ONU Mujeres
8. Borghello, C., Temperini, M.G.: Suplantación de identidad digital como delito informático en argentina. In: X Simposio Argentino de Informática y Derecho (2012)
9. Büchi, M., Festic, N., Latzer, M.: The chilling effects of digital dataveillance: A theoretical model and an empirical research agenda. Big Data & Society **9**(1), 20539517211065368 (2022)
10. 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 **119** (2022)
11. Carranza Torres, L.: La revocatoria de mandatos: Un tema clave para una nueva democracia (2002), https://www.diariojudicial.com/news-43682-la-revocatoria-de-mandatos-un-tema-clave-para-una-nueva-democracia
12. Chaturvedi, R., Chaturvedi, S.: It's all in the name: A character-based approach to infer religion. Political Analysis **32**(1), 34–49 (2024)
13. Douglas, D.M.: Doxing: a conceptual analysis. Ethics and information technology **18**(3), 199–210 (2016)
14. Ferreyra, E.: Democracia segmentada: Acerca de la explotación de datos personales con fines electorales. Informe, Asociación por los Derechos Civiles (2019)
15. Fundación Vía Libre: Gestión de datos personales por parte del Estado (2024)
16. Gibson, H.: Acquisition and preparation of data for OSINT investigations. Open source intelligence investigation: From strategy to implementation (2016)
17. Gordillo, F., Heurtley, R.: Así funciona la fábrica de votantes en las provincias de Argentina (2017), https://www.connectas.org/especiales/fabrica-votantes-malvinas/
18. 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)
19. Juels, A., Catalano, D., Jakobsson, M.: Coercion-resistant electronic elections. In: Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society (2005)

20. 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)
21. Lyon, D.: Surveillance, Snowden, and big data: Capacities, consequences, critique. Big data & society **1**(2) (2014)
22. Marx, G.T.: What's in a name? Some reflections on the sociology of anonymity. The information society **15**(2), 99–112 (1999)
23. 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)
24. Navarrete Montoya, J.G., Mancera Morales, C., Muñoz, F.A., Cubaque Barrera, C., Jímenez Angel, F.: Mecanismos de participación ciudadana en Colombia: 20 años de ilusiones. Misión de Observación Electoral (2012)
25. Open Data Córdoba: Análisis del padrón electoral de Villa Allende (2015), https://github.com/OpenDataCordoba/analisis-padron-electoral-villa-allende
26. Ozan, Ö., Sadıkzade, A.R.: Mapping the landscape of content moderation: A bibliometric perspective. İnterdisipliner Medya ve İletişim Çalışmaları **1**(2), 85–109 (2024)
27. Puccinelli, O.: El derecho al olvido digital. La nueva cara de un derecho tan viejo como polémico. Revista Derecho Constitucional (2019)
28. Revista Crisis: Las milicias digitales de la ultraderecha (2024), https://revistacrisis.com.ar/notas/las-milicias-digitales-de-la-ultraderecha
29. 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)
30. Rubinstein, I.S.: Voter privacy in the age of big data. Wis. L. Rev. (2014)
31. Schoenebeck, S., Lampe, C., Trieu, P.: Online harassment: Assessing harms and remedies. Social Media+ Society **9**(1) (2023)
32. Soldevilla, F.T.: Perú: entre la participación y la gobernabilidad local (1997-2013). In: La dosis hace el veneno: análisis de la revocatoria del mandato en América Latina, Estados Unidos y Suiza, pp. 7–30. Instituto de la Democracia (2014)
33. Solove, D.J.: Access and aggregation: Public records, privacy and the constitution. Minn. L. Rev. **86**, 1137 (2002)
34. Uriel, D.G.: Los secuestros virtuales. Revista Penal México **11**(21), 167–190 (2022)
35. 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)