ANÁLISIS

Las medidas de seguridad del Departamento de Justicia para recolectar padrones electorales son inadecuadas

Las leyes estatales y federales obligan a mantener seguros los datos privados sensibles de las listas de registro de los votantes.

Lisa J. Danetz

febrero 25, 2026

Que todos puedan votar

Suscríbete aquí al boletín informativo del Brennan Center en español [link-1]

- **El DOJ no ha brindado ninguna garantía detallada que explique cómo protegerá la información privada y sensible de toda la ciudadanía estadounidense.**
- **Según la ley federal y muchas leyes estatales, las autoridades electorales estatales deben proteger la seguridad de la información sobre el registro de sus ciudadanos votantes.**

Desde la primavera de 2025, el Departamento de Justicia (DOJ, por su sigla en inglés) ha estado intentando obtener los padrones electorales [link-2] de todas las personas votantes de la nación. Esa lucha [link-3] ha llegado a la justicia, donde el DOJ ha presentado demandas judiciales [link-4] contra 24 estados desde septiembre.

Cabe destacar que la mayoría de esos estados ya le han provisto información de dominio público sobre el registro de sus votantes, pero el DOJ ha exigido acceso a los padrones completos y sin editar, que contienen información personal sensible,

como los números de licencia de conducir y de seguridad social del electorado.

Gran parte de esta controversia se ha centrado [link-5] en los distintos argumentos jurídicos sobre por qué el DOJ no tiene derecho a recabar esta información, por ejemplo, el requisito de la Ley de Derechos Civiles (*Civil Rights Act*) de explicitar la justificación y propósito de esa información, las disposiciones de la Ley de Privacidad (*Privacy Act*) y las violaciones a las leyes estatales. Pero hay otra razón menos conocida: el DOJ no ha brindado ninguna garantía detallada que explique cómo protegerá la información privada y sensible de toda la ciudadanía estadounidense y parece estar ignorando las leyes federales que lo obligan a hacerlo.

Según la ley federal y muchas leyes estatales, las autoridades electorales estatales deben proteger la seguridad de la información sobre el registro de sus ciudadanos votantes. En el ámbito federal, la Ley Ayudar a América a Votar [link-6] (*Help America Vote Act*, HAVA) les exige a las autoridades electorales locales y estatales tomar las "medidas de seguridad tecnológicas adecuadas [link-7] " para proteger las bases de datos estatales de registro de los votantes. Los estados determinan [link-8] cómo cumplen con este requisito y también pueden requerir una protección más estricta [link-9] que la especificada por las normas mínimas de la ley HAVA.

Las leyes federales también obligan al gobierno federal a tomar ciertas medidas para garantizar la seguridad de toda la información sensible que recolecta y almacena. La Ley Federal de Modernización de la Seguridad de la Información [link-10] (*Federal Information Security Modernization Act*, FISMA) estipula que las agencias gubernamentales federales y sus contratistas [link-11] deben diseñar y poner en práctica programas de seguridad de la información para proteger sus sistemas informáticos y la información que allí almacenan.

El nivel de protección dispuesto por la ley depende de los riesgos que impliquen los datos en cuestión y debe basarse en las normas federales obligatorias [link-12] . La ley FISMA también requiere que las agencias federales monitoreen con regularidad sus propios programas de seguridad de la información y los de sus contratistas.

En teoría, las leyes HAVA, FISMA y las leyes estatales deberían garantizar la seguridad

de toda la información sensible sobre el registro de los votantes. Desafortunadamente, la realidad parece ser otra. El acuerdo [link-13] que ha propuesto el DOJ sobre la transferencia de los datos de los estados, que contienen información sensible sobre el registro de votantes, es ambiguo en cuanto a sus planes de seguridad y, cuando sí enumera esos planes, es también deplorablemente deficiente. Un análisis [link-14] reciente detalla las deficiencias en materia de seguridad de la información. Esta falta de protección da miedo.

Entre las varias carencias de seguridad, se pueden enumerar las siguientes:

- Los datos tienen una encriptación inadecuada, es decir, la conversión de la información sobre el registro de votantes en un código indescifrable no es la correcta. Tener una encriptación inadecuada significa que un *hacker* puede acceder fácilmente a los datos personales del electorado.
- No hay suficientes controles de acceso ni de minimización de los datos. El acuerdo permite el acceso a los datos mediante una contraseña, en lugar de requerir también la autenticación multifactor. Tampoco restringe el intercambio de datos más allá del propósito establecido para su recopilación.
- El DOJ no ha explicado cómo se asegurará de realizar la investigación de los antecedentes de sus contratistas, con los que tiene planes explícitos de compartir los datos, y cómo se asegurará de que ellos se comprometan a salvaguardar la información privada del electorado, tal como lo exigen las leyes federales.
- No hay ningún análisis de registro de auditoría ni ningún proceso de notificación establecido. Nadie va a revisar ni analizar quiénes acceden a los datos; por lo tanto, nadie podrá detectar cualquier problema que surja. En caso de que el DOJ detecte algún problema, como un acceso no autorizado a la información u otras filtraciones de datos, no hay ningún plazo de tiempo requerido para notificar los problemas a los estados afectados.
- El DOJ planea "archivar" y almacenar los datos después de sus análisis, en lugar de destruirlos. El archivo de estos datos creará un registro federal permanente con información sensible de todo el electorado, que siempre estará disponible.

Estas deficiencias en materia de ciberseguridad exacerban lo que se conoce

como el efecto mosaico [link-15] . Las listas de registro de votantes contienen cantidades importantes de información sobre cada persona votante: ciertas combinaciones de su nombre, dirección residencial, fecha de nacimiento, número de licencia de conducir, número completo o parcial de seguridad social, dirección de correo electrónico, número de teléfono, fecha de registro como votante, estatus de registro, historial de votación y partido político.

La recopilación de tantos datos sobre el registro de las personas votantes, combinados con otros tipos de información disponible de *data brokers* comerciales, infiltraciones de datos financieros y bases de datos federales, ofrece un sitio centralizado de fácil ataque para los actores dañinos.

La posible filtración de estos datos plantea, al menos, tres riesgos. Primero, el efecto mosaico le permitiría a un actor dañino usar la información de cualquier votante para robarle su identidad.

Segundo, al infiltrar información sobre una violación de seguridad exitosa, cualquier nación adversaria podría aprovecharse de esos datos recopilados para sembrar el miedo, reafirmar su poder y debilitar la confianza del público en nuestro gobierno.

Tercero, cualquier actor dañino podría usar esa información para eliminar determinados nombres de las listas de registro de votantes sin ser detectado fácil o rápidamente.

Dados los ejemplos recientes de una seguridad o manejo deficientes de la información por parte de varias agencias federales, no es seguro confiar ciegamente en los procesos del DOJ. En 2025, un grupo de empleados de una agencia federal cargaron [link-16] indebidamente datos confidenciales de la Administración del Seguro Social a un servidor privado no autorizado y firmaron un "acuerdo sobre los datos de los votantes" para transferir esa información a un grupo activista político que buscaba pruebas de un presunto fraude electoral y quería anular los resultados de las elecciones.

El director interino de la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA, por su sigla en inglés), una agencia creada para "defender y garantizar la seguridad del ciberespacio", cargó [link-17] archivos sensibles de la agencia en una versión pública de ChatGPT, con lo cual le permitió a OpenAI usar esa información para responder preguntas de cualquiera de los más de 700 millones de usuarios activos

que tiene la compañía. Y el líder del Grupo de Trabajo de Instrumentalización Política del propio DOJ, establecido [link-18] bajo el mando de la actual fiscal general para inspeccionar [link-19] las actividades de las personas que habían investigado o demandado al presidente y sus empresas, infiltró [link-20] material de un gran jurado.

Proteger a su ciudadanía debería ser el sello característico de todo gobierno. Dada la obligación de los funcionarios estatales de proteger la información sensible de su electorado, la clara falta de medidas de seguridad adecuadas del DOJ, tal como lo exigen las leyes federales, es una más de las muchas razones por las que los estados deben resistirse al intento de recopilar los datos de registro de las personas votantes a lo ancho del país.

Traducción de Ana Lis Salotti

MORE ON

Election Integrity [link-21]

Links

link-1: Suscríbete aquí al boletín informativo del Brennan Center en español https://go.brennancenter.org/el-newsletter

link-2: obtener los padrones electorales https://www.brennancenter.org/es/our-work/research-reports/mapa-solicitudes-informacion-votantes-presentadas-departamento-elecciones-estados-unidos

link-3: lucha https://www.brennancenter.org/es/our-work/analysis-opinion/tribunales-federales-rechazan-intentos-trump-obtener-informacion-privada-votantes

link-4: demandas judiciales https://www.brennancenter.org/our-work/analysis-opinion/trump-administration-has-sued-more-20-states-refusing-turn-over-voter

link-5: centrado https://www.brennancenter.org/our-work/analysis-opinion/justice-department-has-demanded-voter-files-least-21-states

link-6: Ley Ayudar a América a Votar https://www.eac.gov/sites/default/files/eac_assets/1/6/HAVA41.PDF

link-7: medidas de seguridad tecnológicas adecuadas https://uscode.house.gov/view.xhtml?req=(title:52%20section:21083%20edition:prelim)

link-8: determinan https://uscode.house.gov/view.xhtml?hl=false&edition=prelim&req=granuleid%3AUSC-prelim-title52-section21085&num=0&saved=%7CKHRpdGxlOjUyIHNlY3Rpb246MjEwODMgZWRpdGlvbjpwcmVsaW0p%7C%7C%7C0%7Cfalse%7Cprelim

link-9: protección más estricta https://uscode.house.gov/view.xhtml?hl=false&edition=prelim&req=granuleid%3AUSC-prelim-title52-section21084&num=0&saved=%7CKHRpdGxlOjUyIHNlY3Rpb246MjEwODMgZWRpdGlvbjpwcmVsaW0p%7C%7C%7C0%7Cfalse%7Cprelim

link-10: Ley Federal de Modernización de la Seguridad de la Información https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title44-chapter35-subchapter2&saved=%7CZ3JhbnVsZWlkOlVTQy1wcmVsaW0tdGl0bGU0NC1zZWN0aW9uMzU1MQ%3D%3D%7C%7C%7C0%7Cfalse%7Cprelim&edition=prelim

link-11: agencias gubernamentales federales y sus contratistas https://uscode.house.gov/view.xhtml?hl=false&edition=prelim&req=granuleid%3AUSC-prelim-title44-section3554&num=0&saved=%7CZ3JhbnVsZWlkOlVTQy1wcmVsaW0tdGl0bGU0NC1zZWN0aW9uMzU1MQ%3D%3D%7C%7C%7C0%7Cfalse%7Cprelim

link-12: obligatorias https://uscode.house.gov/view.xhtml?req=(title:40%20section:11331%20edition:prelim)

link-13: acuerdo https://www.brennancenter.org/our-work/analysis-opinion/confidential-agreements-show-trump-administrations-plans-states-voter

link-14: análisis https://epic.org/documents/analyzing-dojs-mou-for-voter-registration-list-data-for-fisma-compliance/

link-15: efecto mosaico https://ostradecraft.medium.com/the-mosaic-effect-why-harmless-data-isnt-harmless-bc63bbd3d072

link-16: cargaron https://www.npr.org/2026/01/23/nx-s1-5684185/doge-data-social-security-privacy

link-17: cargó https://www.politico.com/news/2026/01/27/cisa-madhu-gottumukkala-chatgpt-00749361?mc_cid=6f311a1887&mc_eid=2927a70260

link-18: establecido https://www.justice.gov/ag/media/1388506/dl?inline

link-19: inspeccionar https://abcnews.com/US/bondi-new-ag-launches-weaponization-working-group-review/story?id=118501463

link-20: infiltró https://www.cnn.com/2026/02/04/politics/ed-martin-review-improperly-handled-grand-jury

link-21: Election Integrity https://www.brennancenter.org/topics/voting-elections/election-integrity