LEY QUE PREVIENE Y SANCIONA LAS OPERACIONES DIGITALES COORDINADAS ILÍCITAS DENOMINADAS GRANJAS DE TROLLS Y BOTS, FORTALECIENDO LA INTEGRIDAD DE LOS PROCESOS ELECTORALES

Los diputados integrantes del Grupo Parlamentario Ahora Nación, a iniciativa del diputado de la República **CÉSAR AUGUSTO MUEDAS BALBIESE** y en ejercicio de la atribución conferida por el artículo 107 de la Constitución Política del Perú y por los artículos 98 y 107 del Reglamento de la Cámara de Diputados, presentan la siguiente proposición legislativa:

FÓRMULA LEGAL

LEY QUE PREVIENE Y SANCIONA LAS OPERACIONES DIGITALES COORDINADAS ILÍCITAS DENOMINADAS GRANJAS DE TROLLS Y BOTS, FORTALECIENDO LA INTEGRIDAD DE LOS PROCESOS ELECTORALES

Artículo 1.- Objeto

La presente ley previene y sanciona las operaciones digitales coordinadas ilícitas ejecutadas mediante redes automatizadas, cuentas falsas o perfiles inauténticos, comúnmente conocidos como granjas de trolls o bots, con la finalidad de manipular o alterar ilegítimamente la formación de la voluntad electoral produciendo una grave afectación a la integridad de los procesos electorales, derechos fundamentales de terceros, así como la transparencia del financiamiento político.

La aplicación de la ley respeta las libertades de información, opinión, expresión y difusión del pensamiento reconocidas por la Constitución Política del Perú y por los tratados internacionales de derechos humanos ratificados por el Estado peruano.

Artículo 2.- Finalidad

La norma busca proteger la integridad, transparencia y legitimidad de los procesos electorales. También procura evitar ventajas indebidas obtenidas mediante redes

digitales clandestinas, reforzar la fiscalización del financiamiento electoral, tutelar el honor y la buena reputación frente a agresiones sistemáticas, preservar el acceso a información y resguarda el correcto funcionamiento de la administración pública.

Artículo 3. Incorporación del artículo 12-B a la Ley N.º 30096, Ley de Delitos Informáticos

Se incorpora el artículo 12-B a la Ley N.º 30096, Ley de Delitos Informáticos, en los siguientes términos:

"Artículo 12-B. Operación y financiamiento de redes digitales inauténticas con finalidad ilícita

El que, mediante tecnologías de la información o de la comunicación, cree, administre, promueva, financie, opere, dirija o contrate una red digital automatizada o inauténtica coordinada mediante el uso masivo de perfiles falsos o bots, con el propósito de difundir de forma sistemática imputaciones falsas contra el honor o la reputación de una o más personas, o para simular identidad de terceros atribuyendo hechos falsos con relevancia electoral, será reprimido con pena privativa de libertad no menor de cuatro ni mayor de seis años y con ochenta a ciento veinte días-multa.

La pena será no menor de cinco ni mayor de ocho años de privación de libertad y de ciento veinte a doscientos cuarenta días-multa cuando concurra cualquiera de las siguientes circunstancias agravantes:

1. La operación sea financiada, total o parcialmente, con aportes, donaciones, u otros recursos provenientes de una fuente prohibida por la legislación electoral.
2. El agente tiene la condición de autoridad electa, funcionario o servidor público.
3. El agente utilice fondos, bienes, infraestructura, información, servicios o personal de una entidad pública para crear, administrar, operar o financiar la red.
4. El agente ejerce cargo directivo, es fundador, afiliado o aportante de una organización política.
5. La conducta se ejecute mediante inteligencia artificial, generación o alteración sintética de imágenes, audios o videos, deepfakes u otras tecnologías equivalentes, destinados a atribuir declaraciones o hechos falsos a candidatos o autoridades electorales.

6. La conducta es ejecutada como parte de las actividades de una organización criminal o por encargo de esta.

Artículo 4. Incorporación del literal r) al artículo 85 de la Ley N.º 30057, Ley del Servicio Civil

Se incorpora el literal r) al artículo 85 de la Ley N.º 30057, Ley del Servicio Civil, en los siguientes términos:

"Artículo 85. Faltas de carácter disciplinario

Son faltas de carácter disciplinario que, según su gravedad, pueden ser sancionadas con suspensión temporal o con destitución, previo proceso administrativo:

(...)

r) Crear, administrar, financiar, operar, dirigir o utilizar, en ejercicio de la función pública y/o con uso indebido de recursos, infraestructura, bienes o personal estatal, una red digital automatizada o inauténtica coordinada destinada a la difusión masiva de contenido falso, difamatorio, o para manipular la voluntad electoral.

La infracción comprende la participación en la amplificación artificial de contenidos, tendencias o aparentes respaldos ciudadanos, así como la difusión coordinada de ataques contra el honor o la reputación de una persona.

Artículo 5. Modificación del artículo 36 de la Ley N.º 28094, Ley de Organizaciones Políticas

Se incorpora el numeral 9 al literal c) del artículo 36 de la Ley N.º 28094, Ley de Organizaciones Políticas, en los siguientes términos:

"Artículo 36. Infracciones

(...)

c) Constituyen infracciones muy graves:

(...)

9. Crear, promover, financiar, contratar o utilizar, directa o indirectamente, una red digital automatizada o inauténtica coordinada destinadas a la difusión de pauta publicitaria no declarada ante el órgano electoral correspondiente, o a la emisión sistemática de imputaciones falsas contra una autoridad, candidato a elección popular, o contra cualquier persona.

Artículo 6. Transparencia y fiscalización de los gastos digitales de campaña

Las organizaciones políticas y los candidatos declaran ante la Oficina Nacional de Procesos Electorales (ONPE), de acuerdo con los procedimientos y formatos que esta establezca, los gastos destinados a:

1. publicidad y propaganda digital;
2. contratación de agencias, consultores o empresas de comunicación digital;
3. administración profesional de cuentas y perfiles digitales;
4. contratación de sistemas automatizados, inteligencia artificial u otras herramientas tecnológicas destinadas a la comunicación electoral; y
5. cualquier otro servicio tecnológico destinado directamente a la publicidad electoral.

La ONPE establece mecanismos de identificación, registro, verificación y fiscalización de dichos gastos.

Artículo 7. Coordinación institucional

La Oficina Nacional de Procesos Electorales, el Jurado Nacional de Elecciones, el Ministerio Público y la Policía Nacional del Perú establecen, dentro de sus competencias, mecanismos de coordinación para prevenir, detectar, investigar y perseguir operaciones digitales ilícitas que puedan afectar los procesos electorales.

La actuación de las autoridades respeta el libre ejercicio de los derechos a la información, opinión, expresión, difusión del pensamiento conforme al artículo 2 inciso 4to de la Constitución, así como el debido proceso, la protección de datos personales, el secreto de las comunicaciones, el ejercicio libre del periodismo o de comunicación, no constituye delito el uso de seudónimos, la sátira, humor político, ni la difusión de la pauta publicitaria legalmente contratada y declarada conforme a ley.

Artículo 8. Aplicación de las normas penales vigentes

Las disposiciones de la presente ley se aplican sin perjuicio de los delitos previstos en el Código Penal y demás leyes especiales.

Cuando una misma conducta configure simultáneamente el delito previsto en el artículo 12-B de la Ley N.º 30096, se aplican las reglas del concurso de delitos previstas en el Código Penal.

DISPOSICIÓN COMPLEMENTARIA FINAL

PRIMERA. - Fortalecimiento de la fiscalización del financiamiento digital

La Oficina Nacional de Procesos Electorales implementa mecanismos especializados de fiscalización de los gastos digitales de campaña. Estos comprenden procedimientos para identificar servicios de amplificación artificial, publicidad digital encubierta y contratación de servicios tecnológicos vinculados con campañas electorales.

La fiscalización se desarrolla respetando las normas sobre protección de datos personales, secreto de las comunicaciones y demás

Lima, 7 de setiembre de 2026

CESAR AUGUSTO MUEDAS BALBIESE
Diputado de la República

José Marcelo Salazar

Cesar D. Holguin Loaiza
Vocero

Indira Huilca

Jair J. Quiroz

Freshman Quintero Martínez

Marleny Dimitra L.

EXPOSICIÓN DE MOTIVOS

I. PLANTEAMIENTO DEL PROBLEMA PÚBLICO

Hace pocos días se conoció la detención en Bolivia del consultor político argentino Fernando Cerimedo por un presunto intento de feminicidio. Ese hecho abrió una discusión regional sobre presuntas redes internacionales de desinformación y manipulación digital utilizadas en campañas políticas para atacar a ciertos candidatos y favorecer a otros.

La presunta red habría tenido presencia o participación activa en procesos electorales recientes de Sudamérica, entre ellos Bolivia, Brasil, Argentina y Chile; también se ha planteado la necesidad de revisar posibles conexiones con el Perú.
El avance tecnológico, la sofisticación de los entornos digitales y el uso masivo de redes sociales han generado formas complejas de distorsión del debate público. Entre ellas se ubican las redes inauténticas coordinadas, conocidas usualmente como granjas de bots y trolls.

Investigaciones y hechos recientes en la región muestran que estas herramientas pueden operar de manera industrializada. Su finalidad es fabricar tendencias, alterar la visibilidad algorítmica y diseminar información falsa de forma sistemática. International IDEA ha advertido que la inteligencia artificial y otras tecnologías de manipulación digital generan riesgos crecientes para los procesos electorales, especialmente mediante contenidos sintéticos, deepfakes y campañas de desinformación.

Esta problemática transciende la simple emisión de opiniones; se trata de una manipulación automatizada que persigue los siguientes objetivos fácticos:

a) **Simulación de respaldo o consenso político:** creación de corrientes ficticias de opinión pública mediante cuentas automatizadas que carecen de soporte humano real. Con ello se busca aparentar que una propuesta, candidatura u opinión cuenta con respaldo ciudadano masivo, pese a tratarse de una construcción artificial y malintencionada.
b) **Alteración del debate político:** sustitución de la exposición de propuestas programáticas por ataques sistemáticos dirigidos a dañar la reputación y el

honor de autoridades, ciudadanos o candidatos durante una contienda electoral.

Una modalidad particularmente dañina consiste en promover teorías de conspiración durante el proceso electoral. Esa práctica pone en duda los resultados, la actuación de autoridades o los vínculos de determinados candidatos, como ha ocurrido en países vecinos.

c) **Uso indebido de inteligencia artificial:** manipulación o alteración técnica de imágenes, audios y videos, incluidos deepfakes, con capacidad de inducir a error al electorado y afectar la credibilidad institucional. Estas prácticas también pueden buscar posicionar tendencias en plataformas como X, TikTok, Facebook o Instagram mediante miles de cuentas coordinadas.

La tecnología de acceso público permite convertir espacios digitales en centros operativos de difusión de noticias falsas, cuando esos contenidos se repiten de manera constante y agresiva, pueden influir en la opinión pública sobre todo si quienes los difunden conocen que carecen de fuente confirmada.

d) **Financiamiento clandestino:** al no existir una regulación expresa sobre estas actividades, los recursos destinados a sostener infraestructuras digitales inauténticas pueden operar fuera de la supervisión electoral, con riesgos vinculados al lavado de activos y al financiamiento prohibido de campañas.

Estas operaciones requieren inversión, equipamiento tecnológico y personas encargadas de ejecutar o dirigir la red. En ese contexto, no se trata de simples opiniones aisladas, sino de conductas organizadas que pueden resultar incompatibles con la legalidad electoral y penal.

La legislación penal vigente sobre delitos informáticos, financiamiento prohibido de organizaciones políticas y protección del honor permite perseguir ciertos componentes individuales. Sin embargo, resulta insuficiente frente a ataques digitales masivos, coordinados y asimétricos, lo que evidencia una zona de punibilidad que requiere respuesta legislativa.

El ordenamiento actual permite sancionar conductas específicas, pero no regula de manera expresa el uso de una red digital inauténtica coordinada como instrumento de una operación ilícita con finalidad electoral o de ataque sistemático.

El problema no comienza ni termina con el caso de Fernando Cerimedo. Ese episodio sirve para mostrar una amenaza más amplia contra la democracia peruana: la utilización deliberada, coordinada y organizada de mecanismos digitales inauténticos o automatizados con una finalidad ilícita concreta.

II. EVIDENCIA QUE SUSTENTA EL PROBLEMA

El caso conocido a partir de la detención en Bolivia del consultor político argentino Fernando Cerimedo evidenció la posible existencia de una red internacional con presencia o participación en procesos electorales sudamericanos. Las investigaciones periodísticas la vinculan no solo con campañas políticas, sino también con desinformación, manipulación electoral y ataques contra la honra y el honor.

Estudios periodísticos y fiscales internacionales advierten la existencia de estructuras transnacionales de consultoría política dedicadas a la guerra digital asimétrica. Estos antecedentes muestran la vulnerabilidad de los procesos electorales democráticos frente a estrategias coordinadas de desinformación masiva, con afectación directa a la autodeterminación del elector y a la igualdad de condiciones en la competencia política.

En el caso peruano, información oficial del Jurado Nacional de Elecciones – JNE - reportó 704 alertas de desinformación electoral durante los once meses previos a febrero de 2026, en el marco de las Elecciones Generales 2026. De ese total, 242 correspondieron a diciembre de 2025 y 215 a enero de 2026. El JNE identificó como ámbitos recurrentes la fiscalización electoral, propaganda, publicidad, neutralidad, Jurados Electorales Especiales e interferencia política.

Las campañas estructuradas de desinformación electoral no deben entenderse solo como un problema de comunicación política. Constituyen un riesgo para la integridad electoral, la legitimidad de las instituciones democráticas y el ejercicio de la autodeterminación ciudadana; por ello, resulta razonable desarrollar normas de prevención, investigación y sanción frente a conductas dirigidas a alterar ilegítimamente la voluntad popular.

III. OBJETIVOS GENERALES Y ESPECÍFICOS

Objetivo general

Establecer un marco jurídico específico y proporcional para prevenir, investigar y sancionar el uso deliberado de redes digitales automatizadas o inauténticas coordinadas cuando sirvan como instrumento de operaciones ilícitas. La regulación se orienta a proteger la integridad electoral, la transparencia del financiamiento político, los recursos públicos y el honor de personas determinadas, sin desconocer la libertad de expresión ni el pluralismo democrático.

Objetivos específicos

a) Incorporar una regulación penal específica para las operaciones digitales coordinadas que utilicen estructuras automatizadas o inauténticas con una finalidad ilícita determinada.
b) Establecer agravantes cuando las operaciones digitales sean utilizadas para obtener ventajas electorales indebidas.
c) Establecer una respuesta agravada frente a campañas digitales coordinadas que configuren, además, los elementos del delito de difamación.
d) Prevenir y sancionar el uso de bienes, recursos, infraestructura, sistemas o personal del Estado para ejecutar operaciones digitales ilícitas.
e) Fortalecer la transparencia y fiscalización de los gastos digitales vinculados con campañas electorales.
f) Establecer responsabilidades administrativas para los servidores civiles que utilicen indebidamente recursos públicos en este tipo de operaciones.
g) Fortalecer los mecanismos de responsabilidad de las organizaciones políticas cuando estas financien, contraten, autoricen o utilicen operaciones digitales coordinadas ilícitas.

IV. FUNDAMENTACIÓN DE LA INICIATIVA

El ordenamiento jurídico peruano ya sanciona diversas conductas ilícitas. La Ley N.º 30096 – Delitos Informáticos - regula modalidades de criminalidad cometidas

mediante tecnologías de la información y comunicación; el Código Penal contempla los delitos contra el honor, incluida la difamación; y la legislación electoral incorpora reglas sobre financiamiento prohibido de organizaciones políticas.
La Ley N.º 28094 - Organizaciones Políticas - regula el control y fiscalización del financiamiento público y privado de las organizaciones políticas. A su vez, en la Ley N.º 30057 – SERVIR - establece el régimen disciplinario aplicable a los servidores, directivos y funcionarios civiles.

Estas normas atienden supuestos específicos, pero no regulan expresamente la utilización de una estructura digital inauténtica coordinada como instrumento de una operación organizada con finalidad ilícita. La incertidumbre aparece cuando concurren automatización, anonimización, coordinación, financiamiento oculto y finalidad electoral o reputacional ilícita.

Las estructuras descritas no constituyen un ejercicio regular de la libertad de expresión. Son mecanismos capaces de manipular algoritmos, fabricar falsas mayorías, dañar honras en pocos minutos y afectar la autodeterminación del elector. La falta de regulación expresa permite que el financiamiento de estas redes opere en la clandestinidad y eluda la supervisión electoral, con riesgo de lavado de activos y financiamiento prohibido de campañas.

V. ANTECEDENTES LEGISLATIVOS

- Constitución Política del Perú (1993): Artículos 2, 31 y 35.
- Ley N° 30096, Ley de Delitos Informáticos: regula el acceso ilícito, la identidad digital y el fraude informático, pero no contiene un tipo penal específico para sancionar acciones coordinadas e inauténticas con fines de manipulación social, electoral o reputacional.
- Ley Nº 28094, Ley de Organizaciones Políticas: regula el financiamiento público y privado, pero mantiene un vacío respecto del gasto o inversión en activos digitales inauténticos, como modalidad de propaganda encubierta.

VI. SECTORES COMPRENDIDOS

La implementación y aplicación de la presente norma vincula a las siguientes entidades:

- Jurado Nacional de Elecciones - JNE

- Oficina Nacional de Procesos Electorales – ONPE
- Ministerio de Justicia y Derechos Humanos – MINJUSDH
- Poder Judicial
- Ministerio Público
- Policía Nacional del Perú
- Consejo Nacional de Ciencia, Tecnología e Innovación del Perú – CONCYTEC.

VII. EFECTOS DE LA VIGENCIA DE LA NORMA SOBRE LA LEGISLACIÓN NACIONAL

La propuesta incorpora el artículo 12-B a la Ley N.º 30096 - Ley de Delitos Informáticos. La finalidad es sancionar la creación, administración, financiamiento, operación, dirección o contratación deliberada de redes digitales automatizadas o inauténticas coordinadas cuando se utilicen con una finalidad ilícita determinada por la ley.

También se incorporan circunstancias agravantes cuando la conducta sea financiada con fuentes prohibidas, cuando el autor sea autoridad, funcionario o servidor público, o cuando se usen recursos públicos. La agravación alcanza además a las campañas sistemáticas de difamación, al empleo de inteligencia artificial como instrumento esencial de la operación ilícita y a los supuestos ejecutados por una organización criminal o por encargo de esta.

En materia de difamación, la propuesta no crea un nuevo delito autónomo. El artículo 132 del Código Penal mantiene su regulación vigente. La reforma reconoce que el uso organizado de una red digital puede aumentar considerablemente la propagación y el daño causado por imputaciones falsas; por ello, establece una agravación específica cuando concurran los elementos adicionales previstos.

La propuesta modifica la Ley N.º 30057 - Ley del Servicio Civil - e incorpora el literal r) al artículo 85 para establecer responsabilidad disciplinaria cuando servidores civiles utilicen indebidamente recursos, infraestructura, sistemas o información del Estado en operaciones digitales ilícitas.

Finalmente, se modifica la Ley N.º 28094 mediante la incorporación del numeral 9 al inciso c) del artículo 36, a fin de calificar como infracción muy grave la financiación, contratación,

promoción o utilización de operaciones digitales coordinadas ilícitas atribuibles a una organización política.

VIII. ANÁLISIS COSTO-BENEFICIO

La aplicación de la ley no genera egresos adicionales al Tesoro Público, porque la fiscalización y el juzgamiento recaen en la estructura existente del sistema penal, los organismos electorales y la Policía Nacional del Perú.

En términos de beneficio social, la norma favorece una contienda electoral más limpia, protege los recursos públicos frente a su uso indebido en propaganda encubierta y refuerza la confianza ciudadana en las instituciones democráticas.

IX. RELACIÓN CON LAS POLÍTICAS NACIONALES DEL ESTADO

El proyecto se relaciona con dos políticas de Estado del Acuerdo Nacional:

1. Democracia y Estado de Derecho: esta política comprende el fortalecimiento del régimen democrático y el respeto de las garantías fundamentales. Su contenido promueve elecciones libres y transparentes, pluralismo, alternancia en el poder y participación ciudadana en la toma de decisiones públicas, con especial atención al papel de los partidos políticos.
2. Estado eficiente, transparente y descentralizado: esta política afirma principios éticos y valores sociales orientados a la vigilancia ciudadana, la transparencia y la confianza institucional. La propuesta se vincula con ese objetivo al prohibir el uso indebido de recursos, infraestructura y personal estatal en operaciones digitales con fines políticos o ilícitos.

El Acuerdo Nacional reconoce, de manera concurrente, la necesidad de fortalecer la democracia y proteger las garantías y libertades fundamentales.