Boletín N° 18.820-19

Proyecto de ley, iniciado en Moción de los Honorables Senadores señoras Núñez y Vodanovic y señores Flores, Ossandón y Walker, que modifica la ley N° 21.663, marco de ciberseguridad, con el objeto de establecer nuevas obligaciones para las instituciones privadas que operen agentes de inteligencia artificial.

FUNDAMENTOS

La utilización de sistemas de inteligencia artificial capaces de ejecutar acciones sobre redes y sistemas informáticos exige que las instituciones que los emplean conserven un control efectivo sobre su funcionamiento. Cuando un sistema puede acceder a información, modificar archivos, utilizar credenciales o encomendar tareas a otros agentes, resulta necesario determinar quién autorizó su operación, cuáles son sus permisos y de qué manera puede interrumpirse una actuación que exceda lo autorizado.

Esta necesidad adquiere especial relevancia en actividades de cuya continuidad dependen prestaciones indispensables para la población. Una actuación no autorizada sobre los sistemas que sostienen esos servicios puede comprometer información sensible, alterar procesos o extender sus efectos a otras instituciones. La prevención requiere que los límites de operación sean verificables y que existan medios para hacerlos cumplir durante toda la ejecución de una tarea.

La ley N° 21.663 establece deberes de prevención, reporte y respuesta frente a incidentes de ciberseguridad, junto con obligaciones específicas para los operadores de importancia vital. Sobre esa base, el presente proyecto incorpora exigencias relativas a los agentes de inteligencia artificial, atendidas su capacidad de actuar sin intervención humana en cada acción y la posibilidad de delegar tareas o activar otros agentes.

La propuesta comprende tanto los sistemas que ejecutan acciones autónomamente como aquellos que requieren autorización humana para determinadas operaciones. La existencia de una aprobación previa no elimina la necesidad de controlar los accesos ni de verificar que la ejecución se mantenga dentro de lo permitido. Por ello, la regulación atiende a las capacidades y permisos del agente, con independencia de la denominación comercial o de la tecnología utilizada.

El proyecto exige que cada agente cuente con una identidad digital verificable, vinculada a la institución que lo opera. Esta identificación permitirá distinguir sus actuaciones de las realizadas por personas naturales o por otros sistemas y reconstruir las autorizaciones bajo las cuales intervino. Su finalidad es asegurar la trazabilidad de la operación y facilitar la determinación de responsabilidades cuando corresponda.

Los permisos deberán definirse antes de la puesta en operación y limitarse a lo necesario para la tarea encomendada. La autorización deberá precisar los recursos accesibles, las acciones permitidas y su vigencia. Si el agente delega una tarea o activa otro agente, los permisos derivados deberán mantenerse dentro de los límites de la autorización original. Con ello se busca evitar que una sucesión de delegaciones termine ampliando accesos que la institución nunca autorizó.

El control de estas operaciones requiere mecanismos independientes de las instrucciones y del entrenamiento del modelo. La institución deberá disponer de medios para detectar desviaciones, suspender o revocar accesos e interrumpir la actividad de manera segura. Cuando se exija una aprobación humana, su verificación deberá efectuarse mediante mecanismos que el propio agente no pueda sustituir ni modificar. La interrupción deberá considerar sus posibles efectos sobre las personas y la continuidad de los servicios esenciales.

Las obligaciones también serán exigibles cuando la operación se realice por medio de proveedores. En estos casos, la institución deberá establecer las condiciones técnicas y contractuales que le permitan acceder a los registros pertinentes y hacer efectiva la suspensión o revocación de los accesos. La contratación de un tercero debe ser compatible con el cumplimiento de los deberes de seguridad que corresponden a quien utiliza estos sistemas.

La propuesta contempla exigencias adicionales para las instituciones privadas calificadas como operadores de importancia vital. Estas deberán incorporar a su sistema de gestión de seguridad de la información un registro actualizado de los agentes con acceso a sistemas de producción y evaluar sus controles antes de ponerlos en operación, después de modificaciones sustanciales y periódicamente, según el riesgo. Las pruebas deberán permitir comprobar si las medidas de segundad pueden ser eludidas o presentan fallas que requieran corrección.

Asimismo, se incorpora el registro interno de los cuasi incidentes de pérdida de control. Se trata de eventos en que una actuación supera una medida de seguridad, pero es contenida por otra antes de comprometer los bienes protegidos por la ley. Su examen permitirá identificar

deficiencias y corregirlas oportunamente. Este deber no sustituye ni posterga los reportes y comunicaciones que resulten exigibles conforme a las disposiciones vigentes.

Respecto de los incidentes de pérdida de control, el proyecto precisa que tendrán efecto significativo aquellos en que un agente obtenga privilegios de administración no autorizados sobre sistemas de producción o se propague fuera de su entorno autorizado con capacidad efectiva para ejecutar código o utilizar credenciales privilegiadas en otros sistemas. La gravedad de estas situaciones justifica su calificación aun cuando no se haya producido una interrupción del servicio o un perjuicio patrimonial.

Las medidas exigidas deberán ser proporcionales a la autonomía del agente, sus permisos, la sensibilidad de la información y la criticidad de los sistemas involucrados. Se permitirá utilizar soluciones tecnológicas equivalentes que satisfagan los mismos objetivos de seguridad. Los registros deberán limitarse a la información necesaria, sujetarse a la normativa sobre protección de datos personales y excluir contraseñas, claves privadas y otros secretos de autenticación.

El ámbito de las nuevas obligaciones se circunscribe a las instituciones privadas comprendidas en el artículo 4º de la ley, con las exclusiones expresamente previstas para los organismos y entidades estatales, el Coordinador Eléctrico Nacional y las personas jurídicas con participación o control del Estado. El proyecto incorpora estas exigencias al régimen de infracciones existente y establece que la sola ocurrencia de un incidente o cuasi incidente no será prueba suficiente de incumplimiento. Para sancionar deberá acreditarse una acción u omisión imputable a la institución y el deber específico infringido.

Finalmente, se contempla un plazo de doce meses desde la publicación de la ley para su entrada en vigencia, a fin de permitir la adecuación de los sistemas, la revisión de los contratos con proveedores y la implementación de los controles exigidos.

IDEA MATRIZ

Establecer, en la ley N° 21.663, obligaciones de identificación, autorización, trazabilidad y control de los agentes de inteligencia artificial operados por las instituciones privadas que determina el proyecto, directamente o por medio de terceros, con exigencias adicionales para los operadores de importancia vital, reglas de gestión de incidentes y cuasi incidentes de pérdida de control y adecuaciones al regimen de infracciones, para proteger la seguridad de

la información y la continuidad de los servicios esenciales.

PROYECTO DE LEY

“Artículo único. - Introdúcense las siguientes modificaciones en la ley N° 21.663, marco de ciberseguridad:

1) Agréganse en el artículo 2º los siguientes numerales 16, 17, 18 y 19:

“16. Agente de inteligencia artificial: sistema de inteligencia artificial capaz de seleccionar y ejecutar acciones sobre redes y sistemas informáticos para cumplir objetivos determinados, sin requerir intervención humana en cada una de ellas. Se incluyen los sistemas en que determinadas acciones requieran autorización humana previa.

17 Identidad digital: conjunto de identificadores y atributos asociados a una persona natural o jurídica, dispositivo, sistema o proceso informático, que permite su individualización y distinción dentro de un determinado entorno digital.

18 Incidente de pérdida de control: incidente de ciberseguridad originado en la ejecución, por un agente de inteligencia artificial, de acciones que excedan sus permisos o el alcance autorizado de su operación.

19 Cuasi incidente de pérdida de control: evento en que una actuación de un agente de inteligencia artificial supera una medida destinada a limitar sus permisos o su ámbito de operación, pero es contenida por otra medida antes de perjudicar o comprometer cualquiera de los elementos señalados en el numeral 10.”.

2) Incorpórase el siguiente artículo 7° bis:

“Artículo 7º bis. - Identificación y control de agentes de inteligencia artificial. Las obligaciones de este artículo serán aplicables exclusivamente a las instituciones privadas comprendidas en el artículo 4°. Quedan excluidos los organismos y entidades señalados en los incisos segundo y tercero del artículo 1°, el Coordinador Eléctrico Nacional y las personas jurídicas en cuyo capital participe el Estado o sus organismos, o cuya administración sea

controlada por éstos, directa o indirectamente.

Las instituciones privadas señaladas en el inciso anterior que operen agentes de inteligencia artificial, directamente o por medio de terceros, deberán:

a) Mantener una identidad digital verificable para cada agente, vinculada a la institución que lo opera, que permita distinguir sus actuaciones de las realizadas por personas naturales o por otros agentes.

b) Determinar y registrar, antes de su operación, la autorización correspondiente, la persona que la otorga, los recursos a los que podrá acceder, las acciones permitidas y los límites y vigencia de sus permisos. Estos deberán restringirse a lo necesario para la tarea encomendada.

c) Autorizar y registrar la delegación de tareas y la creación o activación de otros agentes. Los permisos derivados no podrán exceder el objeto, alcance ni vigencia de la autorización original.

d) Mantener registros que permitan reconstruir las actuaciones de cada agente, su fecha y hora, las autorizaciones aplicables y las delegaciones realizadas, y detectar alteraciones no autorizadas de tales registros. Su contenido y conservación se limitarán a lo necesario para fines de seguridad, auditoría y cumplimiento de obligaciones legales, con sujeción a la normativa sobre protección de datos personales. No deberán contener contraseñas, claves privadas u otros secretos de autenticación.

e) Implementar controles de acceso y supervisión independientes de las instrucciones y del entrenamiento de los modelos utilizados, que permitan detectar desviaciones, suspender o revocar los accesos e interrumpir la operación de manera segura. Las aprobaciones humanas exigidas deberán verificarse por medios que el agente no pueda sustituir o modificar. La suspensión o revocación procederá sin demora indebida cuando termine la finalidad o vigencia de los permisos, o existan antecedentes fundados de su compromiso o utilización no autorizada, y comprenderá los permisos derivados que dependan de ellos.

Estas obligaciones se cumplirán mediante medidas proporcionales a la autonomía del agente, sus permisos, la sensibilidad de la información y la criticidad de los sistemas involucrados, sin perjuicio de los protocolos y estándares que resulten aplicables conforme al artículo 7°. Podrán emplearse soluciones tecnológicas equivalentes que cumplan los mismos objetivos de seguridad. La interrupción de la operación deberá considerar los riesgos para las personas y

la continuidad de los servicios esenciales.

La desactivación temporal de controles para realizar pruebas requerirá autorización previa y documentada, una evaluación del riesgo y medidas compensatorias verificadas. Las pruebas deberán efectuarse en entornos separados de los sistemas de producción y no podrán afectar sistemas de terceros sin autorización de sus titulares o administradores facultados. En todo caso, deberán mantenerse controles independientes que aseguren el aislamiento, la trazabilidad y la interrupción segura de la actividad.

Cuando intervengan proveedores, la institución privada deberá establecer las condiciones técnicas y contractuales necesarias para cumplir las obligaciones de este artículo, incluido el acceso a los registros pertinentes y la suspensión o revocación de accesos. La contratación de terceros no la eximirá de estas obligaciones.”.

3) Agréganse en el artículo 8º las siguientes letras j) y k):

“j) Tratándose de instituciones privadas sujetas al artículo 7º bis, mantener, como parte del sistema de gestión de seguridad de la información, un registro actualizado de los agentes de inteligencia artificial que operen, directamente o por medio de terceros, con acceso a sistemas de producción propios o de terceros. El registro deberá identificar cada agente, su finalidad, los sistemas a los que tenga acceso, sus permisos y la persona responsable de su supervisión, así como la configuración o versión utilizada cuando sea relevante para la seguridad.

k) Tratándose de instituciones privadas sujetas al artículo 7° bis, evaluar los controles de los agentes señalados en la letra anterior antes de su puesta en operación, después de modificaciones sustanciales que puedan afectar su seguridad y periódicamente según el riesgo. Las evaluaciones deberán comprender la eficacia de los controles exigidos en dicho artículo, mediante pruebas destinadas a detectar su elusión o funcionamiento defectuoso. Su periodicidad, resultados y medidas correctivas deberán quedar documentados en el sistema de gestión de seguridad de la información.”.

4) Incorpórase el siguiente artículo 9° bis:

"Artículo 9º bis. - Gestión interna de cuasi incidentes de pérdida de control. Las instituciones privadas sujetas al artículo 7º bis deberán mantener un registro interno de los cuasi incidentes de pérdida de control de que hayan tomado conocimiento respecto de los agentes de inteligencia artificial que operen, directamente o por medio de terceros. El registro deberá

identificar al agente involucrado, la fecha del evento, las medidas de control superadas, las que permitieron contenerlo y las acciones correctivas adoptadas.

Las instituciones señaladas en el inciso anterior deberán evaluar las deficiencias evidenciadas por estos eventos y adoptar las medidas correctivas que correspondan, atendida la naturaleza y magnitud del riesgo.

No será exigible registrar como cuasi incidentes los resultados esperados de pruebas previamente autorizadas y documentadas que se mantengan dentro de su alcance y entorno de ejecución. Esta exclusión no comprenderá las desviaciones imprevistas que constituyan cuasi incidentes.

El contenido, conservación y protección del registro se sujetarán a lo dispuesto en la letra d) del inciso segundo del artículo 7º bis. Tratándose de instituciones privadas calificadas como operadores de importancia vital, el registro se integrará a su sistema de gestión de seguridad de la información.

El registro y la gestión interna previstos en este artículo no sustituirán ni postergarán los reportes exigidos en el artículo 9° ni las comunicaciones que correspondan conforme a la letra d) del artículo 8°. La contención o interrupción de un evento no eximirá de cumplir dichas obligaciones cuando concurran sus presupuestos.”.

5) Intercalase en el artículo 27 el siguiente inciso segundo, nuevo, pasando los actuales incisos segundo, tercero y cuarto a ser incisos tercero, cuarto y quinto, respectivamente:

“Tratándose de agentes de inteligencia artificial operados por instituciones privadas sujetas al artículo 7º bis, directamente o por medio de terceros, se considerarán asimismo de efecto significativo los incidentes de pérdida de control en que un agente obtenga privilegios de administración no autorizados sobre sistemas de producción, propios o de terceros, o se propague fuera de su entorno autorizado con capacidad efectiva de ejecutar código o utilizar credenciales privilegiadas en otros sistemas. Esta calificación no requerirá que se haya producido una interrupción del servicio o un perjuicio patrimonial.”.

6) Modificase el artículo 38 en los siguientes términos:

a) Agrégase en el inciso tercero el siguiente numeral 8:

“8. No establecer o mantener las medidas de identificación, autorización, limitación de

permisos, control de delegaciones y supervisión exigidas en las letras a), b), c) y e) del inciso segundo del artículo 7º bis, o desactivar temporalmente controles sin cumplir las condiciones establecidas en el inciso cuarto de dicho artículo.”.

b) Agrégase el siguiente inciso final:

“La sola ocurrencia de un incidente o cuasi incidente de pérdida de control no constituirá prueba suficiente del incumplimiento de las obligaciones establecidas en los artículos 7º bis y 9º bis y en las letras j) y k) del artículo 8°. La determinación de una infracción requerirá acreditar la acción u omisión imputable a la institución privada y el deber específico infringido.”.

7) Modificase el artículo 39 en los siguientes términos:

a) Agrégase en el inciso segundo el siguiente numeral 7:

“7. Incumplir la obligación de mantener actualizado el registro señalado en la letra j) o de documentar la periodicidad, los resultados y las medidas correctivas de las evaluaciones y pruebas conforme a la letra k).”.

b) Agrégase en el inciso tercero el siguiente numeral 6:

“6. No realizar las evaluaciones y pruebas de los controles de agentes de inteligencia artificial exigidas en la letra k).".

Artículo transitorio. - La presente ley entrará en vigencia transcurridos doce meses desde su publicación en el Diario Oficial.”.