EL MERCURIO Legal

Versión para imprimir El Mercurio.com

Privacidad de los datos y rol de la Agencia Nacional de Datos frente a la Agencia Nacional de Inteligencia: un diálogo imprescindible

Por ello, para garantizar el uso democrático de la información por parte de la ANI con fines de defensa nacional, es imperativo formular legislativamente una buena excepción destinada a asegurar el equilibrio necesario entre seguridad y privacidad. Cada día, con más frecuencia, son empleadas las tecnologías de IA en las iniciativas de contraterrorismo, debido a que en este campo existen grandes volúmenes de datos personales que son susceptibles a ser procesados por sistemas inteligentes capaces de detectar patrones sutiles en el comportamiento humano.

Viernes, 19 de diciembre de 2025 a las 19:00

Betty Martínez-Cárdenas

En un reciente *workshop*, desarrollado por la Vicerrectoría de Investigación, Creación Artística y Doctorado de la Universidad Finis Terrae y el Ministerio de Defensa Nacional de Chile, tuve la oportunidad de presentar mi ponencia sobre los desafíos éticos y regulatorios relacionados con la Inteligencia Artificial (IA) en el sector para la seguridad y defensa nacional. Allí, como parte de las estrategias a seguir, presenté la necesidad de establecer un diálogo con la que será próximamente la Agencia Nacional de Datos (ANDP).

¿Por qué este diálogo es imprescindible? Pues bien, en Chile, la reciente la Ley 21.719, que reemplazó a la Ley 19.628, si bien previó principios de legalidad, finalidad, proporcionalidad, seguridad y transparencia para proteger el derecho de la persona a tomar decisiones sobre el procesamiento de datos personales por entidades públicas y privadas, no menciona ni indica algún tipo de excepción ordinaria y general para el procesamiento de información para seguridad nacional, defensa o inteligencia.

Sin embargo, la Ley 19.974, sobre el Sistema de Inteligencia del Estado (SIE), regula el régimen de

inteligencia, reconoce que son justamente los datos los que hace posible esta labor.

En efecto, de acuerdo con el artículo 2 de esta ley, se entiende por Inteligencia "el proceso sistemático de recolección, evaluación y análisis de información, cuya finalidad es producir conocimiento útil para la toma de decisiones". En consecuencia, la Agencia Nacional de Inteligencia (ANI) está facultada para capturar y evaluar datos sobre todos los dominios nacionales e internacionales (art. 8.a). Esta misma norma establece que los informes de inteligencia son secretos (art. 8.b) y se autoriza a la ANI a solicitar información de todos los servicios de la Administración del Estado que se requiera para proporcionar la información (art. 8.d–e). Esto indica la existencia en Chile de un régimen sectorial especial para el procesamiento de información, incluidos los datos personales, bajo un marco de secreto y cooperación obligatoria que actúa efectivamente como una excepción funcional al régimen general de protección de datos.

Lo anterior se apoya en lo que se conoce como el sistema de inteligencia chileno, consistente en regulaciones, decretos y Ley de Transparencia. La Ley 19.974 establece que la organización operativa del SIE está acompañada de regulaciones y normas internas, muchas de las cuales no se divulgan y son privadas. Como han señalado informes legislativos de diversos tipos, desde la evaluación del sistema de inteligencia de la BCN hasta el BER, un alcance sustancial del funcionamiento interno y, en particular, los métodos de procesamiento de información se encuentran fuera de la vista del público en general.

La excepción en favor de la ANI, debido al carácter secreto de la información que gestiona, fue reconocida como preferente frente a la obligación de transparencia la Corte Suprema. En efecto, la corte estimó en esa ocasión que la ANI no tiene la obligación de proporcionar información con respecto al tipo de información que almacena, o, al mismo tiempo, la cantidad o categorías de datos utilizados en seguridad nacional (Fisco con Consejo para la Transparencia, 2019). Por todo ello, es extraño que dicha excepción no haga parte de la nueva ley de protección de datos personales (Ley 21.719).

En contraste, otros países de la región incluyeron este tipo de excepción en la norma destinada a regular el uso de datos personales. Colombia, por ejemplo, en el artículo 2 del Estatuto General de Protección de Datos Personales, Ley 1581, de 2012, establece las excepciones explícitas en defensa y seguridad nacional con fines, además de estos, de prevención, detección y control del lavado de activos y financiación del terrorismo: inteligencia y contrainteligencia. Allí la ley enumera específicamente regiones donde la protección de datos está exenta bajo la ley, permitiendo al Estado manejar información personal sin cumplir con las condiciones estándar de consentimiento, transparencia o los derechos del individuo cuya información se utiliza.

En consecuencia, en Chile, ante la ausencia de este tipo de excepción en la ley de protección de datos personales, es probable que surja una colisión de competencias entre la ANI y la futura Agencia Nacional de Datos (ANPD), cuyas funciones son las de fiscalizar, sancionar y regular en lo técnico la materia, así como la supervisión del tratamiento de datos por todos los órganos públicos.

Vamos a verlo detenidamente. En principio, como la Ley 21.719 no contiene una excepción específica para seguridad e inteligencia, la ANPD teóricamente tendría jurisdicción sobre la ANI y las otras agencias de inteligencia. Sin embargo, en la práctica, la ANI, como lo vimos, está facultada a operar bajo reglas de secreto que impedirán o limitarán cualquier supervisión real. Por esta razón, un choque de competencias se revelará: la ANPD está legalmente obligada a supervisar a la ANI, pero, al mismo tiempo, la ANI está legalmente autorizada a no divulgar la información. Eso conduciría al sistema a un estado de

incompatibilidad estructural.

Ante esta situación, sin una excepción bien regulada, ninguna de las dos instituciones tendrá ventajas. En efecto, de un lado, la ANPD carecerá de las herramientas prácticas para obligar a la ANI a revelar qué datos personales recopila, cómo los utiliza, cómo los almacena o cuántos datos procesa; es decir, la ANPD no podrá fiscalizar una de las áreas que representa el mayor riesgo para los derechos fundamentales. Del otro, la ANI parecería ganar una ventaja, pero que es en esencia peligrosa: Chile podría estar implementando sistemas de vigilancia automatizados sin evaluación de impacto, sin transparencia y sin límites claros.

En efecto, el peligro de la falta de una buena excepción en el uso de datos para labores de vigilancia por parte del Estado ya se ha manifiesto en varios países, al emplear prácticas como la vigilancia predictiva y el perfilamiento masivo. En China, por ejemplo, la campaña "Strike Hard" permite a las autoridades en Xinjiang utilizar tecnología como aplicaciones móviles, cámaras y sistemas de Big Data para monitorear a comunidades y minorías. Human Rights Watch ha documentado cómo la convergencia de datos (movilidad, consumo, actividades religiosas) en una plataforma genera alertas de "sospecha" que resultan en detenciones arbitrarias. Por ello, este caso se destaca como la ilustración perfecta de cómo el extremo uso de IA y la Big Data en la identificación de "riesgos" se realiza sin control democrático.

Por ello, para garantizar el uso democrático de la información por parte de la ANI con fines de defensa nacional, es imperativo formular legislativamente una buena excepción destinada a asegurar el equilibrio necesario entre seguridad y privacidad. Cada día, con más frecuencia, son empleadas las tecnologías de IA en las iniciativas de contraterrorismo, debido a que en este campo existen grandes volúmenes de datos personales que son susceptibles a ser procesados por sistemas inteligentes capaces de detectar patrones sutiles en el comportamiento humano.

Un reciente artículo de una candidata a doctora de la Universidad de Iowa, Aisha Suleiman, aparecido en 2024 en el International Journal of Scientific Research and Modern Technology (IJSRMT), 3(5), 21-34, titulado "Enhancing the United States Counterterrorism Policy through Artificial Intelligence: A Comprehensive Analysis of Machine Learning Applications, Challenges, and Strategic Implications", nos recuerda que el manejo de la información por parte de organismos de inteligencia debe basarse en principios éticos como la proporcionalidad, que asegura que los métodos de vigilancia se correspondan al riesgo; necesidad, justificando el uso de IA al comprobar la ineficacia de opciones menos invasivas; efectividad, proporcionando evidencia de mejoras en seguridad, y responsabilidad, definiendo quién es responsable de las decisiones tomadas por IA.

Asimismo, Suleiman enfatiza la importancia de la confianza y legitimidad en el uso de IA contra el terrorismo, ya que esto impacta directamente en la efectividad del contraterrorismo. En efecto, se requiere voluntad política, rendición de cuentas y adecuada coordinación en el manejo de los datos privados para fines de seguridad y defensa nacional con sistemas IA. Si la Inteligencia Artificial se percibe como discriminatoria o invasiva, podría erosionar esa confianza social. Para mantenerla, es fundamental implementar gobernanza transparente e involucrar a las comunidades afectadas. Estrategias como el diálogo comunitario, informes transparentes, supervisión independiente y mecanismos de reparación son los recomendados para construir y mantener esta confianza.

Por todas estas razones, es que el pasado jueves, en el marco de nuestro *workshop*, sugerí establecer vía

legislativa una excepción expresa y bien regulada para la ANI, que no solo venga a colmar el vacío que se abre con la ANPD, sino que permita evitar la colisión de competencias, fomente un verdadero diálogo entre ambas autoridades y permita establecer puentes de confianza con los ciudadanos.

** Betty Martínez-Cárdenas es profesora investigadora de la Universidad Finis Terrae.*