



MINISTERIO DE SEGURIDAD Y JUSTICIA
Decreto N° 1673

MENDOZA, 14 DE AGOSTO DE 2026

Visto la Ley Provincial N 9562 (B.O. 15/08/2024), la Ley Nacional N° 25326 de Protección de los Datos Personales, su Decreto Reglamentario N° 1558/2001, el Artículo 43 de la Constitución Nacional, la Ley Nacional N° 27.699 aprobatoria del Protocolo modificatorio del Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal (ETS N° 108), la Resolución AAIP N° 47/2018 sobre medidas de seguridad para el tratamiento de datos personales, la Resolución AAIP N° 161/2023 y la Guía para entidades públicas y privadas en materia de Transparencia y Protección de Datos Personales para una Inteligencia Artificial responsable; y

CONSIDERANDO:

Que la Ley N° 9562 regula la utilización de videocámaras para captar imágenes y datos en espacios públicos, con o sin asistencia de inteligencia artificial, y su posterior tratamiento, fijando principios y garantías para la protección de derechos fundamentales;

Que resulta necesario reglamentar los procedimientos de integración de alarmas vinculadas, reconocimiento facial, categorización de alertas, y protocolos operativos, bajo criterios de razonabilidad, proporcionalidad, mínima intervención, confidencialidad y trazabilidad;

Que el reconocimiento facial constituye una herramienta de orientación investigativa sujeta a verificación y doble validación, que no identifica personas por sí solo, solo genera una hipótesis de coincidencia sobre determinadas personas incluidas en estrictas listas con fuente habilitante;

Que ningún resultado, alerta, coincidencia, inferencia o recomendación generada por sistemas automatizados podrá producir por sí sola consecuencias jurídicas, policiales, administrativas o restrictivas de derechos respecto de una persona, sin intervención humana significativa, verificación independiente, fuente habilitante vigente y documentación trazable de la decisión adoptada;

Que en tal sentido, este reglamento establece las bases del procedimiento para el proceder operativo a partir de la alerta generada por inteligencia artificial con base en fuente habilitante judicial vigente, sujetándose a estándares reforzados de legalidad, finalidad determinada, necesidad, proporcionalidad, minimización, seguridad, trazabilidad, supervisión humana significativa, no discriminación, explicabilidad, evaluación de impacto y rendición de cuentas;

Por ello, conforme con lo dispuesto por el Artículo 128, incisos 1 y 2 de la Constitución Provincial y Art. 5° de la Ley N° 9562,

EL

GOBERNADOR DE LA PROVINCIA

DECRETA:



CAPÍTULO I DISPOSICIONES GENERALES

Artículo 1º - El presente decreto tiene por objeto reglamentar aspectos de la Ley N° 9562, estableciendo disposiciones operativas, técnicas y procedimentales en relación al funcionamiento del Sistema Provincial de Videovigilancia (SPV) y su eventual asistencia por tecnologías de analítica e inteligencia artificial, incluyendo el reconocimiento facial.

Artículo 2º - El tratamiento de imágenes, datos personales, alertas, inferencias y registros vinculados al Sistema Provincial de Videovigilancia tendrá exclusivamente las finalidades previstas en los Artículos 2º y 3º de la Ley N° 9562, quedando prohibido todo tratamiento incompatible, ulterior, masivo, indiscriminado, comercial, político-partidario, discriminatorio, de inteligencia social o de elaboración de perfiles.

Artículo 3º - La Autoridad de Aplicación y los operadores deberán ajustar toda operación del sistema a los principios de:

- a) legalidad estricta;
- b) finalidad determinada, explícita y legítima;
- c) proporcionalidad;
- d) razonabilidad;
- e) exactitud, calidad y actualización de los datos;
- f) no discriminación y prevención de sesgos;
- g) supervisión humana significativa;
- h) confidencialidad, integridad y seguridad de la información;
- i) minimización de datos;
- j) limitación del plazo de conservación;
- k) trazabilidad y auditabilidad;
- l) explicabilidad y transparencia algorítmica compatible con la seguridad pública;
- m) responsabilidad proactiva y transparencia institucional.

Artículo 4º - El Ministerio de Seguridad y Justicia, es la autoridad de aplicación conforme el Artículo 5º de la Ley N° 9562.

CAPÍTULO II DEFINICIONES

Artículo 5º - Definiciones



A los efectos del presente decreto, se entiende por:

- a) Sistema Provincial de Videovigilancia (SPV): conjunto de cámaras, dispositivos, centros de monitoreo, sistemas de almacenamiento, redes, software, herramientas de analítica y procedimientos operativos bajo control de la Autoridad de Aplicación.
- b) Dato personal: toda información de cualquier tipo referida a personas humanas determinadas o determinables, incluyendo imágenes, voz, rasgos físicos, datos biométricos, ubicación, metadatos, identificadores técnicos o cualquier otro dato que permita directa o indirectamente su identificación.
- c) Sistema de Inteligencia Artificial: sistema automatizado o semiautomatizado que, mediante modelos algorítmicos, estadísticos, de aprendizaje automático u otros métodos computacionales, procesa datos de entrada y genera resultados, inferencias, clasificaciones, alertas, recomendaciones o predicciones que pueden incidir en una actuación humana posterior.
- d) Reconocimiento facial: tratamiento automatizado o semiautomatizado de imágenes faciales orientado a comparar un rostro con una o más imágenes de referencia, con el objeto de generar una hipótesis de coincidencia o similitud.
- e) Fuente habilitante: orden judicial, requerimiento formal de autoridad competente, comunicación oficial vigente o acto administrativo fundado que autorice la incorporación de una persona determinada a una lista de alerta, con indicación de finalidad, plazo, alcance, autoridad requirente, expediente o legajo y nivel de intervención autorizado.
- f) Alerta de coincidencia: resultado técnico que indica similitud entre una imagen captada y un registro incorporado a una lista de alertas, con carácter meramente indiciario, orientativo y no concluyente.
- g) Falso positivo: alerta de coincidencia respecto de una persona que no corresponde con el registro buscado.
- h) Operador habilitado: agente formalmente autorizado para operar el sistema, capacitado, sujeto a confidencialidad, trazabilidad y responsabilidad funcional.
- i) Supervisión humana significativa: intervención de persona humana que evalúa críticamente la alerta, verifica su consistencia, documenta la decisión y evita que el resultado algorítmico produzca consecuencias automáticas.
- j) Evaluación de Impacto: procedimiento documentado y periódico, destinado a identificar, evaluar, prevenir y mitigar riesgos para la privacidad, la protección de datos personales, la igualdad, la no discriminación, la libertad ambulatoria, el debido proceso y demás derechos fundamentales derivados del diseño, implementación, operación o modificación sustancial del sistema.

CAPÍTULO III ALERTAS

Artículo 6º - En el ámbito del SPV, y a los efectos de la generación de alertas de reconocimiento facial, se tendrán en cuenta los siguientes códigos operativos con capacidad de integrar el



sistema:

- a) Código RF-1 — Búsqueda de paradero: personas denunciadas como desaparecidas, extraviadas o respecto de quienes exista requerimiento competente de localización, con especial identificación de niñas, niños, adolescentes, personas mayores o personas en situación de vulnerabilidad.
- b) Código RF-2 — Control sobre prisiones/detenciones domiciliarias: personas que se encuentren en situación de prisión o detención domiciliaria y respecto de quienes exista una orden de autoridad judicial que ordene su control por esta vía.
- c) Código RF-3 — Captura o detención: personas con pedido de captura o detención, fuga, con orden de autoridad judicial competente.

Los códigos solo podrán surgir de fuente judicial habilitante verificable, entendiéndose por tal la emanada del Ministerio Público Fiscal Nacional o Provincial y Poder Judicial Nacional o Provincial, y tendrán carácter confidencial, de acceso restringido y sujeto a control, revisión periódica y auditoría.

En caso de evasión o fuga, paradero de riesgo u otros casos de urgencia, la autorización judicial podrá ser emitida de forma telefónica, debiendo dejar debida constancia.

La autoridad competente podrá rechazar la inclusión de una alerta cuando existan razones técnicas que hagan inviable su procedencia, debiendo fundar dicha situación ante la autoridad judicial.

CAPÍTULO IV PROCEDIMIENTO

Artículo 7º - El reconocimiento facial solo podrá operar respecto de personas determinadas e individualizadas que correspondan a alguno de los códigos mencionados. Queda prohibida la creación informal, paralela o no documentada de listas.

Artículo 8º - No se considerará alerta de coincidencia válida para aplicar el procedimiento previsto aquí, umbrales de coincidencia por debajo de lo que determine la autoridad de aplicación por resolución fundada. En ningún caso el umbral técnico bastará por sí solo para tener por identificada a una persona ni para adoptar medidas restrictivas de derechos.

Artículo 9º - Generada la alerta se requerirá validación reforzada con intervención humana significativa. El operador habilitado del Centro Estratégico de Operaciones (CEO) que advierta o reciba la alerta deberá efectuar una primera validación humana significativa, consistente en verificar la calidad de la imagen, el umbral alcanzado, la correspondencia visual preliminar y el tipo de código de alerta.

Cuando dicha validación resulte positiva el CEO comunicará la novedad al personal policial correspondiente, dejando constancia trazable de la alerta, operador interviniente, horario, cámara, fuente habilitante, tipo de código y motivos de la actuación.

El personal policial desplazado realizará una validación humana significativa en el lugar o por canal oficial seguro, mediante constatación fehaciente de identidad y verificación actualizada de



la medida, pudiendo recurrir a medios digitales, de comunicación policial o consulta a la división judiciales de la Policía de Mendoza.

En los códigos de búsqueda de paradero, la actuación deberá priorizar el resguardo de la persona y la protección reforzada de niñas, niños, adolescentes, personas mayores o personas en situación de vulnerabilidad.

Artículo 10º - En caso de falso positivo, se deberá dejar asentado para los informes y auditoría correspondiente.

En caso de detectarse falta de consistencia entre lo notificado por la autoridad judicial y lo que la supervisión humana significativa constata en el momento de la alerta, esto es, que formalmente figure una notificación judicial sobre algún pedido correspondiente a cualquier código y que, no se encuentre vigente o se haya dado la baja en el expediente sin notificar debidamente a la autoridad competente de esta ley, no se tomará ninguna medida con la persona habida o se dispondrá la inmediata liberación en su caso, dejando constancia e informando a la autoridad judicial para que proceda a notificar formalmente la baja de la medida.

CAPÍTULO V COORDINACIÓN JUDICIAL

Artículo 11º - La Autoridad de Aplicación establecerá mecanismos de coordinación con el Poder Judicial y el Ministerio Público Fiscal, en el marco de sus respectivas competencias, para que aquellos comuniquen las altas, modificaciones, prórrogas, suspensiones, ceses y bajas de las solicitudes de paradero, pedidos de captura, órdenes de detención, medidas de prisión/detención domiciliaria, restricciones vigentes u otras medidas legalmente habilitantes.

Dicha comunicación deberá efectuarse en tiempo oportuno, por canales formales, seguros y trazables, acompañando la información mínima necesaria para la correcta identificación de la persona, la finalidad de la medida, la autoridad requirente, el expediente o legajo correspondiente, el plazo de vigencia si lo hubiere y toda otra información relevante para la actuación operativa.

La Autoridad requirente será responsable de informar de manera inmediata cualquier modificación, cese, revocación, cumplimiento, caducidad o pérdida de vigencia de la medida que motivó la incorporación al sistema de alertas.

En casos de urgencia debidamente fundada, la comunicación podrá efectuarse por canal excepcional, seguro y trazable, siempre que permita identificar a la autoridad requirente, la medida solicitada, la persona individualizada, el expediente o legajo, la finalidad y el plazo de vigencia. La documentación formal respaldatoria deberá acompañarse dentro del plazo máximo de cuarenta y ocho (48) horas. Vencido dicho plazo sin ratificación formal, la incorporación deberá cesar automáticamente y eliminarse del sistema, dejando constancia auditable.

CAPÍTULO VI — REGISTROS, SEGURIDAD Y CONFIDENCIALIDAD

Artículo 12º - El personal habilitado a operar con el sistema de alerta se logueará con doble sistema de autenticación, siempre los usuarios serán nominados, quedará registro de todo acceso y toda acción que realice en el sistema el operador logueado.



Todo el personal con acceso al sistema se encuentra alcanzado por el deber de secreto y confidencialidad previsto en la Ley 9562, aun luego de finalizada su función.

Artículo 13º - La Autoridad de Aplicación implementará medidas de ciberseguridad en orden al resguardo de la información contenida en el sistema.

Artículo 14º - Queda prohibida la comunicación y/o publicación de eventos relacionados al sistema de videovigilancia y reconocimiento facial, cuando medien razones de seguridad o fuere necesario a los fines de evitar obstaculizar el éxito de una investigación.

En su caso, toda comunicación pública, institucional o periodística relativa a procedimientos, alertas o resultados exitosos producto de la aplicación del sistema deberá respetar la presunción de inocencia, la dignidad, la intimidad, el honor, la protección de datos personales y especialmente la protección del interés superior de niñas, niños y adolescentes.

En caso de tratarse de niñas, niños y adolescentes se deberá dar comunicación a la autoridad interviniente que corresponda.

CAPÍTULO VII CONSERVACIÓN, DISPONIBILIDAD Y DESTRUCCIÓN

Artículo 15º - En eventos que generen alertas, el sistema deberá resguardar el extracto fílmico estrictamente necesario para documentar el incidente, junto con los metadatos mínimos asociados, etiquetando el registro para su recuperación rápida y eventual puesta a disposición de autoridad competente.

La conservación se ajustará a los plazos previstos en la Ley N° 9562. Vencidos dichos plazos, y salvo requerimiento fundado de autoridad competente, podrá según el caso procederse a su destrucción.

CAPÍTULO VIII EVALUACIÓN DE IMPACTO

Artículo 16º - La Autoridad de Aplicación está obligada a realizar la evaluación de impacto sobre el sistema al menos una vez al año, y/o ante cualquier cambio relevante del sistema, proveedor, algoritmo, fuente de datos, finalidad o modalidad de uso, realizando informe a tal fin, obligándose a gestionar las recomendaciones que surjan del mismo.

Artículo 17º - La Autoridad de Aplicación deberá publicar en su sitio web institucional, y en otros medios idóneos de acceso público general, en lenguaje claro y accesible, información general sobre el SPV, sobre los tipos códigos de alerta, las finalidades del SPV, autoridad responsable, derechos de las personas, canales de contacto, criterios generales de funcionamiento de tecnologías de inteligencia artificial y la existencia de evaluaciones de impacto.

La publicación no deberá revelar ubicaciones específicas, parámetros operativos sensibles, investigaciones en curso ni información que comprometa la seguridad pública.

CAPÍTULO IX Derecho de Acceso a la Información

Artículo 18º - Toda persona podrá ejercer, conforme la Ley N° 25.326 y la normativa aplicable, los derechos de acceso, rectificación, actualización, supresión, confidencialidad, oposición



cuando corresponda y revisión humana respecto de los datos personales en el marco del SPV.

La Autoridad de Aplicación deberá habilitar canales presenciales y digitales para la recepción de solicitudes, establecer plazos de respuesta, mecanismos de acreditación de identidad, registro de trámites y vías de reclamo.

Deberá dictar una resolución con las especificaciones conducentes al efectivo ejercicio de este derecho.

Cuando la entrega de imágenes pudiera afectar derechos de terceros, investigaciones en curso o la seguridad pública, la autoridad de aplicación deberá fundar la excepción.

Cuando resulte posible y sea razonable a la custodia de los objetivos mencionados en el párrafo anterior, podrá entregar información parcial, anonimizada, pixelada o disociada.

Será de aplicación lo dispuesto en el artículo 17, incisos 1 y 2, de la Ley N° 25.326, en su caso.

CAPÍTULO X DISPOSICIONES COMPLEMENTARIAS

Artículo 19º - La Autoridad de Aplicación protocolizará por acto administrativo interno los procedimientos y protocolos que sean necesarios para la aplicación y ejecución de la ley y esta reglamentación.

Artículo 20º - Comuníquese, publíquese, dese al Registro Oficial y archívese.

LIC. ALFREDO V. CORNEJO

MGTR. MARÍA MERCEDES RUS

Publicaciones: 1

Fecha de Publicación	Nro Boletín
20/08/2026	32659