Solicitud de Acceso a la Información Pública

JUZGADO LETRADO DE PRIMERA INSTANCIA EN LO CONTENCIOSO ADMINISTRATIVO DE TURNO:

Patricia Myrna Díaz Charquero, titular de la cédula de identidad número [redacted], con domicilio real en [redacted], constituyendo domicilio electrónico en [redacted], al Sr. Juez se presenta y DICE:

Que al amparo de la Ley Nº 18.381 viene a interponer acción de acceso a la información pública contra el **Ministerio del Interior con domicilio en la calle Mercedes 993, Montevideo,** en mérito a las siguientes circunstancias de hecho y fundamentos de derecho.

ANTECEDENTES

1. La aquí compareciente, Dra. Patricia Díaz se desempeña desde el año 2020 como coordinadora del proyecto Datysoc - Laboratorio de Datos y Sociedad, parte de la asociación civil Data Uruguay.
2. Datysoc impulsa estudios de investigación y acción en el área de derechos digitales y el impacto de las tecnologías de la información en los derechos humanos. Desde este laboratorio académico y activista se desarrollan análisis multidisciplinarios sobre el uso y explotación de datos personales por parte de actores públicos y privados. Como parte de la sociedad civil organizada, Datysoc cumple además un rol de educación y difusión sobre las implicancias del uso de tecnologías digitales en distintas áreas centrales en la vida de las personas.
3. El presente pedido de acceso a la información, realizado por la Sra. Patricia Díaz a título personal, se enmarca dentro de este contexto, y específicamente en la línea de investigación-acción sobre el uso de videovigilancia y reconocimiento facial automatizado con fines de seguridad pública.[1] Como se dirá, la información solicitada reviste alto interés público y corresponde su entrega a la solicitante.

VÍA ADMINISTRATIVA

[1] Datysoc. *Uso policial del reconocimiento facial automatizado en Uruguay*. (2022). Información ampliatoria disponible en: https://datysoc.org/2022/03/23/uso-policial-del-reconocimiento-facial-automatizado-en-uruguay/

4. Con fecha 2 de noviembre de 2021, la Sra. Díaz se presentó ante el Ministerio del Interior y solicitó al amparo de la Ley Nº 18.381 de acceso a la información pública acceder a la siguiente información:

   4.1. ¿Se encuentra inscripta la Base de Reconocimiento Facial a las que hace el art. 191 de la referencia la Ley Nº 19.924 en el Registro de Bases de Datos Personales?, ¿Cuál es el Número de registro?

   4.2. Nombre y datos de contacto del delegado de protección de datos del Ministerio del interior.

   4.3. ¿Se realizó una evaluación de impacto sobre el uso del Sistema de identificación facial contratado por Licitación Pública (13/2019 Ministerio del Interior | Secretaría del Ministerio del Interior)? De ser así, se solicita acceder a esta evaluación.

   4.4. ¿El sistema de identificación facial ya se encuentra operativo o en producción?

   4.5. ¿Qué tipo de uso específico se le da o dará a este software de identificación facial (RFA)? ¿están previstos algunos de los siguientes usos?: a) Verificación de identidad (por ejemplo, cuando un sospechoso es arrestado, pero se niega a dar su nombre a la policía o cuando una persona no porta su cédula en la vía pública). b) Identificación retrospectiva o forense (con imágenes de Circuitos cerrados de videovigilancia - CCTV). c) Ciberpatrullaje (tomar las imágenes públicas en la web, por ej. en redes sociales, y usar el software RFA para confirmar la identidad y los vínculos de quienes figuran en las fotografías). d) RFA en vivo (RFA 1 a N para identificar a las "personas de interés" para las autoridades mientras atraviesan las inmediaciones del espacio público).

   4.6. Los Protocolos de uso (Protocolo de intercambio de datos con la DNIC para actualizar la base, Protocolo de protección de datos y de seguridad, Protocolo de uso por personal policial para verificación de identidad, Protocolo de actuación para identificación en ambientes no controlados, Protocolo de Auditoría, entre otros).

   4.7. Los diferentes perfiles (roles) de usuarios qué acceden a la plataforma de identificación facial existen, ¿cómo se definen estos roles?, ¿qué funcionarios del ministerio del interior se incluyen dentro de cada rol?

4.8. ¿En base a qué criterios se crearán las listas de “personas de interés” para alimentar el sistema de identificación facial?, ¿se requerirá orden judicial para la creación de este tipo de listas?

4.9. Nombre y cantidad de instancias de formación (cursos, talleres, etc.) sobre el funcionamiento del software de RFA se hicieron o se planifican realizar para el personal policial ¿cuál es la población objetivo que recibirá esta formación dentro del Ministerio del Interior? Temario cubierto en las formaciones.

4.10. Nombre y cantidad de instancias de formación (cursos, talleres, etc.) sobre el funcionamiento del software de RFA se hicieron o se planifican realizar para los actores del sistema judicial, ¿cuál es la población objetivo que recibirá esta formación dentro del sistema judicial? Temario cubierto en las formaciones.

5. La petición fue tramitada ante el Ministerio del Interior en expediente Nº 2021-4-1-0007031 en el cual se produjo la situación prevista en el Artículo 18 de la Ley Nº 18.381 de Silencio Positivo por no haber Resolución dentro del plazo legalmente previsto de 20 días hábiles.

6. Con posterioridad a dicho plazo, el día 2 de diciembre de 2021 recayó Resolución denegando el acceso a la solicitud. Por dicho acto administrativo, el Ministerio resolvió: “Desestimar la solicitud formulada por la señora Patricia Díaz Charquero, titular de la cédula de identidad número [redacted] referente al acceso a la información pública al amparo de lo dispuesto por la Ley Nº 18.381, de 17 de octubre de 2008, detallada en el Resultando, conforme los fundamentos expuestos en los Considerandos de la presente”. Acompaña este escrito copia simple de la Resolución.

7. De acuerdo a los Considerandos de dicha resolución, la peticionante cumplió con los requisitos formales para la solicitud de información exigidos por el Artículo 13 de la Ley de Acceso a la Información Pública.

8. Respecto a los aspectos sustanciales, el Ministerio rechazó el acceso por entender que se encuentra amparado en una de las excepciones de la Ley Nº 18.381. Así, manifestó que la información solicitada, reviste la calidad de “Reservada” en virtud de lo dispuesto por las Resoluciones Nº 5905 y 5909, de 25 y 30 de julio de 2012 respectivamente.

9. Dentro de los considerandos incluye también las disposiciones de la Ley Nº 18.331 de Protección de Datos Personales y la excepción del Artículo 14 de la Ley de Acceso a la Información Pública por la cual los organismos no tienen la obligación de producir información con la que no cuentan.

ANTECEDENTE: RESOLUCIÓN DE LA UNIDAD DE ACCESO A LA INFORMACIÓN PÚBLICA

10. Ante la denegatoria del Ministerio del Interior en la vía administrativa, esta parte concurrió ante la Unidad de Acceso a la Información Pública (UAIP) a efectos de obtener la opinión del organismo competente y especialista en la materia.
11. La petición tramitó en el Expediente Nº 2021-2-10-0000432 en el cual se dió vista al Ministerio del Interior. Con fecha 3 de Junio de 2022, el Consejo Ejecutivo dictó la Resolución Nº 13/2022 la cual resolvió "Indicar que el Ministerio del Interior debe proceder a entregar la información que es pública a la solicitante, así como clasificar la información reservada de acuerdo con los parámetros legales establecidos en la Ley N° 18.381." (Se adjunta copia de la Resolución).
12. La Resolución no fue recurrida por el Ministerio del Interior, quedando firme el acto administrativo.
13. El análisis del órgano especialista en la materia y encargado de velar por el cumplimiento de la Ley de Acceso es contundente respecto a la obligación del Ministerio de hacer entrega de la información.
14. Esta parte comparte el análisis efectuado por la UAIP y los fundamentos allí vertidos, al cual se remite. En el análisis que sigue se incorporan los Resultandos de la Resolución sobre cada uno de los argumentos que fundamentan esta solicitud.

SOLICITUD JUDICIAL DE INFORMACIÓN

15. En virtud de la denegación de acceso a la información que viene de relatarse, la aquí compareciente, se presenta ante la Sede a entablar la Acción Judicial de Acceso a la Información Pública de acuerdo al Capítulo Quinto de la Ley Nº 18.381.
16. La denegación administrativa por parte del Ministerio del Interior no resulta ajustada a derecho por los argumentos que se dirán e imponen que la solicitud

sea revisada y concedida por la justicia en el marco del proceso legalmente previsto.

17. A efectos de no redundar, la información solicitada en el marco de esta acción judicial corresponde a toda la que fuera oportunamente solicitada en la vía administrativa (Numeral 4 Puntos 1 a 10 de este escrito).

18. En líneas generales, la información solicitada hace referencia al manejo de datos personales por parte del Ministerio del Interior, y específicamente al despliegue y uso de tecnologías de reconocimiento facial por parte del organismo.

19. Como es de público conocimiento, desde el año 2010, el Ministerio del Interior comenzó a instalar sistemas de monitoreo y cámaras de vigilancia en la vía pública con el fin de mejorar la estrategia para prevenir el delito y aportar pruebas a la justicia. Actualmente hay casi 9 mil cámaras instaladas en todo el país según los datos del mismo Ministerio.

20. En los últimos años, la implementación de los sistemas de cámaras de vigilancia ha sido acompañada en otros países por la incorporación de tecnologías de reconocimiento facial automatizado (RFA). La tecnología de RFA utiliza imágenes del rostro de una persona y las convierte en una plantilla facial o una representación matemática de la imagen. Luego, un algoritmo puede comparar esa plantilla con una plantilla generada a partir de otra foto. De esta manera, puede determinar el nivel de similitud entre los rostros. El RFA, como tecnología biométrica, puede incluir funciones de detección, verificación e identificación facial.

21. Acerca de las tecnologías de RFA, el Consejo de Naciones Unidas ha establecido: “Los avances en el campo de la tecnología de reconocimiento biométrico han llevado a que cada vez sea más utilizada por las fuerzas del orden y los organismos de seguridad nacional. El reconocimiento biométrico se basa en la comparación de la representación digital de determinados rasgos de una persona, como el rostro, la huella dactilar, el iris, la voz o la forma de andar, con otras características de este tipo recogidas en una base de datos. A partir de la comparación se deduce una probabilidad mayor o menor de que la persona en cuestión sea aquella cuya identidad debe ser determinada. Estos procesos se realizan cada vez más en tiempo real y a distancia. En particular, las autoridades

de todo el mundo hacen un uso cada vez mayor del reconocimiento facial remoto en tiempo real".[2]

22. Uruguay parece no ser la excepción respecto a estos usos con fines de seguridad pública. Según el sitio web de la Agencia Reguladora de Compras Estatales, en febrero de 2020, el Ministerio del Interior publicó una licitación pública para la adquisición y mantenimiento de una Plataforma de Identificación Facial. Según surge de la Resolución publicada en el mismo sitio, la Licitación fue adjudicada al Consorcio en Formación integrado por DDBA Ltda. con CDT Lata LLC y TTY Sociedad Anónima por un monto total de U$S 896.258 por conceptos de Software, importación y mantenimiento.

23. Posteriormente, la Ley de Presupuesto del año 2020 creó una "base de datos de identificación facial" con fines de seguridad pública. Así, el Artículo 191 de la Ley Nº 19.924 de fecha 18 de diciembre de 2020 estableció:

> "Créase en el Inciso 04 "Ministerio del Interior", Unidad Ejecutora 001 "Secretaría del Ministerio del Interior", una base de datos de identificación facial para su administración y tratamiento con fines de seguridad pública, en estricto cumplimiento de los cometidos asignados por la Ley N° 19.315, de 18 de febrero de 2015, y a lo dispuesto en la Ley N° 18.331, de 11 de agosto de 2008."

24. Seguidamente, el Artículo 192 de la misma Ley:

> "Autorízase en el Inciso 04 "Ministerio del Interior", Unidad Ejecutora 031 "Dirección Nacional de Identificación Civil", la migración actualizada a la Unidad Ejecutora 001 "Secretaría del Ministerio del Interior", de la totalidad de las imágenes faciales de las personas mayores de edad de las que lleva registro, los nombres y apellidos de sus titulares, sexo, fecha de nacimiento, nacionalidad, número de cédula de identidad, fecha de expedición y fecha de expiración de esta última.
>
> Lo dispuesto en el presente artículo entrará en vigencia a partir de la promulgación de la presente ley."

---

[2] Asamblea, G. *Informe de la Alta Comisionada de las Naciones Unidas para los Derechos Humanos.* A/HRC/48/31. 13 de septiembre de 2021. Párr. 25. En: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G21/249/24/PDF/G2124924.pdf?OpenElement

25. La información que se solicita refiere a diferentes aspectos relativos a la implementación, uso y capacitación sobre los sistemas y bases de los que dan cuenta la licitación y los artículos antedichos. Como se verá, esta información reviste especial relevancia para la vigilancia de los derechos humanos y el control democrático al que se encuentran sujetos los organismos públicos.
26. Como se verá, la inclusión de la información solicitada dentro de una clasificación de reserva genérica se aparta del régimen legal establecido por la Ley Nº 18.381 y el marco regional que rige este derecho, lo cual obliga revisar la resolución y conceder el acceso peticionado.

SOBRE EL DERECHO DE ACCESO A LA INFORMACIÓN Y SUS EXCEPCIONES

27. En Uruguay, el Derecho de Acceso a la Información Pública cuenta con protección internacional emanada -entre otros instrumentos ratificados por el país- de la Convención Americana sobre Derechos Humanos y del Pacto Internacional de Derechos Civiles y Políticos. Asimismo posee tutela constitucional resultante del bloque de constitucionalidad de los derechos humanos y de los artículos 7, 29, 72, 82 y 332 de la Carta, y protección legal específica a partir de la sanción de la Ley Nº 18.381 del 17 de Octubre de 2008 reglamentada por el Decreto del Poder Ejecutivo Nº 232/2010.
28. La Ley Nº 18.381 incorporó el principio de máxima divulgación para la administración pública. De acuerdo al Artículo 4 de la norma, se presume pública toda información “producida, obtenida, en poder o bajo control de los sujetos obligados”. En la misma línea, el Artículo 2 señala que es pública toda la información que "emane o esté en posesión de cualquier organismo público, sea o no estatal, salvo las excepciones o secretos establecidos por ley, así como las informaciones reservadas o confidenciales”.
29. El Tribunal de Apelaciones de 2º Turno ha manifestado: “el derecho de acceso a la información es una herramienta crítica para el control del funcionamiento del Estado y la gestión pública, y para el control de la corrupción. El derecho de acceso a la información es un requisito fundamental para garantizar la transparencia y la buena gestión pública del gobierno y de las restantes autoridades estatales. El pleno ejercicio del derecho de acceso a la información es una garantía indispensable para evitar abusos de los funcionarios públicos, promover la rendición de cuentas y la transparencia en la gestión estatal y

prevenir la corrupción y el autoritarismo. De otra parte, el libre acceso a la información es un medio para que, en un sistema democrático representativo y participativo, la ciudadanía pueda ejercer adecuadamente sus derechos políticos. Sólo a través del acceso a la información bajo control del Estado que sea de interés público es que los ciudadanos pueden cuestionar, indagar y considerar si se está dando cumplimiento adecuado a las funciones públicas".[3]

30. En consonancia con lo que viene siendo expresado, la Ley Nº 18.381 dispuso un régimen legal de excepciones que es de interpretación estricta y que comprende las informaciones definidas como secretas por la ley, y las que sean clasificadas como reservada o confidencial conforme las causales taxativas que enumera la norma (Arts. 8, 9 y 10).

31. En el derecho nacional, la Suprema Corte de Justicia ha dejado claramente expresado que la regla es la publicidad de la información (principio de máxima divulgación), por lo cual las excepciones deben ser lo más acotadas y respetar los principios expuestos. En este sentido, el máximo órgano judicial ha dicho: "cabe partir de la base de que la solución de principio en materia de acceso a la información pública, es la más amplia publicidad y difusión de la información de interés público, de manera que las excepciones legalmente previstas (entre ellas la establecida en el art. 14 inc. 1o invocada por la demandada en el caso), **son de interpretación estricta** y **debe estar adecuadamente motivada**.[4] (Destacado nuestro).

32. El artículo 9 de la referida ley establece las condiciones por las cuales un organismo puede clasificar determinada información como reservada. Entre otras causales se encuentran: a) Comprometer la seguridad pública o la defensa nacional; (...) y d) Poner en riesgo la vida, la dignidad humana, la seguridad o la salud de cualquier persona.

33. Así, la Guía de Implementación de la Ley Modelo Interamericana de Acceso a la Información Pública aprobada por la OEA en base al trabajo realizado por un Grupo de Expertos de toda la región en el año 2010, dispone que: "La presunción de la divulgación requiere, pues, que la excepción sea lo menos restrictiva posible; es decir, la no divulgación debe tener un efecto directo en el ejercicio de una excepción en particular, ser proporcionada para el interés público o privado e

---

[3] Tribunal de Apelaciones en lo Civil turno 2º. (2020, agosto 3). (Sentencia N° 144/2020). Recuperado de: http://bjn.poderjudicial.gub.uy/BJNPUBLICA/hojaInsumo2.seam?cid=145170

[4] Suprema Corte de Justicia. (Sentencia Nº 405/2022).

interferir lo menos posible con el ejercicio efectivo del derecho de acceso. En las palabras del Relator Especial para la Libertad de Expresión, la excepción debe pasar una prueba de tres partes: a) debe estar relacionada con uno de los objetivos legítimos que la justifican; b) debe demostrarse que la divulgación de la información efectivamente amenaza causar un perjuicio sustancial a ese objetivo legítimo; y c) debe demostrarse que el perjuicio al objetivo es mayor que el interés público en contar con la información".[5]

34. Por lo tanto, la sustracción de determinada información del acceso público debe efectuarse, cuando es procedente, en la mínima medida posible, limitándose a lo que sea estrictamente necesario para obtener el objetivo imperioso perseguido. Además el Tribunal de Apelaciones en lo Civil de 2º Turno ha dicho: "es claro que no basta con aducir un motivo sino que éste debe existir realmente de acuerdo a la ley, debiendo la Administración detallar específicamente los motivos y fundamentos legales que la llevan a rechazar el pedido de información realizado".[6]

35. Como ha expresado la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, se debe asegurar la existencia de recursos judiciales idóneos y efectivos para que aquellos solicitantes de información que se vean afectados por decisiones que nieguen el acceso a información que consideran debiera ser pública puedan impugnarlas ante los órganos del Poder Judicial. "Los órganos judiciales están llamados a cumplir un papel fundamental para garantizar el derecho de acceso a la información y ejercer el control de convencionalidad y constitucionalidad de las normas que limitan el acceso a la información".[7]

36. Por tanto, el amparo en una Resolución de Reserva no excluye el control jurisdiccional acerca de la legalidad y la adecuación del dictamen al marco nacional y regional de derechos humanos. Los Tribunales tienen la facultad de ordenar la publicación de la información si fue indebidamente negada como ocurre en este caso.

---

[5] Consejo Permanente de la OEA, *Comentarios y Guía de Implementación para la Ley Modelo Interamericana sobre Acceso a la Información*, (2010), p. 11, en: http://www.oas.org/es/sla/ddi/docs/AG-RES_2841_XL-O-10_esp.pdf

[6] Tribunal de Apelaciones en lo Civil turno 2º. (2020, agosto 3). (Sentencia N°. 144/2020).

[7] Relatoría Especial para la Libertad de Expresión, Comisión Interamericana de Derechos Humanos, *Derecho a la Información y Seguridad Nacional,* (2020), párr. 87, en: https://www.oas.org/es/cidh/expresion/informes/DerechoInformacionSeguridadNacional.pdf

ILEGITIMIDAD DE LA RESOLUCIÓN QUE DENIEGA EL ACCESO A LA INFORMACIÓN

I) AUSENCIA DE PRUEBA DE DAÑO

37. Con el propósito de robustecer la protección del derecho de acceso a la información pública contra posibles abusos en la clasificación de información, la Ley Nº 19.178 del 9 de enero de 2014, brindó estatus legal a la llamada "prueba de daño". De acuerdo a esta disposición, la clasificación de información debe realizarse mediante "resolución debidamente fundada y motivada, en la que se demuestre la existencia de elementos objetivos que permitan determinar que la divulgación de la misma genera un riesgo claro, probable y específico de daño al interés público protegido, de acuerdo con las excepciones referidas".
38. Las pruebas de interés público y pruebas de daño son normas contra las que se deben ponderar la justificación de una excepción a la divulgación a fin de determinar si satisface los requisitos de proporcionalidad y necesidad. "Es por ello que si no existe un daño por divulgar información que en principio se encuentra dentro de las excepciones, la misma debería ser liberada, y en caso de que existiera el daño, debe procederse a evaluar si el interés del público por conocer la información no supera el daño potencialmente causado".[8]
39. Como ha establecido la Organización de Estados Americanos a través de su Ley Modelo 2.0 de Acceso a la Información Pública, "Al invocar la existencia de una causal de reserva ante una solicitud de Información, el sujeto obligado deberá aplicar la prueba del daño. La prueba de daño debe establecer que la divulgación de la Información solicitada puede generar un daño real, demostrable e identificable"[9]. La Ley establece además los criterios a seguir por el sujeto obligado para acreditar que el daño es mayor que el beneficio de su publicación.
40. Al resolver la solicitud administrativa que motiva esta acción, el Ministerio del Interior incluyó la información solicitada dentro de la excepción de reserva según las clasificación realizada en las Resoluciones 5905 y 5909 del año 2012.

---

[8] CAinfo, *Venciendo la Cultura del Secreto*, *Obstáculos en la implementación de políticas y normas de acceso a la información pública en siete países de América Latina,* p. 36. Recuperado de: http://www.cainfo.org.uy/images/LIBRO%20-%20Venciendo%20la%20Cultura%20del%20Secreto.pdf

[9] Ley Modelo Interamericana 2.0 sobre Acceso a la Información Pública, Artículo 35. Disponible en: https://www.oas.org/es/sla/ddi/docs/publicacion_Ley_Modelo_Interamericana_2_0_sobre_Acceso_Informacion_Publica.pdf

41. Esta Resolución, al igual que las dictadas en 2012, no cumple con los requisitos legales de proporcionalidad, prueba de daño y divisibilidad de la información, por lo cual se impone su revisión por el proceso judicial previsto en la ley.

42. La Resolución no realiza una prueba de daño, esto es, indicar de qué forma la publicación de la información ocasiona un daño mayor que el que se protege con la reserva. En este sentido, recaía sobre la institución el deber de acreditar que la publicación representaba un riesgo "real, demostrable e identificable de perjuicio significativo a un bien jurídico (...) que no hay un medio alternativo menos lesivo para el interés público de conocer la información (...) que la limitación se adecua al principio de proporcionalidad, que la restricción no atenta contra la esencia misma del derecho a la información"[10].

43. Como se desprende de la lectura de la solicitud, la información solicitada refiere a cuestiones administrativas que no podrían ocasionar un daño ni al Ministerio ni a los ciudadanos. Se trata de información acerca del cumplimiento del organismo sobre disposiciones legales, conocer si los sistemas se encuentran en funcionamiento e información sobre instancias de formación. ¿De qué manera puede afectar la seguridad pública conocer los datos del encargado de datos personales del Ministerio? ¿O conocer si se brindó capacitación a los funcionarios en la materia? ¿O si se realizó una evaluación de impacto legalmente requerida? A todas luces indica que no existen motivos legales válidos para restringir el acceso a la ciudadanía.

44. Esta parte se hace eco de los Considerandos presentes en la Resolución de la UAIP ante la petición administrativa:

> "X. que respecto a lo solicitado en los puntos 1, 2, 4 y 7, en general no se identifica el daño que podría causar a la seguridad pública brindar esta información al solicitante, por tanto, sería información pública;
>
> XI. que, no obstante, sobre los puntos 3 y 6, en ambos casos podría tratarse documentos cuyos contenidos podrían ser reservados en virtud de los dispuesto por el artículo 9° literal A, previa prueba de daño;

---

[10] Ley Modelo Interamericana 2.0 sobre Acceso a la Información Pública, Artículo 35. Disponible en: https://www.oas.org/es/sla/ddi/docs/publicacion_Ley_Modelo_Interamericana_2_0_sobre_Acceso_Informacion_Publica.pdf

XII. que lo anterior no debería impedir que el Ministerio informe a la solicitante si se ha realizado o no la evaluación de impacto, tal como lo establece la Ley N° 18.331;

XIII. que, sobre lo solicitado en los puntos 4 y 5 tampoco se identifica el daño que podría causar informar si ya se comenzó a utilizar y con qué alcance, tendiendo en cuenta que la prueba de daño debe concluir que el daño debe ser mayor al del interés público en conocer esa información;

XIV. que, por último, respecto a lo solicitado en los puntos, 8, 9 y 10, es claro que informar sobre si se requiere orden judicial, la cantidad de cursos que se han impartido a los funcionarios, así como lo criterios que son utilizados, no podría afectar la seguridad pública, por ende también es información pública y como tal debería ser brindada al solicitante".[11]

45. Es decir, la UAIP correctamente analiza para cada uno de los 10 puntos solicitados la posibilidad de que exista un daño que justifique la reserva dispuesta. Concluye que, excepto en los puntos 3 y 6 no es posible identificar un daño, e incluso en estos dos puntos el Ministerio debería informar si se realizó una evaluación de impacto de datos personales o no.
46. La respuesta a muchas de las preguntas planteadas pueden ser respondidas con un "sí" o "no", lo cual no requiere entrar en detalles que pudieran fundamentar la negación.
47. Las resoluciones genéricas dictadas por el Ministerio del Interior en el año 2012 no realizan prueba de daño requerida por mandato legal y ello le hace caer en una clasificación genérica que se aparta de la ley y los estándares que rigen el derecho de acceso a la información pública.

II) INTERÉS PÚBLICO DE LA INFORMACIÓN SOLICITADA

48. Como viene de verse, aún en caso de que existiera el daño, la administración no debe denegar el acceso a la información automáticamente. Por el contrario, debe procederse a evaluar si el interés del público por conocer la información supera el daño potencialmente causado y en tal caso proceder a hacer entrega. Pues bien,

[11] Resolución Nº 13 del 3 de junio 2022 del Consejo Ejecutivo de la Unidad de Acceso a la Información Pública. (Documento Letra "C").

nada de ello es evaluado por el Ministerio en su Resolución, transgrediendo una vez más el derecho fundamental.

49. Como ha expresado la Corte Interamericana de Derechos Humanos en el caso Claude Reyes: "para que las personas puedan ejercer el control democrático es esencial que el Estado garantice el acceso a la información de interés público bajo su control y se fomente una mayor participación de las personas en los intereses de la sociedad".[12]

50. Según la Organización de Estados Americanos, '"Información de interés público" se refiere a la Información que resulta relevante o beneficiosa para la sociedad y no simplemente de interés individual, cuya divulgación resulta útil para que el público comprenda las actividades que llevan a cabo los sujetos obligados, tales como Información referente a la salud pública, medio ambiente, **seguridad pública**, asuntos socioeconómicos y políticos y transparencia en la gestión pública. Esta definición retoma los elementos de la sentencia de la Corte Europea de Derechos Humanos en el caso SIOUTIS v. GREECE".[13]

51. La CIDH ha considerado de interés público "aquellas opiniones o informaciones sobre asuntos en los cuales la sociedad tiene un legítimo interés de mantenerse informada, de conocer lo que incide sobre el funcionamiento del Estado, o afecta derechos o intereses generales o le acarrea consecuencias importantes".[14] El derecho de acceso se fundamenta por la importancia del rol que desempeñan las autoridades públicas en una democracia constitucional, pues a partir de su trabajo de comunicación, la ciudadanía despierta un sentido crítico, se genera sus propias opiniones y participa en el debate público.

52. Existe información que puede ingresar a la categoría de seguridad nacional, pero está rodeada de un interés público superior de que se divulgue. En una sociedad democrática no toda información relacionada con seguridad pública puede ser objeto de una reserva, sino que se requiere para ello demostrar que la divulgación

---

[12] Corte IDH, *Caso Claude Reyes vs. Chile, (Fondo, Reparaciones y Costas),* Sentencia de 19 de septiembre de 2006, Serie C N° 151, párr. 87. En: https://www.corteidh.or.cr/docs/casos/articulos/seriec_151_esp.pdf

[13] Ley Modelo Interamericana 2.0 sobre Acceso a la Información Pública. Disponible en: https://www.oas.org/es/sla/ddi/docs/publicacion_Ley_Modelo_Interamericana_2_0_sobre_Acceso_Informacion_Publica.pdf

[14] Corte IDH, *Caso Fontevecchia y D'amico vs. Argentina, (Fondo, Reparaciones y Costas),* Sentencia de 29 de noviembre de 2011, Serie C No. 238, párr. 61. En: https://corteidh.or.cr/docs/casos/articulos/seriec_238_esp.pdf

puede generar un daño mayor a la seguridad que el interés público en la información.[15]

53. La información solicitada reviste un alto interés público, puesto que resulta imprescindible para que la sociedad en su conjunto pueda conocer las políticas públicas llevadas adelante por el Ministerio del Interior en un área sensible para el mantenimiento de la democracia como es la seguridad pública.

54. Se encuadra este pedido en el derecho fundamental del ciudadano a acceder a la información de interés público, entendido como el "interés de la ciudadanía por tomar parte en el quehacer de los asuntos públicos [lo que implica], entre otros aspectos, el fomento del debate público, de la transparencia en la actividad de los organismos del Estado, del control por parte de la ciudadanía respecto de tal actividad y, en general, de la participación ciudadana".[16]

55. El reto que enfrentan los gobiernos en la lucha contra el terrorismo y el crimen organizado, por un lado, y por otro, la irrupción de las nuevas tecnologías de la comunicación e información han creado un fuerte desafío en materia de derechos humanos en todo el mundo. La tecnología ha contribuido a garantizar la libertad de expresión y el acceso a la información, el conocimiento y la cultura en formas antes no concebidas. Sin embargo, tal como lo ha señalado recientemente el Alto Comisionado de las Naciones Unidas para los Derechos Humanos, "en la era digital, las tecnologías de la comunicación también han aumentado la capacidad de los gobiernos, las empresas y los particulares para realizar actividades de vigilancia, interceptación y recopilación de datos".[17]

56. Acerca de sus riesgos para los derechos humanos el Consejo de Derechos Humanos de Naciones Unidas ha establecido claramente: "El reconocimiento

---

[15] En este sentido, la Relatoría Especial para la Libertad de Expresión de la CIDH ha establecido: "El derecho de acceso a la información pública protege el derecho de toda persona a acceder a información en poder de las autoridades públicas, lo cual incluye la información que se relaciona con la seguridad nacional. Excepcionalmente, se podrá restringir el acceso a esta información con base en las excepciones claras y precisas establecidas en la ley, siempre que estas resulten necesarias en una sociedad democrática para salvaguardar intereses legítimos de la seguridad nacional. Los intereses de la seguridad nacional se ven favorecidos en la práctica cuando la sociedad está debidamente informada sobre las actividades del Estado, incluidas aquellas llevadas adelante para resguardar la seguridad nacional" *Derecho a la Información y Seguridad Nacional,* (2020), párr. 81, en: https://www.oas.org/es/cidh/expresion/informes/DerechoInformacionSeguridadNacional.pdf

[16] González, Felipe. *La libertad de expresión en el Sistema Interamericano de Derechos Humanos.* AA.VV. *Tendencias jurisprudenciales de la Corte Interamericana y el Tribunal Europeo de Derechos Humanos.* (2008). Tirant lo Blanch, Valencia. P. 253.

[17] Asamblea, G. *Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos.* A/HRC/27/37. 30 de junio de 2014. Párr. 2. En: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G14/068/74/PDF/G1406874.pdf?OpenElement

biométrico a distancia en tiempo real plantea graves preocupaciones en lo que respecta al derecho internacional de los derechos humanos, tal y como la Alta Comisionada ha destacado con anterioridad. Algunas de estas preocupaciones reflejan los problemas asociados a las herramientas de predicción, en particular la posibilidad de una identificación errónea de las personas y consecuencias desproporcionadas para los miembros de ciertos grupos. Además, la tecnología de reconocimiento facial puede utilizarse para elaborar perfiles de personas en función de su etnia, raza, origen nacional, sexo y otras características".[18]

57. En este sentido, su uso puede implicar graves riesgos para varios de los derechos consagrados internacionalmente en el marco jurídico. El Consejo de Derechos Humanos de Naciones Unidas ha señalado el impacto negativo de esta tecnología en el derecho a la privacidad, la libertad de expresión y la reunión pacífica: "El reconocimiento biométrico a distancia conlleva un grave riesgo de injerencia en el derecho a la privacidad. La información biométrica de una persona constituye uno de los atributos fundamentales de su personalidad, ya que revela características únicas que la distinguen de otras personas. Además, el reconocimiento biométrico a distancia aumenta considerablemente la capacidad de las autoridades del Estado de identificar y rastrear sistemáticamente a las personas en los espacios públicos, lo que socava la capacidad de estas de hacer su vida sin ser observadas y tiene un efecto negativo directo en el ejercicio de los derechos a la libertad de expresión, de reunión pacífica y de asociación, así como a la libertad de circulación". [19]

58. "La imagen de una persona constituye uno de los atributos fundamentales de su personalidad, ya que revela características únicas que la distinguen de otras. El hecho de grabar, analizar y conservar las imágenes faciales de alguien sin su consentimiento constituye una injerencia en el ejercicio del derecho a la vida privada. Al desplegar la tecnología de reconocimiento facial en las reuniones y manifestaciones, la injerencia adquiere una escala enorme e indiscriminada, ya que se requiere la recopilación y el procesamiento de imágenes faciales de todas las personas captadas por una cámara equipada con un sistema de tecnología de reconocimiento facial o conectada a un sistema de este tipo".[20]

---

[18] Asamblea, G. *Informe de la Alta Comisionada de las Naciones Unidas para los Derechos Humanos.* A/HRC/48/31. 13 de septiembre de 2021. Párr. 26.
[19] Ibídem, párr. 27.
[20] Asamblea, G. *Informe del Alto Comisionado de las Naciones Unidas para los Derechos Humanos.* A/HRC/44/24. 24 de junio de 2020. Párr. 33. En:

59. Además, la tecnología de reconocimiento facial puede perpetuar y amplificar la discriminación sobre grupos minoritarios o tradicionalmente excluidos como las personas afrodescendientes y personas con discapacidad. Esta tecnología puede ser utilizada para el perfilado de personas sobre la base de su etnia, raza, origen nacional, género y otras características generando muchas veces discriminaciones o sesgos involuntarios que en el ámbito de la seguridad pública puede tener importantes consecuencias.[21]

60. Frente a estos desafíos la comunidad internacional ha venido trabajando en los últimos años para promover una serie de estándares y principios que permitan la armonización de los diferentes derechos en juego y contribuya a resolver la tensión entre seguridad y acceso a la información, vigilancia y privacidad.

61. En 2013 con el apoyo de más 500 expertos internacionales se dieron a conocer los Principios globales sobre seguridad nacional y el derecho a la información ("Principios de Tshwane"). Estos Principios recogen los estándares emanados del derecho internacional de los derechos humanos y de las decisiones de los órganos jurisdiccionales y cuasi-jurisdiccionales en materia de derechos humanos, así como las mejores prácticas identificadas a nivel global. Tiene por fin orientar el diseño y la aplicación de los marcos jurídicos en materia de seguridad y acceso a la información pública en todo el mundo.[22] Los Principios han sido apoyados además por el Consejo de Europa[23] y la Comisión Interamericana de Derechos Humanos[24].

62. Conforme los Principios de Tshwane, "si bien a veces puede haber cierto grado de tensión entre el interés de un gobierno por preservar el carácter reservado de cierta información por razones de seguridad nacional y el derecho de la población a acceder a información en poder de autoridades públicas, un examen exhaustivo del pasado reciente indica que los intereses legítimos de seguridad nacional, en la

---

https://documents-dds-ny.un.org/doc/UNDOC/GEN/G20/154/38/PDF/G2015438.pdf?OpenElement

[21] Ibídem, párr. 32.

[22] Open Society Foundations; Open Society Justice Initiative. *Principios Globales sobre Seguridad Nacional y el Derecho a la Información "Principios de Tshwane".* (2013). Recuperado de: https://www.oas.org/es/sla/ddi/docs/acceso_informacion_Taller_Alto_Nivel_Paraguay_2018_documentos_referencia_Principios_Tshwane.pdf

[23] Resolución de la Asamblea Parlamentaria del Consejo de Europa, 2 de Octubre 2013.

[24] "El presente informe acoge expresamente estos principios, debido a su robusto proceso de construcción y en el entendido de que constituyen una herramienta clave para garantizar la instrumentación adecuada de los estándares interamericanos sobre el derecho a la información en la legislación y en las prácticas nacionales." RELE CIDH, Derecho a la Información y Seguridad Nacional, (2020), párr. 9, en: https://www.oas.org/es/cidh/expresion/informes/DerechoInformacionSeguridadNacional.pdf

práctica, se ven favorecidos cuando la sociedad está bien informada sobre las actividades del Estado, incluidas aquellas llevadas a cabo para resguardar la seguridad nacional. El acceso a la información, al facilitar el escrutinio público de los actos del Estado, no sólo previene abusos por parte de funcionarios públicos, sino que además permite que la población intervenga en la definición de las políticas del Estado y, por ende, constituye un elemento clave para la preservación efectiva de la seguridad nacional, la participación democrática y la formulación de políticas sólidas".[25]

63. De acuerdo con el Principio número 3, las restricciones al acceso a la información pública por razones de seguridad nacional deben estar establecidas por ley, deben referir a la protección de un interés legítimo de seguridad nacional y deben ser necesarias en el marco de una sociedad democrática. Este último requisito conlleva que: (i) La divulgación de la información debe representar un riesgo real e identificable de perjuicio significativo para un interés legítimo de seguridad nacional. (ii) El riesgo de perjuicio que supondría la divulgación debe superar al interés público de difundir la información. (iii) La limitación debe adecuarse al principio de proporcionalidad y representar el medio menos restrictivo disponible para evitar el perjuicio. (iv) La restricción no debe atentar contra la esencia misma del derecho a la información.[26]

64. En el caso de la información sobre Vigilancia, se establece claramente que esta se encuentra entre las categorías de información sobre las cuales existe una fuerte presunción o un interés preponderante a favor de su divulgación (Principio 10).[27] Así, conforme a estos estándares que cuentan con el más amplio respaldo de la comunidad internacional, el marco jurídico general en materia de vigilancia de todo tipo, así como los procedimientos a seguir para su autorización, la selección de los objetivos y el uso, intercambio, almacenamiento y destrucción del material interceptado, debería ser accesible para la sociedad.[28]

65. También la Relatoría Especial para la Libertad de Expresión de la CIDH ha establecido la fuerte presunción que existe sobre información sobre vigilancia estatal:

---

[25] Ibídem, p. 6.
[26] Ibídem, pp. 18-19.
[27] Ibídem, pp. 25-32.
[28] Ibídem, p. 30.

"Al tomar iniciativas para garantizar la seguridad nacional y prevenir o contrarrestar otras amenazas, resulta indispensable que el Estado **asegure que las personas puedan estar debidamente informadas como mínimo**, sobre el marco jurídico en materia de vigilancia y la **finalidad de la misma**, así como el marco regulatorio de programas de vigilancia; **los procedimientos a seguir para su autorización, la selección de objetivos y el uso o manejo de datos**; los protocolos de intercambio, almacenamiento y destrucción del material interceptado, así como con respecto a las entidades autorizadas para llevar a cabo acciones de vigilancia y las estadísticas relativas al uso estas acciones y los órganos encargados para implementar y supervisar dichos programas".[29] (Destacado propio)

66. En definitiva, como viene de verse el uso de herramientas de RFA aumenta de manera exponencial la capacidad de vigilancia del Estado sobre las personas lo que demanda una mayor transparencia en su uso y aplicación.

67. Considerando la amplia red de cámaras desplegadas en la vía pública por todo el país y la base de datos centralizada de la Dirección Nacional de Identificación Civil con información de todas las personas residentes en el país, las posibilidades de identificar a una persona en cualquier momento y en cualquier lugar. Este poder supone un incremento notable en las capacidades de control y vigilancia por parte de las autoridades que antes no tenían.

68. Este aumento no puede pasar por fuera del escrutinio público teniendo en cuenta los riesgos que supone para los derechos humanos como viene de referirse, de acuerdo al Consejo de Derechos Humanos de Naciones Unidas y expertos internacionales en derechos humanos. El pleno ejercicio, sin intromisiones abusivas en derechos como la privacidad, la libertad de expresión y la reunión pacífica resultan fundamentales para el mantenimiento de un Estado democrático.

69. Es por ello que se impone contar con información sobre cómo y de qué manera se lleva adelante el control sobre las personas la máxima autoridad en la materia. Respecto a la transparencia sobre el uso de los sistemas de RFA, el Consejo de Derechos Humanos de Naciones Unidas ha dicho: "En todas las circunstancias, las autoridades deben ser transparentes en cuanto al uso de la tecnología de grabación y reconocimiento facial y notificar siempre a los ciudadanos cuándo

[29] Relatoría Especial para la Libertad de Expresión, Comisión Interamericana de Derechos Humanos, *Derecho a la Información y Seguridad Nacional,* (2020). Párr. 117.

están siendo grabados y puedan ser grabados y/o que sus imágenes podrían ser procesadas en un sistema de reconocimiento facial".[30]

70. En el mismo sentido se ha expresado la Asamblea Global de Privacidad de la cual forma parte Uruguay desde el año 2009 a través de la Unidad Reguladora y de Control de Datos Personales.[31] En su Resolución sobre Tecnología de Reconocimiento Facial de Octubre de 2020, la Asamblea reiteró la importancia de:

"Los principios de necesidad y proporcionalidad, que garantizan que la tecnología de reconocimiento facial sólo se utilice cuando el propósito no pueda lograrse por medios menos intrusivos;

La transparencia y la rendición de cuentas responsable [y demostrable] sobre el uso y la gestión de datos personales en las aplicaciones de reconocimiento facial, y los derechos aplicables a las personas, incluyendo el suministro de la tecnología a los organismos encargados de hacer cumplir la ley y su utilización por dichos organismos".[32]

71. Como se puede apreciar, lejos se encuentra la implementación de Reconocimiento Facial de ser un tema saldado y exento de controversia. Los debates acerca de la legitimidad, conveniencia y eficacia sobre esta tecnología por parte de los gobiernos se encuentra en discusión en todo el mundo.

72. A modo de ejemplo, el 12 de abril de 2022 un juez de la ciudad de Buenos Aires ordenó, mediante medida cautelar, la suspensión del sistema de reconocimiento facial de prófugos. Por otro lado, el 22 de marzo del mismo año una jueza en São Paulo ordenó a la Compañía Metropolitana de São Paulo suspender el sistema de monitoreo electrónico del metro de la ciudad. Esta medida implica la suspensión de la captura y tratamiento de datos biométricos, de la instalación de nuevos equipos, y la imposición de una multa diaria en caso de incumplimiento.[33]

---

[30] Asamblea, G. *Informe del Alto Comisionado de las Naciones Unidas para los Derechos Humanos.* A/HRC/44/24. 24 de junio de 2020. Párr. 37.

[31] Lista de miembros acreditados de la Asamblea de Privacidad Global. Recuperado de: https://globalprivacyassembly.org/participation-in-the-assembly/list-of-accredited-members/

[32] 42° Asamblea Global de Privacidad. *Resolución adoptada sobre la tecnología de reconocimiento facial.* (2020). P. 3. Recuperado de: https://globalprivacyassembly.org/wp-content/uploads/2020/10/FINAL-GPA-Resolution-on-Facial-Recognition-Technology-ES.pdf

[33] Arroyo, Verónica. (20 de abril de 2022). *Buenos Aires y São Paulo suspenden el reconocimiento facial, ¿qué espera al resto de América Latina?* [Publicación en blog]. Recuperado de: https://www.accessnow.org/buenos-aires-y-sao-paulo-suspenden-reconocimiento-facial/

73. Como viene de verse, la solicitud que aquí se entabla pretende acceder a información que reviste alto interés para el ejercicio de los derechos humanos en Uruguay. Sin acceso a esta información no es posible saber si se respetan los derechos a la protección de datos de las personas ni qué medidas ha adoptado el Ministerio para proteger las bases de datos.

74. Además, el uso de datos personales por parte del Ministerio del Interior, y específicamente sobre las bases de la Dirección Nacional de Identificación Civil se han encontrado en la agenda pública del país.

75. Este interés por parte de gobernantes y gobernados puede ser corroborado con los debates que la cuestión ha suscitado en el Parlamento Nacional con motivo de la aprobación de la rendición de cuentas donde se incluyeron los Artículos 191 y 192 antes mencionados. Según trascendió en varios medios de prensa, los intercambios entre legisladores del gobierno y oposición apuntaban hacia la legalidad del sistema a utilizar.

76. Así en nota publicada por El País el 24 de noviembre de 2020:

> "Los senadores de la coalición multicolor aprobaron ayer en comisión la creación de la base de datos para reconocimiento facial y el pasaje de los datos personales desde la Dirección Nacional de Identificación Civil (DNIC) a la Secretaría General del Ministerio del Interior. Con estos artículos del Presupuesto, el 178 y el 179, el oficialismo le da un marco legal al nuevo sistema de control y seguridad pública que fue diseñado por el anterior gobierno. Por su parte, los legisladores del FA advierten que este cambio "no es legal sin la autorización de cada titular de la imagen" y buscan una nueva fórmula para acordar con el oficialismo". (Documento Letra F)

77. La seguridad de las bases de datos de la Dirección Nacional de Identificación Civil ha estado en el centro de debates públicos en los últimos tiempos. Según trascendidos de prensa, en el año 2020 la DNIC fue víctima de un hackeo que comprometió la información de, al menos, 84.000 pasaportes electrónicos. La dirección del organismo lo reconoció con un comunicado donde declaró: "Informamos que el 8 de diciembre la DNIC detectó un incidente de ciberseguridad que se contuvo y por el que se desplegaron medidas técnicas, operativas y administrativas para contrarrestar el evento con expertos en la materia, tanto del

Ministerio del Interior como del Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CertUy)".[34]

78. Por otra parte, el reciente caso sobre la emisión de pasaportes uruguayos para personas de nacionalidad rusa que involucró personal de Presidencia de la República también involucró el uso ilegítimo de las bases de datos de la DNIC según ha sido publicado por los principales medios del país.

79. En este mismo caso, según ha reportado la prensa se investiga el uso que realizaba el encargado de Seguridad Presidencial de las cámaras de la vía pública del Ministerio del Interior desde el edificio de Presidencia. (Documentos Letras K y L).

80. Resulta por tanto información de interés público para el debate acerca de la implementación de esta tecnología y las seguridades asociadas a la protección de los derechos de las personas. Contar con información como la que se solicita y a la cual se tiene derecho de acuerdo al marco legal, contribuiría sustancialmente a la mejora en el debate público y control sobre las acciones de los gobernantes.

III) ACERCA DE LAS RESOLUCIONES 5905 Y 5909

81. La Resolución recaída en el expediente administrativo de solicitud no hace lugar a la entrega fundándose en las Resoluciones Números 5905 y 5909 del 25 y 30 de julio de 2012 (Considerandos VI y VII).

82. Estas Resoluciones forman parte de un conjunto de actos administrativos dictados por el Ministerio del Interior en el año 2012. En aquél año, la Secretaría de Estado dictó 8 resoluciones en la que se reservan genéricamente todo tipo de datos referentes al organismo.

83. Estas Resoluciones, incluyendo las números 5905 y 5909, no fueron dictadas de acuerdo a la Ley Nº 18.381 y su Decreto Reglamentario.

84. En este sentido, las resoluciones fueron objeto del Dictamen No 17/2013 de la UAIP del 20 de diciembre de 2013. La UAIP, órgano rector en la materia, observó que la clasificación genérica de información realizada por el Ministerio resulta ilegal. El dictamen, que acompaña este escrito, señala:

---

[34] LaRed21. *Dirección de Identificación Civil reconoce que detectó incidente de ciberseguridad.* Disponible en nota adjunta.

"(...) III) que con relación a la información reservada, esta Unidad ha entendido que la clasificación se deberá realizar por el sujeto obligado en forma particular, identificando en cada caso la información a reservar y la causa legal de reserva al amparo de lo dispuesto por el artículo 9 de la norma antes referida; [35]

IV) que dicha exigencia se sustenta en lo dispuesto por el artículo 25 del Decreto reglamentario N° 232/2010 de 2 de agosto de 2010, que requiere que toda clasificación de información reservada debe estar precedida y justificada en una "prueba de daño", tendiente a demostrar con elementos objetivos, el daño efectivo al interés tutelado que sería causado en caso de publicitarse la misma;

V) **que, por ende, las resoluciones analizadas no constituyen actos de clasificación propiamente dichos debido a su generalidad**, sin perjuicio de lo cual podrán oficiar como matriz de criterios para proceder a clasificar la información en cada caso concreto". (Destacado nuestro)

85. En la parte final del informe, la UAIP insta al Ministerio del Interior a adecuar la clasificación realizada a lo establecido en la LDAIP y su decreto reglamentario.

86. La UAIP señaló este punto en la Resolución dictada ante la denuncia de la compareciente por el presente caso. El Numeral V de los Considerandos de la Resolución señala que las prácticas del Ministerio del Interior no se ajustan a la Ley Nº 18.381: "además, se menciona como fundamento la resolución genérica No 5909 de 2012, y esta Unidad ya se ha pronunciado en varias oportunidades, señalándole al Ministerio que las resoluciones genéricas solo pueden servir como una matriz de criterios, pero no como fundamento legal para reservar información pública".

87. La doctrina se ha pronunciado en igual sentido. Al comentar una acción de solicitud contra el Ministerio del Interior fundamentada en las mismas resoluciones, Thomasset Loureiro afirmó: "Puede apreciarse que se trata de reservas genéricas, lo cual no se ajusta a lo requerido en la Ley Nº 18.381, norma

[35] Dictamen N° 02/2011 de 12 de mayo de 2011.

que exige fundamentaciones concretas para cada caso en particular, así como observar criterios tales como la prueba o balance de daño".[36]

88. Bazán y Pérez, al comentar las resoluciones afirmaron: "Evidentemente, en la clasificación efectuada no hubo una interpretación estricta, sino que genéricamente se clasificó toda la información relativa a los cometidos del organismo y no se fundamentó el por qué, siendo totalmente arbitraria y contraria a los preceptos reglamentarios, legales y constitucionales".[37]

89. Como se puede apreciar, luego de casi diez años, la justificación del Ministerio del Interior en Resoluciones no ajustadas a derecho se mantiene. El dictamen del órgano legalmente competente y rector en la materia de acceso ha sido desatendido por las sucesivas autoridades ministeriales que han continuado apelando a dichas resoluciones ante diversas solicitudes administrativas y judiciales.

90. En el mismo sentido, el Dr. Gabriel Delpiazzo, Ex-Presidente de la UAIP, actual integrante del Consejo Consultivo de la Unidad por la Universidad de la República y reconocido profesor especialista en la materia, manifestó en una entrevista brindada al Semanario Brecha en 2022: "Discrepamos con los criterios con los que el Ministerio del Interior clasifica la información"[38] haciendo directa referencia al criterio ilegal de clasificación de información del Ministerio.

91. Esta política de clasificación genérica de información llevada adelante por el Ministerio del Interior en las sucesivas administraciones también ha sido denunciada desde la sociedad civil organizada como un obstáculo para el monitoreo social de la política pública sobre seguridad y en general, por su apartamiento de los estándares en materia de acceso a la información pública. Esta situación genera cada vez más preocupación, puesto que pese a no contar con un marco normativo robusto en materia de seguridad nacional que permita armonizar distintos derechos, el país ha avanzado en técnicas de vigilancia por medio de nuevas tecnologías como la videovigilancia, compra de drones para el Ministerio del Interior y avanzados sistemas de escuchas telefónicas.

---

[36] Thomasset, Martín. *Transparencia y democracia: el acceso a la información pública*. (2016). FCU, Montevideo.

[37] Bazán, Pablo; Pérez, Maida. *Límites al acceso a la información pública en Seguridad Pública: Nota de Administración.* Pp.155-168.
Schiavi, Pablo, coord. *Estudios de información pública y datos personales: recopilación de trabajos de investigación de los cursos de postgrado 2012-2013.* [T.1] Universidad de Montevideo.

[38] Delpiazzo, Gabriel. Brecha. [Robaina, Mónica]. *Discrepamos con los criterios con los que el Ministerio del Interior clasifica la información.*

92. Por todo ello que se impone revisar por una autoridad judicial independiente la legalidad de los actos y desestimar la negativa de acceso, brindando a esta parte la información solicitada.

IV) INOPONIBILIDAD DE EXCEPCIONES SOBRE VIOLACIONES A DERECHOS HUMANOS

93. La Ley de Acceso a la Información Pública en su Artículo 12 prevé la inoponibilidad de excepciones en casos de violaciones a los derechos humanos:

    "Los sujetos obligados por esta ley no podrán invocar ninguna de las reservas mencionadas en los artículos que anteceden cuando la información solicitada se refiera a violaciones de derechos humanos o sea relevante para investigar, prevenir o evitar violaciones de los mismos''.

94. El derecho a la protección de datos personales se encuentra consagrado en nuestro ordenamiento como un derecho fundamental inherente a la persona humana (Artículo 72 de la Constitución). Desde el año 2008 se cuenta además con una ley específica en la protección de este derecho (Ley Nº 18.331).
95. Por lo tanto, teniendo en cuenta el derecho fundamental afectado y el despliegue de esta tecnología, la información solicitada resulta de relevancia para la investigación sobre el derecho a la protección de datos personales de todas las personas que se mueven por la vía pública en el país. Las brechas de seguridad reportadas sobre los datos que maneja el Ministerio del Interior hacen suponer que también resultan relevantes para la prevención y control sobre las violaciones de este derecho fundamental.
96. Resulta inoponible por tanto la excepción esgrimida por el Ministerio del Interior, en virtud del artículo 12 de la Ley de Acceso a la Información Pública.

V) OBLIGACIÓN DE NO PRODUCIR INFORMACIÓN

97. La Resolución por la cual el Ministerio del Interior denegó el acceso también incluye dentro de sus considerandos el límite establecido en el Artículo 14 de la citada Ley Nº 18.381 que refiere a la no obligación de crear o producir información, o de realizar evaluaciones o análisis (Considerando V).
98. Sin embargo, el Ministerio no aclara cuál o cuáles de los puntos que se solicitaron podrían encontrarse en esta situación. La remisión genérica a este límite al

derecho de acceso no impide que la autoridad administrativa detalle cuál es la información con la que no cuenta. Así lo ha entendido la Suprema Corte de Justicia: “no puede obviarse que el art. 14 inciso 1o de la ley nro. 18.381 puede ser una tentadora vía de escape o salvoconducto de la Administración para evitar proporcionar información de interés público; de ahí que su interpretación debe ser estricta, y de aplicarse, debe estar adecuadamente motivada”.[39]

99. Por otra parte, el Artículo 14 al que hace referencia el Considerando de la Resolución del Ministerio expresamente prevé el límite al uso de esta excepción cuando los organismos tienen la obligación de contar con la información al momento de efectuarse el pedido. La UAIP indica: “en el artículo 14 si bien se indica que el organismo no está obligado a producir información de la que no dispone, también señala que hay información que sí debe tener el organismo cuando es parte de sus cometidos” (Numeral VI de la Resolución Nº 13/2022). Por tanto hay información que sí debe tener el organismo cuando es parte de sus cometidos.

100. La información solicitada refiere a documentación e información que obviamente está en posesión de la demandada o que al menos debería tener por haberla producido de acuerdo al mandato legal. En este sentido, el Artículo 191 de la Ley No 19.924 crea la base de datos de reconocimiento facial, en estricto cumplimiento de los cometidos asignados al Ministerio por la Ley No 19.315, de 18 de febrero de 2015, y a lo dispuesto en la Ley No 18.331, de 11 de agosto de 2008.

101. Como indicó la UAIP en su Resolución sobre el caso de autos (Considerando VII), lo solicitado en los Puntos 1, 2, 3 y 7 refiere a obligaciones impuestas a los organismos que almacenan y tratan datos personales, por tanto, es un derecho de las personas conocer cómo se cumple con estas obligaciones por parte del Ministerio. Específicamente repasamos de dónde surge cada una de estas obligaciones:

- Punto 1 (Inscribir Base de Datos de Reconocimiento Facial): Artículo 29 Ley Nº 18.331
- Punto 2 (Designar Delegado de protección de datos): Artículo 40 Ley Nº 19.670 y Artículo 10 del Decreto Nº 64/2020.

[39] Suprema Corte de Justicia, Sentencia Nº 405/2022.

- Punto 3 (Realizar Evaluación de Impacto): Artículos 12 y 18 BIS Ley Nº 18.331 y Artículo 6 Decreto Nº 64/2020.
- Punto 7 (Definición de roles de acceso): "Política de Seguridad de la Información para Organismos de la Administración Pública" obligatoria para el Ministerio del Interior según lo dispuesto por el Decreto Nº 452/2009.

102. El Ministerio del Interior no se encuentra exento de las obligaciones establecidas en la Ley Nº 18.331 de Protección de Datos.

103. Como parte de la investigación realizada por Datysoc en el uso del reconocimiento facial por el Ministerio, se solicitó una entrevista con la Unidad Reguladora y de Control de Datos Personales (URCDP), el órgano encargado del cumplimiento de la Ley Nº 18.331. Acompaña este escrito la respuesta brindada por el organismo (Documento Letra E) a las diferentes preguntas realizadas acerca de las obligaciones de la cartera de gobierno sobre la protección de datos.

104. Respecto a la obligación del Ministerio del Interior de cumplir con la normativa, la URCDP manifestó:

> “Con carácter general, de acuerdo con el artículo 3° literal b) de la Ley N° 18.331 de 11 de agosto de 2008, las bases de datos que tienen como objeto la seguridad pública se encuentran excepcionadas de la aplicación de esta normativa. En el caso del Ministerio del Interior por tanto, aquellas bases de datos que tengan esta finalidad, no están alcanzadas por las obligaciones que establece esta normativa.
>
> No obstante, cabe indicar que, aun en los casos indicados en el párrafo anterior, se ha interpretado por parte de la URCDP que igualmente resultan aplicable con carácter general los principios de la protección de datos personales. (...)
>
> Además, en el caso concreto esta norma indica que el tratamiento de datos personales con fines de seguridad pública, sin previo consentimiento de los titulares, queda limitado a aquellos supuestos y categorías de datos que resulten necesarios para el estricto cumplimiento de las misiones legalmente asignadas a aquéllos para la seguridad pública.”

105. Siendo clara en el alcance de la responsabilidad proactiva del Ministerio, la URCDP declaró:

"[E]l Ministerio del Interior debe adaptar su actividad a las nuevas regulaciones de protección de datos personales **procediendo a designar el delegado de protección de datos, realizar si corresponde las respectivas evaluaciones de impacto, adoptar medidas de privacidad por diseño y por defecto, así como toda otra obligación que se desarrolle en aplicación del principio de responsabilidad proactiva** de las disposiciones indicadas en la pregunta". (Destacado propio)

106. La URCDP también destaca la excepcionalidad de las bases que no se encuentran sujetas a la Ley Nº 18.331 por motivos de "seguridad pública": "el concepto de seguridad pública queda limitado a aquellos supuestos y categorías de datos que resulten necesarios para el estricto cumplimiento de las misiones legalmente asignadas. Por tanto, se debe estar a este **criterio restrictivo** para identificar cuáles bases de datos quedan excepcionadas". (Destacado propio)

107. En el mismo sentido se pronuncia la doctrina nacional. Como indica Durán Martínez: "el hecho de que los casos indicados queden exceptuados de la aplicación de la ley no significa que se estén creando islas de irresponsabilidad. El régimen de la responsabilidad no se ve alterado, por lo que continúa rigiéndose por las normas generales".[40]

108. Como también expresa Santos refiriéndose al uso de datos biométricos por parte del Ministerio del Interior: "los datos recolectados deben ser los mínimos necesarios para el cumplimiento de la finalidad informada y no emplearse para fines distintos o incompatibles con aquellos que motivaron su recolección. Resultando de menester adoptar medidas para garantizar la seguridad y confidencialidad de los datos y otras medidas técnicas y organizativas comprobables para garantizar un tratamiento acorde a la legislación vigente".[41]

109. Continúa Santos: "si bien el tratamiento de datos personales con fines de seguridad pública sin el previo consentimiento de sus titulares por parte de Organismos Policiales está autorizado por el art. 25 de la LPDP, su inciso final establece que las bases de datos en tales casos "deberán ser específicas y

---

[40] Santos, Yessica. (Junio 2022). Reconocimiento facial con fines de Seguridad Pública en Uruguay. Revista de Derecho Público. Año 31. Número 60. P.120. Recuperado de: http://www.revistaderechopublico.com.uy/ojs/index.php/Rdp/article/view/170/152

[41] Ibídem.

establecidas al efecto", en especial cuando nos encontramos ante datos sensibles como son los datos biométricos".[42]

110. En definitiva, el Ministerio del Interior se encuentra obligado a contar con la información solicitada puesto que ello resulta de diversas normas legales que resultan obligatorias para esta cartera. La justificación en el Artículo 14 resulta por fuera de derecho y no puede de ninguna manera dar lugar a un escape a la producción de información con la cual la administración debe contar.

V) INFORMACIÓN REFERIDA A DATOS PERSONALES

111. La Resolución también incluye dentro de sus fundamentos de denegatoria aquella que se encuentra protegida por la Ley Nº 18.331 de Protección de Datos Personales (Considerando V).

112. Nuevamente el Ministerio apela a una remisión genérica a la norma sin especificar cuál o cuáles de los puntos solicitados se encuentran dentro de este límite.

113. La información que podemos suponer que implica datos personales podría ser la solicitada en el Punto 2 del Delegado de Protección de Datos del Ministerio. Sin embargo, como viene de decirse se trata de un cargo que debe ser designado por disposición legal y de función pública por lo que mal puede ampararse en la Ley 18.331 que es la misma que impone la obligación de comunicar quién ejerce este cargo. El motivo y rol del delegado es que las personas cuenten con un punto de contacto dentro de la organización que maneja sus datos personales por lo cual resulta inherente a su función ser publicado y de fácil acceso.

114. El resto de la información solicitada no contiene, por su propia naturaleza, datos que puedan ser catalogados como personales. Y aún en el caso de que los contuviera, el Ministerio debería proceder bajo el principio de divisibilidad y discriminar, manteniendo la publicidad como la regla y exceptuando aquella que no puede ser entregada por motivos de secreto.

115. El Artículo 7 del Decreto 232/2010 establece que si un documento tiene algunas secciones que pueden publicitarse y otras que no, se debe dar acceso a las primeras, mediante la realización de versiones públicas que disocien los datos personales.[43]

116. Como ha expresado la Relatoría Especial para la Libertad de Expresión: "En función del principio de máxima divulgación, cuando un registro contenga

[42] Ibídem, p. 122.
[43] Dictamen Nº 10 del 23 de agosto de 2013 de la Unidad de Acceso a la Información Pública.

información exenta y no exenta, las excepciones a la divulgación se aplican únicamente a la información específica protegida por la excepción y no a la totalidad del documento. En este caso, solamente podrá negarse la divulgación de la información específica cuando se haya demostrado la validez de la restricción para cada sección cuya publicidad se pretende impedir".[44]

117. En definitiva, si el Ministerio del Interior pretendía denegar información por vulnerar datos personales debería haber aclarado cuáles de los ítems solicitados hacía referencia y hacer entrega de la información aplicando el criterio de la divisibilidad.

CONCLUSIÓN

118. El Ministerio del Interior denegó el acceso a información de alto interés público utilizando una resolución de reserva que contraviene la normativa de acceso a la información pública. Tanto la Resolución recaída en el expediente de solicitud como las Resoluciones dictadas en el año 2012, no se ajustan a derecho por ser genéricas, no realizar prueba de daño, denegar información de interés público y no aplicar el criterio de divisibilidad de la información.

119. En definitiva, por los fundamentos expuestos corresponde al interés y derecho de esta parte acceder a la información solicitada en el Numeral 4 de este escrito.

PRUEBA

Solicita se agreguen conforme al artículo 170.1 del Código General del Proceso, los siguientes documentos:

A. Copia de la solicitud administrativa realizada a través del Sistema de Acceso a la Información Pública el 2 de noviembre de 2021.
B. Copia de la Resolución del 2 de diciembre 2021 del Ministerio del Interior en Expediente Nº 2021-4-1-0007031.
C. Copia de la Resolución Nº 13 del 3 de junio 2022 del Consejo Ejecutivo de la Unidad de Acceso a la Información Pública.
D. Copia de las Resoluciones Nº 5902, 5903, 5905, 5906, 5907, 5908, 5909 del año 2012 del Ministerio del Interior.

---

[44] Relatoría Especial para la Libertad de Expresión, Comisión Interamericana de Derechos Humanos, *Derecho a la Información y Seguridad Nacional,* (2020). Párr. 129.

E. Entrevista por Escrito de Datysoc con la Unidad Reguladora y de Control de Datos Personales.
F. Copia de la nota “Base de datos personales va al Ministerio del Interior para identificación facial”, publicada en el diario El País el 24 de Noviembre de 2020. Disponible en: https://www.elpais.com.uy/informacion/politica/base-datos-personales-ministerio-interior-identificacion-facial.html
G. Copia de nota periodística “Hackeo a Identificación Civil afectó datos de 84.000 pasaportes; autoridades desconocen alcance real del ataque” de El Observador del 9 de julio de 2022. Disponible en: https://www.elobservador.com.uy/nota/hackeo-a-identificacion-civil-afecto-a-84-000-personas-y-autoridades-desconocen-alcance-real-del-ataque-202279162616
H. Copia de la entrevista periodística Brecha a Gabriel Delpiazzo.
I. Llamado a Licitación Pública Nº 13/2019 y Acta del 14 de Febrero de 2020 para la adquisición de una Plataforma de Identificación Facial y servicio técnico de soporte, corrección, actualización y mantenimiento local y del/los fabricante/s por el periodo de 3 años para toda la solución. Disponible en: https://www.comprasestatales.gub.uy/consultas/detalle/id/744940
J. Copia de la nota “Dirección de Identificación Civil reconoce que detectó incidente de ciberseguridad” del medio La Red 21 publicada el 13 de febrero de 2021, Disponible en: https://www.lr21.com.uy/comunidad/1441771-direccion-de-identificacion-civil-reconoce-que-detecto-incidente-de-ciberseguridad
K. Copia de la nota “Investigan el uso que hacía Astesiano de las cámaras del Ministerio del Interior desde Presidencia” del medio El Observador publicada el 4 de noviembre de 2022, Disponible en: https://www.elobservador.com.uy/nota/investigan-el-uso-que-hacia-astesiano-de-las-camaras-del-ministerio-del-interior-desde-presidencia-202211316480
L. Copia de la nota “Astesiano tenía capturas de las cámaras de videovigilancia del MI y legajos policiales reservados en su oficina de la Torre Ejecutiva” del medio La Diaria publicada el 4 de noviembre de 2022. Disponible en: https://ladiaria.com.uy/justicia/articulo/2022/11/astesiano-tenia-capturas-de-las-camaras-de-videovigilancia-del-mi-y-legajos-policiales-reservados-en-su-oficina-de-la-torre-ejecutiva/

DERECHO

La compareciente funda su derecho en lo establecido en la Constitución de la república artículos 7, 29, 72, 82 y 332; Pacto Internacional de Derechos Civiles y Políticos Arts. 2, 19 y 25 (Ley Nº 13.751); Convención Americana sobre Derechos Humanos, Arts.1, 2, 13 y 25 (Ley Nº 15.737); Código General del Proceso, Ley Nº 18.381, su Decreto Reglamentario Nº 232/10, Ley Nº 18.331, normas concordantes y complementarias.

PETITORIO

Por lo expuesto al Sr. Juez PIDE:

1) Se la tenga por presentada con los recaudos adjuntos, por denunciado el domicilio real y constituido el procesal electrónico, así como interpuesta la acción de acceso a la información pública.

2) Se dé traslado de la demanda y se convoque a audiencia dentro del plazo de tres días de la fecha de presentación de la demanda.

3) En definitiva, se haga lugar a esta acción de acceso a la información pública ordenando al Ministerio del Interior la entrega de la información solicitada, fijando un plazo perentorio para hacerlo.

PRIMER OTROSI DICE: Que atento a lo dispuesto por el Artículo 44 del Código General del Proceso, Patricia Díaz confiere representación procesal al Dr. Matías Jackson, manifestando haber sido debidamente instruida de su alcance y que su domicilio real es el denunciado en la comparecencia.

SEGUNDO OTROSI DICE: que a los efectos de los dispuesto por los Artículos 85, 90, 105, 106 y 107 de la ley 15.982, así como el retiro de oficios, desgloses, ejemplares del edicto, testimonio y demás autoriza indistintamente al profesional firmante, a la Dra. [redacted], al Dr. [redacted] y la Sra. [redacted].