OBJETO: PROMOVER ACCIÓN JUDICIAL DE AMPARO DE ACCESO A LA INFORMACIÓN PÚBLICA

Señor/a Juez de Primera Instancia:

MARICARMEN SEQUERA BUZARQUIS, por mi propio derecho, con domicilio real en la calle 15 de agosto número 823 de la ciudad de Asunción, y constituyendo el procesal en Olegario Andrade 3245 casi Escurra de la Ciudad de Asunción, bajo patrocinio de los abogados **FEDERICO LEGAL AGUILAR**, con Mat. 29.503 y **EZEQUIEL FRANCISCO SANTAGADA**, con Mat. N° 16.716, ante Usía respetuosamente digo:

OBJETO. Que, de acuerdo con los Art. 28, 38 y 134 de la Constitución de la República, los Art. 13 y 25 de la Convención Americana sobre Derechos Humanos (Ley 1/89), así como en los términos del Art. 23 de la ley 5.282, y normas concordantes del Código Procesal Civil (Art. 565 y ss.), y conforme con lo dispuesto en la Acordada 1.005 del 21 de septiembre de 2015 de la Corte Suprema de Justicia, **vengo a interponer acción judicial de amparo de acceso a la información contra el Ministerio del Interior** (en adelante, "MDI"), con domicilio legal en la calle Chile 1002 esquina Manduvirá de la ciudad de Asunción, de conformidad con el siguiente relato que pasaré a exponer.

HECHOS. El día 8 de abril de 2019 ingresé una solicitud de acceso a la información pública mediante el Portal Unificado de Información Pública[1] (en adelante, "Portal Unificado", creado por Decreto 4.064/15), consignada como **Solicitud #19983** (en adelante, "solicitud AIP") bajo el título "**Cámaras de videovigilancia – Biometría**"[2], dirigida al MDI. En este sentido, en el escrito de la solicitud señalé que de acuerdo con noticias que fueron publicadas en distintos medios de masiva circulación y portales oficiales, la Policía Nacional y el Ministerio del Interior pusieron en marcha en julio de 2018 una serie de iniciativas del sistema 911 con el objeto de implementar una "tecnología biométrica" o de "reconocimiento facial" en las calles de Asunción y zonas del Área Metropolitana. En este sentido, a raíz del evidente interés público de la noticia, solicité al MDI, con base en la ley 5.282 y sus normas reglamentarias, lo siguiente (la cursiva, negrita y subrayado me pertenece):

---

1 El Portal Unificado se encuentra en el siguiente link: https://informacionpublica.paraguay.gov.py

2 El pedido de información puede verse en: https://informacionpublica.paraguay.gov.py/portal/#!/ciudadano/solicitud/19983

*1. Detallar el **sistema de tecnología biométrica que se encuentra implementando el Ministerio del Interior y la Policía Nacional desde Julio del año pasado**. Adjuntar la **copia de las resoluciones que detallen el tipo de tecnología que son utilizados para el sistema de reconocimiento facial**, u otro documento oficial que describa la tecnología y su funcionamiento.*
*2. Informar sobre los **detalles de implementación, protocolos y cualquier tipo de tratamientos de datos personales de las personas que son utilizados en el sistema de reconocimiento facial**.*
*3. Brindar un **mapa detallado con la ubicación de las cámaras de seguridad del sistema 911 y con que incluyen el sistema de identificación biométrica (reconocimiento facial)**.*
*4. Facilitar **información sobre los puntos futuros a nivel nacional y en los cuáles será ampliado el sistema de tecnología biométrica**.*
En el punto mencionado ut supra, vinculados al tratamiento de datos personales por parte del Ministerio del Interior, se solicita en detalle los siguientes puntos:
*a) ¿Cual es el **fin por el cual está siendo implementado el sistema de identificación biométrica**?*
*b) ¿Qué **datos personales están siendo recolectados, procesados y almacenados**?*
*c) ¿Qué **dependencia del Ministerio del Interior y/o Policía Nacional, se encarga de la administración de esa base de datos de identificación de las personas que transitan por las zonas de vigilancia con reconocimiento facial**?*
*d) ¿Qué otras **instituciones del Estado acceden a la base de datos de información personal y cómo**?*
*e) ¿**Qué empresas acceden a esta base de datos y cómo**?*
*f) Informar sobre las **condiciones y términos de uso de software (licencia) del sistema de biometría de reconocimiento facial**.*
*g) ¿**Se llevaron a cabo análisis sobre el impacto en la protección de datos personales y/o derechos humanos respecto al uso del sistema biométricos en las calles de Asunción y áreas metropolitanas**? En caso que la respuesta sea afirmativa, detallar la metodología seguida en el proceso. En caso que no haya realizado, explicar los motivos de la decisión.*
*h) **A qué base de datos biométricos accede la dependencia encargada del Ministerio del Interior, para cruzar los rostros capturados para el funcionamiento del sistema de reconocimiento facial**?*
*i) ¿**Cómo se evaluaron las tasas de error del algoritmo que utiliza el software de reconocimiento facial**? ¿**Cuál es la tasa de rechazo falso y la tasa de aceptación falsa que implementa dicho software**?*

*j) ¿**Se desarrollaron medidas y protocolos para la rendición de cuentas sobre el uso de sistemas de identificación de datos personales en el sistema de vigilancia biométrica**? En caso de existir, adjuntar una copia. En caso de que no exista, explicar los motivos. Y detallar los procesos que plantea efectuar la supervisión sobre el uso del sistema de identificación biométrica para evitar riesgos como abusos y usos ilícitos.*
*k) ¿**Por cuanto tiempo planean almacenar los datos recolectados por las cámaras de reconocimiento facial**?¿**Tienen previsto aplicar algún tipo de protocolo de destrucción de datos una vez hayan cumplido el fin para el cual fueron recolectados**?*

Como primera observación que podrá realizar Usía, la solicitud de acceso a la información pública contiene una serie de requerimientos sobre un tema de elevadísimo interés público, ya que, en esencia, se trata sobre el cómo las instituciones del Estado encargadas de la seguridad manejan y administran datos personales de la población paraguaya, en este caso para la implementación de una tecnología de reconocimiento facial. Esto, desde ya, como se explicará más adelante, implica que existe una obligación positiva por parte del Estado de dar respuesta oportuna, clara y detallada sobre todo lo vinculado a esta iniciativa.

El 26 de abril de 2019, la Oficina de Acceso a la Información Pública (en adelante, "OAIP") del MDI contestó a través del Portal Unificado mencionando con respecto al primer punto de la solicitud que "*[l]a Adquisicion del sistema de tegnología biométrica, fue realizada por la Comisión Nacional de Telecomunicaciones (CONATEL), a través de la Licitación Pública N° 2/2017 con el objeto de otorgar subsidio a la Policia Nacional a través del Fondo de Servicios Universales (FSU), a ser ejecutado dentro del marco de la Ley de Presupuesto General de la Nación, para el Ejercicio Fiscal del año 2017, para la expansión del Sistema de Atención y Despacho de Llamadas de Emergencia - SADLE 911 de la Policia Nacional para la ciudad de Asunción y Área Metropolitana*" (sic) (la cursiva me pertenece). Asimismo, mencionó que los "detalles" estaban disponibles en el siguiente link: https://www.conatel.gov.py/images/iprincipal/2017/Noviembre/PBC%20LIC.PUB.02-2017-RD%201723-2017.PDF

Cabe observar a Usía que si bien la OAIP del MDI adjuntó el link referente de una licitación pública por la cual se habría adquirido el sistema de tecnología biométrica, no se explica de manera clara cuál es el sistema adquirido, qué tipo de tecnología se trata o cómo funciona esta tecnología. Tampoco se adjuntó contrato alguno o documento descriptivo de acuerdo con lo que se requirió en la solicitud AIP. En este sentido, **la fuente pública no informó de acuerdo con lo requerido**.

Por otro lado, en relación con el cuarto punto, la OAIP del MDI contestó que "*[l]a ampliación del sistema de tegnología biométrica fue*

desarrollada por la Comisión Nacional de Telecomunicaciones (CONATEL), a través de la Licitación Pública FSU N° 2/2018 con el objeto de otorgar subsidio a la Policia Nacional a través del Fondo de Servicios Universales (FSU), a ser ejecutado dentro del marco de la Ley de Presupuesto General de la Nación, para el Ejercicio Fiscal del año 2018, para la expansión del Sistema de Atención y Despacho de Llamadas de Emergencia - SADLE 911 de la Policia Nacional para la ciudad de Coronel Oviedo, Caaguazú, San Ignacio, Ciudad del Este y Encarnación" (sic) (la cursiva me pertenece).

Igualmente, mencionó en la contestación que los "detalles" se encontraban disponibles en el siguiente link: https://www.conatel.gov.py/images/iprincipal/2018/10-Octubre/LPN%2002/PBC%20LP%20FSU%20Nro%202-2018%20AMPLIACION%20911%20INTERIOR.pdf

Finalmente, mencionó que, con relación al punto segundo y tercero, eran denegados "en base a la Resolución N° 238/19 del Ministerio del Interior".

En el mismo Portal Unificado la OAIP del MDI adjuntó copia de la Resolución mencionada. Como podrá observar Usía, tal acto administrativo resolvió, según sus términos, "dar respuesta parcial" a la solicitud AIP. Como se puede observar igualmente, la respuesta y la fundamentación por parte del MDI es escueta, vaga y ambigua, ya que se limitó simplemente a señalar que se trataban de "datos de seguridad" y que son "reservados" (en relación con el segundo y tercer punto, y las preguntas de la "a" a la "k").

En el segundo artículo de la Resolución se hizo mención de los Art. 2 y 20 (entiendo que se refiere al 22) de la ley 5.282 para justificar la denegación.

Como podrá observar Usía, la fuente pública obligada no hizo un mínimo esfuerzo para fundamentar las negativas. Es más, a saber, **lo requerido no se encuentra calificado como reservado por ninguna ley de la República de manera "expresa" como lo requiere el Art. 22 de la Ley 5.282**. Tampoco se hizo ninguna consideración de hecho, y menos de derecho, sobre las razones que llevaron a denegar la información. En este sentido, el MDI calificó de manera arbitraria como reservada la información sin señalar, cuanto menos, la ley en que basa su calificación y cuáles serían los riesgos (al menos, hipotéticos) para un interés de "seguridad" en caso de dar a conocer la información.

Tal actuar por parte del MDI se trata de un acto manifiestamente ilegítimo, ya que se ha apartado de su obligación legal de actuar de acuerdo con el principio de legalidad (que encuentra su base en la Constitución en su Art. 257, "los órganos del Estado se subordinan a los dictados de la ley"). La misma ley 5.282 obliga en su Art. 19 a las fuentes públicas, en caso de denegaciones de solicitudes de información, a dictar

"resolución fundada" por la máxima autoridad de la fuente pública requerida, quien debe expresar "los motivos de hecho y de derecho en que se basa la decisión", cuestión que no se verifica en el presente caso.

Independientemente ante la potencial calificación por parte de Usía respecto con la naturaleza pública de la información requerida, deberá declarar la ilegitimidad del acto por parte del MDI al verificar que esta institución pública se ha apartado de su obligación de actuar de acuerdo con la ley, lo que además me ha llevado forzosamente, ante tal actuar arbitrario, a acudir a la justicia para el amparo de un derecho humano fundamental, con las cargas que una acción así me obliga a soportar. Esto, por sí, deberá ser considerado por Usía al momento de imponer las costas.

DERECHO. La Constitución de la República del Paraguay reconoce de manera expresa en su Art. 28 el derecho que tiene toda persona a recibir información por parte de las fuentes públicas y la obligación positiva del Estado de dar información "veraz, responsable y ecuánime". Asimismo, la Convención Americana sobre Derechos Humanos o Pacto de San José de Costa Rica, tratado internacional ratificado por el Paraguay por medio de la Ley 1/89, reconoce este derecho en su Art. 13. De acuerdo con la interpretación de esta normativa por parte de los órganos que conforman el Sistema Interamericano de Derechos Humanos (SIDH), el derecho de acceso a la información pública debe ser garantizado por el Estado bajo un régimen limitado de excepciones interpretadas de manera restrictiva[3].

La Corte Suprema de Justicia de la República del Paraguay reconoció el valor interpretativo de la Corte Interamericana de Derechos Humanos (en adelante, "Corte IDH") mediante el Acuerdo y Sentencia 1306 del 15 de octubre de 2013 y ejerció el control de convencionalidad con base en los postulados de ese tribunal interamericano. Así, en palabras de la Corte IDH "*…cuando un Estado ha ratificado un tratado internacional como la Convención Americana, sus jueces, como parte del aparato del Estado, también están sometidos a ella, lo que les obliga a velar porque los efectos de las disposiciones de la Convención no se vean mermadas por la aplicación de leyes contrarias a su objeto y fin, y que desde un inicio carecen de efectos jurídicos"*[4]. En este sentido, la Corte Suprema de Justicia del Paraguay mencionó que es "*lógico y razonable*" que las decisiones de la Corte IDH sean consideradas lo que "*permitirá evitar eventuales decisiones adversas para nuestro país por inobservancia de los principios de la Convención, que comprometerían su responsabilidad internacional*"[5].

---

3 Cfr. CIDH. *El derecho de acceso a la información en el marco jurídico interamericano*. 2da. Ed. Washington, OEA, 2012.

4 Corte IDH. *Caso Almonacid Arellano y otros Vs. Chile. Excepciones Preliminares, Fondo, Reparaciones y Costas.* Sentencia de 26 de septiembre de 2006.

En materia de acceso a la información pública, la decisión fundamental de la Corte IDH es el caso de "**Claude Reyes y otros Vs. Chile**" (Sentencia del 19 de septiembre del 2006). En este caso (que también fue tenido en cuenta por nuestra CSJ en el citado caso del Acuerdo y Sentencia número 1306).

En una sociedad democrática es indispensable que las autoridades estatales se rijan por el principio de máxima divulgación[6], el cual establece la presunción de que toda información es accesible sujeta a un sistema restringido de excepciones.[7]

La Ley 5.282, que reglamenta el Art. 28 de la Constitución, fue concebida bajo la doctrina del caso Claude y a la luz de los PRINCIPIOS SOBRE EL DERECHO DE ACCESO A LA INFORMACIÓN y de la Ley Modelo sobre Acceso a la Información Pública (constan en la exposición de motivos del proyecto original).

La ley 5.282 dispone en su Art. 2, numeral 2, que se entiende como "**información pública**" a "*[a]quella producida, obtenida, bajo control o en poder de las fuentes públicas, independientemente de su formato, soporte, fecha de creación, origen, clasificación o procesamiento, salvo que se encuentre establecida como secreta o de carácter reservado por las leyes*" (la cursiva me pertenece). El Decreto reglamentario 4.064 señala como regla de interpretación que la aplicación de las disposiciones de tal cuerpo normativo se realice "*de forma tal que se priorice el más amplio y efectivo acceso a la información que obra en poder de las fuentes públicas de información*" (la cursiva me pertenece).

Además, tanto la ley 5.282 como su decreto reglamentario recogen el principio de que las disposiciones consagradas en esos cuerpos normativos no puedan ser utilizadas o entendidas "*para negar, menoscabar o limitar la libertad de expresión, la libertad de prensa o la libertad de ejercicio del periodismo*" (Art. 1, ley 5.282) o "*la libre circulación de la información que sea de acceso público"* (Art. 2, Decreto 4.064). Por ello, **una denegación arbitraria o infundada de información pública debe considerarse como una restricción indirecta a la libertad de expresión** (expresamente prohibido por el Art. 13.3 de la Convención Americana sobre Derechos Humanos[8]).

---

5 Acuerdo y Sentencia 1306/13. Corte Suprema de Justicia de Paraguay.

6 La Corte IDH al interpretar el artículo 13 de la Convención Americana sobre los Derechos Humanos.

7 Caso Claude Reyes y otros vs. Chile, Fondo, Reparaciones y Costas. Sentencia de 19 de setiembre de 2006. Serie C No 151.

8 **Artículo 13. Libertad de Pensamiento y de Expresión**. "[…] No se puede restringir el derecho de expresión […] por cualesquiera otros medios encaminados a impedir la comunicación y la circulación de ideas y opiniones. […]".

De acuerdo con los principios en materia de libertad de expresión desarrollados por la Comisión Interamericana de Derechos Humanos (en adelante, "CIDH"), "[l]as restricciones en la circulación libre de ideas y opiniones, como así también la imposición arbitraria de información y la creación de obstáculos al libre flujo informativo, violan el derecho a la libertad de expresión"[9].

Según la Corte IDH, lo dispuesto en el Art. 13.3 de la Convención no resulta taxativo[10]. Por ello, la expresión de "cualquiera otros medios" debe aplicar necesariamente cuando la denegación de una información de naturaleza pública ha sido arbitraria.

Asimismo, el Decreto 4.064 (norma aplicable al MDI) recoge los estándares del Sistema Interamericano de Derechos Humanos e introduce en su Art. 35 la obligación para las instituciones públicas de desarrollar una serie de criterios que para rechazar el acceso a la información. Así, menciona esta normativa que "*la fuente pública deberá dictar resolución* ***debidamente fundamentada y la carga de la prueba recaerá en ella a fin de demostrar que la información solicitada se ajusta al caso concreto de excepción contenida en una norma jurídica con una mayor jerarquía no inferior a la de la ley***" (la cursiva, negrita y subrayado me pertenece). Asimismo, menciona que de manera particular esta argumentación debe considerar "*que la excepción es legítima y estrictamente necesaria en una sociedad democrática sobre la base de los estándares y jurisprudencia del sistema interamericano de protección de los derechos humanos*"; "*que la divulgación de la información podría causar un daño sustancial a un interés protegido por la ley*"; y, "*que la probabilidad y el grado de dicho daño es superior al interés público en la divulgación de la información*" (la cursiva me pertenece).

Como quedó plenamente demostrado en el presente caso, **el MDI incumplió con la obligación de proveer información que, a saber, no encuentra una causal de reserva establecida en una ley de manera expresa de acuerdo con el Art. 22 de la ley 5.282**. Asimismo, **la fuente pública incumplió con su obligación de demostrar de manera clara y expresa la circunstancia de hecho y de derecho por la cual la información requerida podría considerarse como reservada y cuál es el daño sustancial a lo calificado como "seguridad"**. No quedó claro qué circunstancias reales podrían llevar a lesionar el alegado criterio de seguridad; y cuáles son los

---

9 CIDH/Relatoría Especial para la Libertad de Expresión. *Marco Jurídico Interamericano sobre Libertad de Expresión*. Washington, OEA, 2010, párr. 96.

10 Corte I.D.H., Caso Ríos y otros Vs. Venezuela. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 28 de enero de 2009. Serie C No. 194, párr. 340; Corte I.D.H., Caso Perozo y otros Vs. Venezuela. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 28 de enero de 2009. Serie C No. 195, párr. 367.

vínculos del acceso a la información con esas potenciales circunstancias (si las hubiera).

Que, si bien el acceso a la información admite restricciones, el MDI no demostró, como se mencionó, la circunstancia real para calificar la información como reservada. En consideración de la Corte IDH en el caso *Claude Reyes*, una restricción debe estar fijada en la ley de manera previa "como medio para asegurar que no queden al arbitrio del poder público"[11]. Además, esta restricción debe responder a un objetivo permitido por la Convención Americana[12]. Estas restricciones se encuentran en el Art. 13.2. Si bien la Convención señala la posibilidad de restringir información por motivos de seguridad nacional, esta no puede ser calificada en abstracto y de manera vaga o ambigua o "de cualquier forma"[13]. Pero además, **el concepto de "seguridad" no puede abarcar sobre el manejo que hacen las instituciones públicas sobre información que afecta a la intimidad de las personas, ya que se trata de un derecho humano reconocido por la Constitución así como en la Convención Americana, a la par de que no pueden oponerse excepciones frente a graves violaciones a los derechos humanos**[14]. Por último, estas restricciones deben ser estrictamente necesarias y orientadas a "satisfacer un interés público imperativo"[15]. El **MDI tampoco demostró que la medida adoptada sea la menos restrictiva y, como tal, que tal denegación cumpliría con un interés público que supere el derecho de toda la sociedad a conocer la información**.

En palabras de la Corte IDH, "la restricción debe ser proporcional al interés que la justifica y debe ser conducente para alcanzar el logro de ese legítimo objetivo, interfiriendo en la menor medida posible en el efectivo ejercicio del derecho"[16]. Igualmente, en palabras de la Corte IDH "corresponde al Estado demostrar que al establecer restricciones al acceso a la información bajo su control ha cumplido con los anteriores requisitos"[17].

---

11 Cfr. CIDH. *El derecho de acceso a la información en el marco jurídico interamericano*. 2da. Ed. Washington, OEA, 2012, párr. 24.

12 Cfr. CIDH. *El derecho de acceso a la información en el marco jurídico interamericano*. 2da. Ed. Washington, OEA, 2012, párr. 52.

13 Cfr. CIDH. *El derecho de acceso a la información en el marco jurídico interamericano*. 2da. Ed. Washington, OEA, 2012, párr. 87.

14 Cfr. CIDH. *El derecho de acceso a la información en el marco jurídico interamericano*. 2da. Ed. Washington, OEA.

15 Cfr. CIDH. *El derecho de acceso a la información en el marco jurídico interamericano*. 2da. Ed. Washington, OEA, párr. 12.

16 Cfr. CIDH. *El derecho de acceso a la información en el marco jurídico interamericano*. 2da. Ed. Washington, OEA, párr. 53.

17 Cfr. CIDH. *El derecho de acceso a la información en el marco jurídico interamericano*. 2da. Ed. Washington, OEA, párr. 66.

Finalmente, en caso de duda, el Decreto 4.064 menciona en su Art. 36 que “se debe optar por la publicidad de la información”, mientras que en su Art. 37 señala que “si un documento contiene información que puede ser conocida e información que se encuentra alcanzada por una causal de excepción, se debe dar acceso a la primera”.

Asimismo, la Corte Europea de Derechos Humanos en el asunto Szabo and Vissy v. Hungary (2016) resolvió que “dada la particular característica de la interferencia y el gran potencial de las tecnologías de vigilancia para invadir la privacidad de los ciudadanos, la Corte considera que los requerimientos relativos a ‘necesarios en una sociedad democrática’ deben ser interpretados en este contexto como ‘estrictamente necesarios’ en dos aspectos. Una medida de vigilancia secreta sólo puede ser acorde con la Convención únicamente si es estrictamente necesaria, como consideración general, para salvaguardar las instituciones democráticas, y, además, ser estrictamente necesaria, como consideración particular, para obtener información de inteligencia en una operación individual. A consideración de la Corte, cualquier medida de vigilancia secreta que no satisfaga esos dos criterios se encontraría sujeta a abuso para las autoridades dada la tecnología con la que cuentan”[18].

Pero todavía cuando el MDI considere que la información puede afectar un interés de seguridad, tiene la obligación de informar mínimamente algunas cuestiones que resultan de interés público y para nada afectan intereses de seguridad. Por ejemplo, en un caso dado en México, frente al conocimiento público de que el Estado adquirió un software con la capacidad de realizar tareas de espionaje, la Comisión Interamericana de Derechos Humanos (CIDH) instó al Estado garantizar el acceso a la información sobre “programas de vigilancia o espionaje, su alcance y los controles existentes”[19]. En este sentido, “esta obligación abarca la información sobre su marco regulatorio, los contratos para la adquisición de estos programas, los protocolos y procedimientos de

---

18 Fuente: Case of Szabo and Vissy v. Hungary (Application no. 37138/14) Judgment Strasbourg, 12 January 2016. “*However, given the particular character of the interference in question and the potential of cuttingedge surveillance technologies to invade citizens’ privacy, the Court considers that the requirement “necessary in a democratic society” must be interpreted in this context as requiring “strict necessity” in two aspects. A measure of secret surveillance can be found as being in compliance with the Convention only if it is strictly necessary, as a general consideration, for the safeguarding the democratic institutions and, moreover, if it is strictly necessary, as a particular consideration, for the obtaining of vital intelligence in an individual operation. In the Court’s view, any measure of secret surveillance which does not correspond to these criteria will be prone to abuse by the authorities with formidable technologies at their disposal*”.

19 CIDH. *Relatoría Especial manifiesta preocupación ante denuncias sobre espionaje de periodistas y defensores de derecho humanos en México e insta a desarrollar una investigación completa e independiente.* 12 de julio de 2017.

autorización, de selección de objetivos y de manejo de datos, así como información sobre el uso y control de estas técnicas"[20].

En esa misma intervención, en las observaciones preliminares, el Relator Especial de la ONU sobre la libertad de expresión y el Relator Especial sobre libertad de expresión de la CIDH después de su visita conjunta en México, el 27 de noviembre al 4 de diciembre de 2017[21], señalaron que "la tecnología de vigilancia tiene implicaciones profundas para ejercer la libertad de expresión, que perjudican la capacidad de los individuos para compartir o recibir información y establecer contacto con activistas y otros"; "crea incentivos para la autocensura y directamente perjudica la capacidad de los periodistas y defensores de derechos humanos para realizar investigaciones y construir y mantener relaciones con fuentes de información": "*La vigilancia debería ser una opción para los gobiernos únicamente bajo las reglas más estrictas en el contexto de cumplimiento con la ley, esto es que estén disponibles y sean adoptadas públicamente y operando sobre principios de necesidad y proporcionalidad y con supervisión judicial de cerca. (...)*".

Lo anterior se encuentra basado en una declaración conjunta del Relator Especial de las Naciones Unidas (ONU) para la Protección y Promoción del Derecho a la Libertad de Opinión y de Expresión y la Relatora Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la OEA, quienes sostuvieron que "*[l]os derechos a la privacidad y a la libre circulación del pensamiento e información se encuentran protegidos por el derecho internacional de los derechos humanos*" y que estos instrumentos "*reconocen de manera expresa el derecho de toda persona, sin discriminación, a manifestar libremente su pensamiento y a buscar y recibir informaciones de toda índole*" como, asimismo, "***prohíben injerencias arbitrarias o abusivas en la vida privada, incluidas las comunicaciones, y a obtener la protección del Estado contra ese tipo de injerencias***"[22] (la cursiva, negrita y subrayado me pertenece).

En el sentido anterior, mencionan que "*los Estados deben garantizar que la intervención, recolección y uso de información personal, incluidas todas*

---

20 CIDH. *Relatoría Especial manifiesta preocupación ante denuncias sobre espionaje de periodistas y defensores de derechos humanos en México e insta a desarrollar una investigación completa e independiente.* 12 de julio de 2017

21 *Observaciones preliminares del Relator Especial de la ONU sobre la libertad deexpresión y el Relator Especial sobre libertad de expresión de la CIDH después de suvisita conjunta en México, 27 de noviembre – 4 de diciembre 2017. Disponible en: https://www.oas.org/es/cidh/expresion/docs/Observaciones_Preliminares_ESP.PDF*

22 Relator Especial de las Naciones Unidas (ONU) para la Protección y Promoción del Derecho a la Libertad de Opinión y de Expresión Relatora Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la OEA. Declaración Conjunta sobre Programas de Vigilancia y su Impacto en la Libertad de Expresión. 21 de junio de 2013. Disponible en: http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=926&lID=2

las limitaciones al derecho de la persona afectada a acceder a información sobre las mismas, estén claramente autorizadas por la ley a fin de proteger a la persona contra interferencias arbitrarias o abusivas en sus intereses privados" y que "***la ley deberá establecer límites respecto a la naturaleza, alcance y duración de este tipo de medidas, las razones para ordenarlas, las autoridades competentes para autorizar, ejecutar y supervisarlas y los mecanismos legales para su impugnación***"[23] (la cursiva, negrita y subrayado me pertenece).

Con respecto a los "**deberes de publicidad y transparencia"**, mencionan que "*[t]oda persona tiene derecho a acceder a información bajo el control del Estado. Este derecho incluye la información que se relaciona con la seguridad nacional, salvo las precisas excepciones que establezca la ley, siempre que estas resulten necesarias en una sociedad democrática. Las leyes deben asegurar que el público pueda acceder a información sobre los programas de vigilancia de comunicaciones privadas, su alcance y los controles existentes para garantizar que no puedan ser usados de manera arbitraria. En consecuencia, **los Estados deben difundir, por lo menos, información relativa al marco regulatorio de los programas de vigilancia; los órganos encargados para implementar y supervisar dichos programas; los procedimientos de autorización, de selección de objetivos y de manejo de datos, así como información sobre el uso de estas técnicas, incluidos datos agregados sobre su alcance. En todo caso, los Estados deben establecer mecanismos de control independientes capaces de asegurar transparencia y rendición de cuentas sobre estos programas***"[24] (la cursiva, negrita y subrayado me pertenece).

En la resolución del "Derecho a la privacidad en la era digital" Pública A/C.3/71/L.39[25], el Consejo de Derechos Humanos de la ONU advirtió que la vigilancia y la interceptación ilegales o arbitrarias de las comunicaciones, así como la recopilación ilegal o arbitraria de datos personales, al constituir actos de intrusión grave, violan el derecho a la privacidad: "*Reafirmando el derecho humano a la privacidad, según el cual nadie debe ser objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, y el derecho a la protección de la ley*

---

23 Relator Especial de las Naciones Unidas (ONU) para la Protección y Promoción del Derecho a la Libertad de Opinión y de Expresión Relatora Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la OEA. Declaración Conjunta sobre Programas de Vigilancia y su Impacto en la Libertad de Expresión. 21 de junio de 2013. Disponible en: http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=926&lID=2

24 Relator Especial de las Naciones Unidas (ONU) para la Protección y Promoción del Derecho a la Libertad de Opinión y de Expresión Relatora Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la OEA. Declaración Conjunta sobre Programas de Vigilancia y su Impacto en la Libertad de Expresión. 21 de junio de 2013. Disponible en: http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=926&lID=2

25 Asamblea General de la ONU - 16 de noviembre de 2016. Disponible en: https://undocs.org/A/C.3/71/L.39/Rev.1

contra esas injerencias, y reconociendo que el ejercicio del derecho a la privacidad es importante para materializar el derecho a la libertad de expresión y a abrigar opiniones sin injerencias, ***y el derecho a la libertad de reunión y asociación pacíficas, y es una de las bases de una sociedad democrática****"* (negrita y subrayado me pertenece).

Poniendo de relieve que la vigilancia arbitrarias a través de cámaras de vigilancia con reconocimiento facial, así como la recopilación ilegal o arbitraria de datos personales en la vía pública y espacios privados, al constituir actos de intrusión grave, violan el derecho a la privacidad y pueden interferir con el derecho a la libertad de expresión, de reunión y asociación pacífica y ser contrarios a los preceptos de una sociedad democrática, en particular cuando se llevan a cabo a gran escala.

Observando en particular que la vigilancia en espacios públicos, debe ir acompañado de una análisis previo de evidencia, análisis de impacto de derechos y debe ser compatible con las obligaciones internacionales en materia de derechos humanos y debe llevarse a cabo sobre la base de un marco jurídico que sea de acceso público, claro, preciso, amplio y no discriminatorio, y que ninguna injerencia en el derecho a la privacidad debe ser arbitraria o ilegal, teniendo en cuenta lo que sea razonable para la persecución de objetivos legítimos, y recordando que los Estados que son partes en el Pacto Internacional de Derechos Civiles y Políticos deben adoptar las medidas necesarias para aprobar las leyes u otras disposiciones que hagan falta a fin de hacer efectivos los derechos reconocidos en el Pacto"....".

En un Estado democrático de derecho, el gobierno abierto permite que la ciudadanía vigile la gestión de sus representantes, mientras que en un Estado autoritario, el gobierno es el que realiza la vigilancia (surveillance) en clave de espionaje (nonopticon)[26] de la ciudadanía; de allí que a fin de garantizar la prevalencia del Estado democrático de derecho frente al Estado autoritario deba rendirse cuentas y transparentarse toda actuación y elemento relacionado –incluso en forma indiciaria– con el espionaje de las autoridades (o particulares que actúen con aquiescencia del Estado) en perjuicio de la ciudadanía.

La "cibervigilancia" por parte del Estado ya sea por adquisición de software de vigilancia a través de cámaras de reconocimiento facial, interceptación de los metadatos (geolocalización, IP,datos personales entre otros), se ha convertido en un tema de debate e interés público tanto en la agenda nacional como internacional, pues por su incidencia "silenciosa" y su uso en contra de ciudadanos comunes (activistas, defensores de derechos humanos y periodistas) ha generado gran preocupación en la

26 A diferencia del panopticon en donde se sabe que se es vigilado y quién vigila, en el nonopticon no se sabe jamás si se es vigilado, ni por quien, ni con qué grado de indiscreción. Mattelart, Armand; Vitalis, Andre . De Orwell al cibercontrol. Barcelona, Gedisa, 2015, p. 205

sociedad en general, así como de diversos organismos internacionales de protección de derechos humanos[27].

El concepto de "seguridad nacional" en modo alguno tiene el alcance de legitimar el uso de tecnología de control y vigilancia masiva o selectiva de la vida privada de la ciudadanía dentro de la sociedad cuando dicha intromisión se despliega fuera del contexto de una investigación criminal judicialmente autorizada; de modo que los alcances de ese tipo de espionaje tecnológico son públicos (y no reservables) cuando derivan de un determinado software utilizado en un contexto de desviación de poder que más que "seguridad nacional" produce inseguridad jurídica y personal para los integrantes de la sociedad dentro del Estado.

De acuerdo a los principios de Tshwane[28], si bien los Estados "enfrentan múltiples desafíos al procurar encontrar un equilibrio entre el interés público en la divulgación y la necesidad de la clasificación para proteger intereses legítimos de la seguridad nacional", "la información relacionada con violaciones de los derechos humanos[29] o el derecho humanitario está sujeta a una alta presunción de divulgación, y en ningún caso puede ser clasificada invocando razones de seguridad nacional de forma tal que se evite la rendición de cuentas por dichas violaciones, o se despoje a la víctima de la oportunidad de acceder a una reparación efectiva".

De acuerdo con lo señalado precedentemente resulta claro que aun cuando el MDI considere que la información se vincula con algún principio de seguridad, posee la obligación expresa de proveer información sobre una serie de cuestiones, por sobre todo acreditar mediante **elementos objetivos** que la difusión de la información podría causar un daño en

---

27 La Asamblea General de las Naciones Unidas a través de la resolución 68/167 de 18 de diciembre de 2013 destacó que la capacidad de los gobiernos y las empresas para llevar a cabo actividades de vigilancia, interceptación y recopilación de datos de las personas, suscita cada vez más preocupación. Al respecto; véase http://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_28_L27.pdf.

28 Principios Globales sobre Seguridad Nacional y el derecho a la información, emitidos el 12 de junio de 2013 y redactados por 22 organizaciones (entre las que destacan Amnistía Internacional; Artículo 19, Campaña Mundial para la Libertad de Expresión, la Universidad Central Europea (Budapest/ Europa); Centre for European Constitutionalization and Security (CECS), Universidad de Copenhague (Copenhague/Europa) y Open Society Justice Initiative (OSJI) (Nueva York/global), así como por 500 expertos procedentes de 70 paises y 4 relatores de las Naciones Unidas; visible en: https://www.opensocietyfoundations.org/sites/default/files/tshwane-espanol10302014%20%281%29.pdf.

29 Tales como, a manera de ejemplo, crímenes de derecho internacional, violaciones sistemas o generalizadas a la libertad y seguridad personales, así como cuando un Estado está sometido a un proceso de justicia transicional durante el cual se ve especialmente obligado a garantizar la verdad, justicia y garantías de no repetición.

términos de “seguridad nacional”. En el caso concreto, ninguno de los pedidos de información se encuentra fuera de estos supuestos de transparencia y publicidad.

Se puede concluir que el MDI incumplió con su obligación de proveer información que debe ser considerada pública, y con su obligación de fundar adecuadamente la negativa del acceso a la información.

INEXISTENCIA DE VIAS PREVIAS O PARALELAS: De acuerdo con lo establecido en el art. 21 de la ley 5282/14, interpuse el pedido de solicitud el día 08 de abril del 2019 mediante el Portal Unificado de Información Pública en donde obtuve una comunicación en fecha 26 de abril del 2019, en la cual se manifestó que se ha respondido sobre el punto 1 y 4 enviando dos links (acceso directo a la página de la institución) donde acotan que allí se encuentra la información solicitada, siendo que no contiene toda la información. Y sobre los puntos 2 y 4 me denegaron bajo Resolución N° 238/19 de la institución que, como se observó, carece de una mínima fundamentación jurídica.

Si tomamos como fecha de presentación de la solicitud el 08 de abril del 2019, los quince días hábiles se cumplieron el día 2 de mayo del 2019. Como me han respondido en fecha 26 de abril del 2019, esta deberá ser la fecha de referencia.

Finalmente, a los fines de lo previsto en la Acordada Nro. 6 del 18 de agosto de 1969 declaro bajo fe de juramento que no existe en los tribunales de la República ningún asunto pendiente de resolución que pudiera tener relación directa con el objeto o materia del presente amparo.

PRUEBA: Por tratarse de actos que se han realizado a través de medios electrónicos que, en los términos de la **Ley 4017/10 “De la firma electrónica, la firma digital, los mensajes de datos y el expediente electrónico”**, poseen plena validez jurídica, señalo, de acuerdo con el Art. 568 *in fine* del CPC, la indicación del medio en el cual Usía podrá acceder a la prueba:

A. **Solicitud #19983 (Cámaras de videovigilancia – Biometría):** https://informacionpublica.paraguay.gov.py/portal/#!/ciudadano/solicitud/19983 (se adjunta captura impresa).

B. Documentos adjuntos a la respuesta de la Solicitud #19983:

a. Licitación Pública FSU 2/2017

https://www.conatel.gov.py/images/iprincipal/2017/Noviembre/PBC%20LIC.PUB.02-2017-RD%201723-2017.PDF

b. Licitación Pública FSU 2/2018

https://www.conatel.gov.py/images/iprincipal/2018/10-Octubre/LPN%2002/PBC%20LP%20FSU%20Nro%202-2018%20AMPLIACION%20911%20INTERIOR.pdf

c. **Resolución 238/19 del Ministerio del Interior, "POR LA CUAL SE DA RESPUESTA PARCIAL A LA SOLICITUD INGRESADA AL PORTAL DE ACCESO A LA INFORMACIÓN PÚBLICA DE LA DIRECCIÓN GENERAL DE TRANSPARENCIA Y ANTICORRUPCIÓN DEL MINISTERIO DEL INTERIOR, A TRAVÉS DEL NÚMERO 19983"**

https://informacionpublica.paraguay.gov.py/public/500459-Resol238jpeg-Resol238.jpeg (se adjunta impreso)

https://informacionpublica.paraguay.gov.py/public/332864-Res238jpeg-Res238.jpeg (se adjunta impreso)

AUTORIZADOS. Como esta acción judicial se enmarca dentro de los casos impulsados por la Clínica Jurídica para promover el derecho de la información pública de la Facultad de Derecho y Ciencias Sociales de la Universidad Nacional de Asunción, cuyo fin es la promoción y defensa del derecho de acceso a la información pública mediante la asistencia profesional y procuración de justicia en tribunales a ciudadanos que no hayan recibido respuestas a sus solicitudes de información pública dentro del marco de la Ley N° 5282/14 "*De libre acceso ciudadano a la información pública y transparencia gubernamental*", quedan autorizados a revisar el expediente y agregar y retirar documentos o el expediente mismo en los casos previstos en la ley procesal, las siguientes personas integrantes de la Clínica: Nancy Belén Morel Vigo, con C.I. N° 4.525.036; Evelyn Yazmín Acosta Balbuena, con C.I. N° 4.574.440; Alejandro Luis López Niella, con C.I. N° 3.948.658; Fabián Darío Riveros Agüero, con C.I. N° 3.525.671; Zulma Raquel Bogado Domínguez, con C.I. N° 5.001.525; y, Viviana Belén Melgarejo Paniagua, con C.I. N° 4.480.706.

PETITORIO. Por lo expuesto, a Usía solicito:

1. Me tenga por presentada, por parte, por denunciado mi domicilio real y por constituido el procesal.
2. Admita la presente acción de amparo contra el Ministerio del Interior y ordene a ésta que produzca en el plazo de ley el informe circunstanciado previsto en el art. 582 del CPC acerca de los antecedentes y trámites que se le dio a la solicitud de acceso a la información realizada en el sitio web del Portal Unificado de Información Pública el día 08 de abril del 2019.

3. Oportunamente, dicte sentencia definitiva ordenando al Ministerio del Interior a entregarme y publicar en el Portal Unificado de Acceso a la Información Pública y/o en su sitio web toda la información pública solicitada, con costas por ser éste un imperativo legal.
4. Con la consideración de que por el actuar arbitrario por parte del Ministerio del Interior me ha obligado a iniciar la presente acción judicial, declare la imposición de costas en su totalidad a la autoridad en los términos del Art. 587 del CPC.

Usía proveerá de conformidad y,

HARÁ JUSTICIA