La enajenación continua de nuestros derechos

Sistemas de identidad: biometría y cámaras de vigilancia no reguladas en Paraguay

Luis Alonzo Fulchi
Eduardo Carrillo
Maricarmen Sequera

TEDIC
TECNOLOGÍA & COMUNIDAD

Tabla de contenidos

Esta publicación es un análisis de la política de implementación de los sistemas de identificación: biometría y cámaras de vigilancias en espacios públicos en Paraguay. Realizado por la ONG TEDIC de Paraguay. Julio 2018.

Autores:

Eduardo Carrillo

Maricarmen Sequera

Luis Alonzo Fulchi

Introducción

El anuncio por parte de la Policía Nacional, el Ministerio de Interior y la Comisión Nacional de Telecomunicaciones (CONATEL) sobre el nuevo sistema de video vigilancia biométrica del sistema 911, se constituye en un golpe que violenta derechos fundamentales de la población paraguaya.

Esta iniciativa tiene un objetivo legítimo que es el orden público y la seguridad de la población. Sin embargo, el diseño del sistema de prevención y persecución de delitos debe tener en cuenta que no puede, por sí solo, acabar con la cadena criminal que busca combatir. La delincuencia no se acaba con inundar la ciudad de cámaras o drones, esto en realidad generará una falsa sensación de seguridad momentánea.

El *problema de la seguridad*

Durante el inicio del mes de julio de este año, autoridades de diversos estamentos del sector público presentaron *in extenso* el nuevo conjunto de equipos y servicios tecnológicos del Sistema 911 de la Policía Nacional, para la ciudad de Asunción y el Área Metropolitana.

Mediante la Licitación Pública FSU N° 2/2017- *"Para el otorgamiento de subsidio a través del fondo de servicios universales para la expansión del sistema de atención y despacho de llamadas de emergencia-sadle 911 de la Policía Nacional para la ciudad de Asunción y Área Metropolitana"*[i] fueron adquiridos una serie de insumos tecnológicos consistentes en:

- 100 cámaras PTZ IP de video vigilancia;
- 44 cámaras de reconocimiento de placas (L.P.R);
- 10 cámaras de reconocimiento facial (F.R)
- 9 torres de comunicaciones de radio bases, además de infraestructura y equipos inalámbricos de acceso.

Distribuidas en zonas estratégicas de la ciudad, las 100 cámaras se suman a un total de 800 ya existentes en toda el área metropolitana. A su vez, las cámaras de reconocimiento de placas fueron colocadas en puntos de peaje y rutas y las “novedosas” cámaras de reconocimiento facial fueron colocadas en puntos de alta concentración y circulación de personas, como la Terminal de Ómnibus de Asunción, el Aeropuerto Internacional Silvio Pettirossi y la sede del Congreso Nacional. Estas últimas ya poseen una base de datos de 50.000 personas y que puede ser fácilmente ampliada, según el proveedor del Estado que se encargó de explicar el sistema.

Desde la organización TEDIC surgen una serie de análisis y reflexiones sobre potenciales peligros que pueden surgir en el marco de la implementación de estas tecnologías, habida cuenta del débil contexto institucional, y la falta de garantías a un *debido proceso* en sistema policial y judicial paraguayos.

Fondos de Servicios Universales: ¿de quién?¿para quién?

Mediante el Contrato 53/2017[ii]de diciembre pasado, la empresa Tecnología, Seguridad y Vigilancia del Paraguay S.R.L, obtuvo la adjudicación de 18.500 millones de guaraníes (unos 3 millones de dólares) para proveer los distintos tipos de cámaras de vigilancia. Los recursos provienen de la CONATEL a través de los Fondos de Servicios Universales (FSU)[1] que según su reglamento tiene como objetivos:

- a) Promover a través del financiamiento la expansión de los servicios públicos de telecomunicaciones en áreas rurales y lugares de interés público y social.
- b) Promover el acceso a los servicios públicos de telecomunicaciones de más paraguayos de manera eficiente, procurando servicios de calidad y precios razonables tomando en consideración los niveles de ingreso de la población beneficiaria.
- c) Maximizar el beneficio económico en la dotación de los servicios de telecomunicaciones mediante la reducción de costos en la provisión de los servicios más básicos como salud y educación[iii].

Una primer observación que que surge sobre el uso de los fondos tiene que ver con el hecho que no se identifica de manera explícita, ninguna razón que justifique su uso para comprar tecnología de vigilancia. Los objetivos de los FSU son claros: **acceso a servicios**, provisión de servicios de **salud y educación**, y expansión de **servicios de telecomunicaciones** que no tienen nada que ver con tecnologías de vigilancia y seguridad. Además, tradicionalmente, los FSU se utilizan para llevar conectividad en lugares recónditos y para fines relacionados a disminución de brechas de acceso a Internet[2].

En contextos como el paraguayo, en donde la brecha digital de género es una realidad[iv], es imperativo encontrar mecanismos de diálogo entre distintos actores que definan cuáles son las prioridades más urgentes que un recurso como el FSU debe subsanar para beneficio de todos y todas.

Nada nuevo bajo el sol

No resulta nada nuevo ni innovador el intento de perseguir el crimen utilizando tecnologías de *"alta gama"*. Diversos Estados del Norte y Sur global, dependiendo de sus recursos y contextos, la utilizan para perseguir los fines que sus agendas priorizan. Países como Estados Unidos, Inglaterra y otras potencias se caracterizan por un fuerte discurso de **seguridad nacional** y la construcción de un *"enemigo"*, foráneo y peligroso. Luego de la Segunda Guerra Mundial, fue la amenaza del comunismo, y a principios del Siglo XXI es principalmente el *"terrorismo"*.

La solución a este problema del enemigo externo, es una *tecnosolución*, es decir, que se aplica el uso de la tecnología como la *"salvadora"* que pretende asegurar y mantener el *status quo* y modo de vida de sus sociedades.

---

1 Los FSU son un fondo administrado por la CONATEL que se encuentra financiados principalmente por el 20% de los aportes abonados por empresas operadoras de servicios de telecomunicaciones en concepto de la Tasa de Explotación Comercial.

2 Para más información sobre la manera en la cuál se ejecutan los Fondos de Servicios Universales, ingresar aquí: https://www.conatel.gov.py/index.php/2015-02-17-19-32-56/2015-02-25-12-59-40

Es así que estas sociedades se inundan de tecnologías de vigilancia, cámaras, escáners, drones, controles, aumento de policía, militarización, abundancia de armas, etc.. Muchas veces, el remedio se convierte en enfermedad.

Mirando hacia el Sur y más allá de los matices el discurso plantea similitudes: en el contexto latinoamericano, conocido por sus **tremendas desigualdades** y **falta de oportunidades**, el tejido social se caracteriza por un constante **choque de intereses** y los Estados están encargados de mantener el orden que beneficia a los más privilegiados. En ese contexto, la seguridad adquiere un papel central, traducido en el discurso clásico de prevención del crimen: *para evitarlo, todo es válido, y nada es excesivo*. Claro que acá *"el crimen"* no refiere a comunistas ni terroristas, sino a "motochorros" y ladrones de baja categoría. Por su parte, **grandes medios de difusión** son el recordatorio constante de que todo se viene abajo.

Un mapeo rápido a distintas experiencias de la región latinoamericana y países del mundo demuestran que el uso de cámaras de vigilancia y reconocimiento facial responde a un complejo entramado que para implementar sistemas altamente intrusivos que violentan los derechos fundamentales de la mayoría de la población.

Colombia y el Transmilenio

El Transmilenio es uno de los sistemas de transporte más utilizados en la ciudad de Bogotá. En ella, se transportan más de 2.560.000 pasajeros[v], una cantidad de pasajeros mayor a los habitantes de la ciudad de Asunción. El año pasado, hubo un intento fallido de implementar un sistema de video-vigilancia biométrica que generó una alerta entre defensores de derechos humanos y sectores de la ciudadanía. Estos señalaron una serie de problemas que podría generar la implementación de dicho sistema en los derechos las personas que utilizan el transporte público colombiano.

La Fundación Karisma, señala en su informe *"Cámaras Indiscretas"*[vi], que finalmente el sistema no fue implementado por una serie de factores asociados a la creación, gestión y manejo de la base de datos que hubiese sido generada por dicho sistema. Más allá del gasto que significó para el erario público, es una importante experiencia a tener en cuenta, ya que hubo todo un proceso de instalación y testeo del sistema, que finalmente no fue aplicado. El informe mencionado contiene claves para comprender en profundidad cuáles fueron los motivos que llevaron al descartar este sistema.

Chile y los drones

Con el discurso de pacificación de la región de la Araucanía[vii], el gobierno chileno anunció en 2013 el uso de drones como parte de su estrategia de contención de la región. Los medios de difusión informaron sobre licitaciones de altos montos, que alertaron a organizaciones de derechos humanos sobre el uso de este tipo de tecnología.

El dron puede verse como una cámara de seguridad con alas que es capaz de registrar las acciones de personas realizadas al aire libre, tanto en espacios públicos como privados. Los Servicios de Inteligencia y la policía han identificado los usos que pueden darse a los drones en "lucha contra el

crimen": identificación de puntos de calor y concentración de personas, registro de rostros y muchas otras funcionalidades. Organizaciones como Derechos Digitales[3] han denunciado estos usos de los drones, ya que vulneran los derechos fundamentales de las personas.

Derechos Digitales realizó solicitudes de acceso a la información, a modo de entender mejor el proceso de funcionamiento y despliegue institucional que están detrás de este tipo de tecnologías, a fin de determinar mejor a qué vulnerabilidades sería expuesta la ciudadanía.

El uso de drones se extendió posteriormente a otras regiones de Chile, generando una serie de posicionamientos y estrategias legales por parte distintas organizaciones para limitar su uso. Estos intentos de limitación fueron desestimadas por parte de la Corte Suprema y el sistema sigue adelante[4].

Estados Unidos y BIPA

En Estados Unidos, donde existen grandes empresas recolectando y monetizando información biométrica sin el consentimiento y conocimiento de usuarios, aparece un caso interesante: en el estado de Illinois, se ha promulgado una "ley de privacidad de información biométrica" (BIPA por sus siglas en inglés), que **prohíbe al sector privado** recopilar, usar o compartir información biométrica sin el consentimiento de usuarios[viii].

China no democrática

El uso de tecnologías de reconocimiento facial en la persecución del crimen, puede presentar realidades todavía más complejas en países con regímenes no democráticos, como el de China.

El gigante asiático, con su inmensa cantidad de habitantes, es un caso paradigmático: cuenta con una red interconectada de 20 millones de cámaras, potenciadas por un sistema de inteligencia artificial que almacena lo que sucede a lo largo de distintas locaciones del país y permite identificar el sexo, edad, color de piel, características de la ropa y hasta rasgos únicos de los ciudadanos. Puede reconocer también vehículos por marca, modelo y color, así como saber si los mismos están en movimiento o estacionados[ix].

Basado en *machine learning* e *inteligencia artificial*, el sistema chino se enmarca en el programa anticorrupción "Sky Net"[x] del gobierno, y se encuentra conectado a una **base de datos policial** que permite la identificación y captura de fugitivos y políticos corruptos.

De más esta decir que todo su proceso de implementación no fue transparente, y la mayoría de la ciudadanía china se enteró de su existencia luego de su inauguración. Algo parecido a lo que ha ocurrido hace pocos días en Paraguay.

3 Derechos digitales: www.derechosdigitales.org

4 Para más información sobre los argumentos en Chile en contra del uso de estos sistemas, ingresar aquí: http://www2.latercera.com/noticia/ong-derechos-digitales-rechazan-uso-naves-no-tripuladas/

Aspectos legales y tecnologías de vigilancia biométrica

Más allá de los ejemplos internacionales, vale la pena destacar que Paraguay cuenta con normativas generales para la protección de la privacidad. El **artículo 33** de la **Constitución Nacional** reconoce y garantiza el derecho a la intimidad. Además la Convención Americana sobre Derechos Humanos ("Convención Americana") ratificada el 24 de agosto de 1989, obligan al gobierno paraguayo a respetar y proteger derechos tales como: derecho a la libertad de opinión y expresión (art. 13), derecho a la reunión (art. 15) y derecho a la honra y dignidad (art. 11). Por otra parte, el Pacto Internacional de Derechos Civiles y Políticos (PIDCP), ratificado por Paraguay el 10 de junio de 1992, en sus artículos 19 y 17 sobre Privacidad y Libertad de expresión. Estos derechos están estrechamente vinculados y "el derecho a la privacidad se entiende a menudo como un requisito esencial para la realización del derecho a la libertad de expresión"[xi].

El artículo 11 de la Convención Americana protege a los individuos de "*la injerencia arbitraria o abusiva en su vida privada, en su familia, en su domicilio o en su correspondencia*" y reconoce que "*toda persona tiene derecho a la protección de la ley contra tal interferencia o ataques*". Del mismo modo, el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos (PIDCP) protege a los individuos de "*interferencias ilegales con su vida privada, su familia, su domicilio o su correspondencia, ataques ilegales a su honor y reputación*". La Observación General 16 exige que "*la legislación pertinente debe especificar en detalle las circunstancias precisas en que tales interferencias pueden ser permitidas*" y "*debe ser hecha solamente por la autoridad designada por la ley, y en cada caso particular*". Además, la recolección arbitraria de información personal por parte del gobierno constituye un acto altamente intrusivo que "*viola los derechos a la privacidad y a la libertad de expresión y puede contradecir los principios de una sociedad democrática*".

También se encuentra la **Ley 1682/2001** "*Que reglamenta la información de carácter privado*" que regula ciertos aspectos del tratamiento de datos en nuestro país, que a su vez, dista de cumplir con estándares mínimos de protección de datos personales. En este sentido, la regulación 2016/679 de la Unión Europea que entró en vigencia el pasado 25 de mayo, otorga mayor control de las personas sobre sus datos personales para mitigar los abusos del sector privado y estatal. Este un ejemplo a seguir en la consolidación de una legislación que proteja efectivamente todos los derechos anteriormente enunciados.

El ex Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión (ONU), Frank La Rue[xii] y el Alto Comisionado de Derechos Humanos (ONU), Navi Pillay[xiii]han expresado preocupación por las violaciones del derecho a la intimidad debidas a la falta de medidas de protección eficaces en la utilización de tecnologías biométricas.

Por su parte, el ex Relator Especial sobre la promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo de la ONU, Martin Scheinin, determinó en su informe publicado en el año 2009 que, si bien el uso de la biometría se presenta en determinadas circunstancias como una herramienta legítima para la identificación de sospechosos por casos de terrorismo, preocupa especialmente:

> *"los casos en que la biometría no se almacena en un documento de identidad, sino en una base de datos centralizada, incrementando los riesgos para la seguridad de la información y dejando a los individuos vulnerables. A medida que aumenta la información biométrica, las tasas de error pueden aumentar significativamente".*

El incremento en las tasas de error puede llevar a la criminalización ilícita de individuos o a la exclusión social. A la vez, el Relator destaca un aspecto que mencionamos anteriormente, la irrevocabilidad de los datos biométricos.

> *"(...) Una vez copiados y/o utilizados fraudulentamente por un actor malicioso, no es posible emitirle a un individuo una nueva firma [identidad] biométrica"*[xiv].

Anonimato en los espacios públicos, el límite de la vigilancia

La participación de las personas en el debate público sin revelar su identidad es una práctica habitual en las democracias modernas. La protección del discurso anónimo favorece la participación de las personas en el debate público ya que, al no revelar su identidad, puede evitar ser objeto de represalias injustas por el ejercicio de un derecho fundamental. De hecho, quienes ejercen el derecho a la libertad de pensamiento y de expresión toman parte en el debate público y en la vida política de una comunidad. Esto se encuentra reconocido en la Constitución Nacional en sus artículos: 26 - Libertad de expresión y 32 - De la libertad de reunión. Y también son reconocidos estos derechos por la Comisión Interamericana de Derechos Humanos (CIDH) a través de sus artículos artículo 11 y 13 respectivamente que protegen el discurso anónimo de las restricciones gubernamentales.

> *No se trata solamente de redactar "artículos de opinión" o de participar en "foros de debate", sino que también implica la capacidad de convocar movilizaciones sociales, protestas, y organizarse políticamente, entre otras -Relator Especial de la CIDH para la Libertad de Expresión, y el Internet, 2013*[xv].

El artículo 19 (3) del PIDCP y el artículo 13 (2) de la Convención Americana prevén circunstancias limitadas en las que un Estado Parte puede restringir el derecho a la libertad de expresión. De conformidad con el artículo 19 (3), estas restricciones deben ser "*previstas por la ley"* y necesarias para "*el respeto de los derechos o la reputación de los demás"* o "*para la protección de la seguridad nacional o del orden público, la salud y la moral públicas"*. Para luego aplicar el test de los principios "necesario y proporcionado" y evaluar y balancear las medidas tomadas para mitigar a través de las restricciones. De conformidad con el artículo 13 (2), la libertad de expresión no puede ser objeto de censura previa y las restricciones deben estar "*expresamente establecidas por la ley en la medida necesaria para garantizar", "el respeto de los derechos o la reputación de los demás" o "la seguridad nacional, el orden público, la salud o la moral públicas*".

Toda legislación o iniciativa que restrinja la libertad de expresión "*debe ser accesible al público"* y debe ser "*formulada con suficiente precisión para permitir que un individuo regule su conducta en consecuencia"*. Dicha legislación "*no debe conferir discrecionalidad absoluta para restringir libertad de expresión a los encargados de su ejecución"*. Además, cualquier restricción a la libertad de expresión "*debe ajustarse a estrictos criterios de necesidad y proporcionalidad"* (Comentario General N.º 34). Por

último, las medidas restrictivas "*deben ser el instrumento menos intrusivo entre aquellos que podrían lograr su función protectora; deben ser proporcionales al interés a ser protegido*" (Comentario General No. 27).

Por tanto, se observa la existencia de normativas vigentes a nivel nacional que protegen los derechos fundamentales, y que a su vez son complementadas por las interpretaciones legales y recomendaciones de expertos de organismos internacionales. En ese sentido, las autoridades nacionales deberán tenerse en cuenta para balancear las medidas intrusivas del sistema 911, a través de sus cámaras de vigilancias y software de reconocimiento facial y buscar mitigar de manera holística los delitos callejeros que por lo general son productos de la desigualdad social y económica de la población paraguaya.

La vigilancia en Paraguay, una Hidra[5] versión guaraní

Así como la inmortal Hidra de la saga de Hércules la vigilancia en Paraguay tiene múltiples cabezas y aristas a ser analizadas.

Teniendo como terrible antecedente la dictadura *stronista*, Paraguay cuenta con una tradición de vigilancia y registro del comportamiento de sus ciudadanos. Sin buscar equiparar distintas épocas, se identifica una tendencia a utilizar este tipo de mecanismos para prevenir conductas ciudadanas que pueden "salirse de lo establecido". La dictadura de Stroessner fue de las pocas de la región que mantuvo un registro pormenorizado de las actividades de sus ciudadanos así como las acciones aplicadas contra quienes desafiaban la autoridad. El Plan Condor[6] cuenta con una dolorosa base de llamada "Archivo del Terror" que está resguardada en el Palacio de Justicia en la ciudad de Asunción y da cuenta de un régimen y una transición que aún tiene mucho camino por recorrer, sobre todo en lo que refiere al esclarecimiento de lo ocurrido y al reclamo de justicia de las víctimas de la represión estatal.

Ya en nuestros días, la investigación *"Vigilancia Estatal de las Comunicaciones y Derechos Fundamentales en Paraguay"* de TEDIC arroja hallazgos preocupantes que tienen que ver con la compra de software de vigilancia altamente intrusivo por parte de entes del estado. Estas se realizaron sin estándares mínimos de control y rendición de cuentas, evidenciando así potenciales abusos por parte de funcionarios o instituciones estatales. El caso de espionaje a la periodista de ABC Color por parte de fuerzas militares vino a fortalecer dicha hipótesis, sin obtener respuestas satisfactorias por parte del gobierno[7].

Así también, la investigación *"Quien Defiende Tus Datos"*[xvi] de TEDIC levantó una serie de preocupaciones sobre la entrega de metadatos de llamadas telefónicas por parte las Proveedoras de Internet (ISP) sin orden judicial, al Ministerio Público.

5 El mito de la Hidra de Lerna: https://es.wikipedia.org/wiki/Hidra_de_Lerna
6 Para más información sobre el Plan Cóndor, ingresar aquí: https://es.wikipedia.org/wiki/Plan_C%C3%B3ndor
7 Ver detalles del caso en artículo de TEDIC: https://www.tedic.org/espionaje-a-periodista-confirma-que-el-estado-intercepta-comunicaciones-ilegalmente

Por último, la falta de regulación con respecto a este tipo de prácticas así como la violación de normativas existentes y preceptos constitucionales, complejizan mucho más la situación. A esto se suma la dificultad de la población, de comprender los peligros que representan este tipo de prácticas de vigilancia, así como lo que implica la vulneración de sus derechos fundamentales de privacidad e intimidad.

Cámaras y reconocimiento facial: un problema de varias dimensiones

En el contexto anteriormente descrito, la instalación de un nuevo sistema de vigilancia de alta gama pareciera, cuanto menos, problemático.

Más allá de las distintas problemáticas y coyunturas sobre diferentes países señalados más arriba y a modo de comprender riesgos de este tipo de vigilancia, el contexto paraguayo arroja 3 dimensiones importantes de analizar: la social, la político-institucional y la económica.

La dimensión social

La implementación de este sistema plantea serios riesgos de vulnerar –todavía más– derechos de minorías históricamente excluidas y marginadas. Para comprender mejor sobre los potenciales riesgos de exclusión, es primordial analizar a las tecnologías biométricas, los contextos y prácticas alrededor de ellas.

El reconocimiento facial, así como el reconocimiento de la huella dactilar, huella palmar, patrones de venas, iris, voces y otras exposiciones del cuerpo incluyendo ADN y la secuencia de la pulsación de las teclas, entre otros, son considerados datos biométricos. Su recolección y uso consiste en métodos automatizados que pueden reconocer de manera precisa a un individuo con base en las características físicas, biológicas o de comportamiento.

Para justificar la recolección de datos biométricos, que son datos sensibles[xvii], se debe analizar si no hay alguna alternativa que afecte en menor medida a los derechos de las personas y pueda alcanzar los objetivos que se persigue. La medida de instalación de cámaras biométricas busca prevenir cualquier tipo de ilícito en las calles de Asunción, refleja una desproporción en cuanto al fin perseguido a la vez que deja de lado del principio de una intervención mínima a través del aparato punitivo del Estado, propio de lo que se denomina *“derecho penal mínimo”*.[xviii]

Por otro lado, la nota de prensa de inauguración del sistema 911, sólo describe que pasados los 6 meses se eliminarán los datos biométricos, por lo que se vuelve indispensable garantizar que se haga efectiva dicha eliminación una vez transcurrido un periodo justificado. Por tanto, se necesita normativas que obliguen la eliminación dentro del plazo establecido y mecanismos de control y auditoría externa como forma de aumentar las garantías y salvaguardas de protección de datos personales y de los derechos humanos.

Los falsos positivos en la evidencia biométrica

Existen a nivel internacional investigaciones que concluyen que la evidencia biométrica genera un elevado número de *"falsos positivos"*, y que esto puede implicar alto riesgo de discriminación. En Inglaterra, el sistema de cámaras de reconocimiento facial tiene un 98% de "falsos positivos"[xix] y de hecho, la policía ha logrado acertar la identidad solo 2 veces[xx]desde que comenzó a implementar este sistema. De estos 2 aciertos, ninguna persona[xxi] había cometido un delito.

Por otro lado, el Congreso norteamericano revela[xxii] que el FBI almacena datos biométricos de adultos estadounidenses, con y sin consentimiento, para la búsqueda de presuntos delincuentes. Alrededor del 80% de las fotos almacenadas no pertenecen a personas con antecedentes penales, incluyen además licencias de conducir y pasaportes. Los algoritmos utilizados para identificar coincidencias son inexactos aproximadamente el 15% de las veces, y tiende a identificar erróneamente a personas afrodescendientes con mayor frecuencia que a personas de blancas.

Otro ejemplo de vulneración de derechos ocurrió cuando el software de identificación facial de Google clasificó a una pareja de afroamericanos como gorilas[xxiii] y este caso no fue el único[xxiv]. Tampoco se trata de un simple error de programación, sino una demostración de cómo los prejuicios de los programadores se trasladan al código del software, posiblemente de forma inconsciente incluso. Esto es un recordatorio de que la tecnología es producida por personas que impregnan sus ideas y defectos en ella.

En Chile, la Corte Suprema se ha expedido sobre un caso conocido como JUNAEB[xxv] y ha señalado que los datos recolectados en los colegios son sensibles en un doble sentido: por un lado, por ser datos biométricos y por otro por almacenar datos de niños y adolescentes. Por tanto debe estar sujeta a autorización expresa, informada y por escrito de los padres.

Por lo tanto se observa que algunos de los principales problemas de los programas informáticos de identificación biométrica[xxvi], están relacionados con la exactitud del software de identificación o reconocimiento facial. A partir de lo cual surgen una serie de preguntas: ¿Los algoritmos han sido probados en profundidad?, ¿Cuáles fueron los resultados de esas pruebas?, ¿Cómo fueron entrenados los algoritmos?, ¿Pueden haber conflictos con la identificación/verificación de determinadas indentidades? ¿Se ha evaluado la seguridad integral del sistema que se pretende correr?.

La dimensión político-institucional

La segunda dimensión a considerar es la político-institucional. Paraguay es un país conocido por su **debilidad institucional**, que se traduce en una serie de problemáticas que impactan en la vida de sus ciudadanos y ciudadanas, entre las que se encuentran altos índices de corrupción a todo nivel, ineficacia del sistema judicial, vulnerabilidad económica de gran parte de la población, informalidad económica, etc..

Diversas mediciones como el Latinobarómetro 2017[xxvii], colocan al país en los últimos lugares en transparencia y rendición de cuentas. Esto está estrechamente ligado con potenciales peligros sobre el almacenamiento de información personal y biométrica que surge de la instalación de estas cámaras. La falta de garantías por parte de las instituciones del orden público y la justicia pueden ser acentuadas todavía más en ésta nueva coyuntura.

Sumado a lo anterior, la falta de una **ley integral de protección de datos personales** deja al descubierto a millones de ciudadanos y ciudadanas que ven expuesta su privacidad a diario, y que a la fecha, solamente han sido mitigadas por medidas puntuales y específicas que abordan solo un aspecto de un problema mucho más amplio[8].

En ese sentido, dos investigaciones realizadas por TEDIC que abordan el manejo de datos personales en bases de datos públicas y privadas arrojan **resultados mixtos** que evidencian, una preocupante discrecionalidad en el manejo de los datos así como una determinación ad-hoc, sobre qué datos son considerados públicos y cuáles no. Esto provoca que la población quede en una "zona gris" donde la protección de sus datos personales queda a criterio de funcionarios, quiénes muchas veces no cuentan con los conocimientos legales o técnicos suficientes para resguardar los datos a su cargo.

Un análisis integral sobre la normativa de datos personales y privacidad en Paraguay puede ser encontrado en "Estado de la Privacidad en Paraguay", realizado por TEDIC en alianza con la organización Privacy International.

La dimensión económica

La última dimensión, desde donde podemos analizar la problemática de las cámaras de vigilancia es la económica: detrás de la puesta en marcha, implementación y mantenimiento de este tipo de sistemas, existen contratos millonarios del Estado con empresas privadas.

En Paraguay se sabe poco sobre este tipo de empresas. En el caso de la licitación que hace referencia a este informe, la empresa adjudicada para la implementación del sistema es *Seguridad, Vigilancia y Tecnología del Paraguay*.

En su página web, se encuentra una descripción de la misma:

- En Tecnología, Seguridad y Vigilancia del Paraguay (TSV), somos profesionales con amplia experiencia en Seguridad, Telecomunicaciones y tecnologías avanzadas
- Nuestro campo abarca soluciones de voz, datos, video y seguridad ofreciendo servicios con un alto nivel de calidad, otorgando garantías en nuestros productos y servicios
- Nuestro diseño de solución permite adaptar proyectos a la problemática de cada cliente, aportando soluciones tecnológicas flexibles competitivas y basando el éxito de nuestro trabajo en la calidad, agilidad y continua comunicación con nuestros clientes[xxviii].

Como puede observarse, la empresa posee una cartera de servicios con tecnología de amplia gama que levantan una serie de dudas sobre los clientes que compran estos servicios y el uso que se da a los mismos: ¿quiénes son sus principales clientes? ¿A qué instituciones del Estado ha proveído de

8 Un ejemplo de esto es la ley "parche" antispam: https://www.tedic.org/ley-anti-spam-es-una-ley-parche

este tipo de tecnologías? ¿Qué empresas privadas tienen potestad de instalar y utilizar este tipo de sistemas? ¿Cuáles son los mecanismos de auditoría que existen ante potenciales abusos con este tipo de sistemas?

La experiencia de Argentina puede proveer de una radiografía interesantes sobre el tema. En el capítulo "Vigilar y entretener, un modelo de negocios feliz" del libro "Guerras de Internet", la periodista Natalia Zuazo hace un detallado análisis del mercado alrededor de los sistemas de vigilancia en dicho país, evidenciando un entramado de relaciones políticas y económicas a nivel nacional e internacional. Estas relaciones facilitan y sostienen un discurso que vincula más seguridad con mayor cantidad de cámaras, sin ofrecer muchos elementos y justificaciones, pero sí generando negocios multimillonarios con gobiernos a nivel local y nacional.

En la Ciudad Autónoma de Buenos Aires (CABA), existen 3200 cámaras que vigilan y sistematizan el movimiento de 3 millones de habitantes, es decir una proporción de una cámara cada 930 habitantes. Estas cámaras son proveídas en su mayoría por pocas empresas que tienen casi un monopolio en el mercado de la seguridad:

> *"En la Argentina, tres empresas se reparten la instalación y el mantenimiento de los sistemas de videovigilancia en los municipios. No sólo venden las cámaras, sino también equipos de seguimiento satelital, dan soporte técnico y se encargan de las redes de fibra óptica necesarias para transmitir las imágenes. Las relaciones que establecen estas compañías con los municipios son vitales, ya que son ellos los que manejan los presupuestos para tecnologías de seguridad que reciben desde los gobiernos provinciales o nacionales, pero también las que otras veces deciden destinar partidas económicas propias «a pedido de los vecinos». El poder de estas empresas es el lobby y como en otros negocios de la tecnología se trata de monopolios que se reparten un territorio para vender sus productos"*[xxix].

Sumado a esto, existe cierta homogeneidad, ya que se utilizan las mismas marcas y modelos de cámaras en los distintos municipios argentinos, lo que puede evidenciar un involucramiento de poderosas multinacionales como Bosch, cuanto menos, de manera indirecta.

En Asunción, capital del país, el auge de las cámaras de vigilancia encuentra suelo fértil. Solo la Policía Nacional tiene 690 cámaras de seguridad, una por cada 760 habitantes[xxx].A lo anterior hay que sumar las cámaras en manos del sector privado, que muchas veces también son accedidos por la policía y se contabilizan en unas 3000. Cabe resaltar que Asunción y su área metropolitana son las áreas más inseguras del país, con 62.474 causas nuevas ingresadas según un informe del Ministerio Público[xxxi].

Lo anterior refuerza la hipótesis de que mayor cantidad de cámaras no implica mayores índices de seguridad. Según el Safest City Index[xxxii], Sao Paulo y Beijing se encuentran entre ciudades más inseguras del mundo a la vez que tienen la mayor cantidad de cámaras por habitante. Tokyo por su parte, tiene altísimos índices de seguridad, y una relación de cámaras por habitante mucho menor.

De lo anterior se desprenden una serie de razones que deben ser exploradas en mayor profundidad, y que hacen a la justificación e implementación de este tipo de sistemas de vigilancia en las ciudades y espacios públicos y en donde, quizá, el lucro, es un factor preponderante.

Conclusiones preliminares

Se parte del supuesto de una buena predisposición por parte del Estado a la hora de asegurar el bienestar de todos sus ciudadanos. Sin embargo, un análisis más profundo del entramado económico y de poderes que están detrás de estos tipos de sistemas, ayuda a comprender mejor las motivaciones y riesgos que se esconden detrás de los mismos.

Para determinar qué tan efectiva puede ser la implementación de un sistema como este, se deben analizar el marco teórico sobre la criminalidad y la experiencia histórica subyacente, el marco legal nacional e internacional, y también el tipo de actores implicados, tanto públicos como privados.

La situación se agrava en el contexto actual, en donde este sistema de video vigilancia biométrica ***ya está*** siendo aplicado. Más allá de que estas cámaras con reconocimiento facial aún sean pocas y estén distribuidas en pocos puntos, se asume que el proyecto es de mayor escala y busca replicarse en otros puntos con mayor tránsito de personas.

Intentando comprender al ciclo de políticas públicas como un proceso que apunte a ser más democrático y participativo –y tomando el ejemplo de "gobierno abierto" como camino medianamente exitoso hacia ese ideal– se evidencia que el actual proceso de implementación de las cámaras de video vigilancia, carece de un un componente democrático y de transparencia. No existieron procesos de consulta pública para determinar si la ciudadanía está de acuerdo con este tipo de mecanismos de vigilancia, ni se facilitó la totalidad de la información para dar la oportunidad de una decisión informada y legítima por parte de todos y todas relacionado al tema.

Surgen además una serie de preguntas que tienen que ver con: ¿quiénes tienen permisos de acceso a la información generada por estas cámaras? ¿con qué de base de datos se alimenta qué actores tienen acceso total a los registros? ¿cómo son los resguardos y medidas de seguridad correspondientes sobre estos sistemas? Todas son preguntas que deben estar públicamente disponibles y deberían responderse con los más altos estándares de protección, si es que se apunta a generar algún tipo de confianza en estos sistemas.

Paraguay debe transitar hacia una "nueva era" en políticas de seguridad que busque tener un enfoque holístico e integral, que se formule con metodologías de múltiples partes interesadas y garantice el respeto irrestricto de los derechos humanos. Este se vuelve un ejercicio fundamental en un contexto político y social, donde un único partido ha tenido la hegemonía en el gobierno y el presidente entrante pertenece a una familia directamente vinculada a la dictadura más larga de Latinoamérica[xxxiii].

La vigilancia biométrica es una amenaza creciente para la privacidad. La información biométrica se puede recolectar a distancia y sin conocimiento expreso de las personas. A esto se suma el hecho de que las personas no poseen la capacidad para protegerse de esta intromisión y posibles abusos de privacidad.

Recomendaciones

La recolección de masiva de datos biométricos es innecesaria y desproporcionada. Esta iniciativa es intrusiva y desproporcionada porque recolecta datos sensibles de las personas que circulan en espacios públicos, independientemente de si han sido o sospechosas de conductas indebidas y sin ninguna garantía aparente. La recolección indiscriminada de datos sensibles debe buscar otra medida menos intrusiva para prevenir la actividad fraudulenta.

Se necesita transparencia del software de datos biométricos y su uso y alcance. Falta información mediante la cual se pueda conocer acerca de la tecnología y mecanismos utilizados para la vigilancia biométrica, debido a la amenaza creciente contra la privacidad.

El gobierno y las autoridades deben concentrar sus esfuerzos en implementar políticas basadas en evidencia. Deben analizar previamente el contexto y las medidas a tener en cuenta para la persecución de los delitos, y evaluar para que único impacto no sea beneficiar a la industria de la vigilancia, sino la calidad de vida de las personas.

Paraguay necesita una ley de protección de datos personales. Falta de marcos jurídicos suficientes que permitan garantizar un adecuado tratamiento de datos biométricos recolectados, tanto por parte del Estado como el sector privado. En especial su recolección, análisis y almacenamiento de datos biométricos, así como los alcances de esta políticas.

Próximos pasos

Si bien las notas de prensa nacional cubrieron la adquisición de estos dispositivos, no se indagó sobre los detalles de la operación, ni la normativa que rige para el funcionamiento de estos dispositivos en nuestro país. En este marco, TEDIC realizó el 7 de julio, solicitud de acceso a la información pública que está actualmente en curso.

Estas son algunas de las preguntas y preocupaciones presentadas a través de dicha herramienta:

- ¿Cuáles son todas las políticas y procedimientos relativos a la recopilación y retención de bases de datos de información personal (biométrica)? Esto puede incluir información que explique dónde se almacenará la información, quién tendrá acceso a la información y cuánto tiempo se mantendrá la información.
- ¿Se prevén salvaguardas para evitar la manipulación y adulteración de las copias de los datos biométricos almacenados? ¿Qué instituciones del Estado van a acceder a esos datos? ¿Se podrá garantizar que la solicitud de los datos biométricos se haga mediante una orden judicial previa? ¿Habrán sanciones en caso de abusos por parte de los responsables de las bases de datos o de las autoridades?
- ¿Cuáles son las políticas de eliminación de los datos biométricos de la base de datos? ¿Cómo se implementa y quién la controla?
- ¿Implementarán informes de transparencia del uso de la herramienta de video-vigilancia y reconocimiento facial?

- ¿Qué salvaguardas tienen previstos para la protección de los datos sensibles? ¿Cómo será el cifrado de las bases de datos? ¿Cómo se garantizará integridad de los datos personales, y la seguridad del sistema de las bases de datos?

Una vez obtenida dicha información, la misma será debidamente publicada a través de los distintos canales de comunicación de la organización, a modo de tener una comprensión más profunda sobre el tema, y poder determinar cuáles serán los próximos pasos colectivos relacionados al tema, y también para sensibilizar a la ciudadanía sobre el tema.

i Licitación Pública FSU N° 2/2017 (2017) Para el otorgamiento de subsidio a través del fondo de servicios universales para la expansión del sistema de atención y despacho de llamadas de emergencia-sadle 911 de la Policía Nacional para la ciudad de Asunción y Área Metropolitana". Recuperado de: https://www.conatel.gov.py/images/iprincipal/2017/Noviembre/Licitaci%C3%B3n%20Publica%20FSU%20N%C2%B02/CIRCULAR%201%20-%20Licitacion-2-2017.PDF

ii Contrato 53/2017 (2017). Para el otorgamiento de subsidio a través del fondo de servicios universales para la expansión del sistema de atención y despacho de llamadas de emergencia-sadle 911 de la Policía Nacional para la ciudad de Asunción y Área Metropolitana. Recuperado de: https://www.conatel.gov.py/images/2015-2/FSU_CONTRATOS/CONTRATO%2053-17.PDF

iii CONATEL. Fondos de Servicios Universales: Delineamientos Generales. Recuperado de: https://www.conatel.gov.py/index.php/2015-02-17-19-32-56/2015-02-25-12-57-51

iv Acuña, J. (2018) Derechos en línea de la Mujer: Reporte de Calificaciones. Recuperado de: https://www.tedic.org/a-mitad-de-camino-de-la-igualdad-digital-auditoria-arroja-resultados-mixtos-de-paraguay/

v Transmilenio (2018) Colombia, segundo país en Latinoamérica en movilizar pasajeros en sistema de transporte BRT. Recuperado de: http://www.transmilenio.gov.co/Publicaciones/colombia_segundo_pais_en_latinoamerica_en_movilizar_pasajeros_en_sistemas_de_transporte_brt

vi Sáenz, P. & Spanger A., (2018) Cámaras Indiscretas: Análisis del fallido sistema de videovigilancia inteligente para Transmilenio. Recuperado de https://karisma.org.co/camaras-indiscretas/

vii Derechos Digitales (2014). ¿Es un pájaro? ¿Es Superman? ¡No, es un "drone"! Vigilancia y nuevas tecnologías en La Araucanía. Recuperado de: https://www.derechosdigitales.org/6796/es-un-pajaro-es-un-superman-es-un-drone-vigilancia-y-nuevas-tecnologias-en-la-araucania

viii Juárez, L (2018) Illinois encara a empresas con ley de privacidad biométrica. Mediatelecom. Recuperado de https://tecnologia.mediatelecom.com.mx/2018/07/06/illinois-encara-a-empresas-con-ley-de-privacidad-biometrica/

ix Álvarez, R (2017) 20 millones de cámaras equipadas con inteligencia artificial hacen que China sea el verdadero "Gran Hermano". Xataka.Recuperado de: https://www.xataka.com/privacidad/20-millones-de-camaras-equipadas-con-inteligencia-artificial-hacen-que-china-sea-el-verdadero-gran-hermano

x Redacción EC (2017) Sky Net": así funciona el complejo sistema de cámaras de seguridad en China. El Comercio. Perú. Recuperado de: https://elcomercio.pe/tecnologia/actualidad/sky-net-funciona-complejo-sistema-camaras-seguridad-china-noticia-461131

xi Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue* A/HRC/23/40. ONU – Abril 2013.

xii Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue* A/HRC/23/40. ONU – Abril 2013.

xiii UN News Centre, UN rights chief urges protection for individuals revealing human rights violations. ONU – Julio 2013.

xiv La identidad que no podemos cambiar. Asociación por los derechos civiles (ADC). Abril 2017.

xv Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue* A/HRC/23/40. ONU – Abril 2013.

xvi Sequera, M. (2017) Quien Defiende Tus Datos. Asunción: TEDIC. Recuperado de: https://qdtd.tedic.org/

xvii Datos biométricos https://www.tedic.org/la-desproporcionalidad-del-proyecto-de-ley-para-la-activacion-de-servicio-de-telefonia-movil-incumple-estandares-de-tratamiento-de-datos-biometricosThe Perpetual Line-up: Unregulated Police Face Recognition in America", C. Garvie, A. Bedoya, J. Frankle, Center on Privacy & Technology, Georgetown University Law School, octubre 2016, P.49. https://www.perpetuallineup.org-huella-dactilar/

xviii "Derecho penal mínimo significa la reducción al mínimo de las circunstancias penales y su codificación general mediante la despenalización de todas aquellas conducta que no ofendan bienes fundamentales y que saturan el trabajo judicial con un dispendio inútil e inocuo de aquel recurso escaso y costoso que es la pena y tienen el triple efecto del debilitamiento general de las garantías, de la ineficacia de la maquinaria judicial y de la devaluación de los bienes jurídicos merecedores de tutela penal." Ferrajoli, Luigi. Crisis del sistema político y jurisdicción: la naturaleza de la crisis italiana y el rol de la magistratura. Revista Pena y Estado año 1 número 1–Argentina 1995: Editores del Puerto s.r.l. p. 113.

xix El reconocimiento facial de Inglaterra es un fiasco y podría representar un riesgo. https://www.fayerwayer.com/2018/07/reconocimiento-facial-inglaterra/ Junio 2018.

xx Zero arrests, 2 correct matches, no criminals: London cops' facial recog tech slammed https://www.theregister.co.uk/2018/05/15/met_police_slammed_inaccurate_facial_recognition/ .Mayo 2018

xxi The Perpetual Line-up: Unregulated Police Face Recognition in America", C. Garvie, A. Bedoya, J. Frankle, Center on Privacy & Technology, Georgetown University Law School, octubre 2016, P.49. https://www.perpetuallineup.orgLondon's top cop isn't expecting facial recog tech to result in 'lots of arrests' https://www.theregister.co.uk/2018/07/04/met_police_commish_im_not_expecting_facial_recognition_tech_to_result_in_lots_of_arrests/ Julio 2018

xxii Facial recognition database used by FBI is out of control, House committee hears https://www.theguardian.com/technology/2017/mar/27/us-facial-recognition-database-fbi-drivers-licenses-passports

Marzo 2017.
xxiii Google pide perdón por confundir a una pareja negra con gorilas http://www.bbc.com/mundo/noticias/2015/07/150702_tecnologia_google_perdon_confundir_afroamericanos_gorilas_lv Julio 2015.
xxiv Facial recognition database used by FBI is out of control, House committee hears https://www.theatlantic.com/technology/archive/2016/04/the-underlying-bias-of-facial-recognition-systems/476991/ Abril 2016.
xxv Biometría: tecnosolucionismo a costa de nuestros derechos https://www.derechosdigitales.org/11333/biometria-tecnosolucionismo-a-costa-de-nuestros-derechos/
xxvi The Perpetual Line-up: Unregulated Police Face Recognition in America", C. Garvie, A. Bedoya, J. Frankle, Center on Privacy & Technology, Georgetown University Law School, octubre 2016, P.49. https://www.perpetuallineup.org
xxvii Corporación Latinobarómetro (2017). Latinobarómetro. Buenos Aires. Recuperado de http://www.latinobarometro.org/latNewsShow.jsp
xxviii TSV. La Empresa ¿Quiénes Somos? Recuperado de: http://www.tsv.com.py/empresa.php
xxix Zuazo, N (2015). Vigilar y entretener, un modelo de negocios feliz. En: *Guerras de Internet*. 1era Edición. Buenos Aires. Debate
xxx El Surtidor; TEDIC (2017) El Retorno de los Pyrawebs. elsurti. Asunción. Recuperado de: https://elsurti.com/pyrawebs/
xxxiÚltima Hora (2015) El hurto, el robo y manejar ebrio, entre los delitos más frecuentes a nivel país. Última Hora. Recuperado de: https://www.ultimahora.com/el-hurto-el-robo-y-manejar-ebrio-los-delitos-mas-frecuentes-nivel-pais-n864994.html
xxxii The Economist (2017) Safe Cities Index 2017. Recuperado de: http://safecities.economist.com/safe-cities-index-2017
xxxiii Acuña, J. (2018). Los hombres del dictador siguen en el poder. Asunción: Kurtural. Recuperado de: https://kurtural.com/loshombresdeldictador/

Decir “no tengo nada que esconder”
no es una respuesta válida
cuando se vulneran nuestros derechos