FUNDAMEDIOS

La videovigilancia en Ecuador vulnera derechos ciudadanos

2021

Ecuador avanza hacia la vigilancia biométrica sin protección jurídica

La videovigilancia en Ecuador vulnera el derecho a la privacidad, a la intimidad y a la asociación pacífica. Esta situación se agravará con la implementación de inteligencia artificial y la puesta en funcionamiento de sistemas de reconocimiento facial. Las leyes ecuatorianas no protegen adecuadamente a los ciudadanos de la vigilancia masiva, por lo que se requiere con urgencia regulación específica que controle la implementación de esta tecnología prevista a partir de diciembre de 2021. La ONU pidió la moratoria en su implementación hasta que no haya garantías de protección de los derechos ciudadanos. En consonancia con ello, Fundamedios exhorta a las entidades públicas a abstenerse e implementar tecnologías de vigilancia biométrica.

Gracias al apoyo de:

@ | DERECHOSDIGITALES
Derechos Humanos y Tecnología en América Latina

Investigación de Fundamedios realizada por:

Maria Fernanda Almeida
Sonia Romero
Dagmar Thiel

Diseño y diagramación:
Mary Liseth Donoso

30 de noviembre 2021

CONTENIDO

CONTENIDO

INTRODUCCIÓN

La videovigilancia es un sistema que combina la tecnología audiovisual con redes de comunicación con el objeto de supervisar imágenes, comportamientos, perfiles de ciudadanos y el entorno en espacios públicos o privados para alertar sobre situaciones de emergencia o que estén fuera del orden normal.

Fortalecer la seguridad ciudadana y reducir los índices de criminalidad han sido las razones de gobiernos locales y nacionales de todo el mundo para expandir el alcance de la vigilancia masiva.

Con la implementación de inteligencia artificial muchos países han pasado de la videovigilancia a la tecnología de reconocimiento facial. Un software específico permite que imágenes captadas con cámaras de mayor resolución puedan ser cruzadas con bases de datos, con el propósito de que el rostro humano captado sea identificado. Para ello se consideran a los datos biométricos como las características físicas o inferencias de características como la etnia, el género, la edad y condición de discapacidad.

La vulneración de los derechos humanos, así como errores de identificación que han afectado de manera especial a las poblaciones más vulnerables, han llevado a cuestionar la videovigilancia y en particular el reconocimiento facial. Human Rights Watch y Amnistía Internacional, entre muchas otras organizaciones, han pedido desde 2020 que se prohíba el uso, desarrollo, producción, venta y exportación de tecnología de reconocimiento facial con fines de vigilancia masiva por la policía y otros organismos del Estado[1]. Su pedido se respalda en investigaciones que han demostrado que los sistemas de reconocimiento facial procesan algunos rostros con más precisión que otros, dependiendo de características claves como el color de la piel, la etnia y el género.

La preocupación por las potenciales violaciones a los derechos humanos con el uso de inteligencia artificial en servicios públicos es tal, que en septiembre de 2021, la alta comisionada para los derechos humanos de la ONU, Michelle Bachelet, hizo público el reporte de la organización en el que destacan los efectos catastróficos del uso de la inteligencia artificial y la afectación a los derechos de las personas. Por ello pidió la moratoria en su uso. "El documento también defiende una moratoria en el uso de las tecnologías biométricas en los espacios públicos, especialmente en el control de las personas en la calle. Esta medida se aplicaría al menos hasta que las autoridades demuestren que los sistemas cumplen con altos estándares de privacidad y protección."[2]

1 Amnistia Internacional, Amnistia Internacional pide que se prohiba el uso de tecnología de reconocimiento facial con fines de vigilancia masiva, Junio 2020. https://www.amnesty.org/es/latest/research/2020/06/amnesty-international-calls-for-ban-on-the-use-of-facial-recognition-technology-for-mass-surveillance/

2 ONU, UN News Bachelet asks for moratorium on sale and use of Artificial Intelligence, 15 Septiembre 2021, https://news.un.org/pt/story/2021/09/1763212

Por otro lado, esta tecnología recopila datos personales sensibles de manera masiva y generalizada, sin sospecha razonable e individualizada de delito, lo que constituye una vigilancia masiva e indiscriminada. La captación indiscriminada de datos biométricos vulnera los derechos a la privacidad, a la libertad de expresión, de asociación y de reunión pacífica.

En 2019, el relator especial de las Naciones Unidas sobre la libertad de opinión y de expresión, David Kaye, cuestionó el uso de esta tecnología para perseguir a políticos, periodistas y activistas. "Los sistemas de vigilancia pueden interferir con los derechos humanos, desde el derecho a la privacidad y la libertad de expresión hasta los derechos de asociación y reunión, las creencias religiosas, la no discriminación y la participación pública. Sin embargo, no están sujetos a ningún control efectivo ni a nivel mundial ni nacional", mencionó[3].

En Ecuador el despliegue masivo de la videovigilancia e inminentes contrataciones de equipos para reconocimiento facial llevaron a Fundamedios a hacer una investigación sobre la potencial vulneración de derechos ciudadanos con la creciente generalización de la vigilancia de los espacios públicos.

Durante el segundo semestre de 2021, con el apoyo de Derechos Digitales, Fundamedios revisó decretos, contratos públicos y resoluciones ministeriales; realizó más de 25 peticiones de información pública a varias instituciones, y alrededor de 12 entrevistas a funcionarios públicos, privados y expertos para comprender cómo funciona este sistema en Ecuador. Preguntamos ¿qué tipo de tecnología se utiliza, qué protocolos se implementan y si los sistemas instalados se interconectan con bases de datos de los ciudadanos del Registro Civil o de la Policía Nacional? La investigación se centra en información de ECU 911, y los municipios de Guayaquil, Quito, Cuenca y Latacunga.

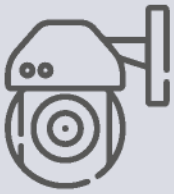
Fundamedios además realizó un análisis legal para evaluar si los sistemas de videovigilancia vulneran o no los derechos de los/las ciudadanas; y si la nueva normativa de Protección de Datos Personales prevé la protección de los derechos ciudadanos ante las tecnologías como el reconocimiento facial. Para ello revisamos el marco legal vigente así como denuncias presentadas a la Defensoría del Pueblo y más de 51 sentencias relacionadas con el artículo 178 del Código Orgánico Integral Penal referido a la violación de los derechos de intimidad. Además investigamos las cuentas sociales y el uso promocional dado a las imágenes captadas por el ECU 911 y otras instituciones que usan la videovigilancia.

Al finalizar este estudio, Fundamedios concluye que en Ecuador los sistemas de videovigilancia actualmente operativos violan los derechos humanos. Al no existir en el país las garantías necesarias para la implementación del reconocimiento facial, y en consonancia con la Oficina de la Alta Comisionada de Derechos Humanos de la ONU, Fundamedios exhorta a las entidades públicas a abstenerse de implementar mecanismos de vigilancia biométrica, como es el reconocimiento facial, a la Asamblea Nacional a regular con precisión el funcionamiento de la videovigilancia para que cumpla con estándares de derechos humanos. Y a la ciudadanía defender su derecho a la privacidad e intimidad.

[3] ONU, UN News, Un experto pide regular el uso de las herramientas de vigilancia para que cumplan con los derechos humanos, 25 junio 2019, https://news.un.org/es/story/2019/06/1458401

PRINCIPALES HALLAZGOS

1. Información clave sobre el funcionamiento del procesamiento de **datos personales de los ecuatorianos es considerada de carácter reservado** desde la creación del ECU 911 en el gobierno de Rafel Correa. La reserva permanece hasta el 2028.



2. **La ineficiencia marcó la falta de operación de las primeras cámaras de reconocimiento facial. En las cuatro ciudades analizadas existen 353 cámaras con capacidad de reconocimiento facial,** cuya compra representa casi 3 millones de USD. La falta de conexión y software compatible con las bases de datos no permiten su operación. **Pero hacia finales de 2021 se planea la instalación masiva de esta tecnología.**

3. **En las compras de equipamiento para videovigilancia o reconocimiento facial,** únicamente consideran justificaciones para reducir la criminalidad, pero las entidades públicas que lo adquieren **no realizan análisis respecto a limitaciones jurídicas o afectación a derechos humanos** antes de su implementación, contraviniendo las disposiciones de ONU para que los gobiernos hagan debida diligencia de posible afectación de derechos humanos en la implementación de inteligencia artificial.

4. **La mitad de las adquisiciones** de equipamiento para videovigilancia hechas por ECU 911 entre 2012 y 2017 fueron con créditos chinos y se **adjudicaron a la empresa estatal China National Electronic Import (CEIEC). Aunque el contrato venció en 2018, se mantienen las condiciones para la contratación de los servicios de mantenimiento de los sistemas bajo régimen especial y sin concurso públic**o al proveedor chino.

5. **Los responsables de la videovigilancia ignoran que el rostro es un dato sensible que merece protección especial.** La mayoría de **los funcionarios** entrevistados o entidades que respondieron a los pedidos de información **no son conscientes de la captación de datos sensibles personales a través de las cámaras y de las potenciales vulneraciones de derechos humanos.**

6. La Constitución del Ecuador garantiza la protección de los datos personales y la recientemente aprobada Ley de Protección de Datos prohíbe el tratamiento de los datos sensibles, como son los datos biométricos. Pero **no existe en la normativa un señalamiento específico que reconozca la protección de los datos personales obtenidos mediante cámaras de videovigilancia (ni la tecnología de reconocimiento facial), ni establece las limitaciones** adecuadas.

7. Al haber omisiones legales **tampoco se contemplan políticas públicas que incluyan la capacitación de servidores y operadores judiciales** en la protección del derecho a la privacidad potencialmente vulnerado con la videovigilancia y en mayor medida con el reconocimiento facial. Es fundamental **capacitar a los funcionarios públicos sobre los riesgos asociados a la captación masiva de datos biométricos** y el derecho a la privacidad de los ciudadanos y derechos asociados.

8. **Es importante elevar la conciencia de la población ecuatoriana sobre su derecho a la intimidad.** La investigación concluye que los ciudadanos no lo defienden ni exigen su respeto a la privacidad.

9. Las instituciones públicas **utilizan indiscriminadamente las imágenes de videovigilancia para campañas de comunicación o de relaciones públicas, vulnerando el derecho a la privacidad de los ciudadanos.** Estas imágenes sólo deberían ser accesibles con orden judicial y para fines de investigación.

10. Las entidades proporcionan limitada información respecto al uso de la videovigilancia por lo que consideramos que **no existe suficiente transparencia** respecto al manejo de datos personales de los ciudadanos.

11. **En Ecuador no se cumplen los estándares internacionales de derechos humanos** que establecen que los estados deben tomar medidas eficaces para impedir la retención, el procesamiento y el uso ilegales de datos personales almacenados por las autoridades públicas y por empresas.

12. La simple existencia de sistemas secretos de vigilancia interfieren con el derecho a la privacidad. **Estas técnicas sólo deben contemplarse cuando existan indicios concretos del cometimiento real de un delito grave, como la violencia o el uso de armas de fuego..**

13. Tampoco se cumple la recomendación hecha por el Relator Especial de Libertad de Opinión y Expresión de la ONU para que la videovigilancia sea selectiva y se aplique únicamente cuando hay sospecha de delito. **La vigilancia indiscriminada vulnera además el derecho de reunión pacífica.**

14. ECU 911, Policía Nacional y varios municipios **avanzan en los procesos de compra masiva de software y equipos que habiliten el reconocimiento facial** hacia finales de 2021 y 2022, sin que se hayan considerado las vulneraciones de derechos humanos.

PRIMER CAPÍTULO

Análisis jurídico de vulneración del derecho a la privacidad, intimidad y protección de datos personales

Diagnóstico de la videovigilancia, reconocimiento facial y violaciones de derechos.

El derecho a la privacidad desempeña un papel fundamental en el ejercicio de otros derechos humanos, que incluyen la libertad de expresión, libertad de asociación y reunión, hasta el acceso y goce de los derechos económicos sociales y culturales. El derecho a la vida privada se aplica por igual a todas las personas. La existencia de diferencias en cuanto a su protección de este derecho por cualquier motivo es incompatible con el derecho a la igualdad y no discriminación consagrados en el artículo 26 del Pacto Internacional de Derechos Civiles y Políticos.

La privacidad, de conformidad con instrumentos internacionales, se entiende como la esfera de desarrollo autónomo, interacción libre de la intervención del Estado y de la intervención excesiva no solicitada de otros individuos[4]. Por esta razón, la protección que debe darse a este derecho es amplia y no puede limitarse a los espacios privados, sino también a los espacios públicos y a la información de acceso público. Para ello deben considerarse los estándares de derechos humanos internacionales y nacionales existentes, pues estos contienen principios necesarios para la garantía de este derecho como la no arbitrariedad, legitimidad, legalidad, necesidad y proporcionalidad en relación con las prácticas de vigilancia.

El desarrollo tecnológico ha llevado a que la vida privada esté expuesta cuando los gobiernos llevan a cabo actividades de identificación, rastreo, establecimiento de perfiles, reconocimiento facial o calificación de las personas a través de los sistemas de vigilancia. Estas acciones constituyen actos intrusivos que violan y vulneran el derecho a la privacidad e interfieren con el ejercicio de otros derechos. Si bien las cámaras de vigilancia cuando son utilizadas de forma adecuada, legal y legítima, pueden contribuir a garantizar la identificación de violencia, cuando no son utilizadas de forma legítima pueden ser instrumentos que facilitan el cometimiento de distintas vulneraciones de derechos, por ejemplo con la implementación del reconocimiento facial.

Ésta tecnología consiste en la comparación de la representación digital de un rostro capturado en una imagen digital o "plantilla" con otras plantillas de una base de datos. La comparación que se realiza entre estas distintas bases de datos permite deducir la probabilidad que la persona sea objeto de autenticación o identificación a criterio del usuario del sistema[5].Por lo tanto, el uso de esta tecnología representa importantes riesgos para el goce de ciertos derechos como la señalización inexacta de personas como sospechosas de cometer un delito; el refuerzo y amplificación de la discriminación de personas que históricamente se han encontrado en situaciones de desigualdad (se ha demostrado que las cifras de precisión en el caso de reconocimiento de personas de piel oscura y mujeres son menores)[6], así como las distintas vulneraciones generadas a los derechos a la libertad de expresión y la reunión pacífica.

Un estudio del Instituto Nacional de Estándares y Tecnología NIST (EE.UU.) indicó que se midieron tasas hasta 100 veces más altas de falsos positivos en personas afroamericanas, asiáticas y, en particular, mujeres afroamericanas en comparación a las personas blancas[7]. Esto podría, según Amnistía Internacional, exacerbar el riesgo de que la policía cometa violaciones de derechos humanos en las

4 Informe anual del Alto Comisionado de las Naciones Unidas para los Derechos Humanos e informes de la Oficina del Alto Comisionado y del Secretario General. 3 de agosto de 2018 Resolución A/HRC/39/29

5 Informe anual del Alto Comisionado de las Naciones Unidas para los Derechos Humanos e informes de la Oficina del Alto Comisionado y del Secretario General, 24 de junio de 2020, A/HRC/44/24.

6 Joy Buolamwini y Timnit Gebru, "Gender shades: intersectional accuracy disparities in commercial gender classification", Proceedings of Machine Learning Research, vol. 81 (2018), págs. 1 a 15; e Inioluwa Deborah Raji y Joy Buolamwini, "Actionable auditing: investigating the impact of publicly naming biased performance results of commercial AI products", Conferencia sobre Inteligencia Artificial, Ética y Sociedad (2019).

7 EL COMERCIO, Tecnología de reconocimiento facial presenta errores masivos, según estudio del gobierno de Estados Unidos

comunidades negras o indígenas, al cometer errores en la supuesta identificación de sujetos, por ejemplo, sospechosos de un crimen y acusados erróneamente debido a falencias de la inteligencia artificial. Los investigadores de NIST, también encontraron que dos algoritmos asignaron el género incorrecto a las mujeres negras, casi el 35% de las veces.

Por estas razones, distintos organismos internacionales han recalcado la importancia de contar con una normativa adecuada, así como políticas públicas que se amparen en los estándares internacionales para disminuir estos riesgos.

La Declaración Universal de Derechos Humanos en su artículo 12 establece que nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. En concordancia el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos señala que toda persona tendrá derecho a la protección de la ley contra injerencias o ataques.

La Carta Iberoamericana de Gobierno Electrónico señala que el uso de comunicaciones electrónicas promovidas por la Administración Pública debe tener observancia de las normas en materia de protección de datos personales con el objetivo de precautelar el derecho de las personas a la privacidad.

La observación general núm. 16 (1988) del Comité de Derechos Humanos sobre el derecho a la intimidad ha recomendado a los Estados a tomar medidas eficaces para impedir la retención, el procesamiento y el uso ilegales de datos personales almacenados por las autoridades públicas y las empresas .

El Relator Especial sobre el derecho a la libertad de reunión pacífica y de asociación en su Informe sobre los derechos a la libertad de reunión pacífica y de asociación del año 2019, pidió que se prohíba la vigilancia indiscriminada y no selectiva de quienes ejercen su derecho de reunión pacífica en espacios tanto físicos como digitales. Estableció que dicha vigilancia sólo debe realizarse de manera selectiva cuando exista una sospecha razonable de cometer o planear cometer delitos graves, de acuerdo a los principios de necesidad y proporcionalidad bajo control judicial.[8]

El Comité Jurídico Interamericano de la Organización de Estados Americanos-OEA adoptó la declaración de principios de privacidad y protección de datos personales en las Américas, a partir de lo cual desarrolló un proyecto de Ley Modelo sobre protección de datos personales.

En el reporte de la Oficina de la Alta Comisionada de Derechos Humanos sobre la afectación de la inteligencia artificial a los derechos humanos, publicado el 15 de septiembre de 2021 la organización destaca la interferencia del reconocimiento biométrico remoto, que es el ejercido con cámaras de reconocimiento facial, en el derechos a la privacidad de los ciudadanos.

En el reporte señala expresamente que “el reconocimiento biométrico a distancia aumenta drásticamente la capacidad de las autoridades estatales para identificar y rastrear sistemáticamente a las personas en los espacios públicos, lo que socava la capacidad de las personas para llevar a cabo 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.”[9]

Bajo estas consideraciones, la ONU exhorta a los estados a que

(a) Respeten y protejan el derecho a la privacidad, incluso en el contexto de las comunicaciones digitales y las tecnologías digitales nuevas y emergentes;

(b) Adopten medidas para poner fin a las violaciones y los abusos del derecho a la intimidad y creen las condiciones necesarias para prevenirlos, entre otras cosas garantizando

[8] Informe del Relator Especial sobre los derechos a la libertad de reunión pacífica y de asociación, 17 de mayo de 2019, A/HRC/41/41.

[9] HUMAN RIGTHS COUNCIL, ADVANCED EDITION, 13 septiembre 2021, A_HRC_48_31_REport on Privacy on DIgital Age Sep 2021

que la legislación nacional pertinente cumpla las obligaciones que les incumben en virtud del derecho internacional de los derechos humanos;
(...)

(e) Garanticen que las tecnologías de identificación y reconocimiento biométrico, incluidas las tecnologías de reconocimiento facial por parte de agentes públicos y privados, no permitan la vigilancia arbitraria o ilegal, incluso de quienes ejercen su derecho a la libertad de reunión pacífica;"[10]

A nivel nacional la Constitución de la República en su artículo 66 numeral 19 reconoce y garantiza a las personas el derecho a la protección de datos de carácter personal, que incluye el acceso a la decisión sobre información y datos de este carácter, así como su correspondiente protección; asimismo, señala que la recolección, archivo, procesamiento, distribución o difusión de estos datos personales requieren de la autorización del titular o el mandato de ley.

Por otro lado en el artículo 92 de la misma Constitución se establece que toda persona tiene el derecho a conocer de la existencia y acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico, así como el derecho a conocer el uso que se haga de ellos, su finalidad, origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos.

La Acción Estratégica clave del enfoque para Gobierno de protección de datos personales del Eje 6 del Plan Nacional de la Sociedad de la Información y del Conocimiento 2018-2021 señala la necesidad de promulgar una Ley Orgánica de protección de datos personales para garantizar el derecho constitucional .

En este sentido, el 26 de mayo de 2021 entró en vigencia la Ley Orgánica de Protección de Datos Personales misma que define en su artículo 4 a los datos personales como todo dato que identifica o hace identificable a una persona natural directa o indirectamente; y, al dato genético como el dato personal único relacionado a características genéticas heredadas o adquiridas de una persona natural que proporciona información única sobre la fisiología o salud de un individuo.

Pese a la existencia de esta normativa en Ecuador se ha detectado la vulneración de estos preceptos jurídicos debido a la videovigilancia indiscriminada, la difusión de las imágenes con fines de relaciones públicas y la falta de transparencia en los protocolos de manejo y archivo de la información recopilada.

Desde un enfoque jurídico, estas vulneraciones se pueden atribuir a dos causales específicas:

Falta de normativa específica que proteja los datos personales sensibles del reconocimiento facial con cámaras de videovigilancia.

La Asamblea Nacional del Ecuador aprobó por unanimidad la Ley Orgánica de Protección de Datos Personales que entró en vigencia el 26 de mayo del 2021. Este cuerpo legal fue producto de extensos debates desarrollados en el órgano legislativo que contaron con aportes de distintas organizaciones de la sociedad civil.

Este cuerpo normativo abarca ampliamente la protección de datos personales a través de un registro nacional de protección de datos, la creación de una Superintendencia de Protección de Datos Personales y la sanción de quienes incumplan dicha normativa. Entre sus definiciones la norma señala al dato biométrico como el dato personal único relativo a las

[10] HUMAN RIGTHS COUNCIL, ADVANCED EDITION, 13 septiembre 2021, A_HRC_48_31_REport on Privacy on DIgital Age Sep 2021

características físicas o fisiológicas, o conductas de una persona natural que permita o confirme la identificación única de dicha persona como imágenes faciales o datos dactiloscópicos, entre otros.

En este sentido, la normativa considera de forma correcta la imagen de una persona como un dato personal pues constituye uno de los atributos fundamentales de su personalidad al revelar características únicas que la distinguen de otras. Por lo tanto, el grabar, analizar y conservar las imágenes faciales de alguien sin su consentimiento constituye una injerencia en el ejercicio de su derecho a la privacidad.

Sin embargo, el literal f) artículo 2 de esta Ley Orgánica señala que el contenido de la misma no será aplicado a datos o bases de datos establecidos para la prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, llevado a cabo por los organismos estatales competentes en cumplimiento de sus funciones legales. En cualquiera de estos casos deberá darse cumplimiento a los estándares internacionales en la materia de derechos humanos y como mínimo a los criterios de legalidad, proporcionalidad y necesidad.

Esto quiere decir que, pese a que las imágenes faciales son un dato personal, de acuerdo a la normativa vigente aquellas que sean obtenidas de cámaras de videovigilancia -pues su finalidad es la investigación, detección y posible atribución de infracciones a determinadas personas- no recibirán el tratamiento establecido en la Ley, sin establecer limitación alguna a la injerencia enorme e indiscriminada que se aplican con cámaras equipadas por un sistema de tecnología de reconocimiento facial, pues requieren la recopilación y el procesamiento de imágenes faciales de todas las personas captadas, y el posible tratamiento erróneo que se podría generar a estos datos.

El derecho a la privacidad se ve comprometido cuando se generan y reúnen datos relativos a la identidad, la familia o la vida de una persona pues a través de esas acciones, la persona pierde el control sobre una información que puede poner en riesgo su vida privada, así como cuando esta información es examinada o utilizada por un ser humano o algoritmo. La simple existencia de sistemas secretos de vigilancia interfieren con el derecho a la privacidad.

Es decir, se legitima la capacidad de identificación y rastreo selectivo de personas, e ignora lo establecido por instrumentos internacionales cuando establecen que las técnicas de grabación audiovisual y de reconocimiento facial “sólo deben utilizarse cuando dichas medidas cumplan la triple condición de la legalidad, la necesidad y la proporcionalidad, dada su invasividad”[11]. Por lo tanto, respetando la proporcionalidad, estas técnicas sólo deben contemplarse cuando existan indicios concretos del cometimiento real de un delito grave, como la violencia o el uso de armas de fuego. Es decir, todos los datos que no correspondan a segmentos específicos que puedan ser necesarios para llevar a cabo una investigación penal y el enjuiciamiento de delitos violentos, deben ser eliminados.

Asimismo, toda persona que se considere afectada debe tener el derecho de acceder y solicitar la rectificación y eliminación de toda la información almacenada sin un propósito legítimo y sin fundamento jurídico. Para poder delimitar el uso de esta tecnología acorde a lo antes señalado deben existir bases jurídicas claras, sólidas y respetuosas de derechos humanos, con disposiciones que protejan de forma eficaz los datos personales, sobre todo al tratarse de imágenes faciales y datos derivados de ellas, algo que no se encuentra establecido en la Ley Orgánica de Protección de Datos Personales.

El Relator Especial sobre el derecho a la privacidad ha mencionado esta problemática, pues en muchas jurisdicciones, los servicios de inteligencia y policías quedan fuera del ámbito de la aplicación de las leyes de protección de datos, lo que impide que estos límites se encuentren establecidos en la Ley, no obstan-

11 Estudio de la Agencia de los Derechos Fundamentales de la Unión Europea, pág. 34.

te las injerencias que pueda realizar el Estado siempre deben ser especificadas con detalle de las circunstancias precisas en las que podrán autorizarse dichas injerencias, cuando estas injerencias concretas no se encuentran establecidas en la Ley, o son incompatibles con la dispuesto en el Pacto de Derechos Civiles y Políticos, comprometen la esencia del derecho como tal.

Por esto, es necesario describir cuáles serán las naturalezas de los delitos que pueden ser objeto de vigilancia, toda vez que las definiciones excesivamente amplias como la que encontramos en la Ley Orgánica de Protección de Datos Personales no son suficientemente claras ni específicas. Lo que facultan a los organismos encargados de manejar esta información a actuar discrecionalmente en perjuicio de los derechos de los ciudadanos.

Al no existir una normativa que garantice este aspecto del derecho a la privacidad, tampoco existe una tipificación específica para la vulneración del derecho a la privacidad a partir del uso de la videovigilancia. Esto se demuestra con la nula cantidad de casos iniciados a partir del uso de estas tecnologías. Sin embargo, de la vulneración de este derecho se generan delitos como robo de identidades, seguimiento y vigilancia ilegal de personas, y discriminación en las fronteras debido al uso de cámaras de videovigilancia para el control de la migración, que actualmente no se encuentran reconocidas en nuestra legislación a partir de la información obtenida por cámaras de videovigilancia pues se legitima su mal uso a partir de un discurso legitimado de “seguridad ciudadana”.

Falta de políticas públicas que incluyan la capacitación de funcionarios públicos y operadores judiciales.

De las entrevistas e información solicitada se ha detectado la falta de políticas públicas que permitan la capacitación en esta área. Si la propia Ley no lo define claramente, hay un marco de regulación y supervisión débil, lo cual resulta en el crecimiento de la vigilancia sistemática y la implantación masiva de tecnologías de reconocimiento facial en espacios públicos.

Además, la mayoría de estas entidades encargadas del manejo de base de datos obtenida de cámaras de videovigilancia no cuentan con protocolos de protección y seguridad para impedir el abuso y redistribución de estos datos, o evaluaciones del impacto en la privacidad que incluya la prohibición del uso de reconocimiento facial mediante la vigilancia sin autorización judicial o supervisión independiente.

Esto representa un vacío legal enorme, pues la administración pública debe actuar en el marco de sus competencias y de lo establecido en la ley. A su vez cada acción realizada por la potestad pública se fundamenta en un acto administrativo motivado que debe establecer los parámetros sobre los cuales se ejercerá la vigilancia, sobre todo cuando existe el riesgo de vulnerar el derecho a la privacidad de las personas.

Todos estos vacíos dan como resultado la falta de conocimiento y preparación de las y los servidores públicos, que como observamos de la información recopilada, no identifican el rostro como un dato personal que debe ser protegido por el Estado o utilizan las imágenes con fines de promoción institucional. Por lo que es primordial contar con unos entrenamientos específicos les permita contar con aptitudes técnicas necesarias para proteger eficazmente la privacidad de las personas.

Falta de transparencia en acceso a la información y clasificación de información.

Como demostraremos más adelante en esta investigación existe falta de transparencia del Sistema Integrado de Seguridad ECU 911, organismo central del manejo de la información captada ahora por videovigilancia y en los próximos meses por tecnología de reconocimiento facial. Los manuales, protocolos y procedimientos, metodologías e instructivos generados y que lleguen a generarse en el ECU 911 como consecuencia o para la prestación del servicio de despacho de recursos para la atención de emergencias, videovigilancia y recepción de llamadas a la línea única 911 han sido declarados como reservados hasta el año 2028.

En la Ley Orgánica de Transparencia y Acceso a la Información Pública el artículo 4 señala que el ejercicio de la función pública, está sometido al principio de apertura y publicidad de sus actuaciones. Esto, va acorde a lo establecido en estándares internacionales de derechos humanos en los que se señala que la máxima divulgación de la información es la regla, mientras que las limitaciones de entrega de información son la excepción.

En este sentido el artículo 13 numeral 2 de la Convención Americana de Derechos Humanos, establece que las limitaciones al derecho de acceso a la información pública deben responder a la excepcionalidad, legalidad, que las limitaciones estén encaminadas a cumplir los objetivos legítimos de la Convención, y proporcionalidad.

El artículo 17 de la Ley Orgánica de Transparencia y Acceso a la Información Pública establece dichas limitaciones en los siguientes casos: a) documentos calificados de manera motivada como reservados por el Consejo de Seguridad Nacional, por razones de defensa nacional que son los planes, órdenes de defensa nacional, militar, movilización, operaciones especiales y bases e instalaciones militares ante posibles amenazas contra el Estado; información en el ámbito de la inteligencia; e información sobre la ubicación del material bélico y fondos destinados para fines de defensa nacional.

Es obligación de la entidad demostrar que las restricciones al acceso a la información se encuentran amparadas por lo establecido en la Ley así como en estándares internacionales de DDHH, sin embargo las causales establecidas por el ECU 911 para negar el acceso a la información de los protocolos de manejo de información, no responden a las disposiciones legales.

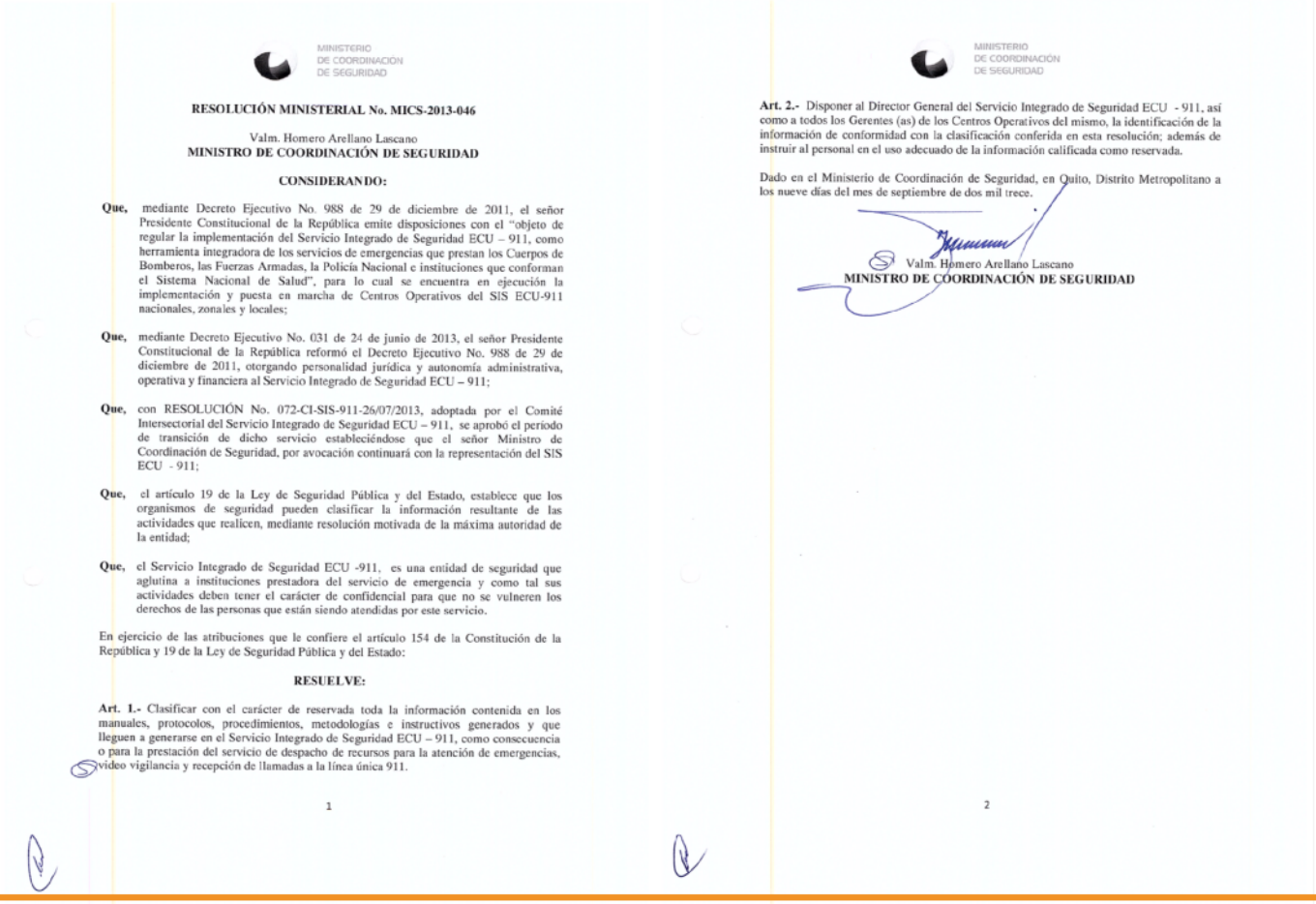
SEGUNDO CAPÍTULO

Vigilancia masiva que vulnera derechos

El Sistema de Seguridad Integral funciona bajo protocolos de carácter reservado.

La videovigilancia como mecanismo para resguardar la seguridad ciudadana, oficialmente nace en Ecuador con la creación del Sistema Integrado de Seguridad ECU 911 en el gobierno de Rafael Correa. Esta plataforma, que articula a varias instituciones públicas para atender emergencias, cuenta en su casa matriz, en Quito, con una sala dedicada exclusivamente a la videovigilancia en la que laboran rotativamente más de 100 funcionarios. El ECU 911 fue creado el 29 de diciembre de 2011, a través del decreto ejecutivo 998, que fue reformado dos años después otorgándole personalidad jurídica, administrativa y financiera.

El 9 de septiembre de 2013, el Ministro Homero Arellano, quien presidía la secretaría del Ecu 911 por resolución ministerial MICS-2013-046, se amparó en el artículo 19 de la Ley de Seguridad Pública y del Estado y clasificó como reservada "toda la información contenida en manuales, protocolos y procedimientos, metodología e instructivos generados y que lleguen a generarse en el ECU 911 como consecuencia o para la prestación del servicio de despacho de recursos para la atención de emergencias, videovigilancia y recepción de llamadas a la línea única 911". La reserva aún continúa vigente, y ha sido la razón por la cual ninguno de estos documentos fue facilitado por el ECU 911 para la investigación . El decreto MICCS-2013-046 no especifica el acceso a imágenes contenidas en el sistema de videovigilancia.[12]



MINISTERIO DE COORDINACION DE SEGURIDAD

RESOLUCIÓN MINISTERIAL No. MICS-2013-046

Valm. Homero Arellano Lascano
MINISTRO DE COORDINACIÓN DE SEGURIDAD

CONSIDERANDO:

Que, mediante Decreto Ejecutivo No. 988 de 29 de diciembre de 2011, el señor Presidente Constitucional de la República emite disposiciones con el "objeto de regular la implementación del Servicio Integrado de Seguridad ECU – 911, como herramienta integradora de los servicios de emergencias que prestan los Cuerpos de Bomberos, las Fuerzas Armadas, la Policía Nacional e instituciones que conforman el Sistema Nacional de Salud", para lo cual se encuentra en ejecución la implementación y puesta en marcha de Centros Operativos del SIS ECU-911 nacionales, zonales y locales;

Que, mediante Decreto Ejecutivo No. 031 de 24 de junio de 2013, el señor Presidente Constitucional de la República reformó el Decreto Ejecutivo No. 988 de 29 de diciembre de 2011, otorgando personalidad jurídica y autonomía administrativa, operativa y financiera al Servicio Integrado de Seguridad ECU – 911;

Que, con RESOLUCIÓN No. 072-CI-SIS-911-26/07/2013, adoptada por el Comité Intersectorial del Servicio Integrado de Seguridad ECU – 911, se aprobó el período de transición de dicho servicio estableciéndose que el señor Ministro de Coordinación de Seguridad, por avocación continuará con la representación del SIS ECU - 911;

Que, el artículo 19 de la Ley de Seguridad Pública y del Estado, establece que los organismos de seguridad pueden clasificar la información resultante de las actividades que realicen, mediante resolución motivada de la máxima autoridad de la entidad;

Que, el Servicio Integrado de Seguridad ECU -911, es una entidad de seguridad que aglutina a instituciones prestadora del servicio de emergencia y como tal sus actividades deben tener el carácter de confidencial para que no se vulneren los derechos de las personas que están siendo atendidas por este servicio.

En ejercicio de las atribuciones que le confiere el artículo 154 de la Constitución de la República y 19 de la Ley de Seguridad Pública y del Estado:

RESUELVE:

Art. 1.- Clasificar con el carácter de reservada toda la información contenida en los manuales, protocolos, procedimientos, metodologías e instructivos generados y que lleguen a generarse en el Servicio Integrado de Seguridad ECU – 911, como consecuencia o para la prestación del servicio de despacho de recursos para la atención de emergencias, video vigilancia y recepción de llamadas a la línea única 911.

1

MINISTERIO DE COORDINACIÓN DE SEGURIDAD

Art. 2.- Disponer al Director General del Servicio Integrado de Seguridad ECU - 911, así como a todos los Gerentes (as) de los Centros Operativos del mismo, la identificación de la información de conformidad con la clasificación conferida en esta resolución; además de instruir al personal en el uso adecuado de la información calificada como reservada.

Dado en el Ministerio de Coordinación de Seguridad, en Quito, Distrito Metropolitano a los nueve días del mes de septiembre de dos mil trece.

Valm. Homero Arellano Lascano
MINISTRO DE COORDINACIÓN DE SEGURIDAD

2

Resolución ministerial MICS 2013-046 de 2013 que estipula la reserva en la información del ECU -911.

[12] MINISTERIO DE GOBIERNO Y SEGURIDAD, Resolución Ministerial No. MICS 2013-046, 9 septiembre 2013, https://www.ecu911.gob.ec/-TransparenciaArchivo/JUNIO%202017/anexo%20a3)/Acuerdo%20Ministerial%20MICS-2013-046.pdf

Según Genny Vélez, coordinadora General de Transparencia y Acceso a la Información Pública de la Defensoría del Pueblo, entidad que vela por el cumplimiento de la entrega de la información pública de las instituciones, confirmó a Fundamedios que el ECU 911 mantiene su información reservada por 15 años, es decir hasta el 2028, según el último informe presentado por la institución en 2020.

La funcionaria señaló que la Defensoría no conoce las razones de la reserva y, por lo tanto, no tiene la facultad para emitir juicio sobre la pertinencia de esta medida. Cabe indicar que la declaración de reserva fue dada por decreto ejecutivo y suscrita por el Ministerio Coordinador de Seguridad, que fue extinto en 2017 por el presidente Lenin Moreno.

Renata Moreno, directora de Asesoría Jurídica del ECU 911, confirmó que la reserva únicamente se aplica a los protocolos, instructivos y procedimientos, pero la información generada del sistema de videovigilancia "no se maneja como reservada". Eso sí, aclaró que cuando la información ha sido judicializada se maneja por cadena de custodia con acceso único a los operadores de justicia.

Según Vélez, el ECU 911 es la única institución que puede acceder a la información confidencial. La Ley Orgánica de Acceso a la Información Pública (LOTAIP) establece que la información podrá ser desclasificada por el Consejo de Seguridad en caso de temas de seguridad nacional o la Asamblea Nacional con voto de mayoría.

En 2014 se suscribió el convenio interinstitucional SAEI-FJ con la Función Judicial para el pedido de los contenidos de videovigilancia por los operadores de justicia. Un total de 113.867 solicitudes fueron respondidas a través de esta plataforma hasta el 14 de julio de 2021. Los ciudadanos no tienen ninguna posibilidad de solicitar o acceder a videos producidos por el ECU 911.

Fundamedios revisó manuales, instructivos y procedimientos de instituciones que velan por la seguridad ciudadana y constató que no tienen carácter reservado. Por ejemplo, en el sitio web de la Policía Nacional son públicos los instructivos y manuales de atención a la COVID -19 y de operaciones para el orden público y la seguridad ciudadana, así como planes de operaciones, instructivos y protocolos. Los Gobiernos Descentralizados Autónomos que, por competencia, velan por la seguridad ciudadana no tienen reserva en la documentación relacionada con la seguridad ciudadana.

El coronel Juan Zapata, director del Sistema Integrado de Seguridad ECU 911, al ser entrevistado por Fundamedios, reconoció que la condición de reserva podría ser revisada. "(...) Esa resolución de 2013 a lo mejor, no todo tiene razón y lo podemos evaluar, habrá que hablarlo en el Comité Intersectorial, que es el que regula al 911, porque puede haber información que no necesariamente tenga que ser reservada".

El director del ECU 911 se sinceró y dijo no ser "muy apasionado de las reservas", por lo cual estaría en sus manos mejorar la transparencia que regula el Sistema Integrado de Seguridad bajo el gobierno de Guillermo Lasso y dejar esta regulación para los gobiernos venideros en beneficio de los ecuatorianos.

Juan Pablo Torres, subdirector de Tecnología del ECU 911, añadió que la reserva no implica que existan procedimientos violatorios a los derechos humanos o contradictorios a la intimidad de las personas. " (...) desde ese punto de vista nosotros garantizamos transparencia, en el sentido que todos nuestros procedimientos, los de contratación o los procedimientos de videovigilancia, son de acceso público (...), detalló.

En el informe Derecho a la Información y Seguridad Nacional[13] de la RELE-CIDH publi-

[13] RELE- CIDH, Derecho a la información y seguridad nacional, Julio 2020, http://www.oas.org/es/cidh/expresion/informes/DerechoInformacionSeguridadNacional.pdf

cado en julio de 2020, se destaca el riesgo de la falta de transparencia en la información estatal concerniente a la seguridad nacional para ocultar violaciones a los derechos humanos. "…. los obstáculos para el acceso a la información pública y la falta de transparencia que perdura en torno a las actividades de vigilancia llevadas a cabo por los Estados de las Américas operan en muchos casos como barreras que impiden la rendición de cuentas sobre su utilización legítima, que debería seguir los requisitos de autorización judicial previa y ser estrictamente necesaria y proporcional a los fines legítimos que se busca proteger por parte del Estado."[14]

Cabe indicar que los protocolos, manuales y procedimientos de los sistemas de videovigilancia municipales de Quito, Cuenca y Latacunga no son reservados.

Los riesgos de sistemas de seguridad con protocolos reservados.

Uno de los riesgos de crear al ECU 911 bajo un decreto presidencial es que responde únicamente al poder Ejecutivo, lo cual lo hace más vulnerable de ser instrumentado por intereses políticos y no contar con independencia para cumplir con el objetivo en favor de la seguridad ciudadana. Varias investigaciones periodísticas[15] de medios nacionales e internacionales revelaron que durante los primeros años de creación, el ECU 911 compartió la información obtenida de sus cámaras a través de un sistema espejo con la ex Secretaría de Inteligencia (SENAIN), creada en 2009. A través de la SENAIN, el gobierno de Rafael Corra espió y persiguió a políticos, funcionarios públicos, activistas y periodistas.

En 2019, el mandatario Lenin Moreno, sucesor de Correa, denunció que el ECU 911 fue usado de forma "perversa" para tareas de espionaje con el propósito de presionar a los adversarios políticos y a quienes pensaban distinto al Ejecutivo. Moreno anunció en ese entonces un proceso de renovación de equipos y garantizó la independencia de sus funciones.[16]

La ex Secretaría Nacional de Inteligencia (SENAIN), recibía información de las cámaras del ECU 911 para perseguir a los detractores del régimen, intervenía escuchas telefónicas ilegales e incluso se utilizaba los medios públicos para filtrar información privada. Así lo publicó un amplio reportaje de investigación del medio estadounidense The New York Times titulado: "Made in China, Exported to the World: The Surveillance State". El reportaje devela el aparataje de vigilancia y espionaje de la Senain con cámaras del ECU 911.[17]

El coronel Mario Pazmiño, ex director de Inteligencia Militar del Ejército denunció al Estado por vulneración al derecho a la intimidad. Desde la sala de su domicilio, ubicado al norte de Quito, narró a Fundamedios que durante la época de Rafael Correa fue víctima de espionaje tras denunciar públicamente el creciente tráfico de drogas en Ecuador y la corrupción de la Policía Nacional.

Pazmiño explicó que una cámara de 360 grados fue ubicada al frente de su domicilio. "Era raro porque estas cámaras se ponen

---

[14] RELE- CIDH, Derecho a la información y seguridad nacional, Julio 2020, http://www.oas.org/es/cidh/expresion/informes/DerechoInformacionSeguridadNacional.pdf

[15] CODIGO VIDRIO, Hecho en China, exportado al mundo: El estado de espionaje, 24 abril 2019, https://www.codigovidrio.com/code/hecho-en-china-exportado-al-mundo-el-estado-de-espionaje/

[16] NOTIMUNDO, Presidente Moreno afirmó que el ECU 911 se usó de manera "perversa" para espionaje , 25 de abril 2019, https://notimundo.com.ec/presidente-moreno-afirma-que-el-ecu-911-se-uso-de-manera-perversa-para-espionaje/

[17] CODIGO VIDRIO, Hecho en China, exportado al mundo: El estado de espionaje, 24 abril 2019, https://www.codigovidrio.com/code/hecho-en-china-exportado-al-mundo-el-estado-de-espionaje/

Is Chinese-style surveillance becoming normalized? A Times investigation found the Chinese surveillance state is spreading past its borders. Jonah M. Kessel/The New York Times

https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html

específicamente en sectores donde hay confluencia mayor, por ejemplo, en La Marín, en El Labrador, zonas donde hay mucho tráfico, aquí no hay nada, pero la cámara está direccionada hacia el área de mi domicilio y además de eso al frente, en esa casa verde, tenía un sistema de escucha mediante conos de la SENAIN. Tengo fotografías de los equipos de vigilancia que me estuvieron siguiendo", indica.

Para Pazmiño pese al tiempo transcurrido, estos hechos deben investigarse, transparentarse y judicializarse. El ex director de Inteligencia Militar confirmó que la vigilancia de la ex SENAIN fue contra políticos, activistas y opositores fue también aplicada, entre otros, a los periodistas Martha Roldós, Juan Carlos Calderón, Carlos Vera, Christian Zurita, Emilio Palacio, Kléver Jiménez y al Director de Fundamedios, César Ricaurte. Asegura que tuvo acceso a documentos y mapas en los que se reconocía a los opositores del régimen.

Christian Zurita y Juan Carlos Calderón aseguraron a Fundamedios que nunca tuvieron constancia de que fueron blanco de un espionaje con videovigilancia. Eso sí, Calderón sospecha que la ex SENAIN hackeó su correo electrónico y publicó información en el diario estatal El Telégrafo sobre fondos obtenidos de la National Endowment for Democracy (NED) para el quehacer periodístico con la intención de desestabilizar al gobierno correísta. Lo mismo le ocurrió a Martha Roldós.

La ineficiencia marcó la operación de las primeras cámaras de reconocimiento facial.

En Ecuador, actualmente, pese a existir equipos de reconocimiento facial, no se ha podido implementar este tipo de videovigilancia y aplicar la inteligencia artificial debido a la falta de conexión entre los equipos y las bases de datos. Pero tanto municipios como el ECU 911 pretenden implementar el sistema en diciembre de 2021 y en 2022, de acuerdo a la información publicada por medios de comunicación y recopilada para esta investigación.[18]

Se aspira que, a diciembre de 2021, por primera vez, Ecuador cuente con un sistema de videovigilancia de reconocimiento facial. Un pedido de información enviado por Fundamedios el 5 de octubre de 2021 al Sistema Integrado ECU 911 señala que la institución adquirirá un total de 1.294 cámaras con reconocimiento facial. Se espera también contratar 23 drones y 3 sistemas de video wall. Para ello, se analiza junto al personal del departamento de Criminalística de la Policía Nacional la adquisición de los equipos y la interconexión con una base de datos para la activación de esta tecnología biométrica. Al cierre de esta investigación, los procesos de contratación no fueron subidos al Servicio Nacional de Contratación Pública (Sercop).

En una entrevista concedida a Fundamedios, el director del ECU 911, Juan Zapata aseguró que el ECU 911 solamente comprará los equipos y la Policía Nacional será la entidad que cuente con bases de datos para operar con un software especial que identifique los rostros. Las bases de datos estarán encriptadas y serán de acceso único de la Policía Nacional.

En el ámbito municipal, la Secretaría General de Seguridad y Gobernabilidad del Municipio de Quito, el Gobierno Autónomo Descentralizado (GAD) de Latacunga y el Consejo de Seguridad de Cuenca y la Corporación para la Seguridad Ciudadana de Guayaquil han adquirido cámaras con capacidad de reconocimiento facial, pero no han gestionado el cruce con bases de datos, que es el principal requerimiento para aplicar la tecnología biométrica.

El Municipio de Quito se ha visto envuelto en un escándalo de corrupción por la adquisición de 203 cámaras con estas características entre 2019 y 2020, bajo la administración del exalcalde Jorge Yunda. La compra se hizo sin los análisis pertinentes previos para la compatibilidad del software y las cámaras compradas, que permitan una conexión eficaz con las bases de datos. Además, cada cámara de reconocimiento facial fue adquirida por 2.551 USD, pero al no activarse con una base de datos, cumplen la función de una cámara valorada entre 400 y 900 USD, es decir, se adquirió una tecnología costosa que no está siendo aplicada.

[18] TELEAMAZONAS, Cámaras con reconocimiento facial estarían operativas en un mes, 2019 https://www.teleamazonas.com/camaras-con-reconocimiento-facial-estarian-operativas-en-un-mes/

El Municipio de Quito adquirió cámaras de videovigilancia en dos fases. En estas ganaron las empresas Andeantrade y el Consorcio de Reconocimiento Facial de Quito (firmas: Full Tecnología Fulltec Cia.Ltda. y Megasupply).

La ineficiencia e inoperatividad de las cámaras con reconocimiento facial se repite en otras ciudades. El GAD de Latacunga cuenta con seis cámaras con esta tecnología, pero actualmente no están activadas. El software detecta rostros precisos, pero básicamente se usa para controlar el uso obligatorio de mascarillas en áreas públicas y evitar contagios por la COVID-19. Cuando se detecta un caso de incumplimiento a través de la cámara de videovigilancia con capacidad de reconocimiento facial, los operadores del sistema alertan a miembros de la Policía local para que se acerquen presencialmente al sitio donde ocurre el hecho y ubiquen a la persona que podría ser sancionada por incumplir con la Ordenanza Municipal, según aseguraron los funcionarios entrevistados

En el GAD de Latacunga ganó el concurso público el Consorcio de Cámaras de Reconocimiento Facial, que en el Servicio de Rentas Internas aparece como la empresa Fulltec, cuyos administradores son: Joe Luis Burbano y Óscar Trujillo, los mismos que administran Andeantrade. El representante legal de Fulltec es Francisco Javier Atiencia en ambos casos.

En el caso del Consejo de Seguridad de Cuenca, existen 10 cámaras con capacidad de reconocimiento facial que no cuentan con un servidor informático y una base de datos de rostros ni información biométrica alguna. Actualmente, están siendo usadas solamente por su capacidad de alcance visual.

La Corporación para la Seguridad Ciudadana de Guayaquil (CSCG) informó a Fundamedios el 16 de julio de 2021, a través de un pedido de acceso a la información, que no cuentan con cámaras de reconocimiento facial. Sin embargo, en el portal nacional de compras públicas consta la ejecución de un contrato de adquisición de 100 cámaras de videovigilancia con megafonía y analítica de reconocimiento facial para el control y vigilancia del entorno de centros educativos del cantón Guayaquil por 2'569.906.41 USD otorgados a la empresa Unión Eléctrica S.A. El contrató fue realizado el 12 de noviembre de 2019.

Con motivo de la celebración de la ciudad, la alcaldesa Cynthia Viteri anunció que se aplicará inteligencia artificial en la nueva compra. Diario Expreso informó que "el Concejo Municipal aprobó un nuevo convenio entre el Municipio de Guayaquil y la Corporación para la Seguridad Ciudadana de Guayaquil, por alrededor de $ 33 millones para adquirir otras 15.000 cámaras durante los próximos cuatro años.[19]

El 24 de septiembre, Fundamedios envió un correo electrónico a Kristel Salcedo, asesora de Relaciones Públicas de la Corporación, consultando sobre este tema. Cuatro días después respondió señalando que Cristian Cherrez, director ejecutivo de la CSCG, está en una visita interinstitucional fuera del país y que responderá las dudas a su regreso. Sin embargo, hasta el 30 de octubre no contestó las dudas ni concedieron una entrevista que también fue solicitada a mediados de octubre. De acuerdo a información entregada a Fundamedios por el ECU 911 a través de la Ley de Acceso a la Información Pública (Lotaip), las contrataciones para la adquisición del sistema de videovigilancia (cámaras) entre 2012 y 2017 ascendieron a 180' 368.626,50 USD. De este valor, el 50% (178 '151.920 USD) correspondió a créditos chinos entre 2012 y 2016 usados para la implementación tecnológica del ECU 911 adjudicados a la empresa estatal China National Electronic Import (CEIEC). Esta empresa fue cuestionada por mal uso de recursos públicos para este fin y la construcción de sedes del ECU 911.

De hecho, Juan Pablo Torres, subdirector de tecnología del ECU 911, explicó que la tecnología desarrollada por CEIEC es única y esa característica hace que se necesite la contra-

[19] EXPRESO, Guayaquil: más de $ 30 millones en cámaras que aún no se sabe si se usarán, 17 octubre 2021, https://www.expreso.ec/guayaquil/30-millones-camaras-usaran-113847.html

tación de la empresa para el mantenimiento posterior de la plataforma. Si bien, el contrato feneció en 2018, esta condición obliga al ECU 911 a contratar los servicios para mantenimiento de sistemas de seguridad ciudadana con régimen especial y sin concurso público.

En los procesos de adquisición de equipos no se analizan limitaciones jurídicas o afectación a derechos humanos.

CSC CONSEJO DE SEGURIDAD CIUDADANA CUENCA

TERMINOS DE REFERENCIA

1. **DATOS GENERALES**

1.1 OBJETO:	Contratar los servicios de mantenimiento preventivo y correctivo, para el sostenimiento tecnológico de los sistemas de video vigilancia y de alarmas comunitarias del Consejo de Seguridad Ciudadana de Cantón Cuenca.
1.2 JUSTIFICACIÓN:	El Consejo de Seguridad Ciudadana del cantón Cuenca cuenta en su POA 2020 con el programa Tecnología aplicada a la seguridad en el proyecto Sistema Preventivo y de Alerta por Audio y Video llevado por la Coordinación de Innovación y Tecnología; que consiste en el dimensionamiento, adquisición, instalación, sistemas de video vigilancia que están colocados en la ciudad en lugares donde es necesario realizar la recuperación del espacio público y generar un sector más seguro para la ciudadanía. Asimismo dentro del mismo programa se tiene el proyecto Alertas Comunitarias que consiste en el dimensionamiento y la implementación de sistemas de alarmas comunitarias instalados en los distintos barrios de la ciudad y de botones de auxilio en los mercados y terminal terrestre. Los sistemas adquiridos de video vigilancia están organizados en: Sistemas de Puntos Seguros, Parques Seguros, Plazas Seguras, Mercados Seguros y Alertas ante Crecientes de Ríos. Todos estos sistemas requieren de mantenimientos preventivos y correctivos, de manera permanente. Además parte fundamental de estos sistemas son los servidores de grabación, los cuales también requieres de mantenimiento preventivo periódico el cual consiste en limpieza, actualización de software y reconfiguración de los mismos para asegurar su mejor rendimiento y operatividad. Actualmente contamos con 187 puntos de video vigilancia cada uno cuenta con cámaras, intercomunicadores y sistemas de perifoneo, los cuales están instalados en sitios públicos del cantón Cuenca y al estar a la intemperie requieren de mantenimiento continuo.

2 de 30

CSC CONSEJO DE SEGURIDAD CIUDADANA CUENCA

En el cuadro a continuación se detalla las cantidades de sistemas instalados en años anteriores:

PROYECTOS (O ACTIVIDADES) EJECUTADOS DURANTE EL PERÍODO 2014-2019		
AÑO	PROYECTO	NRO
2015	Punto Seguro	2
	Alerta ante Crecientes de Ríos	2
	Total	**4**
2016	Alerta ante Crecientes de Ríos	4
	Mercado Seguro	3
	Parque Seguro	6
	Total	**13**
2017	Mercado Seguro	22
	Parque Seguro	19
	Sistema de Control de pozas de Anfibios	10
	Plaza Segura	3
	Total	**54**
2018	Punto Seguro	4
	Alerta ante Crecientes de Ríos	8
	Mercado Seguro	2
	Parque Seguro	56
	Plaza Segura	16
	Mega Parques	9
	Total	**95**

3 de 30

Términos de referencia del contrato CIE-CS-005-2020 del Consejo de Seguridad Ciudadana de Cuenca.

En Ecuador, según el artículo 23 de la Ley Orgánica del Sistema Nacional de Contratación Pública, antes de iniciar un procedimiento precontractual, la entidad deberá contar con los estudios y diseños completos, definitivos y actualizados, planos y cálculos; sin embargo no hace referencia a un posible análisis jurídico sobre eventuales vulneraciones a los derechos humanos.

Lo mismo ocurre con el artículo 105 de la Resolución SERCOP 072, que es una ampliación a la Ley Orgánica del Sistema de Contratación Pública, y el numeral 3 del artículo 109 especifica que los términos de referencia deben tener: antecedentes, alcance, metodología, objetivos, diagnóstico, estadística. Según expertos consultados en el tema existe un vacío legal en la norma.

Fundamedios revisó las contrataciones, los estudios técnicos y los términos de referencia del ECU 911, así como de las instituciones competentes para la videovigilancia en Guayaquil, Quito, Cuenca y Latacunga y comprobó que las causas que motivan las contrataciones de este tipo de tecnología son escuetas. Básicamente se limitan a argumentar el uso de la tecnología a favor de la reducción del índice delictivo sin presentar pruebas o estadísticas que permitan atribuir la reducción de la criminalidad al uso de videovigilancia. En sus análi-

sis, no se especifican ni se incluye mención a la posible vulneración de los derechos ciudadanos a la privacidad. Tampoco hay referencia alguna a los diversos instrumentos legales internacionales que analizan este problema.

Por ejemplo, los estudios técnicos del Municipio de Quito solamente mencionan las especificaciones de la adquisición de tecnología, mientras que los documentos de autorización de la etapa preparatoria de la contratación en dos fases, justifican únicamente la necesidad de compra de las cámaras de reconocimiento facial "para disminuir las oportunidades para la comisión de delitos y la violencia, y reducir la percepción de inseguridad". No existe un análisis jurídico de la legalidad del uso de programas de reconocimiento facial automatizado, teniendo en consideración las posibles afectaciones al derecho a la intimidad, al derecho a la protección de datos personales, al derecho a la inviolabilidad de las comunicaciones, entre otros.

Una situación similar se repite con la contratación del GAD de Latacunga que justifica la adquisición de cámaras de videovigilancia con el único fin de reducir la percepción de inseguridad y optimizar los recursos. Los dos contratos del Consejo de Seguridad de Cuenca entre 2019 y 2021 tampoco incluyen un análisis jurídico. En el caso de la Corporación para la Seguridad Ciudadana de Guayaquil, se constató que en los documentos previo al contrato en el que adquiere 100 cámaras de reconocimiento facial para ser colocadas en el exterior de entidades educativas, se menciona que el interés de comprar esta tecnología es para prevenir actos delictivos que afecten a la niñez y juventud.

Los responsables de la videovigilancia ignoran que el rostro es un dato personal.

Una de las conclusiones más preocupantes del presente informe es que no hay un consenso entre los funcionarios públicos responsables del manejo del sistema de videovigilancia en sus ciudades sobre la calificación del rostro como dato personal sensible.

La reciente Ley de Protección de Datos en Ecuador define dato personal como un "dato que identifica o hace identificable a una persona natural, directa o indirectamente", siendo el rostro el rasgo más importante. Los datos sensibles que competen a los datos biométricos tienen un tratamiento especial en la Ley y queda prohibida su exposición salvo en los siguientes casos: "salvo que el titular haya dado su consentimiento especificando los fines, para cumplimiento de obligaciones en el ámbito laboral, de seguridad y protección social, por no estar capacitado físico o jurídicamente para dar un consentimiento, para el tratamiento con fines de archivo de interés público o cuando los datos de salud se sujeten a las disposiciones de la Ley".[20]

Fundamedios realizó un pedido de información al GAD de Latacunga, amparándose en la Ley de Transparencia y Acceso a la Información Pública (LOTAIP), acerca del reglamento que regula el manejo de datos de los ciudadanos obtenidos a través del sistema de videovigilancia.

La respuesta de Luigi Calderón, especialista 1 de Seguridad Ciudadana del GAD de Latacunga, fue alarmante: "ningún dato personal se obtiene a través del sistema de videovigilancia municipal (...) ningún funcionario de la institución maneja datos personales (...) Las acciones que realiza la Unidad de Agentes de Control Municipal, de acuerdo a la normativa legal que los ampara, se realiza en coordinación con el sistema de videovigilancia más no reúne datos personales".

Otro caso es el de Quito. Adrián Haro, gerente general de EP EMSEGURIDAD del Municipio quiteño, respondió que: "dentro de los sistemas de videovigilancia con analítica de video

[20] LEY ORGANICA DE DATOS PERSONALES, 26 de mayo 2021, https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Ley-Organica-de-Datos-Personales.pdf

entregados está la capacidad de almacenar información captada en el espacio público sin la necesidad de incluir datos personales".

En ambos casos, para los funcionarios el rostro de por sí no constituye un "dato personal". Según los entrevistados antes mencionados, adquiere esta calidad solamente cuando se identifica la cara o por extensión los movimientos del cuerpo que también son datos biométricos captados por videovigilancia, con el nombre y apellido de la persona.

Sin embargo, en entrevista con Fundamedios, Daniela Valarezo, Secretaría de Seguridad y Gobernabilidad del Municipio de Quito, discrepó con Haro y reconoció que el rostro sí es un dato personal. La diversidad en concepciones sobre un tema tan delicado entre funcionarios dedicados a resguardar la seguridad de la capital, demuestra la falta de definiciones y lineamientos claros en el cabildo.

Los ecuatorianos no son conscientes de su derecho a la intimidad.

La legislación ecuatoriana contempla opciones para que los ciudadanos accedan al sistema judicial y exijan el respeto a su derecho a la intimidad vulnerado por capturas mediante sistemas de videovigilancia o publicación de estas imágenes con fines institucionales, como hemos visto. Sin embargo, la investigación de Fundamedios concluye que los y las ciudadanas no son conscientes de este derecho.

En Ecuador en 2014 se aprobó el Código Orgánico Integral Penal (COIP) que en el artículo 178 se refiere, por primera vez, a la violación de la intimidad. Fundamedios solicitó, a través de un pedido de acceso a la información, las denuncias presentadas a esta institución entre 2014 y 2021 que tengan relación con el artículo antes mencionado. La Defensoría remitió 14 casos, ninguno de ellos tuvo relación con temas de videovigilancia.

También se solicitó información de denuncias basadas en el artículo 178 del COIP a la Fiscalía General desde 2014 al 22 de octubre de 2021. Un total de 12.332 denuncias fueron presentadas. De estos casos, más de 7 mil causas fueron archivadas, lo cual evidencia el poco tratamiento judicial y seguimiento a casos relacionados con el derecho a la intimidad. De los 12.332 casos, 22 terminaron con una sentencia condenatoria y 25 sentencias ratificaron el estado de inocencia. Al solicitar los motivos de las denuncias para constatar si en alguna se mencionaba a la videovigilancia, la institución judicial señaló que no existe esa clasificación en la estadística.

Fundamedios también solicitó información al Consejo de la Judicatura, que es el ente judicial que recopila el tratamiento de casos en todas las instancias. Desde 2014 a julio de 2021 se reportaron 27 sentencias condenatorias y 24 que ratifican el estado de inocencia. Fundamedios revisó cada uno de los casos en el sistema de consulta de procesos judiciales (SATJE), pero ninguno de los casos tenía relación con sistemas de videovigilancia.

La revisión de los casos reportados en la Defensoría del Pueblo, en la Fiscalía y en el Consejo de la Judicatura nos permite concluir que el sistema judicial no cuenta con una clasificación del delito de violación a la intimidad por sistemas de videovigilancia, seguramente, por la ausencia de menciones expresas en la normativa.

22 sentencias condenatorias sobre violación a la intimidad se resolvieron en Ecuador entre 2014 y 2021.

No existe suficiente transparencia.

Otro hallazgo es que existe reserva en la entrega de información relacionada a la videovigilancia y seguridad. El Ministerio de Gobierno, que es el organismo que regula seguridad interna del país, no contestó la petición de información enviada con fecha de 19 de julio de 2019 en la cual Fundamedios buscó información acerca del Plan Nacional de Seguridad Ciudadana y Convivencia Social Pacífica 2019-2030; la reducción o aumento de los índices de delito; los protocolos para el tratamiento de datos personales obtenidos a través de la videovigilancia y el reglamento del uso de este sistema en protestas sociales.

Fundamedios envió dos peticiones de información a la Policía Nacional. La primera con fecha de 20 de julio en la que solicitó información acerca de un eventual sistema de videovigilancia de la Policía, el cruce de bases de datos y el monto destinado a este fin. La institución contestó que no cuenta con un sistema de videovigilancia propio ni presupuesto destinado para este objetivo. Aseguró que únicamente destina personal policial para trabajar en las tareas de videovigilancia del ECU 911. Por esta razón, Fundamedios envió una nueva petición el 16 de agosto solicitando información acerca del número de servidores que realizan tareas de videovigilancia en el ECU 911, la capacitación que reciben, si cruzan bases de datos con otras instituciones para tarea de vigilancia. Sin embargo, al cierre de esta investigación (30 de octubre de 2021), la petición no fue respondida, pese a que la Ley de Acceso a la Información Pública da un plazo de diez días. También solicitamos una entrevista con la comandante general de la Policía, Tannya Varela, pero no fue aceptada.

El Municipio de Quito respondió a la petición de acceso a la información enviada el 20 de julio acerca de los sistemas de videovigilancia. Algunas de sus respuestas no fueron específicas y al ser consultados sobre estudios que justifiquen la necesidad de adquirir tecnología de reconocimiento facial y un análisis jurídico sobre la legalidad de adquirir esta tecnología, teniendo en cuenta posibles afectaciones a los derechos ciudadanos, señalaron que no tienen competencia para hacerlo. “No le corresponde a esta Empresa Pública la elaboración o aplicación de documentos y minutas, sobre el uso de este tipo de programas, ya que no es la generadora de la necesidad, ni es la operadora de los sistemas de videovigilancia para el control del espacio público, conforme las competencias establecidas en el Código Municipal del DMQ”.

Las imágenes captadas en videovigilancia son usadas para campañas de relaciones públicas, vulnerando los derechos de los ciudadanos a la privacidad.

La investigación de Fundamedios demuestra que la captación de información por videovigilancia, su archivo y su difusión pública por parte de las instituciones que manejan estos datos no son entendidas desde el punto de vista del respeto a los derechos ciudadanos. Esto se comprueba por la contínua publicación de contenido obtenido de los sistemas de videovigilancia en las redes sociales de las instituciones con el fin de implementar campañas de relaciones públicas.

Entre julio y octubre de 2021, Fundamedios revisó las cuentas de Twitter del ECU 911, de la Corporación para la Seguridad Ciudadana de Guayaquil (CSCG) y del Consejo de Seguridad de Cuenca y de Agentes de Control Metropolitano de Quito. Con el pretexto de prevenir delitos, capturar a ciudadanos sospechosos, retirar a bebedores del espacio público o prevenir suicidios, las instituciones analizadas publican los contenidos exponiendo los rostros de los ciudadanos sin ningún filtro.

Esto lesiona el derecho a la intimidad de las personas captadas con intención de ejemplarizar o aquellas que circunstancialmente se encuentran en la escena utilizada como propaganda.

La CSCG es la institución que con mayor frecuencia expone rostros en su cuenta de Twitter para informar sobre robos, control de personas, accidentes de tránsito u otras infracciones. El Consejo de Seguridad de Cuenca y el ECU 911 lo hacen también en menor medida, y con mayor precaución. La investigación encontró también buenas prácticas como fue el caso de los Agentes de Control Metropolitano de Quito que en todas sus publicaciones difumina el rostro de las personas que se ven involucradas en las imágenes captadas.

Entre julio y octubre, Fundamedios revisó decenas de tuits del ECU 911 (@ECU 911), de la Corporación para la Seguridad Ciudadana de Guayaquil (@cscgye), del Consejo de Seguridad de Cuenca (@CSC_CUENCA) y del Cuerpo de Agentes de Control Metropolitano de Quito (@agentesdequito) para analizar qué contenidos grabados por los sistemas de videovigilancia son difundidos al público y en qué medida esto vulneran o no el derecho a la privacidad de los y las ciudadanas.

La investigación constató que la exposición de rostros es evidente en eventos como accidentes de tránsito, intentos de suicidio, fiestas clandestinas u operativos de control en espacios públicos (consumidores de bebidas alcohólicas y estupefacientes en la vía pública, exceso de aforo permitido, etc).

Las cuatro instituciones analizadas manejan diversos protocolos y estándares para el uso de imágenes obtenidas de los sistemas de videovigilancia para la difusión institucional. Por un lado, el ECU 911 emplea las imágenes obtenidas de la videovigilancia, principalmente, para el control de tránsito en carreteras y en las calles de las principales ciudades. No obstante, se pudo constatar que los ECU 911 regionales, con el pretexto del control de aglomeraciones en el espacio público, exponen el rostro de las personas sin ningún filtro con el objeto de informar a la ciudadanía las actividades que realizan.

Control de aglomeraciones en el espacio público.
ECU 911, @ECU911Esmeralda, https://twitter.com/ECU911Esmeralda/status/1448794484888768513

Si bien el ECU 911 utiliza las redes sociales con una tónica informativa y de prevención, existen intentos de suicidio que fueron expuestos en sus redes sociales durante el periodo analizado. En los ejemplos encontrados no se aprecia de forma nítida el rostro de la persona cuyo intento de suicidio fue captado, pero es evidente que las restricciones y protocolos institucionales para presentar contenidos de tanta sensibilidad para la persona involucrada no son lo suficientemente rigurosos y pueden vulnerar los derechos de privacidad e intimidad de estas personas. Además, ¿qué pasaría si las cámaras empleadas para detectar este incidente serían más modernas y con un mejor zoom? Seguramente el rostro de la persona captada sería fácilmente identificable.

Intento de suicidio.
ECU 911, @ECU911_, https://twitter.com/ECU911_/status/1443322397294215169,

En la cuenta de Twitter del Consejo de Seguridad de Cuenca también se encontraron ejemplos de la exposición de rostros sin ningún filtro. Pese a que en entrevista con Fundamedios el director de la institución, Froilán Salinas, tenía clara conciencia de los límites legales impuestos a la difusión de estos contenidos y la obligación de resguardar este derecho, en la práctica ocurre lo contrario.

Control del aforo permitido en "Mundialito de los pobres".
Consejo para la Seguridad Ciudadana de Cuenca, @CSC_CUENCA, https://twitter.com/CSC_CUENCA/status/1444123795460083714

Control del uso y consumo de bebidas alcohólicas.
Consejo para la Seguridad Ciudadana de Cuenca, @CSC_CUENCA, https://twitter.com/CSC_CUENCA/status/1444123822358155266

La Corporación para la Seguridad Ciudadana de Guayaquil fue la institución que con más frecuencia vulnera el derecho a la intimidad de las personas. Si bien la videovigilancia puede usarse como una herramienta para la disminución del índice delictivo, la legislación nacional establece que todos los ciudadanos son inocentes hasta que se demuestre lo contrario y se emita una resolución judicial en firme. Presentar los rostros de personas en operativos de control o presuntos sospechosos de actos indebidos lesiona el derecho a la presunción de inocencia, pero además vulnera el de privacidad e intimidad.

Personas sospechosas. Al fondo se exponen incluso los rostros de menores de edad.
Corporación para la Seguridad Ciudadana de Guayaquil, @cscgye,
https://twitter.com/cscgye/status/1419052268507312130

Personas sospechosas en Guayaquil. Se capta el rostro de un ciudadano.
Corporación para la Seguridad Ciudadana de Guayaquil, @cscgye,
https://twitter.com/cscgye/status/1418998104309878792

Cuerpos de Agentes Metropolitanos de Quito, @agentesdequito,
https://twitter.com/agentesdequito/status/1434155624758194179

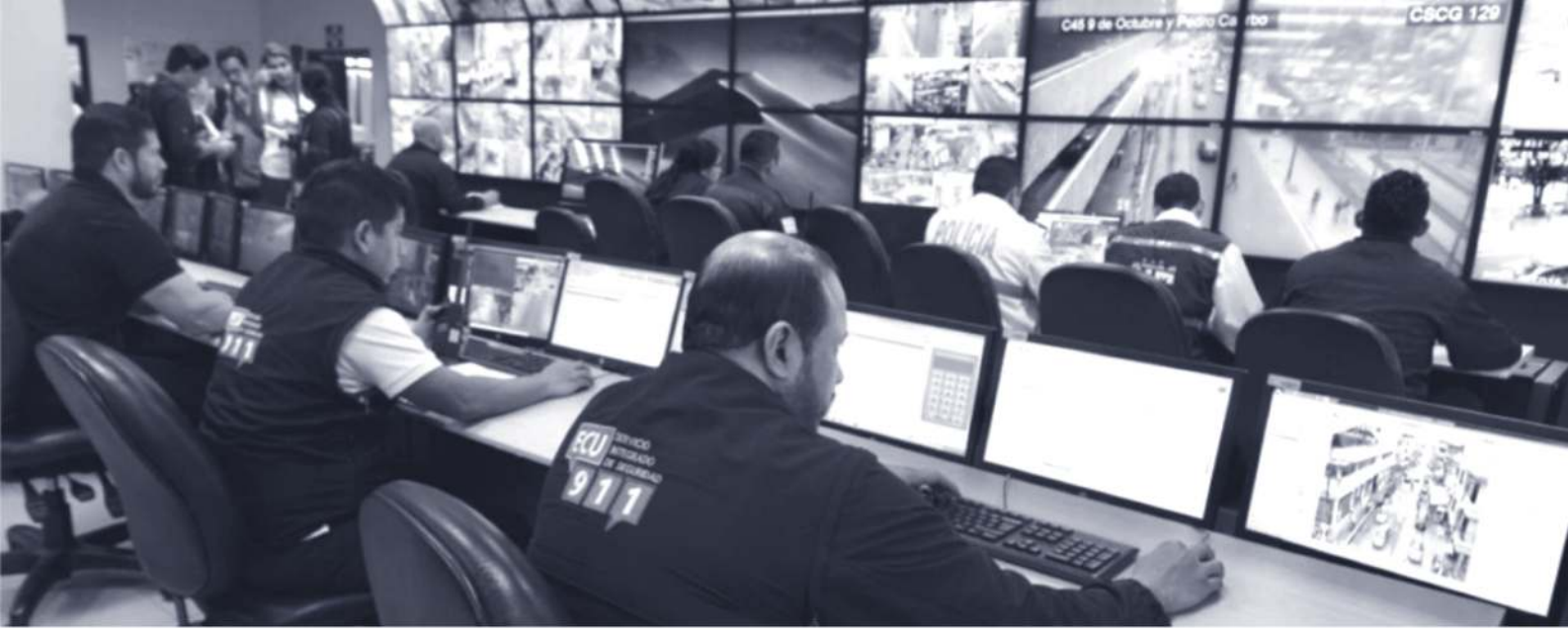
A diferencia de estas instituciones, el Cuerpo de Agentes de Control Metropolitano de Quito utiliza, de forma muy esporádica, imágenes obtenidas de los sistemas de videovigilancia en su red social. La mayoría de recursos multimedia corresponden a fotografías y videos producidos por el área de comunicaciones de la entidad. Esta institución sí usa filtros y difumina los rostros, incluso de transeúntes. Sin embargo, captamos un *tuit* en el que se difumina un *graffiti*, más no las caras de las personas que caminan en el espacio público.

Retiro de libadores de la vía pública.
Corporación para la Seguridad Ciudadana de Guayaquil, @cscgye, https://twitter.com/cscgye/status/1426802574775275523

Estos ejemplos claramente abren un debate en torno al uso indiscriminado de la videovigilancia y la difusión del contenido sin un criterio enfocado en derechos humanos, pues no solo se lesiona el derecho a la intimidad de una persona sino que también se la expone indiscriminadamente dejándola en estado total de indefensión como en el caso de personas con problemas de salud mental, como es el ejemplo de los intentos de suicidio.

TERCER CAPÍTULO

Los operadores de la vigilancia y sus procesos



El ECU 911 es la mayor plataforma de videovigilancia del país.

El Servicio Integrado de Seguridad ECU 911 es la plataforma tecnológica más grande de Ecuador que fue creada el 29 de diciembre de 2011 con Decreto Ejecutivo 998[21], bajo la presidencia de Rafael Correa. Esta herramienta tecnológica, integradora de los servicios de emergencia que prestan la Agencia Nacional de Tránsito, la Secretaría de Gestión de Riesgos, Bomberos, Policía Nacional, Fuerzas Armadas y otras instituciones, fue promocionada ante la ciudadanía como la iniciativa más exitosa para garantizar la seguridad ciudadana y reducir los indicadores delictivos.

En el discurso de inauguración del ECU 911 el entonces presidente, Rafael Correa, afirmó que, en una primera fase, la inversión para este centro de monitoreo, "el más moderno de América Latina", costaría 240 millones de dólares, y dejó en claro que el gobierno, la embajada y la empresa pública china serían responsables del levantamiento del sistema.

El artículo 5 del decreto de creación conformó un Comité Intersectorial integrado por: el Ministro Coordinador de Seguridad o un delegado; el Ministro de Defensa o delegado; Ministro del Interior o delegado; Ministro de Salud o delegado; Ministro de Telecomunicaciones y de la Sociedad de la Información o delegado; Secretario Nacional de Gestión de Riesgos o delegado y Secretario Nacional de Inteligencia. La secretaría técnica la asumió el titular del Ministerio Coordinador de Seguridad, en ese entonces, Homero Arellano.

Entre las principales funciones del Comité están expedir políticas intersectoriales en crisis internas; promover la realización de estudios técnicos, legales y evaluaciones; aprobar planes estratégicos, informe de labores, presupuestos, normas y procedimientos, entre otras funciones.

El Decreto Ejecutivo 988 no incluye salvaguardas de los derechos ciudadanos en relación al uso de datos de videovigilancia o recolección de los mismos.

El 24 de junio de 2013, el ECU 911, a través de la reforma al Decreto Ejecutivo 998, adquirió personalidad jurídica y autonomía administrativa, operativa y financiera.

Expertos consultados por Fundamedios aseguran que la creación de este sistema de seguridad pública por un decreto ejecutivo podría poner en riesgo su independencia y constituirse con otros fines violatorios de los derechos humanos.

El ECU 911 actualmente cuenta con 16 centros a nivel nacional y desde 2019 está dirigido por el ingeniero Juan Zapata.

[21] Decreto 998, Rafael Correa, creación de ECU 911, https://www.ecu911.gob.ec/TransparenciaArchivo/ENERO2015/Anexos%20a2/DECRETO-988.pdf

La videovigilancia del ECU 911, cifras y alcances.

El Sistema Integrado del ECU 911 trabaja los 365 días del año. Al 22 de octubre de 2021, 925 evaluadores laboraban en operaciones de videovigilancia. De ellos, 478 son funcionarios directos del ECU 911 y 447 de instituciones articuladas.

De acuerdo a estadísticas publicadas en el sitio web del ECU 911[22], desde el 01 de enero de 2020 al 19 de noviembre de 2021 se han reportado 675.191 alertas recibidas por sistemas de videovigilancia en el país, es decir, un promedio de 657 por día.

Desde 2012 al 22 de octubre de 2021, el ECU 911 cuenta con 5.002 cámaras de videovigilancia (largo alcance, domo, fija, lectora de placas, térmica, etc) en todo el país. Guayas, Manabí y Pichincha son las provincias con mayor número de cámaras: 686, 536 y 842 respectivamente. Cabe indicar que aún no existen cámaras de reconocimiento facial.

PROVINCIA	NÚMERO DE CÁMARAS	TIPO
Azuay	306	Domo, fija, lectora de placas
Bolívar	54	Domo
Cañar	74	Domo, fija
Carchi	129	Domo, fija, largo alcance, lectora de placas
Chimborazo	118	Domo, fija, largo alcance
Cotopaxi	117	Domo, domo HD, fija, largo alcance, térmica
El Oro	280	Domo, fija, largo alcance, lectora de placas
Esmeraldas	255	Domo, fija, largo alcance, lectora de placas
Galápagos	29	Domo, domo HD, largo alcance
Guayas	686	Domo, domo HD, fija, Hikvision, Huawei Domo, largo alcance, lectora de placas
Imbabura	287	Domo, fija, largo alcance

[22] ECU 911, web https://www.ecu911.gob.ec/

PROVINCIA	NÚMERO DE CÁMARAS	TIPO
Loja	175	Domo, fija, largo alcance, lectora de placas.
Los Ríos	187	Domo, fija, lectora de placas.
Manabí	536	Domo, largo alcance.
Morona Santiago	119	Domo, domo HD, fija, largo alcance
Napo	28	Domo y fija.
Orellana	6	Domo.
Pastaza	33	Domo, domo HD, fija.
Pichincha	842	Domo, fija y largo alcance.
Santa Elena	85	Domo, domo HD, fija, Huawei domo, largo alcance
Santo Domingo de los Tsáchilas	182	Domo y fija.
Sucumbíos	121	Domo, fija, Huawei domo, largo alcance, lectora de placas.
Tungurahua	324	Domo, domo HD, fija, largo alcance, lectora de placas térmica.
Zamora Chinchipe	29	Domo y fija.

Las cámaras domo tienen la capacidad de moverse en tres ejes por la cúpula semiesférica que poseen, mientras que las de largo alcance permiten monitorear zonas elevadas, incluso los volcanes..

El ECU 911 no cruza bases de datos con otras instituciones pues, hasta el momento, no se ha hecho operativa la tecnología de reconocimiento facial ni el software para que un rostro captado sea asociado con la identidad de una persona.

Fundamedios consultó al Registro Civil sobre un eventual cruce de información de datos personales. “Actualmente, la Dirección General de Registro Civil, Identificación y Cedulación DIGERCIC, no posee un instrumento

legal suscrito con el Sistema Integrado ECU 911 para intercambio o tratamiento de datos personales", señaló la institución en un oficio.

Si hay un convenio con la Policía Nacional del Ecuador para la verificación manual por parte del operador, para revisar en línea la identidad de personas registradas en la base de datos de la DIGERCIC, a través de un servicio web. Este servicio proporciona información sobre la condición de cedulado, número de cédula, apellido(s), nombres(s), fecha de nacimiento, nacionalidad, estado civil, nombre del cónyuge, instrucción, profesión u ocupación, fecha de defunción, fecha de expedición de cédula, sexo, lugar de nacimiento y fecha de matrimonio.

Las 18 cámaras de reconocimiento de placas que tiene el ECU 911 en el país sí funcionan con una base de datos y un software que solamente maneja la Policía Nacional. El ECU 911 solamente brinda el medio tecnológico que es la cámara con el algoritmo de lectura de placas. Bolívar Tello, director de Operaciones del ECU 911, explicó que la Policía tiene asignadas cámaras específicas de vigilancia en "puntos calientes" donde hay mayor índice delictivo o problemas de orden público. "Ellos (Policía) tienen la base de datos, nosotros no intervenimos en esa base de datos, no conocemos esa base de datos y lo que hacemos es enviarles nuestro registro de las cámaras de nuestros chequeos (...) Policía Nacional hace un chequeo con la base de datos que tienen y determinan si ese vehículo es robado o no, o si está inmerso en algún delito".

Ecuador va hacia la masiva implementación de tecnología de reconocimiento facial.

Al momento de esta investigación el ECU 911 no cuenta con la tecnología de reconocimiento facial. Juan Zapata, director de la institución, dijo en entrevista a Fundamedios que hasta finales de 2021 esperan adquirir por primera vez esta tecnología biométrica y mejorar la ya existente dentro de una fase de repotenciación.

Hasta el 05 de octubre de 2021, el ECU 911 estaba en la etapa preparatoria del proceso de adquisición de 1.294 cámaras con reconocimiento facial. Hasta el cierre de esta investigación, tanto el ECU 911 como la Policía Nacional, mantenían conversaciones para evaluar "la pertinencia de realizar la adquisición de cámaras con características de reconocimiento facial". Además, la Contraloría General del Estado se encontraba realizando un informe de pertinencia como requisito previo a la suscripción de los procesos de contratación pública en el Servicio Nacional de Contratación Pública (SERCOP).

Actualmente, las autoridades del ECU 911 analizan con la Policía Nacional la tecnología más adecuada para implementarla en la fase de repotenciación y junto al Departamento de Criminalística también evalúan el uso de un software que sea compatible para el cruce con la base de datos que, según Juan Pablo Torres, siempre va a estar encriptada, protegida y de acceso único para la Policía Nacional.

Fundamedios envió un pedido de información a Policía Nacional el 16 de agosto en el que se solicitaba información acerca del cruce de bases de datos con otras instituciones, pero el requerimiento nunca fue contestado. También solicitamos una entrevista con la Comandante General, Tannya Varela, pero también nos fue negada.

El ECU 911 además, encamina dos procesos más para potenciar su tecnología. El primero contempla la compra de 23 drones sin reconocimiento facial y el segundo proceso contratará un sistema de video wall para tres centros. Estos procesos estuvieron en el Sercop pero el primero fue suspendido y el segundo cancelado por violación sustancial de un procedimiento precontractual.

Más de 180 millones de dólares en contratos y atados a proveedores chinos.

Los contratos desde 2012 al 2017 para la adquisición del sistema de videovigilancia (cámaras) ascendieron a 180' 368.626,50 USD, según información entregada por el ECU 911. De este valor, (178 '151.920 USD) correspondió a créditos chinos entre 2012 y 2016 usados para la implementación tecnológica del ECU 911 adjudicados a la empresa estatal China National Electronic Import (CEIEC).

Juan Pablo Torres, subdirector de tecnología del ECU 911, reconoció que cuando se realizan contratos de esta índole, la tecnología desarrollada por CEIEC es única y esa característica hace que se necesite la contratación de la empresa para el mantenimiento posterior de la plataforma. Si bien, el contrato feneció en 2018, esta condición obliga al ECU 911 a contratar los servicios para mantenimiento de sistemas de seguridad ciudadana con régimen especial y sin concurso público.

Para la adquisición del sistema de videovigilancia (cámaras), el ECU 911 registra cuatro contratistas: BPE Electronic, Huawei Technologies CO LTDA, Conexión Total S.A. COTOT y China National Electronic Import (CEIEC).

El mantenimiento del sistema de videovigilancia requiere otro presupuesto. Entre 2014 y 2021, se destinaron 6 '455.041,05 USD para este fin, siendo Richard Alberto Apolo Loaiza el contratista que mayor monto recibió en estos años (2' 831.774,66 USD), seguido por Conexión Total S.A. COTOT (2' 458.529,21 USD).

A CEIC además de la implementación tecnológica también se le asignó la construcción de varios centros del ECU 911. La estatal china celebró el contrato 17 (monto de 38.1 millones USD) y además, se comprometió a concluir con la construcción de otros centros mediante el contrato 045 que, inicialmente, le fue otorgado a la empresa china Engineering Co. Ltd. CAMC (monto de 68.1 USD). Debía construir 12 centros del ECU 911, pero sólo entregó siete, pese a que cobró la totalidad del monto.

El informe con indicios de responsabilidad penal de la Contraloría General del Estado de 2017, reveló un sobreprecio en la construcción de los centros y glosas por 33' 256.991,63 USD. Esta información fue publicada en 2018 por el medio de comunicación Portal de Investigación[23].

Cabe indicar que en 2020 EE.UU sancionó a la estatal china CEIC por "restringir el servicio de internet y realizar vigilancia digital y operaciones cibernéticas contra oponentes políticos" en Venezuela.

Gobiernos Autónomos Descentralizados (GADS).

El artículo 54, literal n, del Código Orgánico de Organización Territorial, Autonomía establece la creación y coordinación de los consejos de seguridad ciudadana municipal con la participación de la Policía Nacional, la comunidad y otros organismos relacionados con la materia de seguridad para formular y ejecutar políticas locales, planes y evaluación de resultados sobre prevención, protección, seguridad y convivencia ciudadana.

En esa línea, el Municipio de Quito cuenta con la Secretaría de Seguridad y Gobernabilidad; el Municipio de Guayaquil con la Corporación de Seguridad Ciudadana de Guayaquil; Cuenca con el Consejo de Seguridad Ciudadana de Cuenca y el Municipio de Latacunga con un departamento destinado para este fin.

Estos cuatro municipios han establecido sus protocolos de atención a la seguridad ciuda-

[23] PERIODISMO DE INVESTIGACION, ECU 911, más de USD 33 millones de perjucio, 13 septiembre 2018, https://periodismodeinvestigacion.com/2018/09/13/ecu-911-mas-de-usd-33-millones-de-perjuicio/

dana y tienen sistemas de videovigilancia, independientes del ECU 911. Los municipios de Quito, Cuenca y Latacunga tienen cámaras con capacidad de reconocimiento facial pero, al cierre de esta investigación, no ejercen su capacidad biométrica al no estar conectados con una base de datos. La Corporación de Seguridad Ciudadana de Guayaquil manifestó no tener cámaras con estas características; sin embargo, Fundamedios accedió a un contrato suscrito por la entidad en 2020 en la que adquirió más de 100 cámaras con estas características.

Consejo de Seguridad Ciudadana de Cuenca.

El Consejo de Seguridad Ciudadana de Cuenca tiene 185 cámaras en la ciudad (adquiridas entre 2019 y julio de 2021). De estas, 10 tienen la capacidad de reconocimiento facial y fueron compradas por la capacidad de mayor zoom, resolución y alcance, dentro de un proceso de mantenimiento para reemplazar cámaras ya existentes. Sin embargo, no se ha activado la tecnología biométrica ni se han cruzado con bases de datos dichas cámaras.

Nº DE CÁMARAS	PARROQUIA
14	Yanuncay
2	Sinincay
14	Machángara
10	Bellavista
15	El Vecino
8	Huayna Capac
16	Monay
10	Totoracocha
5	Hermano Miguel
11	San Sebastián
9	Ricaurte
4	Turi
3	Sucre
13	Batán
5	San Blas
7	Cañaribamba

Nº DE CÁMARAS	PARROQUIA
7	Baños
7	San Joaquín
8	Nulti
1	Tarqui
5	Gil Ramírez Dávalos
1	Paccha
1	Llacao
8	El Sagrario
1	Molleturo

"Al momento el Consejo de Seguridad Ciudadana no tiene bases de datos de personas, ni de rostros, ni de características biométricas (...) estamos muy claros que dentro de nuestras competencias, esa característica técnica del sistema deberá responder a quien mantiene la custodia de aquello, que es básicamente Policía Nacional, a través de las listas de los más buscados o de personas desaparecidas. La intención del Consejo de Seguridad Ciudadana no es tener bases de datos, ni acceso a las mismas", aseguró Froilán Salinas, director de la entidad.

El sistema de videovigilancia monitorea incidencias, que son acciones a controlarse en el espacio público como aglomeraciones, tráfico vehicular, libadores en la vía pública, accidentes de tránsito y delitos. Sin embargo, estos últimos incidentes no son difundidos en redes sociales pues tienen acuerdos de confidencialidad con la Fiscalía cuando son solicitados dentro de una investigación judicial. Desde 2019 al 2021 el Consejo entregó 126 vídeos obtenidos de las cámaras de videovigilancia a operadores de justicia.

Toda la información generada de los sistemas de videovigilancia se almacena por 60 días en un storage físico en el data center local al que también tiene acceso el ECU 911 a través de un acuerdo de mutua cooperación. De hecho, las cámaras también están enlazadas al sistema nacional ECU 911.

La información obtenida de las cámaras de videovigilancia no es reservada, tampoco sus protocolos o instructivos. El Manual de Procedimientos establece que un operador que monitorea incidencias puede determinar posibles incidentes, haciendo un seguimiento de videos y emitiendo un informe (en el caso que fuese necesario) para activar la intervención de Policía Nacional o de otras instituciones si fuese necesario.

Froilán Salinas no descarta que podrían generarse márgenes de error al captar incidentes por avería de las cámaras, ausencia de las mismas en espacios públicos, entre otros factores. Sin embargo, cree que de ejecutarse el reconocimiento facial o implementarse la tecnología biométrica, tampoco garantiza la eliminación de errores. "Al final, la inteligencia artificial termina siendo un algoritmo que realiza un patrón y que da un reporte, eso le descarga de trabajo al operador y le da mayor fiabilidad al sistema. Pero decir que va a captar todo lo que hay, decir que se van a eliminar errores humanos, no es así", explicó.

Considera que para aplicar el reconocimiento facial hay que ser cautos porque existe un vacío legal y una falta de normativa local. No hay tampoco un ente rector que establezca los límites en el uso de la tecnología y esto hace que los derechos humanos puedan verse lesionados. "Es necesario establecer hasta dónde llega esa videovigilancia (...) respetar el libre albedrío del ciudadano, no sentirse vigilado cuando no es necesario hacerlo", puntualizó.

Municipio de Latacunga.

El 13 de julio de 2021 entró en vigencia el plan *"Más cerca de tí"* con el propósito de controlar el uso del espacio público y promover una convivencia pacífica, a través de la implementación de un moderno sistema de videovigilancia con 26 cámaras HD y seis de reconocimiento facial, que se suman a los otros equipos antes instalados.

Nº DE CÁMARAS	PARROQUIA ASIGNADA
3	Juan Montalvo
6	Ignacio Flores
9	Eloy Alfaro
14	La Matriz

Pese a haber adquirido estas cámaras, la tecnología biométrica no se aplica al igual que el caso de Cuenca y, actualmente, la capacidad de reconocimiento de rostros se activa solamente para uso preventivo de la mascarilla en el contexto de la pandemia. El operador detecta a una persona (rostro) que no usa tapabocas pero no define su identidad porque no se encuentra asociada a ninguna base de datos.

Luigi Calderón, especialista 1 de Seguridad Ciudadana del GAD de Latacunga, explica que en el caso de detectar a una persona que no use la mascarilla, desde la sala de monitoreo se advierte de este hecho a un agente que esté cerca del sitio para que se acerque presencialmente a la persona que incumple con la Ordenanza y le advierta de una posible sanción.

Calderón dejó en claro que el sistema no considera como dato personal un rostro a menos que esté cotejado con una base de datos. En un oficio enviado por esta institución a Fundamedios se menciona que ningún funcionario maneja datos personales obtenidos del sistema de videovigilancia. Sin embargo, según la Ley Orgánica de Protección de Datos Personales, aprobada en mayo de 2021, considera el rostro como un dato personal.

El sistema de monitoreo del GAD de Latacunga reporta problemáticas del espacio público como el control del uso de sustancias no permitidas, consumo de bebidas alcohólicas, delitos o riñas callejeras. Cuando se visualizan estos incidentes a través de las cámaras, se da aviso a la Policía Nacional para que actúe.

El GAD municipal suscribió un convenio con el Comando de la Policía de la subzona Cotopaxi N° 05 para el reforzamiento de patrullajes en apoyo a la seguridad ciudadana en el que establece tres parámetros respecto al sistema de videovigilancia. El primer acuerdo es que el sistema esté interconectado al ECU 911 (que podría desarrollarse en 2022). El segundo es fortalecer el trabajo conjunto de los agentes de control municipal y la Dirección de Seguridad

Ciudadana con la Policía Nacional y el tercero menciona la ampliación de una base de datos del sistema de videovigilancia municipal para optimizar todos los recursos tecnológicos con los que se dispone.

Luigi Calderón no niega que la Policía Nacional pueda requerir este servicio. Aclara que el GAD no debe interconectarse a una base de datos de la institución. "Únicamente se ingresan los datos personales de las personas que se vaya a requerir buscar, lo que hace el sistema es que esa persona si algún rato pasó por alguna cámara, se va a dar la alerta (...) esa es la forma de operar de ese sistema en el caso de requerir la parte de reconocimiento facial", comentó.

Actualmente hay 12 servidores municipales en el sistema de monitoreo de la videovigilancia trabajando las 24 horas del día. Si bien la información de las cámaras y los protocolos, manuales e instructivos no tienen reserva, existen acuerdos de confidencialidad para la difusión de los contenidos de las cámaras, salvo cuando sean solicitados por los operadores de justicia o la ciudadanía.

Calderón aseguró que se tomó el modelo de gestión de la Corporación para la Seguridad Ciudadana de Guayaquil en el que se puede entregar el material a los ciudadanos con una petición escrita, acompañada de copias de sus documentos personales. Por ejemplo, en casos de afectación personal de un ciudadano víctima de un delito y que solicita la evidencia como prueba.

Fundamedios solicitó el reglamento bajo el cual opera el sistema de videovigilancia, pero se encontraba en fase de revisión técnica.

Corporación para la Seguridad Ciudadana de Guayaquil (CSCG).

Entre 2019 y julio de 2021, la CSCG contabilizó 132 cámaras del sistema de videovigilancia en Guayaquil. Según el oficio entregado a Fundamedios, la institución manifiesta que no cuenta con cámaras de reconocimiento facial, pero alaba la ventaja de esta tecnología para luchar contra la delincuencia, identificar a delincuentes y proteger a víctimas.

La Corporación para la Seguridad Ciudadana monitorea incidencias al igual que en las instancias de seguridad de otras ciudades antes mencionadas. De acuerdo al protocolo, los operadores alertan al Jefe de Sala de posibles hechos que alteren la seguridad ciudadana para que contacten a las instituciones pertinentes de ser el caso.

Las cámaras de la CSCG tienen un sistema espejo con las del ECU 911 y viceversa que, según la institución, sirven para visualizar la imagen de las cámaras de una y otra entidad más no para operar las mismas.

El Jefe de Sala es la única persona que tiene acceso directo al material del sistema de videovigilancia y a la descarga de grabaciones para atender solicitudes de operadores de justicia (garantizando la cadena de custodia), de otras instituciones y de la ciudadanía que debe exponerse el interés legítimo de acceder al material (esclarecimiento de accidentes, infracciones de tránsito, posibles robos, hurtos, esclarecimiento de accidentes, infracciones de tránsito, destrucción de bienes). Si un proceso se encuentra en etapa de indagación previa o proceso penal, no se entregan videos a particulares, solo a operadores de justicia.

ESTADÍSTICAS DE VIDEOS ENTREGADOS ENERO 2019 A DICIEMBRE 2019

ENTIDADES	ENERO	FEBRERO	MARZO	ABRIL	MAYO	JUNIO	JULIO	AGOSTO	SEPTIEMBRE	OCTUBRE	NOVIEMBRE	DICIEMBRE	TOTALES
FISCALÍA	242	78	235	275	180	222	224	324	240	238	190	248	2.696
CIUDADANÍA	74	27	57	63	65	56	74	63	53	70	56	43	701
CTE	18	13	1	14	23	22	10	22	17	8	9	14	171
ATM	14	3	18	16	19	19	25	16	11	13	10	12	176
POLICIA	2	2	17	3	1	4	1	1	3	2	6	1	43
TOTALES	350	123	328	371	288	323	334	426	324	331	271	318	3.787

ESTADÍSTICAS DE VIDEOS ENTREGADOS ENERO 2020 A DICIEMBRE 2020

ENTIDADES	ENERO	FEBRERO	MARZO	ABRIL	MAYO	JUNIO	JULIO	AGOSTO	SEPTIEMBRE	OCTUBRE	NOVIEMBRE	DICIEMBRE	TOTALES
FISCALÍA	295	154	89	10	21	451	354	497	501	241	116	212	2.941
CIUDADANÍA	62	50	16	0	0	18	42	20	45	40	38	27	358
CTE	16	20	9	0	0	65	47	35	33	29	20	22	296
ATM	3	4	1	0	0	10	12	17	27	29	10	0	113
POLICIA	0	0	0	0	0	1	3	1	1	3	2	1	12
TOTALES	376	228	115	10	21	545	458	570	607	342	186	262	3.720

ESTADÍSTICAS SOLICITUDES DE VIDEOS ENTREGADOS DE ENERO 2021 A DICIEMBRE 2021

ENTIDADES	ENERO	FEBRERO	MARZO	ABRIL	MAYO	JUNIO	TOTALES
FISCALÍA	295	253	240	404	209	330	1.731
CIUDADANÍA	39	35	11	41	17	54	197
CTE	26	36	13	21	28	38	162
ATM	3	11	12	23	4	22	75
POLICIA	1	1	5	4	0	4	15
TOTALES	364	336	281	493	258	448	2.180

La CSCG señala que en caso de optar por una tecnología biométrica, “el acceso a la base de datos donde se encuentra dicha información y el uso de dicha tecnología serán exclusivos para la Policía Nacional, en razón de ser aquella la entidad competente para el manejo de las imágenes, debiendo resaltarse además que tal reconocimiento facial se circunscribiría exclusivamente a ciudadanos que hayan recibido sentencias por delitos cometidos que amenacen la seguridad de la población”.

Pese a que la Corporación señaló en su oficio que no ha adquirido cámaras con reconocimiento facial, Fundamedios accedió al contrato CSCG-SIE-007, suscrito el 12 de noviembre de 2019, en el que se adquirieron 100 cámaras de videovigilancia con megafonía y analítica de reconocimiento facial para la vigilancia de centros educativos en Guayaquil concedido a Unión Eléctrica S.A. por 2’ 569.906,41 USD.

Fundamedios solicitó una entrevista en dos ocasiones con Christian Chérrez, director de la CSCG, para aclarar este tema, pero la petición nunca fue contestada. El 25 de octubre, la organización pidió una entrevista con la alcaldesa del Municipio de Guayaquil, Cynthia Viteri, tras el anuncio del convenio entre el Municipio y la Corporación para la Seguridad Ciudadana de Guayaquil para adquirir 15 mil cámaras de reconocimiento facial con una inversión de más de 30 millones de USD a un plazo de cuatro años. Este plan ha sido denominado "Servicio de sistema automatizado de monitoreo y alerta de captura, transmisión, almacenamiento y análisis de información de audio y video con analítica de datos automática. La entrevista no fue otorgada.

Secretaría de Seguridad y Gobernabilidad del Municipio de Quito.

En Quito, existen 958 cámaras destinadas a la videovigilancia adquiridas entre 2018 y 2020. Están ubicadas en el parque Metropolitano (norte), mercados, centro histórico de la capital, en El Panecillo y en otros espacios públicos. Una cuarta parte de las cámaras (237) son de reconocimiento facial (analítica de video).

NÚMERO DE CÁMARAS	UBICACIÓN	AÑO
15	Parque Metropolitano	2018
19	Espacios Públicos	2018
78	Centro de Quito (Fase I)	2019
24	Quitumbe (Fase II)	2020
2	Sur de Quito (Fase II)	2020
20	Calderón (Fase II)	2020
21	Centro de Quito (Fase II)	2020
3	La Delicia (Fase II)	2020
48	La Mariscal (Fase II)	2020
3	Tumbaco (Fase II)	2020
4	Norte de Quito (Fase II)	2020

Al igual que las otras ciudades tienen capacidad biométrica pero no están conectadas a ninguna base de datos, según información entregada por la institución. “El sistema de videovigilancia con analítica de video del Municipio de Quito funciona correctamente dentro de las competencias municipales, sin la necesidad de conectarse a una base de datos externa (ejemplo: Policía Nacional, Fiscalía, etc…) debido a que puede crear bases de datos propias de acuerdo a sus necesidades y competencias. Sin embargo, está disponible como apoyo a las Entidades del Sistema Integrado de Seguridad Metropolitano cuando estas lo requieran”, indica el oficio.

Fundamedios solicitó los documentos y minutas donde conste un análisis jurídico de la legalidad del uso de programas de reconocimiento facial, tomando en cuenta la consideración a posibles afectaciones al derecho a la intimidad, pero la Secretaría afirmó que no le corresponde la elaboración de dichos documentos.

El Cuerpo de Agentes de Control Metropolitano de Quito que es responsable de las actividades de monitoreo y videovigilancia, según el artículo 268 del Código Orgánico de las Entidades de Seguridad Ciudadana y Orden Público, también evadió la inquietud al ser consultado. Aseguran que los proyectos de videovigilancia se encuentran bajo la custodia de EP EMSEGURIDAD.

Daniela Valarezo, secretaria de Seguridad y Gobernabilidad del Municipio de Quito, en entrevista con Fundamedios, reconoció que las cámaras no tienen activada su capacidad de reconocimiento facial porque no están conectadas a una base de datos. Pese a ello, el cabildo de Quitó deberá pagar hasta el 2023, 460 mil USD para el mantenimiento de los equipos, cuya función es subutilizada.

Antes de realizar la conexión de datos con Policía Nacional, la secretaria de Seguridad asegura que trabajarán en un modelo de gestión para articular el funcionamiento de esas cámaras entre sí y que sean compatibles con el ECU 911, pues esperan que sea la institución que opere los equipos. “Esto no significa que el Municipio deje de utilizar el sistema de videovigilancia para responder desde el ECU 911, cualquier circunstancia que amerite la atención municipal”, explicó la Secretaria anunciando además que también se incluirán las 172 cámaras de la Empresa municipal de pasajeros, ninguna de ellas con reconocimiento facial.

Una vez concluido con este proceso, está previsto que para 2022 se compagine el sistema de analítica de las 203 cámaras con el departamento de Criminalística de la Policía Nacional, que será la única entidad que maneje la base de datos.

Valarezo reconoce que las imágenes obtenidas de las cámaras de reconocimiento facial son “sensibles” y por ello está previsto capacitar a los funcionarios que realizan tareas de videovigilancia no solo en el ámbito técnico sino también en derechos. Asegura que el rostro es un dato personal. Sin embargo, el gerente de EP EMSEGURIDAD, Adrián Haro, aseguró en un oficio enviado a Fundamedios el 29 de julio de 2021, que en el monitoreo de videovigilancia no se receptan datos personales, lo cual deja entrever una falta de concordancia respecto a definiciones trascendentales entre funcionarios públicos.

Contrataciones y proveedores de tecnología biométrica sin operar.

En Quito, Cuenca, Guayaquil y Latacunga hay un símil. Estas ciudades cuentan con cámaras de reconocimiento facial que funcionan pero no se ha activado su capacidad biométrica, pese al monto destinado para su adquisición.

En las cuatro ciudades existen 353 cámaras con capacidad de reconocimiento facial, cuya compra suma 2’973.108,81 de USD sin incluir el software de reconocimiento facial, las licencias de reconocimiento facial, el servidor de reconocimiento para rostros y otros soportes que suman más de 400.000 USD, solo en el caso del Municipio de Quito (2019 y 2020).

INSTITUCIÓN	CARACTERÍSTICAS DE CÁMARAS	Nº DE CÁMARAS	COSTO UNITARIO	COSTO TOTAL
Municipio de Quito (I Fase)	Cámara PTZ 4 MP 36 X Marca Hikvision Modelo DS-2DF8A436IX-AEL	46	2.551 USD	117.346 USD por 46 cámaras
Municipio de Quito (I Fase)	Cámara Bala 4 MP Marca Hikvision Modelo DS- 2CD7A46G0-IZS	32	976 USD	31.232 USD por 32 cámaras
Municipio de Quito (II Fase)	Cámara PTZ 4 MP 36X Marca Hikvision Modelo DS-2DF8A436I (N) X-AEL (C)	49	2.550 USD	124.950 USD por 49 cámaras
Municipio de Quito (II Fase)	Cámara Bala 4M CAPTURA FACIAL / Marca Hikvision Modelo DS-2CD7A46G0-IZ (H) S	76	950 USD	72.200 USD por 76 cámaras.
Municipio de Cuenca	Cambio a cámara PTZ 4 MP 36 X	10	3.262 USD	36.534, 40 USD por 10 cámaras antiguas adecuadas a la nueva tecnología.
GAD Latacunga	CÁMARA IP PTZ 42X	6	3.490 USD	20.940 USD por 6 cámaras
Corporación para la Seguridad Ciudadana de Guayaquil	No se especifica ni modelo, ni valor unitario de cámaras ni el detalle de la instalación.	100	2'569.906.41 USD	2'569.906.41 USD
ECU 911	No se especifica el modelo de las cámaras ni el monto para instalación.	1.294	En análisis	No hay monto
Municipio de Guayaquil	No se especifica el modelo de las cámaras ni el monto para instalación.	15.000	No hay monto	30 millones USD (2022,2023,2024 y 2025)

El Municipio de Quito realizó dos contrataciones entre 2019 y 2020 de 203 cámaras con reconocimiento facial en dos fases a través de los procesos SIE-EMS-06-2019 y SIE-EMS-04-2020. En total adquirió 203 cámaras. Las cámaras tienen la capacidad de captar hasta 30 rostros al mismo tiempo. El servidor de reconocimiento facial soporta un análisis facial, comparación de rostros en la imagen, vídeo en tiempo real y grabación de video. Las características técnicas de atributo facial detectan el género, la edad, las gafas y la sonrisa y puede comparar 240 piezas (imágenes de la cara) por segundo. La biblioteca agrupa al menos un millón de listas de comparación de rostros. El servidor tiene 40 canales de reconocimiento facial con 16 TB de almacenamiento para rostros.

Estas características no están siendo usadas y las autoridades consultadas en Quito, Cuenca y Latacunga aseguraron que las cámaras fueron compradas por su excelente capacidad de zoom, más no solo por la característica de reconocimiento facial.

Fundamedios comparó los precios de estas cámaras con otros equipos de características similares pero sin la capacidad de reconocimiento facial para evaluar la diferencia en los costos. Según el catálogo de junio de 2021 de la marca Hikvision, una cámara IP TUBO 8MP 4K, modelo DS 2CD2683G1-IZS, cuesta 394,62 USD, otra más moderna PTZ con la capacidad de rotar y con un zoom de 32x asciende a 948,63 USD. Ambas sirven para realizar tareas de videovigilancia con excelen-

tes resultados, según fuentes consultadas que prefirieron no ser citadas.

Cabe indicar que las características de las cámaras adquiridas por el Municipio de Quito son muy similares a las de Cuenca y Latacunga.

Llama la atención que en el caso de Cuenca, las cámaras de videovigilancia fueron adecuadas para reconocimiento facial. Sin embargo, el monto unitario para esta adecuación incluso es más alto que una cámara nueva adquirida por el Municipio de Quito (ver cuadro superior).

En el caso de Quito y Latacunga existen similitudes en las contrataciones. Las empresas Andeantrade y el Consorcio de Reconocimiento Facial de Quito (firmas Fulltec Cia.Ltda, C y Megasupply) sellaron contratos con el Municipio de Quito para adquirir las cámaras de reconocimiento facial entre 2019 y 2020.

Mientras que el GAD de Latacunga firmó un contrato con el Consorcio de Cámaras de Reconocimiento Facial de Latacunga que, en el Servicio de Rentas Internas (SRI), aparece como Fulltec, cuyos administradores son: Joe Luis Burbano y Óscar Trujillo, los mismos que administran Andeantrade, la empresa que ganó el concurso para Quito y que también brindó mantenimiento al sistema de videovigilancia del ECU 911 en 2020 por 58.698,88 USD.

La Corporación para la Seguridad Ciudadana de Guayaquil (CSCG) cuenta con otros proveedores desde 2019: Unión Eléctrica, Dilexa y Humanitas S.A. El primero de ellos ha sellado contratos con la institución, incluso desde años anteriores. También es proveedor para otras instituciones como Cuerpo de Bomberos y la Empresa Pública de Hidrocarburos. En 2019 suscribió un contrato CSCG-SIE-007 -2019 por más de 2 millones USD para la compra de 100 cámaras de reconocimiento facial y su instalación. En el contrato ni siquiera se especifican los montos desglosados por los servicios.

En Cuenca hay dos proveedores desde 2019. Se trata de Juan Diego Villavicencio, representante legal de la empresa Techtronic y Juan Andrés Granda, representante de Tesla, una empresa que no consta en la Superintendencia de Compañías y cuya dirección colocada en un sitio web poco amigable dirige a una dirección física inexistente rastreada por Google maps.

RECOMENDACIONES

El 30 de noviembre de 2021, Fundamedios realizó el diálogo virtual *"Videovigilancia en Ecuador desde la perspectiva de los Derechos Humanos"* con representantes de las instituciones enmarcadas en la presente investigación y participantes de la sociedad civil. El propósito fue presentar de primera mano los hallazgos a las entidades públicas a cargo de la videovigilancia y recoger sus comentarios finales en este informe.

Recomendaciones de Fundamedios.

- En concordancia con la moratoria solicitada por la ONU, insta a que las entidades públicas del Ecuador a que se abstengan de implementar mecanismos de vigilancia biométrica, como es el reconocimiento facial.
- Solicitar a la Asamblea Nacional que dicte leyes y/o reglamentos que regulen con precisión el funcionamiento de la videovigilancia y el uso de herramientas de inteligencia artificial para que cumpla con estándares de derechos humanos.
- Instar a la ciudadanía a defender su derecho a la privacidad y derechos asociados.
- Levantar la reserva que tiene el ECU 911 respecto a "toda la información contenida en manuales, protocolos y procedimientos, metodología e instructivos generados y que lleguen a generarse en el ECU 911 como consecuencia o para la prestación del servicio de despacho de recursos para la atención de emergencias, videovigilancia y recepción de llamadas a la línea única 911". Esta reserva fue declarada secreta en 2013 por decreto ministerial hasta 2028.
- Cumplir con los estándares internacionales de derechos humanos que establecen que los Estados deben tomar medidas eficaces para impedir la retención, el procesamiento y el uso ilegales de datos personales almacenados por las autoridades públicas y por empresas.
- Generar políticas públicas que incluyan la capacitación de servidores y operadores judiciales en la protección del derecho a la privacidad que podría ser vulnerado con la videovigilancia y en mayor medida con el reconocimiento facial.
- Mejorar los protocolos internos de cada institución pública para que la información obtenida de la videovigilancia no se difunda sin filtro en las redes sociales de los organismos a manera de relaciones públicas.

- Generar una cultura institucional transparente y cumplir con lo estipulado en la Ley Orgánica de Acceso a la Información Pública (Lotaip) para la entrega de información en el plazo de 10 días contemplado en la legislación.

Recomendaciones y comentarios de participantes en el diálogo entre partes interesadas.

- Bolívar Tello, subdirector técnico de Operaciones del ECU 911, aceptó algunas recomendaciones presentadas por Fundamedios respecto al manejo correcto de imágenes de videovigilancia en redes sociales; sin embargo, estuvo en desacuerdo respecto a frenar el reconocimiento facial en videovigilancia pues a su criterio es una herramienta que garantiza la seguridad y previene el delito. Eso sí mencionó que es importante tener ética y respetar la privacidad, logrando un equilibrio entre ambos. Pero defendió la implementación de la tecnología para luchar contra la delincuencia y planteó las siguientes inquietudes: "¿Qué pasa con el 8% de delitos que se concentran en el espacio público en América Latina? ¿Cómo vamos a controlar estos delitos? ¿Qué pasa cuándo exista un conflicto y nosotros no tenemos la videovigilancia para controlar ciertas alteraciones de orden público que son más del 80% en Ecuador y el 20% es violencia criminal?"

- Para Luigi Calderón, jefe de seguridad ciudadana del GAD de Latacunga, la seguridad de los ciudadanos es primordial en este momento y por ello es necesario generar políticas públicas adecuadas para reducir la percepción de inseguridad. La videovigilancia representa un ahorro para el control del espacio público. Sin embargo, reconoce que el sistema normativo ecuatoriano no es claro sobre las limitaciones del uso de la videovigilancia y las herramientas de inteligencia artificial.

- Froilán Salinas, director del Consejo de Seguridad Ciudadana de Cuenca, concordó que en Ecuador no hay una estructura jurídica adecuada. El marco normativo se establece con la Ley Orgánica de Protección de Datos y la Ley Orgánica de Transparencia y Acceso a la Información Pública, pero a su criterio en ninguno de los cuerpos legales se determina quién es el ente regulador de la videovigilancia y de control que establezca límites claros. Esto a su criterio puede vulnerar derechos humanos, pues incluso solo con la videovigilancia sin reconocimiento facial se podría atentar contra la privacidad de las personas. Reiteró que desde una visión progresista hay que analizar cómo se están gestionando las herramientas tecnológicas, no desde una visión de seguridad del estado sino más bien desde la mirada de la seguridad de los ciudadanos.

- Por su parte, Alfredo Velazco, Cofundador de Derechos Digitales pidió que exista claridad de cuándo y cómo se utilizan las imágenes captadas por medio de la videovigilancia para ser parte de procesos legales.

BIBLIOGRAFÍA

- Constitución del Ecuador.
- Ley Orgánica de Acceso a la Información Pública (LOTAIP).
- Ley Orgánica de Protección de Datos Personales.
- Código Orgánico de Organización Territorial (COOTAD).
- Ley Orgánica del Sistema Nacional de Contratación Pública.
- Ley Orgánica del Sistema Nacional de Registro de Datos Públicos.
- Código Orgánico Integral Penal.
- Decreto Ejecutivo 998.
- Resolución Ministerial MICS-2013-046.
- Procesos de contratación pública: SIE-EMS-001-2020, SIE-EMS-003-20219 SIE-GADM-CL-057-2020, CIE-CSC-005-2020, SIE-CSC-004-2019, CSCG-SIE-007-2019.
- Informe anual del Alto Comisionado de las Naciones Unidas para los Derechos Humanos e informes de la Oficina del Alto Comisionado y del Secretario General. 3 de agosto de 2018 Resolución A/HRC/39/29.
- Informe anual del Alto Comisionado de las Naciones Unidas para los Derechos Humanos e informes de la Oficina del Alto Comisionado y del Secretario General, 24 de junio de 2020, A/HRC/44/24.
- Joy Buolamwini y Timnit Gebru, “Gender shades: intersectional accuracy disparities in commercial gender classification”, Proceedings of Machine Learning Research, vol. 81 (2018), págs. 1 a 15; e Inioluwa Deborah Raji y Joy Buolamwini, “Actionable auditing: investigating the impact of publicly naming biased performance results of commercial AI products”, Conferencia sobre Inteligencia Artificial, Ética y Sociedad (2019).
- Informe del Relator Especial sobre los derechos a la libertad de reunión pacífica y de asociación, 17 de mayo de 2019, A/HRC/41/41.
- Estudio de la Agencia de los Derechos Fundamentales de la Unión Europea, pág. 34.
- Amnistía Internacional https://bit.ly/3CwsZT2
- Diario El Comercio https://bit.ly/3Cvspoy
- Naciones Unidas https://bit.ly/3bptMcM
- Diario Expreso https://bit.ly/3EuH9op
- Portal Periodismo de Investigación https://bit.ly/3bn4Kuy
- RELE-CIDH, Derecho a la Información y Seguridad Nacional https://bit.ly/3oIQrXt

Pedidos de acceso a la información:

- Fiscalía General del Estado
- Defensoría del Pueblo
- Consejo de la Judicatura
- Policía Nacional
- Secretaría de Seguridad y Gobernabilidad del Municipio de Quito
- Cuerpo de Agentes Metropolitanos del Distrito de Quito
- Municipio de Latacunga
- Corporación para la Seguridad Ciudadana de Guayaquil
- Consejo para la Seguridad Ciudadana de Cuenca
- Ministerio de Gobierno
- ECU 911
- Registro Civil

Entrevistas:

- Froilán Salinas, director del Consejo de Seguridad de Cuenca
- Luigi Calderón, especialista 1 de Seguridad Ciudadana del GAD de Latacunga
- Daniela Valarezo, secretaria de Seguridad y Gobernanza del Municipio de Quito
- Juan Zapata, director del ECU 911
- Juan Pablo Torres, subdirector de tecnología del ECU 911
- Bolívar Tello, director de Operaciones del ECU 911
- Renata Moreno, directora de Asesoría Jurídica del ECU 911
- Genny Vélez, coordinadora General de Transparencia y Acceso a la Información Pública de la Defensoría del Pueblo
- Mario Pazmiño, ex director de Inteligencia Militar de Ecuador
- Arturo Torres, periodista e investigador
- Juan Pablo Solines, abogado y experto en derechos digitales
- Alfredo Velasco, director de Usuarios Digitales
- De Gaulle Hanze Morla, gerente de operaciones y monitoreo de la empresa Totem

FUNDAMEDIOS