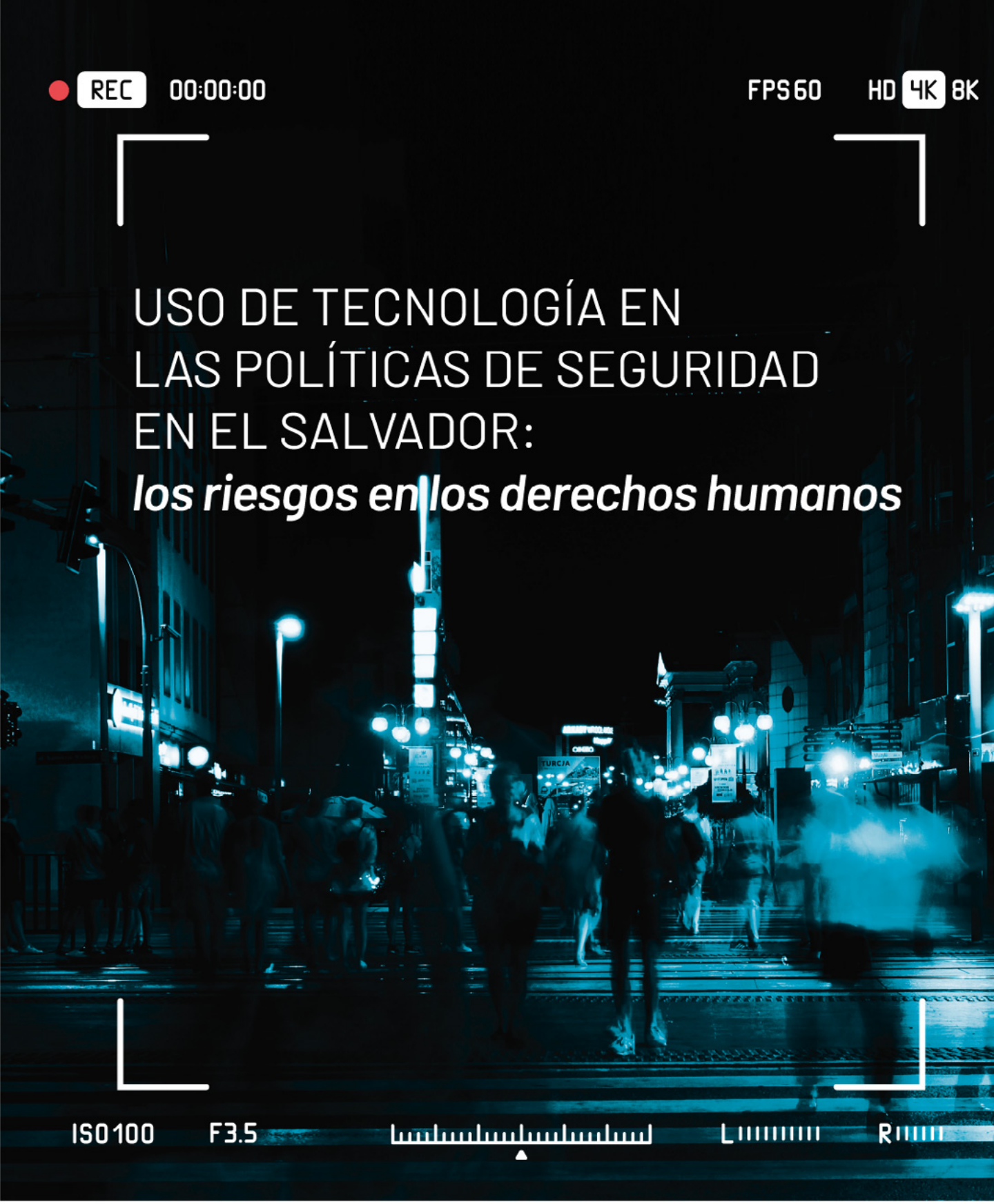

USO DE TECNOLOGÍA EN LAS POLÍTICAS DE SEGURIDAD EN EL SALVADOR:

los riesgos en los derechos humanos

sspas Servicio Social Pasionista

REC 00:00:00 FPS 60 HD 4K 8K

USO DE TECNOLOGÍA EN LAS POLÍTICAS DE SEGURIDAD EN EL SALVADOR:

los riesgos en los derechos humanos

sspas Servicio Social Pasionista

ISO 100 F3.5 L R

Uso de tecnología en las políticas de seguridad en El Salvador:
los riesgos en los derechos humanos

Servicio Social Pasionista – SSPAS

Dirección General - SSPAS
Carlos San Martín

Programa de Derechos Humanos - SSPAS

Equipo de redacción
Verónica Reyna, directora del Programa de Derechos Humanos
Maya Olivares, Técnica de Investigación
Karoline Alvarado, Técnica de Investigación

Diseño y diagramación:
Mariacela Arbizú

San Salvador, septiembre 2021.

Primera edición, 300 ejemplares.

Con el apoyo de Open Society Foundations.

Contenido

Pág.

Introducción

América Latina es una región que históricamente ha sido caracterizada por distintas problemáticas de índole social, económica y política como la desigualdad, la corrupción y la violencia, teniendo como consecuencia, entre otras cosas, el aumento de los índices de criminalidad en diversos ámbitos, espacios y hacia distintas poblaciones. El paso de los años ha demostrado que estas problemáticas no han cesado, sin embargo, lo que sí se ha demostrado es que los actores que ejecutan actos ilícitos han sofisticado las técnicas que les permiten la comisión de delitos.

Los gobiernos han recurrido a la reorganización de las estrategias de prevención y persecución del delito plasmadas en sus planes de seguridad, ahora, con la implementación del uso de dispositivos tecnológicos especializados para acompañar las acciones que las instituciones, agentes y profesionales de la seguridad pública necesitan en un escenario como el actual donde la tecnología acompaña todos los procesos sociales.

Las instituciones encargadas se ven obligadas a incorporar técnicas y tecnologías innovadoras acordes con las nuevas tendencias y contextos exigiendo una restructuración de los mecanismos de acción por parte de los gobiernos de turno hacia las corporaciones policiales, juzgados, centros penitenciarios, entre otros, e impulsar reformas a las leyes vinculadas a este aspecto o bien la creación de marcos legales especializados, reasignaciones presupuestarias, tecnificación de profesionales y la ratificación de convenios internacionales.

Estos elementos por incorporar representan una de las principales debilidades en el proceso actual de implementación de las tecnologías en el ámbito de la seguridad puesto que los Estados no siempre cuentan, por un lado, con la infraestructura necesaria para poder determinar lineamientos a seguir en este aspecto por lo que hacen uso de empresas privadas que cuentan con la capacidad de administrar estos recursos y, por otro lado, tampoco cuentan con un marco legal que regule el control de estos dispositivos y las repercusiones en los derechos humanos de las personas que buscan proteger. Esto supone, sin duda, un riesgo en cuanto a la utilización de los datos y la información recopilada durante estos procesos de vigilancia y monitoreo, pudiendo afectar a las mismas personas en diversos aspectos, representando así una potencial vulneración a derechos humanos, en particular en lo relativo a los derechos a la intimidad, privacidad e integridad personal, entre otros.

La tendencia regional del uso de tecnologías para el acompañamiento de estrategias de seguridad se observa de manera cada vez más fuerte en El Salvador, es por ello que este estudio pretende realizar un primer acercamiento a la temática, con el fin de identificar usos y efectos de estos, principalmente, en los derechos de las personas y en el uso responsable y transparente de estas herramientas para la protección de la población, cuidando el resguardo de sus datos personales y haciendo uso adecuado de la información recopilada con fines meramente de seguridad ciudadana.

De acuerdo con la Comisión Interamericana de Derechos Humanos (en adelante CIDH), el concepto Seguridad Ciudadana es el más adecuado para el abordaje de los problemas de criminalidad y violencia desde una perspectiva de derechos humanos, en lugar de los conceptos como Seguridad Pública, Seguridad Interior u Orden Público. La seguridad ciudadana deriva de la construcción de mayores niveles de ciudadanía democrática con la persona humana como objetivo central de las políticas, a diferencia de la seguridad del Estado o el de determinado orden político[1]. Por lo tanto, la construcción de políticas públicas de seguridad ciudadana requiere de trabajo conjunto entre instituciones del Estado, representantes de la sociedad civil y la ciudadanía en general donde la articulación es entendida de manera reciproca entre las autoridades en todos sus niveles.

La implementación de la tecnología tiene implicaciones en su uso y requiere de conocimientos específicos teniendo en cuenta la necesidad de identificar las posibles afectaciones en el ejercicio de los derechos humanos. Además, requiere de la voluntad política para abrir las puertas a centros de investigación, universidades, proveedores de softwares, etc., que permitan mantener un trabajo conjunto e interdisciplinario entre distintos actores sociales y estatales.

Es fundamental mantener un equilibrio en el uso de estos recursos tecnológicos para la prevención y el control del delito, tomando en cuenta que una sociedad altamente tecnologizada es una forma de control estatal[2], lo que permite en muchas ocasiones que la violencia social se perpetúe de manera legítima por agentes del estado (policía y ejército) teniendo repercusiones directas en la sociedad y provocando daños a la protección a los derechos individuales y vulneración a la privacidad. Por lo tanto, el uso de estas herramientas debe estar regulada y respaldada por procedimientos transparentes que permitan establecer que la recolección de la información

1 CIDH, "Informe sobre seguridad ciudadana y derechos humanos", 2009, 8.
2 Jon Murelaga Ibarra, "Breve reflexión de la sociedad tecnologizada actual Tecnología digital, individuo, globalización e Internet", Revista Latina de Comunicación Social, N° 59, 2005, 6.

está dentro de los márgenes de la ley y acompañadas de evaluaciones que permitan monitorear su funcionamiento y determinar si cumplen con el objetivo para el cual fueron implementadas.

Existe poca evidencia en América Latina acerca de los resultados obtenidos en relación con los usos de distintos tipos de tecnologías en el ámbito de la seguridad, principalmente el uso de drones[3], sistemas de videovigilancia[4] y datos biométricos[5], no obstante, esta investigación tiene como finalidad explorar las experiencias que han podido registrarse en la región y las particularidades de cada caso para realizar un primer acercamiento al tema e incluir, además, una revisión de los esfuerzos realizados en El Salvador.

En el primer capítulo se presenta el escenario actual de los países como México, Argentina, Brasil, Costa Rica, entre otros, en el uso de drones, sistemas de videovigilancia y datos biométricos y los resultados de su implementación. El segundo capítulo explora el caso salvadoreño y las formas de uso de estas tecnologías dentro de las estrategias de los gobiernos municipales y el gobierno central. En el tercer capítulo se hace un recorrido sobre las implicaciones de la tecnología en el ejercicio de derechos humanos, identificando las valoraciones sobre los marcos normativos que regulan estas acciones, además de los riesgos y potenciales vulneraciones que pueden concretarse ante la ausencia de una normativa que determine quiénes administran la información, cómo y para qué se usa. Finalmente, se presenta un espacio de conclusiones y recomendaciones relativas al abordaje de esta temática desde un enfoque de derechos humanos.

3 Pequeño vehículo aéreo no tripulado utilizado en el ámbito militar (para reconocimiento táctico desde gran altura, vigilancia del campo de batalla o guerra electrónica) y civil (vigilancia de manifestaciones, control de la contaminación y de incendios forestales, etc.) "Drone" es un término en inglés que se traduce en 'zángano', que hace referencia al insecto que vuela.
4 Utilización de imágenes de video, ya sea en tiempo real o en visualización de grabaciones, para funciones de vigilancia de incidentes de seguridad.
5 Son aquellos datos personales referidos a las características físicas, fisiológicas o conductuales de una persona que posibiliten o aseguren su identificación única.

Capítulo 1

Una mirada hacia Latinoamérica

En este breve acercamiento se conocerán las experiencias de los países del continente en la implementación de distintas iniciativas especializadas en el uso de tecnologías en las ciudades y comunidades de las principales urbes de la región y el tipo de uso que se le da a cada tipo de dispositivo en este ámbito.

Drones

Un drone es un "Vehículo Aéreo No Tripulado" (VANT), que también puede definirse como el conjunto de elementos configurables consistentes en un artefacto aéreo piloteado remotamente, que está asociado a una estación de pilotaje que requiere enlaces de comando y control y cualquier otro sistema que sea requerido durante operaciones de vuelo[6]. Este dispositivo tiene diversos usos, sin embargo, dentro del uso cívico se encuentra el realizado por los gobiernos, ya que la adquisición de drones para el patrullaje en territorios donde no se puede acceder, la inspección de terrenos, vigilancia de fronteras, control aéreo en eventos masivos, como protestas, ferias, estadios, conciertos, entre otros, han sido parte de las iniciativas gubernamentales donde se ha hecho uso de estas herramientas.

De acuerdo con la Fundación Datos Protegidos (2018), la categorización de drones civiles y militares se ve difuminado por el uso que los gobiernos le dan[7], que viene determinado también por las características de los equipos utilizados y sus capacidades de uso en dichos ámbitos. Este tipo de drones se convierten en dispositivos de gran valor para las industrias de seguridad pública ya que les permite el control de grandes espacios, la posibilidad de poder generar perfiles de personas, identificar y monitorear situaciones u objetos, generando un impacto directo en la recolección de datos personales de manera masiva y en poco tiempo. Algunas de las posibilidades de estos equipo son: a) videovigilancia, permitiendo almacenar en vivo imágenes, reconocimiento facial (permitiendo identificar personas, objetos, conductas, leer e identificar vehículos), sistemas de infrarrojos con capacidad de grabar en condiciones de baja visibilidad y de noche; b) sistemas de detección, permitiendo identificar vehículos y objetos, algunos incluso a través de paredes u otros objetos con sistemas infrarrojos u otros; c) equipamiento de radio-fre-

6 Organización de Aviación Civil Internacional. "Términos utilizados frecuentemente", Consultado el 10 de septiembre de 2021. https://www.icao.int/safety/UA/UASToolkit/Pages/FAQ_es.aspx
7 Datos protegidos, "Drones en Chile: Un análisis de los discursos, industria y los derechos humanos", 2018, 4.

cuencia, para ser utilizados como antenas para capturar posiciones de Wi-Fi y controlar señales de celular y conexiones inalámbricas[8].

Argentina, Chile, Brasil, entre otros países, hacen considerables inversiones para la utilización de drones en sus políticas y programas de seguridad pública y combate a la delincuencia debido a que la falta de regulación y las crecientes desigualdades de la región permiten expandir los drones como elementos de vigilancia[9].

Chile, específicamente la municipalidad Las Condes, implementó un sistema de videovigilancia con drones en zonas consideradas de alta peligrosidad. Esta estrategia fue presentada al público generando grandes expectativas y aceptación por parte de la población. Los drones utilizados fueron DJI, modelo 600 Pro, con una cámara y zoom con la capacidad de reconocer objetos pequeños (como un lápiz rojo) a 150 metros de distancia. La compañía Dronestore, proveedor de la municipalidad de Las Condes, facturó $63,000 en los últimos 5 años sólo en contratos públicos. De acuerdo a su CEO, Jorge Zalaquett, en un año (2014 a 2015) aumentaron sus ventas en un 300% y en el período de 2015-2016 sus ventas se incrementaron en un 75%[10]. Esta compañía fue la primera en vender drones DJI[11] en Chile y, en la actualidad, son seis compañías las distribuidoras oficiales de esta marca en dicho país.

Otro de los países que hace uso de drones para la persecución del delito es Argentina, específicamente en Buenos Aires. Desde 2017 cuenta con un sistema de globos aerostáticos de vigilancia que complementan la iniciativa "Anillo Digital" que consiste en un cinturón en las entradas y salidas de la ciudad y por las autopistas que conectan con el resto del país[12]. Los globos cuentan con cámaras con visión diurna y nocturna que trasmiten en tiempo real y permiten la identificación y el monitoreo en un radio amplio.

En Brasil el uso de drones inició para la Copa Mundial de Futbol de 2014 y los Juegos Olímpicos en Río de Janeiro en 2016, donde se adquirieron para mantener la seguridad de los eventos. Los montos invertidos por la defensa brasileña rondan los $350 millones[13]. Brasil es el país con la mayor cantidad de empresas de fabricación de drones en América Latina y sus usos por parte del Estado no se limitan: hacen monitoreos de fronteras, combate al narcotráfico y grupos delictivos en favelas, zonas rurales, etc. [14]

8 Ibidem, 20.
9 Sebastián Becker Castellaro, *"Drones en Latinoamérica: industria, discursos y violaciones a los derechos humanos"*, 5o Simposio Internacional LAVITS, Vigilancia, Democracia y Privacidad en América Latina: Vulnerabilidades y resistencias, Santiago, Chile, 2017, 185.
10 Ibidem, 187.
11 SZ DJI Technology Co., o DJI Sciences and Technologies Ltd. , es una empresa de tecnología china fabricante líder mundial de vehículos aéreos no tripulados para fotografía aérea y videografía.
12 Gobierno de Buenos Aires, "Anillo Digital", Consultado el 5 de septiembre de 2021. https://www.buenosaires.gob.ar/baobras/anillo-digital-0
13 Datos protegidos, "Drones en Chile: Un análisis de los discursos, industria y los derechos humanos", 2018, 12.
14 Jeffer Chaparro Mendivelso et. al. "El dron como herramienta tecnológica de control territorial", Revista electrónica de recursos en internet sobre geografía y ciencias sociales, 2018, 7.

A pesar de los avances existentes en la implementación de estas tecnologías existen posturas que expresan que los drones son un riesgo serio a la privacidad de terceros y, por tanto, exhortan a que no se recolecten datos sin previa autorización. Estas nuevas dinámicas han provocado que derechos como el derecho a la protección de datos y la privacidad, entre otros, se vuelven cada vez más importantes de discutir para protegerse ante la actuación del Estado.

> *«Los drones podrían estar regulados hasta en una ley de aviación civil [...] la complejidad es que no está integrado en los procesos de denuncia legal para este tipo de tecnologías»*
>
> Entrevista a Tanya Loockwood, directora ejecutiva de la Fundación Acceso. Abril de 2021

Sistemas de videovigilancia

Se referirá específicamente a los sistemas de videovigilancia como aquel conjunto de elementos que captan masivamente información identificatoria de las personas (es decir, datos personales)[15]. A lo largo del tiempo se ha tratado de convencer a la población de que la instalación de videocámaras de vigilancia y uso de satélites para geolocalización y software especializados, como los de reconocimiento facial, intervienen y fortalecen la seguridad tanto ciudadana como la nacional[16].

La videovigilancia se ha transformado en un elemento destacado para la industria de la seguridad. La innovación tecnológica avanza a pasos agigantados y cada vez son más las personas que demandan el uso de tecnología ocasionando que los mercados se expandan de manera insospechada. A esto se le suma que los gobiernos plantean la necesidad de invertir en sistemas integrales de videovigilancia, por lo tanto, la regulación de la videovigilancia y la posible comisión de delitos resulta entonces un gran tema que se debe considerar en el desarrollo tecnológico, ético y por supuesto legal[17].

Chile es uno de los países de la región que cuenta con diversas iniciativas tecnológicas entre ellas el Sistema de Información Geográfica (SIG) que funciona como una base de datos de información geográfica dentro de un mapa digital, asimismo, cuentan con un Sistema de Consulta de Imputado Conocido (SCIC) es un sistema que la policía chile-

15 Véase: "Videovigilancia en el espacio público: un obstáculo para las libertades civiles", Red en Defensa de los Derechos Digitales, 29 de enero de 2020.
16 Joaquín Rueda Carrillo, "Videovigilancia ¿derecho del ciudadano o facultad del estado? el caso de la ciudad de México", INFOTEC Centro de investigación e innovación en tecnologías de la información y comunicación, 2019, 26.
17 Joaquín Rueda Carrillo, "Videovigilancia ¿derecho del ciudadano o facultad del estado? el caso de la ciudad de México", INFOTEC Centro de investigación e innovación en tecnologías de la información y comunicación, 2019, 30.

na tenía sólo a disposición para investigar. Desde el 2017, el SCIC está disponible en comisarías facilitando la labor de los funcionarios operativos. A través de este sistema se dispone de la siguiente información de los imputados conocidos: redes, mapas y delitos más comunes[18], lo que permite un análisis de datos a partir de la recolección de diversa información a través de sistemas de monitoreo digitales.

Argentina cuenta con un programa de protección ciudadana donde existe una Red Sistematizada de Videovigilancia en los territorios de San Miguel de Tucumán y Yerba Buena, que tiene como objetivo detectar situaciones de peligro. Esta información llega a centros de control y monitoreo especializados. También se ha implementado el Sistema de Atención de Emergencias 911 Provincial que contempla la instalación de centrales telefónicas equipadas con monitores que permiten cartografiar el área denunciada mediante la llamada telefónica recibida y con un sistema de localización de vehículos (patrullas, camiones de bomberos y ambulancias) con el objetivo de disminuir los tiempos de respuesta frente a las denuncias de quienes llaman[19]. Otro es el proyecto Buenos Aires Ciudad Segura (BACS), a través del Ministerio de Seguridad de la Nación y del Ministerio de Ciencia, Tecnología e Innovación Productiva, con un Centro de Comando y Control que articula las instituciones del Estado. Este proyecto incorpora una red de fibra óptica de 500 kilómetros que interconecta 1,200 cámaras fijas de videovigilancia, 336 cámaras fijas de reconocimiento de patentes en los accesos a la ciudad y antenas de la red WiMax, en los edificios del Ministerio de Interior, de Seguridad, de Gendarmería, Prefectura, Policía Federal y las 53 comisarías[20].

Según algunos autores, "la videovigilancia también ayuda a inhibir la comisión delictiva por lo menos en donde se encuentran colocadas por lo que inciden en la prevención del delito y también contribuyen en la persecución e investigación del delito ya que los videos e imágenes pueden ser aportadas como pruebas en los juicios penales. También contribuyen en la reacción inmediata"[21], sin embargo, la información recogida no siempre se encuentra regulada y protegida, sumada a la poca información y transparencia con la que se cuenta para conocer a cabalidad la información recogida y su uso por parte de las autoridades.

En Ecuador, a partir del 2013, se desarrolla el Sistema Integrado de Seguridad (SIS) ECU-911, que tiene como objetivo la coordinación inmediata de diversas instituciones estatales como la Policía Nacional, las Fuerzas Armadas, los Cuerpos de Bomberos, Ministerio

18 Lucía Dammert y Anamaría Silva, *"Seguridad y Tecnología en América Latina: EXPERIENCIAS Y DESAFÍOS"*, Universidad de Santiago de Chile, 2015, 29.
19 Ibidem, 20.
20 Lucía Dammert y Anamaría Silva, "Seguridad y Tecnología en América Latina: EXPERIENCIAS Y DESAFÍOS", Universidad de Santiago de Chile, 2015, 122.
21 Joaquín Rueda Carrillo, *"Videovigilancia ¿derecho del ciudadano o facultad del estado? el caso de la ciudad de México"*, INFOTEC Centro de investigación e innovación en tecnologías de la información y comunicación, 2019, 35.

de Salud, etc. Este sistema articula los servicios de videovigilancia, botones de pánico, alarmas comunitarias, atención de emergencias, entre otros. Actualmente, se mantiene en uso este sistema que cuenta con Centros de Funcionamiento C4 que incluye mecanismos de alerta como las cámaras de videovigilancia, las llamadas de emergencia y la coordinación interna y externa: 2,450 cámaras de video vigilancia a nivel nacional, botones de auxilio, que son alarmas fijas y móviles ubicadas en edificios y espacios públicos[22]. Aquí se incluyen 55,000 kits de cámaras instalados en taxis y buses como parte del proyecto Transporte Seguro de la Agencia Nacional de Tránsito; y el aplicativo inclusivo "Smartphone", de descarga gratuita para teléfonos inteligentes[23].

Uruguay también cuenta con diversas inversiones en tecnología, una de ellas impulsó la instalación de más de 108 cámaras de videovigilancia en 44 puntos de amplia afluencia turística y plazas de Montevideo, así como 15 cámaras en Maldonado Punta del Este y otras 214 en centros penitenciarios, 14 cámaras en Colonia y otras en Salto y Rivera[24].

> *«Creo que hay casos de violencia sexual donde [los sistemas de videovigilancia] han sido exitosos. Es decir, la violencia de género contra las mujeres, particularmente en espacios públicos, en la calle, evidentemente este tipo de tecnología han podido identificar en el momento al sujeto, su recurrencia. Se tiene este tipo de posibilidad de evidencia y en muchos casos también pueden agilizar una denuncia»*
>
> Entrevista a Tanya Loockwood, directora ejecutiva de la Fundación Acceso. Abril de 2021

En Brasil se implementó el proyecto Radar de la Policía Militar del Estado de São Paulo, desde 2014, que a través de cámaras tenía como objetivo disminuir los niveles de hurto y robo de vehículos donde las placas de los carros registradas son monitoreadas y los radares envían los datos de los vehículos al centro de procesamiento de datos y se comparan con los bancos de datos oficiales[25].

Actualmente, la Ciudad de México cuenta con un Centro de Monitoreo y Supervisión Virtual, un Sistema Informático de videograbación en patrullas, Áreas de Policías de Ciberdelincuencia Preventiva y Ciber alertas. De acuerdo con Lucia López (2019) la instalación de los dispositivos en la Ciudad se ha realizado por demanda ciudadana que frente al miedo de ser víctimas de algún delito solicitan a las instituciones de gobierno cámaras

22 Lucía Dammert y Anamaría Silva, *"Seguridad y Tecnología en América Latina: EXPERIENCIAS Y DESAFÍOS"*, Universidad de Santiago de Chile, 2015, 35.
23 Ibidem, 91.
24 Gobierno de Uruguay, *"Montevideo y Canelones contarán con 5.000 cámaras de videovigilancia en 2018, que reforzarán la seguridad ciudadana"*, Consultado el 11 de septiembre de 2021, https://www.gub.uy/presidencia/comunicacion/noticias/montevideo-canelones-contaran-5000-camaras-videovigilancia-2018-reforzaran
25 Lucía Dammert y Anamaría Silva, *"Seguridad y Tecnología en América Latina: EXPERIENCIAS Y DESAFÍOS"*, Universidad de Santiago de Chile, 2015, 29.

de videovigilancia y alarmas[26]. Además, México hace uso de los C4 que son los Centros de Comando, Control, Comunicación y Cómputo, que son espacios físicos donde se unifica la información y se articulan acciones en materia de seguridad, control y administración, a través de infraestructura tecnológica. En la Ciudad de México funcionan botones de auxilio, que se definen como un interlocutor de contacto directo con los C4 y que se ubican en el poste de diversas cámaras de videovigilancia de la Ciudad de México los cuales deben ser presionados por gente que requiera el apoyo inmediato de algún servicio de emergencia[27].

Sin embargo, según Coding Rights, las ciudades con mayores cámaras en el mundo no son necesariamente las más seguras[28]. Estos dispositivos de vigilancia han generado controversia en dos puntos: su eficacia, donde no existen evaluaciones fidedignas, y segundo, si los dispositivos contribuyen a profundizar los conflictos locales y la desconfianza mutua, ya que estos pudieran generar sensación de seguridad en algunos grupos poblacionales, pero mayor sentimiento de inseguridad y hostigamiento en otros. Un dispositivo de vigilancia es un rótulo de marca indeleble en el plano de la vida social, sobre todo en parte de los estratos socioeconómicos más desfavorecidos[29]. La implementación de sistemas de vigilancia no solo podría afectar las expectativas de privacidad en espacios privados, sino también en los espacios públicos. El Tribunal Europeo de Derechos Humanos ha señalado al respecto:

> *"quien se siente inseguro de sí en todo momento que se registran sus comportamientos divergentes y se catalogan, utilizan (...) procurará no llamar la atención con esa clase de comportamientos. Quien sepa de antemano que su participación, por ejemplo, en una manifestación cívica va a ser registrada por las autoridades y que podrán derivarse riesgos para él por este motivo, renunciará presumiblemente a lo que se supone un ejercicio de los correspondientes derechos fundamentales"*[30]

Dos estudios de metaanálisis de 17 programas de videovigilancia en Gran Bretaña y Estados Unidos, y de 13 programas de videovigilancia en Gran Bretaña[31], señalan como conclusión general que la videovigilancia tiene un escaso éxito en la reducción de la delincuencia, uno de ellos indica una reducción en torno al 4%, y el otro menciona que los efectos negativos y positivos de la implantación de videocámaras se contrarrestan. Sin embargo, estos dos estudios también señalan poca efectividad para delitos violentos e impulsivos, en comparación con delitos no violentos y premeditados; que serían más

26 Lucía Carmina Jasso López, *"Prevención del delito y tecnología: La instalación de cámaras de videovigilancia y alarmas como medida de protección de los hogares en México"*, Instituto de Investigaciones Sociales de la Universidad Nacional Autónoma de México, 2019, 166.
27 Ibidem.
28 Datos protegidos, *"Drones en Chile: Un análisis de los discursos, industria y los derechos humanos"*, 2018, 25.
29 Ibidem, 26
30 Ibidem, 27
31 José Luis Díez Ripollés y Ana Isabel cerezo Domínguez, *"La prevención de la delincuencia callejera mediante videocámaras. Regulación jurídica y eficacia"*, Universidad de Málaga, España, 2009.

eficaces en lugares cerrados que en centros de ciudades o zonas residenciales; que son más eficaces en lugares de acceso limitado y controlado; que su eficacia podría estar proporcionalmente relacionada con la cobertura y número de cámaras instaladas; que el impacto de estos sistemas podría depender de cada país; que la eficacia puede depender de factores de organización de la sala de mando, la relación entre sus operadores y la policía, o el carácter fijo o móvil de las cámaras; y, que la vigilancia puede ocasionar un desplazamiento del delito hacia zonas sin videocámaras.

Datos biométricos

El uso de datos biométricos o lectores biométricos es otra de las innovaciones tecnológicas que se están utilizando en América Latina para la seguridad ciudadana. Estos se pueden definir como sistemas informáticos de reconocimiento con base en uno o varios patrones biológicos de un individuo; extraen un patrón de estos datos adquiridos y comparan el ejemplo contra una plantilla previamente registrada y puede estar almacenada en una base de datos centralizada[32]. Esta tecnología se basa en la detección y el reconocimiento de una o más características físicas de un individuo o grupo: huellas digitales, lectura facial, lectura de iris, etc.

De acuerdo con Jaramillo (2021) es especialmente significativo el reconocimiento facial al ofrecer la posibilidad de detectar a una persona, incluso entre una gran multitud, a través de los parámetros del rostro[33]. Esto se nutre de relevancia ya que se ha incorporado a los sistemas de videovigilancia por parte de las instituciones de seguridad en algunos países. Este es un método técnico de identificación de personas a través de una fotografía o imagen captada por una videocámara que lleva incorporado dicho sistema. Para que la persona sea detectada, previamente debe haberse inscrito la imagen de su rostro en una base de datos informática. Dicha imagen es la que posteriormente se comparará con los datos del rostro de la persona detectados por el instrumento cuando esta desee acceder a un lugar o sea localizado de forma encubierta en un espacio, ya sea público o privado[34].

Los lectores de datos biométricos son múltiples y varían de acuerdo a las funciones que tengan. Lucero et al. (2020) plantean que en la mayoría de los países la identificación de los individuos es a través de objetos como el documento de identidad y tarjetas de identificación; por medio de conocimientos, como preguntas secretas, claves personales; patrones conductuales, firma, forma de teclear; atributos físicos, huellas dactilares, iris, retina, etc., y algunos otros atributos como la voz y el ADN[35].

32 Milton Lechner, *"Tecnologías aplicadas a la seguridad ciudadana: desafíos para la justicia transicional ante nuevos mecanismos de control social"*, Repositorio Institucional Digital de Acceso Abierto de la Universidad Nacional de Quilmes, 2016, 8.
33 Cristina Domingo Jaramillo, *"Utilización del sistema de reconocimiento facial para preservar la seguridad ciudadana"*, El Criminalista Digital, 2021, 1.
34 Ibidem, 21.
35 Boris A. Lucero et. al. *"Aspectos éticos del uso de identificadores biométricos"*, Centro de Investigación en

En Chile, en 2011 se implementó, a través del Ministerio del Interior y Seguridad Pública y Carabineros de Chile, el STAD[36] que hace uso del Sistema de Análisis de Información Territorial (SAIT) en el mapeo los delitos, y el Sistema Integrado de Control de Gestión que triangula la encuesta de victimización y la revisión de patrones delictuales.

México también cuenta con un programa denominado Plataforma México, creado por el Consejo Nacional de Seguridad Pública, con el objetivo de prevenir y combatir el delito a través de la inversión en tecnología para fortalecer la Red Nacional de Telecomunicaciones y el Sistema Nacional de Información. Esta plataforma permite compartir audios, video, texto y registros biométricos. Además, el Sistema Único de Información Criminal integra bases de datos biométricas, licencias de conducir, vehículos robados y recuperados, registro público vehicular, registro de antecedentes penales, registro de la población penitenciaria, denuncias realizadas por los ciudadanos, registro de las armas y municiones asignadas a las instituciones de seguridad pública. Sin embargo, hay algunas implicaciones en este uso.

> *"Aquí en México estamos en esa discusión porque el presidente propuso una reforma en la que todos tenemos que dar nuestros datos biométricos para adquirir un teléfono celular: iris, huella digital, captura de voz. Y el problema es que la idea es buena en cuanto a términos de protección, sin embargo, el marco jurídico en el cual se amparan los datos personales en el país es muy deficiente"*
>
> Entrevista a Daniel Tagle, Profesor e Investigador de la Universidad de Guanajuato
> Marzo de 2021

Los sistemas de videovigilancia (que incluyen a los drones) y datos biométricos convergen en un único sistema de control y vigilancia, conformando así lo que expertos en el ámbito de la seguridad denominan una gran red o malla panóptica que concentra el poder y dominación de la información al servicio de los Estados[37]. Es así como a través de la tecnología aplicada a la seguridad ciudadana se da lugar a la vigilancia y control de la sociedad en su conjunto.

De acuerdo con las experiencias registradas en la región existe una latente necesidad de que las regulaciones a sus usos logren incluir lineamientos que retomen de manera fundamental los mecanismos de protección de las personas con un enfoque de derechos humanos, no solamente relativos al uso técnico de los dispositivos.

Neuropsicología y Neurociencias Cognitivas, Facultad Ciencias de la Salud, Universidad Católica del Maule, Chile, 2020, 44.

36 Diego Piñol et. al. *"STAD: Análisis de los nudos críticos para la implementación de un sistema de análisis delictual en Chile"*, Centro de Estudios en Seguridad Ciudadana del Instituto de Asuntos Públicos de la Universidad de Chile, 2014.

37 Milton Lechner, "Tecnologías aplicadas a la seguridad ciudadana: desafíos para la justicia transicional ante nuevos mecanismos de control social", Repositorio Institucional Digital de Acceso Abierto de la Universidad Nacional de Quilmes, 2016, 14.

Capítulo 2

La experiencia de El Salvador

Tras la firma de los Acuerdos de Paz y la creación de una nueva institucionalidad que permitiera brindar ciertas garantías y derechos fundamentales a la población salvadoreña, los gobiernos de turno implementaron una serie de políticas públicas de seguridad orientadas a enfrentar las oleadas de violencia y criminalidad en los territorios. Este contexto exigió a los gobernantes a desarrollar estrategias efectivas de persecución del delito tanto a nivel local como a nivel nacional. Los gobiernos municipales a lo largo de los últimos años han recurrido a la instalación de diversos mecanismos de control y disuasión del delito en sus localidades, apostando principalmente por la incorporación de sistemas de videovigilancia en los centros de las ciudades para dar respuesta a la inseguridad en los territorios, no obstante, las acciones predominantes de las políticas de seguridad implementadas a nivel nacional y dirigidas por parte del Órgano Ejecutivo han estado marcadas por el enfoque manodurista, negándose a desarrollar de manera consistente y profunda una política que responda a la complejidad del fenómeno de la violencia de manera diferenciada y a largo plazo.

Con la llegada de Nayib Bukele a la presidencia se instaló un discurso oficial caracterizado por convencer a la población que se llevaría a cabo «una nueva forma de hacer política» y, con ello, el reto de mejorar aquellos aspectos que las administraciones anteriores no pudieron resolver en relación con las necesidades de la población ante la creciente demanda por un país más seguro. Bajo esta premisa, Bukele planteó modernizar al Estado, sobre todo haciendo énfasis en el uso de la tecnología en diversos ámbitos, principalmente en el de la seguridad, para finalmente prevenir la violencia y la comisión de delitos.

En este capítulo se abordarán las decisiones más representativas y las acciones que se han implementado en el marco de la actual política de seguridad del gobierno de El Salvador relacionadas al uso de dispositivos tecnológicos y, a su vez, la experiencia que han tenido algunos municipios en este ámbito.

Alcaldías municipales: la primera apuesta por incorporar tecnología para garantizar la seguridad

La llegada de nuevas tecnologías para incorporarse a las tareas de seguridad es relativamente reciente en El Salvador. Desde entonces, los gobiernos locales han liderado la iniciativa para poder implementar el uso, principalmente, de sistemas de videovigilancia en los centros de las ciudades ante las oleadas de violencia y criminalidad.

En Santa Ana, durante la administración del exalcalde Alfredo Peñate (entre 2009 y 2012) hubo un proyecto de este tipo el cual solo funcionó dos años. En el Centro Histórico de la ciudad aún hay instaladas dos cámaras, las cuales no funcionan desde finales del 2015; y el centro de monitoreo, con el equipo dañado, está cerrado desde esa época[38].

En 2013, el municipio de La Libertad instaló 16 cámaras de videovigilancia invirtiendo un monto de $35 mil dólares[39]. El centro de monitoreo fue ubicado en la sede de la Policía Nacional Civil para facilitar que las patrullas llegasen de inmediato en caso de que se cometieran hechos delictivos.

La Alcaldía de Santa Tecla también ha implementado los servicios de videovigilancia. En 2016 se instalaron 300 cámaras de alta resolución y detección inteligente. La municipalidad, en coordinación con la Policía Nacional Civil y la Fiscalía General de la República, mantuvo especial vigilancia en aquellas zonas donde las tasas delincuenciales eran más críticas. Como resultado, según el exalcalde Roberto d'Aubuisson, desde su implementación en febrero de 2016, homicidios, robos, hurtos y delitos de todo tipo descendieron en más del 80%[40]. El proyecto tuvo una inversión de $6 millones de dólares.

En el año 2018 la Policía Nacional Civil, de la mano con la Agencia Coreana de Cooperación Internacional (KOIKA), anunció la incorporación al Sistema de Video Vigilancia en cinco municipios del área metropolitana de San Salvador: Apopa, Cuscatancingo, Mejicanos, Ayutuxtepeque y Soyapango, en el marco del Plan El Salvador Seguro, política de seguridad de la administración del presidente Salvador Sánchez Cerén. Un total de 208 cámaras fueron instaladas en los municipios las cuales se interconectarían a más de 700 que ya funcionaban en diferentes puntos de área metropolitana[41]. Según las autoridades, los dispositivos contaban con un software que permitía la lectura de placas y cruce automático contra listado de vehículos con reporte de robo, además del análisis forense de videos: colores, tamaños, conteo de personas, automóviles, seguimiento de patrones entre otros. El monto para este proyecto de video vigilancia fue de $3,728,188.80 dólares, que incluyó, además, la instalación de fibra óptica para un mejor desempeño[42]. Los cinco municipios en los que instalaron estos dispositivos formaron parte de los territorios priorizados en el Plan El Salvador Seguro. Un ejemplo de los resultados de este proyecto estuvo relacionado con la ayuda a las autoridades a sustentar casos como el de Mario Huezo, acusado por la Fiscalía General de la República del feminicidio de la periodista

38 Jonathan Henríquez, *"Santa Ana busca tener un sistema de videovigilancia"*, El Diario de Hoy, 3 de junio de 2018.
39 Lucinda Quintanilla et. al., *"Videovigilancia reduce delitos en los municipios"*, El Diario de Hoy, 22 de enero de 2013.
40 Pablo Balcáceres, "Región gesta sus primeras 'smart cities'", El Economista, 11 de septiembre de 2017.
41 ACAN-EFE, *"Estos cinco municipios conflictivos de San Salvador estarán monitoreados con videovigilancia"*, La Prensa Gráfica, 25 de abril de 2018.
42 Miguel Sáenz Varela, *"Sistemas de vídeo vigilancia contribuirá a prevención de delitos en 5 municipios"*, Periódico Verdad Digital, 25 de abril de 2018.

Karla Turcios, en el que el análisis de los videos de siete cámaras de video vigilancia facilitó al ministerio público la acusación contra el agresor[43].

En el mismo año, la alcaldía de Antiguo Cuscatlán ejecutó el proyecto Ciudad Inteligente (Smart City), por un costo de $6.25 millones[44]. El sistema contaba con cámaras inteligentes, cámaras móviles para los uniformes de los agentes municipales, aplicaciones para encontrar parqueos disponibles y lámparas led.

Por su parte, la alcaldía de San Salvador implementó en 2020 el proyecto de «Smart City», por medio de la empresa "Eyetech Solutions", por un monto de $84 millones[45]. El proyecto estuvo compuesto por un Centro Inteligente de Operaciones (CIO), una red de 3,335 cámaras de última generación, 25 botones de pánico y decenas de puntos de acceso a wifi gratuito[46].

Ante las afectaciones de la delincuencia y otros tipos de criminalidad en los territoritos, la implementación de los sistemas de videovigilancia en los municipios ha presentado retos significativos. La misma Policía Nacional Civil afirma que dentro de los gobiernos locales no existe la experticia necesaria para el manejo de estas herramientas tecnológicas y atender situaciones de violencia.

> *«En Santa Tecla hubo un caso en el que mataron a un policía en una funeraria. Él, en su tiempo libre, iba a trabajar a esa funeraria. En ese momento no sabíamos si eran mareros, pero se vio el movimiento de las dos personas. Desde ahí era de alertar al 911, pero no. Lastimosamente quien hizo el monitoreo era gente de la alcaldía y ellos no tiene preparación para eso. Solo tenían guardada la grabación»*
>
> Entrevista a José Ismael Mejía, jefe del Departamento de Seguridad Informática de la Policía Nacional Civil, abril de 2021

Además, expertos afirman que recurrir a la adquisición de estas herramientas tecnológicas van más allá de asegurar la seguridad de la población a nivel local y, en su lugar, responde a intereses particulares.

> *"En la década anterior comienzan a llegar estas tecnologías a América Latina, pero específicamente en El Salvador se ha convertido en una moda, diría yo, porque no tienen una aplicación técnica, criminológica o victimológica, sino que ha sido uno*

43 Para más información ver: *"Cinco municipios se interconectarán con sistema de video vigilancia"*, El Metropolitano Digital, 25 de abril de 2018.
44 Melissa Pacheco, *"Antiguo Cuscatlán busca convertirse en una "Smart City"*, La Prensa Gráfica, 8 de diciembre de 2018.
45 Magaly Torres, *"Santa Tecla y Antiguo Cuscatlán gastaron millones en sistemas de videovigilancias"*, Diario El Salvador, 19 de octubre de 2020.
46 Ibidem.

> *de los recursos utilizados por muchos municipios, por muchos alcaldes y alcaldesas, para generar negocios vinculados a maniobras que pueden tener vinculación con corrupción y que sólo han buscado lucrarse de las municipalidades"*
>
> Entrevista a Ricardo Sosa, experto en seguridad y criminología. Marzo de 2021

El trabajo de las alcaldías en este ámbito se ha caracterizado por realizarse como parte de las obras propias de los municipios, con excepción de aquellos municipios en los que los proyectos han sido ejecutados con el trabajo articulado entre las comunas y la Policía Nacional Civil mediante lineamientos emitidos directamente desde el Órgano Ejecutivo. En ese sentido, el siguiente apartado pretende analizar las decisiones más representativas por parte de las autoridades encargadas de gestionar acciones que responden a la política pública de seguridad vigente actualmente, donde la Fuerza Armada tiene un especial protagonismo.

Gobierno central: un plan de seguridad modernizado, pero con tintes represivos

Actualmente, el Plan Control Territorial (PCT) es oficialmente la política de seguridad del gobierno de Nayib Bukele. El PCT fue anunciado como una iniciativa que se impulsaría con el fin de recuperar el control del Estado en territorios dominados por pandillas. Según declaraciones del presidente y sus funcionarios, el plan está compuesto por siete fases, de las cuales, hasta la fecha se han presentado cuatro.

Tabla 1. Descripción de las fases del Plan Control Territorial

Fase 1: Recuperación de territorios	20 de junio de 2019	Para esta primera fase, el gobierno desplegó a 2,500 agentes de la PNC y 3,000 militares en las calles de los centros urbanos de los municipios con mayores índices de violencia y criminalidad, y solicitó a la Asamblea la autorización para reorientar fondos por más de $30 millones aprobados en julio de 2019.
Fase 2: Oportunidad	2 de julio de 2019	Se enfoca en acciones dirigidas a la prevención de la delincuencia, a cargo de la Dirección de Reconstrucción del Tejido Social, instancia que pretende dirigir su trabajo hacia las condiciones subyacentes que llevan a las juventudes a unirse a las pandillas. Esta fase busca enfocar las acciones del plan en las comunidades y sus poblaciones para que prevengan la incorporación de niñez y juventudes a los grupos criminales. La ejecución de esta segunda fase del PCT incluye un préstamo internacional por $91 millones el cual fue recibido de modo favorable por los integrantes de la Asamblea Legislativa en 2019.

Fase 3: Modernización	6 de noviembre de 2019	Con esta fase el gobierno central busca fortalecer y equipar a la Policía Nacional Civil y la Fuerza Armada de El Salvador en sus tareas de seguridad. Esta fase implicó la negociación de un préstamo por $109 millones con el Banco Centroamericano de Integración Económica (BCIE) para mejorar el equipamiento de las fuerzas de seguridad.
Fase 4: Incursión	19 de julio de 2021	Su finalidad es incrementar la cantidad de militares en la Fuerza Armada de 20,000 a 40,000 elementos en cinco años, y con esta capacidad militar incursionar en los territorios dominados por las pandillas para su recuperación.

Fuente: Elaboración propia.

El PCT se caracteriza por dar énfasis al trabajo conjunto entre miembros de la policía y elementos de la Fuerza Armada para llevar a cabo tareas de seguridad. Es por esta razón que tres de las cuatro fases conocidas hasta la fecha están centradas en dotar de recursos a estas instituciones.

En noviembre de 2019, Nayib Bukele presentó a la Asamblea Legislativa la tercera fase del Plan Control Territorial, que implicaba la negociación de un préstamo por $109 millones con el Banco Centroamericano de Integración Económica (BCIE) para mejorar el equipamiento de las fuerzas de seguridad.

Tabla 2. Distribución de fondos aprobados para la ejecución de la Fase III del PCT

Tipo de rubro	Cantidad (en dólares)	Porcentaje de asignación en relación con el total
Equipo e infraestructura de videovigilancia	$25.9 millones	23.8%
Movilidad estratégica	$46.9 millones	43%
Adquisición de equipo táctico	$17.4 millones	16%
Modernización hospitalaria para personal de seguridad	$15.5 millones	14.2%
Administración, supervisión y auditoría, imprevistos y comisión del BCIE	$3.3 millones	3%

Fuente: Elaboración propia con base en Asamblea Legislativa (@AsambleaSV), "Emiten dictamen para suscribir préstamo por $109 millones para seguridad ciudadana. Leer más en el siguiente enlace: https://asamblea.gob.sv/node/10152", Twitter, 9 de marzo de 2020. https://twitter.com/asambleasv/status/1237165877646315520

Con estos recursos se pretende adquirir cámaras de reconocimiento facial y de placas para identificar mejor a las personas que pudieran cometer delitos y los vehículos en que se movilizan, además, también contemplan la adquisición de vehículos aéreos no tripulados (UAV) con visión nocturna para, entre otras cosas, identificar campamentos de pandilleros y que así permitan planificar mejores acciones de ataque o defensa[47].

A esas alturas, la Asamblea Legislativa sostenía que para aprobar dicho préstamo el presidente debería presentar a detalle cómo se utilizarían los fondos. Sin embargo, como medida de presión para la aprobación de la negociación de este préstamo, el presidente Bukele militarizó la Asamblea junto a cientos de manifestantes, provocando una serie de críticas y llamados de atención de la comunidad internacional ante lo que se consideró como una ruptura del orden constitucional y un intento de autogolpe de Estado. Sin embargo, dos años después, con la llegada de la nueva legislatura en la cual se instaló una mayoría oficialista (56 de 84 diputados), se aprobó el crédito para finalmente financiar la fase 3 del PCT[48].

Por medio de una solicitud de acceso de la información dirigida al Ministerio de Hacienda[49], se conoce el documento denominado "Formulación para la ejecución del Programa de Modernización en Seguridad Ciudadana en el marco del Plan de Control Territorial en su Fase III", elaborado por el BCIE con información proporcionada por el Gobierno, en el que aparece el presupuesto detallado de compras a realizar con el préstamo. Según el documento, el equipamiento para modernizar está vinculado a la videovigilancia, incluyendo cámaras especializadas, drones y sus sistemas tecnológicos respectivos; equipo de movilidad estratégica tales como helicópteros, equipo terrestre y marítimo; equipamiento táctico que mejore la operatividad de los servicios de seguridad ciudadana tales como equipamiento de protección al personal operativo y equipo operativo en general (GPS, radios); y equipo médico que mejore decididamente la atención de elementos operativos y administrativos de la PNC y del Ministerio de Defensa Nacional[50].

El programa de financiamiento contempla la ejecución de un componente relacionado con la Modernización de equipo estratégico y táctico. El costo de la inversión de este componente es $90,193.71 millones de dólares, que representa el 82.75% del costo total[51], distribuido de la siguiente manera.

47 Para más información ver: *"El Salvador aprueba un préstamo de 109 millones de dólares para seguridad y defensa"*, Infodefensa.com, 15 de mayo de 2021.
48 Para más información ver: *"Legisladores autorizan crédito de $109 millones para la fase III del "Plan Control Territorial"*, Asamblea Legislativa, 06 de julio de 2021.
49 Unidad de Acceso a la Información Pública (UAIP), respuesta a solicitud UAIP/RES.038.3/2020, Ministerio de Hacienda, 2020.
50 BCIE, *"Formulación para la ejecución del Programa de Modernización en Seguridad Ciudadana en el marco del Plan de Control Territorial en su Fase II"*, 2019, 11.
51 BCIE, *"Formulación para la ejecución del Programa de Modernización en Seguridad Ciudadana en el marco del Plan de Control Territorial en su Fase II"*, 2019, 14.

Tabla 3. Distribución presupuestaria para la ejecución del componente "Modernización de equipo estratégico y táctico"

Subcomponente	Cantidad asignada (en dólares)
Equipo e infraestructura de video vigilancia	$25,895.68 millones
Movilidad estratégica	$46,895.94 millones
Equipo táctico	$ 17,402.09 millones

Fuente: Elaboración propia con base en BCIE, "Formulación para la ejecución del Programa de Modernización en Seguridad Ciudadana en el marco del Plan de Control Territorial en su Fase II", 2019, 15.

Por la naturaleza de este estudio, para analizar las implicaciones del uso de dispositivos tecnológicos en el ámbito de la seguridad se hará énfasis en el financiamiento dirigido al subcomponente de Equipo e infraestructura de video vigilancia, el cual se detalla de la siguiente manera.

Tabla 4. Descripción de las actividades financiables para el subcomponente "Equipo e infraestructura de video vigilancia"

Cámaras	Ampliación del alcance de videovigilancia con la compra e instalación de 4,075 cámaras en 21 municipios ubicados estratégicamente en las principales ciudades del país con el fin de mejorar la operatividad policial. Las cámaras incluyen cámaras blindadas, lectoras de matrícula y cámaras con la capacidad de video de 360°, inclinaciones y ampliaciones para la reacción inmediata de elementos policiales.
Instalación de fibra óptica	Adquisición de una infraestructura e instalación de red de fibra óptica propia por 750 km lineales.
Mejoramiento equipamiento tecnológico y mobiliario	Instalación de sistema de almacenamiento masivo, servidores, computadores de escritorio, software para la grabación de cámaras, instalaciones eléctricas, UPS, gabinetes, servidores, pantallas LED videowall, switchs, y demás equipo necesario para el funcionamiento de las cámaras.
Drones	113 drones de vigilancia, entre ellos 111 drones tácticos de doble propósito (diurno y nocturno), con capacidad de captura térmica que facilita la detección de una persona en una zona rural y urbana, sin arriesgar la integridad del personal policial; un dron de búsqueda y rescate (naval y terrestre) y un dron estratégico VANT (Vehículo Aéreo No Tripulado) de largo alcance.
Sistemas de videovigilancia	Adquisición e implementación de tecnología (hardware y software) de un sistema de reconocimiento facial para el Sistema 911 y sistemas para administración y monitoreo de drones para ambas instituciones.

Fuente: Elaboración propia con base en BCIE, "Formulación para la ejecución del Programa de Modernización en Seguridad Ciudadana en el marco del Plan de Control Territorial en su Fase II", 2019, 15.

En El Salvador el uso de drones es relativamente novedoso para colaborar con tareas de seguridad ejercidas, principalmente, por la PNC. Este tipo de dispositivos han de requerir ciertas características para considerarse aptos en este campo de acción.

> *«Un dron debe de cumplir requerimientos técnicos y específicos para poder coadyuvar y contribuir a la labor de información de interés fiscal y policial. No es cualquier tipo de imagen. No es cualquier tipo de toma. No es cualquier tipo de cámara a la que estamos acostumbrados en El Salvador, como la que se usa para capturar imágenes de la ciudad»*
>
> Entrevista a Ricardo Sosa, experto en seguridad y criminología. Marzo de 2021

Actualmente, con la aprobación del financiamiento por parte del BCIE, en julio de 2021, el director de la Policía Nacional Civil (PNC), Mauricio Arriaza Chicas, junto al ministro de Justicia y Seguridad, Gustavo Villatoro, realizaron el lanzamiento de patrullajes con drones como nueva medida al combate a la delincuencia. Fueron 9 drones los que se presentaron, 3 unidades grandes y 6 pequeños, en los que invirtieron más de $120,000[52]. De acuerdo al ministro de Seguridad, se comprarán más equipos similares con la finalidad de tener drones en cada delegación policial a lo largo del país. Recientemente, en Ciudad Real, Santa Ana, se usaron drones con cámaras térmicas para detectar movimientos durante la noche mientras desarrollaban un operativo[53]. El presidente Nayib Bukele también lo expresó por medio de su cuenta de twitter en que mostraba imágenes del procedimiento en horas de la mañana[54].

> *«Los nuevos dispositivos que hemos incorporado al trabajo policial poseen tecnología de última generación que nos permite realizar patrullajes y operativos más eficientes para combatir a los grupos criminales en esta Fase 4 Incursión del Plan Control Territorial»*
>
> Gustavo Villatoro, ministro de Justicia y Seguridad

Las autoridades del Ministerio de Justicia y Seguridad han detallado que entre las diferencias de los drones comerciales con los equipos adquiridos por la corporación policial es que tienen un alcance de varios kilómetros, sensores de calor y capacidad de elevar-

52 Karla Ramírez, *"Presentan drones que realizarán patrullajes aéreos en combate a la delincuencia"*, La Prensa Gráfica, 20 de julio de 2021.
53 Ibidem.
54 Nayib Bukele (@nayibbukele), *"Así se ve la #Fase4 del #PCT La cámara térmica capta una columna de nuestros agentes, ingresando en una de las colonias con mayor presencia de pandillas en Santa Ana."*, Twitter, 1 de agosto de 2021. https://twitter.com/nayibbukele/status/1421878152469549057?s=20

se a más de 500 metros para no ser detectados ni interceptados[55] y para aprovechar al máximo estos recursos, en agosto de 2021 clausuraron un curso para capacitar a efectivos policiales en el manejo de estos equipos de alta tecnología utilizados para patrullajes no tripulados[56] especialmente en las zonas con presencia de pandilleros[57].

Tabla 5. Costo de equipo de vigilancia a adquirir con fondos del BCIE para el Ministerio de Justicia y Seguridad Pública

Artículo	Cantidad	Costo Unitario	Total
Cámaras PTZ	2,900	$3,041.38	$8,820,002.00
Cámaras fijas (blindada)	275	$3,500.00	$962,500.00
Cámaras LPR	800	$2,400.00	$1,920,000.00
Cámaras FR	100	$2,400.00	$240,000.00
Fibra óptica (km)	750	$7,516.26	$5,637,195.00
Sistema de análisis de reconocimiento facial	1	$929,998.00	$929,998.00
Centro de monitoreo S.S.	1	$1,482,810.00	$1,482,810.00
Centros de monitoreo regionales	12	$220,624.58	$2,647,495.00
Dron DJI MAVIC 2 Enterprise DUAL	89	$4,500.00	$400,500.00

Fuente: Jimmy Alvarado, "El préstamo del BCIE, un paso más en la militarización de la seguridad pública de Bukele", El Faro, 8 de marzo de 2020.

Por otro lado, el Ministerio de Defensa a cargo de René Francis Merino Monrroy, confirmó que los vehículos aéreos no tripulados que se planea adquirir serán utilizados para patrullar la zona rural norte del territorio en las fronteras con Honduras y Nicaragua[58].

> *"Estamos por adquirir, por segunda vez, un vehículo aéreo no tripulado para la parte marítima y parte fronteriza no habilitada. Tiene la capacidad de poder elevarse a unos 500 metros"*[59]
>
> René Francis Merino Monrroy, ministro de Defensa Nacional

55 Para más información ver: "La PNC y la Fuerza Armada ya usan tecnología de última generación en la fase 4 del Plan Control Territorial", Presidencia de la República, 1 de agosto de 2021.
56 Para más información ver: "Clausuran curso sobre manejo de drones", Presidencia de la República, 11 de agosto de 2021.
57 Para más información ver: "Los policías se están especializando en patrullajes aéreos no tripulados para modernizar sus técnicas de intervención", Presidencia de la República, 12 de agosto de 2021.
58 Para más información ver: "El Salvador empleará su flota de drones para patrullar zonas rurales del norte del país", Infodefensa.com, 1 de julio de 2021.
59 Ibidem.

De acuerdo al plan de intervenciones que tenía previstas la Fuerza Armada en el plan de seguridad, se adquirirían al menos 24 drones de vigilancia, búsqueda y rescate, "tácticos doble propósito"; además de un sistema de monitoreo y administración para los mismos[60].

Tabla 6. Costo del equipo de vigilancia adquirido con fondos del BCIE para el Ministerio de Defensa

Artículo	Cantidad	Costo Unitario	Total
Drones vigilancia búsqueda y rescate (Naval y terrestre)	1	$1,686,177	$1,686,177
Dron estratégico tipo VANT	1	$1,000,000	$1,000,000
Drones Tácticos doble propósito (diurno-nocturno)	22	$4,500	$99,000
Sistema de monitoreo y administración de drones	1	$70,000	$70,000

Fuente: Jimmy Alvarado, "El préstamo del BCIE, un paso más en la militarización de la seguridad pública de Bukele", El Faro, 8 de marzo de 2020.

Organizaciones de derechos humanos se han mostrado preocupadas por el acceso que tendrá Defensa a información sensible ante la falta de garantías legales de protección de información privada de la ciudadanía.

> *"El enfoque de esta administración, con este préstamo, es mantener de forma permanente al Ejército en tareas de seguridad pública. Esa sería su labor principal. Si es esa la visión, el componente principal del PCT es militar. No es de seguridad"*[61]
>
> Manuel Escalante, IDHUCA

El documento que detalla el uso de fondos para estas actividades plantea que, para el mantenimiento y sostenibilidad de los vehículos aéreos no tripulados, drones, se ha incluido la adquisición de licenciamiento para 5 años de un software especializado, un lote de repuestos ante fallas comunes y la capacitación para conocer el sistema. Además, se contempla la necesidad de contar con 18 personas para los drones vigilancia, búsqueda y rescate (naval y terrestre), 22 personas para drones tácticos doble propósito

60 Gabriela Villarroel, *"Ministerio de la Defensa alista licitación para nuevo dron estratégico"*, Diario El Mundo, 27 de marzo de 2021.
61 Jimmy Alvarado, *"El préstamo del BCIE, un paso más en la militarización de la seguridad pública de Bukele"*, El Faro, 8 de marzo de 2020.

(diurno-nocturno) y 6 personas para los drones del tipo estratégico VANT (por las siglas de "Vehículos Aéreos No Tripulados")[62]

A pesar de la fuerte inversión en estos equipos, las autoridades no han brindado información sobre las especificaciones técnicas de los equipos que se están adquiriendo, así como tampoco han definido lineamientos técnicos y normativos que permitan garantizar que la información registrada será de uso exclusivo de las autoridades de seguridad y que esta información será resguardada de forma segura y confidencial y desechada cuando no se limite a las competencias dirigidas a la investigación de delitos.

En los último dos años, la Policía Nacional Civil ha prescindido de este tipo de dispositivos para el monitoreo de marchas pacíficas en el país. Como muestra del descontento generalizado ante las decisiones de la administración actual se realizaron movilizaciones en las que participaron diversos sectores de la sociedad. En este contexto, específicamente, previo a la marcha que se llevó a cabo el 17 de octubre de 2021, la Comisionada Zoila Palma Noguera, subdirectora General de la PNC, giró un memorándum[63] el 16 de octubre, con carácter de información urgente, en el que exhorta a los agentes de la corporación a "cumplir las misiones establecidas en el Protocolo de actuación para la intervención policial ante actos de protesta que generen concentraciones y movilizaciones de personas". El Protocolo enmarca estas acciones como parte del cumplimiento de su Plan Estratégico Institucional 2020-2024, dentro de la línea estratégica 1 "Represión de la criminalidad", específicamente en la acción 1.1. "Implementar acciones operativas para el control territorial, a fin de reducir la incidencia delictiva, para mejorar la tranquilidad, orden y percepción de seguridad en el área urbana y rural", buscando minimizar los desórdenes y bloqueos de calles por las personas manifestantes. Entre sus lineamientos generales establece que "la Subdirección de Áreas Especializadas Operativas, garantizará el monitoreo por medio de patrullajes aéreos virtuales a través de la operación de drones, en cada una de las marchas, concentraciones que se realicen". Además, indica a la División de Emergencia 911 a "implementar y desarrollar dispositivos de seguridad virtual a través del sistema de videovigilancia, a fin de garantizar el control y seguimiento de las diferentes marchas y concentraciones de protesta". El mismo Protocolo indica que la información recaba deberá ser remitida a los Departamentos de Inteligencia a nivel nacional para la toma de decisiones.

El uso de estas herramientas tecnológicas para el seguimiento, control y vigilancia de las acciones ciudadanas pone en un nuevo escenario de riesgo a la población. El Salvador no cuenta con normativa suficiente que permita regular el uso de dispositivos como los drones por parte de instituciones del Estado, principalmente en torno a la información

62 BCIE, *"Formulación para la ejecución del Programa de Modernización en Seguridad Ciudadana en el marco del Plan de Control Territorial en su Fase II"*, 2019, 53.
63 PNC, Memorándum N° 5771, 16 de octubre de 2021.

recogida, el uso de esta información y las implicaciones sobre derechos fundamentales, como el derecho a la intimidad, la privacidad y el derecho a la autodeterminación informativa, entre otros.

En ese mismo orden de ideas, siguiendo con el tipo de dispositivos usados para el ámbito de la seguridad, los sistemas de videovigilancia representan la herramienta tecnológica más emblemática utilizada en El Salvador. Desde las competencias estatales, actualmente se hace uso de estas herramientas a través la Policía Nacional Civil, la cual cuenta con un Centro de Control de Videovigilancia que opera en diversas zonas de los municipios del país desde el año 2018. Este proyecto es parte del sistema de emergencia 911 y contó inicialmente con, al menos, 200 cámaras instaladas en San Salvador, Soyapango, Apopa, Mejicanos, Cuscatancingo y Ayutuxtepeque. Los dispositivos tienen la capacidad de captar placas de vehículos y realizar un cruce automático contra el listado de vehículos con reporte de robo. El costo superó los 3.7 millones de dólares e incluyó la instalación de fibra óptica[64].

Actualmente, el financiamiento del BCIE para la fase tres del PCT también contempla la adquisición de cámaras para distribuirse en delegaciones de la PCN presentes en los municipios con mayores índices de violencia y criminalidad.

Tabla 7. Centros de monitoreo de videovigilancia a ser intervenidos y distribución de cámaras delegaciones policiales

Municipio	Centro de Monitoreo	Total de cámaras
San Salvador	San Salvador 911	1110
Mejicanos		158
Apopa		133
Soyapango		183
Ilopango		181
San Martín		151
Colón		171
San Marcos		181
Ciudad Delgado		156
San Miguel	Regional 911	195
Santa Ana	Regional 911	199
Ahuachapán	Regional 911	150
Sonsonate	Regional 911	207
Usulután	Regional 911	145

64 Jaime López, *"Así funcionará el nuevo Centro de Control de Videovigilancia del sistema de emergencia 911"*, El Diario de Hoy, 25 de abril de 2018.

La Unión	Regional 911	140
Cojutepeque	Regional 911	90
Chalatenango	Regional 911	140
San Vicente	Regional 911	80
Zacatecoluca	Regional 911	145
Sensuntepeque	Regional 911	80
San Francisco Gotera	Regional 911	80
Total General por los Centros de Monitoreo		**4,075**

Fuente: Unidad de Acceso a la Información Pública (UAIP), respuesta a solicitud UAIP/RES.038.3/2020, Ministerio de Hacienda, 2020. 16.

Según lo planteado por el Ministerio de Hacienda, el proyecto de financiamiento aumentará en un 482% las cámaras de video, el cual es considerado como un disuasivo de delitos y como coadyuvante en la investigación policial[65]. Para estos efectos, el Gobierno de El Salvador ha estimado que, una vez instaladas las 4,075 cámaras a ser adquiridas, aumentará en un 75% la efectividad en la captura de delincuentes en general, es decir, se espera que, en el primero año de operación luego de la ejecución del proyecto, existan 1,349 capturas adicionales utilizando el sistema de videovigilancia, de los cuales se estima que 348 serán recuperaciones de vehículos[66].

Los procesos de implementación de tecnologías en el ámbito de la seguridad también son de relevancia para las acciones encabezadas por la Fiscalía General de la República en su labor de investigación en diversos casos, en los que Policía Nacional Civil se adscribe a las órdenes de la institución. Fiscalía ha resaltado la importancia y utilidad en los procesos judiciales de los vídeos que contienen imágenes de las cámaras de seguridad en relación al esclarecimiento de delitos.

> *"El fiscal ordena investigar si hay evidencias a través de video en tal lugar. Hay un libro de entrada y salida, y hay jefes de la policía, uno de ellos y yo, y hay otro que está en mi área, que son los que recibimos y marginamos los documentos. Hasta ahí. De ahí nadie más [de la policía] puede venir a sacar nada"*
>
> Entrevista al Subcomisionado Fredman Adonay, jefe del Departamento de Control de Vídeo Vigilancia de la Policía Nacional Civil. Abril de 2021

El representante de la PNC valora que el uso de estas herramientas presenta resultados significativos en la investigación del delito; no obstante, no se presentó documentación institucional que respaldara estas mejoras.

65 Unidad de Acceso a la Información Pública (UAIP), respuesta a solicitud UAIP/RES.038.3/2020, Ministerio de Hacienda, 2020. 32.
66 Ibidem, 33.

> *"Creemos, nosotros como policía, que la videovigilancia ha sido una herramienta que sigue siendo una herramienta efectiva. Es un plus para la seguridad pública. Hemos logrado muchos avances; cosas que nos eran difícil comprobar como el tema de los homicidios o accidentes de tránsito que podemos observar a través de una cámara que capta y luego graba lo que sucedió verdaderamente"*
>
> Entrevista al Subcomisionado Fredman Adonay, jefe del Departamento de Control de Vídeo Vigilancia de la Policía Nacional Civil. Abril de 2021

De los tres tipos de tecnologías aplicadas en el ámbito de la seguridad que se han estudiado en esta investigación, el uso de datos biométricos permanece en un generalizado desconocimiento, al menos para su uso estricto en esta área por parte de las instituciones correspondientes en El Salvador.

> *"Por ejemplo, aquí [en la policía] nosotros tenemos lectores biométricos, pero no sé de qué tipo. Eso no lo sé. Solo sé que sirve para mi huella y para registrar que entré a una hora y salí a otra. Eso es lo que conozco"*
>
> Entrevista al Subcomisionado Fredman Adonay, jefe del Departamento de Control de Vídeo Vigilancia de la Policía Nacional Civil. Abril de 2021

El préstamo acordado con el BCIE incluye la compra de un sistema de análisis de reconocimiento facial, que se vinculará a la información recogida por el sistema de videovigilancia. Los datos biométricos en El Salvador han sido utilizados en otras instancias estatales que no precisamente realizan labores de seguridad pública pero que pueden llegar a complementar las estrategias fiscales y policiales.

> *"Las bases más robustas pueden ser las del Registro Nacional de las Personas Naturales (RNPN), es decir, la del documento único de identidad (DUI) y la base de licencia de conducir. El DUI es la mejor base que tiene el país en cuanto a personas naturales y que permiten también hacer un cruce de información con diferentes tipos de mecanismos de videovigilancia"*
>
> Entrevista a Ricardo Sosa, experto en seguridad y criminología. Marzo de 2021

Al respecto, la Dirección de Informática y Desarrollo Tecnológico del Ministerio de Justicia y Seguridad Pública plantea que, durante el período 2019-2020, ha ejecutado acciones en coordinación con instituciones que poseen información ciudadana como el Registro Nacional de Personas Naturales (RNPN) y el Viceministerio de Transporte (VMT). La cartera de Estado plantea que con este cruce de datos se busca contar con una herra-

mienta de telecomunicaciones propia en la cual exista disponibilidad para la transmisión de imágenes, datos, video, voz y todos aquellos elementos digitales que deben ser enviados y recibidos para consolidar un sistema nacional[67]. La Dirección contempla como proyección apoyar en los componentes informáticos relacionados al PCT en su fase 3 a través del fortalecimiento de la seguridad pública por medio de un Sistema de Identificación Biométrica Nacional, un Sistema Nacional de Video Vigilancia, la construcción de una Infraestructura de Telecomunicaciones basada en fibra óptica a nivel nacional y la implementación de Unidades Autónomas de Vuelo[68]. Para ejemplificar los riesgos que estas decisiones estatales pueden generar, en octubre de 2021, el Parlamento Europeo votó una resolución a favor de prohibir completamente la vigilancia a través de sistemas de detección biométrica, como es la tecnología de reconocimiento facial, debido a su grave impacto en las libertades y derechos fundamentales como la privacidad[69].

La disrupción e implementación no regulada de la tecnología puede dañar las sociedades y afectar los derechos y libertades. Hay gobiernos que implementan y regulan las tecnologías para usarlas como mecanismos de represión, control, vigilancia y menoscabo de los derechos humanos. En México, durante la administración del presidente Enrique Peña Nieto, se intensificó la combinación del amedrentamiento, técnicas de manipulación de la información y sofisticadas tecnologías para desarrollar una oleada de abusos policiales. Este despliegue de tecnologías de vigilancia fue usado para espiar a la oposición política, lo cual es un acto claramente ilícito y que atenta directamente a la libertad de expresión, la seguridad de las personas afectadas y el ejercicio de la democracia[70]. Sin embargo, La Comisión Interamericana de Derechos Humanos (CIDH) y la Oficina en México del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (ONU-DH) publicaron un comunicado en el que expresaron su preocupación ante las nuevas revelaciones sobre el uso del malware Pegasus para espiar a personas defensoras de derechos humanos, periodistas y opositores, pidieron una investigación al Gobierno de México y reiteraron su llamado a una moratoria contra la venta y compra de este tipo de tecnología[71]

Ante esto, al no conocer un documento oficial del PCT no se tiene información suficiente sobre los usos en seguridad u otros que pudieran tener estos recursos tecnológicos por parte de las instituciones, lo cual debería estar descrito específicamente en la Política Nacional de Justicia y Seguridad Pública, pero que tampoco permite identificar las for-

67 MJSP, Informe de Labores 2019-2020, El Salvador, 2021, 19.
68 Ibidem, 21.
69 Para más información ver: *"Parlamento europeo vota a favor de prohibir la vigilancia masiva biométrica"*, Red en Defensa de los Derechos Digitales, 12 de octubre de 2021. Disponible en: https://r3d.mx/2021/10/12/el-parlamento-europeo-vota-a-favor-de-prohibir-la-vigilancia-con-inteligencia-artificial/?utm_campaign=meetedgar&utm_medium=social&utm_source=meetedgar.com
70 Alex Argüelles, *"Vigilancia en México: ¿Estos son los resultados?"*, Organización Derechos Digitales, 29 de noviembre de 2018.
71 Véase: *"CIDH y ONU-DH piden al gobierno de México investigar, castigar y regular el uso de tecnologías de vigilancia"*, Red en Defensa de los Derechos Digitales, 6 de agosto de 2021.

mas en que se utilizarán especialmente ante un contexto de control de las instituciones del Estado por parte del presidente luego del 1 de mayo del presente año.

Los desafíos para la implementación de tecnologías en El Salvador son diversos. Hay retos económicos, educativos, jurídicos y regulatorios para el abordaje de estas herramientas que aún no han sido tomados en cuenta, sobre todo para considerar las posibles afectaciones hacia los derechos humanos de la población relacionados con su privacidad e intimidad. La tecnología es multidimensional, y es por ello que las discusiones actuales respecto al uso, implementación y regulación de la tecnología son abordadas cada vez más de manera multidisciplinaria considerando principalmente el aspecto legal, ético y humano. Existe, pues, la necesidad imperante que se retomen diálogos articulados entre distintos actores tanto dentro y fuera del aparato estatal para concretar marcos legales que garanticen la protección de los datos e integridad de las personas al hacer uso de estas herramientas.

Capítulo 3

Tecnologías y Derechos Humanos

En la era tecnológica, cuando se habla del uso de distintos dispositivos de control y vigilancia abarca una serie de actividades: monitorear, interceptar, recoger, analizar, usar, preservar, guardar, interferir u obtener información que incluya o refleje las comunicaciones pasadas, presentes o futuras de una persona.[72] El alcance de la intromisión en este ámbito, sobre todo a cargo de los gobiernos a nivel global, salió a la luz en 2013, cuando el antiguo contratista de la Agencia Central de Inteligencia (CIA, por sus siglas en inglés), Edward Snowden, filtró información clasificada de la Agencia de Seguridad Nacional de los Estados Unidos. Según las filtraciones, alrededor del 90 por ciento de las comunicaciones interceptadas no pertenecían a objetivos, sino a gente común.

> *"Los gobiernos en todas las regiones están utilizando también herramientas de vigilancia digital para localizar y atacar a los defensores de los derechos humanos y a las personas percibidas como críticas, incluidos abogados, periodistas, activistas de derechos a la tierra o al medio ambiente, y personas que apoyan la igualdad para los miembros de la comunidad LGBTI ".*
>
> Michelle Bachelet, Alta Comisionada de las Naciones Unidas para los Derechos Humanos[73]

Las condiciones en las que las sociedades se desarrollan y dinamizan actualmente están permeadas por la era tecnológica. Desde diversos ámbitos, la tecnología tiene la capacidad de generar y almacenar grandes cantidades de información que sin regulaciones y limitaciones podrían convertirse en sistemas de vigilancia permanente para toda la población, asimismo, podría vulnerar y restringir de manera directa e indirecta derechos humanos como el derecho a la intimidad y la privacidad. Así, pues, las implicaciones que tendría el uso de la tecnología en relación con la seguridad ciudadana aún no han sido retomadas dentro de los marcos normativos a nivel regional. Los esfuerzos para regular el uso de los dispositivos tecnológicos han tenido resultados considerando principalmente aspectos meramente técnicos dejando sin prioridad la protección de la información de las personas.

72 Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, "Cambios de Tecnología y Definiciones". Disponible en: https://es.necessaryandproportionate.org/text
73 Véase: 70 años después de la Declaración Universal de Derechos Humanos: 30 artículos sobre los 30 artículos - Artículo 12, ONU, Disponible en: https://www.ohchr.org/SP/NewsEvents/Pages/DisplayNews.aspx?NewsID= 23907&LangID=S

Estas tecnologías representan una grave amenaza contra los derechos de las personas, su intimidad o privacidad, principalmente, porque su uso no está regulado legalmente. Asimismo, tampoco se conoce suficiente sobre sus finalidades, alcances y límites, ni sobre las formas en que han sido adquiridas o desarrolladas, quiénes son las empresas proveedoras ni cuánto dinero se ha invertido exactamente; mucho menos se conoce sobre sus políticas o planes de uso, ni de protocolos de protección de datos personales. En este capítulo se analizará la situación que enfrenta El Salvador en relación con las ausencias de regulación de los dispositivos tecnológicos para el ámbito de la seguridad, las propuestas presentadas por medio de los grupos parlamentarios y las posibles afectaciones que pueden darse en este contexto desde un enfoque de derechos humanos.

Marco legal nacional

Desde hace algunos años la administración pública salvadoreña habría estado invirtiendo en la adquisición de recursos tecnológicos para mejorar la prestación de sus servicios en múltiples ámbitos de su funcionamiento: por ejemplo, desde agilizar la captura de datos en la gestión de documentos personales, pasando por mejorar el control sobre la jornada laboral de los servidores públicos, hasta ampliar las posibilidades de identificación de las personas. No obstante, actualmente se ha mostrado un mayor interés por llevar esta inversión a montos más elevados y, con ello, adquirir y desarrollar un mayor número de recursos tecnológicos con capacidades de vigilancia. Desde la seguridad ciudadana existe la premisa que el Estado no debe adoptar o aplicar una práctica de vigilancia sin el derecho del público de conocer sus límites, además, si existe una ley esta debe ser lo suficientemente clara y precisa, asegurando que las personas cuentan con suficiente información sobre su existencia y puedan prever su aplicación[74]. La tendencia a nivel regional refleja, en primer lugar, que este principio no está siendo aplicado en el uso de tecnología en las distintas ciudades y, en segundo lugar, tampoco hay regulaciones que prioricen el enfoque de derechos frente a los aspectos técnicos para su utilización.

> *"A mí me llama la atención que, evidentemente, no he encontrado ningún marco normativo o ninguna referencia en nuestro ordenamiento que prohíba el uso de estas tecnologías. Sin embargo, tampoco he encontrado ninguno que permita hacer uso de las tecnologías. Entonces, claro, mi impresión es que estas tecnologías se están utilizando por una interpretación incorrecta del principio de legalidad o el principio de libertad. Es decir, los gobernantes han decidido aplicarlo porque la ley no se los prohíbe"*
>
> Entrevista a Manuel Escalante, director del Instituto de Derechos Humanos de la UCA (IDHUCA) Marzo de 2021

74 Fundación Acceso, Privacidad digital para defensores y defensoras de derechos: un estudio sobre cómo los marcos legales de El Salvador, Guatemala, Honduras y Nicaragua pueden ser utilizados para la protección, criminalización y/o videovigilancia digital de defensoras y defensores de derechos humanos, 1° Edición, San José, Costa Rica, 2015, 36.

A partir del año 2011 en El Salvador entró en vigor la Ley de Acceso a la Información Pública (LAIP), la cual tiene como objetivo garantizar el derecho de acceso de toda persona a la información pública, a fin de contribuir con la transparencia de las actuaciones de las instituciones del Estado. En cuanto a protección de datos, la LAIP regula y desarrolla expresamente lo relativo a protección de datos personales en manos de entidades públicas o privadas que administran servicios públicos en sus artículos del 31 al 39. Sin embargo, la entidad encargada de ejecutar dicha ley, el Instituto de Acceso a la Información Pública (IAIP), también emitió los Lineamientos Generales de Protección de Datos Personales para las Instituciones que conforman el Sector Público, los cuales establecen las políticas generales que deberán observar las dependencias y entidades de la Administración Pública para garantizar a las personas la facultad de decisión sobre el uso y destino de sus datos personales con el propósito de: a) Asegurar su adecuado tratamiento e impedir su uso para finalidades distintas de aquellas que motivaron su suministro, b) Evitar la transferencia de datos personales que sea ilícita y lesiva para la dignidad y derechos de la persona afectada y c) Instar a la Administración Pública a adoptar una cultura institucional y una concientización acerca de la importancia de poner en práctica los principios de acceso a la información pública y la transparencia, en equilibrio con el derecho a la protección de datos personales de las personas administradas, con las limitaciones que establece la Ley[75].

Durante el año 2020 las autoridades de las instituciones de seguridad del Gobierno de El Salvador se prepararon para implementar uno de los memorandos que firmó con Estados Unidos en 2019 sobre asuntos migratorios, específicamente el que regula al intercambio de información biométrica y otros datos personales[76]. Además, como estrategia de contención del virus y de atención de pacientes contagiados, las autoridades de salud también invirtieron en equipos tecnológicos con capacidad de reconocimiento facial que fueron destinados al Hospital El Salvador[77], el hospital nacional construido exclusivamente para atención a pacientes afectados por COVID-19. Este tipo de software de reconocimiento facial también habría sido utilizado en la realización de la prueba académica AVANZO, por parte del Ministerio de Educación, que tuvieron que rendir estudiantes del último año de bachillerato a nivel nacional[78].

75 IAIP, Lineamientos Generales de Protección de Datos Personales para las Instituciones que conforman el Sector Público, El Salvador, 2020.
76 Instituto de Derechos Humanos de la UCA (@idhuca), *"Comunicado sobre las acciones emprendidas en relación al Memorando firmado entre los Gobiernos de El Salvador y Estados Unidos, relativo al intercambio de información biométrica y otros datos personales"*, Twitter, 31 de enero de 2020. https://twitter.com/idhuca/status/ 1223301601542184961
77 Véase: *"Presidente Nayib Bukele inaugurará primera fase del hospital para COVID-19 en instalaciones de CIFCO"*, Presidencia de la República, 20 de junio de 2020. Disponible en: https://www.presidencia.gob.sv/presidente-nayib-bukele-inaugurara-primera-fase-del-hospital-para-covid-19-en-instalaciones-de-cifco/
78 Laura Jordán, *"Dilema legal de la Prueba AVANZO por el uso de datos"*, La Prensa Gráfica, 29 de noviembre de 2020.

Por medio de la solicitud de acceso a la información pública con referencia UAIP 32-2021 se requirió la copia digital de los lineamientos para el manejo, mantenimiento, seguridad y protección de datos personales dictados por el Instituto de Acceso a la Información Pública (IAIP), con base en el artículo 58, literal j, de la LAIP, en relación a los sistemas, programas y/o aplicaciones informáticas, los sistemas de video vigilancia, la tecnología de identificación mediante datos biométricos (huella, voz, imagen, etc.) o reconocimiento facial y los drones con cámaras u otros dispositivos de identificación y/o seguimiento. La resolución manifestó: *«este Instituto conformó un equipo multidisciplinario con la finalidad de analizar las capacidades institucionales tanto del IAIP como de los demás entes obligados, en materia de protección de datos personales; para lo cual, tomando en cuenta el contexto actual, se ha realizado una revisión interna de la normativa en la materia»*. Y agrega: *«se confirma que la información solicitada por la persona requirente es inexistente, puesto que tal como se ha señalado en los romanos anteriores, se está en proceso de elaboración de la normativa pertinente en materia de protección de datos personales; además, de que a la fecha no se cuenta con los registros y sistemas relacionados en el Art. 35 de la LAIP».*

Por otro lado, El Salvador también cuenta con la Ley Especial contra Delitos Informáticos y Conexos que entró en vigor en el año 2016. La ley tiene por objetivo proteger los bienes jurídicos de aquellas conductas delictivas cometidas por medio de las tecnologías de la información y la comunicación, así como la prevención y sanción de los delitos cometidos en perjuicio de los datos almacenados, procesados o transferidos; los sistemas, su infraestructura o cualquiera de sus componentes, o los cometidos mediante el uso de dichas tecnologías que afecten intereses asociados a la identidad, propiedad, intimidad e imagen de las personas naturales o jurídicas. La Comisión de Seguridad Pública y Combate a la Narcoactividad, de la Asamblea Legislativa, ha vuelto a retomar discusiones relacionadas a esta ley; en septiembre de 2021 el diputado de Nuevas Ideas, Francisco Villatoro, con el apoyo del especialista en ciberseguridad, Víctor Rodríguez, propuso a la Comisión que se añadan artículos y capítulos al Código Procesal Penal que estén relacionados con el manejo que se debe hacer de la evidencia digital[79]. De acuerdo con Rodríguez, al no tener una regulación concreta, cada uno de los jueces, según su experiencia, decide cómo incorporar, producir y valorar la evidencia digital, lo cual genera un vacío de ley. El experto en ciberseguridad planteó, además, que también se debe regular la figura del "agente encubierto digital", que estará a cargo de la Policía Nacional Civil (PNC), pero que serían autorizados por orden de la Fiscalía General de la República (FGR), sin que medie opinión de un juez[80].

> *"Uno de los principales desafíos es establecer los límites o las líneas sobre las cuales uno pueda decidir que sí vale la pena usar ese tipo de tecnología para garantizar*

79 Para más información ver: *"Diputados siguen escuchando a expertos antes de elaborar propuesta para reformar Ley Contra Delitos Informáticos"*, Asamblea Legislativa, 29 de septiembre de 2021.
80 Denni Portillo, *"Nuevas Ideas propondrá usar 'agentes encubiertos digitales'"*, La Prensa Gráfica, 12 de octubre de 2021.

> *el derecho a la Seguridad Ciudadana, pero sin abrir la peligrosa puerta a una vulneración sistemática a otros derechos, como el derecho a la privacidad, a la autodeterminación informativa y a que se puedan utilizar los datos para otros abusos en materia de Derechos Humanos, como el seguimiento, espionaje, amedrentamiento para evitar la contraloría social, amedrentamiento a la prensa, etcétera"*
>
> Entrevista Carlos Palomo, presidente de la Asociación Transparencia, Contraloría Social y Datos Abiertos (TRACODA) Abril de 2021

En este marco, aunque existan tanto esta ley como la LAIP, el país aún no cuenta con leyes que protejan a las personas del uso indiscriminado que puedan hacer con sus datos recolectados por medio de dispositivos tecnológicos como drones, cámaras de videovigilancia o datos biométricos, principalmente en el contexto actual donde estas herramientas están siendo utilizadas como parte del plan de seguridad de la administración actual a cargo del presidente Nayib Bukele.

Propuestas de ley impulsadas desde el Órgano Legislativo

En 2017, la Gran Alianza por la Unidad Nacional (GANA), a través de su diputado Osiris Luna Meza, presentó una propuesta de Ley de videovigilancia donde estipula la necesidad de la creación y regulación de un sistema nacional de videovigilancia que fortalezca la investigación tecnológica del delito y pueda ser un apoyo para la judicialización de los casos, es decir, que pueda ser un medio probatorio para el sistema judicial. Esta propuesta de ley contemplaba la regulación de cámaras, fijas o móviles, sistemas de videovigilancia, dispositivos de grabación de video y sonido en bienes públicos, vehículos policiales, transporte público y privado de pasajeros, establecimientos comerciales, circuitos cerrados de televisión, etc. Expresaba, además, que las encargadas del manejo de toda la información son las autoridades de seguridad pública y empresas privadas. No obstante, las disposiciones de la propuesta hacia las herramientas tecnológicas no hacían énfasis en los límites de los usos, es decir, la información que los sistemas recolectan quedaría sin garantías de protección efectiva.

Si bien los sistemas de videovigilancia son utilizados dentro de las acciones de prevención que contemplan las políticas de seguridad con el fin de tener un objetivo disuasorio, en general pasan a ser un elemento represivo debido a que resguardan la información por un tiempo determinado, para luego, ante la ocurrencia de un hecho delictivo o su sospecha, proceder a buscar en los registros de imágenes para individualizar a los sospechosos del resto de la sociedad[81], es decir, se recurre a prácticas que atentan contra el derecho de los ciudadanos a la privacidad y a no ser discriminado, y no siempre se tiene la garantía de que un delito registrado por una cámara será debidamente procesado ante las instituciones correspondientes.

81 Milton Lechner, Tecnologías aplicadas a la seguridad ciudadana: desafíos para la justicia transicional ante nuevos mecanismos de control social", Revista Divulgatorio, Número 1, 2016, 5.

> *"Actualmente, carecemos de leyes que estén regulando el tema de la vigilancia. La policía lo hace en base al artículo 159 de la Constitución, que es lo que nos ampara para garantizar la seguridad pública y bajo esa línea se desarrolla la seguridad a través de las cámaras, pero no hay algo más hasta este momento. Esperaríamos que en los próximos meses o años se promueva algo para poder tener un sustento [...] es necesario crear una normativa que sea específica para el tema del uso de la tecnología en el caso de la videovigilancia, de los drones y cosas como esas"*
>
> Entrevista al Subcomisionado Fredman Adonay, jefe del Departamento de Control de Vídeo Vigilancia de la Policía Nacional Civil. Abril de 2021

En noviembre de 2020, el grupo parlamentario del partido político Alianza Republicana Nacionalista (ARENA), a través del diputado Mauricio Vargas, presentó la Ley de Seguridad Nacional de la Republica de El Salvador donde se propone la creación de El Sistema de Seguridad Nacional del Estado de El Salvador (SISENES) y el Consejo de Seguridad Nacional (COSEN) entidad que sería la encargada de la aplicabilidad de lo estipulado en la ley. Según la propuesta: "es necesario que el Estado salvadoreño tenga un marco legal que reglamente lo referente a seguridad nacional, para que le permita estar preparado y contar con las herramientas indispensables para afrontar lo que pueda afectar u obstaculice el desarrollo nacional ante los diferentes antagonismos, riesgos y vulnerabilidades, así como *las nuevas amenazas de carácter multidimensional en los ámbitos económicos, políticos, sociales y hasta en el ciberespacio".*

Esta propuesta de ley no contempla explícitamente el uso de tecnologías para velar por lo que define como Seguridad Nacional, sin embargo, es importante tomarla en cuenta ya que deja entrever la noción de lo que se prioriza en los sectores más conservadores que ostentan el poder dentro de los Órganos del Estado, es decir, un sentido muy contrario a lo que permite dirigir los esfuerzos hacia ejercer la función pública desde una perspectiva de seguridad ciudadana para potenciar los derechos individuales y colectivos; más hacia la ciudadanía que a la seguridad nacional (desde una perspectiva política) y brindar las garantías necesarias para proteger a la sociedad de cualquier abuso de poder.

> *"Existen litigios estratégicos en la CIDH y es importante pensar cómo incluir esto en los sistemas nacionales; en los de justicia como leyes federales o en la suprema corte. Es un desafío que cada grupo en su país tiene que hacer. Lo otro es expandir los efectos de la tecnología para los derechos fundamentales y pensar en la protección de los datos como derechos fundamentales y hacer interpretaciones extendidas no solo conceptualizar"*
>
> Entrevista a Rafael Zanatta, director de Investigación de la Asociación de Privacidad de Datos, Brasil. Marzo de 2021

Contando con algunas reglas dispersas, como un breve capítulo en la Ley de Acceso a la Información Pública (LAIP) y algunas normas en leyes (Ley de Regulación de los Servicios de Información sobre el Historial de Créditos de las Personas, Ley de la Firma Electrónica, etc.), en abril de 2021 la Asamblea Legislativa aprobó la Ley de Protección de Datos Personales y Hábeas Data. Uno de los objetivos de la misma es garantizar que toda persona pueda ejercer el derecho para conocer su información, para qué es utilizada la misma, así como su protección, corrección, rectificación o actualización, frente a instituciones públicas o privadas[82]. A nivel de país esto representaría un importante precedente sobre todo tomando en consideración diversos casos como el que ocurrió en noviembre de 2020, donde una investigación periodística reveló que la información de usuarios que accedieron al sistema de solicitudes del Instituto de Acceso a la Información pública (IAIP) era transferida automáticamente a Casa Presidencial[83]. Sin embargo, esta ley fue vetada por la presidencia[84] aduciendo falta de armonía con el marco legal vigente y que no han sido considerados aspectos sobre el derecho a la autodeterminación informativa, entre otros. Además, el presidente vetó la Ley de Creación de la Autoridad Nacional Digital, la cual buscaba complementar la Ley de protección de datos personales[85].

> *"Un reto sería establecer el marco de análisis o el marco conceptual bajo el que, o sobre el cual, el estado salvadoreño o la asamblea legislativa o las entidades correspondientes que vayan a implementar la tecnología sepan discernir qué tecnología puedan utilizar, o que puedan preponderar si una tecnología da resultados lo suficientemente eficaces como para afectar en alguna medida los derechos"*
>
> Entrevista Carlos Palomo, presidente de la Asociación Transparencia, Contraloría Social y Datos Abiertos (TRACODA) Abril de 2021

Si bien en Latinoamérica la implementación masiva de estos tipos de dispositivos tecnológicos fue mucho más tardía que en otras regiones del mundo, esto no exenta de la responsabilidad a los gobiernos y órganos legislativos para atender la necesidad de legislar en la materia, principalmente para contrarrestar las potenciales violaciones a los derechos humanos en las que puede incurrir su uso. Así mismo, existe el riesgo de que sean utilizadas para para controlar, atacar o reprimir a la oposición política, periodistas o personas defensoras de derechos humanos, junto a sus familias. Considerando el contexto del país, en el siguiente apartado se analizarán las vulneraciones a derechos

82 Laura Hernández, *"Ley de datos personales: sin pausa, pero sin prisa y de cara a la sociedad"*, Derechos Digitales, 19 de marzo de 2021.
83 Jessica Ávalos, *"Los audios que comprometen al IAIP en la filtración de información confidencial"*, Revista Factum, 13 de noviembre de 2019.
84 Juan Carlos Menjívar, *"Presidencia veta Ley de Protección de Datos Personales y Hábeas Data"*, Revista Derecho y Negocios, 18 de mayo de 2021.
85 Gobierno de El Salvador, Índice de vetos a Decretos Legislativos: 2021/05/11 Decreto Legislativo No. 873 *"Ley de Creación de la Autoridad Nacional Digital"*.

humanos específicos mediante el uso de las tecnologías con capacidades de vigilancia que sean implementadas sin la debida regulación.

Afectaciones a derechos humanos

La sociedad salvadoreña, como la mayoría de sociedades en la región, parece haber abrazado los avances de las nuevas tecnologías de la información y la comunicación sin mayor discusión sobre los riesgos y efectos contraproducentes que estos avances podrían afectar sobre sus garantías fundamentales. Estas nuevas dinámicas han provocado que derechos como el acceso a la información, el derecho a la protección de datos y la privacidad, entre otros, se vuelven cada vez más importantes de discutir para protegerse ante la actuación del Estado. Dicha urgencia queda en evidencia cuando en El Salvador existen casos en donde las empresas, por ejemplo, manejan datos de cualquier persona sin su consentimiento e incluso con su desconocimiento sobre la existencia de los mismos.

La población salvadoreña no sabe quién y para qué se están almacenando, gestionando o utilizando sus datos personales; ignora a quién tiene que dirigirse para solicitar la cancelación de informaciones erróneas o incluso desconoce si puede exigirlo jurídicamente, porque no existe, en el país, un marco jurídico que lo proteja contra el uso abusivo de sus datos personales[86]. En este apartado se analizarán las principales afectaciones hacia derechos humanos fundamentales ante la ausencia de un marco legal nacional que les garantice.

Derecho a la intimidad

Según su definición, en la intimidad personal, nadie puede, por ningún motivo o circunstancia, tener acceso a determinada información sin autorización del titular del derecho[87]. La privacidad, como esfera de protección del derecho a la intimidad, consiste en el poder de controlar la información personal, decidir con quién se comparte y para qué se utiliza con terceros, así como el derecho a que ésta se trate de forma adecuada, para permitir el ejercicio de otros derechos y evitar daños a su titular[88]. Así, pues, el derecho a la privacidad contempla la protección de la persona y no de los lugares o espacios públicos, es decir, poder transitar en el anonimato, sin ser identificado, grabado o monitoreado. En circunstancias poco favorables esto tiene repercusiones en el comportamiento de las personas frenando su derecho a expresarse debido a que la vigilancia permite identificar lo que personas expertas denominan como la otredad peligrosa; personas o grupos que representan una amenaza latente para el Estado y la sociedad en general[89].

86 José María Ayala et al. La protección de datos personales en El Salvador, El Salvador, UCA Editores, 2005, 21.
87 Sandra Santos, *Derecho a la Intimidad Derechos Fundamentales*, UCA, 2016.
88 Instituto Nacional de Transparencia, *Acceso a la Información Pública y Protección de Datos Personales, Guía práctica para ejercer el derecho a la protección de datos personales*, México (s.f.)
89 Emilio Daniel Cunjamá et. al. *"Sociedad de la vigilancia y Estado policial: Análisis de las tecnologías y aparatos de control"*, El Cotidiano, núm. 161, mayo-junio, 2010, 9.

Ante la ausencia de marcos normativos que regulen tanto aspectos técnicos y administrativos, así como las afectaciones que puedan experimentar las personas, este escenario puede dar lugar a la criminalización de grupos específicos de la sociedad, puesto que su vigilancia y control estaría justificado bajo premisas que no podrían comprobarse legalmente.

> *"Para mí, el principal riesgo es la posibilidad de que perdamos el derecho a la privacidad porque podemos tener tal grado de vigilancia que pueda realizar un perfil tan exhaustivo de mí para que sepan con quién me reúno o frecuento y que puedan utilizarse para intentar amedrentarme o amenazarme. Es decir, en alguna medida limitar mi ejercicio de otros derechos como, por ejemplo, el de contraloría y el de fiscalización ciudadana, porque perfectamente pueden ir a estos sistemas y tener algún elemento con el que puedan intentar chantajearme, amedrentarme o con el cual puedan hacer presión pública"*
>
> Entrevista Carlos Palomo, presidente de la Asociación Transparencia, Contraloría Social y Datos Abiertos (TRACODA) Abril de 2021

La falta de regulación y, particularmente, la ausencia de un enfoque de derechos humanos y la armonización con estándares internacionales de derechos humanos genera condiciones de incertidumbre y desprotección ante el poder del Estado, el cual pudiera registrar una gran cantidad de información personal sin controles y con la posibilidad de utilizar la misma con amplia discrecionalidad.

> *"Sin duda, el eje transversal de todos estos dispositivos debería de ser el respeto a los Derechos Humanos. Existen en muchos lugares del mundo, en Centroamérica y en El Salvador, donde estos tipos de dispositivos que no están considerando el enfoque de derechos humanos cometen violación a la privacidad y a la intimidad"*
>
> *Entrevista a Ricardo Sosa, experto en seguridad y criminología. Marzo de 2021*

Las modalidades a través de las cuales pueden realizarse vulneraciones a la esfera protegida por el derecho de intimidad son muchas: por ejemplo, la intercepción de comunicaciones telefónicas y electrónicas, divulgación de información bancaria, divulgación de historias clínicas, allanamientos ilegítimos de domicilio, secuestro de computadoras, acceso a los datos en manos de terceros, entre otras[90].

90 Fundación Acceso, Privacidad digital para defensores y defensoras de derechos: un estudio sobre cómo los marcos legales de El Salvador, Guatemala, Honduras y Nicaragua pueden ser utilizados para la protección, criminalización y/o videovigilancia digital de defensoras y defensores de derechos humanos, 1° Edición, San José, Costa Rica, 2015, 75

Para proteger este derecho, la jurisprudencia constitucional a nivel nacional ha recurrido al recurso de amparo como la garantía para la protección de los derechos fundamentales en general y, por lo tanto, del derecho a la intimidad. En algunos casos, la Sala de lo Constitucional también ha utilizado como garantía el habeas corpus, por medio del cual han surgido importantes líneas y criterios jurisprudenciales para proteger el derecho a la intimidad de las personas[91].

Derecho a la autodeterminación informativa

Por su parte, es el derecho que tiene por objeto garantizar la facultad de las personas para conocer y acceder a las informaciones archivadas en bancos de datos que les conciernen, así como controlar su calidad, lo cual implica la posibilidad de corregir o cancelar los datos inexactos o indebidamente procesados, y disponer sobre su transmisión. En esta faceta se destaca: i) La facultad de conocer, en el momento específico de la recolección de los datos, el tipo de información personal que se va a almacenar; ii) la potestad de conocer la existencia de bancos de datos automatizados; iii) la libertad de acceso a la información; iv) la facultad de rectificación, integración o cancelación de los datos para asegurar su calidad y el acceso a ellos; y, v) la potestad de conocer la transmisión de los datos personales hacia terceros"[92].

> *"Todos estos datos que se recaban pueden utilizarse para propósitos de los cuales yo ni siquiera estoy enterado y para los cuales evidentemente no he dado autorización. Y ese derecho de autodeterminación informativa comprende que yo tenga el poder de decidir quiénes utilizan mis datos, para qué los utilizan y oponerme en caso de que yo esté en desacuerdo con el uso que se les esté dando, con el tratamiento, con los cruces de información, si los están vendiendo, etcétera"*
>
> Entrevista Carlos Palomo, presidente de la Asociación Transparencia, Contraloría Social y Datos Abiertos (TRACODA) Abril de 2021

La protección de datos personales en El Salvador tiene su mejor expresión en la jurisprudencia. El derecho a la autodeterminación informativa no está regulado expresamente ni en la Constitución ni en algún tipo de ley. De acuerdo con algunas experiencias, para ejercer tal derecho debe recurrirse de manera complementaria al derecho a la intimidad, regulado en el artículo 2 de la Constitución, ya que se considera a la autodeterminación informativa como una manifestación del derecho de intimidad[93]. La Constitución de la

91 Ibidem, 76.
92 Sala de lo Constitucional. Corte Suprema de Justicia de El Salvador. Sentencia de Amparo 142-2012.
93 Fundación Acceso, Privacidad digital para defensores y defensoras de derechos: un estudio sobre cómo los marcos legales de El Salvador, Guatemala, Honduras y Nicaragua pueden ser utilizados para la protección, criminalización y/o videovigilancia digital de defensoras y defensores de derechos humanos, 1° Edición, San José, Costa Rica, 2015, 77.

República, en el artículo 2, garantiza el derecho al honor, a la intimidad personal (derecho a la autodeterminación informativa), y a la propia imagen; asimismo, el artículo 247 reconoce el amparo como mecanismo de protección ante la violación de este derecho. En razón de ello, el amparo -de manera supletoria- se convierte en la garantía para proteger derechos como la autodeterminación informativa, entre otros[94]. A la fecha, las respuestas ante vulneraciones del derecho a la autodeterminación informativa se han dado a través de criterios emitidos por la Sala de lo Constitucional, de la Corte Suprema de Justicia, en sentencias provenientes de recursos de amparo.

Desde la sentencia de Amparo 934-2007, la Sala de lo Constitucional sostuvo que: *«... el derecho a la autodeterminación informativa tiene por objeto preservar la información de las personas que se encuentra contenida en registros públicos o privados frente a su utilización arbitraria —especialmente la almacenada a través de medios informáticos—, sin que necesariamente se deba tratar de datos íntimos».*

En la sentencia de Amparo 142-2012, la Sala señaló que: *«la faceta material de este derecho permite a las personas definir la intensidad con que desea que se conozcan y circulen tanto su identidad como otras circunstancias y datos personales; combatir las inexactitudes o falsedades que las alteren; y defenderse de cualquier utilización abusiva, arbitraria, desleal o ilegal que pretenda hacerse de esos datos; que, para conseguir estos fines, se cuenta con la técnica de protección de datos, que se encuentra integrada por un conjunto de derechos subjetivos, deberes, principios, procedimientos, instituciones y reglas objetivas".* En esta sentencia se reconocen los derechos de los usuarios, así como los principios de la protección de datos personales y algunas reglas para este fin.

Estos recursos legales fueron el antecedente para la protección de datos personales en El Salvador. Algunas de estas consideraciones fueron incorporadas en la LAIP (art. 31 a 39) y en los Lineamientos Generales para la Protección de Datos Personales en los Entes Obligados, emitidos por el IAIP.

Un informe de coyuntura presentado por el Departamento de Estudios Legales de FUSADES destacó y analizó la sentencia de amparo 142- 2012, emitida por la Sala de lo Constitucional en octubre de 2014, que estableció la violación al derecho a la autodeterminación informativa por parte de una sociedad privada, evidenciando la necesidad de aprobar en el país una ley de protección de datos personales. El informe subraya que en dicha sentencia se reiteró el asidero constitucional del derecho a la autodeterminación informativa y el derecho a ser protegido en su goce[95]. Por su parte, INDATA, una asociación sin fines de lucro, la cual muestra interés en temas como protección de datos, habeas data,

94 Ibidem, 79.
95 Fundación Salvadoreña para el Desarrollo Económico y Social, Informe de coyuntura legal e institucional, El Salvador, 2014, 95.

autodeterminación informativa y derecho informático, presentó la demanda de inconstitucionalidad contra la empresa EQUIFAX-DICOM por el procesamiento arbitrario e ilegal de datos personales de miles de personas, la cual fue resuelta a favor de INDATA[96].

De lo anterior se debe entender que toda persona que estime violaciones a su derecho a la intimidad y al derecho a la autodeterminación informativa, por causa de su inclusión en una base de datos delictiva, crediticia u otra naturaleza, y especialmente por el uso no autorizado de su información personal, tiene derecho a interponer ante la Sala de lo Constitucional el recurso de amparo correspondiente.

> *"Otro reto sustancial es como empoderamos a la gente de tal manera que pueda fiscalizar la tecnología porque es una materia bien especializada en la que no cualquiera puede entrar, pero tampoco podemos permitir que sólo sea un grupo selecto y minúsculo de personas el que tenga el poder de analizar estos sistemas o que tenga el poder de involucrarse con ellos. Entonces, en alguna medida, tenemos que buscar como lo aterrizamos al público en general, que no necesariamente es informático, y cómo hacemos para animarlos a exigir que los sistemas informáticos, los sistemas de vigilancia, ya sean drones, etcétera, sean más transparentes, que sean más auditables"*
>
> Entrevista Carlos Palomo, presidente de la Asociación Transparencia, Contraloría Social y Datos Abiertos (TRACODA) Abril de 2021

Las regulaciones hacia estas tecnologías aplicadas a la seguridad, tales como drones, cámaras de videovigilancia y sistemas biométricos, han dejado de lado los aspectos sociales generadores de conflictos relacionados con las violaciones del derecho a la intimidad y otros y se focalizan en conformar una red de control a cargo de las instituciones de seguridad, en particular la policía, pero también las fuerzas armadas.

Las autoridades crean un discurso desde la coyuntura política que determina acciones populistas y simplistas que pretenden solucionar las problemáticas estructurales, recurriendo a la tecnología como si esta fuera la solución mágica para resolver problemas profundos e históricos, prometiendo modernizar el Estado y su respuesta. Aunque se valora como necesario y pertinente el uso de la tecnología aplicada al ámbito de la seguridad ciudadana, su uso debe ser siempre responsable y medido, protegiendo todos los derechos y garantías constitucionales.

96 Asociación Salvadoreña para la Protección de Datos e Internet (INDATA), Disponible en: http://indatasv.blogspot.com

Conclusiones

Hoy día, las nuevas tecnologías de la información y la comunicación se están abriendo paso con fuerza y extendiendo su uso a cada vez más ámbitos de la sociedad. La seguridad pública no es ajena a esta expansión, pues aquellas se están implantando con el objetivo de garantizarla de forma más efectiva y eficiente. En Latinoamérica hay un incremento notable del despliegue del uso de nuevas tecnologías como la videovigilancia y el uso de drones en las ciudades, integrando sistemas de registro de grandes cantidades de datos personales, incluyendo los datos biométricos, que se ven alimentados por estas herramientas.

El uso de la tecnología, como los priorizados en el estudio, pueden implicar una amplia gama de herramientas efectivas para la prevención, investigación y sanción del delito, por lo que la utilización de estas pudiera llevar a resultados positivos en torno a las obligaciones estatales de garantizar la seguridad y reducir la impunidad. No obstante, el uso de estas requiere un fuerte compromiso de parte de los Estados con la transparencia, el respeto a la legalidad, la rendición de cuentas y la legislación participativa e integral, desde un enfoque de derechos humanos, para determinar los límites y la implementación de estas desde el respeto, la protección y la garantía de derechos.

Sobre las experiencias en Latinoamérica

El uso de drones se ha convertido en una apuesta de los Estados para la persecución del delito funcionando como elementos de vigilancia en zonas consideradas de alta peligrosidad, fronteras, entre otros espacios, sin embargo, estos dispositivos también se han utilizado para mantener la seguridad de diversos eventos públicos. Se utilizan dispositivos que trasmiten en tiempo real y permiten la identificación y el monitoreo diversos blancos en un radio amplio.
La necesidad de invertir en sistemas videovigilancia se mantiene latente en la región. Su instalación se ha concretado como resultado de las demandas ciudadanas frente al miedo de ser víctimas de algún delito por lo que solicitan a las instituciones de gobierno cámaras de videovigilancia y alarmas en sus comunidades. Además, el uso de estos sistemas permite generar bases de datos de información geográfica dentro de mapas digitales, así como para dar seguridad a instalaciones de las instituciones gubernamentales. También existen sistemas de videovigilancia que se articulan con alarmas fijas y móviles ubicadas en edificios y espacios públicos, puntos de amplia afluencia turística y plazas, con el objetivo de disminuir los niveles de hurto y robo de vehículos.

Los datos biométricos han sido utilizados a nivel regional a través de su obtención por medio de los sistemas de videovigilancia y por la generación de distintas bases de datos recolectados por instituciones estatales que albergan información personal de la pobla-

ción. Como para los demás tipos de tecnología estudiados, existen pocas regulaciones a nivel regional que eviten usos indiscriminados con la información de las poblaciones y sus afectaciones al ejercicio de derechos humanos.

Sobre su aplicación en seguridad pública

El Plan Control Territorial (PCT), principal política de seguridad del actual gobierno, busca colocar el uso de la tecnología como herramienta fundamental para la mejora de la efectividad y eficiencia institucional para la prevención y el abordaje del delito. Este Plan, declarado como información reservada por el Gobierno, no ha sido socializado hasta la fecha y solo han sido develadas cuatro de sus siete etapas por el presidente Nayib Bukele en algunas actividades públicas o a través de sus redes sociales. Su fase tres, denominada "Modernización", hace alusión a la necesidad de equipar a la Policía Nacional Civil y la Fuerza Armada de El Salvador de herramientas que les permitan desarrollar una mejor respuesta en el combate al delito. No obstante, la poca información obtenida sobre este equipamiento, a través de un documento de estudio de un préstamo otorgado por el Banco Centroamericano de Integración Económica, no permite conocer a profundidad las características de los equipos adquiridos, mucho menos da cuenta de las limitaciones establecidas por el Estado salvadoreño sobre su utilización en el abordaje de la criminalidad.

El uso de drones se ha transformado en un elemento clave para llevar a cabo estrategias de persecución del delito por parte de las autoridades encargadas, las cuales pretenden vigilar las zonas fronterizas y costeras, los puntos de reunión de grupos en conflicto con la ley y también monitorear movilizaciones ciudadanas.

Los gobiernos municipales han sido los pioneros en implementar sistemas de videovigilancia en El Salvador, ya sea como parte de su trabajo local o bien como parte de las acciones articuladas junto a la Policía Nacional Civil especificadas en los planes y/o políticas de seguridad. Sin embargo, la PNC también cuenta con centros de monitoreo de videovigilancia en distintos municipios, principalmente aquellos que han sido priorizados por sus altos índices de violencia y criminalidad. El MJSP prevé que se creará un Sistema Nacional de Videovigilancia como parte de las estrategias que complementarán al PCT en los próximos años.

A nivel general no existe un uso específico de los datos biométricos para el ámbito de la seguridad, pero las instituciones encargadas recurren a otras instancias estatales que recolectan y almacenan información de la población como el Viceministerio de Transporte, en Ministerio de Salud y el Registro Nacional de las Personas Naturales. Al igual que con los sistemas de videovigilancia, el MJSP prevé crear un Sistema Nacional de Datos Biométricos que permitirá articular formalmente a las instituciones y así dinamizar la generación de información sobre personas en conflicto con la ley ante la comisión de delitos.

La oferta de tecnología y modernización ante un ambiente de inseguridad y alta criminalidad ha llevado a condiciones de restricción de derechos humanos, lo cual puede ser contraproducente en un contexto de retroceso democrático y posibles abusos de poder, incluyendo abusos de las fuerzas de seguridad.

La vigilancia y el control, formal e informal, tiende a dirigirse a poblaciones estigmatizadas y criminalizadas, en el caso salvadoreño, hombres adolescentes y jóvenes de territorios marginalizados que han vivido una sistemática discriminación, la cual ha llevado a un ejercicio abusivo que ha implicado el uso excesivo de la fuerza, así como detenciones arbitrarias e ilegales, la criminalización y el cometimiento de ejecuciones extrajudiciales[97] y desapariciones forzadas.

La falta de transparencia de la principal política de seguridad del Gobierno impide a la sociedad contar con información suficiente sobre el tipo y el alcance del equipo que las instituciones estatales se encuentran adquiriendo en el país. Hasta la fecha, las instituciones responsables y obligadas no han brindado detalles técnicos del equipo que se está comprando por parte de la PNC y la FAES. En ese sentido, se vuelve pertinente la exigencia de transparentar la información necesaria y suficiente sobre el tipo de equipo y el uso que este permite en términos técnicos, así como su posible afectación a los derechos humanos.

Por otra parte, el fortalecimiento que esta fase contempla dar a la Fuerza Armada de El Salvador, se complementa con el anuncio de la implementación de la fase cuatro, llamada "Inmersión", que implica duplicar las fuerzas armadas de 20 mil efectivos a 40 mil, lo cual deja en evidencia el uso permanente e inconstitucional del ejército en tareas de seguridad pública.
La restricción y violación de derechos humanos en nombre de la seguridad ha sido una práctica frecuente en los países latinoamericanos, el uso de la tecnología para controlar y vigilar, sin regulación y limitaciones brinda un escenario altamente peligroso en cuanto al uso de la información recolectada en términos de persecución, chantaje y manipulación de actores incómodos al poder estatal. Esto, en un escenario de falta de independencia de las institución y ruptura del estado de derecho y controles estatales, como es el contexto actual salvadoreño, representa un ámbito más de desprotección de la población ante el ejercicio del poder del Estado.

La aplicación de drones y el sistema de videovigilancia 911 para vigilar y control protestas ciudadanas, como la realizada el pasado 17 de octubre en El Salvador, es solo una muestra del alcance de este tipo de equipamiento que, alegando posibles afectaciones a la

97 PDDH, *"Informe especial de la señora procuradora para la defensa de derechos humanos, Licenciada Raquel Caballero de Guevara, sobre las ejecuciones extralegales atribuidas a la Policía Nacional Civil en El Salvador, período 2014-2018"*, (San Salvador: 2019). PP. 141.

seguridad y el orden, son utilizadas para recoger información y vigilar manifestaciones sociales legítimas, pero contrarias al poder gubernamental.

Por otro lado, la adopción de la tecnología biométrica está aumentando rápidamente. Sin embargo, su aplicación conlleva de manera latente la preocupación respecto de la violación de la privacidad y los derechos de las personas. Entre los factores que se pueden incluir en este sentido se podría mencionar la posibilidad de fraude, robo de identidad, violaciones a la libertad de los individuos e inexactitud de los datos. Estos riesgos de error o violación de derechos podrían crear conflictos entre aquellos a cargo del tratamiento de los datos personales y los titulares de los datos, ya que, por ejemplo, podrían ser acusados de un delito o ser víctimas de discriminación de manera injusta y con base en evidencia biométrica equívoca.

Sobre la necesidad de regular su uso

El uso de la tecnología para mejorar el análisis de información delictiva, la efectividad de respuesta ante la misma y la judicialización de casos que requieren de evidencia certificada resulta pertinente en contextos con elevados índices delictivos como El Salvador. La tecnología y su utilización, en sí misma, no debiera representar un riesgo para los derechos fundamentales de la población, sino más bien, esta debiera servir como un medio para garantizar su pleno acceso y libre ejercicio; sin embargo, en el caso de El Salvador, la falta de regulación sobre el uso de estas herramientas, así como de mecanismos claros que definan límites de aplicación y garanticen derechos fundamentales como la privacidad, la intimidad y la autodeterminación informativa, entre otros, puede tener una afectación directa en la violación sistemática y descontrolada de derechos humanos de la población, principalmente, de la que ya se encuentra en situación de estigmatización y discriminación.

Las instituciones estatales no han sido capaces de construir y aplicar lineamientos procedimentales para el resguardo, la protección y la destrucción, de forma segura y bajo estrictas normas de confidencialidad, de la información recogida y almacenada por estas. Aun así, el Ministerio de Justicia y Seguridad Pública ha anunciado dentro de sus proyecciones la integración de sus sistemas de información con las generadas por el Registro Nacional de Personas Naturales y el Viceministerio de Transporte Terrestre, buscando crear un Sistema Nacional de Datos Biométricos.

La presidencia de la república ha vetado la propuesta de Ley de datos personales y habeas data aprobada en el mes de abril de 2021, manteniendo el vacío legal existente para la regulación del registro, utilización, almacenamiento y destrucción de información personal, incluyendo la imposibilidad de protección ante violaciones a derechos fundamentales. La modernización del Estado solo puede realizarse en el marco del respeto, protección y garantía de derechos humanos, por lo que cuando este marco normativo no

se garantiza el uso de la tecnología en seguridad pública representa un grave riesgo de profundizar la vulneración de derechos.

El uso de la tecnología en el ámbito de seguridad puede brindar resultados positivos en la medida en que esta se encuentra debidamente regulada, permite el análisis objetivo y científico de la información, busca limitar su utilización en función del respeto, la protección y la garantía de derechos fundamentales, mantiene mecanismos públicos y sistemáticos de rendición de cuentas y transparencia y permite orientarse a la mejora del comportamiento policial en el marco de legalidad.