IMPLEMENTACIÓN DE PLATAFORMA DE MEJORA DE LA SEGURIDAD URBANA CON CIENCIA DE DATOS, INTELIGENCIA ARTIFICIAL Y MACHINE LEARNING

JUAN CARLOS LÁZARO GUILLERMO
JOSÉ ALFREDO HERRERA QUISPE
ERNESTO DAVID CANCHO RODRIGUEZ
NIORBERTO ULISES ROMAN CONCHA
JESSY ISABEL VARGAS FLORES
JANETT DEISY JULCA FLORES

Depósito Legal: N° 2022-12312

ISBN: 978-612-49137-4-7

9 786124 913747

BRITISH LIBRARY HSITIRB

MAR CARIBE
EDITORIAL

Implementación de Plataforma de Mejora de la Seguridad Urbana con Ciencia de Datos, Inteligencia Artificial y Machine Learning

Juan Carlos Lázaro Guillermo, José Alfredo Herrera Quispe, Ernesto David Cancho Rodriguez, Norberto Ulises Roman Concha, Jessy Isabel Vargas Flores, Janett Deisy Julca Flores

Adaptado por: Ysaelen Odor Rossel

Compilador: Alcimar del Carmen García

Jefe de arte: Alcimar del Carmen García

Diseño de cubierta: Juan Carlos Lázaro Guillermo

Ilustraciones: Juan Carlos Lázaro Guillermo

Editado por: Editorial Mar Caribe de Josefrank Pernalete Lugo

Jr. Leoncio Prado, 1355 – Magdalena del Mar, Lima-Perú

RUC: 15605646601

Libro electrónico disponible en http://editorialmarcaribe.es/?page_id=265

Primera edición – diciembre 2022

Formato: electrónico

ISBN: 978-612-49137-4-7

Hecho el Depósito Legal en la Biblioteca Nacional del Perú N° 2022-12312

Contenido

Prólogo

El uso de la tecnología se ha convertido en un medio empleado por los gobiernos para garantizar la seguridad de los ciudadanos mediante el uso de diferentes innovaciones tecnológicas basadas en la inteligencia artificial. Cabe señalar que esta práctica se hace cada vez más común, y se espera que continúe aumentando en los próximos años. El Estado, está cada vez más inmerso en el empleo de las tecnologías disruptivas para garantizar la seguridad ciudadana.

Sin embargo, la relación entre la seguridad urbana y la tecnología no se encuentre libre de tensiones. Debido a que muchos ciudadanos ven vulnerados sus derechos individuales y colectivos con las propuestas en materia de seguridad hechas por el Estado. Mientras la IA artificial aplicada a la seguridad urbana apunta a la implementación de más mecanismos y medios para el control y combate de los delitos, con cámaras de seguridad, monitoreo de transeúntes y vehículos, geolocalización, etcétera. Los ciudadanos de las grandes metrópolis ven en estas tecnologías elementos invasivos y violatorios de la intimidad personal. Es decir, gran parte de la ciudadanía piensan que estas prácticas atentan contra los derechos a la privacidad y a no ser discriminados.

Empero, no se puede negar que el paisaje urbano ha cambiado radicalmente, en la actualidad es muy común observar la rápida proliferación de medios de seguridad basados en IA para el control de la inseguridad, ejemplo de ello son Londres, Nueva York, Chicago, y las grandes metrópolis de China. La contribución hecha por la tecnología para garantizar la seguridad es muy grande, en la actualidad los servicios de emergencia pueden detectar de una forma más precisa y rápida donde se presenta una situación irregular, y llegar hasta la ubicación en cuestión de minutos. El tiempo que puedan tardar en llegar las fuerzas del orden público, bomberos o paramédicos puede ser la diferencia entre la vida y la muerte.

En este aspecto, la planificación es fundamental en el diseño de la políticas pública, hechas para garantizar la seguridad urbana en concordancia con los derechos de los ciudadanos. Porque la correcta definición de las acciones que debe seguir la administración pública es parte integral de la gobernabilidad del país.

Al pensar en el diseño y planificación de sistemas de seguridad, estos deben ser parte de los programas de seguridad de todos los países de la región, porque

su uso es diario y constante, y los resultados muestran que este crecimiento continuará en los próximos años. La planificación debe centrarse en iniciativas que promuevan el desarrollo de políticas públicas de videovigilancia en interés de la seguridad ciudadana, que a nivel local permitan una estrategia nacional, como la propuesta de Perú de crear un centro nacional de videovigilancia, o incluso una propuesta internacional, como la Carta para el Uso Democrático de la Videovigilancia publicada por el Foro Europeo de Seguridad Urbana, donde los gobiernos latinoamericanos lideran por consenso el uso, regulación y cooperación del tema.

En esta obra se enfoca la seguridad urbana desde el punto de vista de aplicación de tecnologías basadas en inteligencia artificial para una ciudad como Lima metropolitana. En los primeros capítulos se define algunos conceptos relacionados con la inseguridad y sus estadísticas históricas y actuales tanto en Perú como en Lima metropolitana, posteriormente se establecen consideraciones sobre la inteligencia artificial, sus orígenes y aplicabilidad en diferentes contextos internacionales y nacionales. En la última parte de la obra se instauran propuestas sobre el uso de la tecnología al servicio de la seguridad urbana en Lima, así como también se tocan los aspectos legales que debe regir al momento de implementar estos medios tecnológicos en la sociedad.

Capítulo 1

1.1. América Latina: Violencia urbana.

Según la organización mundial de la salud (1999), a finales del siglo XX la violencia ha sido la primera causa de muerte en Latinoamérica entre los individuos de 15 y 44 años. El Salvador, un diminuto territorio que venía de conseguir unos convenios de pacificación que pusieron fin a una guerra interna bastante cruenta, vio incrementar la tasa de asesinatos de 72 a 139 asesinatos por cada cien mil pobladores entre 1990 y 1995 (Cruz, Trigueros y González, 2000) o sea, comenzaron a registrarse más muertes en la tranquilidad del bienestar que en las tormentas de la guerra: una forma de vida urbana violenta había hecho su aparición en Latinoamérica.

Este carácter novedoso del fenómeno de la violencia, tanto por sus dimensiones como por las singularidades de los procesos sociales que ahí se hallan relacionados, es lo que aspira plasmar este libro, así como las alternativas que pueden contribuir a su control en los grandes centros urbanos de Latinoamérica.

> La violencia no fue ajena a los procesos de cotidianidad o transformación social de Latinoamérica: violenta ha sido la conquista, agresivo el esclavismo, violenta la libertad, violentos los procesos de apropiación de las tierras y de expropiación de los excedentes.

Sin embargo, actualmente hablamos de un proceso diferente, singular, y que tiene relación con la violencia delincuencial y urbana. Ciertamente la violencia

política ha estado presente en la zona: la represión militar de los gobiernos dictatoriales del Cono Sur o Centroamérica; los conflictos guerrilleros actuales en Perú, Colombia o México; el clásico actuar de los "coroneles", los señores de la tierra del nordeste brasileños o las actividades de los paramilitares en Urabá, Colombia, son una muestra fehaciente de eso.

Un maltrato que tenemos la posibilidad de calificar de social, por manifestar conflictos sociales y económicos; pero no político, puesto que no posee una vocación de poder. Una forma de maltrato que no posee su campo de acción únicamente en las regiones rurales, sino que también se encuentra en las metrópolis y, más que nada, en las regiones pobres, segregadas y excluidas de los grandes centro urbanos. Los crímenes violentos se incrementan tanto en esos territorios como en aquellos donde hay bajas tasas de asesinatos –Costa Rica o Argentina– o como aquellos en donde ya las tasas eran muy elevadas –Colombia o El Salvador.

1.2. Pobreza

Un rasgo bastante relevante de la nueva forma de violencia urbana es que se encuentra principalmente entre los que poseen poco dinero de los grandes centros urbanos. La clase media y los sectores adinerados ven a los que tienen poco dinero como una amenaza, y se sienten a sí mismos como las víctimas de las agresiones y delitos.

> Desde luego que la clase media sufre la delincuencia; no obstante, quienes realmente sufren la violencia, y en especial la violencia más fuerte o letal, son los que tienen poco dinero, víctimas y victimarios en este proceso. Es una violencia de pobres contra pobres.

Se puede pensar, desde esta cruda realidad, que la pobreza es la causa de la violencia. No obstante, no hay una correlación clara entre estas dos situaciones, puesto que las naciones más pobres de Latinoamérica, como los casos de Haití, Bolivia o Perú, no aparecen entre esos que tienen o exhiben altas tasas de asesinatos. Y lo mismo pasa en el interior de las naciones: las grandes tasas de inseguridad y violencia entre los brasileños no se encuentra en los que tienen poco dinero en los estados del nordeste, sino en los ricos y cosmopolitas estados de Sao Paulo y Rio de Janeiro.

En Venezuela los asesinatos ocurren en la zona metropolitana de Caracas y en los estados de Carabobo y Aragua y no en las entidades pobres con más grandes necesidades primordiales insatisfechas, como Apure, Trujillo o Sucre. Frente a este surge una premisa: es el empobrecimiento y la diferencia, y no la pobreza, lo que origina la violencia urbana que estamos presenciando. Según las estadísticas de la CEPAL, el empobrecimiento es la causa que para año el 1998, en trece de dieciocho países de Latinoamérica el sueldo mínimo fuera inferior al de 1980, y que el número total de pobres superase los 220 millones de individuos.

1.3. Exclusión escolar y laboral

Los estudios actuales del Banco Mundial toman como medida de la pobreza el umbral de un dólar por persona por día (para lo que se estima el dólar con paridad de poder de compra a costos de 1985), según dichos cálculos el 24% de los Latinoamericanos y el caribeños, (1 de cada 4), vive con menos de un dólar por día. Y en ciertos territorios, como Guatemala, más de la mitad de los habitantes está en dicha situación. Esto crea una situación creciente de exclusión entre la población, empero esa exclusión se observa especialmente en el trabajo y en la enseñanza. Conforme con la Comisión Económica para América Latina y el Caribe, el desempleo en la zona pasó de 5,7% en 1990 a 9,5% en 1999. Llama la atención, que no es únicamente el crecimiento de los desocupados, sino la particularidad de los nuevos trabajos, puesto que de cada 10 empleos entre el 1990 y 1997, siete de ellos se correspondían al área informal.

En América Latina y el Caribe, el desempleo pasó de 5,7% en 1990 a 9,5% en 1999.

En la educación, la situación no es más halagadora. Se calcula que el 30% de los chicos no había completado la enseñanza primaria a los 14 años. Y se ven forzados a buscar empleo en el precario mercado laboral, puesto que sus padres no tienen la posibilidad de seguir cubriendo sus crecientes necesidades de consumo, por lo tanto, también tienen que contribuir con el mantenimiento del núcleo familiar.

Se estima que de cada cien chicos que ingresan al primer nivel del colegio en Bolivia, Brasil, Colombia o Perú, solamente quince llegan al noveno nivel de estudios. El caso es todavía peor en otros territorios como Guatemala, Haití o República Dominicana, donde de los mismos cien estudiantes solamente 6 alcanzan a completar la educación primaria. En Caracas, Venezuela, el 27% de los adolescentes masculinos entre 15 y 18 años ni labora ni estudia.

1.4. Expectativas rotas

Uno de los aspectos significativos de la violencia urbana, según las tesis de la sociología de la modernización, es que la violencia no se encuentra presente entre los inmigrantes llegados a las metrópolis desde el campo. La violencia aparece en la segunda o tercera generación urbana, en individuos que nacieron en las metrópolis y que habían perdido toda relación con su pasado rural. Es de pensar

que la explicación radica en la insatisfacción de las expectativas creadas en las generaciones pobres que han nacido en las metrópolis.

En ésta cuestión se encuentran presentes dos elementos: Por un lado, está el proceso de logro de las pretensiones que tuvo la primera generación, y en ciertos países inclusive la segunda. Para las familias que venían del campo, lo urbano representaba un grupo de beneficios relevantes que no podían obtener en sus sitios de procedencia: en la urbe podían tener acceso a servicios sanitarios cercanos, el colegio para los hijos, agua potable en la vivienda o alrededor de ella, la electricidad, y con ello una refrigeradora y un televisor; en fin, varias situaciones que implicaban, en su precariedad, un cambio fundamental en la calidad de vida.

Es de resaltar que en Latinoamérica este proceso migratorio, denominado "éxodo rural-urbano", coincidió con una fase de extensión del capitalismo y mejoría de las condiciones sociales de la economía mundial. Aunque en ciertos partes el aceleramiento del proceso de urbanización ha sido sostenido por las exportaciones durante la segunda guerra mundial, y en los años cincuenta el aumento del desplazamiento migratorio delineó aquel nuevo fenómeno urbano que conforman las favelas, villas miseria, comunas o pueblos, y que la sociología denominó marginalidad, asentamientos urbanos no planificados o sobrepoblación relativa.

Empero las personas que nacen en la urbe no descubren nada novedoso en la electricidad, la televisión, los nosocomios o las escuelas. Sin embargo, sus pretensiones son otras. Es aquí donde se encuentra el segundo aspecto de la sociedad contemporánea que queremos resaltar: la homogenización e inflación de las expectativas.

La existencia de los medios de comunicación, y más que nada de la televisión, ponen a las personas de los más diversos niveles sociales y capacidad adquisitiva, en contacto con un grupo de bienes, servicios y estilos de vida que no podían conocer o imaginarse.

Los medios de comunicación y la publicidad han democratizado la información sobre los productos y servicios que ofertan los mercados, y con ello hicieron que aumenten las expectativas en la población.

Por lo tanto, todos tienen la posibilidad de desear el mismo tipo de camisa, la misma marca de zapatos y el mismo modelo de coche, empero no todos poseen la capacidad de comprarlos. Puesto que una gran proporción permanecen desempleados o ganan sueldos mensuales que son inferiores al precio de los zapatos de moda. En el proceso de homogeneización e inflación de las expectativas de la segunda o tercera generación urbana, se estancan las de generar mayores ingresos económicos y las de mejoría social, generando un abismo entre lo que se aspira como calidad de vida y posibilidad real de alcanzarla.

Este choque, que se crea entre las expectativas y la imposibilidad de satisfacerlas por los medios prescritos por la sociedad y la ley, propician la violencia. Incentivando el delito como un medio de obtener por la fuerza lo que no es posible de conseguir por las vías formales. En este entorno el tráfico de drogas y el hurto de carros se transforman en los medios proscritos predilectos, por las altísimas ganancias que reportan, que posibilita saciar las expectativas y enseñar hasta con vulgaridad los símbolos de triunfo y riqueza sin tener muchas más herramientas que las armas de la violencia.

1.5. Armas de fuego en Latinoamérica

Durante las últimas dos décadas, la proliferación de armas de fuego ligeras entre la población latinoamericana ha sido impresionante. Algunos países tienen un mercado libre de armas, otros tienen más restricciones, pero muchas armas en manos de la guerrilla son transferidas a usuarios particulares y delincuentes comunes. Los narcotraficantes también son responsables de proporcionar armas a sus traficantes como parte de pago y como medio de protección del territorio. Los ciudadanos honestos también deciden armarse para defender su propiedad y su familia, y aunque las cifras reales son difíciles de obtener, se tiene que:

> El 23% de los residentes de Cali y San José de Costa Rica, y el 28% de Santiago de Chile posee armas de fuego.

El mercado de armas es muy complicado y está relacionado con el comercio y la industria que tiene muchos efectos en la sociedad y los negocios. Los países europeos con controles de armas más estrictos entre sus ciudadanos se han negado a controlar la exportación armas a otros países. Se supone que deben venderlos a empresas "serias", pero luego terminan en el mercado negro de armas mundial, y en las etapas finales involucran a la policía o los ejércitos locales, que se convierten en los principales contrabandistas de armas. Al fin y al cabo, el que quiera puede comprar un arma para delinquir o defenderse, y el que no puede comprarla, puede alquilarla para el fin de semana.

Lo que caracteriza a la violencia América Latina, así como de los Estados Unidos de América y el mundo contemporáneo, no es la existencia de varios crímenes o conflictos interpersonales, sino la mortalidad implícita en la violencia. Es decir, el nivel de agresividad es mayor, con el resultado de más víctimas mortales. La letalidad está básicamente muy relacionada con las armas de fuego, ya que es más fácil de matar con ellas, que con un arma blanca.

Según la Organización Mundial de la Salud, el 63 por ciento de todos los homicidios en el mundo son causados por armas de fuego, pero en América Latina esa cifra es mucho mayor, más del 80 por ciento. Además de su función utilitaria, el arma también tiene importantes funciones simbólicas, refleja la masculinidad y el coraje en los jóvenes. Es importante señalar que casi el 90 por ciento de las víctimas de homicidio son hombres. Los hombres juegan un papel audaz y valiente en la construcción de una cultura de masculinidad, mientras que evitar el conflicto se identifica claramente como un rasgo femenino y no debe ser imitado por nadie puesto que se considera una actitud femenina.

Se atribuye gran parte de la violencia urbana a estas dimensiones culturales de la masculinidad. Esto se hace aún más evidente en los adolescentes que están en la fase de definición de su identidad y por lo tanto son más vulnerables a este valor, ya que deben demostrar sistemáticamente que ya no son niños sino hombres, incluso a costa de su propia vida.

1.6. Costos económicos de la violencia

El aumento de los homicidios y los delitos contra la propiedad ha creado un temor generalizado entre las ciudades de América Latina. Si hay algo que tienen en común los habitantes de distintas metrópolis es el miedo a ser objeto de violencia. La encuesta de Latinobarómetro muestra que en promedio el 30 por ciento de los hogares de la región, han sido asaltados en los 12 meses anteriores a la encuesta.

Los resultados muestran cifras alarmantes en países como Guatemala, México y El Salvador, donde más de 50% de los hogares ha sido víctimas de algún delito. Otros países como Argentina (34,2%), Bolivia (32,8%), Costa Rica (32,7%) o Chile (32,0%), acercándose a la media. Sólo Panamá (25,1%) y Uruguay (21,4%)

tenían las tasas de victimización más bajas, y aun así uno de cada cuatro o cinco hogares han sido objeto de asaltos.

No obstante, el temor a ser víctima es mayor, que el porcentaje de las de las víctimas reales. El 30% de las personas violentadas cuentan sus experiencias a vecinos y amigos, que se sienten víctimas potenciales. Por ejemplo, aproximadamente el 24% de los ciudadanos en Río de Janeiro, el 26% en Santiago de Chile y el 46% en California restringieron las salidas nocturnas por temor a ser víctimas de la violencia.

Por la misma razón, en Caracas, alrededor del 33 por ciento limitan las horas de estudio o trabajo vespertino. El mismo miedo se apodera de la población en ciudades más seguras como Buenos Aires o Montevideo, u otros centros urbanos con menos población y violencia, pero en cambio, por la influencia de los medios, viven los hechos de otras ciudades. Y tienden a experimentar un miedo mayor del que objetivamente les corresponde de ser víctima en el lugar donde viven.

Esta sensación de miedo tiene un enorme impacto económico en la sociedad y se suma al daño significativo que la violencia y el crimen han hecho a la sociedad. A los costes directos ya asociados a los daños a la salud pública y a los bienes, hay que sumar los costes que tuvieron que pagar los hogares y las empresas para protegerse y los costes indirectos asociados a las restricciones que impone el crimen a la actividad económica.

El costo económico directo de la violencia es del 11,4% del producto interno bruto (PIB) en Colombia y del 6,9% en El Salvador, pero estos costos directos también son significativos en Venezuela con un 6,9% y un 4,9% en México, 3,3% en Brasil y 2,9% Perú. De todos estos países, Perú tiene la tasa más baja, y aun así supera el porcentaje anual del PBI requerido para el desarrollo tecnológico.

Cuando se incluyen los costos indirectos, en algunos países estas cifras se elevaron significativamente, alcanzando el 24,9% del PIB en El Salvador, Colombia 24%, México 12,3%, Venezuela 11,8%, Brasil 10,5% y 5,1% del PIB en Perú. Según el Banco Interamericano de Desarrollo, las pérdidas y transferencias de recursos en la región debido a la violencia ascendieron al 14,2% del PIB, equivalente a US$168 mil millones. Así, además del costo psicológico por el dolor y el sufrimiento de la víctima, la violencia tiene un impacto económico medible, en las medidas preventivas, de protección y seguridad.

1.7. La justicia

La nueva violencia urbana plantea importantes desafíos al sistema de justicia penal debido a la singularidad del fenómeno que describimos. Por supuesto, como escribió Durkheim (1978), el crimen es normal en la sociedad. Esto significa que es normal seguir las reglas al igual que es normal esperar que alguien las rompa.

El problema del sistema penal es que el control social que cabría esperar sólo puede ser efectivo si el número de delincuentes es pequeño, pero se vuelve bastante ineficaz cuando aumenta a las escalas que hemos visto en la nueva violencia urbana. Entonces el sistema sancionador se enfrenta a una especie de doble dificultad. Por un lado, carece de la capacidad para llevar a cabo sus propias tareas: la cantidad y diversidad de delincuentes la ha vuelto ineficaz en muchos países.

El castigo ha perdido la función disuasoria que debería haber tenido, porque la frecuencia de aplicación es demasiado baja, y porque el poder simbólico que la ley debería tener ya no existe. Si en el mundo se sabe que el sistema penal castiga solo a una pequeña parte de los delincuentes, entonces en las nuevas condiciones del crimen, esto reviste mucha gravedad.

En Colombia, en la década de 1960, se juzgaba el 35% de los asesinatos cometidos. En la década de 1990, este porcentaje se redujo al 6%. Se estima que en Cali sólo el 5% de los asesinatos son enjuiciados, sin embargo, el juicio no significa que el delincuente haya sido condenado, pues en este caso el porcentaje sería menor. Todo esto produce la sensación de que, los castigos son pocos y demasiado tardíos.

Por otro lado, incluso suponiendo que la justicia pueda ser eficaz para enjuiciar y condenar a los delincuentes, quedan fuertes interrogantes sobre qué función social desempeñará. En otras palabras, ¿el sistema penal y las prisiones pueden contribuir a reducir la violencia? No parece haber una respuesta clara a esta pregunta. Las cárceles se han convertido en lugares muy peligrosos, y es de suponer que deberían ser los lugares más seguros. Para dar un ejemplo: en Venezuela, la tasa de homicidios en las cárceles es mucho más alta que en el resto de la sociedad. Parece haber un consenso generalizado de que las prisiones se han convertido en fábricas de violencia cotidiana y no cumplen su función donde las

personas luego de cometer un delito, deben ser objetos de intervenciones de manera que logren reintegrarse a la sociedad.

1.8. Investigación abierta

Lo puntos descritos brevemente son temas candentes, pero no los únicos, del estudio de la violencia y la sociedad. Es necesario formular propuestas de investigación que respondan al desafío de la nueva realidad latinoamericana. Se necesitan estudios diversos y variados, tanto sobre los temas a considerar como sobre las metodologías que se pueden utilizar.

Necesitamos estadísticas mucho mejores sobre el fenómeno, es necesario medir en detalle qué está pasando y dónde está pasando. Pero, al mismo tiempo, existe la necesidad de comprender mejor los procesos sociales. Se deben tomar en cuenta las opiniones de los diferentes actores: las víctimas, los delincuentes, la policía.

Se necesita más investigación sobre el aparato policial y el sistema penal, de manera que logre adecuarse a la sociedad contemporánea. Y todo esto hay que verlo desde una perspectiva interdisciplinar. Si la violencia es un fenómeno multicausal, debemos tratar de verla desde diferentes ángulos y con otros ojos. Tenemos que acercar la criminología y la epidemiología, tenemos que asegurarnos de que los geógrafos nos den buenos mapas, y con los economistas podemos ser más precisos sobre la violencia y los costos de controlarla, los costos de las cárceles, y la sociología nos puede ayudar a ver si la sociedad está dispuesta a pagar esa factura.

Capítulo 2

2.1. Antecedentes: La inseguridad en Perú

La inseguridad provocada por la violencia y el crimen no es un problema nuevo en la sociedad peruana. Durante la última década, el Perú sufrió los efectos de hechos subversivos muy violentos que mataron a casi 30.000 personas y provocaron pérdidas materiales por aproximadamente 25 mil millones de dólares. Cuando en 1992 fue capturado el líder de Sendero Luminoso Abimael Guzmán, que inició la rápida derrota de la organización terrorista más importante del Perú, todo hizo suponer que el sensible escenario anterior había sido finalmente derrotado.

Sin embargo, la reducción de la violencia política, desde el punto de vista de la seguridad nacional hizo posible un fenómeno que se desarrolló hace años: la violencia criminal, presentando nuevos desafíos a la política de seguridad del país. El daño que causa la delincuencia es grande en comparación con el tamaño de la economía peruana, pero, por otro lado, crea un ambiente de desconfianza, que es muy perjudicial para el orden social.

La delincuencia general es un fenómeno muy complejo que no responde a criterios organizativos ni a estrategias específicas, pero el panorama de inseguridad en el Perú incluye otros factores importantes en su composición. El narcotráfico es uno de ellos. Durante la última década, esta actividad ilegal ha sufrido una "transformación" debido a las fluctuaciones internacionales en el precio de las drogas y las políticas de prohibición implementadas en la región latinoamericana El resultado hasta el momento ha sido la reducción de las áreas de cultivo de coca y, por otro lado, que el Perú dejará de ser el único productor de la materia prima y pasará a ser el productor final de clorhidrato de cocaína.

Una de las consecuencias de estos cambios en el narcotráfico es el crecimiento explosivo del consumo de estas sustancias en el país, especialmente en los mercados urbanos. Por otro lado, las violaciones a los derechos humanos también deben ser consideradas como un factor importante que afecta la seguridad nacional. Si bien se reconoce internacionalmente que el Perú ha logrado avances significativos en esta área durante los últimos años, es claro que persisten problemas serios. Junto a estas manifestaciones ilegales, existen actos de violencia que amenazan la seguridad de los ciudadanos.

Los más conocidos son la violencia doméstica contra mujeres y niños y, por otro lado, los accidentes de tráfico. En ambos casos, se muestra un rápido aumento de casos en el Perú, lo cual es muy ilustrativo para medir el deterioro de las condiciones de vida, sin duda son síntomas de graves problemas arraigados en la sociedad.

La otra cara del problema es la incapacidad institucional para hacer frente a esta realidad. Es un hecho que la policía peruana está en una profunda crisis, por lo que los agentes pueden ser parte del problema, considerando los agentes involucrados en delitos. También otros organismos públicos relacionados con la seguridad pública, como el Poder Judicial y el Buró Penal, atienden sus propias crisis, que resultan perjudiciales para las condiciones actuales del país.

La inacción del Estado ha llevado a la sociedad a optar por formas de protección, que organizados por los municipios de la ciudad de Lima metropolitana son bastante espontáneas y sin control institucional. Estas iniciativas sociales no solo son onerosas e ineficaces, sino también peligrosas y contraproducentes para reducir la inseguridad. En áreas urbanas marginales, por ejemplo, el linchamiento de delincuentes es cada vez más común. De esta forma, la seguridad se ha convertido en un aspecto clave de la agenda que se desarrolla en el Perú. El público se siente más vulnerable al crimen, los comerciantes están preocupados por los altos costos de la seguridad y las autoridades están tratando de desarrollar estrategias apropiadas para enfrentar el problema urgente.

2.2. Consideraciones sobre el índice de inseguridad

El índice de inseguridad para Perú tiene un valor aproximado, no absoluto ni final. Su contribución se encuentra en la posibilidad de hacer seguimiento a las tendencias y comparación de fenómenos complejos como la violencia y el crimen. Esto se debe a que, por un lado, estos fenómenos involucran aspectos cualitativos que son difíciles de observar estadísticamente. Y, por otro lado, las estadísticas existentes presentan diversas limitaciones: una de las más comunes es una subestimación más o menos significativa de los delitos o actos de violencia que contienen estas estadísticas por diversas razones.

Por lo tanto, si consideramos que los índices compilados ayudan a identificar las tendencias generales y la situación relativa de los distintos departamentos peruanos en materia de inseguridad. Estos se podrían fortalecer,

mejorando la calidad de las estadísticas existentes, para acceder a la información proporcionada por fuentes oficiales, de una forma más precisa, y obtener una mejor percepción de la población.

La evaluación de la inseguridad en el Perú debe considerar las siguientes variables:

Delitos contra la vida,

La integridad física y la salud,

Delitos contra la propiedad,

Violaciones de los derechos humanos,

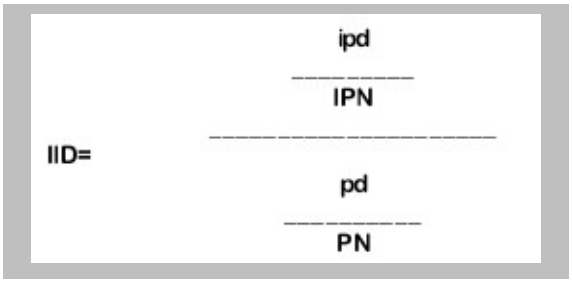
Narcotráfico,

Terrorismo,

Accidentes de tránsito y

Consumo de drogas

Los índices de inseguridad se construyen comparando las operaciones policiales de cada departamento con sus incidentes totales en todo el país. La fórmula como se obtienen los índices es la siguiente:



ipd = intervenciones policiales en el departamento

IPN = intervenciones policiales a nivel nacional

Pd = población departamental

PN = población nacional

IDD = índice de inseguridad departamental

De esta forma, el índice de inseguridad para la variable de delincuencia se obtiene dividiendo la proporción de delitos del barrio entre los delitos estatales por la proporción de la población, este número se multiplica por la gravedad de cada tipo de delito. El índice de inseguridad total de un departamento se obtiene de sumando los índices de inseguridad para cada tipo de delito. El puntaje de cada departamento se multiplica por un factor de corrección arbitrario de 0.6, resultando números entre 1 y 0. El índice de inseguridad nacional total del año se obtiene promediando los índices de inseguridad de los 25 departamentos.

Tabla 2.1.

Ponderación de la gravedad de los delitos.

Variable delictiva	Peso
Delitos contra la vida,el cuerpo y la salud	0.3
Delitos contra el patrimonio	0.2
Violaciones de DD.HH.	0.2
Narcotráfico	0.1
Terrorismo	0.08
Accidentes de tránsito	0.05
Consumo de drogas	0.05
Amenazas de otros Estados	0.02

Fuente: Reyna (1999).

2.3. Estadísticas delictivas de Perú: siglo XX

Con un promedio no mayor a 1, el índice de inseguridad para Perú en la última década de siglo XX, es de 0,41, el puntaje más alto se presentó el año 1995 cuando registró 0,50, y el nivel más bajo fue de 0,3 para el año 1999. En términos generales, no hubo una variación significativa de un año a otro hasta 1994, pero en 1995 se presenta un aumento en los índices de inseguridad.

Cuestión de ejemplificar por niveles la inseguridad, en el país se establecen 4 grupos para comparar:

- El primer grupo sería de "máxima inseguridad" y presentó índices superiores a 0,8.
- En el segundo, la "inseguridad media alta" oscila entre 0,5 y 0,8.
- El tercero lo llamamos "inseguridad media baja" y sus índices varían de 0,2 a 0,5.
- El cuarto grupo es de "inseguridad baja" y tiene índices por debajo de 0,2.

En el primer grupo se encuentra el departamento de Lima, representa al 28% de los habitantes del país.

El segundo grupo comprende los departamentos de Junín, Ayacucho, Amazonas, Tacna, Arequipa y Callao. Representan el 16% del país y tiene el 17% de la población.

Para el tercer grupo tenemos los siguientes departamentos en orden descendente: Lambayeque, La Libertad, San Martín, Ica, Apurímac, Tumbes, Huánuco, Ancash, Ucayali, Moquegua, Pasco, Huancavelica, Madre, Cusco, Madre de Dios, Piura y Puno. Juntos, conforman el 50% de la superficie del país y el 46% de la población.

En el cuarto grupo se encuentran los departamentos de Loreto y Cajamarca. Representa el 31% del Perú y el 9% de la población.

.

2.3.1. Delitos contra la vida

Esta variable incluye asesinatos, abortos, lesiones y otros (amenazas abandono de personas, genocidio, etc.). Este fue considerado el principal tipo de la inseguridad, por lo que tiene una severidad de 0,3. El puntaje de incertidumbre promedio para este conjunto entre 1990 y 1996 es 0,26, los puntajes más altos en 1995 y 1996 (ambos 0,27) y los más bajos en 1994 (0,22).

Por lo que se puede apreciar, no existe una variación significativa de un año a otro. Los promedios quinquenales muestran que los departamentos de Lambayeque (0,52) y Amazonas (0,50) son los de mayor incidencia relativa este tipo de delitos. Entre los dos suman una sexta parte de la población del país.

De igual forma, el siguiente grupo sería Arequipa, Callao, Lima y Tacna, que están entre 0,4 y 0,5. En todos ellos existe una alta incidencia promedio de este tipo de delitos, involucrando al 37% de la población del país. Por encima de la media nacional, es decir, entre 0,2 y 0,3 estarían los departamentos de Junín, La Libertad, Moquegua, Ica, Cusco, Madre de Dios, Tumbes y Ancash. Juntos, constituyen el 24% por ciento de la población.

Los departamentos que reportan una baja incidencia de este tipo de delitos promedian entre 0.0 y 0.2. Son San Martín, Piura, Huánuco, Apurímac, Ucayali, Puno, Pasco, Ayacucho, Cajamarca, Loreto y Huancavelica. Todos ellos conforman el 33% de la población del Perú.

2.3.2. Delitos patrimoniales

Estos incluyen hurto, malversación, fraude, engaño y otros (chantaje, daños, etc.). El peso de severidad dado a esta variable es de 0,2. El índice para los años 1990-1996 es 0,14. A diferencia de otros índices, muestra un aumento pequeño pero continuo. Así, el promedio de es 0,13 en 1990, es 0,1 en 1991, 1992 y 1993 y 0,15 en 1994, 1995 y 1996.

A nivel departamental, Lima, Callao y Arequipa lideran el ranking con índices de 0,37, 0,3 y 0,33. Esta incidencia excede el promedio nacional, involucrando al 36% de la población. Otro grupo, también por encima del promedio nacional, serían los departamentos de Tacna (0,28), La Libertad (0,21), Ica (0,21), Tumbes (0,18), Moquegua (0,17), Lambayeque (0,17), Junín (0,15) y Ancash (0,15), representando el 24% de la población.

En el promedio nacional se encuentran Amazonas (0,1), Ucayali (0,12) y Cusco (0,11), estos departamentos tienen el 8% de la población. Por debajo del promedio nacional se encuentran Huánuco (0,09), Madre de Dios (0,08), Piura (0,08), Loreto (0,07), San Martín (0,07), Puno (0,06), Pasco (0,06) y Ayacucho. (0,04), Apurímac (0,04), Cajamarca (0,03) y Huancavelica (0,01), representan 32% de la población total.

2.3.4. Violación de derechos humanos

A diferencia de los demás ítems, es el único que mide la inseguridad ciudadana provocada por el Estado. Abarca los siguientes aspectos:

- Demanda de garantías individuales,
- Muerte,
- Detención,
- Abuso de poder,
- Situación jurídica,

.

Tienen un peso de 0,2. La media es de 0,13, en 1990, el promedio es 0.1, disminuye a 0,12 en 1991, aumenta a 0,15 en 1992, disminuye a 0,14 en 1993 y aumenta nuevamente a 0,15 en el1994. En 1995 el índice era de 0,11 y en 1996 bajó a 0,08. Una característica de esta variable es la aparente concentración de sus frecuencias en algunos departamentos. Así, Ayacucho (0,51), Apurímac (0,6), Lima (0,3), Junín (0.35) y Huancavelica (0.25) constituyen el grupo con mayor frecuencia.

Esto quiere decir que 39% de la población del Perú se encuentra en un entorno con violaciones de los derechos humanos. El segundo grupo está formado por aquellos departamentos ubicados en el promedio del país. Son Huánuco (0,16), Pasco (0,1), Amazonas (0,13) y San Martín (0,17). Juntos, tienen el 8% de la población del Perú. Debemos considerar que el índice más alto de este conjunto es 0,10 alcanzado por Ancash. También es importante señalar que cuatro de los departamentos (Tumbes, Tacna, Madre de Dios y Moquegua) presentan un índice de 0.

2.3.4. Tráfico de estupefacientes

Todos los operativos policiales realizados en 1993, 1995 y 1996 incluyen esta variable. Recibe un promedio de severidad de 0,1 siendo el índice promedio nacional de 0,11. Los departamentos con los índices más altos son Tumbes (0,41) y Ucayali (0,28), le siguen San Martín (0,25), Tacna (0,25), Amazonas (0,22), Huánuco (0,20), Loreto (0,19), Ayacucho (0,12) y Lima (0,12). Todos ellos conforman el 5 por ciento de la población del país.

En el promedio nacional se encuentran Madre de Dios (0,11), La Libertad (0,11), Lambayeque (0,09), Piura (0,08), Pasco (0,08) e Ica (0,06), conformando el 20 por ciento de la población del Perú. Por debajo de la tasa promedio se encuentran Cusco (0,05), Ancash (0,05), Junín (0,04), Callao (0,03), Arequipa (0,02), Puno (0,02), Cajamarca (0,02) y Moquegua (0,02). También Huancavelica y Apurímac, ambos con índice 0 en esta región.

Tales cifras no son un fiel reflejo de lo que en realidad está sucediendo y probablemente, esto se debe, a la falta de registros. La policía parece ejecutar más acciones en las puertas de salida de las drogas que en sus sitios de producción. Por lo tanto, lugares como Tumbes, Tacna y Callao (es decir, zonas fronterizas y de envío) son los locaciones con los índices más altos, sin embargo, las áreas de producción, ya sea Huánuco, Ayacucho y en cierta medida Cusco, no se encuentren entre los departamentos donde la policía realice las mayorías de las intervenciones.

2.3.5. Terrorismo

Las estadísticas son actividades subversivas registradas por la policía en los años 1990-1996. Hay que tener en cuenta que en este caso la información sobre el Callao está recogida en los datos de Lima. El peso de gravedad asignado es 0,08. Los índices medios anuales reflejan que, a principios de la década el terrorismo amenazaba gran parte del territorio del país, pero desde 1994 se ha concentrado en departamentos con baja densidad poblacional, resultando en índices relativos elevados sobre la media anual.

Del efecto estadístico creado por el fenómeno del terrorismo, se puede concluir que el índice promedio para los años 1990-1996 es de 0,06. Muchos departamentos están claramente por encima de la media nacional, son; Ayacucho (0,21), San Martín (0,19), Huancavelica (0,16), Junín (0,15), Pasco (0,13) y Lima-Callao (0,09). Todos ellos conforman el 44% de la población del Perú.

El promedio nacional incluye Ucayali (0,06), Ancash (0,06), Puno (0,05), La Libertad (0,05) y Apurímac (0,04). Constituyen el 18% de la población del país. El resto entre 0,04 y 0 se ubica así: Amazonas (0,03), Cusco (0,03), Piura (0,03), Lambayeque (0,03), Cajamarca (0,02), Ica (0,02), Arequipa (0,02), Tacna (0,02). 0,02), Loreto (0,01), Tumbes (0,01), Moquegua (0,01) y Madre de Dios (0,00).

2.3.6. Consumo de drogas

Las actividades policiales, se realizan por departamento solo para los años 1993, 1995 y 1996. Esta variable recibe un peso de severidad de 0,05. El promedio nacional resultante es 0,03. Los departamentos de Lima y La Libertad encabezan la lista con índices de 0,09 y 0,08, le siguen Tumbes (0,07), Ica (0,06) y Lambayeque (0,06). Estos departamentos tienen la mayor prevalencia de drogadicción, y conforman 24% de los habitantes del país.

Luego se tienen una banda de 0.05 y 0.3 que incluye Tacna (0.05), Ucayali (0.05), Huánuco (0.04), Loreto (0.04), Piura (0.03) y Junín (0.03), están dentro de la media nacional y cubren el 20% de la población. Del 0,02 al 0,00 están San Martín (0,02), Ancash (0,02), Cajamarca (0,02), Amazonas (0,02), Pasco (0,01), Moquegua (0,01), Madre de Dios (0,01), Puno (0,01), Cusco (0,01) y Callao (0,01). También Huancavelica, Apurímac, Arequipa y Ayacucho, todas con un índice de 0.00.

2.3.7. Accidentes de tránsito

En este caso, solo se dispone de datos hospitalarios de los años 1994, 1995 y 1996. Tiene un peso de 0,05. El índice obtenido a nivel nacional es de 0,03, y los departamentos con mayor prevalencia son Lima y Moquegua, con índices de 0,1 y 0,09. Le siguen en el rango 0.08-0.03 Tacna (0.08), Junín (0.08), Arequipa (0.08), Callao (0.07) e Ica (0.06). Juntos, estos dos bloques representan el 45% de la población del país.

La incidencia por debajo del promedio nacional se encuentra en Ancash, La Libertad, Ayacucho, Lambayeque, Tumbes, Huánuco, Piura y Puno. Todos ellos tienen un índice entre 0,03 y 0,02. En cambio, Ucayali, Madre de Dios, Cajamarca, San Martín, Cusco, Amazonas y Loreto tienen un índice de 0,01. Por su parte, Huancavelica, Pasco y Apurímac muestran un índice de 0.00.

Capítulo 3
3.1. Inteligencia artificial

Con la aparición de la humanidad aparece la información y con ella diversas formas de preservarla. En la actualidad, la información sigue siendo uno de los objetos más valiosos para la sociedad y las organizaciones, especialmente a la hora de tomar decisiones. La seguridad comenzó cuando las organizaciones agregaron procesos computarizados donde los administradores de sistemas y los analistas técnicos buscaban fallas de seguridad y trataban de solucionarlas por todos los medios posibles.

No había una comprensión clara del procesamiento de datos y la seguridad, por lo que, durante su desarrollo, la facilidad de transmitir información a través de procesos automáticos permitió el uso de Internet como plataforma para el almacenamiento de información. De esta forma, se ha logrado fluidez en la comunicación interpersonal, la comunicación intersectorial, las transacciones o el flujo digital de cualquier tipo. Pero esto dejó una gran cantidad de datos en sus sistemas a terceros no autorizados.

Cada día, las organizaciones se enfrentan a todo tipo de amenazas en contra de la información. Debido e esto, muchos expertos en seguridad han investigado y practicado sus las formas de preservación de datos y ofrecer sus servicios a organizaciones como proveedores o contratistas de servicios.

A mediados de la década de 1990, con la llegada del comercio electrónico, las pequeñas y medianas empresas, e incluso el público en general, se integraron gradualmente a la Web y surgieron males mucho más sofisticados. Se lanzaron nuevas técnicas de explotaciones intrusivas o vulnerables y hubo una falta de formación adecuada sobre la gestión de servidores y su seguridad.

El comportamiento anómalo al momento de compartir información se da por la falta de una plataforma de capacitación que fortalezca la seguridad informática. Jóvenes de todo el mundo ingresan al Internet para divertirse con los sistemas informáticos, engañando así a las centrales telefónicas mientras intercambian información con sus pares del otro lado del mundo. De allí salen los mejores especialistas en seguridad informática y ciberhackers de su tiempo. A nivel mundial, las tecnologías de la información y la comunicación son los motores del desarrollo y el progreso, mostrando la mejora de los procesos sociales y las aplicaciones estratégicas.

El mundo se convirtió gradualmente en el protagonista de su propio desarrollo con la ayuda de Internet y, a medida que se desarrollaba, la comunicación con él se hizo cada vez más necesaria, por lo que las personas se convirtieron en productores de contenido virtual. Este desarrollo trae nuevas perspectivas: las infraestructuras y propiedades adquiridas en la vida real debe recibir seguridad, también debe dársele seguridad a la información gestionada digitalmente.

Teniendo en cuenta las nuevas amenazas a los datos que se han desarrollado en paralelo con el crecimiento continuo de la tecnología y todo lo relacionado con la seguridad informática, se empiezan a definir los controles necesarios para reducir los riesgos al momento de procesar información. Hasta el día de hoy, esto sucede con la creación de buenas prácticas para garantizar sistemas de información seguros y confiables basados en la implementación del uso de la inteligencia artificial como generadora de controles tanto a nivel de hardware como de software; puesto que existen intrusos que pueden dañar el sistema operativo, las aplicaciones instaladas, o simplemente tomar el control de los sistemas informáticos de seguridad. Asimismo, se hizo necesario el establecimiento de políticas o parámetros que aseguren el acceso libre y abierto a la información, y tecnologías seguras utilizadas para proteger los activos de cualquier organización.

La ciberseguridad garantiza que las funciones de seguridad de la información que se mantengan dentro de una organización proporcionen acceso a sistemas que no sean vulnerables a ataques, intrusiones o indisponibilidad del entorno cibernético que afecten la integridad y confidencialidad de los datos. Actualmente se buscan formas de proteger y fortalecer el entorno cibernético, especialmente utilizando tecnologías avanzadas y autónomas en áreas técnicas y cognitivas, donde los problemas pueden resolverse en poco tiempo.

Así, estamos hablando del uso de la inteligencia artificial, que está diseñada para ser un componente importante de la promoción y sostenibilidad de la ciberseguridad. La inteligencia artificial estudia y analiza el comportamiento humano desde la perspectiva de la comprensión, la observación, la resolución de problemas y la toma de decisiones, lo que, reproducido en una computadora, permite la creación de aplicaciones de inteligencia artificial que simulan principalmente las actividades de los humanos. Con estos parámetros, los sistemas de IA procesan datos numéricos utilizando algoritmos heurísticos o clásicos que les permiten tratar problemas sin soluciones.

3.2. Inteligencia artificial e información segura

Actualmente, la inteligencia artificial afecta la vida cotidiana del mundo de formas diferentes, ya que su aplicación da forma a nuestro entorno. Los métodos que incorporan principios éticos y abordan cuestiones sociales son necesarios para garantizar que los sistemas desarrollados sean compatibles con los valores humanos.

El crecimiento tecnológico y los avances científicos cambian cada vez más los estilos de vida y reorganizan la sociedad, y aportan nuevos productos y servicios, haciendo que estos avances funcionen en varios frentes. Los líderes empresariales entienden las ventajas competitivas de hoy y cómo se pueden mejorar con nuevas tecnologías. De esta forma las sociedades tendrán una comprensión más clara de cómo la tecnología está dando forma a la economía global y cómo invertir en nuevas formas de educación e infraestructura a medida que este cambio disruptivo continúa avanzando.

Por otro lado, la seguridad de la información tiene tres principios básicos:

.

- Confidencialidad,
- Integridad, y
- Disponibilidad

Estos soportan y son la base de todos los sistemas implementados, ya que la seguridad de la información se vuelve esencial para todo tipo de organizaciones, y la importancia de esta no se puede estimar. En este sentido, la inteligencia

artificial ha estado muy involucrada en la implementación de diferentes áreas de la seguridad, como su uso en la detección de intrusos en la red y el bloqueo de spam, análisis de forenses, antivirus, etc.

Los sistemas basados en inteligencia artificial tratan problemas utilizando un modelo informático de razonamiento humano, pero la mayoría de estos sistemas requieren un mantenimiento constante para lograr un buen rendimiento. El desarrollo de sistemas inteligentes se basa en el aprendizaje automático y la teoría conexionista, y ambos utilizan conjuntos de datos relacionados, algoritmos y herramienta de red neuronal. Por lo tanto, los datos previamente analizados se examinan de manera diferente para producir resultados que validan la aplicabilidad del mismo análisis a los datos del mundo real.

El crecimiento de la información, la facilidad de acceso a la información y los avances tecnológicos han sido factores fundamentales en el desarrollo de sistemas que pueden registrar, analizar y tomar decisiones (inteligencia artificial). Los resultados obtenidos durante la investigación y la aplicabilidad de herramientas para administrar y prevenir comportamientos anormales de sistemas de información basados en ciberseguridad fueron bien recibidos por la sociedad en todo el mundo, lo que permitió maximizar la inteligencia autónoma en investigación y desarrollo, para gestionar y tratar datos, asegurando su protección y conservación.

El procesamiento de datos en cualquier nivel requiere el uso de lineamientos regulatorios establecidos por las autoridades pertinentes, a nivel global y nacional, para lograr la implementación de nuevas tecnologías usando inteligencia artificial de manera regulada. El objetivo es gestionar la seguridad de la información.

Estas pautas están sujetas a requisitos de ciberseguridad en constante evolución. La cantidad de datos digitales que se generan hoy requiere sistemas de almacenamiento seguros que aseguren la integridad, la calidad y la entrega de los datos, de lo contrario, son vulnerables a ataques o intrusiones en el entorno cibernético. Como consecuencia de lo anterior, surge la necesidad de adoptar técnicas basadas en inteligencia artificial para la mejora continua de la seguridad de la información, ya que es un mecanismo eficaz para prevenir y responder a los riesgos inmediatos, que posibilita el cumplimiento de los lineamientos de ciberseguridad: confidencialidad, integridad y disponibilidad.

3.3. Significado de la inteligencia artificial

La Inteligencia Artificial (IA) es una nueva forma de analizar, trabajar y comunicar que está cambiando al mundo, como parte de la transición digital en la que están inmersos todos los países. Desde un punto de vista económico, la inteligencia artificial se está convirtiendo en un factor determinante en la competitividad de las empresas. Su uso e inclusión en las cadenas de valor de diferentes sectores económicos y en diferentes procesos de negocio define la capacidad de las empresas para competir en el mercado global.

El desarrollo acelerado y simultáneo de múltiples tecnologías crea cambios disruptivos que deben gestionarse. Estas tecnologías incluyen inteligencia artificial, adquisición y análisis de datos, sensores biónicos, robótica, comunicaciones inalámbricas de banda ancha y supercomputadoras. La inteligencia artificial es sin duda una de las tecnologías con mayor potencial disruptivo. Las disrupciones tecnológicas relacionadas con la inteligencia artificial son provocadas por varios factores que podemos identificar:

Uno de los aspectos que más puede limitar el desarrollo de diversas tecnologías, y en especial de la inteligencia artificial, es la falta o ausencia de habilidades suficientes. Se prevé que la industria de la seguridad tenga una escasez de profesionales durante los próximos años. La misma carencia se observa, por ejemplo, en los campos de la inteligencia artificial o Big Data.

La inteligencia artificial se ha convertido en una tecnología de alto valor que acelera aún más las tendencias del ecosistema digital, tanto positivas (competitividad y prosperidad) como negativas (ciberataques). Esto crea riesgos y desafíos únicos a nivel mundial. Los países deben considerar la estrategia de sumarse a esta disrupción tecnológica y las administraciones públicas pueden promover su desarrollo e implementación. Pero la estrategia también debe tener en cuenta que esta nueva realidad requiere un marco normativo consensuado basado en el principio de precaución. Por lo tanto, los gobiernos deben:

- Reforzar sus conocimientos en Ciberseguridad, y
- Auspiciar la transición hacia una economía de datos, para garantizar la seguridad y privacidad, que ofrece la Inteligencia Artificial.

La inteligencia artificial se ha convertido en una tecnología intersectorial integrada en muchos sistemas y aplicaciones utilizados por empresas, instituciones y gobiernos. Por tanto, los aspectos de seguridad son especialmente importantes en el diseño y uso de la inteligencia artificial.

En la actualidad los automóviles, dispositivos médicos y electrodomésticos ahora son computadoras con cosas conectadas a ellos. El refrigerador es la computadora que mantiene las cosas frías, y el horno de microondas es la computadora que las calienta. El automóvil es una computadora en cuatro ruedas. Las computadoras ya no son solo una pantalla que encendemos y miramos. Lo que era seguridad informática, en su propio campo, es ahora la seguridad de todos.

De manera similar, cuando consideramos la inteligencia artificial como un factor central en la automatización de decisiones, hay diferentes niveles de soporte de decisiones respaldados por el uso masivo de datos y algoritmos de IA que se ejecutan en sistemas informáticos. La inteligencia artificial se ha convertido en una tecnología intersectorial integrada en muchos sistemas y aplicaciones muy utilizadas. Por tanto, los aspectos de seguridad son especialmente importantes en el diseño y uso de la inteligencia artificial:

- Las personas toman todas las decisiones sin la ayuda de una computadora.
- La computadora ofrece una gama completa de opciones para que una persona elija.
- La computadora muestra las opciones para la opción seleccionada.
- La computadora ofrece una alternativa.
- La computadora ejecuta la decisión cuando la persona la acepta.
- La computadora ejecuta una decisión que permite a una persona usar el veto por un tiempo limitado.
- La computadora realiza una operación e informa su decisión al humano.
- La computadora realiza una operación y, si es necesario, informa sobre ella.
- La computadora realiza la acción e informa a la persona si lo considera oportuno.
- Una computadora realiza sus tareas independientemente de un humano.

Cada uno de estos niveles tiene diferentes implicaciones en el campo de la seguridad, especialmente cuando vamos más allá del nivel de automatización controlado por humanos (niveles 1-4) y entramos al nivel de automatización que controlan las máquina (7-10).

Entre los puntos considerados importantes al momento de desarrollar una inteligencia artificial confiable, se tienen:

1. Control humano: Debe estar bajo control humano, tomando las debidas precauciones.

2. Durabilidad y Seguridad: Los sistemas deben ser "resistentes" a posibles intentos de manipulación o piratería y contar con planes de contingencia.

3. Protección y control de datos: la privacidad de los datos de los ciudadanos debe garantizarse durante todo el ciclo de vida de la IA.

4. Transparencia: la IA debe ser transparente, lo que significa que debe ser posible reconstruir cómo y por qué se comporta de cierta manera, y quienes interactúan con estos sistemas deben saber que es IA y también qué tipo de personas controlan.

5. Diversidad, no discriminación y justicia: La IA debe considerar la diversidad social desde su desarrollo hasta la ausencia de algoritmos subyacentes sin sesgos discriminatorios directos o indirectos.

6. Bienestar social y ambiental: El desarrollo tecnológico debe considerar sus impactos sociales y ambientales para ser sostenible y ambientalmente responsable.

7. Responsabilidad: La inteligencia artificial y sus resultados deben rendir cuentas a los auditores externos e internos.

Capítulo 4
4.1. Inteligencia artificial y seguridad ciudadana

El uso de la tecnología se ha convertido en un medio posible para garantizar la seguridad de los ciudadanos. Hay estudios en América Latina que muestran una gran cantidad de programas y actividades que requieren innovaciones tecnológicas diferentes para ser implementadas. Cabe señalar que este uso fue común, especialmente por parte de los gobiernos, y se espera que aumente en los próximos años, por lo que estamos inmersos en el "proceso tecnológico del Estado en seguridad ciudadana". Sin embargo, existen tensiones entre seguridad ciudadana y tecnología.

Por otro lado, la seguridad ciudadana tiene como objetivo fortalecer la ciudadanía mediante la promoción de los derechos individuales y colectivos; es una propuesta ciudadana más que de seguridad, mientras que la mayor parte de la tecnología apunta a mejorar la seguridad. El proceso tecnológico es ascendente y especializado en el tiempo: cada vez se utilizan tecnologías más diversas y se desarrollan inventos que se enfocan en problemas o situaciones específicas.

Por ejemplo, el uso de sistemas de información geográfica para el análisis de casos delictivos y la producción de inteligencia, el desarrollo de primeros auxilios, posicionamiento para el procesamiento de eventos y delitos en tiempo real, control automático de acceso a áreas estratégicas, control y gestión de vehículos y personas con escáneres, gestionar alarmas instaladas en ciudades y vías públicas, y utilizar aplicaciones por parte de los gobiernos y ciudadanos para hacer frente a problemas como el acoso callejero.

Desde la perspectiva del gobierno, la inversión en tecnología "es una medida primordial para la seguridad ciudadana". Como parte del proceso de seguridad tecnológica, la prevención de delitos por video, definida como una forma sistemática de vigilancia llevada a cabo por los gobiernos utilizando tecnología—principalmente cámaras de video—para monitorear situaciones y contextos, especialmente aquellos considerados de riesgo.

Existen diferentes tipos de sistemas de videovigilancia con características especiales; algunos permiten que la inteligencia artificial escanee y reconozca rostros y comportamientos. Existen cámaras corporales utilizadas por la policía y drones equipados con cámaras para monitorear eventos, con potentes lentes que

“nos observan desde el cielo”. Nuestro planeta es monitoreado por más de 1700 satélites. A una distancia de unos 500 kilómetros, algunos de ellos pueden enfocarse y obtener una imagen detallada del barrio en el que vivimos, que los gobiernos utilizan con fines de seguridad.

En las ciudades latinoamericanas, las cámaras de seguridad han logrado una difusión significativa entre las políticas gubernamentales de seguridad, empleadas principalmente para la prevención de delitos. Sin embargo, una de las objeciones fundamentales a la videovigilancia es que no previene el crimen, sino que simplemente lo repele.

En otras palabras, utiliza prácticas que vulneran el derecho de los ciudadanos a la privacidad y a no ser discriminados, y no hay garantía de que un delito captado en cámara sea debidamente perseguido por las instituciones correspondientes. Estos son debates que autoridades gubernamentales, ciudadanos y académicos deben abordar en profundidad.

En varias ciudades latinoamericanas, sin embargo, las cámaras son parte del paisaje urbano: están en la calle, en los centros comerciales, en casi todas partes. Sin embargo, “en América Latina, como en otros lugares”, esto no ha ido acompañado de una evaluación de su eficacia en el combate a la inseguridad, ni se han logrado avances significativos en la regulación y protección de los derechos fundamentales que pueden vulnerar los sistemas de videovigilancia. En este sentido, es necesario que las ciencias sociales aborden la videovigilancia del país como objeto de estudio en el contexto latinoamericano. Por lo tanto, se debe explorar, en profundidad, la relación entre seguridad ciudadana y tecnología; especialmente en relación con el uso, planificación y regulación por parte de los gobiernos latinoamericanos de la videovigilancia.

Si bien es cierto que América Latina tiene características políticas, económicas y culturales, que dificultan definir un enfoque metodológico único para considerar todas las implicaciones que tiene el uso de la inteligencia artificial en la seguridad ciudadana. En otras latitudes se han logrado avances significativos, como la carta publicada por el Foro Europeo de Seguridad Urbana sobre el uso democrático de la videovigilancia y la Inteligencia artificial, mientras que, en América Latina, y más específicamente en Perú, existen avances aislados y prácticas que aún se consideran inadecuadas. No obstante, se han dado discusiones como la propuesta del gobierno de crear un centro nacional de videovigilancia para garantizar la seguridad de los ciudadanos a través de la

policía nacional. Y en el caso de Santa Tecla en El Salvador, donde los contribuyentes exigieron 300 servicios de cámara a la oficina del alcalde.

4.2. Videovigilancia en Latinoamérica

Hay diferencias específicas en la historia de la videovigilancia en Latinoamérica, especialmente considerando que la vigilancia no solo ha cambiado con los años y con el desarrollo de la tecnología, sino que también tiene características específicas de acuerdo con cada contexto local y cada cultura, según las necesidades de seguridad pública. A diferencia de una ciudad como Londres o Nueva York, donde la videovigilancia masiva era parte de una estrategia de seguridad nacional como mecanismo reactivo y preventivo implementado después de un ataque terrorista.

Destacan dos hechos, en el mundo: los atentados terroristas de Londres en 1993, que supusieron la instalación de cámaras de vigilancia, especialmente en calles y edificios estratégicamente ocupados. Y Los atentados del 15 y 11 de septiembre de 2001, que sirvieron de pretexto para legislar el desarrollo de nuevas medidas de control que dependen más de la tecnología.

En América Latina, la situación fue diferente, Ciudad de México fue uno de los primeros centros urbanos donde se introdujeron dispositivos de videovigilancia forma masiva, en el 2008 implementó el programa Ciudad Bicentenario que incluyó 8088 colocaciones de cámaras. Actualmente, la videovigilancia se ha incrementado en las ciudades latinoamericanas y se espera que esta tendencia continúe en el futuro cercano. Si bien existen registros oficiales en los que las agencias gubernamentales registran el número de estos dispositivos, no es posible saber exactamente cuántas cámaras están en funcionamiento, y menos aún que los ciudadanos puedan saber su ubicación, porque en la mayoría de los casos se ha determinado que es información confidencial que no se puede revelar.

Sin embargo, podemos aprender que las ciudades latinoamericanas probablemente tienen menos cámaras de CCTV que otras ciudades más emblemáticas en materia de seguridad ciudadana. En los Estados Unidos, Manhattan tiene un estimado de 20.000 cámaras colocadas oficialmente que funcionan mediante el empleo de la IA. Chicago tiene un estimado de 32.000

dispositivos de circuito cerrado de televisión para combatir la epidemia de homicidios en el centro. Gran Bretaña reconoce la presencia de una cámara de vigilancia por cada 14 habitantes, lo que significa que los habitantes de una gran ciudad como Londres pueden ser filmados unas 300 veces al día.

América Latina, se ha incorporado al debate del empleo de IA y de la videovigilancia, más tardíamente. En países como México, Brasil, Argentina o Perú la llegada de videovigilancia ha tenido consecuencias directas sobre la forma de abordar el tema desde el punto de vista académico. Por lo tanto, se considera que el análisis sobre el empleo de la IA en la seguridad de los grandes centros urbanos es importante.

Sin embargo, hay que reconocer que se han realizado decenas de estudios en diversos países latinoamericanos y esfuerzos significativos para formular el análisis de las implicaciones de IA. Entre ellos destaca la Red Latinoamericana de Investigación en Ciencia, Tecnología y Sociedad (LAVITS), fundada en 2009, con el objetivo de actuar como un centro de discusión e intercambio de información sobre estas nuevas tecnologías y la IA.

4.3. Socialización de la IA y videovigilancia en Latinoamérica

El estudio sobre el uso y socialización de las cámaras de videovigilancia por parte de los gobiernos latinoamericanos es importante porque permite medir el grado de difusión y adopción de este tipo de tecnología para la seguridad ciudadana en la región. Se ha analizado desde la sociología que las representaciones sociales de la tecnología se construyen a partir de la interacción de los individuos con ella.

Así, se dice que existen tres enfoques teóricos para el estudio de esta interacción: su uso en la vida cotidiana, el uso técnico relacionado con la manipulación de la tecnología y las formas socio históricas de uso en las rutinas a nivel individual y colectiva. Se ha observado que los gobiernos latinoamericanos se basan en diferentes narrativas cuando se trata de videovigilancia e IA. De acuerdo con la sistematización de la información aplicada, la comunicación se refiere principalmente a la distribución de cámaras y la información relacionada con el uso profesional, que se realiza a través de la vigilancia y otros medios, así como los posibles tipos de cámaras.

La difusión de expansión numérica o expansión espacial de cámaras de videovigilancia es una de las formas más comunes de comunicación. Por ejemplo, en enero de 2018, el alcalde de Lima anunció que se instalarán otras 300 cámaras en la ciudad, haciendo un total de 700 cámaras. En lo referente al empleo de la IA, cámaras de videovigilancia y otras tecnologías, el centro de monitoreo y videovigilancia de la Policía Federal de la ciudad de Buenos Aires cuenta con 1.200 cámaras ubicadas en puntos estratégicos de la ciudad. De forma similar, el gobierno local desplegó su propia red de videovigilancia, con más de 2.000 cámaras distribuidas por toda la ciudad y centros de monitoreo bajo la responsabilidad de la policía metropolitana.

También se tiene la experiencia de Uruguay, donde como parte de la videovigilancia de las ciudades, la Secretaría de Gobernación contempla la instalación de más de 6,500 cámaras en todo el país y, centros de monitoreo basados en la IA, para la vigilancia de la república. De los tipos de cámaras, el portal de noticias del presidente de la República de Uruguay se refiere a la instalación de un sistema de videovigilancia, iniciado en 2013, que actualmente incluye cámaras de diferentes categorías con un software que alerta sobre comportamiento sospechoso, así como la velocidad de cualquier vehículo. También hacen zoom en las matrículas de vehículos, que se pueden consultar, entre otras cosas, en la base de datos.

Por otro lado, la comunicación pública y privada también crea un relato que refleja la socialización de la videovigilancia en América Latina. Esto es importante porque, como se ha señalado, la tecnología es una de las formas de representación social, un medio y forma de comunicación entre los sujetos sociales. El intercambio comunicativo está representado por medios digitales como Google, a través del cual personas buscan y preguntan sobre temas de interés. Google Trends se puede utilizar para medir el interés en temas diferentes.

El análisis sobre la utilización y la socialización de las cámaras de videovigilancia para los gobiernos latinoamericanos está relacionado con la amplitud de la penetración y la apropiación de este tipo de tecnología. Desde la sociología se ha analizado que las representaciones sociales de la tecnología se basan en la interacción de los individuos con ella. Así, afirma que existen tres enfoques teóricos para el estudio de esta interacción:

- Desde el uso cotidiano
- Desde el involucrado en la manipulación de la tecnología, y
- Desde el conocimiento sociohistórico del uso en las costumbres individuales y grupales.

Se ha observado que los gobiernos de América Latina utilizan una variedad de narrativas para abordar el problema de CCTV. De acuerdo con el proceso metodológico de la información, se ha encontrado que la comunicación se refiere principalmente al aumento de cámaras de videovigilancia y sobre el uso que el gobierno hace de este tipo de tecnologías. La difusión de información referida al aumento en el número o la expansión del territorio de las cámaras de videovigilancia es uno de los puntos de comunicación más comunes.

Otra forma de comunicación a los ciudadanos sobre la videovigilancia es aquella en que el gobierno demuestra las ventajas del empleo la tecnología, la coordinación que puede existir entre diversos departamentos y ciudades, y la transparencia del uso de los dineros pública para el uso de IA. Por ejemplo, la experiencia de socialización de los servicios tecnológicos, del ministro del Interior de Uruguay, confirmando que el monitoreo de video tiene el efecto deseado en la población, afirmando que hasta ahora ha reducido en un 80% los hurtos. Es una forma de difusión de información muy significativa, porque demuestran a la sociedad que la IA y los sistemas de videovigilancia son cada vez más útiles en la prevención del delito.

En Perú, la apertura del Centro de Videovigilancia y Comunicación de Parcona atrae a más personas, incluso a aquellas que no se preocupan por el empleo de las tecnologías. De igual forma, está el proceso de socialización que se enfoca

en temas de coordinación y apunta a la transformación regional. En El Salvador durante una reunión con alcaldes y representantes municipales en 2015 se dieron a conocer las medidas de seguridad y destacar esfuerzos de los municipios en esta materia. En la reunión se presentó la experiencia de la implementación de sistemas de videovigilancia en San Salvador en cooperación con las alcaldías en sistemas de videovigilancia y prevención de violencia, así como la necesidad de vincular estos sistemas con otros mecanismos de atención ciudadana, como los servicios de emergencia 911.

Uno de los temas tocados con menor frecuencia en la sociedad, es la inversión en la adquisición de esta tecnología, que debe ser promovida en todos los gobiernos latinoamericanos como un ejercicio de transparencia y rendición de cuentas, sobre todo al considerar que la industria de la videovigilancia y el empleo de la IA ha crecido en gran medida por los recursos públicos. Al respecto, destaca la información pública compartida por el Ministerio del Interior de Uruguay en agosto de 2017, indicando la firma de contrato con Sonda Uruguay S.A, para la colocación de un sistema de videovigilancia basado en la IA, por un monto de 19,5 millones de dólares. De igual forma, en 2017, el gobierno de Uruguay anunció la donación de 1.000 cámaras por parte de la República de China. Al respecto, el Canciller señaló que China es el principal socio de Uruguay en términos de financiamiento en materia de seguridad. En concreto, el sistema de videovigilancia mejorará las políticas de privacidad.

Los casos presentados anteriormente son solo algunos de los cientos de comunicados oficiales que los gobiernos nacionales han realizado en Latinoamérica en materia de CCTV. Muestran que diversos factores contribuyen a la construcción de representaciones sociales, como la difusión de intereses y la conexión a nuevas infraestructuras, aunque en menor medida, incluida la socialización, a través de cuestiones fundamentales como la transparencia y la rendición de cuentas. Principalmente refleja que en las ciudades latinoamericanas el uso diario y de largo plazo de la videovigilancia es cada vez mayor y requiere planificación y regulación.

4.4. Planes sobre videovigilancia basada en IA: Latinoamérica

Como se analizó anteriormente, la videovigilancia con fines de seguridad ciudadana ha aumentado en América Latina, así como en otras regiones del mundo,

y se espera que continúe aumentando en los próximos años. Por ello, se requieren procesos de planificación gubernamentales que "orienten el curso de acción a seguir para lograr el objetivo", que en este caso se define como videovigilancia en un contexto de seguridad, seguridad ciudadana.

Las políticas de seguridad ciudadana en América Latina y el Caribe han tenido avances significativos en los últimos diez años, aunque estas políticas son mucho más débiles que las que se han llevado a cabo en los países desarrollados, advirtiendo sobre una posible debilidad de las políticas con respecto a estas tecnologías de vigilancia. Lo que se ha mantenido constante en América Latina es que la institucionalidad en materia de seguridad ciudadana está en transición y se va construyendo por reformas del Estado (descentralización y privatización) y la introducción del concepto de seguridad ciudadana (convivencia entre individuos) sobre la base de la seguridad pública (preservación del orden público por parte del estado).

En lo referente a videovigilancia e implementación de sistemas de seguridad basados en IA, los programas nacionales de seguridad pública, en su mayor parte, se identifican con los objetivos relacionados con la seguridad y la tecnología, pero no en todos los casos. Al hacer referencia específicamente a la videovigilancia, en América Latina, no existe planes oficiales para estos sistemas.

En la mayoría de los programas analizados no se encontró evidencia de planificación de CCTV, pero sí de tecnología utilizada con fines de seguridad. En la mayoría de estos países, la nueva tecnología no es conocida a profundidad. Con respecto a las estrategias, objetivos y procedimientos, se ha determinado que Bolivia, Colombia, Costa Rica, Ecuador, Salvador, Nicaragua, México y Perú incluyen en el contexto de planificación estatal el empleo de estas tecnologías, y también se ha encontrado como Venezuela, lo consideró parte de la seguridad del ciudadano.

En Bolivia, el objetivo de garantizar la seguridad de los ciudadanos para una vida libre de violencia está incluido en el plan nacional de gobierno, estableciendo en el marco de la reforma institucional de la policía boliviana, que se mejorará la infraestructura, el equipamiento y la tecnología, para prevenir, investigar y sancionar los delitos cuando sea necesaria. Además, propone la elaboración e Implementación de un Programa de Fortalecimiento de Infraestructura y Equipamiento Policial (Cámaras de Seguridad, etc.).

En Colombia, el tratado “Política de Defensa y Privacidad. Todos por un Nuevo País”, identifica el uso de la tecnología como un medio para combatir el crimen y la delincuencia. Se reconoció la importancia de la tecnología para la seguridad de los ciudadanos y se propuso ampliar la cobertura, la coordinación interinstitucional y la integración del sistema CCTV, mediante la instalación de nuevas cámaras en ciudades claves. Costa Rica, en su política integral para la seguridad sostenible de sus ciudadanos y la promoción de la paz social, incluyó acciones estratégicas encaminadas a eliminar las formas más cercanas de violencia y abuso mediante la aplicación intensiva de tecnología para el control de áreas y actividades de alto riesgo, para hacer más eficiente el trabajo policial. Y de esta forma aumentar la percepción de seguridad.

En Ecuador, el Plan Integral de Seguridad Nacional 2014-2017 establece como meta fortalecer la investigación científica y tecnológica al servicio de la seguridad. Con respecto al CCTV, surgió el Servicio Integral de Seguridad (ECU-911) como una respuesta del Estado para atender y responder rápidamente a las emergencias y contribuir a través de la video vigilancia al combate de la delincuencia mejorando la seguridad, es decir, ECU-911 se describe como una respuesta estatal basada en videovigilancia.

En El Salvador, la Política Nacional de Justicia, Seguridad y Convivencia 2014-2019 recomienda la implementación de sistemas de vigilancia electrónica en las zonas con mayor índice de criminalidad para prevenir e investigar los delitos. Además, se define la estrategia de seguridad pública, los criterios para la distribución de los recursos federales de seguridad, y el fortalecimiento de los sistemas de videovigilancia y geolocalización. Actualmente, en la mayoría de las ciudades y municipios del país, los sistemas de videovigilancia y posicionamiento no funcionan, y no existe un programa para la capacitación y mantenimiento de los sistemas.

En Nicaragua, el modelo policial propuesto promueve la adopción de nuevas tecnologías, donde se considera el uso de la videovigilancia. Por su parte, en Venezuela existe un claro aumento de los servicios de seguridad privada, esto se puede verificar en el crecimiento explosivo de los servicios privados de vigilancia, protección e investigación, que brindan desde redes domiciliarias, puertas blindadas, sistemas de alarma, cámaras de video hasta personal de seguridad. Se considera que este tipo de seguridad privada no es necesariamente compatible con la seguridad del ciudadano, por lo que es necesario modificar la normativa para adecuarla a las necesidades del país.

En Perú, el Plan Nacional de Seguridad Ciudadana 2013-2018 "Pacto Nacional de Seguridad Ciudadana" propone la creación de un "Centro Nacional de Videovigilancia y Radiocomunicaciones para la Seguridad Ciudadana" como una plataforma interactiva de la Policía Nacional del Perú. Esta es una de las propuestas en América Latina que proyecta un mayor crecimiento en videovigilancia y seguridad basada en IA.

Localmente, en cada país, hay esfuerzos de planificación que se desarrolla intensamente, pero no ha logrado penetrar a nivel nacional en todos los países de la región. En Buenos Aires, el Plan de Acción 2012-2014 del gobierno de la Ciudad Autónoma de Buenos Aires establece que la política de seguridad se basa principalmente en el control de los lugares públicos con una extensa red de cámaras de vigilancia. Mientras que, en México, los resultados indican que las tres cuartas partes de las entidades incluyen la videovigilancia en su planificación local. La videovigilancia en las ciudades de América Latina parece estar muy relacionada con el problema de la inseguridad. La seguridad ha adquirido importantes dimensiones no solo en la planificación del gobierno, sino también en la agenda mediática y en las últimas campañas electorales.

4.5. Marco jurídico: IA y sistemas de video seguridad

En general, en América Latina existe un vacío en la regulación de la videovigilancia y la IA en comparación con otras partes del mundo que cuentan con un marco regulatorio desde hace décadas. Destacan Estados Unidos, Alemania, Bélgica, Dinamarca, España, Francia, Holanda, Nueva Zelanda, Reino Unido y Suecia por contar con un marco legal en esta materia.

En España existe desde 1997 la Ley Orgánica 4/1997, que regula el uso de cámaras de vídeo por parte de las fuerzas y organismos de seguridad en los lugares públicos. En cambio, en América Latina la legislación sobre sistemas de seguridad basados en IA es escasa. Para ilustrar este punto, sirve el caso de México, que siendo uno de los líderes en el despliegue generalizado de sistemas de videovigilancia en América Latina, no cuenta con una legislación nacional, solo marcos normativos locales, como las leyes reglamentarias que regulan el uso de tecnologías disruptivas para las instalaciones de sistemas de seguridad.

La legislación peruana ha mostrado avances a este respecto, desde el 2015 existe una ley en materia de uso público o comercial: el Decreto Legislativo N° 1218, que regula el uso de cámaras de circuito cerrado de televisión. Este reglamento define el uso de estos dispositivos tecnológicos en bienes de dominio público, transporte público de pasajeros y locales comerciales abiertos al público con capacidad para 50 personas o más. De particular interés, es el artículo 10, que establece que las cámaras de circuito cerrado de televisión no podrán capturar ni grabar ninguna imagen, video o sonido de cualquier espacio que viole la privacidad o intimidad de cualquier persona, protegiendo, así, un derecho que puede ser violado mediante videovigilancia. Además, en marzo de 2018, se emitió una norma que establece que la instalación y manejo de cámaras de circuito cerrado de televisión debe realizarse de acuerdo con los planes distritales de seguridad ciudadana, los cuales deben coordinarse en todo momento con la Policía Nacional del Perú.

En Argentina, por lo menos existen dos marcos legales que rigen la videovigilancia, se relacionan con la protección de datos personales, instalación de cámaras en las entradas y salidas de salas de baile y/o similares, además establece los requisitos mínimos que los sistemas de videovigilancia deben cumplir. Si bien la introducción masiva de cámaras ha ido más rezagada en América Latina que en otras partes del mundo, esto no absuelve a los gobiernos y legislaturas de sus responsabilidades, pues la sociedad tiene una necesidad legislativa al respecto, especialmente sobre la violación de derechos que pueda causar el circuito cerrado de televisión. Sin una legislación que regule o designe un organismo responsable de la protección de los derechos fundamentales, se creará un ambiente propicio para la vulneración de estos derechos.

En América Latina, se observa un aumento notable en el despliegue de videovigilancia en las ciudades, como mecanismo utilizado por los gobiernos con fines de seguridad ciudadana. Es claro que este crecimiento continuará en los próximos años, como también han advertido expertos en la materia. Por lo tanto, es necesario implementar procesos de planificación y gestión en todos los países de la región para evitar contextos de abusos a los derechos humanos que pueden verse afectados por CCTV.

La evidencia demuestra que los gobiernos latinoamericanos ven la videovigilancia como una herramienta potencial en términos de seguridad ciudadana y la han implementado como parte de las estrategias nacionales y locales. Además, han construido relatos que comparten, a través de la

comunicación formal, el interés de legitimar esta videovigilancia, al tiempo que implementa diversas formas para presentarlo al público, a una audiencia específica y a la sociedad en general.

Sin embargo, se ha observado que existe una brecha significativa entre el uso de la videovigilancia y la planificación de políticas públicas para la seguridad de los ciudadanos. Si bien no es posible realizar un análisis comparativo entre las variables, ya que las referencias a la videovigilancia en sus respectivos programas de seguridad nacional o equivalentes son breves, es posible conocer que ocho países de la región integran la videovigilancia como parte de los lineamientos nacionales. Perú tiene la propuesta más avanzada de coordinación, interoperabilidad y transformación regional para la seguridad ciudadana. En el proceso de diseño de políticas públicas, la planificación es fundamental, ya que define los procedimientos que debe seguir la acción pública, y es un componente esencial de la gestión gubernamental.

La planificación de CCTV en América Latina debe estar en la agenda de seguridad de todos los países de la región, ya que se utiliza de forma diaria y continua, y los resultados indican que seguirá aumentando en los próximos años. La planificación debe avanzar hacia iniciativas que contribuyan al diseño de lineamientos sobre la videovigilancia con fines de seguridad ciudadana. Ejemplo de esto son: la propuesta de Perú de establecer centros nacionales de videovigilancia, o la Carta para los Usos Democráticos de la Videovigilancia, publicada por el Foro Europeo de Seguridad Urbana, en la que los gobiernos latinoamericanos establecen los lineamientos generales de uso, regulación y cooperación en este campo.

Además, la planificación debe incluir, en la medida de lo posible, innovaciones tecnológicas como el uso de drones, utilizados en América Latina para problemas agrícolas y para videovigilancia. En la misma línea, las políticas deben incentivar la creación un marco legal que defina los propósitos, alcances, objetivos y limitaciones, entre muchos otros aspectos de la videovigilancia, en sus operaciones urbanas. De lo contrario, habrá vacíos legales que permitan abusos a los derechos humanos, así como abusos por parte de las autoridades, que pueden utilizar la videovigilancia como una herramienta de control y no como un mecanismo de seguridad ciudadana.

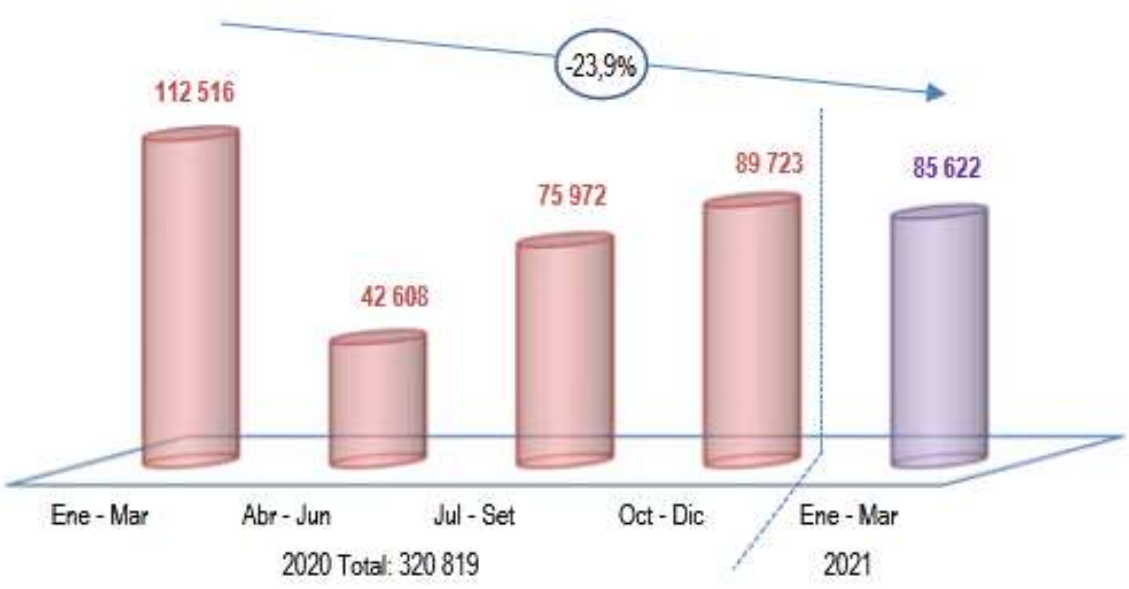
Capítulo 5

5.1. Seguridad ciudadana en Lima metropolitana

En este capítulo se brinda información sobre los delitos registrados en el Sistema de Denuncias Policiales disponible en el Sistema Integrado de Estadísticas Criminales y Seguridad Ciudadana, gradualmente actualizado. De enero a marzo de 2021 se registraron 85 mil 622 denuncias ante la autoridad Disminuyó el número de delitos a nivel nacional, respecto a igual trimestre de 2020 Superior - 23,9% (26 mil 894).

Figura 5.1.

Perú: Denuncias por delitos. Trimestres 2020-2021.



Fuente: INEI (2021).

5.2. Denuncias según los departamentos

Lima Metropolitana registró la mayor cantidad de denuncias de enero a marzo de 2021, con delitos 26.670 cometidos, seguida de Arequipa (5.428) y Lambayeque (5.248), Huancavelica, Pasco, Moquegua y Madre de Dios registraron menos de mil denuncias cada una. Los departamentos con mayor crecimiento porcentual enero-marzo 2021/enero-marzo 2020, fueron Huancavelica (10,3%), San Martín (8,6%) y Cajamarca (7,3%). Por otro lado, cabe destacar que la provincia constitucional de Callao e Ica presentaron una mayor disminución en el periodo de referencia.

Tabla 5.1.

Denuncias por comisión de delitos por departamento. Ene-Mar, 2020-2021.

Departamento	2020	2021	Variación	
	Ene - Mar	Ene - Mar	Absoluta	%
Total	**112 516**	**85 622**	**-26 894**	**-23,9**
Lima Metropolitana 1/	37 760	26 670	-11 090	-29,4
Arequipa	6 461	5 428	-1 033	-16,0
Lambayeque	6 525	5 248	-1 277	-19,6
La Libertad	6 378	4 913	-1 465	-23,0
Piura	6 871	4 677	-2 194	-31,9
Cusco	4 023	3 565	-458	-11,4
Junín	4 254	3 390	-864	-20,3
Ica	4 812	3 051	-1 761	-36,6
Cajamarca	2 817	3 024	207	7,3
Áncash	4 166	2 998	-1 168	-28,0
Departamento de Lima 2/	4 127	2 857	-1 270	-30,8
Prov. Const. del Callao	4 512	2 855	-1 657	-36,7
San Martín	1 908	2 073	165	8,6
Ucayali	2 398	1 779	-619	-25,8
Huánuco	2 094	1 755	-339	-16,2
Loreto	1 703	1 514	-189	-11,1
Puno	2 156	1 470	-686	-31,8
Ayacucho	1 660	1 416	-244	-14,7
Amazonas	1 492	1 269	-223	-14,9
Tumbes	1 347	1 187	-160	-11,9
Tacna	1 358	1 184	-174	-12,8
Apurímac	1 127	1 110	-17	-1,5
Madre de Dios	769	662	-107	-13,9
Moquegua	627	562	-65	-10,4
Pasco	773	526	-247	-32,0
Huancavelica	398	439	41	10,3

Fuente: INEI (2021).

5.3. Tipos de delitos

En enero-marzo de 2021, la mayoría de las denuncias que se presentaron fueron contra la propiedad (50 mil 776), seguido de seguridad pública (9 mil 736), vida, cuerpo y salud (9 mil 526) y libertad (8 mil 919), las cifras son inferiores a las del mismo trimestre de 2020. Según variación porcentual, delitos contra la voluntad popular (392,2%), delitos fiscales (25,0%), delitos contra la confianza y la honradez en los negocios (1 ,3%) y medio ambiente (9, %) presentaron el mayor incremento.

Tabla 5.2.

Denuncias por comisión de delitos, según delito genérico
Ene-Mar, 2020-2021.

Delito genérico	2020	2021	Variación	
	Ene- Mar	Ene- Mar	Absoluta	%
Total	**112 516**	**85 622**	**-26 894**	**-23,9**
Contra el patrimonio	68 635	50 776	-17 859	-26,0
Contra la seguridad pública	12 900	9 736	-3 164	-24,5
Contra la vida, el cuerpo y la salud	11 965	9 526	-2 439	-20,4
Contra la libertad	10 533	8 919	-1 614	-15,3
Contra la administración pública	5 523	3 943	-1 580	-28,6
Contra la familia	1 354	1 268	-86	-6,4
Contra la fe pública	602	596	-6	-1,0
Contra la voluntad popular	51	251	200	392,2
Delitos ambientales	117	128	11	9,4
Contra el orden financiero y monetario	166	121	-45	-27,1
Contra la tranquilidad pública	117	89	-28	-23,9
Contra el honor	82	79	-3	-3,7
Contra la humanidad	331	60	-271	-81,9
Delitos tributarios	36	45	9	25,0
Contra los derechos intelectuales	40	26	-14	-35,0
Contra el patrimonio cultural	27	24	-3	-11,1
Contra la confianza y la buena fe en los negocios	14	16	2	14,3
Contra el estado y la defensa nacional	12	11	-1	-8,3
Contra el orden económico	11	8	-3	-27,3
Contra los poderes del estado y el orden constitucional	-	-	-	-

Fuente: INEI (2021).

Del total de denuncias registradas en enero-marzo de 2021, el 59,3% fueron contra la propiedad, el 11,1% contra la vida, el cuerpo y la salud, el 11,4% contra la seguridad pública y el 10,4% contra la libertad, el resto incluye otros delitos. En 17 de los departamentos registrados, más del 50,0% de los delitos denunciados son contra la propiedad: Ucayali (69,3%) y Lambayeque (68,0%). Cabe destacar, que la mayoría de las denuncias en Tumbes fueron por delitos contra la seguridad pública (3,0%). En la siguiente tabla, se encuentran los delitos denunciados de los 43 distritos de Lima.

Tabla 5.3.

Denuncias por comisión de delitos por tipo de delito, según departamento Ene - Mar, 2021.

Departamento	Total	Contra el patrimonio	Contra la vida, el cuerpo y la salud	Contra la seguridad pública	Contra la libertad	Otros 3/
Total	**85 622**	**59,3**	**11,1**	**11,4**	**10,4**	**7,8**
Amazonas	1 269	60,0	15,8	6,2	9,5	8,4
Áncash	2 998	55,4	14,4	10,8	11,8	7,6
Apurímac	1 110	43,1	15,1	21,8	11,4	8,6
Arequipa	5 428	56,4	8,2	15,3	9,1	11,1
Ayacucho	1 416	54,0	21,0	8,1	10,7	6,2
Cajamarca	3 024	53,7	16,2	10,9	8,8	10,4
Prov. Const. del Callao	2 855	59,3	11,6	8,6	12,6	7,8
Cusco	3 565	45,7	13,4	24,8	9,2	6,8
Huancavelica	439	34,4	32,6	10,7	14,8	7,5
Huánuco	1 755	47,5	18,8	12,6	13,4	7,6
Ica	3 051	55,4	9,0	17,5	11,4	6,7
Junín	3 390	50,4	13,0	14,6	10,5	11,5
La Libertad	4 913	60,5	12,6	9,6	9,1	8,1
Lambayeque	26 670	68,0	8,3	7,1	9,9	6,7
Lima Metropolitana 1/	2 857	52,2	14,7	13,7	11,7	7,7
Departamento de Lima 2/	5 248	65,1	10,2	6,8	11,2	6,8
Loreto	1 514	43,6	8,7	30,4	12,3	5,0
Madre de Dios	662	52,6	9,8	20,8	9,1	7,7
Moquegua	562	50,9	12,3	15,8	12,5	8,5
Pasco	526	46,2	21,5	8,6	15,2	8,6
Piura	4 677	64,7	11,5	6,4	9,4	8,0
Puno	1 470	49,8	16,8	18,1	8,7	6,6
San Martín	2 073	58,2	12,1	7,9	13,2	8,6
Tacna	1 184	48,2	6,7	18,6	18,8	7,8
Tumbes	1 187	33,1	9,9	34,0	6,9	16,1
Ucayali	1 779	69,3	6,1	10,0	9,4	5,1

Fuente: INEI (2021).

En los últimos años, el sector empresarial y la sociedad peruanas han experimentado un constante desarrollo tecnológico, lo que significa nuevas formas de delincuencia, nuevos delitos. Este hecho dio lugar a un debate sobre la necesidad de distinguir los delitos informáticos de otros. En enero-marzo 2021 se reportaron 313 delitos informáticos a nivel nacional, es decir, un 5% más que el mismo periodo de 2020. La mayor parte de denuncias por delitos informáticos en enero-marzo 2021, se observaron en los municipios de Lima (83), Lambayeque (36) y Huánuco (26). En el otro extremo, Huancavelica y Moquegua reportaron solo un (1) caso de este tipo de delitos. Se presentó un crecimiento significativo en los departamentos de Junín, Ucayali y Amazonas.

Tabla 5.4.

Denuncias por comisión de delitos informáticos, según departamento
Ene - Mar, 2020-2021.

Departamento	2020	2021	Variación	
	Ene - Mar	Ene - Mar	Absoluta	%
Total	**297**	**313**	**16**	**5,4**
Amazonas	2	4	2	100,0
Áncash	18	9	-9	-50,0
Apurímac	1	-	-1	-100,0
Arequipa	12	14	2	16,7
Ayacucho	4	7	3	75,0
Cajamarca	2	3	1	50,0
Prov. Const. del Callao	11	13	2	18,2
Cusco	21	23	2	9,5
Huancavelica	-	1	1	-
Huánuco	17	26	9	52,9
Ica	5	6	1	20,0
Junín	9	23	14	155,6
La Libertad	38	20	-18	-47,4
Lambayeque	17	36	19	111,8
Lima Metropolitana 1/	110	83	-27	-24,5
Departamento de Lima 2/	4	2	-2	-50,0
Loreto	2	3	1	50,0
Madre de Dios	2	-	-2	-100,0
Moquegua	1	1	0	0,0
Pasco	-	3	3	-
Piura	12	17	5	41,7
Puno	3	-	-3	-100,0
San Martín	3	5	2	66,7
Tacna	-	2	2	-
Tumbes	-	5	5	-
Ucayali	3	7	4	133,3

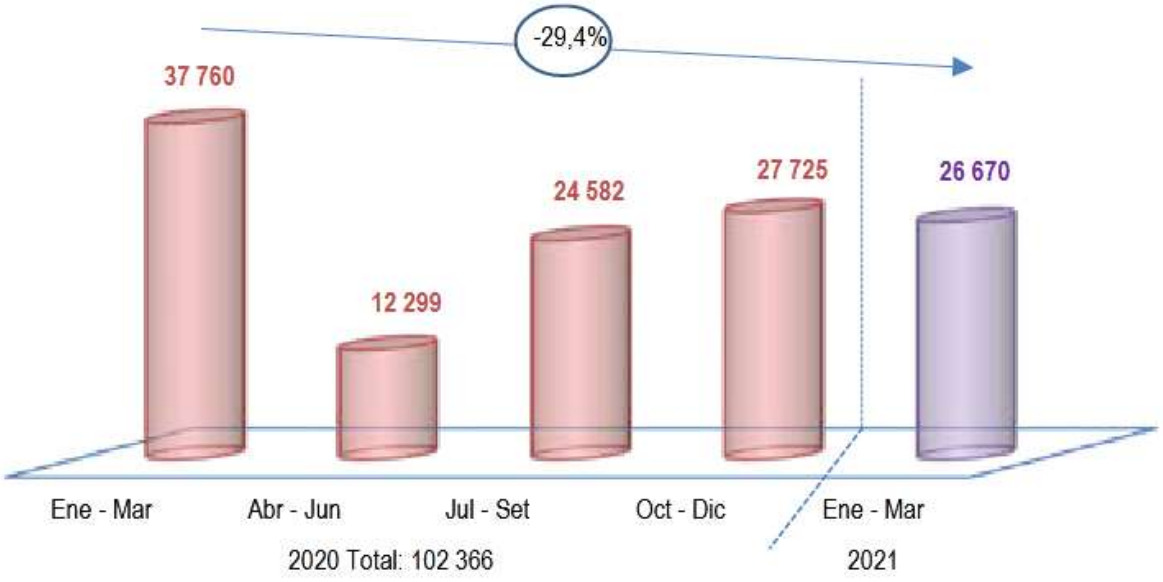
Fuente: INEI (2021).

5.4. Denuncias por delitos en Lima Metropolitana

En enero-marzo de 2021, en la policía peruana se presentaron 26.670 denuncias por la comisión de delitos registrados, lo que supone un -29,4 % (11 mil 90) menos que en igual período de 2020.

Figura 5.2.

Lima Metropolitana: Denuncias por comisión de delitos
Trimestre: 2020 - 2021



Fuente: INEI (2021).

Durante el período enero-marzo 2021/enero-marzo 2020, las áreas metropolitanas de Lima registraron menos denuncias por delitos, a excepción de Surquillo, La Molina, Santa Rosa, Lurín y Chaclacayo, que registraron un aumento. En cuanto a la variación porcentual, Santa Rosa (93,4%), Surquillo

(40,9%) y La Molina (27,5%) son las que más subieron. Por otro lado, el menor crecimiento registrado se encuentra en Chaclacayo (3,7%) y Lurín (7,0%).

Tabla 5.5.

Lima Metropolitana: Denuncias por comisión de delitos, según distrito Enero - marzo, 2020-2021.

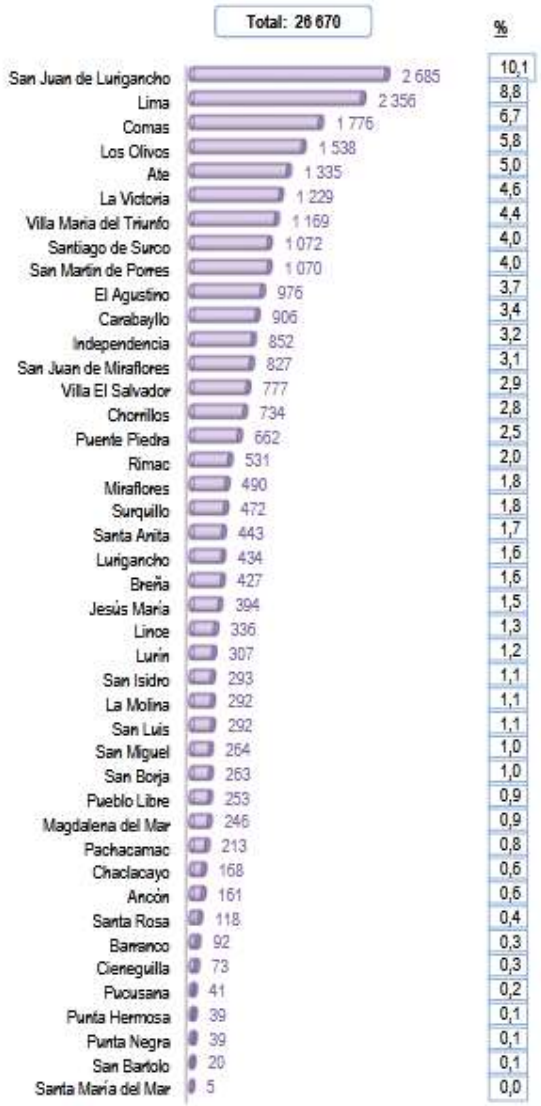
Distrito	2020	2021	Variación	
	Ene - Mar	Ene - Mar	Absoluta	%
Total	37 760	26 670	-11 090	-29,4
Lima	3 830	2 356	-1 474	-38,5
Ancón	257	161	-96	-37,4
Ate	1 691	1 335	-356	-21,1
Barranco	315	92	-223	-70,8
Breña	571	427	-144	-25,2
Carabayllo	1 446	906	-540	-37,3
Chaclacayo	162	168	6	3,7
Chorrillos	921	734	-187	-20,3
Cieneguilla	92	73	-19	-20,7
Comas	2 288	1 776	-512	-22,4
El Agustino	1 176	976	-200	-17,0
Independencia	1 101	852	-249	-22,6
Jesús María	413	394	-19	-4,6
La Molina	229	292	63	27,5
La Victoria	1 472	1 229	-243	-16,5
Lince	599	336	-263	-43,9
Los Olivos	1 808	1 538	-270	-14,9
Lurigancho	599	434	-165	-27,5
Lurín	287	307	20	7,0
Magdalena del Mar	353	246	-107	-30,3
Pueblo Libre	462	253	-209	-45,2
Miraflores	699	490	-209	-29,9
Pachacamac	287	213	-74	-25,8
Pucusana	100	41	-59	-59,0
Puente Piedra	869	662	-207	-23,8
Punta Hermosa	95	39	-56	-58,9
Punta Negra	56	39	-17	-30,4
Rimac	914	531	-383	-41,9
San Bartolo	39	20	-19	-48,7
San Borja	363	263	-100	-27,5
San Isidro	483	293	-190	-39,3
San Juan de Lurigancho	3 845	2 685	-1 160	-30,2
San Juan de Miraflores	1 154	827	-327	-28,3
San Luis	404	292	-112	-27,7
San Martin de Porres	2 077	1 070	-1 007	-48,5
San Miguel	371	264	-107	-28,8
Santa Anita	780	443	-337	-43,2
Santa María del Mar	17	5	-12	-70,6
Santa Rosa	61	118	57	93,4
Santiago de Surco	1 812	1 072	-740	-40,8
Surquillo	335	472	137	40,9
Villa El Salvador	1 153	777	-376	-32,6
Villa María del Triunfo	1 774	1 169	-605	-34,1

Fuente: INEI (2021).

Entre los barrios de Lima Metropolitana, San Juan de Lurigancho presentó el 10,1% de las denuncias por la comisión de delitos- Los principales son Lima (8,8%), Comas (6,7%), Los Olivos (5,8%) y Ate (5,0%). En tanto, Santa María del Mar, San Bartolo, Punta Negra y Punta Hermosa tuvieron un porcentaje menor de (0,1%) en enero-marzo de 2021.

Figura 5.3.

Lima Metropolitana: Denuncias por comisión de delitos, según distrito
Ene - Mar, 2021.



Fuente: INEI (2021).

En el área metropolitana de Lima en enero-marzo de 2021, el 68,0% de las denuncias registradas estuvieron relacionadas con delitos contra la propiedad, el 8,3% contra la vida, la integridad física y la salud, el 9,9% contra la libertad y el 7,1% contra la seguridad pública. Según el grupo de delitos generales básicos, Lince, San Isidro, Miraflores, Pueblo Libre, Surquillo y Breña registran la mayoría de las denuncias por delitos contra la propiedad, cada uno con más del 80.0%; una menor proporción de este delito se registró en Santa Rosa (13,6%).

Tabla 5.6.

Lima Metropolitana: Denuncias por comisión de delitos, según distrito
Enero - marzo, 2021.

Distrito	Total	Contra el patrimonio	Contra la vida, el cuerpo y la salud	Contra la seguridad pública	Contra la libertad	Otros 3/
Total	26 670	68,0	8,3	7,1	9,9	6,7
Ancón	161	62,1	11,2	11,2	7,5	8,1
Ate	1 335	62,1	9,4	14,4	10,0	4,0
Barranco	92	60,9	9,8	7,6	9,8	12,0
Breña	427	80,3	3,7	3,5	7,0	5,4
Carabayllo	906	65,7	14,3	4,0	12,5	3,5
Chaclacayo	168	65,5	7,1	4,2	13,1	10,1
Chorrillos	734	60,6	9,5	9,8	12,7	7,4
Cieneguilla	73	52,1	9,6	2,7	23,3	12,3
Comas	1 776	72,0	7,0	6,2	8,7	6,1
El Agustino	976	73,3	9,7	6,5	7,3	3,3
Independencia	852	71,9	6,9	7,6	9,4	4,1
Jesús María	394	73,4	5,1	1,5	13,7	6,3
La Molina	292	69,9	2,4	6,5	10,6	10,6
La Victoria	1 229	77,0	8,5	5,7	5,5	3,3
Lima	2 356	69,9	10,5	5,1	7,2	7,3
Lince	336	83,6	5,7	0,3	6,5	3,9
Los Olivos	1 538	63,1	5,1	8,5	7,6	15,7
Lurigancho	434	55,3	16,1	6,2	15,7	6,7
Lurín	307	58,0	6,8	18,9	13,4	2,9
Magdalena del Mar	246	78,9	2,4	2,4	8,5	7,7
Miraflores	490	81,4	4,3	2,7	5,3	6,3
Pachacamac	213	61,5	6,1	12,7	13,1	6,6
Pucusana	41	39,0	26,8	4,9	14,6	14,6
Pueblo Libre	253	81,0	3,6	4,0	7,9	3,6
Puente Piedra	662	57,7	10,6	7,1	15,1	9,5
Punta Hermosa	39	59,0	5,1	15,4	17,9	2,6
Punta Negra	39	61,5	2,6	23,1	10,3	2,6
Rímac	531	68,4	15,4	5,8	7,0	3,4
San Bartolo	20	40,0	10,0	20,0	20,0	10,0
San Borja	263	79,5	3,4	5,7	6,8	4,6
San Isidro	293	82,6	1,4	4,4	5,1	6,5
San Juan de Lurigancho	2 685	62,4	9,9	8,3	12,0	7,4
San Juan de Miraflores	827	59,9	8,9	10,2	13,7	7,4
San Luis	292	79,5	2,4	1,7	8,2	8,2
San Martín de Porres	1 070	67,8	7,9	4,7	11,8	7,9
San Miguel	264	71,6	4,5	4,5	13,3	6,1
Santa Anita	443	70,9	7,9	4,1	14,2	2,9
Santa María del Mar	5	60,0	0,0	40,0	0,0	0,0
Santa Rosa	118	13,6	0,8	3,4	1,7	80,5
Santiago de Surco	1 072	77,7	4,9	6,1	6,0	5,4
Surquillo	472	80,9	5,7	3,4	7,6	2,3
Villa El Salvador	777	59,6	7,7	11,6	14,9	6,2
Villa María del Triunfo	1 169	63,1	10,1	11,4	12,1	3,3

Fuente: INEI (2021).

Según los datos, el número de denuncias realizadas por delitos informáticos disminuyó en la capital Lima de 110 (enero-marzo 2020) a 83 (enero-marzo 2021). Las zonas con más denuncias por este delito entre enero y marzo de 2021 fueron Los Olivos (13) y Lima (9). En cuanto a la variación porcentual, con respecto a enero-marzo de 2020, los distritos de Chorrillos, El Agustino, San Miguel y Rímac muestran el mayor crecimiento.

Tabla 5.7.

Lima Metropolitana: Denuncias por comisión de delitos informáticos, según distrito. Enero - marzo, 2020-2021.

Distrito	2020	2021	Variación	
	Ene - Mar	Ene - Mar	Absoluta	%
Total	110	83	-27	-24,5
Ate	1	-	-1	-100,0
Barranco	2	-	-2	-100,0
Breña	8	3	-5	-62,5
Carabayllo	1	1	0	-
Chorrillos	1	2	1	100,0
Cieneguilla	1	-	-1	-100,0
Comas	4	4	0	-
El Agustino	1	2	1	100,0
Independencia	3	3	0	0,0
Jesús María	8	3	-5	-62,5
La Molina	-	4	4	-
La Victoria	2	1	-1	-50,0
Lima	14	9	-5	-35,7
Lince	3	1	-2	-66,7
Los Olivos	3	13	10	-
Miraflores	9	6	-3	-33,3
Pachacamac	-	1	1	-
Punta Negra	-	1	1	-
Puente Piedra	1	1	0	0,0
Rímac	5	6	1	20,0
San Borja	7	4	-3	-42,9
San Isidro	5	3	-2	-40,0
San Juan de Lurigancho	4	3	-1	-
San Juan de Miraflores	1	1	0	-
San Luis	1	-	-1	-100,0
San Martín De Porres	4	1	-3	-75,0
San Miguel	1	2	1	100,0
Santa Anita	2	-	-2	-100,0
Santiago de Surco	8	3	-5	-62,5
Surquillo	4	2	-2	-50,0
Villa El Salvador	2	2	0	0,0
Villa María del Triunfo	4	1	-3	-75,0

Fuente: INEI (2021).

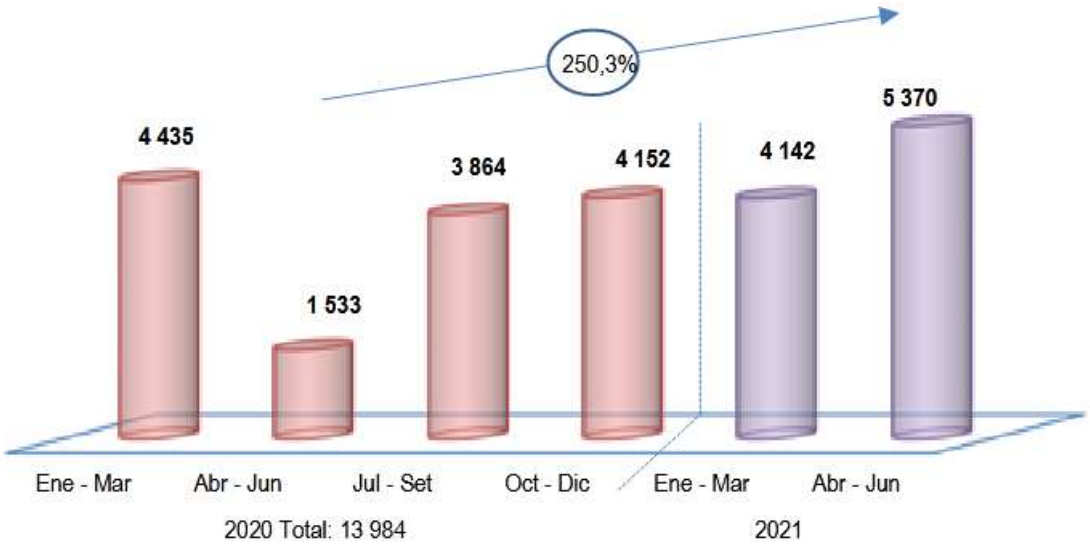
5.5. Vehículos robados y recuperados

5.5.1. Vehículos robados

A nivel nacional, la Policía Nacional del Perú reportó 5.370 denuncias por robo de vehículos en el segundo trimestre de 2021; aumentó en un 250,3 por ciento en comparación con el trimestre correspondiente de 2020.

Figura 5.4.

Perú: Denuncias de vehículos robados
Trimestre: 2020 – 2021.



Fuente: INEI (2021).

5.5.2. Robo de vehículos por departamentos

De abril a junio de 2021, la incidencia de robos de vehículos en Lima metropolitana fue de 1.667, un 155,3% más que en el trimestre correspondiente de 2020 (1.014 denuncias). Le sigue el departamento de Piura con 692 denuncias con un aumento del 247,7% (493 denuncias), Loreto con 436 denuncias, un incremento

de 358.9 por ciento (341). Los datos muestran que el número de casos en el departamento de Puno disminuyó en 6 (-35,3%).

Tabla 5.8.

Perú: Denuncias de vehículos robados, según departamento
Abril-junio, 2020-2021.

Departamento	2020	2021	Variación	
	Abr - Jun	Abr - Jun	Absoluta	%
Total	**1 533**	**5 370**	**3 837**	**250,3**
Lima Metropolitana 1/	653	1 667	1 014	155,3
Piura	199	692	493	247,7
Loreto	95	436	341	358,9
Lambayeque	92	380	288	313,0
La Libertad	109	360	251	230,3
Cajamarca	31	333	302	974,2
Huánuco	13	184	171	1 315,4
Junín	32	176	144	450,0
Ica	32	167	135	421,9
Ucayali	3	162	159	5 300,0
Amazonas	1	109	108	10 800,0
Departamento de Lima 2/	50	106	56	112,0
Prov. Const. del Callao	15	104	89	593,3
Ayacucho	5	83	78	1 560,0
San Martín	51	80	29	56,9
Madre de Dios	15	75	60	400,0
Cusco	38	71	33	86,8
Tumbes	33	44	11	33,3
Áncash	28	33	5	17,9
Pasco	8	31	23	287,5
Apurímac	7	25	18	257,1
Arequipa	5	23	18	360,0
Tacna	-	11	11	-
Puno	17	11	-6	-35,3
Moquegua	1	5	4	400,0
Huancavelica	-	2	2	-

Fuente: INEI (2021).

5.5.3. Modalidad de robo

Los hurtos de vehículos estacionados (4 mil 305) en abril-junio de 2021 fueron superiores a los hurtos por asalto y robo (1 mil 65), en comparación con el período correspondiente de 2020, los robos en las modalidades aumentaron (272,7% y 181,7%).

Tabla 5.9.

Perú: Denuncias de vehículos robados, según modalidad
Abril-junio, 2020-2021.

Modalidad	2020	2021	Variación	
	Abr - Jun	Abr - Jun	Absoluta	%
Total	**1 533**	**5 370**	**3 837**	**250,3**
Asalto y Robo	378	1 065	687	181,7
Estacionado	1 155	4 305	3 150	272,7

Fuente: INEI (2021).

5.5.4. Clase de vehículo

Las denuncias por robo de motos lineales aumentaron significativamente (1.595) abril-junio 2021/abril-junio del año 2020, que proporcionalmente significó el 330,9%. Otros tipos de vehículos que aumentaron significativamente fueron las camionetas y los turismos. La siguiente tabla muestra que el 38,7% de los hurtos de vehículos corresponden a motos lineales en abril y junio de 2021. En los meses correspondientes del año pasado, este porcentaje fue de 31,4%, lo que significa un aumento de 7,3 puntos porcentuales. Los porcentajes de robos de mototaxis (22,3%), turismos (17,4%) y furgonetas (10,9%) son menores en el segundo trimestre de 2021 que en el trimestre correspondiente de 2020.

Tabla 5.10.

Perú: Denuncias de vehículos robados, según clase
Abril-junio, 2020-2021.

Clase de vehículo	2020	2021	Variación	
	Abr - Jun	Abr - Jun	Absoluta	%
Total	**1 533**	**5 370**	**3 837**	**250,3**
Auto	276	936	660	239,1
Camioneta - SW	63	160	97	154,0
Camioneta - P-UP	57	198	141	247,4
Camioneta - Panel	19	60	41	215,8
Camioneta - Rural	52	167	115	221,2
Camión	35	53	18	51,4
Moto lineal	482	2 077	1 595	330,9
Mototaxi	390	1 195	805	206,4
Otros vehículos 1/	159	524	365	229,6

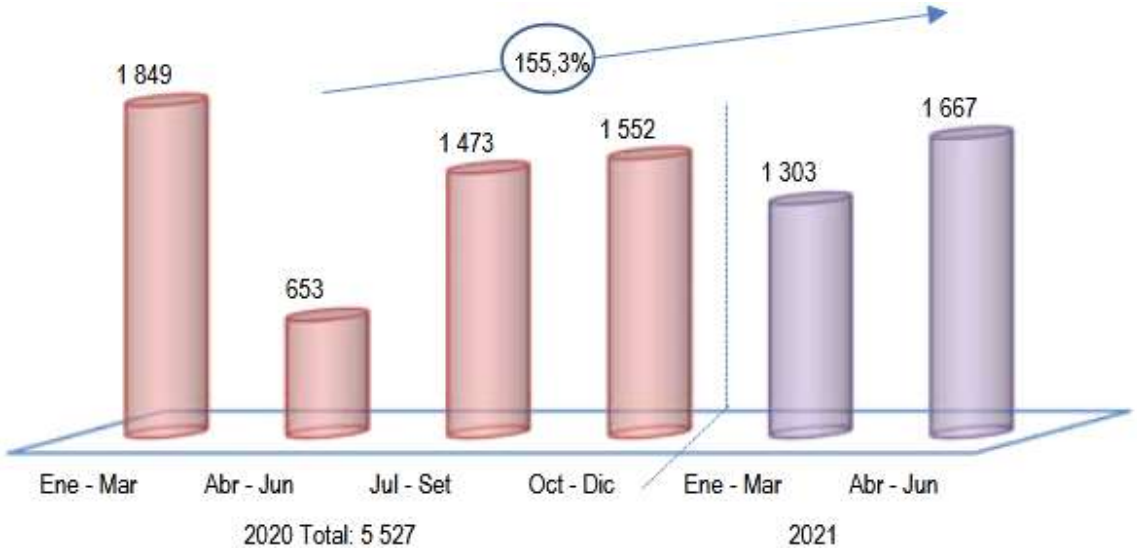
Fuente: INEI (2021).

5.5.5. Robo de vehículos en Lima Metropolitana

Según un informe de la Policía Nacional del Perú, en abril-junio de 2021 se recibió en Lima metropolitana un total de 1.667 denuncias de vehículos robados. Esta cifra aumentó un 155,3% respecto al trimestre correspondiente de 2020 (1.014 denuncias).

Figura 5.5.

Lima Metropolitana: Denuncias de vehículos robados
Trimestre: 2020 – 2021.



Fuente: INEI (2021).

A nivel regional, Villa El Salvador, Carabayllo, San Juan de Lurigancho, Comas y Los Olivos presentaron la mayor cantidad de denuncias por vehículos robados en abril-junio de 2021 (más de 100 denuncias), aumentó el número de denuncias por robo de vehículos en Lima. Sin embargo, las localidades de Santa Anita, San Luis, Lurigancho, Chaclacayo, Breña y Ancón muestran una ligera disminución durante el período mencionado.

Tabla 5.11.

Lima Metropolitana: Denuncias de vehículos robados, según distrito Abril-junio, 2020-2021.

Distrito	2020	2021	Variación	
	Abr - Jun	Abr - Jun	Absoluta	%
Total	**653**	**1 667**	**1 014**	**155,3**
Villa El Salvador	65	209	144	221,5
Carabayllo	74	193	119	160,8
San Juan de Lurigancho	85	186	101	118,8
Comas	36	120	84	233,3
Los Olivos	26	115	89	342,3
Puente Piedra	28	81	53	189,3
San Juan de Miraflores	25	77	52	208,0
San Borja	14	73	59	421,4
Ate	42	72	30	71,4
Chorrillos	15	71	56	373,3
Santa Anita	75	51	-24	-32,0
Lima	12	49	37	308,3
San Martín de Porres	28	46	18	64,3
Santiago de Surco	22	40	18	81,8
El Agustino	11	30	19	172,7
Villa Maria del Triunfo	7	28	21	300,0
Miraflores	3	26	23	766,7
La Molina	11	22	11	100,0
San Luis	25	21	-4	-16,0
Independencia	9	21	12	133,3
Lince	7	20	13	185,7
Surquillo	8	18	10	125,0
Pueblo Libre	1	17	16	1 600,0
Rimac	1	15	14	1 400,0
Jesús Maria	2	14	12	600,0
San Isidro	1	13	12	1 200,0
San Miguel	4	8	4	100,0
Pachacamac	5	7	2	40,0
La Victoria	-	7	7	-
Barranco	-	5	5	-
Lurin	-	4	4	-
Magdalena del Mar	-	3	3	-
Chaclacayo	3	2	-1	-33,3
Lurigancho	5	2	-3	-60,0
Santa Rosa	1	1	0	0,0
Breña	1	-	-1	-100,0
Ancón	1	-	-1	-100,0

Fuente: INEI (2021).

Capítulo 6

6.1. Inteligencia Artificial en Lima Metropolitana

La Inteligencia Artificial (IA), es una tecnología revolucionaria, que ha llegado para cambiar el mundo, tiene múltiples aplicaciones en una amplia variedad de campos, como:

- Dispositivos inteligentes,
- Motores de búsqueda,
- Brindando un poder extraordinario a los sistemas de video vigilancia, y
- Potenciando la investigación y el desarrollo que impulsan la economía y el crecimiento nacional.

En este contexto, la inteligencia artificial transforma la cadena de productos, no solamente en el entorno empresarial, sino también en la sociedad, a través que productos y servicios que contribuyen al bienestar ciudadano. Por ejemplo, en los grandes centros urbanos, permite a los cuerpos de seguridad obtener informes en tiempo real sobre situaciones irregulares. Para ello, la IA utiliza algoritmos aplicados a big data creando patrones, tendencias y perfiles que en las grandes ciudades puede ser empleados para el control de la inseguridad urbana. Esto permite a las autoridades, la rápida toma de decisiones.

6.2. Contexto general de la IA

La Inteligencia Artificial (IA) abre nuevas oportunidades en todas las áreas de negocio, contratos corporativos y políticas gubernamentales a nivel nacional y local. Es por ello por lo que se ha convertido en una prioridad para muchas naciones del mundo. La inteligencia artificial como tecnología tiene una enorme capacidad para transformar los negocios, la sociedad y la vida económica, y la velocidad del cambio es mucho mayor que cualquier revolución anterior. En este sentido, la ONU y otros organismos internacionales emitieron recomendaciones a

las economías de mercados emergentes para promover el uso de herramientas de inteligencia artificial para reducir sus desigualdades socioeconómicas y mejorar la competitividad de las empresas. Por lo tanto, a medida que surgen nuevas aplicaciones en IA, existe un interés creciente en explorar cómo este tipo de tecnología puede mejorar las interacciones con los servicios automatizados entre una empresa y sus clientes.

Así es como la inteligencia artificial (IA) da forma a las empresas y organiza la gestión innovadora de la sociedad. De acuerdo con el rápido desarrollo tecnológico y el reemplazo de las organizaciones humanas, la inteligencia artificial puede obligar a la gerencia a repensar todo el proceso de innovación de la empresa. También es importante considerar algunos de los riesgos existentes que puede causar y cómo mitigarlos para el uso adecuado de la IA.

6.3. IA y conocimiento

La pandemia de COVID-19 reveló muchas deficiencias en las operaciones de las unidades, tales como gestión de procesos, métodos de marketing de las empresas: marketing electrónico, cadena de suministro, distribución de productos, y en general, todos los procesos comerciales y financieros eran inciertos. En este panorama, las ventas de empresas y especialmente Pymes disminuyeron

fuertemente. No obstante, la crisis presentada por la pandemia no se limitó solo al campo económico, también dejó al desnudo los graves problemas sociales como la pobreza y la inseguridad, acrecentado la crisis de gobernanza en las grandes metrópolis.

Por lo anterior, el incremento del uso de tecnologías de control apoyados en herramientas de análisis de datos, pueden crear una nueva perspectiva en la toma de decisiones en los gobiernos locales, y así, disminuir el impacto de un grave problema como lo es la inseguridad en Lima metropolitana. Los sistemas de datos pueden proporcionar confiabilidad y flexibilidad en la toma de decisiones y permitir la simulación de escenarios futuros basados en el comportamiento combinado de variables claves y proporcionando herramientas flexibles que mejoran la aplicación de políticas de seguridad. La IA muestra análisis de datos para la toma de decisiones y brinda apoyo cuantitativo a gerentes y líderes en todos los campos, como ingenieros, analistas, consultores en gestión de proyectos, profesionales de ingeniería, profesionales del servicio sanitario y agentes del orden público, entre otros muchos más.

6.4. Perspectivas de la IA en Perú

La tarea que se está desarrollando en América Latina es muy extensa, si bien es cierto que la inteligencia artificial ha demostrado ser una tecnología transformadora que trae muchos beneficios en todos los campos, incluido el de la seguridad urbana. América Latina y sus gobiernos son muy reacios a adoptar nuevas tecnologías y por lo tanto el cambio es mucho más lento que en el primer mundo, la política pública no tiene un componente tecnológico suficientemente amplio y fuerte. En la implementación de la IA, por parte de los gobiernos de la región, solamente hay iniciativas aisladas y sin la articulación entre diferentes sectores gubernamentales, sin un marco político, legal y financiero adecuado para lograr la implementación y desarrollo de la IA a largo plazo.

Con la implementación de la inteligencia artificial, una adecuada gestión tecnológica y políticas futuras, sería posible realizar una adecuada planificación estratégica del desarrollo humano, así como realizar un adecuado seguimiento del avance de su implementación. América Latina y Perú deben salir del marasmo en el que se encuentran y enfrentar este nuevo milenio de una manera nueva, utilizando efectivamente tecnologías disruptivas. Es importante entender que no

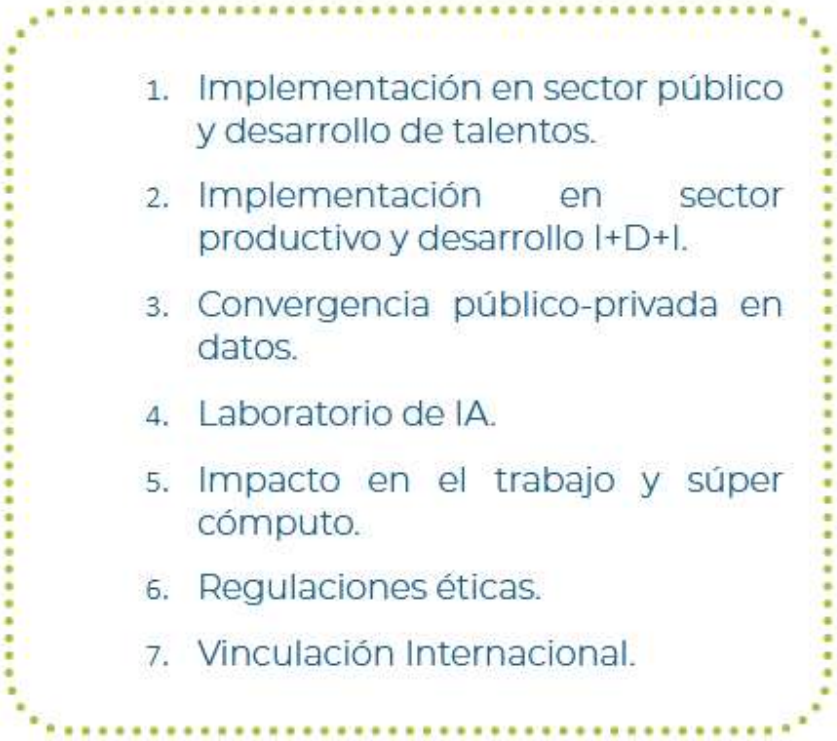
se trata de obtener indicadores de pobreza, desigualdad, competitividad, inseguridad o progreso en el uso de la tecnología, sino de desarrollar políticas adecuadas para resolver los problemas identificados en cada región y liderar el tan esperado desarrollo de la mano con las nuevas tecnología.

La IA ha demostrado una gran capacidad en el procesamiento de datos, extrayendo información de big data con poderosos algoritmos de búsqueda, la información obtenida se puede conducir hasta cualquier área en una compañía o gobierno. En este sentido, la CEPAL, en colaboración con el Instituto Tecnológico de Massachusetts y otros organismos internacionales, organizó un Taller Latinoamericano de Inteligencia Artificial en el verano de 2020, donde los países latinos pudieron presentar sus avances en el campo de la inteligencia artificial y sus planes y políticas sectoriales.

Algunos países latinoamericanos integran políticas públicas y estrategias de digitalización más amplias; mientras que otros identificaron estrategias de IA específicamente para el sector público. En general, los gobiernos, el sector privado, la academia y la sociedad civil están colaborando cada vez más en el campo de la inteligencia artificial para promover la investigación y el desarrollo, y además promover la adopción de marcos legales que puedan abordar cuestiones éticas que viene con el empleo de la IA.

6.5. Gobernanza: IA

Es importante que cualquier país cuente con un modelo de gobernanza de largo plazo liderado por instituciones especializadas en la materia e involucrando a sectores clave de la sociedad, como el gobierno en todos los niveles y poderes (legislativo, ejecutivo y judicial), universidades, industria, organizaciones civiles y ciudadanos en general. Los países latinos puedan aprovechar nuevas tecnologías, como la inteligencia artificial, con instalaciones modernas y competitivas, empresas que realizan I+D y que crean valor agregado y mejoran la economía nacional. Algunos ejemplos dignos de imitar son Chile, Brasil y Colombia, donde el Ministerio de Ciencia y Tecnología es el encargado de dar forma a las políticas públicas como la inteligencia artificial. Algo que debemos enfatizar está relacionado con el eje de desarrollo de la inteligencia artificial:



Latinoamérica, necesita la creación de una estrategia digital intersectorial y articulada con financiamiento adecuado y una política coherente y un marco legal que permita una migración y adopción adecuadas de tecnología de inteligencia artificial. Es por eso, que la prioridad es la implementación de modelos de gobernanza participativa estructurados por el gobierno en alianza con otros actores que incorporen conocimientos técnicos a través de procesos de consulta. El desafío del futuro es la colaboración participativa de todas las partes interesadas en el desarrollo y aplicación de la IA.

En este sentido, iniciativas regionales como la "Feria BID LAC" con el centro de monitoreo de casos de uso o SumMIT, sirven como foro para fortalecer las redes de diálogo y contacto, y la creación de proyectos de cooperación interregional, Estos son ejemplos de espacios de cooperación que deben ser promovidos y fortalecidos en el ecosistema de IA latinoamericano con las estrategias de IA vigentes y/o promover la implementación de la planificación conjunta en los países de la región. Cabe señalar que estos países muestran voluntad política, es hora de que el Perú le dé la importancia necesaria a un

gobierno inclusivo de inteligencia artificial que permita aprovechar y beneficiar esta tecnología.

6.6. Recursos humanos

Vale la pena señalar que la reunión de SumMIT destacó tres propuestas que deben considerarse para un buen diseño de políticas de IA:

1. La necesidad de proteger políticas que aseguren la responsabilidad social y ética en IA.
2. La importancia de definir políticas a través de un pensamiento colectivo holístico y multidisciplinario.
3. Desarrollo de pautas éticas razonablemente establecidas en AI.

Todo esto requiere una población educada y la capacidad de mantener los procesos políticos necesarios, lo que significa desarrollar una política de educación en IA. En este sentido, debemos repensar la importancia de la educación como factor crítico de desarrollo. Por lo tanto, la capacitación en IA es el mayor desafío que tendrán que enfrentar países como Perú y los gobiernos locales como es el caso de Lima metropolitana, en los próximos años.

La educación debe verse como un eje transversal para desarrollar una estrategia que aproveche las oportunidades creadas por la inteligencia artificial.

> Desde la independencia de los países latinoamericanos, la educación ha sido la base para la formación de los estados

El desarrollo de la inteligencia artificial es sistemático, por lo que es todo un desafío crear un ecosistema funcional para la formación del talento humano que asegure las libertades personales y la independencia regional. Para ello, uno de los retos es crear un programa de formación de calidad, porque la inteligencia artificial debe ser considerado un socio importante.

Otro punto importante es la formación de expertos en áreas que promuevan el desarrollo regional, donde se conozcan los perfiles profesionales de técnicos y especialistas necesarios para la región. A través de convenios entre academias y el sector privado, se crearán sinergias apropiadas para maximizar el beneficio de la inversión del gobierno en becas vocacionales, canalizando esa inversión hacia el desarrollo regional donde el sector público y privado desarrollan los técnicos y especialistas que necesita.

Con el propósito de promover el uso de IA en la seguridad urbana en Lima metropolitana, la educación debe basarse en el ambiente de trabajo e investigación requerido por el estado para este propósito. Esta es la única forma de lograr una rentabilidad adecuada y un retorno de la inversión del gobierno. La formación de talentos también debe enfatizar la necesidad de formar a los ciudadanos en nuevas tecnologías a través de la educación para que puedan participar en discusiones y debates relacionados con el uso y aplicación de las tecnologías disruptivas en la sociedad limeña.

La inteligencia artificial requiere expertos avanzados y el incremento la alfabetización de toda la población en este campo. Para ello, las medidas deben centrarse en la educación superior y los nuevos perfiles técnicos e invertir en las primeras etapas de la educación en Perú y promover la participación en todos los sectores. Al mismo tiempo, según posibilidades, los expertos coinciden en que la inteligencia artificial puede convertirse en un catalizador de cambios en el sistema educativo peruano.

Sus características pueden cambiar el método de enseñanza y fomentar un mejor seguimiento de los estudiantes con procesos de aprendizaje personalizados. Podría actuar no sólo como un elemento incluido en la educación para fortalecer la soberanía y la seguridad de la población, sino también como un agente de cambio en el sistema educativo en su conjunto.

Como norma práctica, el gobierno de Lima y en general el de Perú debe utilizar el potencial de la inteligencia artificial para resolver problemas asociados con la de inseguridad urbana, así como la posibilidad de prevenir hurtos y robos en la ciudad, vigilar el tránsito o monitorear las escuelas. En este sentido, también es necesario destacar la posibilidad de que las nuevas tecnologías permitan el acceso gratuito a la formación online sobre inteligencia artificial. Se pueden utilizar múltiples plataformas, así como iniciativas independientes.

Lo que también falta en Perú es la sistematización de la oferta existente y el uso de herramientas para principiantes que facilitan la convergencia de prototipos de aprendizaje automático y soluciones de IA, que resultan útiles para avanzar en programación y la educación de codificación, tratando de hacer que el aprendizaje automático sea más accesible a más personas.

Empero, para concretar este panorama se requiere invertir en infraestructura educativa y cambiar los currículos en todos los niveles educativos, pensar en estrategias de educación continua, y fortalecer la educación para todos al mismo tiempo. Las estrategias para la promoción de la inteligencia artificial en la región presentan varios desafíos para su implementación, tales como:

Universidades en la región de América Latina, especialmente universidades públicas que enfrentan matrículas masivas, bajos presupuestos e infraestructura insuficiente además de desafíos asociados con el desarrollo de la tecnología.

Cambiar la educación superior requiere la creación de capacidad institucional suficiente y la reforma del plan de estudios. También es importante enfatizar que comprender el proceso educativo es importante, antes de intentar

enseñar con IA, donde la tecnología avanzada debe ser una herramienta habilitadora, si no puede reemplazar la mano de obra. La tecnología hace que ciertas cosas sean más fáciles de lograr con un costo y tiempo significativamente menores, lo que permite que las universidades se concentren y mejoren su capacidad para la excelencia educativa. La región cuenta con recursos humanos competitivos como en cualquier parte del mundo, el reto es mantenerlos en nuestro país y colaborar como los mejores para fusionarse con centros de desarrollo global fuera de la región. Por esto, es necesario crear oportunidades competitivas para colocar academias e investigadores avanzados locales en los campos de la inteligencia artificial en LATAM.

En Lima es necesario fortalecer el ecosistema tecnológico y brindar incentivos suficientes para crear oportunidades que permitan desarrollar localmente el sector de IA en función de sus capacidades. La posibilidad de construir sistemas fuertes está fuertemente ligada a la idea de crear sinergias en todo el país y la región Latina. Por ejemplo, para las autoridades del gobierno local de Lima será difícil superar los obstáculos causados por la implementación de AI de forma aislada, es necesario para el desarrollo de la inteligencia artificial fortalecer la cooperación nacional e internacional.

Para mejorar los ecosistemas de IA, también es necesario facilitar la comunicación y el diálogo entre la industria, la sociedad civil, el gobierno nacional, el gobierno limeño y el sector académico; desafío que enfrenta todos los sectores ligados a la innovación y tecnología. En particular, promover la cooperación entre la industria y las universidades, fortalecerá través la formación continua de personas cualificadas.

Para los gobiernos locales, el vínculo entre empresas y universidades se fortalece mediante la investigación en inteligencia artificial. En este sentido, es importante:

1. Promover la transferencia tecnológica entre los países latinoamericanos para el desarrollo de la región.

2. Invertir en investigación científica sobre inteligencia artificial, porque el nivel de aporte científico es bajo. Esto se refleja en el bajo número de innovaciones que tienen consecuencias para el desarrollo de los países de la región.

En suma, se deben intensificar los sistemas científicos y educativos relacionados. El desarrollo de aplicaciones y los proyectos de inteligencia artificial requieren economías de gran escala que requieren mayores recursos mancomunados. Allí se observa claramente la necesidad de cooperación regional para dar forma al ecosistema latinoamericano.

6.7. Panorama de la IA

La infraestructura digital es un factor importante en el desarrollo de la inteligencia artificial. Las siguientes recomendaciones son puntos importantes que las autoridades locales de Lima pueden tomar en cuenta al momento de mejorar sus sistemas de seguridad urbana, apoyándose en el empleo de la IA. Países pioneros en el desarrollo de esta tecnología han desarrollado estrategias para fortalecer la infraestructura, no solo en cuanto a su componente de conectividad, sino también en los siguientes puntos, entre otros:

1. Construir una infraestructura de datos y aumentar las velocidades en megabits. por segundo, como las redes 5G habilitadas para IA en el Reino Unido.

2. Desarrollo de infraestructura de hardware que optimice el flujo de algoritmos, como computación neuromórfica en los Estados Unidos.

3. Infraestructuras distribuidas de hiperescala (nube), como las diseñadas en Francia.

La infraestructura es reconocida mundialmente como un facilitador del desarrollo sostenible. La innovación e infraestructura apalanca el crecimiento económico, el desarrollo social, y en gran medida las inversiones en infraestructura promueven el desarrollo industrial sostenible y el desarrollo tecnológico. Sin embargo, se reconoce que muchos países en desarrollo aún carecen de infraestructura básica como carreteras, TIC, saneamiento, electricidad y agua, lo que puede crear tensiones en la prioridad de las inversiones.

En este contexto, es importante mostrar que Lima necesita abordar aspectos relacionados con la infraestructura, considerándose los más importantes:

1. Políticas nacionales y locales basadas en infraestructura digital que contribuyen a la apertura digital.

2. Atender la falta de infraestructura social en materias tales como salud, educación, servicios públicos, como agua, electricidad o seguridad urbana donde el desarrollo de la inteligencia artificial puede ser un aliado. Llevar acabo la transformación digital y desarrollar infraestructuras de comunicación debe ser una de las áreas clave que los poderes públicos deben abordar.

Todo el país y las grandes metrópolis como Lima deben tener redes y comunicar los beneficios de la inteligencia artificial a la población. También se necesita infraestructura digital para la inteligencia artificial es difícil su promoción y desarrollo en centros urbanos con servicios públicos deficientes. Por lo tanto, es necesario asegurar la formación académica de los cuerpos de seguridad, de los actores gubernamentales y de los residentes de Lima.

Los anteriores son también factores que le permiten a cualquier ciudad del mundo competir y disfrutar de los beneficios de la Cuarta Revolución Industrial. Para que esto pueda funcionar en los 43 distritos de Lima, se debe contar con una mejor asignación y uso de los recursos para mejorar la infraestructura que permite que se amplíe la conectividad a toda la población. Es especialmente importante que los gobiernos aborden la brecha digital en áreas que se encuentran desasistidas, donde estos sistemas se necesitan con mayor urgencia.

El desafío de la infraestructura de América Latina es un factor importante en la promoción de la innovación y los servicios digitales basados en IA. Las políticas de infraestructura digital en los países de la región deben abordarse de manera inclusiva y justa, con el objetivo de reducir la brecha digital y promover el desarrollo de infraestructuras relacionadas con la IA. Asimismo, al momento de planificar políticas nacionales como el despliegue de redes 5G, es importante considerar los estándares internacionales y el uso de bandas de frecuencia en el desarrollo de inteligencia artificial.

Por ejemplo, el gobierno local de Lima debe alentar a las empresas privadas nacionales y regionales a fortalecer la formación del ecosistema latinoamericano en IA, enfatizando la importancia de crear un vínculo entre el sector privado y la educación, y primordialmente promover en las universidades y centros politécnicos el desarrollo de estudios de pregrado y es de posgrado en la áreas de tecnologías basadas en IA. La construcción de vínculos entre ambos debe enfocarse en desarrollar programas de aprendizaje y/o capacitación relevantes y actualizados para brindar valor real a los estudiantes y mejorar el talento y la creatividad de la población.

En este tema, debemos promover la participación de las grandes empresas en iniciativas académicas y prácticas a través de debates, programas, cursos, etcétera y hacer llegar estas iniciativas hasta la educación superior. Existe una brecha muy amplia entre el sector privado y el académico, esta último debe ser el encargado de asegurar que el sector público esté al tanto de todo lo relacionado con la innovación.

Por otro lado, hay que enfatizar que el sector privado es un agente catalizador en la promoción del desarrollo de la inteligencia artificial. En este sentido, estas iniciativas suelen ser de muy corto plazo (cuatro a seis años como máximo) y las expectativas son moderadas para lograr una base sólida sobre la cual trabajar.

Por lo tanto, para que el gobierno local de Lima pueda implementar cualquier tipo de servicio público y garantizar su eficiencia apoyándose en la IA, el sector privado debe liderar y promover iniciativas y trabajar de la mano con las autoridades locales, cuestión de promover y fortalecer el uso y la adecuada regulación de la IA en Lima.

A nivel de suramericano y nacional, cada estado puede compartir sus experiencias, entre otras cosas, para educarse unos a otros y exponer sus avances significativos en el desarrollo de capacidades basadas en las nuevas tecnologías que otros gobiernos pueden imitar y aceptar. Por lo tanto, se necesita promover interacciones entre el sector privado y las universidades para atraer estudiantes exitosos que en la actualidad cursan estudios superiores en el extranjero.

En este sentido, es importante señalar lo estratégico que resulta la implementación de becas de estudio, en colaboración con universidades, y además permitir a los estudiantes participar en proyectos durante el año académico y

acumular créditos por ello. Así, los estudiantes pueden comenzar a formarse en inteligencia artificial y buscar empleo en empresas privadas o en las instituciones públicas. La estrategia para reclutar, capacitar y retener empleados con las habilidades necesarias es invertir dinero, brindar salarios competitivos, y programas de capacitación que sean satisfactorias y no alienten al empleado a buscar oportunidades fuera de Perú.

6.8. Posibles complicaciones para la IA en Lima

Con respecto a las limitaciones potenciales para el desarrollo y la implementación de sistemas de seguridad urbana basados en IA en la metrópolis de Lima, se ha observado que pocas empresas se dedican principalmente al desarrollo de proyectos IA básica y, más bien, la mayoría de las empresas desarrollan proyectos de IA aplicada. Este fenómeno, en general sucede en toda Latinoamérica, y se debe a que la mayoría de las empresas ejercen mucha presión sobre el retorno de la inversión y la captura de valor.

Por esta situación, existe un gran riesgo de que América Latina se quede rezagada en la investigación más básica de IA, especialmente aquella que abordaría problemas generales de la región, como los problemas sociales, de inseguridad y económicos que tienen implicaciones para la IA. Desde este punto de vista macroeconómico, existe el riesgo de que la región no pueda innovar y adaptarse al uso adecuado de esta tecnología, porque la IA está creciendo exponencialmente, afectando la economía en el mediano y corto plazo.

Por lo tanto, Perú y los gobiernos locales deben realizar los cambios necesarios en materia regulatoria y modelos económicos para no verse perjudicados por el rezago. El mayor riesgo está en la seguridad de los datos utilizados. Muchas empresas podrían ofrecer soluciones de IA al público sin tener un sistema de seguridad para prevenir delitos como el robo y el fraude. Es necesario encontrar la manera de evaluar las implicaciones éticas del uso de datos sin obstaculizar el desarrollo del uso de inteligencia artificial en América Latina y en Perú. Por otro lado, hay que reconocer que los problemas tecnológicos que se presentan en Perú y localidades como Lima son significativamente diferentes a los de otros países europeos o los Estados Unidos.

Por lo tanto, las soluciones deben originarse dentro Perú y, por lo tanto, se recomienda evitar las soluciones del extranjero y tratar de encontrar soluciones dentro del propio país. Se puede pensar que los avances en inteligencia artificial y automatización amenazan con reemplazar muchos puestos de trabajo en el sector de la seguridad urbana, sin embargo, esto no es cierto.

La IA en el campo de seguridad urbana, fomentan la creación de muchas nuevas ocupaciones y hace más eficiente el desempeño de la fuerzas de orden publica, así como también de los servicios sanitarios y prevención y control de catástrofes, A este respecto, el papel de la educación es clave para la transición al nuevo mercado laboral de IA, enfatizando que la futura fuerza laboral puede desarrollar habilidades para resolver problemas, empatía, pensamiento sistémico y habilidades digitales. Además, de desarrollar la sensibilización, transformación y readiestramiento de personas que demuestren el impacto de la implementación de la inteligencia artificial en la eficiencia y el rendimiento laboral.

A medida que continuamos analizando las políticas públicas en América Latina, se recomienda enfáticamente desarrollar un ecosistema de datos sólido, y para esto, en el caso de Lima, deben considerarse las políticas de publicidad de datos abiertos para ganarse la confianza de la población. Contribuyendo de esta forma a mejorar la eficiencia de los servicios públicos digitales relacionados con la salud, la educación y la seguridad pública. Otro factor positivo para impulsar estas iniciativas sería la adaptación de los planes de estudios universitarios que contemplen formación sobre inteligencia artificial y análisis de datos.

En este contexto, se enfatiza la importancia de crear políticas que promuevan el desarrollo del ecosistema de información, por lo que se recomienda trabajar en dos ejes: problemas y desafíos relacionados con los datos y la privacidad. Destacando principalmente los problemas y desafíos relacionados con los datos, en la interoperabilidad y el acceso, la gestión flexible de la información, la transformación de las organizaciones y la gobernanza basada en la ética y los derechos humanos.

En este sentido, destaca que, en ciudades como Lima, existen problemas de interoperabilidad y disponibilidad de datos por falta de organización funcional. Por lo tanto, las recomendaciones se refieren a la necesidad de promover una cultura organizacional basada en la recolección, análisis, procesamiento e interoperabilidad de datos, que es una herramienta importante para la trasformación del Estado y de los gobiernos locales.

6.9. Desarrollo de estrategia de IA necesaria en Lima

Para que el País se encamine por el camino del desarrollo, es necesario crear estrategias específicas de IA, como lo hacen los países del primer mundo. En América Latina tenemos solo dos países que han desarrollado estas estrategias: Colombia y Uruguay. En otros países, como México, Argentina, Brasil y Chile, están totalmente desarrollados, y otros países, como Perú, todavía no los incluyen en sus prioridades, a pesar de las recomendaciones de muchos organismos internacionales como CEPAL, BM, BID, OCDE, PNUD, UIT, etcétera.

Si bien la inclusión de herramientas de inteligencia artificial en todos los ciclos y campos de la producción es reciente, la tendencia de su crecimiento y multiplicación es evidente. Teniendo en cuenta las implicaciones culturales específicas de la IA, hay al menos tres aspectos que necesitan ser reconsiderados:

1. Los cambios en la creación y producción de cultura a través del aprendizaje automático y el aprendizaje profundo, para promover la creación de bienes de valor excepcional en varios idiomas y regiones culturales.

2. La posibilidad de que el crecimiento de tales demostraciones y sus modelos de negocio alternativos puedan proporcionar un contrapunto necesario a la lógica de productividad de las grandes empresas tecnológicas.

3. Los aspectos relacionados con los datos culturales que alimentan a la IA, y promueve innumerables oportunidades para el desarrollo de los sectores cultural y creativo a través de impulsos en la productividad, personalización de productos o contenidos, creación de empleos calificados y oportunidades creativas.

Aunque la cultura es punto central en discusión en este aparte, lamentablemente no ha jugado el papel que merecía en la declaración de principios y estrategias de AI. A pesar de las oportunidades emergentes, es necesario señalar banderas rojas a los obstáculos y peligros del uso de la inteligencia artificial. En

general, los artistas y productores culturales no tienen una comprensión sólida del uso del aprendizaje automático y los ecosistemas culturales aún están incompletos.

La regulación de derechos de autor en el campo de IA también causa problemas por ejemplo al definir la propiedad y los reclamos jurisdiccionales de los desarrolladores de tecnología. La concentración económica sigue afectando a los actores tradicionales de la IA; es posible que la brecha digital/creativa se amplíe, además de la preocupación por la producción de contenido. Especialmente cuando se plantean sus beneficios, la inteligencia artificial a menudo se considera erróneamente neutral. Evidentemente, aunque se presenta como un mecanismo de apoyo a la maximización de tareas, se basa en datos representados por videos, sonidos, imágenes, textos, contextualmente etiquetados y no imparciales. La ética de la inteligencia artificial ha estado en la agenda de documentos oficiales y constituye motivo de preocupación desde hace mucho tiempo**.**

En este desarrollo global de asimilación tecnológica, el Perú debe adaptarse a las tendencias mundiales y modernizar su enfoque estatal, las políticas nacionales deben tomar en cuenta los siguientes análisis:

1. Inclusión de la inteligencia artificial en el desarrollo socioeconómico de la región. Los países de América Latina y el Caribe deben madurar sus estrategias relacionadas con la presencia de la IA en el crecimiento socioeconómico de la región. Desarrollando políticas públicas que fomenten las inversiones en IA, las alianzas de las empresas grandes del sector privado con universidades y socios globales son un incentivo para el desarrollo de las nuevas habilidades necesarias para la IA. Se debe fomentar el diálogo entre sectores para evaluar los beneficios y desafíos potenciales de AI en el País.

2. Inclusión de la cultura en las estrategias de desarrollo de la inteligencia artificial. Es imperativo reconocer el impacto que tiene la cultura en la naturaleza altamente disruptiva de las tecnologías digitales impulsadas por IA. Los programas de cultura de IA deben ganar impulso en los países como Perú. La cultura debe abordar las preocupaciones con una fuerza y ética. Desafortunadamente, los desarrolladores de AI tienden a ignorar la variable de la cultura, lo que significa que sus prescripciones pueden ser meras declaraciones

de intenciones sin aplicación concreta en un mundo caracterizado por la heterogeneidad en todos sus dominios, especialmente la cultura.

3. Promoción de la diversidad cultural en las principales plataformas. Los nuevos desarrollos que utilizan inteligencia artificial tienen un impacto en las garantías de la diversidad cultural. Actualmente, gran parte de la disponibilidad y el consumo de expresiones culturales se logra a través de grandes empresas de tecnología, con información creada en la cadena de suministro cultural, monitoreada por inteligencia artificial y distribuida a hiperaudiencias de manera segmentada. De aquí se puede concluir cuán importante es el papel que juega la inteligencia artificial en promover el desarrollo de la cadena productiva cultural de los países latinoamericanos.

4. Construir ecosistemas de conocimiento local. Es necesario fortalecer la capacidad de producción de información cultural y estadística en diversas áreas. El primer paso es la digitalización de todo el material producido en las instituciones culturales: sin colecciones digitalizadas, no es posible utilizar estos datos a través de herramientas de inteligencia artificial que dependen de las ecologías del conocimiento. Una práctica de código abierto puede proporcionar a los desarrolladores locales estadísticas y otras bases de conocimiento. Además, dado que el uso de IA en la cadena de producción cultural implica la recopilación, gestión y uso de datos, es importante que los proyectos desarrollados en LAC estén guiados por marcos éticos de IA.

5. Mapeo y trabajo en red de operadores. Poco se puede decir sobre la presencia de la IA en la cultura de ALC sin una investigación que evalúe las iniciativas existentes en la región tanto en las artes como en las industrias creativas. Este no es solo un estudio que actúa como un observatorio de tendencias, sino principalmente como base para un programa piloto para desarrollar inteligencia artificial en Latinoamérica. Este mapeo puede ayudar a estimular estrategias tanto a nivel local como en redes de conexiones locales y globales.

6. Promoción de actividades de investigación y educación. En la promoción de la IA y la cultura se debe considerar iniciativas educativas y de investigación en las siguientes áreas: acercamiento de

la IA a quienes tienen menos acceso a ella y poco conocimiento de sus herramientas; hacer que la inteligencia artificial sea más completa, usable e interactiva; atender las necesidades de artistas y emprendedores creativos locales e inversión en actividades educativas que promuevan la creación a través de la adopción de IA.

6.10 La paradoja

En 2018, el Pew Research Center (PRC) descubrió que entre el 65 y el 90% de los encuestados en países con economías avanzadas creen que es probable o seguro que los robots y computadoras asuman muchos de los trabajos que actualmente realizan los humanos. La posibilidad de que las máquinas eliminen puestos de trabajo no es una mala noticia si estas tecnologías proporcionan niveles de vida más elevados y mejores.

Pero una encuesta en la República Popular de China muestra que las personas no esperan beneficiarse, la mayoría de las personas creen que la automatización aumentará en gran medida la disparidad entre ricos y pobres y hará que sea aún más difícil encontrar empleos, aunque al menos un tercio de encuestados creen que se crearán nuevos puestos de trabajo mejor pagados. ¿Por qué la gente es pesimista sobre las perspectivas laborales después de una década de crecimiento del empleo? Una posibilidad es que la avalancha de artículos, libros y noticias alarmistas sobre el desempleo que provocará la tecnología abrumó a la población. Otra posibilidad es que el pesimismo de la población refleje las difíciles lecciones de la historia reciente.

A la gente le puede preocupar que la introducción de nuevas tecnologías con una capacidad de desempeño igual al desempeño humano creará una enorme riqueza para una minoría mientras reduce las oportunidades y la riqueza común para el resto de la población. La historia económica confirma que esta opinión no es ni falsa ni errónea. Hay muchas razones para preocuparse acerca de si el progreso tecnológico mejorará o debilitará las perspectivas de empleo e ingresos de la mayor parte de la fuerza laboral.

Las tecnologías nuevas y emergentes aumentan el desempeño económico general y aumentan la prosperidad de países. Por lo tanto, ofrecen a los ciudadanos

la oportunidad de alcanzar un mayor nivel de vida, mejores condiciones de trabajo, mayor seguridad financiera y mejor salud y longevidad. Pero para que los países y sus poblaciones alcancen este potencial, dependerá de las instituciones públicas, la inversión social, la educación, la ley y la gobernanza pública y privada, para convertir la riqueza en un bien común , en lugar de aumentar la desigualdad.

En el debate actual, innumerables opiniones de expertos y artículos de prensa ofrecen predicciones alarmantes sobre la proporción de trabajos actuales que pueden ser afectados por las nuevas tecnologías como la inteligencia artificial y la robótica. Si bien estas predicciones acaparan los titulares, brindan información limitada. La pregunta que nos preocupa es: ¿Qué significan estos cambios en el lugar de trabajo para las perspectivas de empleo, los ingresos y las oportunidades de carrera de los trabajadores con diferentes habilidades y recursos? Y también cómo gestionar este proceso para mejorar las oportunidades de empleo en general.

Para ir más allá del enfoque simplista de hablar sobre los puestos de trabajo, un punto de partida útil es examinar los diversos mecanismos mediante los cuales la automatización cambiar el trabajo humano. Este proceso funciona a través de tres canales separados pero relacionados: sustitución, complementariedad y creación de nuevas tareas. De los tres, sólo el primero (sustitución) es generalmente reconocido en el discurso popular, lo que creemos conduce a un pesimismo excesivo.

La automatización reemplaza a los trabajadores en una clase de tareas, que a menudo involucran actividades físicamente exigentes y repetitivas, por ejemplo: proveer a los trabajadores con excavadoras mecánicas. Este proceso aumenta la productividad y generalmente deja a los trabajadores con trabajos más seguros e interesantes.

Pero la transición no es inofensiva, en Inglaterra, en el siglo XIX, cuando la maquinaria textil industrial reemplazó a los hiladores, fabricantes de cintas y tejedores manuales, el cambio fue una bendición para la productividad y los consumidores, pero una dificultad grave y continua para los trabajadores textiles. Sin embargo, el reemplazo no es del todo una verdadera historia, y, de hecho, las máquinas rara vez reemplazan a los trabajadores humanos uno a uno. La automatización a menudo aumenta las capacidades cognitivas y creativas de los trabajadores.

Por ejemplo, los arquitectos que usan programas de diseño asistido por computadora (CAD) pueden diseñar edificios complejos más rápido que los dibujos en papel. Las máquinas aumentan el valor del conocimiento humano en el desarrollo y la gestión de procesos de producción complejos y proporcionan herramientas que las personas pueden usar para convertir sus ideas en productos y servicios.

La automatización aumenta el poder de las ideas y salva la distancia entre la planificación y la ejecución. Con el tiempo, la automatización cambió fundamentalmente la ventaja relativa del trabajo humano al dominio físico cognitivo, agregando gradualmente requisitos de razonamiento y capacitación a la mayoría de los trabajos. Si el trabajo fuera estático, este sería el final de la historia. Pero las nuevas tecnologías por lo general habilitan o requieren nuevas tareas que requieren conocimiento, creatividad y comprensión humana.

En el siglo XIX, los avances en la metalurgia y el uso generalizado de la electrificación crearon una nueva demanda de operadores de telégrafos, operadores e ingenieros eléctricos. Incluso en el siglo XX, cuando la maquinaria agrícola desplaza a los agricultores, es un punto de partida útil para examinar en profundidad los diversos mecanismos por los cuales la automatización cambia el trabajo humano. Este proceso funciona a través de tres canales diferentes, pero está vinculado a la mecanización y al crecimiento de los ingresos, que han creado nuevos puestos de trabajo en fábricas, oficinas, medicina y finanzas.

En el siglo XXI, cuando las computadoras y el software desplazaron a los trabajadores que realizaban tareas repetitivas, surgieron nuevas oportunidades simultáneamente en trabajos nuevos y cognitivamente intensivos, como diseño, programación y mantenimiento de maquinaria avanzada, análisis de datos y muchos otros. ¿Quizás las cosas son diferentes ahora? En épocas anteriores, la mecanización y la automatización eliminaron gran parte del trabajo no deseado y esencialmente crearon trabajos nuevos y más deseables, mientras aumentaban la productividad y permitían un nivel de vida. Creemos que la era actual es diferente en dos aspectos: la polarización del empleo y la tecnología.

Capítulo 7

7.1. Aplicación de IA en la seguridad urbana: Lima

En los últimos años, el problema de la seguridad en los grandes centros urbanos como Lima metropolitana, ha sido un tema principal en la agenda del gobierno. Para atender esta problemática, se han diseñado diferentes políticas públicas, teniendo como móvil el bienestar social. Como veremos, estas políticas potenciales también pueden afectar las normas de convivencia y los derechos de los ciudadanos. El objetivo principal de este capítulo fue analizar la tecnicidad de la seguridad ciudadana a través de las nuevas tecnologías y su relación con las políticas públicas, que muchos países utilizan para el control social.

Esto ha creado nuevos parámetros para la justicia, que debe adaptarse a los nuevos paradigmas tecnológicos. Por supuesto, la tecnología es ahora un factor clave en el diseño y desarrollo de políticas públicas relacionadas con la incertidumbre y la justicia. A continuación, describimos cómo se han desarrollado las TIC en el campo de la seguridad ciudadana y dónde se inició su aplicación durante las sociedades disciplinarias.

En la actualidad se ha establecido un nuevo paradigma de prevención que utiliza novedosas estrategias para hacer frente a la delincuencia y las consecuencias derivadas de esta. Mediante la implementación de nuevas tecnologías que conforman los sistemas de seguridad electrónica esenciales que intervienen en la seguridad pública, es conveniente conocer cómo se ha adaptado la sociedad a esta nueva perspectiva en el ámbito de la seguridad.

7.2. La seguridad ciudadana y las tecnologías

Los cambios sociales durante los últimos 20 años han afectado la naturaleza del crimen, mientras que las tecnologías actuales transforman los límites y las fronteras. Como resultado, los conceptos de seguridad se han reformulado, los

estilos de vida de los ciudadanos también han cambiado en las instituciones cambiaron su perspectiva sobre los problemas de delincuencia.

Hoy, vemos que se tiene en cuenta la participación de ciudadanos y comunidades al hacer las políticas de seguridad, podemos ver esto, en la nueva forma de tocar el problema y la comprensión del papel de la justicia en seguridad. Pero vemos cómo el desarrollo de las nuevas tecnologías basadas en la comunicación e información, erigieron paulatinamente a las tecnologías disruptivas como el medio para solucionar los problemas de seguridad urbana. Y de esta manera garantizar la prevención, la paz y una mejor calidad de vida para sus habitantes.

Las tecnologías de la información y la comunicación se han convertido en un papel clave en el diseño y desarrollo de políticas públicas relacionadas con los problemas de inseguridad dirigidas a reducir el nivel de criminalidad. Así vemos que los estados se han vuelto más técnicos con métodos y planes tanto para prevenir el crimen como para castigar el crimen dentro de su jurisdicción.

Para una comprensión más profunda de la aplicación de los avances tecnológicos por parte de la autoridad en el campo de la seguridad ciudadana, vale la pena considerar que en general el concepto de seguridad estaba relacionado con un valor, una meta deseada que indicaba incertidumbre, desprotección, inseguridad y peligro. La reducción de la incertidumbre es difícil de identificar porque lo que amenaza la certeza cambia y está históricamente determinado.

De esta manera, las TICs se han conformado como herramientas para reducir la incertidumbre y los riesgos sociales, como protección frente a las amenazas. La información/conocimiento que se genera para promover la seguridad y protección, debía ser constantemente desarrollada y actualizada de acuerdo con las mutaciones de los delitos y amenazas futuras.

Del mismo modo, enfatizando el concepto de seguridad ciudadana, se entendía la participación ciudadana como partícipe del derecho y como productora de seguridad. La misma ha sido definida como el derecho de los miembros de la sociedad a actuar todos los días de tal manera que su privacidad, derechos y propiedad estén en el menor peligro posible. Esto se fundamenta en el deber del Estado de satisfacer las necesidades de los ciudadanos frente a la transferencia de poder que el ciudadano entregaba a las personas encargadas de administrar el aparato estatal. Este concepto excede la idea de seguridad pública y puede verse

en contraste con la doctrina de seguridad nacional implementada hace décadas en América Latina, que se refiere a una garantía del orden público en un país militarizado.

7.3. La seguridad desde la perspectiva tecnológica

El uso de las nuevas tecnologías se ha incrementado significativamente en las últimas décadas y esto ha supuesto un cambio en los hábitos sociales, especialmente comerciales, económicos y de comunicación. La introducción de los medios de pago electrónicos, así como cajeros automáticos, correo electrónico, teléfonos móviles, GPS, comercio electrónico, etc., es prueba de esa gran red de Internet que conecta las tecnologías de la información y la comunicación.

Muchos de estos dispositivos se crearon originalmente con fines militares, luego fueron llevados a la sociedad civil con fines comerciales. Mattelart explicó que la Agencia de Seguridad Nacional (NSA) del gobierno de EE. UU., creó lo que hoy conocemos como Internet: Una de sus misiones era organizar la innovación tecnológica contra un enemigo "globalmente catalogado", comunismo mundial.

Así, el complejo industrial militar se construyó como resultado de la sinergia entre la investigación, la industria y los servicios de inteligencia militar o civil. Como parte de esta colaboración, Arpanet, el predecesor de Internet se inventó en 1958, originado un punto de inflexión para el DARPA (Defense Advanced Research Projects Agency), que es hoy el centro de la red y base de datos del proyecto de integración en seguridad desde la perspectiva tecnológica. Los dispositivos producidos por la industria de la seguridad electrónica incluían sistemas de intrusión, videovigilancia, control de acceso, identificación biométrica, geolocalización, comunicación y sistemas de gestión para centrales de alarma.

A continuación, analizaremos los sistemas de seguridad urbana más importantes, basados en IA que pueden ser implementados en Lima metropolitana, además de sus funciones especiales, así como su uso en dispositivos de vigilancia en el campo de la seguridad.

7.3. Sistemas de geolocalización

El Sistema de Posicionamiento Geográfico se basa en un sistema mundialmente conocido como GPS (Global Positioning System) o Sistema de Posicionamiento Global. Consiste en una red de satélites denominada NAYSTAR, que orbitan aproximadamente a 20.200 kilómetros de la Tierra, con receptores GPS capaces de determinar la posición y altitud de cualquiera punto en la tierra las 24 horas del día y bajo cualquier condición climática.

La triangulación da la altura, latitud y grados de longitud de los objetos ubicados en mapas digitalizados. La difusión del GPS está particularmente relacionada con nuevos sistemas operativos como Android, que es usado en los teléfonos móviles y en aplicaciones web importantes como Twitter, Google y Facebook para publicar automáticamente la ubicación de un dispositivo.

Se empezaron a implementar los sistemas para garantizar la seguridad ciudadana, y paulatinamente se empezó a adherir este tipo de tecnología a los patrulleros de fuerzas de seguridad para controlar las actividades y sus recorridos. En este sentido, se observó cómo la ubicación geográfica se convirtió en una herramienta de control a través de la localización tanto para los ciudadanos como para los agentes de seguridad del Estado.

7.4. Sistemas de videovigilancia

Los sistemas de videovigilancia se convirtieron en la vigilancia de todos los ciudadanos y de las instituciones, alcanzando niveles de control social sin precedentes. Si bien los sistemas de videovigilancia se utilizan como parte de una política preventiva, suelen convertirse en un elemento disuasorio porque su finalidad es proteger los datos durante un tiempo determinado, para que después de que ocurra o se sospeche de un delito, buscar los registros de imágenes e identificar a los sospechosos del resto de la sociedad.

El mecanismo se basa en el control de la información con vigilancia. Los sistemas de videovigilancia innovaron y comenzaron a cambiar sus estructuras y características, instalándose paulatinamente en diversos dispositivos móviles, incluidos drones y unidades patrulleras de los servicios de seguridad con software especialmente diseñado para aplicaciones militares.

Estos sistemas, al igual que los sistemas fijos, cuentan con programas de reconocimiento facial de personas y programas de reconocimiento de patentes vehiculares. Ambos están vinculados en línea a una base de datos que se actualiza constantemente y se combina con los datos recibidos en los dispositivos móviles, de forma que toda la información se vincula automáticamente en tiempo real a través de imágenes a un centro de control.

Asimismo, ante una alerta se activan automáticamente las alarmas de la unidad patrullera más cercana para ir a la ubicación y prestar apoyo a otros policías si es necesario, puesto que incorporan el sistema GPS. Los patrulleros por pueden estar equipados con un moderno sistema de vigilancia con 8 cámaras: 6 en el techo que cubren 360 grados alrededor del auto, un domo también ubicado en el techo, que son controlados desde el auto con una pantalla interactiva (pantalla táctil) o desde un centro de control remoto, y una cámara fija en el interior del vehículo que también graba sonido.

Otros dispositivos más novedosos para acceder a lugares desde el aire son los drones, están en constante desarrollo y son diseñados para diferentes aplicaciones en el campo de la seguridad de los ciudadanos. De esta manera, lo que no se puede monitorear en tierra se puede monitorear por aire a bajo costo y con escasos recursos humanos.

Las imágenes capturadas por las redes de cámaras estatales y dispositivos privados forman una gran red de vigilancia de estilo panóptico que se extiende rápidamente en las sociedades, muchas veces sin control sobre quién ve qué. El monitoreo, de los ciudadanos en los sistemas de videovigilancia tipo red, no está libre del riesgo, debido a que en cualquier sitio donde se encuentren las cámaras se tienen la oportunidad de controlar a todos, grabando sin control imágenes de otros ciudadanos.

Asimismo, todos estos sistemas de videovigilancia se complementan con biometría, creando un sistema combinado de identificación de personas más eficaz y eficiente. Los sistemas de videovigilancia están diseñados teniendo en cuenta el

poder de la información, y el control e identificación de los sospechosos del resto de la sociedad.

7.5. Sistemas biométricos y controles públicos

Después de lo dicho sobre los sistemas de geolocalización y los sistemas de videovigilancia, pasamos ahora a las tecnologías biométricas, que son el eslabón final en el complemento de los sistemas de identificación y vigilancia. La identificación biométrica se refiere a métodos automatizados que aseguran la identificación de individuos basados en características físicas o de comportamiento distinguibles.

Las técnicas utilizadas en biometría incluyen, reconocimiento de huellas dactilares, cara, patrón de venas, iris, voz y pulsación de teclas. Existe una necesidad obvia de mantener un entorno público y privado controlado para mantener la seguridad, ya sea de personas, objetos o información. Sin embargo, la condición de control no puede ser absoluta, y el control público requiere sistemas sofisticados.

La solución en este aspecto es la implementación de sistemas biométricos que se han desarrollado e implementado desde el desarrollo de la dactiloscopia por Juan Vucetich para identificar a personas. Los sistemas biométricos son sistemas de identificación computarizados basados en uno o más modelos biológicos. Solicitan los datos biométricos de un individuo, extraen patrones de los datos resultantes y comparan el ejemplo con patrones registrados previamente.

Dependiendo del uso que se le dé, puede almacenarse en una base de datos centralizada. Uno de los sistemas más conocidos a disposición de las fuerzas de seguridad es el sistema AFIS, que tiene la capacidad de identificar con precisión a un individuo a través de huellas dactilares con aplicaciones tanto preventivas como disuasorias.

En este sentido, no todas estas innovaciones técnicas siempre se entienden como una tecnología positiva para la prevención del delito. El criminólogo Adam Crawford crítica claramente las tácticas de prevención de situaciones de riesgo y el uso excesivo de las TIC, argumentando que: Puede fomentar una fe ciega en la tecnología que puede ser carecer de fundamentos y está impulsada principalmente

por los intereses comerciales de la creciente industria de la seguridad (alarmas, CCTV, iluminación, etc.) y reemplaza la importancia de los agentes humanos en la prevención del delito.

7.6. La sociedad panóptica

La sociedad disciplinaria, como la llamó Michel Foucault, se basó en la obra "El Panóptico" de Jeremy Bentham. Foucault hizo un estudio de una serie de procesos que transformaron la sociedad punitiva del siglo XVIII en la sociedad disciplinaria del siglo XIX. Así, se dedicó al estudio de los instrumentos disciplinarios desde la perspectiva de la prisión, utilizando el término "disciplina" como un conjunto de técnicas y procedimientos a partir de los cuales buscaba producir cuerpos políticamente obedientes y económicamente viables. La "disciplina" no puede equipararse a una institución o un aparato; es una especie de poder, su uso, incluye todo un conjunto de herramientas, técnicas, procedimientos, a nivel de aplicación, y su objetivo es la "física" o "anatomía" del poder.

Estos procesos afectaron no solo a la prisión, sino también a la red de instituciones que componían la sociedad del siglo XIX, como fábricas, comisarías, hospitales y escuelas, donde se producía una visión tecnológica a través de los mecanismos de la sociedad disciplinaria. La doctrina disciplinaria produjo un dispositivo de vigilancia que funcionaba como un microscopio del comportamiento; delicadas y analíticas divisiones formadas alrededor de los hombres para controlar, registrar y dirigir el comportamiento.

El Panóptico consta de los siguientes rasgos que definen el principio general de la normalización disciplinada de las nuevas dinámicas de poder de las sociedades, que puede considerarse una invención técnica equivalente a la máquina de vapor en el proceso productivo. Y se describe como un edificio arquitectónico con una torre central (donde se controlan las funciones de guardia y el personal) rodeada por un anillo de celdas que albergan a prisioneros. El Panóptico está diseñado para optimizar el tiempo de visualización de los presos,

se les visualizaba en sus celdas, pero no se podía ver a los espectadores de la torre central.

El propósito del modelo era poder controlar. El individuo estaba siendo seguido, pero no podía ver si realmente lo estaban siguiendo, y tampoco podía estar seguro de que lo estuvieran siguiendo; pero puede haber estado consciente de la posibilidad de ser vigilado. Así, los operativos de vigilancia comenzaron a cambiar el comportamiento de los internos, cada uno de los cuales se convirtió en su propio normalizador. Estas técnicas de poder se vuelven esenciales para aquellos mecanismos de observación capaces de controlar y moldear el comportamiento de los individuos, asignando sus tareas y comportamientos legitimadores del orden y control social.

7.7. La sociedad del orden

Los mecanismos disciplinarios son tecnologías de poder que se enfocan en ordenar a individuos; donde el panóptico es el orden de los cuerpos y la sociedad sería donde cada individuo es colocado en su lugar adecuado, lo que crea un orden suficiente para el control social. Es así como el aparato de seguridad configura el territorio y su soberanía, utilizando la estadística como solución a los problemas demográficos y aplicando el sistema legal al mismo tiempo que disciplina - a través de cálculos y tácticas entre instituciones (policía, escuelas, juzgados, etc.) - con el objetivo de controlar a la población, lograr el necesario control y orden, estableciendo la rudimentaria estructura de poder del país.

No olvidemos que el objeto principal del poder es el ciudadano como medio de conocimiento de la economía política y como instrumento técnico necesario, de los dispositivos de seguridad. Así, se fortaleció el poder del Estado a partir de dos nuevas estructuras desarrolladas en el ámbito diplomático-militar que se ocupan de la política exterior y de la policía política interior. El objetivo de la policía es regular la vida de los ciudadanos. Por lo tanto, las sociedades fueron diseñadas en el marco del paradigma del orden, donde el orden racional del individuo se establecía dentro de los parámetros de normalidad y regulación.

La sociedad también desarrolló métodos para asegurar que sus miembros correspondieran al orden social dominante y hegemónico, y separó conductas para definirlas como problemáticas, peligrosas, insalubres o desviadas. No es

consciente de los conflictos y problemas sociales. En este sentido, los conflictos se entendían como un disturbio, y para ello era necesario restablecer de alguna manera el control social.

En la misma línea de pensamiento, un fenómeno delictivo se entendía como una grave perturbación o desviación del equilibrio social. Según este punto de vista, todo conflicto era sinónimo de "desorden" y como tal un desequilibrio en la armonía social que había que reorganizar o restaurar. La idea central de este paradigma de orden proviene de años en el desarrollo del pensamiento político occidental- Por lo tanto, el objetivo de la política de seguridad es introducir un orden social, que sea compatible con las teorías económicas basadas en el mercantilismo y el posterior liberalismo. La política de seguridad se basó principalmente en una visión simplista, un conjunto esquemático y simple de parámetros de orden enmarcados dentro de conceptos tradicionales de política pública, orden interno e incluso seguridad interna. Así se formaron los organismos de seguridad desde hace más de 200 años hasta la actualidad.

7.8. Transición del orden a la prevención

Desde la década de 1970, los modelos de instituciones dedicadas a la seguridad pública han sufrido cambios importantes en los países más desarrollados. Estos cambios sociales y políticos comenzaron a implementarse en países del tercer mundo a partir de la década de 1990. Es importante observar el contexto de creación de una nueva prevención, si se considerando primero, que los países estaban en crisis con el modelo anterior, encontrándose con una delincuencia que aumentaba constantemente y no podían continuar con políticas basadas en la demagogia punitiva.

Por lo tanto, se vieron obligados a implementar otras políticas de seguridad pública, seguidas de una serie de cambios sociales, políticos y culturales. Las principales características de la nueva prevención están relacionadas con la creciente delegación de tareas de seguridad -hasta ahora en organismos públicos dedicados a la seguridad centralizada, donde se encuentran las diversas instituciones que componen los gobiernos locales, el sistema judicial y sistema civil. Las organizaciones sociales deben participar activamente en el desarrollo de decisiones específicas relacionadas con la prevención y el combate de la delincuencia.

La comunidad debe asumir la responsabilidad de ser un actor clave en las actividades de prevención y se convertirse en una importante fuente de información, por lo que la participación de ciudadanos junto con la instituciones de seguridad se considera una herramienta de planificación estratégica.

Estas medida se tomaran antes de comenzar el crimen y se entiende que la actuación de las fuerzas de seguridad es más efectiva al momento de su intervención. La nueva labor preventiva tiene varios aspectos relacionados con la lucha contra el delito, pero se enfocar en la prevención del delito, operando sobre tres ejes principales:

1. Aportando medidas en situaciones favorables antes de la ocurrencia de hechos violentos y delitos.

2. Ayudando a sectores y grupos sociales en situaciones de conflicto entre sí y con la ley.

3. Desarrollando recursos y actividades basadas en la prevención del delito.

En el primer punto se debe enfatizar cambiar las situaciones que permiten el conflicto, la violencia y la actividad delictiva. Este tipo de prevención se denomina “Prevención Situacional”. Se caracteriza por el análisis de hechos y circunstancias violentos y delictivos con el fin de planificar y determinar medidas que reduzcan la posibilidad de cometer delitos. A su vez, las tecnologías como el circuito cerrado de televisión (CCTV), alarmas, dispositivos biométricos, geolocalización, drones, botones antipánico etc., amalgamados con los servicios de seguridad privada es una de las tácticas más usadas para garantizar seguridad ciudadana.

Capítulo 8

8.1. Modelo de ciudad basado en IA para Lima

La transformación de Lima basada en la transformación digital como motor de desarrollo de la sociedad, debe contemplar lo siguiente:

Figura 8.1.

Transformación digital como motor del desarrollo social.

Fuente: Chávez (2021).

8.2. Claves para la seguridad urbana

El modelo de ciudad digital tiene como motivación principal la seguridad urbana, que implica, no solamente el control de la delincuencia. Puesto que, en una metrópolis como Lima, también se debe controlar y favorecer el libre tránsito por sus calles y avenidas, monitoreo de los servicios públicos: electricidad, acueductos, servicios sanitarios entre otros.

Figura 8.2.

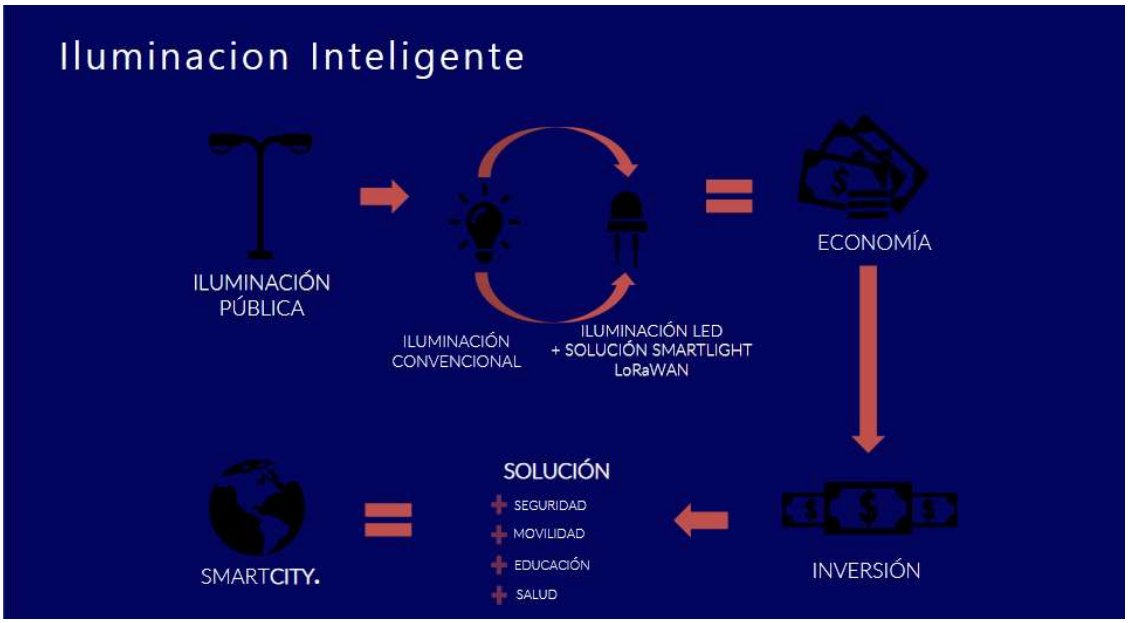
Claves de seguridad urbana.

.Fuente: Chávez (2021).

8.3. Modelo de iluminación inteligente para Lima Metropolitana

Figura 8.3.

Iluminación inteligente



Fuente: Chávez (2021).

8.4. Tendencia en Lima Metropolitana

Figura 8.4.

Tendencia: IA funcionando al borde.

Fuente: Chávez (2021).

8.5. Aplicaciones de IA en Lima Metropolitana

Figura 8.5.

Detección de distanciamiento social.

Fuente: Chávez (2021).

Figura 8.6.

Gestión de tráfico con IA.

Fuente: Chávez (2021).

Figura 8.7.

Gestión de tráfico con IA.

Fuente: Chávez (2021).

Figura 8.9.

Gestión de entrada y salida

Fuente: Chávez (2021).

Figura 8.10.

Detección de máscara facial

Fuente: Chávez (2021).

8.6. Software en IA

Figura 8.11.

Software para gestión

Fuente: Chávez (2021).

Capítulo 9

9.1. Situación de la videovigilancia e IA en el sistema jurídico peruano

El desarrollo de la tecnología ahora permite sistemas de videovigilancia a gran escala para las grandes ciudades. Consideremos, por ejemplo, el caso de China, que cuenta con 176 millones de cámaras de videovigilancia y un sistema en red que también permite el reconocimiento facial y está equipado con inteligencia artificial. Si bien en Perú no existen ciudades de videovigilancia comparables a Londres o Nueva York en cuanto a cantidad y calidad de sistemas de videovigilancia, como vemos, el nuevo decreto legislativo 1218, que regula el uso de cámaras de videovigilancia (DLCV) "sembró la semilla" de lo que podría ser el inicio del sistema de videovigilancia interconectado más grande del país, comenzando por grandes ciudades como Lima o Cusco.

La DLCV y la Ley 30120 (Ley de Seguridad de los Ciudadanos con Cámaras de Videovigilancia Públicas y Privadas; en adelante LSCVPP) conforman el marco general para la regulación de la videovigilancia en el ordenamiento jurídico peruano. Dicho marco debe estar permanentemente conectado con el Código Civil Peruano de 198 (en adelante CC) y la Ley 29733 (Ley de Apoyo a la Seguridad Ciudadana con Cámaras de Videovigilancia Públicas y Privadas; LSCVPP) y su reglamento.

Todo este marco normativo vigente tiene como objetivo hacer frente a los diversos hechos que adquieren relevancia jurídica, generando problemas o desafíos para los diversos actores de la sociedad y del mercado cuando se despliega la videovigilancia. La videovigilancia debe entenderse como "un sistema de seguimiento y grabación de imágenes, videos o sonido de sistemas, lugares, personas u objetos". Ahora bien, es importante señalar que aún existen pocos estudios sobre la videovigilancia, por lo que es interesante discutir el tema. Esto se debe principalmente a que es una nueva tecnología que se usa muy a menudo en la actualidad.

Asimismo, el uso de esta tecnología ha comenzado a generar dudas, entre otras cosas, sobre el ambiente de trabajo, las obligaciones de los proveedores expuestos a las relaciones de consumo, la supervisión del sistema de visitas

familiares y los procedimientos o procesos de control. El propósito de este capítulo es, en primer lugar, familiarizarse con el estudio de la imagen humana como objeto de protección en el ordenamiento jurídico; luego describir, analizar, evaluar y criticar la regulación actual del marco legal de la videovigilancia en el ordenamiento jurídico peruano; y finalmente proponer supuestos fácticos específicos sobre la videovigilancia actual para dar una solución basada en las normas existentes.

9.2. La imagen como objeto de protección

Uno de los aspectos más importantes de una persona es su identidad, ésta puede representarse gráficamente como una apariencia física reproducida en diversos medios, por lo que recibe la protección del ordenamiento jurídico en determinadas situaciones. Veamos las reproducciones existentes más habituales -unas más clásicas y otras más modernas-: pinturas de escenas, caricaturas realistas, fotografía o grabación de vídeo.

Todos estos soportes (lienzo, cuadernos, papel fotográfico, rollo fotográfico negativo, archivo digital, videocasete, CD, DVD, BD y otros) tienen en común que pueden contener una representación gráfica de la imagen de una persona. También es importante que la imagen no solo se refiera al rostro de la persona, sino que también pueda combinarse con aspectos que la hagan reconocible sin necesidad de mostrar el rostro de la persona.

En este contexto, incluso capturar la ropa, los rasgos faciales o las partes del cuerpo de una persona puede proteger su desempeño. Es importante identificar a la persona específica, porque la videovigilancia capta mayoritariamente los más mínimos detalles de una persona, pero a veces el metraje capta sólo elementos sugerentes, como los mostrados, que permiten confrontar el aspecto físico. La representación gráfica de una persona o imagen, como se le conoce, se establece como un objeto protegido por la ley.

9.3 La imagen en la antigua legislación

En el Código Civil (CC) peruano, en el artículo 15 establece una regla sustantiva respecto del derecho a la imagen. El primer párrafo establece negativamente que "no se podrá utilizar la imagen y la voz de una persona sin su consentimiento expreso o, en su caso, sin el consentimiento de su cónyuge, parientes, ascendientes o hermanos, en caso de las persona muertas. Se añaden una excepción las personas famosas, figuras públicas, científicos o académicos, sin que la excepción proceda si afecta el honor, la civilización o la reputación de las personas a quienes se refiere la imagen responde. Por otra parte, el artículo 17 prevé un mecanismo procesal civil que permite la denominada acción preventiva del asentimiento, que es una forma de solicitar el cese de la infracción por uso no autorizado de la imagen y, además, permite exigir una indemnización. Todos estos supuestos cobran especial fuerza cuando el abuso involucra es con fines comerciales, porque somos, al fin y al cabo, un campo de derecho civil.

En lo que respecta a la videovigilancia, es indiscutible que el derecho civil se aplica a cualquier imagen o grabación de video, siempre que cualquiera de los que aparecen en esa captura sean los propietarios de la imagen, que es un derecho inherente a la imagen de una persona. También creemos que una persona podría usar la protección preventiva incluso si las imágenes de videovigilancia son dañinas o si son usadas sin permiso o con fines lucrativos, incluida la compensación si se prueba el daño.

9.4. La imagen en la tuitiva regulación constitucional

En su lista de derechos protegidos, la Constitución peruana también reconoce el derecho a la propia imagen (artículo 2, inciso 7) junto con otros derechos (honor, buena reputación, intimidad, voz). Hoy en día no cabe duda de que es un derecho fundamental independiente de los demás. En este sentido, la Corte Constitucional del Perú demuestra que el derecho a la imagen en la Corte Constitucional... es un derecho autónomo que tiene un ámbito especial de protección contra las reproducciones que propietario tiene el propietario de la imagen. Por tanto, su titular tiene derecho a impedir la difusión de su apariencia física, porque es un elemento definitorio de cada individuo en su identificación,

que proyecta al exterior para reconocerlo como persona. En el ámbito constitucional sólo se protege el nivel patológico, no el fisiológico, pues la protección constitucional tiene por objeto detener conductas que vulneren algún derecho constitucionalmente reconocido. En otras palabras, la protección se activa cuando nos encontramos ante una intrusión o amenaza que pone en peligro el contenido constitucionalmente protegido del referido derecho: en este caso, el derecho a la propia imagen.

Así, el Tribunal Constitucional menciona que este derecho "básicamente protege la imagen humana relacionada con su dignidad y garantiza el alcance de la libertad del ser humano en relación con sus rasgos más propios, pertinentes e inmediatos... como la imagen física, la voz o el nombre, características definitorias, únicas e irreductibles de cada persona".

La constitución peruana no distingue entre derechos constitucionales, fundamentales y derechos humanos. Sin embargo, esto no quiere decir que el derecho a la propia imagen como derecho fundamental se base en la dignidad humana, que tiene por objeto proteger la semejanza física de una persona. El Tribunal Constitucional español demostró exactamente eso: el derecho a la propia imagen [...] se configura en su dimensión constitucional como un derecho personal, que tiene su origen en la dignidad humana y pretende proteger la dimensión moral de las personas, el derecho de su titular a determinar qué información gráfica con base en sus características físicas personales podrá ser divulgada.

La facultad que otorga este derecho fundamental consiste esencialmente en que un tercero queda excluido de la adquisición, reproducción o publicación de su imagen, cualquiera que sea la finalidad solicitada -informativa, comercial, científica, cultural, etc. quien la capta o la difunde. Es importante resaltar que el alcance de la protección constitucional es diferente al definido en los casos de derecho civil, porque la protección del derecho constitucional a la imagen excluye cosas que son esencialmente parte de la titularidad de la imagen. Así, el Tribunal Constitucional español afirmó que "el derecho constitucional a la imagen no debe confundirse con el derecho de toda persona sin permiso, e incluso en determinadas circunstancias, con consentimiento a explotar comercialmente la imagen de una persona que pueda afectar a su identidad" o derecho a su imagen".

En efecto, aunque exista un acuerdo conforme a la legislación que permita el uso de la imagen de una persona, se puede afectar un derecho fundamental, pero

si vulnera la dignidad humana de una persona, la exigencia del reconocimiento es más severa. No puede ser de otra manera, porque sería una vulneración del derecho fundamental a afectar un contrato válido y vigente, vulneración que debe probarse y sustentarse mediante la intromisión en el contenido constitucionalmente protegido.

Otra característica importante del derecho a la propia imagen, que se comparte con el derecho a la privacidad, es la individualidad. Ninguno de estos derechos pertenece a un área geográfica determinada, sino que son derechos que acompañan al titular a donde quiera que vaya. Así, el titular del derecho fundamental a su imagen podría oponerse tranquilamente a la videovigilancia ajena en la vía pública o desde su domicilio.

Sin embargo, como veremos, incluso estos derechos en distintas áreas geográficas pueden verse limitados por el principio de proporcionalidad para proteger otros valores constitucionales. En este sentido, el derecho a la imagen está sujeto a los derechos fundamentales generales a nivel constitucional. De este modo, el Tribunal Constitucional español mostró que como ocurre con otros derechos, el derecho a la propia imagen no es absoluto. Como todo derecho, encuentra limitaciones en el caso de los demás derechos y bienes constitucionales.

El mismo razonamiento se aplica también a otros derechos, como el derecho a la protección de la intimidad. En este sentido, otros valores constitucionales pueden servir de base a medidas legítimas para afectar el derecho a la propia imagen, como la seguridad pública, la protección de la vida y la intimidad, el derecho a la propiedad privada, etc. Ahora bien, las medidas que limitan el derecho a la propia imagen deben ser razonables y proporcionadas a sus objetivos. Así, aun cuando la voluntad del titular de la imagen sea la que prima facie determine la captación o distribución de la imagen, siempre habrá casos en que prevalezcan otros intereses en el mismo nivel constitucional.

En este sentido, el Tribunal Constitucional español señala lo siguiente: ...el derecho a una imagen está limitado por la voluntad del titular del derecho, que es esencialmente quien debe decidir si permite la captura o distribución de su imagen. Sin embargo, como ya se ha señalado, existen circunstancias que pueden dar lugar a una renuncia a la regla expresada, lo que se produce en los casos en que existe un interés público en la captación o difusión de la imagen, y el interés público se considera primordial conforme a la Constitución. Por lo tanto, si este derecho fundamental entra en conflicto con cualquier otro bien o derecho protegido por la

constitución, es necesario sopesar los diversos intereses en conflicto y, considerando las circunstancias específicas de cada caso, decidir qué interés merece más protección que la que merece el interés del propietario.

Por tanto, cuando el derecho a la propia imagen choca con otro valor constitucional, nos encontramos ante un conflicto fundamental, donde los titulares de dos o más derechos fundamentales tienen intereses contrapuestos, por tanto, los derechos entran en conflicto. Es importante mencionar que, junto con el derecho de un propietario en particular, también puede entrar en conflicto con el interés del Estado en proteger los derechos de la población en general.

En todo caso, este tipo de problemas deben ser resueltos mediante el criterio ponderado -método de resolución de antinomias o contradicciones normativas de valores constitucionales de la misma jerarquía- porque no se puede aplicar la subsunción y no se puede resolver la cuestión en base a criterios de uso, jerarquía, cronología o especialidad. La ponderación se emplea para resolver los conflictos a través del principio de proporción y se reduce a los tres subprincipios siguientes:

1. Idoneidad de la medida: debe ser constitucionalmente suficiente para alcanzar el fin jurídico,

2. Necesidad: la medida es más benigno frente a otras del mismo tipo que sean igualmente adecuadas.

3. Proporcionalidad: en sentido estricto, el beneficio logrado por una medida que afecta un derecho fundamental debe compensar los sacrificios que trae consigo al titular o a la sociedad en general.

Ahora es obvio que la implementación de este mecanismo de solución es un requisito previo para la confrontación entre dos jerarquías constitucionales de derechos fundamentales, que en algunos casos están respaldadas por normas internacionales. También es importante subrayar que, tal como lo reconoce la Corte Constitucional peruana, los derechos fundamentales reconocidos constitucionalmente tienen una doble dimensión: un derecho subjetivo y el deber del Estado de garantizar este derecho a toda la nación.

En este sistema constitucional de derechos fundamentales, el derecho a la propia imagen en su dimensión subjetiva garantiza a todos el derecho a determinar y decidir cuándo se puede hacer uso de la imagen La dimensión objetiva impone al Estado, por su parte, la obligación de garantizar el mismo derecho a todos los propietarios a través de sus instituciones.

Todas las administraciones públicas también deben respetar este derecho. En este sentido, el derecho fundamental a la propia imagen sólo puede limitarse para proteger otro derecho. Por ejemplo, la videovigilancia podría proteger los derechos de propiedad privada de los ciudadanos que utilizan sistemas de videovigilancia y audio, o la vida o la integridad de los ocupantes de la propiedad bajo videovigilancia.

El derecho a la propia imagen también se puede limitar si el Estado quiere proteger los derechos básicos de la comunidad o si se debe seguir una medida objetiva, por ejemplo, la seguridad pública o el derecho a la privacidad protección de la población en la vía pública y protección del patrimonio cultural, medio ambiente y demás valores constitucionales bajo tutela estatal, incluidos los bienes de dominio público.

Por otra parte, la acción de amparo conforme a la Constitución peruana es procesalmente la vía idónea para garantizar que el país proteja el derecho a la imagen, tal como lo demuestra la ley procesal constitucional, cuyo fin es restablecer las cosas al estado anterior a la violación o amenaza de violación. En el proceso constitucional no es posible obtener la tutela penal por daños y perjuicios, lo que obliga a distinguir entre las dos vías presentadas hasta ahora (civil y constitucional).

Se permite la presentación de demandas constitucionales para la protección de derechos descentralizados y colectivos. Al igual que ocurre con los derechos fundamentales, el mecanismo de protección –en este caso el amparo– tiene una dimensión bidimensional:

1. Se configuran como un proceso ideal para proteger un derecho fundamental, como es el derecho a la propia imagen.

2. Es un proceso donde se interpreta y tutela más allá del caso particular la disposición constitucional colocada como norma jurídica superior

del sistema, dando pautas sobre cómo interpretar la disposición de autoprotección desde una perspectiva constitucional.

Ahora bien, en cuanto a la videovigilancia, no cabe duda de que la seguridad de los ciudadanos es un fin que vale la pena proteger y puede justificar restricciones legales como la propia imagen de una persona. En este supuesto, no sólo encontramos amenazado el derecho del individuo a su imagen, sino que podemos enfrentar una amenaza a los derechos de un grupo de personas. Sin embargo, como ya hemos señalado, nuestro sistema no es una jerarquía de derechos. Por lo tanto, utilizando la proporcionalidad -al dictar normas que habiliten la videovigilancia- el legislador equilibra los derechos de las personas captadas en la imagen o video (individuales o separadas) y el deber del Estado de proteger la seguridad de los ciudadanos.

9.5. La imagen en la normativa administrativa

La LPDP (Ley de Protección de Datos Personales) definió datos personales como cualquier información sobre una persona natural que la identifique o la haga identificable de manera que pueda ser razonablemente utilizada. La imagen así definida cae claramente bajo el concepto de datos personales. Entonces, como esperábamos, la DGPDP (Dirección General de Protección de Datos Personales) ya declaró que la foto de una persona es un dato personal. Este tipo de reconocimiento y compromiso de alcance -especialmente en el caso de la videovigilancia- nos lleva a introducir y explicar a la videovigilancia todas las obligaciones relativas a las bases de datos personales, situación que se prevé sistemáticamente en la normativa que rige la videovigilancia masiva, como veremos más adelante.

La primera regla es el reconocimiento de la obligación de dar consentimiento al tratamiento de imágenes: los realizadores de las grabaciones deben ser informados antes del tratamiento, lo que puede hacerse, por ejemplo, mediante un aviso visible situado antes de la entrada en del lugares. Otra regla es que el titular de una imagen personal utiliza los derechos como datos personales.

Por tanto, las instalaciones públicas o privadas donde se capturen imágenes personales deberán ser responsables del tratamiento de las imágenes captadas por los sistemas de videovigilancia. Los titulares de los bancos de datos deben cumplir con el principio de proporcionalidad en el marco del sistema de protección personal. También deben observar el principio de finalidad y los datos personales de las imágenes de videovigilancia deben tratarse de acuerdo con la finalidad para la que fueron recopilados.

Especialmente en relación con el problema de la videovigilancia, es importante mencionar que la propia LPDP señala que: las restricciones al ejercicio del derecho fundamental a la protección de datos personales sólo pueden fijarse por ley, respetando su contenido esencial y son justificados, respetando otros derechos fundamentales o bienes protegidos por la constitución). Como ya hemos mencionado, la protección de la vida e integridad humana, la protección de la propiedad privada o garantizar la seguridad pública son algunos de los valores constitucionales, que inspiran la legalidad y constitucionalidad de la videovigilancia. La norma segunda de la LPDP también ampara legalmente esta actividad en relación con la protección de datos personales.

9.6. La protección de la imagen en la videovigilancia

La identidad personal encuentra diferentes medios de protección en diferentes campos (casos civiles, constitucionales, administrativos y penales). También se puede argumentar que la videovigilancia, atañe específicamente al derecho a la propia imagen ya otros derechos, como el derecho a la intimidad o al secreto de las comunicaciones. Así, las tecnologías de videovigilancia afectarían el derecho a la propia imagen. Una operación de videovigilancia tendría un efecto limitante sobre el derecho a la propia imagen con su contenido, porque poner la imagen a disposición de un tercero la enajena al perder el control de su presentación. Por lo tanto, es imperativo que los estándares de videovigilancia pongan "bloqueos" a posibles fugas de datos, como obligaciones de confidencialidad, o restrinjan el acceso a los datos de video tanto como sea posible.

Estos “bloqueos” se pueden establecer como principios u obligaciones que se deben seguir en el trabajo de videovigilancia. Del mismo modo, si se permite la videovigilancia es porque se fundamenta en fines igualmente legítimos a nivel

constitucional, principalmente la seguridad de los ciudadanos y el deber de perseguir los delitos en la calle y en los lugares públicos.

En base a ello, llegamos a dos conclusiones:

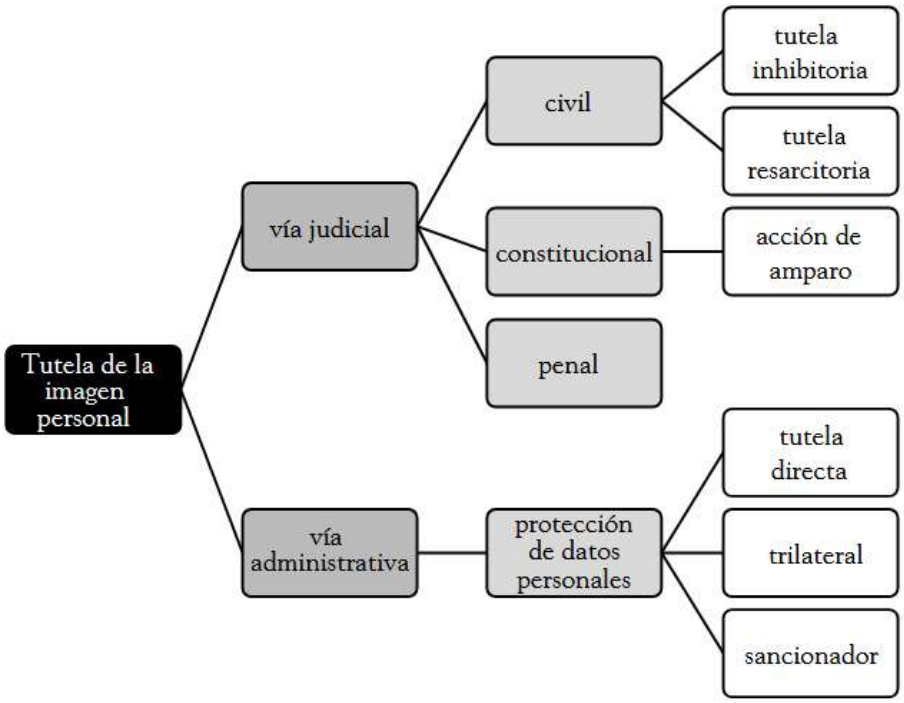
1. La emisión de órdenes de videovigilancia equivale a la consideración que el legislador debe tener en cuenta a la hora de redactarlas. Esto exige el establecimiento de deberes, normas y principios que permitan la protección de los derechos fundamentales, como la correcta imagen de las personas captada por los sistemas instalados en la vía pública y otros lugares (como instituciones externas o domicilios particulares).

2. En segundo lugar, existen formas de proteger a los ciudadanos en los casos de videovigilancia, incluso sin una regla específica. La vía civil permite la protección preventiva y la indemnizatoria, esta última cuando se prueba el daño.

La citación puede ser utilizada contra la amenaza o violación del contenido constitucionalmente protegido de la propia imagen, o contra particulares o contra la actuación del Estado, incluido el personal de videovigilancia. La tutela administrativa permite hacer uso de los derechos reconocidos por la norma de protección de datos personales, sancionando incluso el tratamiento de imágenes de videovigilancia. Por último, también existen presunciones penales que son muy restrictivas a la hora de tipificar los delitos y van siempre más allá de la simple toma de imágenes de videovigilancia.

Figura 9.1.

Formas de tutela de la imagen personal.



Fuente: Murillo Chávez (2019).

9.7. Regulación de la videovigilancia en Perú

Perú solo regula este tema desde el año 2010. Desafortunadamente, esta tarea no es fácil, porque no existe una regulación general y sistemática de la videovigilancia. Si bien sería muy deseable una norma general, solamente se encuentran dos normas específicas en el país, en dos momentos distintos -en 2013 y 2015- aunque con el mismo propósito y respecto a la misma situación: la prevención y el control contra la delincuencia en curso y la investigación de delitos y faltas. Las normas pertinentes son la Ley de Apoyo a la Seguridad Ciudadana con Cámaras de Video Vigilancia Públicas y Privadas (LSCVPP) de 2013 y el Decreto Legislativo N° 1218 de 2015 que Regula el Uso de Cámaras de Video Vigilancia (DLCV). Estas son las primeras normas nacionales que regulan la videovigilancia en general.

9.8. El derecho a la videovigilancia

La primera observación que debemos hacer sobre el ordenamiento jurídico peruano es que, mediante la expedición de todas las normas especiales pertinentes, se define el derecho a la videovigilancia, que consiste en el derecho a crear y utilizar libremente sistemas de videovigilancia ya sea como medio para la protección de la vida y la integridad y la propiedad privada o como medida de la libertad empresarial.

Es claro que este derecho debe cumplir con las disposiciones generales que hemos recopilado a imagen de las leyes establecidas en los ámbitos civil, constitucional, administrativo y penal. Es decir, la toma de una imagen es legal en sí misma y no ilegal, salvo que se haya excedido algún límite legal establecido por el sistema, ya sea por uso no autorizado o por falta de consentimiento para el tratamiento (salvo las excepciones previstas en la LPDP), en violación de un contenido constitucionalmente protegido o punible según el ordenamiento jurídico.

Además, creemos que *ad maioris ad minus* está permitida la toma de fotografías que las personas o el personal de la unidad puedan tomar con un equipo mínimo como cámaras, videocámaras o dispositivos portátiles con cámara integrada. Sin embargo, se puede afirmar que se impone un deber general a todo aquel que disponga de un sistema de videovigilancia: ...al momento de presumirse un delito o falta, se deberá avisar a la autoridad competente y entregar copias de las imágenes y sonidos a la Policía Nacional del Perú o al Ministerio Público, según sea el caso; o si lo solicitan las instituciones pertinentes.

La cooperación de la videovigilancia con la policía o la administración pública se refiere al deber de la persona o entidad propietaria de sistemas de videovigilancia de informar y transmitir imágenes, videos o audio a la policía o ministerio peruano en dos casos:

a) si se presume que el propietario descubrió por sí mismo el delito o la infracción; y

b) si el material es solicitado por la policía o un departamento gubernamental.

Esta transferencia de material está sujeta a la garantía de confidencialidad de los titulares de los sistemas de videovigilancia. Por otro lado, el artículo de la LSCVPP le da a la Secretaría de Gobernación la oportunidad de crear una base de datos actualizada de personas o entidades bajo el control de los sistemas de videovigilancia fuera de los edificios. La citada base de datos es gestionada por el nuevo Centro Nacional de Videovigilancia y Radiocomunicación y Telecomunicaciones para garantizar la seguridad de los ciudadanos.

Así, por un lado, está el derecho a la videovigilancia, que consiste en el derecho a establecer y desplegar libremente sistemas de videovigilancia ya sea para la protección de la vida e integridad o de la propiedad privada, o como medida de autodeterminación- y por otro lado, se confirma el deber de colaboración de la videovigilancia con la policía o el ministerio público, que consiste en el deber de la persona o entidad titular de los sistemas de videovigilancia de informar y transmitir una señal de imagen, video o audio a los representantes de esas dos entidades.

9.9. Tipos de videovigilancia

Como siempre, existen diferentes formas de catalogar los fenómenos e instituciones jurídicas. En el caso de la videovigilancia, con base en lo informado, es posible expresar ciertos tipos en el ordenamiento jurídico peruano. Creemos que el criterio más adecuado es el subjetivo; es decir clasificación según quién ejerce el derecho de videovigilancia o quién cumple el deber de videovigilancia. Por ello, presentamos a continuación los tipos de videovigilancia:

a) Videovigilancia privada: Esta modalidad de videovigilancia se define cuando las personas físicas o jurídicas privadas realizan vigilancia y grabación de imagen, video o audio.

b) Videovigilancia personal: es la vigilancia voluntaria que se realiza en bienes o desde los bienes privados para su seguridad y resguardo.

c) Videovigilancia de empresas: es aquella donde las empresas realizan videovigilancia en áreas comerciales abiertas al público o en sus

oficinas (sede) para el normal desarrollo de sus actividades o para la protección de la propiedad privada, la vida y la integridad de las partes interesadas, incluidos los consumidores y los propios empleados.

d) Videovigilancia pública: en este tipo de videovigilancia las entidades gubernamentales o las administraciones públicas realizan vigilancia y grabación de imagen, vídeo o audio.

No es posible formar una clasificación rígida para los tipos de videovigilancia, porque las clasificaciones se mezclan y combinan. Entonces, contrariamente a la creencia popular, la videovigilancia privada puede ser obligatoria, como se requiere en una tienda abierta al público que contiene al menos 50 personas, y la videovigilancia pública puede ser obligatoria u opcional: por ejemplo, si una agencia gubernamental decide instalar un sistema de videovigilancia en una propiedad que no es pública. De manera similar, tenemos la obligación establecida en de controlar la videovigilancia interior de los vehículos del servicio de transporte público prestado por empresas privadas en el Perú.

9.10. Limitaciones de la videovigilancia

Como informamos, el artículo 10 de la DLCV establece una prohibición general de captar o grabar imágenes, videos o sonidos en lugares que atenten contra la privacidad o la intimidad de las personas. Entre las restricciones, se encuentra la prohibición de que las cámaras de videovigilancia capten o graben imágenes o sonidos en baños, sanitarios, vestidores, vestuarios, baños o los ambientes internos de los departamentos vecinos. También agrega en su segundo párrafo que “las imágenes o audios tomados y grabados no pueden ser distribuidos o transmitidos a una persona no autorizada de ninguna manera.

La violación de esto conlleva responsabilidades administrativas y penales. Confirma que la contratación no es ilegal, sólo las acciones posteriores que se lleven a cabo sin autorización.

9.11. Posibilidad de interconexión a grandes sistemas de videovigilancia basados en IA

Esta posibilidad se fundamenta, cuando el Estado garantiza la conexión de las cámaras de videovigilancia a las plataformas de videovigilancia, radiocomunicaciones y telecomunicaciones de los gobiernos locales y regionales y del Sistema Nacional de Videovigilancia y Radio Centro de Comunicaciones y Telecomunicaciones con el propósito de garantizar la seguridad de los ciudadanos.

Un sistema nacional combinado de videovigilancia significaría tener una gran herramienta o arma. Este tipo de herramienta no debe estar en manos de una comunidad o gobierno sin los "candados" legales necesarios que protejan los derechos fundamentales de las personas sujetas a videovigilancia, como el derecho a acceder a imágenes, videos o audios relevantes utilizados para fines estrictamente definidos y limitados.

Por último, también cabe mencionar el problema del *chilling effect*, que es entendido como la renuncia a un privilegio por miedo a las consecuencias de ejercer el mismo. Se ha demostrado que la conexión y establecimiento de sistemas panópticos de videovigilancia no solo pueden entorpecer el ejercicio de los derechos civiles, sino también cohibir a las personas a ejercer sus libertades colectivas. Por lo tanto, vale la pena prestar atención a la siguiente consideración: las personas dejan de realizar ciertas actividades, incluso legales, por temor a ser grabadas en una cámara de videovigilancia.

Bibliografía

Briceño-León, R. (2002). *Introducción. La nueva violencia urbana de América Latina.* http://bibliotecavirtual.clacso.org.ar/clacso/gt/20101109032208/1intro.pdf

CEPLAN. (2021). *Inteligencia artificial: desafíos y oportunidades para el Perú.* https://cdn.www.gob.pe/uploads/document/file/3294013/CEPLAN%20Inteligencia%20artificial%3A%20desaf%C3%ADos%20y%20oportunidades%20para%20el%20Per%C3%BA.pdf?v=1656342269

Chávez, M. (2021). *Ciudades digitales: ciudades seguras con IA.* https://cdn.www.gob.pe/uploads/document/file/3382802/Seguridad%20Ciudadana%20Per%C3%BA.pdf

CLAD. (2021). Inteligencia artificial y ética en la administración pública. https://clad.org/wp-content/uploads/2021/03/Libro-7-Inteligencia-artificial-y-%C3%A9tica-en-la-gesti%C3%B3n-p%C3%BAblica.pdf

CONCYTEC. (2021). Informe de Vigilancia Tecnológica: Inteligencia Artificial. https://repositorio.concytec.gob.pe/handle/20.500.12390/3090

INEI. (2021). *Estadísticas de la criminalidad, seguridad ciudadana y violencia. Una visión desde los registros administrativos.* https://www.inei.gob.pe/media/MenuRecursivo/boletines/estadisticas_de_criminalidad_seguridad_ciudadana_abr-jun2021.pdf

Jasso López, L. (2020). Seguridad ciudadana y tecnología: uso, planeación y regulación de la videovigilancia en Latinoamérica. *Diké. Revista de investigación en Derecho, Criminología y Consultoría Jurídica, (14)*, 27, pp. 5-27. http://portal.amelica.org/ameli/journal/48/481820001/481820001.pdf

Jaulis Rua, J. y Vilcarromero Giraldo, J. (2015*). Sistema de predicción de hechos delictivos para la mejora del proceso de prevención del delito en el distrito de la molina utilizando minería de datos* [Tesis de Grado, USMP]. https://repositorio.usmp.edu.pe/bitstream/handle/20.500.12727/2022/jaulis_vilcarromero.pdf?sequence=1&isAllowed=y

Martín Ríos, P. (2022). Empleo de big data y de inteligencia artificial en el ciberpatrullaje: de la tiranía del algoritmo y otras zonas oscuras. *Revista de los estudios de derecho y ciencia política.* 36. https://raco.cat/index.php/IDP/article/view/n36-martin/494092

Murillo Chávez, J. (2019). «Brace yourselves. La videovigilancia ya viene»: situación de la videovigilancia en el ordenamiento jurídico peruano. *Derecho PUCP,* 83, pp. 133-178. https://peru.com/epic/tecnologia/camaras-inteligencia-artificial-lima-esta-tecnologia-acabaria-delincuencia-noticia-608867/

Reyna, C. y Toche, E. (1999). La inseguridad en el Perú. https://www.cepal.org/sites/default/files/publication/files/6261/S9900087_es.pdf

Sandoval, R. (2021). Inteligencia artificial y ética en la gestión pública. https://www.researchgate.net/publication/350736029_Inteligencia_Artificial_aplicada_al_gobierno_una_exploracion_internacional_de_casos

Torres, A, Rendón, F. y Gutiérrez. (2020). Revisión de las técnicas de inteligencia artificial aplicadas en seguridad informática. *Revista Ontare*. 7. https://www.researchgate.net/publication/343895399_Revision_de_las_tecnicas_de_inteligencia_artificial_aplicadas_en_seguridad_informatica/citation/download

Zamora, Á. V. (2021). Videovigilancia e inteligencia artificial: entre la utopía y la distopía. *Revista Mexicana de Ciencias Penales, 4*(14), 8-38. https://revistaciencias.inacipe.gob.mx/index.php/02/article/download/432/346

BIOGRAFÍA DE AUTORES

JUAN CARLOS LÁZARO GUILLERMO

Natural de Lima. Tiene Título Propio en Formación Didáctica Online para Docentes Universitarios por la Universidad Internacional de la Rioja. Bachiller en Computación y Administración de Negocios, Licenciado en Computación por la Universidad Nacional Mayor de San Marcos. Maestría en Educación con mención en Docencia y Gestión Educativa por la Universidad César Vallejo. Actualmente egresado del Doctorado en Medio Ambiente y Desarrollo Sostenible de la Universidad Nacional Hermilio Valdizan. Maestrando en Inteligencia Artificial de la Universidad Internacional de la Rioja. Actualmente Docente Investigador RENACYT, con más de 21 años de experiencia profesional y de investigación en Ciencias e Ingeniería. Ha trabajado en diferentes universidades públicas y privadas, ahora es Docente Ordinario del Departamento Académico de Ciencias Básicas de la Universidad Nacional Intercultural de la Amazonia – UNIA. Actualmente tiene el cargo de director nacional de Desarrollo Profesional del Colegio de Matemáticos del Perú (COMAP). Cuenta con Membresía IT-DATA, SPC, ITED, Editorial Mar Caribe. Sus líneas de investigación son: Python para Ciencia e Ingeniería de Datos, Big Data, Data Analytics, BPM, DBA, algoritmos bioinspirados, Bioinformática, Metodología Six Sigma, Cloud Computing, Transformación Digital, R Studio, LMS, Herramientas online. Con capacitaciones y diplomados actualizados del área de Computación, Sistemas, Gestión y Educación. Tiene diversos artículos publicados en Latindex y Scopus. Conferencista nacional 2015-2022 (UNHEVAL, UNMSM, COMAP, UNF, UNIA, UNU) e internacional 2022 (Costa Rica, México, Uruguay y Chile).

JOSÉ ALFREDO HERRERA QUISPE

Natural de Arequipa. Doctor en Ciencia de la Computación por la UNSA con pasantía de formación en el LMTG de la Universidad Paul Sabatier de Francia. Es parte del programa de profesionalización del MIT ha concluido allí el Mastering in innovation & Design Thinking. Sus líneas de investigación son Inteligencia Artificial, Minería de datos y computación aplicada al medio ambiente. Fue director de Información del INAIGEM del MINAM. Actualmente es Profesor Principal en la UNMSM y director del Instituto de Investigación FISI.

ERNESTO DAVID CANCHO RODRIGUEZ

Mg. Ing. Ernesto Cancho-Rodríguez (MBA) es el especialista más reconocido del país en inteligencia de negocios con experiencia como Analista de Inteligencia y Científico de Datos, experto en el desarrollo de sistemas de inteligencia de negocios e inteligencia artificial, tales como modelos de Análisis Predictivo y de Analítica de Datos para Planeamiento Estratégico, de Finanzas, de Estrategias de Marketing, Inversiones Bursátiles y de Gestión de Riesgos. Ernesto ha desarrollado e implementado soluciones analíticas de inteligencia de negocios en Europa, Estados Unidos, OEA y Perú. Se ha graduado como MBA (Magister en Gerencia de Negocios) con Especialización en Inteligencia de Negocios en la Universidad George Washington de Estados Unidos. También siguió el Programa de Certificación en Business Intelligence y Business Data Analytics con el Instituto Integrado de Estadística y la Facultad de Decisions Sciences de dicha universidad. Ernesto domina con fluidez el inglés y francés. Antes del MBA, también había trabajado en el desarrollo de modelos predictivos y sistemas de análisis de datos en el área de Global Pricing Analysis de la Novartis Corporation, en su sede central en la Ciudad de Basel, Suiza (2008-2010). Allí desarrolló y expandió modelos de análisis de estimación de precios de referencia internacional, contribuyendo a la optimización de precios y al incremento de rentabilidades de la organización. Tiene experiencia con tecnologías de Analytics e Inteligencia Artificial de última generación con el programa de certificación arriba mencionado. Ha trabajado en proyectos prácticos desarrollados en Python, R y SAS para Minería de Datos, Hadoop, Spark, SQL Server, Oracle PL/SQL, y software estadístico como SPSS de IBM, Matlab, Stata, entre otras tecnologías para el desarrollo de sistemas y modelos predictivos. Ganó experiencia en el desarrollo de Balance Score Cards, Dashboards, Data Visualization y reportes dinámicos en Tableau, Python, R y Power BI de Microsoft.

NORBERTO ULISES ROMAN CONCHA

Natural del Distrito de El Oro (Ayahuay), provincia de Atabamba, departamento de Apurímac, estudié primaria en el CE. Augusto B. Leguía distrito de Puente Piedra, secundaria en el CE. Sebastián Lorente Cercado de Lima y estudios superiores en la Universidad Nacional Mayor de San Marcos. Actualmente Docente - Investigador del Departamento Académico de Ciencias de la Computación (DACC) de la Facultad de Ingeniería de Sistemas e Informática (FISI) - UNMSM, Jefe de la Oficina de Educación Virtual(OEV) de la UNMSM, Presidente de la Comisión de Grados y Títulos de la FISI, Coordinador del Grupo de Investigación – ITDATA de VRIP (https://itdataperu.net/), Director del Instituto de Investigación de la FISI, Director Académico, Jefe de la Oficina de Calidad Académica y de Acreditación de la Facultad de Ingeniería de Sistemas e Informática, Editor de Revista Digital Catedra Villarreal – Posgrado, Miembro del Comité Editorial de la Revista de Investigación de Sistemas e Informática (RISI) y miembro del Comité de Gestión de la Escuela de Sistemas, Subgerente del Sistema de Gestión Documental con Firma Digital (Cero Papel). Evaluador de proyectos de investigación y asesor de tesis. Experiencia en soluciones de BIG DATA ANALYTICS, BUSINESS INTELLIGENCE, DATA MINING y MACHINE LEARNING. Participantes en congresos nacionales e internaciones (CHILE, COLOMBIA y CUBA). Reconocimiento como Coordinador del Grupo de Investigación ITDATA (RR No. N° 010639-2022-R/UNMSM)-"Premio a la Investigación 2022". Responsable del proyecto "Informática para las comunidades: Fortalecimiento Multidisciplinario a las comunidades y Centros Educativos".

JESSY ISABEL VARGAS FLORES

Natural de Pucallpa, Departamento de Ucayali. Ingeniero en Estadística e Informática de la Universidad Particular San Martin de Porres. Maestría en Ingeniería de Sistemas con mención en Tecnologías de Información y Comunicaciones en la Universidad Hermilio Valdizán. Egresada de la maestría en Estadística Aplicada en la Universidad Nacional Agraria La Molina. Actualmente egresada del Doctorado en Medio Ambiente y Desarrollo Sostenible de la Universidad Nacional Hermilio Valdizán. Docente universitario con más de 20 años de experiencia profesional y de investigación en Ciencias e Ingeniería. Conocimiento de Idiomas Ingles y portugués, dominio de tecnologías. Colegiada en el Colegio de Ingeniero del Perú. Manejo de Software estadísticos como IBM SPSS statistics, The R Project for Statistical Computing, R studio. Docente Ordinário adscrito al Departamento Académico de Ciências Básicas de la Universidad Nacional Intercultural de la Amazonia.

JANETT DEISY JULCA FLORES

Natural de Trujillo – La Libertad. Magister en Ciencias de la Computación. Ingeniero Informático. Catedrática en varias universidades. Tutor Virtual. Perito Informático del Colegio de Ing. La Libertad, de la Corte Superior de Justicia de la Libertad–Ministerio Publico Trujillo. Desarrolladora y consultor en Tecnología de la información. Asesora de Empresas Públicas y Privadas. Investigadora y capacitadora en modelos, metodologías, estrategias y herramientas TIC. Líneas de investigación: Base de Datos, Minería de Datos, Inteligencia de Negocio, Ingeniería de Software, Sistemas de Información, Aplicaciones Móviles y Auditoría de Sistemas.

Depósito Legal N°: 2022-12312

ISBN: 978-612-49137-4-7

Editorial Mar Caribe

www.editorialmarcaribe.es

Jr. Leoncio Prado, 1355. Magdalena del Mar, Lima-Perú

RUC: 15605646601

Contacto:

+51932557744 / +51932604538 / contacto@editorialmarcaribe.es

Libro Indexado por: