Universidad de la República
Facultad de Psicología

Licenciatura en Psicología
Trabajo Final de Grado

Vigilancia inteligente y gubernamentalidad algorítmica en Uruguay: usos estatales de la inteligencia artificial en la gestión de la seguridad y la población.

Mateo Pérez Rodríguez
Cedula: 5.764.441.1
Montevideo, Uruguay

Tutor: Diego Gonzáles García
Revisor: Sofía Monetti Rey

2026

Introducción

En los últimos años, el Estado uruguayo ha incorporado sistemas basados en inteligencia artificial (IA) en el marco de sus políticas públicas de seguridad y gestión social. Esta incorporación se inscribe en un contexto global atravesado por la expansión de las tecnologías digitales y el desarrollo de herramientas algorítmicas capaces de procesar grandes volúmenes de datos. Una de las principales líneas de implementación ha sido la integración de sistemas de videovigilancia con IA, utilizados en diversos ámbitos estatales para el monitoreo de espacios públicos, la identificación de personas mediante reconocimiento facial y la detección automatizada de determinadas situaciones. Por ejemplo, la implementación de herramientas para mejorar la eficiencia en la prevención de la delincuencia; registrar la circulación de vehículos y detectar personas en situación de calle. Según informes oficiales del Ministerio del Interior (Carballo, 2024), estas tecnologías permiten una gestión más rápida de la información, la cual conlleva a una mejor anticipación y respuesta. Todo esto es posible a través de dispositivos capaces de detectar comportamientos y clasificarlos, evaluando si pueden ser considerados como sospechosos y generar alertas automáticas en tiempo real .

Sin embargo, más allá de los discursos institucionales que promueven estos mecanismos como soluciones eficaces, es necesario adoptar una mirada crítica que permita interrogar los efectos reales y simbólicos de estas tecnologías sobre el espacio social, la subjetividad y las prácticas de gobierno. ¿Cómo intervienen en la forma de habitar el espacio público? ¿Qué formas de subjetivación emergen de dichas tecnologías?

En el presente trabajo se abordarán estas tecnologías a partir de la noción de *dispositivos de seguridad* aportada por Foucault (2006) que, más que castigar delitos, buscan anticipar conductas y gestionar riesgos utilizando la estadística y probabilidad. Esta perspectiva nos puede ayudar a entender cómo el poder moderno se centra cada vez más en el gobierno de las conductas, no mediante la prohibición directa, sino que a través de la regulación de sus condiciones de posibilidad .

El concepto de seguridad, en la obra de Foucault, no alude simplemente a la protección frente a la delincuencia, sino a una racionalidad de gobierno que actúa sobre la población

gestionando las probabilidades de los actos. El poder de seguridad no busca eliminar el riesgo, sino distribuirlo hasta umbrales aceptables y reducir su impacto, operando a través de estadísticas y modelos probabilísticos (Foucault, 2006). En este marco, la videovigilancia con IA se inscribe como un nuevo instrumento para gestionar esa distribución, desplazando la estadística humana hacia una eficiencia dada por su entrenamiento automatizado. Además, pensar esta tecnología desde el concepto de gubernamentalidad nos permite comprender cómo estas no solo registran o vigilan, sino que producen subjetividades propias de un entorno donde ser vigilado se vuelve parte de la experiencia cotidiana.

Marco conceptual

Gubernamentalidad

El concepto de gubernamentalidad constituye el eje conceptual desde el cual se organiza la mirada crítica de este trabajo, sobre la implementación de tecnologías de vigilancia con inteligencia artificial en Uruguay.

Foucault (2006) define la gubernamentalidad como el conjunto de técnicas y saberes orientados a “conducir la conducta de los otros”, configurando un campo de acción en el que los sujetos se gobiernan a sí mismos en función de normas disciplinarias, bajo la influencia de dispositivos externos que modulan sus decisiones. Si pensamos sobre este enfoque, la videovigilancia con IA aparece no sólo como un instrumento técnico, sino como una forma específica de ejercer el poder sobre las poblaciones, moldeando tanto las conductas como la percepción de lo normal, lo peligroso y lo tolerable.

> Con esta palabra, "gubernamentalidad", aludo a tres cosas. Entiendo el conjunto constituido por las instituciones, los procedimientos, análisis y reflexiones, los cálculos y las tácticas que permiten ejercer esa forma bien específica, aunque muy compleja, de poder que tiene por blanco principal la población, por forma mayor de saber la economía política y por instrumento técnico esencial los dispositivos de seguridad. Segundo, por "gubernamentalidad" entiendo la tendencia, la línea de fuerza que, en todo Occidente, no dejó de conducir, y desde hace mucho, hacia la preeminencia del tipo de poder que podemos llamar "gobierno" sobre todos los demás: soberanía, disciplina, y que indujo, por un lado, el desarrollo de toda una serie de aparatos específicos de gobierno, [y por otro]* el desarrollo de toda una serie de saberes. Por último, creo que habría que entender la

> "gubernamentalidad" como el proceso o, mejor, el resultado del proceso en virtud del cual el Estado de justicia de la Edad Media, convertido en Estado administrativo durante los siglos XV y XVI, se "gubernamentalizó" poco a poco. (Foucault, 2006, pp. 136-137)

Desde esta perspectiva, el poder no se ejerce exclusivamente de forma jerárquica o represiva, sino que se despliega como una red de tecnologías, saberes y prácticas que tienen como objetivo la población, en tanto conjunto estadísticamente analizable y políticamente gobernable. Esta forma de ejercicio del poder moderno busca controlar los espacios en los que los sujetos se relacionan y desarrollan su vida creando los marcos en los que ellos pueden desplazarse, lo posible, generando un desplazamiento de las formas soberanas de poder, hacia un Estado que busca optimizar, regular y gestionar las condiciones de posibilidad de los sujetos en una multiplicidad de campos y con una diversidad de objetivos.

Por lo tanto, pueden observarse cambios desde el poder soberano, que se ejercía a través del derecho y la amenaza del castigo, hacia el poder disciplinario, encargado de producir cuerpos obedientes mediante la vigilancia institucionalizada, los dispositivos de seguridad operan bajo una lógica de gestión diferencial del riesgo, esto quiere decir que no se centra en evitar que algo ocurra, sino en aceptar su ocurrencia como posibilidad estadística, buscando reducir su impacto y distribuir sus efectos dentro de márgenes tolerables. El problema del gobierno es precisamente cómo permitirle a la población, que ciertas cosas se desarrollen, se regulen, sin que se generen desórdenes radicales.

Este cambio implica la consolidación de una forma de poder que actúa sobre la población a través del conocimiento de sus regularidades como tasas de criminalidad, curvas epidemiológicas, patrones de consumo, conductas de riesgo. Por lo tanto , se apoya en saberes técnicos que permiten medir, comparar, predecir y actuar preventivamente. “Lo que caracteriza en esencia el mecanismo de seguridad es, creo, la gestión de esas series abiertas y que, por consiguiente, sólo pueden controlarse mediante un cálculo de probabilidades” (Foucault, 2006, p. 40).

Castro Gómez (2010) plantea que el concepto de gubernamentalidad constituye una forma analítica del poder que desplaza la mirada del Estado como origen del gobierno

hacia las racionalidades y prácticas que organizan la conducción de las conductas. Señala que “El Estado no es la sede y origen del gobierno, sino únicamente el lugar de su codificación” y que, en consecuencia, “la historia que aquí interesa no es, entonces, la historia del gobierno estatal sino la historia de la ‘gubernamentalización’ del Estado” (Castro-Gómez, 2010, p. 45).

Desde esta perspectiva, la noción de gubernamentalidad permite analizar los modos en que se articulan saberes y mecanismos de poder en la producción de determinadas formas de gobierno. En este sentido, Foucault describe la gubernamentalidad como una herramienta analítica que habilita a indagar las relaciones existentes entre dispositivos de coerción y formas de conocimiento que los legitiman y orientan (Castro-Gómez, 2010). Esta concepción que plantea (Castro-Gómez, 2010) implica un desplazamiento sobre las nociones clásicas de poder, al pensarlo no tanto como imposición directa o como ejercicio jurídico, sino como una forma específica de acción orientada a guiar las conductas posibles, tanto de individuos como de colectivos, a partir de la conducción de la libertad.

En este marco, la gubernamentalidad no se reduce al funcionamiento de instituciones particulares, sino que opera como una lógica más amplia que atraviesa distintos niveles de la vida social, incluyendo las prácticas estatales y las formas en que los sujetos se gobiernan a sí mismos. (Castro-Gómez, 2010) retoma esta idea al señalar que la gubernamentalidad funciona como una matriz interpretativa que permite comprender el conjunto de las relaciones de poder, más allá de sus expresiones formales o institucionalizadas. Desde esta racionalidad gubernamental, los dispositivos de seguridad adquieren un rol central, ya que su objetivo no consiste en la prohibición absoluta ni en el encierro disciplinario, sino en la regulación de fenómenos poblacionales mediante cálculos y previsiones que buscan mantenerlos dentro de ciertos márgenes considerados social y políticamente aceptables.

Así, los dispositivos de seguridad se apoyan en saberes estadísticos y probabilísticos que permiten intervenir sobre variables como la criminalidad, entendida como un dato a administrar en función de criterios de gestión y eficiencia. En este sentido, la lógica que los orienta no se organiza en torno a oposiciones binarias como normal/anormal o permitido/prohibido, sino que opera a partir de distinciones entre lo aceptable y lo inaceptable, definidas en términos de cálculo económico y político (Castro-Gómez, 2010). Finalmente, esta forma de gubernamentalidad implica también la producción de espacios

específicos de seguridad, entendidos como ámbitos estratégicos donde se articulan técnicas de control, gestión del riesgo y gobierno de las poblaciones, lo cual constituye una de las innovaciones centrales del análisis foucaultiano desarrollado a fines de la década de 1970 (Castro-Gómez, 2010).

De la gubernamentalidad neoliberal a la focopolítica.

La transformación del Estado social hacia un Estado neoliberal implica una reconfiguración de las racionalidades de gobierno. El Estado deja de ser garante universal de derechos sociales para asumir un rol facilitador y regulador, organizando las condiciones para que la gestión de la vida se distribuya entre Estado, mercado, familia y comunidad. Este desplazamiento, analizado desde la perspectiva de la gubernamentalidad, supone que la protección social deja de estructurarse como derecho ciudadano y comienza a funcionar como un entramado de responsabilidades descentralizadas y moralmente cargadas (Álvarez, 2008).

En este marco se consolida una *gubernamentalidad de mercado* (Álvarez, 2008), donde los sujetos son interpelados como capital humano, responsables de autogestionar sus trayectorias vitales, quienes logran integrarse al mercado son reconocidos como sujetos de contrato, quienes no, pasan a ser objeto de dispositivos específicos de gestión de la exclusión, este desplazamiento puede pensarse como un pasaje de la biopolítica clásica a una *focopolítica* (Álvarez, 2008). La población no se intenta regular en todo su conjunto sino que se enfatiza en el gobierno de grupos focalizados definidos como “en riesgo”, mediante intervenciones dirigidas y generadas con el propósito de asegurar umbrales mínimos de supervivencia más que a garantizar un bienestar integral.

Bajo esta racionalidad, el sujeto de la política social deja de ser el ciudadano portador de derechos y se convierte en un caso a evaluar, clasificar y monitorear. Los profesionales del campo social asumen funciones de *gatekeepers* (guardianes o porteros que controlan el acceso a información , recursos y/o tomadores de decisiones) , administrando recursos escasos a partir de diagnósticos que traducen desigualdades estructurales en perfiles individuales de riesgo. Se configura así una dialéctica entre *contrato y tutela* (Álvarez, 2008); Autonomía, elección y responsabilidad individual para los integrados; asistencia

condicionada, vigilancia y moralización para los excluidos. La ayuda se transforma en un beneficio a partir de la demostración de “buena conducta” y voluntad de cambio, desplazando el eje desde el derecho hacia el mérito (Álvarez, 2008).

En situaciones de extrema precariedad, como la vida en calle, esta lógica produce una *despolitización de la exclusión* (Álvarez, 2008), La falta de vivienda o ingresos se redefine como problema técnico, déficits personales, falta de habilidades, escaso capital social, eludiendo su carácter estructural. Los dispositivos de intervención, tales como registros, evaluaciones y programas asistenciales, operan como tecnologías de poder que etiquetan, regulan conductas y promueven la internalización de la responsabilidad individual por la propia pobreza, reforzando formas de autovigilancia y autocontrol.

En continuidad con las nociones de poder analizadas por Foucault, algunos desarrollos contemporáneos permiten complejizar la comprensión de los modos actuales de producción de subjetividad. En este sentido los aportes de (Lazzarato, 2012) nos permiten pensar sobre el esquema disciplinario clásico mediante el análisis de un doble registro semiótico en la producción de subjetividad, por un lado se encuentra el sometimiento social y por otro la servidumbre maquínica. El sometimiento social se fundamenta en semióticas significantes que, a través de la lengua y la representación, producen al sujeto, al individuo y al yo, asignándoles identidades y roles sociales fijos como profesión o nacionalidad. Por el contrario, la servidumbre maquínica opera mediante semióticas asignifcantes como lo son los lenguajes informáticos, ecuaciones y funciones numéricas que no buscan la constitución de una conciencia subjetiva, sino la captura y activación de elementos presubjetivos y preindividuales como afectos, percepciones y ritmos para integrarlos como engranajes de una máquina semiótica global.

Bajo este régimen de servidumbre, los seres humanos son pensados como dispositivos de información que funcionan como componentes de *input* (lo que entra al sistema ,datos, señales, estímulos) y *output* (lo que sale del sistema, respuesta, acción, resultado. Lazzarato (2012) explica que este poder ejerce una modulación afectiva en tiempo real que apela a la estimulación de los cuerpos mediante señales perceptivas sin significado que activan respuestas reflejas. En consecuencia, la población deviene en una red neuronal sincronizada por estímulos que conectan al gobierno con el sistema nervioso de cada individuo.

Desde esta perspectiva, la gubernamentalidad algorítmica y la videovigilancia inteligente en Uruguay pueden entenderse como dispositivos técnicos que organizan el espacio público mediante sistemas automatizados de análisis y clasificación de datos.

Dispositivos

Dentro del enfoque gubernamental adoptado en este trabajo, el concepto de dispositivo ocupa un lugar central para pensar cómo se ejercen hoy las formas de poder, particularmente en contextos donde la vigilancia digital y la inteligencia artificial transforman la manera en que se regula el comportamiento en los espacios públicos. La noción de dispositivo es introducida por Michel Foucault en su texto *Microfobia del poder* para describir aquellas configuraciones heterogéneas de saberes, prácticas, instituciones y tecnologías que permiten operar sobre las conductas, moldearlas, prevenir desviaciones y producir sujetos ajustados a determinadas normas sociales.

Foucault define el concepto de dispositivo como “Lo que trato de situar bajo ese nombre es, en primer lugar, un conjunto decididamente heterogéneo, que comprende discursos, instituciones, instalaciones arquitectónicas, decisiones reglamentarias, leyes, medidas administrativas, enunciados científicos, proposiciones filosóficas, morales, filantrópicas; en resumen: los elementos del dispositivo pertenecen tanto a lo dicho como a lo no dicho. El dispositivo es la red que puede establecerse entre estos elementos” (Foucault, 1985, p. 128). Lo que articula a estos elementos no es una estructura fija, sino su funcionalidad en el campo del poder. Es decir, el dispositivo no es una cosa, sino un modo de organizar relaciones entre saberes, cuerpos, tecnologías y normas, con el objetivo de gobernar. Cada dispositivo responde a una determinada racionalidad de gobierno y a una problemática histórica específica, pero todos comparten el hecho de producir efectos de saber-poder sobre los sujetos, interviniendo tanto en lo que hacen como en lo que pueden llegar a ser.

Para Foucault (2002), los dispositivos de vigilancia aparecen como una tecnología disciplinaria que ya operaba desde el siglo XVIII, particularmente a través de un modelo específico denominado panóptico, propuesto por Jeremy Bentham (1979). El panóptico se caracteriza por tener una arquitectura que permite ver sin ser visto, generando en el

sujeto la sensación constante de estar siendo observado, lo que lo lleva a autocontrolarse. Esta tecnología política está diseñada para organizar grupos humanos en cualquier contexto institucional. En palabras de Foucault, el panóptico:

> (...)es polivalente en sus aplicaciones; sirve para enmendar a los presos, pero también para curar a los enfermos, para instruir a los escolares, guardar a los locos, vigilar a los obreros, hacer trabajar a los mendigos y a los ociosos. Es un tipo de implantación de los cuerpos en el espacio, de distribución de los individuos unos en relación con los otros, de organización jerárquica, de disposición de los centros y de los canales de poder, de definición de sus instrumentos y de sus modos de intervención, que se puede utilizar en los hospitales, los talleres, las escuelas, las prisiones. Siempre que se trate de una multiplicidad de individuos a los que haya que imponer una tarea o una conducta, podrá ser utilizado el esquema panóptico. (2002, p. 212)

Sin embargo, este modelo basado en la vigilancia visual y en el encierro físico, actualmente se ve conviviendo con otras prácticas más difusas y móviles de control. Gilles Deleuze (1999), en su texto *Post-scriptum sobre las sociedades de control*, plantea que las sociedades modernas están desarrollando un nuevo régimen que integra lógicas de control continuo y modulante. Sugiere que el modelo disciplinario se encuentra en crisis por lo que las instituciones cerradas (escuelas, fábricas y/o cárceles), comienzan a dar lugar a otro tipo de entornos más fluidos donde el control no se ejerce desde un punto central, sino a través de una modulación constante y flexible que atraviesa al sujeto en todos sus movimientos.

De la centralidad panóptica a la vigilancia distribuida

El modelo panóptico analizado por Michel Foucault permitió comprender cómo la modernidad organizó el poder a través de la visibilidad asimétrica, la inspección jerárquica y la producción de subjetividades disciplinadas en espacios institucionales cerrados. La

prisión, la escuela o la fábrica funcionaban como dispositivos arquitectónicos donde el control se ejercía mediante la posibilidad permanente de ser observado. Sin embargo, las transformaciones tecnológicas y socioculturales contemporáneas han modificado esta lógica. La vigilancia ya no solo se concentra en instituciones delimitadas, ni depende de la inmovilización de los cuerpos, sino que se despliega en entornos abiertos, móviles y digitalmente mediados.

En este contexto, Fernanda Bruno (2013) propone comprender la vigilancia actual como un fenómeno “distribuido”, es decir, como un efecto que emerge de la articulación entre múltiples elementos. Dicho concepto se define como un dispositivo en términos foucaultianos, por lo tanto forma parte de una red de elementos heterogéneos que incluye tecnologías, discursos, leyes, instituciones y prácticas científicas o comerciales.

La observación deja de ser atributo de un vigilante centralizado y se convierte en una función que atraviesa redes sociotécnicas compuestas por plataformas digitales, dispositivos móviles, sensores urbanos, sistemas de almacenamiento masivo de datos y algoritmos de procesamiento. Esta transformación no implica la desaparición del panoptismo, sino su reconfiguración en una arquitectura reticular donde la visibilidad se produce de manera fragmentada, continua y descentralizada. La función vigilante ya no reside en un centro único de mando, sino que se reparte entre múltiples actores, tanto humanos como no humanos. Los algoritmos, los rastreadores digitales (*cookies*, *beacons*), el software de analítica de video y las bases de datos actúan como mediadores que desplazan y transforman la naturaleza de la vigilancia, permitiendo que esta se ejerza a distancia y en tiempo real (Fernanda Bruno , 2013)

La noción de vigilancia distribuida resulta clave porque desplaza la idea de un “ojo” único hacia un entramado de miradas parciales que, al conectarse generan una capacidad ampliada de seguimiento y análisis. En lugar de un centro que observa, encontramos múltiples puntos de captura de información que, integrados por infraestructuras digitales, permiten reconstruir trayectorias, hábitos y patrones de comportamiento. La vigilancia se vuelve así un proceso ambiental, incorporado al funcionamiento cotidiano de los sistemas técnicos que organizan la vida social.

En la actualidad, los dispositivos de vigilancia no solo registran lo que ocurre, sino que producen activamente realidades a través de la generación de datos y la elaboración de conocimientos operativos sobre la conducta.

Estos dispositivos funcionan como verdaderas *máquinas de ver* (Bruno, 2013), en la medida en que expanden la visibilidad más allá de la percepción humana. Sensores, cámaras, bases de datos y algoritmos convierten acciones humanas cotidianas en información cuantificable capaz de ser almacenada y correlacionada. Estas máquinas de ver (2013) deben ser comprendidas como dispositivos sociotécnicos que intervienen de manera activa en la configuración histórica de los regímenes de visibilidad. Esto implica desplazar la idea de que ver es una capacidad originaria del sujeto individual y reconocer, en cambio, que toda experiencia visual se encuentra mediada por entramados técnicos, institucionales y culturales que definen de antemano qué puede aparecer como visible y qué queda del lado de la invisibilidad. La mirada, en este sentido, no es un punto de partida, sino el efecto de una red heterogénea de mediaciones donde se articulan tecnologías de registro, saberes expertos, infraestructuras materiales, normas sociales y marcos institucionales.

Bajo esta perspectiva, dispositivos como cámaras de videovigilancia, sensores, sistemas de almacenamiento de datos y algoritmos de procesamiento de imágenes no realizan tareas neutrales destinadas a reflejar una realidad preexistente sino que estos dispositivos participan activamente en la producción de lo real al operar mediante procesos de selección, encuadre, traducción y clasificación de fragmentos del mundo. Cada una de estas operaciones implica decisiones técnicas y epistemológicas que determinan qué aspectos de la experiencia son capturados, cómo son codificados y bajo qué categorías adquieren sentido. La imagen digital, el dato biométrico o el perfil algorítmico no son simples representaciones, sino construcciones que condensan criterios normativos, supuestos estadísticos y racionalidades de gobierno.

En este marco, la visibilidad se convierte en un efecto político. Las “máquinas de ver” no solo hacen aparecer objetos, cuerpos o conductas, sino que establecen jerarquías de relevancia, delimitan zonas de opacidad y producen distinciones entre lo normal y lo anormal, lo seguro y lo riesgoso. Aquello que logra ingresar en los circuitos técnicos de captación y procesamiento se vuelve susceptible de ser medido, comparado y gestionado, mientras que lo que permanece fuera de esos marcos tiende a quedar excluido de las

formas dominantes de reconocimiento. De este modo, las tecnologías visuales participan directamente en la producción de los regímenes de verdad, ya que definen las condiciones bajo las cuales ciertos fenómenos pueden ser percibidos y problematizados.

Las máquinas de ver no solo transforman la experiencia sensible, sino que se inscriben en racionalidades más amplias de gobierno. Al convertir comportamientos, desplazamientos y presencias en datos analizables, estas tecnologías articulan visibilidad y gobierno, haciendo posible la anticipación, la clasificación y la modulación de conductas a escala poblacional. La visión deja de ser un acto perceptivo y se convierte en una tecnología de poder que produce sujetos, delimita riesgos y organiza estrategias de intervención sobre la vida social (Bruno, 2013).

A diferencia de la disciplina clásica, que buscaba producir cuerpos dóciles mediante la repetición y la normalización, estos dispositivos operan modulando comportamientos a través de alertas, recomendaciones, bloqueos o incentivos. Las intervenciones se realizan sobre el proceso anterior a la acción puntual, orientando decisiones antes de que se materialicen plenamente. El saber producido por la vigilancia se convierte en performativo, al clasificar contribuye a configurar los márgenes de lo posible para los sujetos.

La expansión de estas “máquinas de ver” no sólo transforma las técnicas de gobierno, sino también los modos de constitución de la subjetividad. Bruno (2013) plantea que las redes digitales favorecen una topología de la exterioridad, en la cual la construcción del yo se desplaza hacia espacios de visibilidad, exposición y registro permanente. La identidad se produce a través de huellas digitales, interacciones mediadas e instancias de participación por plataformas y bases de datos.

En este contexto, la vigilancia no opera exclusivamente desde la coerción externa, sino también mediante la participación activa de los sujetos. Publicar, compartir, geolocalizarse o utilizar dispositivos de automonitoreo implica generar información que alimenta los sistemas de observación y análisis. La visibilidad se convierte en un valor asociado al reconocimiento social, la pertenencia y la validación, integrando la captura de datos a prácticas cotidianas de sociabilidad.

De igual forma, esta participación se desarrolla en un marco de profunda asimetría. Los datos producidos por los usuarios son procesados en infraestructuras difusas, donde algoritmos clasifican, puntúan y perfilan sin que los sujetos conozcan plenamente los

criterios ni los efectos de esas operaciones. Así, la subjetivación contemporánea se da en un entorno donde la exposición voluntaria coexiste con formas de monitoreo y categorización, configurando sujetos que son simultáneamente productores de datos y objetos de análisis Bruno (2013).

La noción de vigilancia distribuida ofrece una mirada especialmente pertinente para analizar las tecnologías actuales de seguridad basadas en inteligencia artificial. En estos sistemas, la observación no se concentra en una autoridad visible, sino que se produce a través de la articulación entre cámaras, sensores, bases de datos, software de análisis y operadores humanos. La agencia del control se reparte entre múltiples actores, donde los algoritmos desempeñan un papel central en la detección de patrones, la clasificación de comportamientos y la generación de alertas.

Tomando como ejemplo las cámaras de videovigilancia utilizadas por el Estado uruguayo, en lugar de disciplinar individuos en espacios cerrados, estos dispositivos de vigilancia se orientan a monitorear flujos poblacionales, anticipar eventos y gestionar riesgos en entornos abiertos como la ciudad. La videovigilancia algorítmica no solo registra imágenes, sino que traduce movimientos en datos, identifica regularidades y produce categorías operativas que pueden influir en decisiones policiales, administrativas o preventivas. La vigilancia se vuelve un proceso continuo de evaluación probabilística, en el que las poblaciones son segmentadas según niveles de riesgo o sospecha.

Desde esta perspectiva, las tecnologías de inteligencia artificial no representan una ruptura total con las formas previas de poder, sino una intensificación y reconfiguración de la gubernamentalidad. El funcionamiento de estos sistemas puede comprenderse a partir de lo que Fernanda Bruno (2013, p.177) denomina como *La máquina taxonómica*, un dispositivo sociotécnico que convierte la información digital en insumos para clasificar, perfilar y anticipar conductas. Los movimientos captados por las cámaras, junto con otros datos asociados como horarios, trayectorias, repeticiones, proximidades dejan de ser registros visuales para transformarse en huellas que pueden ser agregadas, correlacionadas y almacenadas de manera potencialmente indefinida. Así, el interés ya no se centra en la identidad biográfica de una persona concreta, sino en fragmentos de comportamiento que al ser procesados algorítmicamente, permiten construir perfiles probabilísticos. Esta lógica, basada en la correlación más que en la explicación causal, produce categorías operativas que simplifican la complejidad de lo social para volverla

computable, asignando niveles de riesgo, normalidad o sospecha a partir de patrones, de esta manera la clasificación se convierte en un acto que produce realidades, ya que estos perfiles funcionan como simulaciones performativas que orientan intervenciones futuras.

Inteligencia Artificial y Algoritmos

En el marco del presente trabajo, resulta imprescindible definir conceptualmente qué se entiende por inteligencia artificial (IA) y por algoritmo, ya que estos no solo constituyen elementos técnicos centrales en los sistemas de videovigilancia contemporáneos, sino que también deben ser abordados como tecnologías sociales e institucionales, profundamente inscritas en racionalidades de gobierno, producción de saber y ejercicio del poder.

Autores como Kate Crawford proponen pensar en la IA desde una mirada crítica que se aleja del pensamiento de que la misma es una forma de inteligencia autónoma, capaz de actuar de manera “objetiva” o “neutral”. Dicha autora describe en su libro “ Atlas de la inteligencia artificial”, como la IA no es una entidad separada de lo humano, sino una forma específica de organización sociotécnica, construida a partir de bases de datos, sistemas computacionales, decisiones humanas, lógicas estadísticas, objetivos políticos y marcos normativos. En este sentido, Crawford (2022), sostiene que la IA no es ni artificial ni particularmente inteligente, más bien está generada a partir de una infraestructura extractiva que recopila datos de los cuerpos, la tierra y las vidas humanas para alimentar redes.

Desde esta perspectiva, la inteligencia artificial debe pensarse como una tecnología profundamente situada, cuyos efectos no son simplemente informáticos, sino sociales, económicos, ecológicos y políticos. En lugar de ver la IA como una herramienta neutral que refleja la realidad, Crawford la define como una estructura que produce realidad, organizando lo visible, lo pensable y lo posible. Otro de los ejes sumamente importantes en los cual se debe reflexionar es en el posicionamiento que muchas veces se le coloca a la IA como una tecnología abstracta o una entidad inmaterial, la IA se manifiesta como una industria extractiva de alcance global, con una materialidad concreta y profundamente dañina. “La IA no es artificial ni inteligente. Más bien existe de forma corpórea, como algo material, hecho de recursos naturales, combustible, mano de obra, infraestructuras, logística, historias y clasificaciones” (Crawford, 2022, p. 33).

Desde una mirada geológica, la inteligencia artificial puede entenderse como una prolongación de la propia Tierra, ya que depende de la explotación sistemática y repetida de minerales cuya formación tardó miles de millones de años en la corteza terrestre. Este fenómeno, conocido como extractivismo, enlaza el “tiempo profundo” del planeta con la inmediatez de las operaciones computacionales actuales. La demanda creciente de recursos como el litio frecuentemente llamado “oro blanco” en zonas como Bolivia o Nevada, evidencia que la base material de la IA es limitada conllevando a su vez procesos de degradación ambiental y contaminación que afectan de manera directa a los ecosistemas locales, “La nube es la columna vertebral de la industria de la IA y está hecha de rocas, litio en salmuera y petróleo crudo” (Crawford, 2022, p. 88).

De igual modo, la infraestructura que sostiene aquello que comúnmente se denomina “la nube” está lejos de ser intangible o liviana. Se trata de una red física de centros de datos altamente demandantes de energía y agua, que convierten estos recursos en capacidad de cómputo. Este sistema genera una contaminación de carbono que ya alcanza niveles comparables a los de la industria aeronáutica mundial, impulsada por un “maximalismo computacional” que requiere grandes cantidades de horas de procesamiento para entrenar modelos de lenguaje. Finalmente, esta materialidad se ve reflejada en la logística del transporte, contenedores estandarizados trasladan hardware a lo largo de rutas que muchas veces reproducen antiguos circuitos coloniales, para terminar en basurales de desechos electrónicos que cierran un ciclo de vida marcado por la obsolescencia programada.

En términos operativos, la inteligencia artificial se basa en la utilización de algoritmos, es decir, conjuntos finitos de instrucciones matemáticas y lógicas que permiten procesar grandes volúmenes de datos, identificar patrones, establecer correlaciones y tomar decisiones automatizadas o semiautomatizadas. Si bien los algoritmos han existido desde hace siglos en el campo de las matemáticas, su incorporación masiva en sistemas informáticos ha dado lugar a una transformación radical del modo en que se gestiona la información en las sociedades contemporáneas. Esta opacidad algorítmica no es solo técnica, sino que tiene consecuencias políticas concretas, los algoritmos no explican por qué toman las decisiones que toman, pero sí generan efectos reales sobre los cuerpos, los territorios y las trayectorias de vida de las personas. De allí que muchos autores hablen hoy de una forma de gobierno algorítmico, es decir, de un tipo de

gubernamentalidad que no actúa mediante leyes explícitas ni normas universales, sino por medio de correlaciones estadísticas, puntuaciones, filtros y segmentaciones de comportamiento.

Esta forma de gobierno algorítmico ha sido analizada por autores como Antoinette Rouvroy y Thomas Berns (2016), plantean que los algoritmos no se basan en la interpretación jurídica ni en la evaluación moral, sino en la anticipación automática de lo probable. “Esta forma de gobierno recae esencialmente sobre lo que podría advenir, sobre las propensiones antes que sobre las acciones cometidas, a diferencia de la represión penal o de las reglas de responsabilidad civil, por ejemplo, que se encuentran concernidas sólo por infracciones que ya se habrían cometido” (Rouvroy & Berns, 2016, p. 106)” Este rasgo anticipatorio es especialmente relevante para el análisis de los sistemas de videovigilancia inteligente, donde la IA no actúa sobre eventos ocurridos, sino sobre comportamientos considerados sospechosos antes de que se produzca un delito, según modelos entrenados sobre datos históricos que cargan, muchas veces, sesgos estructurales.

Una noción que nos sirve para poder pensar y problematizar la noción de inteligencia artificial es la del *Nooscopio*, por un lado nos permite comprender el concepto teórico y técnico de lo que es denominado inteligencia artificial y por otro lado también nos sirve para poder visualizar qué aspectos sociales y políticos son parte de dicho concepto , para comprender la noción de nooscopio se debe pensar a la inteligencia artificial como una infraestructura epistémica y política destinada a la extracción, formalización y explotación del conocimiento social. En este sentido, Pasquinelli y Joler (2020) proponen a dicho concepto como una metáfora crítica que permite desplazar la narrativa dominante sobre la IA como tecnología autónoma o casi mágica, para situarla en el terreno de los dispositivos históricos de medición y captura de información. Así como el microscopio funcionó como una herramienta que amplificó la visión del mundo biológico y el telescopio la del espacio y el cosmos, el nooscopio se desarrolla como un instrumento orientado a observar, medir y modelizar la inteligencia colectiva, es decir, la producción social de conocimiento.

Desde el punto de vista técnico, el funcionamiento de la IA contemporánea se basa en la articulación entre grandes volúmenes de datos, modelos matemáticos y capacidades computacionales de procesamiento. Sin embargo, Pasquinelli insiste en que los datos no

constituyen una materia prima neutral ni espontánea que se encuentra en el campo de observación, más bien son el resultado de procesos sociales de captura, estandarización y codificación que transforman prácticas humanas heterogéneas en unidades cuantificables. La IA depende estructuralmente de esta traducción de la experiencia social en datos, que luego son reorganizados mediante técnicas estadísticas, particularmente el aprendizaje automático para detectar patrones, correlaciones y regularidades. En este sentido, el aprendizaje automático no implica que la máquina “comprenda” el mundo, sino que optimiza funciones matemáticas a partir de ejemplos previos, generando modelos probabilísticos capaces de clasificar o predecir nuevos casos.

La dimensión social del funcionamiento de la IA se vuelve evidente cuando se analiza el origen de esos datos y los efectos de su modelización. Los sistemas de aprendizaje automático se entrenan sobre bases de datos que condensan prácticas culturales, relaciones económicas, desigualdades históricas y decisiones institucionales Pasquinelli y Joler (2020). De este modo, se puede comprender que los sesgos no son anomalías accidentales del sistema, sino la cristalización estadística de asimetrías preexistentes. La IA no inventa los prejuicios, pero puede amplificarlos y naturalizarlos al inscribirlos en algoritmos que operan bajo la apariencia de objetividad técnica. El nooscopio, en tanto instrumento de extracción de conocimiento social, reorganiza la inteligencia colectiva en modelos matemáticos que luego retornan sobre la sociedad en forma de decisiones automatizadas.

Un aspecto central para esta reflexión desarrollada por Pasquinelli y Joler (2020) es que la IA no produce conocimiento en el sentido creativo o inventivo que tradicionalmente se atribuye a la inteligencia humana, sino que redistribuye y recombina saberes ya existentes. El entrenamiento de un modelo implica una fase intensiva de trabajo humano: etiquetado de datos, diseño de arquitecturas y ajuste de parámetros. Incluso en sistemas altamente automatizados, la intervención humana permanece como condición estructural del funcionamiento técnico. La idea de una inteligencia artificial autónoma encubre una extensa red de procesamiento cognitivo distribuido que alimenta y sostiene la infraestructura algorítmica. En este sentido, el nooscopio puede entenderse como un dispositivo de extracción de valor cognitivo, análogo a cómo la máquina industrial extraía fuerza de trabajo físico.

En el plano operativo, los sistemas de IA funcionan principalmente a través de dos grandes operaciones, **clasificación y predicción**. Clasificar implica asignar una entidad ,una imagen, un texto, un rostro, una conducta, a una categoría previamente definida en el entrenamiento del modelo. Predecir alude a estimar la probabilidad de que ocurra un evento futuro a partir de patrones pasados. Estas operaciones tienen consecuencias políticas cuando se aplican a ámbitos como la seguridad, el crédito financiero, la gestión del empleo o la administración pública. La clasificación algorítmica organiza poblaciones en perfiles de riesgo, segmentos de consumo o categorías de comportamiento, mientras que la predicción introduce una lógica anticipatoria que orienta intervenciones preventivas.

El manifiesto de Pasquinelli y Joler (2020) también menciona los límites epistémicos de la IA. Los modelos de aprendizaje pueden alcanzar niveles altos de precisión en tareas específicas, pero su funcionamiento se basa en correlaciones estadísticas y no en comprensión semántica o causalidad explicativa. Esto implica que los sistemas pueden ser altamente eficaces en la identificación de patrones sin poseer un conocimiento del significado o del contexto de los mismos. La opacidad de muchos modelos complejos, particularmente en redes neuronales profundas, refuerza esta limitación, incluso para sus diseñadores, resulta difícil rastrear con exactitud cómo se llega a una determinada decisión.

Otro punto fundamental es la crítica al mito de la autonomía tecnológica. Pasquinelli y Joler (2020) al igual que Crawford (2022) , cuestionan la narrativa según la cual la IA evoluciona por una lógica interna independiente de las condiciones sociales. Por el contrario, el desarrollo de la inteligencia artificial está profundamente implicado con intereses económicos, estrategias corporativas, políticas estatales e infraestructuras materiales específicas. Los centros de datos, la energía necesaria para el entrenamiento de modelos, la propiedad de los conjuntos de datos y la concentración de recursos computacionales configuran un entramado de poder que condiciona qué tipo de sistemas se desarrollan y con qué fines. La IA no es un sujeto histórico autónomo, más bien, es un ensamblaje sociotécnico inscrito en relaciones de producción y gobierno.

Además, la noción de nooscopio nos permite comprender la inteligencia artificial como una tecnología de captura y reorganización de la inteligencia colectiva (Pasquinelli y Joler, 2020). A nivel técnico, opera mediante la extracción de datos, la construcción de modelos estadísticos y la optimización de funciones matemáticas para clasificar y predecir. A nivel

social, reorganiza prácticas humanas en métricas cuantificables, consolida sesgos estructurales en decisiones automatizadas y se inserta en estrategias de acumulación económica y gestión poblacional. La IA, lejos de ser una mente artificial autónoma, funciona como un dispositivo que traduce la complejidad social en patrones matemáticos operativos, reintroduciendo luego esos patrones en la sociedad bajo la forma de normas algorítmicas que influyen en comportamientos, oportunidades y distribuciones de poder.

Seguridad

Michel Foucault en su curso *Seguridad, territorio y población*, dictado en el Collège de France en 1978, Foucault analiza el surgimiento de nuevas racionalidades gubernamentales en Europa a partir del siglo XVIII, y desarrolla con profundidad el concepto de *seguridad* como una forma de gobierno de las poblaciones. Este concepto permite comprender los modos actuales en los que el Estado interviene en la vida de la población, particularmente a través del uso de tecnologías orientadas a la gestión de riesgos y a la previsión de ciertas conductas que no son aceptadas.

A diferencia de las formas de poder soberano centradas en la ley, la prohibición y el castigo o también el poder disciplinario que actúa sobre los cuerpos para moldear a los sujetos y establecer ciertos comportamientos como “normales”, la seguridad se configura como una tecnología de poder que actúa sobre las condiciones de posibilidad de la población. Foucault sostiene que en la seguridad no se trata tanto de impedir que algo ocurra, sino de permitir que ocurra en ciertas condiciones. A través de esta forma de pensar, el gobierno no se preocupa especialmente por erradicar los fenómenos indeseados (como el crimen, la enfermedad o la pobreza), sino por gobernar y controlar su distribución estadística dentro de un umbral aceptable “Lo que caracteriza en esencia el mecanismo de seguridad es, creo, la gestión de esas series abiertas y que, por consiguiente, sólo pueden controlarse mediante un cálculo de probabilidades. “Lo que caracteriza en esencia el mecanismo de seguridad es, creo, la gestión de esas series abiertas y que, por consiguiente, sólo pueden controlarse mediante un cálculo de probabilidades” (Foucault, 2006).

El poder de seguridad se diferencia entonces del castigo, ya que no se centra en el acto individual, sino en el fenómeno social. El problema no es que un sujeto rompa una norma

o regla por sí mismo, sino aquellos actos que son reproducidos socialmente, transformándose en amenazas para la vida colectiva. La seguridad se basa en una lógica gubernamental enfocada en la gestión del riesgo, en la anticipación y regulación de comportamientos probables.

Esta noción de seguridad transforma la noción de lo gobernable, ya que no se gobiernan solamente territorios o individuos como en un pasado, sino que se gobierna a la población como conjunto medible, el cual es transformado en datos que son utilizados por la estadística, la demografía, y en nuestra contemporaneidad los algoritmos.

En *Seguridad, territorio y población*, Foucault muestra cómo esta forma de gobierno implica también una modificación del espacio, ya que la seguridad no actúa en espacios cerrados propios de la sociedad disciplinaria como la escuela, la fábrica o la prisión, sino que como forma de ampliación, sale de los espacios institucionales tradicionales para intervenir en espacios abiertos y urbanos.

La seguridad como racionalidad de gobierno también supone una transformación en la subjetividad. A diferencia de la disciplina, que está enfocada en producir sujetos que respetan normas establecidas y normalizadas, la seguridad busca producir sujetos que se autogestionan en relación con el riesgo, entonces el ciudadano debe administrar su propio comportamiento en un entorno que es vigilado, entendiendo que algunas conductas pueden ser riesgosas o sospechosas. Entonces, esto nos puede servir para pensar sobre el contexto actual, los comportamientos de los sujetos se construyen bajo una lógica de creencias y autocontrol de lo que puede estar bien o lo que puede estar mal, la cual va a estar siendo evaluada por algoritmos y estadísticas a través de la recopilación masiva de datos, la detección automatizada de comportamientos y la generación de alertas predictivas. No se limitan a observar la realidad, sino que participan activamente en su producción, organizando la experiencia de los sujetos, sus márgenes de movimiento, y la manera en que deben anticiparse a sí mismos para no ser detectados como desviación estadística.

Desarrollo

1.0 Gobierno digital, vigilancia y tecnopolítica en Uruguay

1.1 Tecnologías de vigilancia inteligente en Uruguay: despliegue estatal y justificaciones técnicas

El Ministerio del Interior, junto a la Policía Nacional, presentó una nueva tecnología implementada en sus planes de seguridad (Presidencia de la República, 2024). La misma funciona a través de analíticas e inteligencia artificial aplicada a la red de cámaras de videovigilancia instaladas en la vía pública. En términos analíticos, esta incorporación tecnológica puede comprenderse como parte de una racionalidad contemporánea de gobierno que desplaza el eje de intervención hacia el procesamiento de datos y la gestión anticipatoria de las conductas en la vía pública. Esto podría ser pensado a través de Foucault (2006), como un dispositivo de seguridad, en términos de que no busca únicamente prohibir o sancionar hechos consumados, sino intervenir sobre la probabilidad de su ocurrencia mediante el cálculo de variables que permiten regular las condiciones de posibilidad de los ciudadanos.

Nicolás José Martinelli Waksman, Ministro del Interior de Uruguay desde el 6 de noviembre de 2023 hasta el 1 de marzo de 2025, mencionó que en este periodo se realizó una inversión récord (Presidencia de la República, 2024) dirigida hacia las tecnologías aplicadas a la seguridad pública, trayendo tecnología que implementan los países más desarrollados del mundo. El énfasis sobre la infraestructura tecnológica evidencia una transformación en la modalidad de intervención estatal, donde la capacidad de cálculo, almacenamiento y procesamiento de información adquiere un rol estratégico en la definición de políticas de seguridad.

Dentro de estas tecnologías se han incorporado “El sistema de detección temprana de disparos Shotspotter, el escáner 3D que utiliza Policía Científica, los cuatro nuevos escáneres corporales para las cárceles, los inhibidores de señales próximos a ser instalados, el sistema biométrico para medias alternativas, la transmisión de videos en tiempo real desde los helicópteros que patrullan (cuya señal es recibida por el CCU), los handys que operan con antenas propias y con un sistema encriptado que además va a

poder transmitir videos en tiempo real, la compra de nuevas cámaras corporales y drones con visores nocturnos" (Presidencia de la República, 2024). Este conjunto heterogéneo de dispositivos configura una red técnica interconectada que amplía las capacidades de captación y circulación de información, consolidando una infraestructura de vigilancia que opera de manera distribuida sobre distintos espacios y situaciones.

Además, se anunció la futura incorporación del sistema de patrullaje inteligente basado en la geolocalización de los móviles policiales y un sistema de detección temprana de incendios por cámaras, estas prácticas se dirigen hacia una intervención enfocada en la sincronización permanente entre captación de datos y capacidad de respuesta.

El Director General del Centro de Comando Unificado, Gabriel Lima, señaló que su equipo llevó a cabo una investigación detallada sobre los patrones de comportamiento que presentan las personas antes, durante y después de cometer un delito. Esta información fue sistematizada y transferida a la empresa responsable del desarrollo del software de inteligencia artificial, creando así una red neuronal capaz de procesar en tiempo real los datos recogidos por las cámaras de videovigilancia. Este sistema está diseñado para identificar comportamientos sospechosos a partir del análisis de estas conductas previamente modeladas (Presidencia de la República, 2024). Este procedimiento implica un desplazamiento significativo, la intervención no se orienta principalmente hacia sujetos individualizados, sino hacia conductas formalizadas en modelos algorítmicos, en este sentido, este sistema digital puede ser pensado como una máquina taxonómica (Bruno, 2013), en la medida en que transforma rastros visuales recortados de un momento específico, los cuales forman parte de un fragmento de un suceso y luego los clasifica en categorías que habilitan a alertas automáticas.

El proyecto comenzó con la implementación de 2.000 cámaras ubicadas de forma estratégica según un análisis previo de los tipos de delitos más frecuentes, mapas de calor delictivos y datos temporales. El Ministerio del Interior declaró que esta forma de localización permite aplicar analíticas específicas en las cámaras según el contexto espacial y temporal, optimizando así la prevención del delito (Presidencia de la República, 2024). Además, estos análisis previos sirven para prevenir encuentros que dejan al descubierto a los funcionarios públicos por situaciones peligrosas y, por ende, también se disminuye el riesgo a la exposición constante de los funcionarios. La utilización de mapas de calor expresa una racionalidad territorial que considera el espacio público como una

superficie cuantificable, esto podría ser pensado a través de como Foucault (2006), define como operan los dispositivos de seguridad sobre el medio, regulando acciones y circulaciones más que imponiendo prohibiciones absolutas. La ciudad aparece así segmentada en zonas de mayor o menor intensidad de monitoreo en función de su inscripción estadística.

La cantidad de cámaras que se incorporaron en los últimos años fue creciendo de forma significativa, según declaraciones del Ministro del Interior, al inicio del periodo de gobierno (2020) se contaba con aproximadamente 5.900 cámaras operativas, cifra que aumentó a 14.000 al cierre del período de gobierno. Además, se anunció que ya se encontraba planificada una nueva licitación para la instalación de 5.000 cámaras adicionales, con el objetivo de garantizar la continuidad del proyecto en la próxima administración de gobierno (Ministerio del Interior, 2024b).

Se plantea la selección de los lugares en las que se instalan estas cámaras como puntos estratégicos correspondientes a un criterio técnico, el cual está relacionado con el análisis de datos sobre los delitos cometidos y en la percepción subjetiva de inseguridad por parte de la ciudadanía. Este procedimiento, denominado “mapa de calor”, permite identificar zonas de mayor conflictividad o vulnerabilidad desde una lógica tanto estadística como territorial (Ministerio del Interior, 2024b). La articulación entre datos objetivos y percepción subjetiva de inseguridad nos sirve para pensar sobre cómo la gestión del riesgo combina dimensiones cuantificables con elementos vinculados a la sensibilidad social, configurando un campo de intervención donde la seguridad se construye a partir de la convergencia entre cálculo estadístico y demandas ciudadanas.

Además del análisis territorial que determina dónde colocar las cámaras, se suma un avance tecnológico importante, estos dispositivos no solo graban y registran los hechos que suceden en la vía pública sino que también incorporan inteligencia artificial capaz de analizar los movimientos de las personas mientras ocurren. Roba (2024) describe el funcionamiento actual del sistema de cámaras del Ministerio del Interior, expresando que dichas cámaras son capaces de generar alertas automáticas ante la detección de ciertos movimientos corporales considerados atípicos o potencialmente delictivos. Entre estos movimientos se encuentran gestos como levantar las manos, permanecer en el suelo o realizar movimientos considerados erráticos. Esta capacidad de anticipación se basa en la identificación de patrones de comportamiento previamente definidos como “sospechosos”,

lo cual muestra cómo la vigilancia se vuelve predictiva y performativa, moviéndose del registro hacia la intervención de un suceso antes de ser cometido.

La transformación de los gestos corporales en “patrones sospechosos” nos sirve de ejemplo para pensar lo que Fernanda Bruno (2013) denomina como máquina taxonómica, los comportamientos dejan de ser observados para ser clasificados dentro de categorías algorítmicamente definidas, produciendo tipologías de conducta en tiempo real. Además, la intervención inmediata ante estos patrones puede servirnos para pensar la idea de modulación desarrollada por Maurizio Lazzarato (2012), en la medida en que el dispositivo actúa sobre el despliegue del comportamiento, ajustándose dentro de un entorno que opera de manera continua.

Otro de los puntos importantes es la participación de la comunidad. Según expresó el director de Convivencia y Seguridad Ciudadana, Matías Terra (Ministerio del Interior, 2024b), el proyecto se fortalece mediante la articulación con actores locales y el involucramiento de la comunidad. Destacó además que la incorporación de inteligencia artificial en las cámaras implica una transformación en los modos de vigilancia, pasando de una lógica reactiva a una vigilancia proactiva, orientada a la anticipación de eventos y no únicamente a su registro posterior.

Los artículos publicados por la presidencia Uruguaya (Ministerio del Interior, 2024a) muestran cómo estas tecnologías se han ido extendiendo a lo largo del país, por ejemplo, el 14/08/2024 se inauguró la implementación de 17 cámaras nuevas en libertad, San José. El Ministerio del Interior anunció la incorporación de estas nuevas cámaras en la localidad, alcanzando un total de 73 dispositivos operativos en distintos puntos estratégicos de la ciudad. Según informaron autoridades como el director del Centro de Comando Unificado, Gabriel Lima, y el jefe de Policía de San José, Atilio Rodríguez, esta ampliación forma parte de un plan de modernización tecnológica en el sistema policial,ya que en el departamento de San José ya estaban funcionando más de 340 cámaras.

1.2 El software Axxon One como ejemplo de una vigilancia predictiva y automatizada.

La empresa internacional AxxonSoft ha sido incorporada en la comercialización de software gracias a la empresa uruguaya Commandline (que actúa como integrador y representante local de esta empresa de soluciones tecnológicas de videovigilancia), ha desarrollado y comercializa el software de gestión de video con analítica inteligente denominado Axxon Next. Este software funciona mediante algoritmos capaces de identificar en tiempo real ciertos comportamientos humanos que pueden ser considerados sospechosos o potencialmente peligrosos. Algunas de las conductas que reconoce automáticamente suelen estar relacionadas con movimientos poco habituales, permanencias prolongadas en zonas determinadas o gestos y expresiones que pueden indicar situaciones de emergencia.

Según la información técnica difundida por la propia empresa, otra de las características del software es que su precisión puede mejorar a medida que se utiliza, debido a que posee capacidades de aprendizaje automático que le permiten ajustarse progresivamente a los entornos en los que se implementa. Además, este tipo de plataformas tiene la capacidad de integrar distintas fuentes de información como audio, video y ubicación, lo que permite crear mapas dinámicos que muestran zonas de riesgo en tiempo real. No existe información pública oficial que confirme qué software específico utiliza el Ministerio del Interior de Uruguay ni qué empresas han sido responsables de su desarrollo o adaptación, por lo que estas características se describen aquí a modo de referencia tecnológica general.

El software Axxon One desempeña un papel central en la consolidación de un modelo de videovigilancia que se orienta hacia una lógica predictiva y automatizada, en consonancia con los procesos contemporáneos de digitalización de la seguridad pública a nivel internacional. Desarrollado por la empresa AxxonSoft, este Video Management Software (VMS) se caracteriza por su arquitectura modular y escalable, lo cual le permite administrar de manera centralizada y distribuida un número prácticamente ilimitado de cámaras, servidores y estaciones de trabajo, integrando además distintos dispositivos de terceros gracias a su diseño basado en estándares abiertos (AxxonSoft, s.f.a). Esta

flexibilidad técnica resulta clave para comprender cómo la plataforma logra adaptarse tanto a sistemas de pequeña escala como a redes urbanas de gran magnitud.

Entre sus prestaciones más relevantes, Axxon Next incluye un conjunto de herramientas de búsqueda forense inteligente, que marcan un quiebre respecto de los sistemas tradicionales de revisión manual de grabaciones. Dentro de estas herramientas destacan Momento Quest y TimeCompressor, cuya implementación permite comprender la manera en que la vigilancia se vuelve más selectiva y automatizada.

MomentQuest funciona a través de la generación de metadatos, es decir, información adicional que describe los objetos y movimientos registrados en las imágenes de video. Cada fragmento de grabación se acompaña de datos como color, tamaño, dirección y velocidad, lo que habilita búsquedas extremadamente precisas en grandes volúmenes de material audiovisual. Por ejemplo, frente a un hurto en la vía pública, un operador puede solicitar al sistema que localice a “una persona con campera roja que se desplaza hacia el norte”, y el software devolverá en segundos todas las escenas que cumplan esos criterios (Security Informed, s. f.). Esta herramienta acelera la identificación de eventos relevantes y refuerza el carácter proactivo del control, dado que son los algoritmos los que filtran y jerarquizan la información.

En tanto, TimeCompressor condensa horas de grabación en un único vídeo en el cual todos los objetos en movimiento captados en momentos diferentes aparecen proyectados de manera simultánea. Esta función permite que un operador pueda revisar, en pocos minutos, lo que ocurrió durante varias horas, visualizando de manera condensada la circulación de personas y vehículos en un área determinada (SourceSecurity, s. f.). Si bien no altera los eventos originales, este recurso facilita la detección de patrones de movilidad y la identificación de conductas inusuales, optimizando las investigaciones retrospectivas como la anticipación de posibles riesgos.

Otro aspecto relevante de Axxon One es su capacidad de gestión distribuida y acceso remoto. El software habilita la supervisión a través de clientes web o aplicaciones móviles, lo que descentraliza las prácticas de control y permite monitorear en tiempo real desde múltiples dispositivos conectados a internet (AxxonSoft, s.f.c). Esta característica implica que la vigilancia no dependa exclusivamente de un centro de comando único, sino que puede articularse en red, extendiendo su alcance territorial y la inmediatez de las

respuestas. Además, la integración con otros sistemas de seguridad como alarmas, detección de incendios y plataformas de control de accesos implica una lógica de interconexión tecnológica, donde distintos flujos de datos convergen en una misma interfaz.

En forma de análisis se podría pensar que el software Axxon One utilizado en sistemas dirigidos a la seguridad estatal apoya la idea de la máquina taxonómica. A través de herramientas como MomentQuest, que descompone las imágenes en metadatos de color, tamaño y velocidad, el dispositivo deja de interesarse por la identidad integral del sujeto para centrarse en fragmentos del comportamiento que permiten construir perfiles probabilísticos. Esta capacidad de detección automática de movimientos "erráticos" posiciona a la videovigilancia en la lógica de la gubernamentalidad algorítmica, donde el poder ya no actúa sobre infracciones cometidas, sino sobre las probabilidades de lo que podría suceder, también se puede pensar en cómo este software opera como una máquina de ver en el sentido de que participa activamente en la producción de lo real, estableciendo jerarquías de relevancia en la toma de información de su entorno posicionándose en una postura de elección y recorte de lo sucedido en el espacio público.

1.3: Digitalización estatal y tecnopolítica: el caso uruguayo desde la perspectiva de AGESIC.

La Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (Agesic) planteó, en su *Memoria Anual 2017*, una serie de puntos a seguir que marcaron un antes y un después en el proceso de transformación tecnológica y digital del Estado uruguayo.

El documento propone entender la digitalización como algo mucho más profundo que la incorporación de tecnología, se la presenta como un proceso que atraviesa aspectos culturales, sociales y políticos. En ese sentido, se afirma que “transformación digital es una forma de replantearnos lo que hacemos día a día. Se trata de una transformación que socava paradigmas, nos propone otra forma de interactuar, de relacionarnos entre nosotros y con el mundo, a través de un cambio cultural que a veces apenas vemos pero que ya está ahí” (AGESIC, 2017, p. 2).

A partir de esta mirada, AGESIC promueve una redefinición de la acción estatal, que no se limita a modernizar infraestructuras, sino que busca transformar el modo en que el Estado se vincula con la ciudadanía. La propuesta apunta a incorporar herramientas digitales que permitan trabajar con más eficiencia, garantizando al mismo tiempo una mayor equidad y participación. Esto implica cambios en diferentes áreas clave, como la gestión documental, los servicios digitales, la interoperabilidad entre organismos públicos y el fortalecimiento de políticas de ciberseguridad (AGESIC, 2017).

Uno de los ejes donde este enfoque cobra mayor importancia es en el campo de la seguridad pública. Allí, el documento señala una tendencia creciente hacia lo que denomina “gobierno inteligente”, donde el Estado se apoya cada vez más en datos y tecnologías emergentes para planificar e intervenir. Se destacan especialmente herramientas como el análisis predictivo, el aprendizaje automático (machine learning), el Big Data y el Internet de las Cosas (IoT), con el objetivo de adelantarse a posibles escenarios de riesgo, automatizar respuestas y tomar decisiones de forma más ágil y fundamentada (AGESIC, 2017).

También se plantea el compromiso de Uruguay con marcos internacionales vinculados a la gobernanza digital y los derechos humanos, se mencionan aspectos como la interoperabilidad de sistemas públicos, la protección de datos personales y la transparencia en la gestión. La participación activa del país en espacios como el Banco Interamericano de Desarrollo o la OCDE refuerza su posicionamiento regional como referente en transformación digital del sector público.

La transformación digital que propone AGESIC debe de pensarse más allá de la creación y aplicación de nuevas tecnologías digitales, se puede ver cómo se dirige hacia la construcción de un dispositivo de poder moderno. Al decir que esta digitalización "socava paradigmas" y redefine nuestra forma de relacionarnos, AGESIC está describiendo el avance de la gubernamentalidad, ese arte de conducir la conducta de los ciudadanos a través de una red invisible de trámites, datos e interfaces digitales.

1.4 La Estrategia Nacional de Inteligencia Artificial 2024–2030: lineamientos estatales sobre IA.

Uruguay ha avanzado en la construcción de un marco normativo y estratégico para el desarrollo de la inteligencia artificial como parte de su agenda digital. Un hito central en ese proceso fue la publicación de la *Estrategia Nacional de Inteligencia Artificial 2024–2030*, donde se establece que la IA debe ser entendida como una política pública transversal que atraviesa múltiples sectores, la cual puede ser una herramienta clave para el Estado. “La IA constituye una herramienta tecnológica de gran relevancia en un escenario de acelerada transformación digital” (AGESIC, 2024, p. 8).

En este marco, el Estado uruguayo plantea que su desarrollo debe estar orientado al bien público, de forma ética, responsable, sustentable y centrada en las personas.

Esta estrategia Nacional tiene como objetivos específicos:

1- “establecer un marco de gobernanza que garantice el desarrollo y uso ético, responsable y seguro de la IA, asegurando una institucionalidad adecuada, marcos regulatorios claros y procesos eficientes que promuevan la transparencia, la seguridad, la inclusión y la seguridad jurídica en el ámbito de la IA”. (AGESIC, 2024, p. 21).

2- “desarrollar las capacidades y las condiciones nacionales necesarias para fomentar y aprovechar la innovación y la aplicación de la IA, con un enfoque integral que contemple la infraestructura, los datos, la gestión del talento y las habilidades”. (AGESIC, 2024, p. 21).

3- “Aprovechar la IA como motor clave para el crecimiento económico con inclusión, el desarrollo sostenible del país, el fortalecimiento de la competitividad del sector privado, la profundización del proceso de transformación digital del Uruguay, la mejora de la gestión y los servicios públicos, y potenciar la investigación y la innovación. Maximizar los beneficios de esta tecnología para la sociedad considerando los impactos positivos y mitigando los posibles impactos adversos, desarrollando las capacidades para la integración crítica de la IA en la sociedad.” (AGESIC, 2024, p. 21).

Uno de los elementos que más se destaca en la estrategia es el uso de estas tecnologías en el sector público para mejorar la eficiencia de los servicios y anticiparse a problemas

sociales complejos. Se promueve el uso de datos y modelos predictivos, siempre que sean respetados algunos principios fundamentales para la protección de la ciudadanía, como la transparencia, la supervisión humana y la protección de derechos. “cuando los sistemas de IA se utilicen para tomar decisiones o apoyar la toma de decisiones, siempre haya una supervisión humana sobre los resultados producidos por la IA, siendo pertinente considerar las características que debe tener dicha supervisión fundamentalmente en los sistemas de alto riesgo” (AGESIC, 2024, p. 29). En este punto se reconoce que el uso de IA en decisiones críticas implica ciertos riesgos éticos, por esta razón se establece que “cuando los sistemas de IA se utilicen para tomar decisiones ...” (AGESIC, 2024, p. 29), deberá existir supervisión humana. Esta supervisión alude a un intento de mantener el equilibrio entre automatización y control institucional, aunque deja abierto el debate sobre cómo y quiénes supervisan, con qué criterios, y con qué consecuencias.

También aparece en el documento un tema fundamental, el cual se refiere a en qué sectores específicos se espera que la inteligencia artificial tenga un mayor impacto. Entre ellos, se destaca la seguridad, que es abordada como una de las áreas prioritarias para el uso de soluciones tecnológicas basadas en IA. El documento no plantea qué herramientas concretas se utilizaran, pero deja en claro que uno de los objetivos para el desarrollo en los próximos años es el de fortalecer las capacidades del Estado en la gestión de riesgos, tanto a nivel preventivo como operativo.

Por otro lado, también se generan planteamientos sobre los riesgos asociados a este tipo de tecnologías, especialmente en lo que refiere al respeto de los derechos fundamentales. La estrategia advierte que el uso de inteligencia artificial sin control puede afectar derechos como la privacidad, la igualdad, el debido proceso o la libertad de expresión si no se aplican con el debido cuidado. Por eso es importante entender la necesidad de desarrollar y adoptar marcos normativos que garanticen su uso ético y responsable “Para los organismos públicos, la implementación de este principio supone el deber específico de mantener o adoptar medidas para asegurar que las soluciones tecnológicas que utilicen IA que desarrollen, adquieran o utilicen en el ejercicio de sus cometidos, respeten la dignidad humana y los derechos de las personas.”(AGESIC, 2024, p. 28).

En cuanto a este último punto dirigido al desarrollo ético y centrado en las personas, existen algunos elementos que deben analizarse en profundidad para ver si no existen inflexiones en los derechos de los ciudadanos Uruguayo. La ENIA promueve el uso de

modelos predictivos, pero como menciona Pasquinelli y Joler (2020) con su noción del nooscopio, una infraestructura que extrae el conocimiento social para devolverlo en forma de clasificaciones automáticas interfiere también en cómo es pensado al sujeto en el espacio público, se corre el riesgo de que el ciudadano deje de ser considerado como un sujeto de derechos para convertirse en un simple "perfil de riesgo" dentro de una máquina taxonómica. Aunque el documento menciona la necesidad de una "supervisión humana" para sistemas de alto riesgo, el poco conocimiento ciudadano de cómo funcionan en realidad estos sistemas genera una asimetría de poder donde la transparencia no es totalmente clara.

2.0 Aplicaciones estatales de la videovigilancia inteligente en Uruguay

2.1 Reconocimiento facial en la vía pública

El reconocimiento facial automatizado constituye una de las tecnologías de vigilancia biométrica más relevantes incorporadas por el Estado uruguayo en el marco de las políticas de seguridad pública y control poblacional. Su despliegue ha sido impulsado principalmente por el Ministerio del Interior, que ha integrado sistemas de reconocimiento facial a infraestructuras ya existentes de videovigilancia, como el Sistema Integrado de Videovigilancia y Emergencia (SIVVE), así como a dispositivos específicos de control en espectáculos deportivos, control migratorio y supervisión de medidas penales. Este proceso se ha visto facilitado por la creación de una base de datos de identificación facial de alcance nacional, habilitada a partir de los artículos 191 y 192 de la Ley de Presupuesto de 2020, que autorizaron la migración de imágenes faciales de personas mayores de edad desde la Dirección Nacional de Identificación Civil hacia el Ministerio del Interior, adquiriendo la información biométrica necesaria para el funcionamiento de estos sistemas (Datysoc, 2022).

La tecnología de reconocimiento facial se utiliza, por ejemplo, en estadios deportivos, orientada a impedir el ingreso de personas incluidas en registros de antecedentes por hechos de violencia, mientras que en el ámbito penitenciario y de la libertad asistida se emplea como mecanismo de verificación de identidad para personas que cumplen arresto domiciliario. A su vez, en los aeropuertos internacionales y en los pasos fronterizos, el

reconocimiento facial se integra a sistemas automatizados de control migratorio que buscan agilizar los procesos de verificación documental y detectar posibles irregularidades en el ingreso o egreso del país (Díaz Charquero, 2022)

Nuevamente, como señala Bruno (2013), las formas algorítmicas de ver taxonomizan los cuerpos en tiempo real mientras circulan por la vía pública, convirtiendo esa presencia física en datos capaces de ser comparados.

La situación actual del reconocimiento facial en Uruguay se caracteriza por una serie de tensiones normativas y desafíos institucionales que complejizan su análisis. Si bien la Ley N.º 18.331 de Protección de Datos Personales reconoce a los datos biométricos como una categoría especialmente sensible y establece la obligatoriedad de realizar evaluaciones de impacto previas a su tratamiento, las bases de datos destinadas a la seguridad pública quedan excluidas del ámbito de supervisión de la Unidad Reguladora y de Control de Datos Personales. Esta excepción legal ha permitido que el Ministerio del Interior implemente sistemas de reconocimiento facial sin un control especializado externo y sin la publicación de protocolos claros que delimiten sus usos, alcances y criterios de aplicación (Datysoc, 2022). Como consecuencia, los ciudadanos no cuentan con información precisa sobre cuándo se activa la tecnología, qué bases de datos se utilizan para las comparaciones, cuáles son los umbrales de coincidencia definidos y qué mecanismos existen para impugnar posibles errores o abusos.

A estas tensiones se suman las limitaciones técnicas inherentes a los sistemas de reconocimiento facial, tales como la posibilidad de falsos positivos, la existencia de sesgos algorítmicos y la opacidad en los procesos de entrenamiento de los algoritmos, aspectos que adquieren especial relevancia cuando la tecnología se aplica en contextos de vigilancia policial. Diversos informes han señalado que estos sesgos pueden afectar de manera diferencial a determinados grupos poblacionales, incrementando el riesgo de prácticas de vigilancia selectiva o discriminatoria (Datysoc, 2022). En el contexto uruguayo, estas preocupaciones se ven reforzadas por la ausencia de evaluaciones de impacto público.

2.2 Detección de personas en situación de calle

Uno de los usos más recientes de la inteligencia artificial aplicada a la videovigilancia en Uruguay es la detección de personas en situación de calle. Este proyecto, implementado por el Ministerio del Interior a través del Centro de Comando Unificado (CCU), utiliza algoritmos de analítica de video para identificar patrones de conducta asociados a personas que se encuentran acostadas o permaneciendo de forma prolongada en espacios públicos. A través de la generación de alertas automáticas, los algoritmos señalan a los operadores del CCU aquellas imágenes donde se observan personas acostadas en la vía pública, una vez recibida dicha alerta, los operadores verifican la situación y coordinan la intervención de móviles policiales que se trasladan al lugar. El procedimiento establece que los agentes evalúan el estado de la persona y, si corresponde, gestionan la derivación hacia refugios u otros dispositivos de asistencia social, en coordinación con el Ministerio de Desarrollo Social (MIDES) (Ministerio del Interior, 2025, junio 25).

Según las autoridades, este mecanismo se aplicó inicialmente durante la campaña de invierno y en particular frente a olas de frío polar, con el objetivo de prevenir riesgos graves para la salud y la vida de las personas que se encuentran en situación de calle. Las alertas generadas por el sistema permiten una respuesta más rápida y focalizada, en comparación con los mecanismos tradicionales de patrullaje o llamadas telefónicas al 911.

Sin embargo, este uso de la tecnología abre un campo de discusión respecto a los límites entre vigilancia policial y políticas sociales. Si bien el propósito declarado es asistencial, la herramienta se despliega desde un dispositivo de seguridad pública y a través de operadores policiales, lo que plantea interrogantes sobre el rol de la policía en la gestión de problemáticas sociales, más aún, al tratarse de un sistema automatizado, existe el riesgo de que las personas en situación de calle sean categorizadas principalmente como “objetos de alerta” dentro de un esquema de vigilancia, en lugar de ser reconocidas en su dimensión de sujetos de derechos. A través de estas analíticas de video que identifican patrones corporales como "estar acostado" o permanecer de forma prolongada en espacios públicos, el Estado despliega lo que se definió anteriormente como focopolítica (Álvarez, 2008). Esta racionalidad, se centra en el control de grupos focalizados definidos como “en riesgo”, con el fin de asegurar umbrales mínimos de supervivencia más que garantizar un bienestar integral (Álvarez, 2008). Sin embargo, este uso asistencial de la

vigilancia la dirige hacia una despolitización de la exclusión (Álvarez, 2008), Al convertir la falta de un derecho como la vivienda en una “alerta automática” que es monitoreada constantemente, el problema social se redefine como un perfil individual de riesgo y se deja de lado el carácter estructural y político de la situación, el sujeto deja de ser un ciudadano de derechos para convertirse en un "caso" a evaluar, clasificar y monitorear por el sistema de seguridad.

El sistema captura una señal física (el cuerpo en el suelo) para activar una respuesta refleja del Estado, que coordina la intervención de móviles policiales de manera automática, esto nos puede servir para pensar cómo se aplica el concepto de input y output planteado por (Lazzarato, 2012).

2.3 Lectura automática de matrículas vehiculares (LPR) y anillos de vigilancia

Una de las líneas de expansión de la videovigilancia con IA en Uruguay es la incorporación de sistemas de lectura automática de matrículas vehiculares (LPR). Esta tecnología permite identificar en tiempo real las matrículas de los automóviles que circulan por puntos estratégicos del territorio, incorporando la información con bases de datos oficiales y generando alertas inmediatas cuando se detectan vehículos requeridos por la justicia, robados o con matrículas clonadas. Las primeras cámaras lectoras se colocaron en peajes, las mismas tienen la capacidad de registrar matrículas en diversas condiciones de visibilidad y transmitir la información en tiempo real al Centro de Comando Unificado, donde se centraliza la vigilancia urbana (Ministerio del Interior, 2023).

La prensa nacional también destacó el alcance de esta estrategia. En una nota publicada por *La Mañana* se mencionó que el Ministerio del Interior avanza hacia “una vigilancia total del territorio mediante la tecnología”, en referencia a la instalación de anillos de cámaras LPR en la zona metropolitana y en los principales accesos fronterizos del país (La Mañana, 2023). Este señalamiento ilustra cómo la vigilancia vehicular no se restringe a puntos aislados, sino que tiende a configurarse como una red continua de control sobre la movilidad.

Desde un punto de vista crítico podría pensarse a esta tecnología como una herramienta capaz de ampliar la capacidad estatal de cartografiar y anticipar la circulación de la población a través de sus desplazamientos vehiculares. En la práctica, los anillos

metropolitanos y fronterizos habilitan la construcción de un mapa dinámico del tránsito que permite conocer no solo la existencia de hechos ilícitos, sino también patrones de movilidad cotidianos. Esta masificación del registro vehicular abre interrogantes sobre el alcance de la vigilancia estatal y los posibles efectos sobre la privacidad ciudadana, ya que, como advierte *La Mañana*, implica avanzar hacia una vigilancia de carácter “total” que no distingue entre quienes están o no vinculados a hechos delictivos.

La vigilancia LPR funciona como una modulación constante del espacio social, donde la libertad de circulación queda mediada por una red de sensores que evalúa permanentemente las trayectorias que los ciudadanos realizan. Los anillos de vigilancia actúan como una vigilancia distribuida, donde la función de observar y vigilar se reparte entre cámaras, bases de datos y algoritmos que operan en forma de red.

Estas infraestructuras operan como máquinas de ver (falta autor), ya que participan activamente en la producción de lo real al convertir los desplazamientos cotidianos en información cuantificable y almacenable. Según Bruno (2013), este tipo de tecnologías establece jerarquías de relevancia y delimita qué conductas son visibles para el Estado. Al capturar patrones de movilidad, el sistema permite al cartografiar y anticipar la circulación de la población.

Conclusiones

A lo largo de este trabajo analizamos la incorporación de sistemas de videovigilancia con inteligencia artificial en Uruguay como parte de una racionalidad de gobierno más amplia que su uso técnico, dicha racionalidad se encuentra inscripta en lógicas de gestión poblacional, anticipación del riesgo y modulación de las conductas. Desde esta perspectiva, el interés no estuvo puesto en evaluar la eficacia técnica de estas herramientas, sino en interrogar los modos en que su implementación reconfigura las formas de observar, clasificar y gestionar la vida social en el espacio público. La IA aplicada a la vigilancia no aparece como una herramienta plenamente instrumental, sino como un dispositivo que reorganiza el campo de lo visible, lo pensable y lo gobernable en el espacio público. El análisis desde la noción foucaultiana de gubernamentalidad y seguridad permitió comprender que estas tecnologías no buscan eliminar el fenómeno de la delincuencia como tal, sino administrarla dentro de márgenes estadísticamente aceptables. La seguridad actual, entendida como tecnología de poder, opera habilitando

ciertos movimientos, tolerando otros y señalando desviaciones potenciales antes de que se produzcan. En este contexto, la vigilancia algorítmica desplaza el foco desde el acto mismo hacia la probabilidad de cometerlo, creando formas de intervención preventiva que inciden sobre la experiencia cotidiana de habitar la ciudad. Además, la articulación con el concepto de dispositivo permitió visibilizar que la videovigilancia inteligente no se reduce a cámaras o softwares específicos, sino que constituye una red heterogénea que integra saberes técnicos, discursos institucionales, marcos normativos, infraestructuras materiales y prácticas sociales. Esta red produce efectos concretos sobre los sujetos, no sólo en términos de control externo, sino también en la internalización de la vigilancia como condición permanente del espacio público, promoviendo formas de autocontrol y adaptación conductual. La incorporación de aportes como los conceptos de vigilancia distribuida, sociedades de control y gobierno algorítmico permitió complejizar el análisis, mostrando cómo estas tecnologías se inscriben en un escenario donde el control se distribuye en los diferentes ámbitos de la vida cotidiana de los sujetos. Desde una perspectiva crítica de la inteligencia artificial, se puede pensar que los algoritmos utilizados en contextos de seguridad pública no sólo procesan información, sino que cristalizan decisiones políticas, históricas y sociales previas. Lejos de eliminar el sesgo humano, estos sistemas tienden a reproducir y, en algunos casos, intensificar desigualdades existentes, especialmente cuando se aplican sobre poblaciones previamente expuestas a mayores niveles de vigilancia estatal. En este sentido, el uso de IA en la gestión de la seguridad plantea interrogantes relevantes para el campo de la psicología social y política. ¿Qué tipo de subjetividades se producen en contextos donde la anticipación algorítmica se vuelve una forma cotidiana de gobierno? ¿Cómo incide la vigilancia permanente en la relación de los sujetos con el espacio público, con los otros y consigo mismos? ¿De qué manera estas tecnologías redefinen las nociones de normalidad, sospecha y riesgo? Por último, sin adoptar una posición a favor o en contra del uso de estas tecnologías, este trabajo buscó abrir una línea de problematización que permita pensar críticamente los modos en que la inteligencia artificial se integra a las prácticas estatales en Uruguay. En un contexto donde la expansión de la vigilancia algorítmica parece avanzar con rapidez, resulta necesario preguntarse no sólo por su eficacia técnica, sino por sus efectos simbólicos, subjetivos y políticos. Tal vez el desafío no consista únicamente en regular estas tecnologías, sino en interrogar las racionalidades que las sostienen y los modos de gobierno que habilitan, preguntándonos qué tipo de

sociedad se configura cuando la seguridad se gobierna, cada vez más, desde la lógica de los datos y la anticipación automatizada.

Referencias

Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC). (2017). Memoria anual 2017. Gobierno de Uruguay. Recuperado el 28 de febrero de 2026, desde https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/sites/agencia-gobierno-electronico-sociedad-informacion-conocimiento/files/2023-05/memoria-anual-2017.pdf

Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC). (2024). Estrategia Nacional de Inteligencia Artificial 2024–2030. Gobierno de Uruguay. Recuperado el 28 de febrero de 2026, desde https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/sites/agencia-gobierno-electronico-sociedad-informacion-conocimiento/files/documentos/publicaciones/Estrategia%20Nacional%20IA%202024-2030.pdf

Álvarez Leguizamón, S. (2008). Gubernamentalidad y biopolítica: de la gestión de la población a la gestión de los riesgos sociales. Foucault y la focopolítica [Ponencia]. II Encuentro Argentino y Latinoamericano: Prácticas Sociales y Pensamiento Crítico, Universidad Nacional de Córdoba, Argentina

AxxonSoft. (s.f.a). Highlights del software Axxon Next. AxxonSoft. Recuperado el 1 de marzo de 2026 de https://www.axxonsoft.com/partners/why-axxonsoft?.com

AxxonSoft. (s.f.b). Acceso remoto y gestión distribuida. AxxonSoft. Recuperado el 1 de marzo de 2026 de https://www.axxonsoft.com/products/video-management-software/key-features/remote-access/

Bentham, J. (1979). El Panóptico. Madrid, España: Ediciones de la Piqueta.

Bruno, F. (2013). Máquinas de ver, modos de ser: vigilância, tecnologia e subjetividade. Sulina

Carballo, A. (11 de setiembre de 2024). Cámaras con inteligencia artificial: el Ministerio del Interior presentó nueva tecnología para prevenir delitos. *El País*.

https://www.elpais.com.uy/informacion/policiales/camaras-con-inteligencia-artificial-ministerio-del-interior-presento-nueva-tecnologia-para-prevenir-delitos

Crawford, K. (2022). Atlas de inteligencia artificial: Poder, política y costos planetarios. Fondo de Cultura Económica.

Datysoc. (2022, 23 de marzo). Uso policial del reconocimiento facial automatizado en Uruguay. Laboratorio de Datos y Sociedad. https://datysoc.org/2022/03/23/uso-policial-del-reconocimiento-facial-automatizado-en-uruguay/

Deleuze, G. (1999). Post-scriptum sobre las sociedades de control. En Conversaciones (1972-1990). Valencia, España: Pre-Textos.

Díaz Charquero, P. (2022). Fuera de control: Uso policial del reconocimiento facial automatizado en Uruguay. Datysoc - Laboratorio de Datos y Sociedad.

Foucault, M. (1985). Saber y verdad. Ediciones de La Piqueta.

Foucault, M. (2002). Vigilar y castigar: Nacimiento de la prisión. Buenos Aires, Argentina: Siglo XXI Editores Argentina.

Foucault, M. (2006). Seguridad, territorio, población: Curso en el Collège de France (1977-1978). Fondo de Cultura Económica.

Ministerio del Interior. (2024a, agosto 10). Interior instaló 17 nuevas cámaras de videovigilancia en Libertad. https://www.gub.uy/presidencia/comunicacion/noticias/interior-instalo-17-nuevas-camaras-videovigilancia-libertad

Ministerio del Interior. (2024b, noviembre 15). Instalación de 1.337 cámaras: se completa la Fase 4 de optimización del sistema. https://www.gub.uy/ministerio-interior/comunicacion/noticias/instalacion-1337-camaras-se-completa-fase-4-optimizacion-del-sistema

Ministerio del Interior. (2025, 28 de febrero). Informe sobre violencia y criminalidad en todo el país (2023–2024): homicidios 2023 - 2024.

https://www.gub.uy/ministerio-interior/comunicacion/publicaciones/informe-sobre-violencia-criminalidad-todo-pais-2023-2024

Ministerio del Interior. (2025, junio 25). El Ministerio del Interior aplica inteligencia artificial para detectar personas en situación de calle. https://www.gub.uy/ministerio-interior/comunicacion/noticias/ministerio-del-interior-aplica-inteligencia-artificial-para-detectar-personas

Pasquinelli, M., y Joler, V. (2020). El Nooscopio de manifiesto: La inteligencia artificial como instrumento de extractivismo del conocimiento. laFuga.

Presidencia de la República. (2024, septiembre 11). Interior presentó proyecto de videovigilancia basado en inteligencia artificial. https://www.gub.uy/presidencia/comunicacion/noticias/interior-presento-proyecto-videovigilancia-basado-inteligencia-artificial

Roba, N. (31 de agosto de 2024). Vigilados con inteligencia artificial: cámaras del Ministerio del Interior incorporan alerta ante movimientos sospechosos. *El Observador.* https://www.elobservador.com.uy/nacional/vigilados-inteligencia-artificial-camaras-del-ministerio-del-interior-incorporan-alerta-comportamiento-delictivo-n5958675

Rouvroy, A., y Berns, T. (2016). Gubernamentalidad algorítmica y perspectivas de emancipación: ¿La disparidad como condición de individuación a través de la relación? Adenda Filosófica, (1), 88-116.

Security Informed. (s.f.). Detalles técnicos de Axxon Next. Security Informed. Recuperado de https://www.securityinformed.com/axxonsoft-axxon-next-cctv-software-technical-details.html?.com

SourceSecurity. (s.f.). Axxon Next datasheet. SourceSecurity. Recuperado de https://www.sourcesecurity.com/datasheets/axxonsoft-axxon-next-3-1-vms-cctv-software/co-6163-ga/AxxonNext_Tech_Brochure.pdf