Datos policiales e Inteligencia Artificial: Un equilibrio delicado entre la privacidad, la utilidad y la ética

María Teresa Hernández Borges
Jefa de servicio de Seguridad en el Gobierno de Canarias

Pedro Juan Baquero Pérez
Profesor asociado de la Universidad de la Laguna y jefe de servicio de Informática y Comunicaciones del Gobierno de Canarias

RESUMEN: Este artículo aborda la intersección crítica entre la inteligencia artificial (IA), la privacidad y la ética en el ámbito policial. Explora cómo la IA ofrece oportunidades sin precedentes para mejorar la eficiencia en la recopilación y el procesamiento de datos en investigaciones criminales, pero también cómo plantea desafíos éticos y riesgos para la privacidad y la protección de datos. Desde dilemas éticos en la recopilación de datos y el uso de algoritmos de predicción delictiva hasta los riesgos asociados con la inferencia de datos y la creación de perfiles, el artículo examina las diversas facetas del tema. También se considera la tensión entre los enfoques deontológicos y utilitaristas en la ética de la privacidad, y se presentan métodos específicos para mitigar riesgos, como la anonimización, el consentimiento y notificación, la eliminación de datos y la privacidad diferencial. Finalmente, se ofrece un análisis multidimensional de los desafíos y planteamientos en este ámbito emergente.

Palabras clave: Inteligencia Artificial (IA), privacidad, ética, ámbito policial, protección de datos personales

ABSTRACT: This article addresses the critical intersection between artificial intelligence (AI), privacy, and ethics in the realm of policing. It explores how AI offers unprecedented opportunities for enhancing efficiency in the collection and processing of data in criminal investigations, but also how it poses ethical challenges and risks to privacy and data protection. From ethical dilemmas in data collection and the use of predictive crime algorithms to the risks associated with data inference and profiling, the article examines the various facets of the issue. The tension between deontological and utilitarian approaches in privacy ethics is also considered, and specific methods to mitigate risks are introduced, such as anonymization, consent and notification, data deletion, and differential privacy. Finally, it provides a multidimensional analysis of the challenges and approaches in this emerging field.

Keywords: Artificial Intelligence (AI), privacy, ethics, police scope, personal data protection

1. INTRODUCCIÓN

La transformación digital se ha infiltrado en cada faceta de nuestra sociedad. Con la ascensión de tecnologías punteras como la inteligencia artificial (IA), acompañada de la impresionante habilidad para procesar voluminosos conjuntos de datos (Big Data), emergen desafíos inéditos con el potencial de revolucionar la operativa de las administraciones públicas. Estos avances no solo prometen cambiar la manera en que estas entidades funcionan, sino que también proyectan nuevas posibilidades para mejorar la interacción ciudadana y la eficiencia institucional. El ámbito policial no es una excepción a esta revolución tecnológica (Joh, 2017), de hecho, la IA ofrece oportunidades sin precedentes para mejorar la eficiencia en la recopilación y el procesamiento de datos en investigaciones criminales, la toma de decisiones en tiempo real y la prevención del crimen. La IA tiene un rol cada vez más importante en el ámbito policial, especialmente en la recopilación y procesamiento de datos relevantes para la Seguridad Pública y la justicia penal. Mediante técnicas como el aprendizaje automático, una subdisciplina de la IA, se pueden desarrollar algoritmos que aprenden de los datos policiales para realizar predicciones o tomar decisiones en áreas como la predicción de delitos, identificación de sospechosos o análisis de patrones criminales (Jordan y Mitchell, 2015). En el ámbito policial esto es particularmente útil para analizar rápidamente datos de diversas fuentes como registros de detenciones, pruebas de ADN, grabaciones de cámaras, registros de vigilancia, y hasta datos públicos recopilados de redes sociales o plataformas digitales (Dhar, 2013). Estos datos se utilizan para entrenar algoritmos de aprendizaje automático que pueden realizar tareas que van desde la distribución

de medios policiales en zonas de alto riesgo hasta la identificación de redes criminales. Es relevante señalar que la IA no solo tiene el potencial para recopilar y procesar datos en el ámbito policial, sino que también puede generar nuevos datos y mejorar la calidad de estos datos. También, los algoritmos de IA pueden detectar inconsistencias o errores, llenar datos faltantes y eliminar redundancias, contribuyendo así a una mayor exactitud en las investigaciones y decisiones judiciales (Chen et al., 2018). Sin embargo, la adopción de la IA en la esfera policial también plantea una serie de desafíos y preguntas éticas en relación con la privacidad y la protección de datos personales.

Este artículo se propone examinar los aspectos clave de la privacidad y la protección de datos en el contexto de la IA en el ámbito policial (Babuta, 2018), a través de un análisis que busca entender las implicaciones, riesgos y soluciones posibles para equilibrar la eficacia policial y los derechos individuales. Exploramos los retos y oportunidades que surgen al entrelazar la inteligencia artificial (IA) con la recopilación y procesamiento de datos en el ámbito policial. Comenzamos con una revisión de los conceptos esenciales, como es lo que se entiende por privacidad, y ofreciendo una breve descripción del marco regulador español. Abordamos los dilemas éticos que emergen, haciendo mención a Internet de las Cosas (IoT) en la privacidad, y las complejidades de la transferencia de datos entre distintos contextos. Del mismo modo, analizamos los riesgos asociados con la inferencia de datos y la elaboración de perfiles. Más adelante, debatimos sobre el delicado equilibrio entre la privacidad individual y el interés colectivo en la seguridad pública. Finalmente, presentamos estrategias y métodos específicos de mitigación para proteger la privacidad y los datos en el uso de IA en contextos policiales, concluyendo con reflexiones sobre el delicado balance entre las ventajas de la IA y los imperativos éticos y de privacidad.

2. REVISIÓN DE LOS CONCEPTOS CLAVE: PRIVACIDAD Y PROTECCIÓN DE DATOS EN EL CONTEXTO DE LA IA EN EL ÁMBITO POLICIAL

Las intersecciones entre privacidad, protección de datos y la actuación policial cobran una relevancia sin precedentes. No obstante, ¿qué entendemos exactamente por privacidad y protección de datos, especialmente en un contexto donde la IA juega un papel creciente? Y, ¿cómo definimos estos términos en el ámbito específico de la actuación policial? Siguiendo el trabajo de Solove (2008), quien ofrece una visión detallada de los desafíos inherentes a las discusiones sobre privacidad, es crucial reconocer que la privacidad adopta diversas formas, especialmente cuando se intersecta con el ámbito de los datos policiales. En este contexto, la privacidad adquiere matices significativos, pues no sólo se trata del derecho del individuo a mantener ciertos aspectos de su vida alejados del escrutinio público, sino también del imperativo ético y legal de proteger información sensible que podría ser utilizada en investigaciones criminales o procesos judiciales.

La privacidad de los datos en el ámbito policial se refiere al derecho de los ciudadanos a controlar cómo se recopilan, usan, y comparten sus datos personales en el contexto de las actividades de la policía. Según el *artículo 4* del *Reglamento General de Protección de Datos* (RGPD) (Comisión Europea, 2016a), los datos personales son cualquier información relativa a una persona física identificada o identificable. Esto se vuelve particularmente delicado cuando los datos son utilizados en el ámbito policial, ya que podrían incluir información extremadamente sensible como antecedentes criminales, afiliaciones políticas, o incluso la ubicación en tiempo real de un individuo. En este escenario, la protección de datos cobra una relevancia adicional. Con el conjunto de principios y leyes que guían la recopilación, el uso, el almacenamiento y la eliminación de datos personales dentro de las actividades policiales se busca el objetivo de garantizar que estos datos estén seguros, sean tratados de manera justa y ética, y sean accesibles para revisión o modificación solo por las partes autorizadas. Los principios de protección de datos, que también se encuentran desarrollados en el RGPD, toman un nuevo significado en este contexto. Estos principios incluyen la limitación de la finalidad (es decir, que los datos solo se utilicen para el propósito para el cual fueron recopilados), la minimización de datos (recolectar sólo los datos estrictamente necesarios), la exactitud, el almacenamiento limitado, la integridad, y la confidencialidad, entre otros.

En el contexto europeo, es fundamental entender cómo España se adapta y responde a los desafíos y oportunidades de la IA en el ámbito policial. La Unión Europea ha otorgado una importancia considerable a la protección de datos personales, siendo el RGPD (Comisión Europea, 2016a) su pilar fundamental. El RGPD busca armonizar las leyes de protección de datos en todos los estados miembros de la UE y proteger el derecho a la privacidad de los ciudadanos (Comisión Europea, 2016). Adicionalmente, la *Directiva 2016/680 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016* (Comisión Europea, 2016b) que se refiere a la protección de individuos respecto al tratamiento de datos personales por autoridades para la prevención, investigación y enjuiciamiento de delitos o sanciones penales, así como a la libre circulación de esos datos complementa este marco, enfocándose en el tratamiento de datos para fines penales. En España, la normativa en protección de datos se alinea con la de la UE, con sus especificidades. La *Ley Orgánica 3/2018* (España, 2018) traslada al ordenamiento jurídico español las disposiciones del RGPD, el *artículo 1* establece las condiciones para la obtención, uso y almacenamiento de datos personales, subrayando los derechos y libertades de los individuos. Asimismo, la *Ley Orgánica 7/2021* (España, 2021) especifica el tratamiento de datos en el ámbito policial y judicial, armonizando la normativa española con la *Directiva 2016/680* y garantizando la protección de derechos y libertades (*Ley Orgánica 7/2021, Preámbulo III*). Esta *Ley Orgánica* responde a la necesidad de adaptar la legislación a los retos modernos en seguridad y justicia penal, especialmente adaptándose a nuevos tratados y directrices de la Unión Europea que da res-

puestas a algunos retos en el sistema previo, especialmente en su habilidad para combatir la ciberdelincuencia y otros delitos transnacionales. Esta Ley se espera que tenga un impacto notable en la cooperación policial, fortaleciendo la confianza y la fluidez en el intercambio de información. Tanto la *Directiva 2016/680* como la *Ley Orgánica 7/2021* procuran un enfoque equilibrado entre la eficacia y la protección de datos. Thompson et al. (2021) señala que la incorporación de medidas éticas en la legislación refuerza el Estado de Derecho y la confianza del público. Sin embargo, el avance tecnológico en la gestión de datos plantea desafíos éticos. Es crucial que la tecnología aplicada en el ámbito policial se ejecute conforme a directrices éticas, yendo más allá del estricto cumplimiento de la normativa de protección de datos que sea de aplicación.

3. LOS DESAFÍOS DE LA IA EN LA PRIVACIDAD EN EL ÁMBITO POLICIAL

La adopción de la IA en la recopilación y el procesamiento de datos en el ámbito policial y de la Seguridad Pública no está exenta de dilemas éticos complejos que merecen una consideración cuidadosa. Primero, el dilema de la privacidad y el consentimiento se vuelve aún más crítico en el contexto policial. Mientras que la recopilación de datos podría argumentarse como necesaria para la Seguridad Pública, el consentimiento para tal recolección es a menudo inexistente o forzado en situaciones legales, especialmente cuando se trata de vigilancia o de la recopilación de datos a través de tecnologías como el reconocimiento facial o las cámaras corporales (Mittelstadt et al., 2016). Esto desafía las normas convencionales sobre el consentimiento informado y plantea preguntas sobre cuánto control tienen los individuos sobre sus propios datos cuando interactúan con las fuerzas del orden. En segundo lugar, el riesgo de discriminación y falta de justicia se magnifica cuando la IA se utiliza para recopilar y analizar datos policiales. Si los algoritmos se entrenan con datos sesgados o discriminatorios, pueden perpetuar o incluso exacerbar las desigualdades existentes, como el perfil racial o la discriminación basada en el género, la religión o la orientación sexual (Crawford, 2016). Este uso irresponsable de la IA puede tener efectos duraderos en las comunidades marginadas y vulnerables, impactando sus oportunidades de vida y su interacción con el sistema de justicia. Por último, el dilema ético de la transparencia y la explicabilidad se vuelve particularmente apremiante en el ámbito policial. Los algoritmos de IA pueden ser complejos y operar como "cajas negras", haciendo difícil para las partes interesadas, incluidos los ciudadanos y los funcionarios judiciales, entender cómo se toman las decisiones (Burrell, 2016). Esto afecta la capacidad de las personas para cuestionar o impugnar las decisiones que podrían tener un impacto significativo en sus vidas, como detenciones, cargos criminales o sentencias. Estos dilemas éticos subrayan la importancia de abordar las preocupaciones sobre la privacidad, la discriminación y la

transparencia de manera integral, para garantizar que la aplicación de la IA en el ámbito policial sea tanto efectiva como éticamente responsable.

En el ámbito de la Seguridad Pública, la implementación de tecnologías avanzadas como la IA y el Internet de las Cosas (IoT) promete una eficiencia sin precedentes en la recopilación y el procesamiento de datos. La IA puede facilitar tareas que van desde el análisis de patrones delictivos hasta la toma de decisiones en tiempo real, mientras que los dispositivos IoT amplían la red de fuentes de datos. Sin embargo, estas prometedoras aplicaciones también intensifican las preocupaciones existentes sobre la privacidad, la ética y la protección de datos personales. Esta complejidad tecnológica y ética nos lleva a plantearnos diversas preguntas clave. Nos cuestionamos aspectos como hasta qué punto se les debe informar a los ciudadanos sobre cómo se recopilan, procesan y comparten sus datos personales en un entorno tan sensible como el policial. Además, nos cuestionamos problemáticas asociadas con la transferencia de datos sensibles entre diferentes sistemas o jurisdicciones. En el mismo sentido, es crucial determinar qué medidas de gobernanza se requieren para garantizar que la IA y el IoT se implementen de manera éticamente responsable en el ámbito policial. También es esencial explorar cómo aparece el riesgo de discriminación y falta de justicia en los sistemas de IA, especialmente en la recopilación y el análisis de datos policiales. Finalmente, nos enfrentamos al desafío de encontrar un equilibrio entre la eficiencia policial y las preocupaciones éticas y de privacidad que estas tecnologías avanzadas inevitablemente generan. Por tanto, la creciente incorporación de la IA en el ámbito policial abre una serie de cuestionamientos éticos y de privacidad que no podemos pasar por alto.

Este apartado abordará estos desafíos críticos en la privacidad y la protección de datos personales en el contexto policial, considerando los dilemas éticos que surgen en la recopilación y el procesamiento de datos, las implicaciones del uso del Internet de las Cosas, y la transferencia de datos entre diferentes contextos y jurisdicciones. También, mencionaremos cómo trata la norma española estos aspectos. Abordaremos los posibles beneficios y peligros inherentes a la creación de perfiles a través de la IA en la Seguridad Pública. Y examinaremos las aplicaciones y riesgos de la IA en la vigilancia policial y en la predicción del comportamiento delictivo. Finalmente, analizaremos los riesgos asociados con la manipulación y el autoritarismo digital. Enfocándonos en estas cuestiones, nos permitirá analizar el equilibrio entre la utilidad de las tecnologías avanzadas en la Seguridad Pública y la imperante necesidad de proteger la privacidad y los derechos de los ciudadanos.

3.1. El Internet de las Cosas (IoT) y sus implicaciones para la privacidad y la protección de datos

El Internet de las Cosas (IoT) está ganando terreno en las operaciones de las fuerzas de seguridad, desde cada vez se usan más la vigilancia en tiempo real.

Si bien estas aplicaciones pueden mejorar la eficacia policial, plantean serias cuestiones éticas y de privacidad que deben ser abordadas cuidadosamente. Los dispositivos de IoT en el contexto policial, como cámaras de vigilancia, drones, y sensores en vehículos de patrulla, a menudo recogen datos sin el consentimiento explícito o incluso el conocimiento de las personas afectadas. Estos datos pueden ser extremadamente sensibles, incluyendo información de localización, actividades diarias, o incluso conversaciones. A diferencia de las investigaciones convencionales que suelen requerir un mandato, la recopilación de datos a través del IoT puede ocurrir de manera más encubierta y sistemática, lo cual plantea preocupaciones sobre el derecho a la privacidad (Ziegeldorf, Morchon, y Wehrle, 2014). Además, la infraestructura del IoT es susceptible a ataques cibernéticos que podrían comprometer la integridad y la confidencialidad de los datos recopilados. En un entorno policial, esto podría tener graves consecuencias, como la alteración de evidencia o la exposición de información confidencial relacionada con casos en curso o individuos bajo protección (Roman, Zhou, y Lopez, 2013).

La IA desempeña un papel doble en este contexto. Por un lado, la IA puede aumentar la eficiencia del IoT en la recopilación y el análisis de datos, permitiendo una vigilancia más efectiva o incluso la predicción de actividades delictivas. Por otro lado, el uso de IA para analizar estos grandes conjuntos de datos puede resultar en extracciones de información altamente personales o sensibles que podrían ser mal utilizadas si caen en las manos equivocadas (Sicari et al., 2015).

Dada la complejidad y la sensibilidad de estas cuestiones, es imperativo que las fuerzas de seguridad implementen estrictas medidas de gobernanza y protección de datos. Esto incluye garantizar la transparencia en cómo y por qué se recogen los datos, aplicar sólidas medidas de seguridad para proteger los datos recopilados y establecer claras directrices éticas para el uso de la IA y el IoT en el ámbito policial. Como un ejemplo concreto de posibles medidas a aplicar podemos plantearnos una ciudad con crecientes tasas de criminalidad, donde las autoridades deciden implementar un sistema de "Vigilancia Inteligente" en varios barrios residenciales utilizando IoT. Este sistema incluye cámaras de seguridad con reconocimiento facial, micrófonos capaces de detectar disparos o gritos de auxilio, y sensores de movimiento en parques y áreas comunes. A través de la IA, el sistema no solo monitorea, sino que también predice patrones de actividad delictiva, alertando a las fuerzas de seguridad en tiempo real. Aunque esta iniciativa promete mejorar la seguridad del vecindario, los residentes se sienten preocupados al descubrir que las cámaras y micrófonos no solo registran actividades sospechosas, sino también momentos íntimos y cotidianos, como reuniones familiares en patios traseros o conversaciones privadas en espacios públicos. La preocupación aumenta si, por ejemplo, se revelase que un hacker logra acceder a la base de datos del sistema y publicó videos y audios de los residentes en la web. En este contexto, para restaurar la confianza, las autoridades pueden llevar a cabo una serie de acciones. Primero, pueden establecer un portal transparente donde los residentes pueden ver exactamente qué datos

se están recopilando y por qué. Se deberían implementar medidas de seguridad más robustas, con auditorías externas regulares para garantizar la integridad de los datos. Además, establecer un comité ético para revisar y establecer directrices sobre qué datos pueden ser recolectados y cómo se utilizan, asegurará que el respeto a la privacidad sea primordial. Este tipo de medidas no solo protegen la privacidad de los ciudadanos, sino que también ayudan a restaurar la confianza en el uso de tecnologías avanzadas para la seguridad pública.

3.2. La transferencia de datos entre contextos diferentes

Los datos sobre ciudadanos, delitos y patrones de comportamiento ya no se limitan a las bases de datos de una sola institución o jurisdicción. Con frecuencia, estos datos se recopilan en un contexto específico, como una investigación criminal en un ámbito local, y luego se transfieren y aplican en otros contextos, como bases de datos nacionales o incluso internacionales. Este flujo de datos también presenta importantes desafíos en lo que respecta a la privacidad y la protección de datos (Nissenbaum, 2009). Un ejemplo palpable de este fenómeno sería la recolección de datos personales como podría ser el reconocimiento facial por la policía local en una infracción de tráfico, que luego se podría integrar en una base de datos nacional o incluso internacional. Estos datos no solo pueden utilizarse para tratar una infracción de tráfico en el ámbito local, por ejemplo para identificar a la persona infractora, sino también para tareas más complejas como la identificación de patrones de delincuencia transfronterizos o el análisis predictivo de actividades delictivas. Sin embargo, el uso de estos datos puede entrar en conflicto con las expectativas de privacidad de los ciudadanos. Podrían no ser conscientes de que sus datos están siendo compartidos y utilizados en múltiples contextos, lo que podría dar lugar a una serie de cuestiones éticas y legales: ¿En qué medida se les debe informar sobre cómo se utilizan y comparten sus datos personales? Además, la transferencia de datos policiales entre diferentes contextos puede aumentar los riesgos de seguridad. Los datos pueden ser más vulnerables a interceptaciones o filtraciones durante la transferencia, especialmente si los sistemas receptores no tienen medidas de seguridad tan robustas como los sistemas que originalmente recopilaron los datos.

Dicho esto, los contextos en los que se transfieren y usan estos datos a menudo tienen regulaciones y normas de privacidad divergentes. Por ejemplo, las políticas sobre el uso de datos personales pueden variar significativamente entre países, o incluso, en algunos países, entre estados dentro de un país, lo que puede complicar aún más la situación. En el contexto de España, la *Ley Orgánica 7/2021* regula específicamente estas transferencias de datos. Esta Ley establece múltiples capas de supervisión y autorización que deben seguirse para asegurar la legalidad y la protección de datos durante su transferencia. Estos requisitos legales tienen como objetivo equilibrar la necesidad de compartir información para propósitos de seguridad y orden público con el imperativo de proteger los

derechos y libertades individuales, especialmente en transacciones internacionales donde los estándares de protección de datos pueden variar. Esta Ley regula la transferencia de datos personales a nivel nacional e internacional, poniendo especial énfasis en las transferencias hacia países no miembros de la Unión Europea, esto es, que no disponen de una normativa de protección de datos armonizada o similar con Europa. Según el *artículo 43*, las autoridades españolas deben cumplir condiciones específicas como la necesidad de la transferencia y la autorización previa de otro Estado miembro de la UE, si aplica. El *artículo 44* señala que, si la Comisión Europea ha decidido que un estado no miembro tiene un nivel adecuado de protección de datos, no se necesita autorización específica para transferir datos. En el caso contrario, el *artículo 45* establece que se deben presentar "garantías apropiadas", las cuales deben ser evaluadas por la autoridad competente. Según el *artículo 46*, existen excepciones específicas que permiten transferencias sin necesidad de garantías apropiadas o decisión de adecuación, como la protección de intereses vitales. Finalmente, el *artículo 47* permite transferencias excepcionales a destinatarios que no son autoridades en estados no miembros, siempre que se cumplan condiciones estrictas.

Por todo lo anterior, la transferencia de datos policiales entre diferentes contextos representa una preocupación crítica en la protección de datos en el ámbito de la IA aplicada a la Seguridad Pública. Este asunto necesita un enfoque cuidadoso y bien considerado para equilibrar las oportunidades y los riesgos que conlleva el uso de estos datos. Las soluciones podrían incluir políticas de privacidad más transparentes, regulaciones o procedimientos más estrictos en relación con la transferencia y el uso de datos, y tecnologías de seguridad más robustas para proteger los datos durante su transferencia.

3.3. Aplicaciones y riesgos de la IA en la creación de perfiles

La *Ley Orgánica 7/2021* define la "elaboración de perfiles" como cualquier tratamiento automatizado de datos personales que evalúa ciertos aspectos de un individuo, como su salud o comportamiento, lo cual es particularmente relevante para las aplicaciones de IA que involucran la inferencia de datos y la creación de perfiles. En el contexto de los riesgos de la inferencia de datos y la creación de perfiles, esta Ley establece directrices importantes que protegen los derechos individuales y la privacidad de los datos. Según el *artículo 13*, la manipulación de categorías especiales de datos personales, como información sobre origen étnico, creencias religiosas, y datos biométricos, está estrictamente limitada. Solo se permite bajo ciertas condiciones como cuando es necesario para proteger los intereses vitales o cuando el individuo ha hecho públicos dichos datos. El *artículo 14* prohíbe las decisiones que se basan únicamente en tratamientos automatizados, incluida la elaboración de perfiles, que afecten negativamente al individuo. Además, dichas decisiones automatizadas no deben basarse en categorías especiales de datos personales a menos que se hayan tomado medidas

específicas para proteger los derechos del individuo. Por tanto, la *Ley Orgánica 7/2021* busca mitigar los riesgos asociados con el uso de la IA para la inferencia de datos y la creación de perfiles al establecer límites y condiciones estrictas para tal actividad.

En cualquier caso, la elaboración o creación de perfiles a través de la inteligencia artificial en el contexto policial también presenta una dualidad de ventajas y desafíos significativos. En el lado positivo, el perfilamiento a través de la IA puede ser una herramienta valiosa para el mantenimiento del orden y la Seguridad Pública. Un sistema de IA podría, por ejemplo, analizar patrones de crímenes en un área específica para ayudar a predecir dónde y cuándo es más probable que se produzca un delito. Esta información podría ser vital para la asignación eficiente de recursos y personal de Seguridad Pública. Los algoritmos de aprendizaje automático también podrían ser utilizados para analizar grandes cantidades de datos en investigaciones, como redes sociales, registros telefónicos y otros datos digitales, para identificar relaciones o patrones que podrían pasar desapercibidos para un investigador humano.

Uno de los riesgos más prominentes es la capacidad para la recopilación masiva de datos sensibles relacionados con ciudadanos, como antecedentes penales, ubicaciones geográficas, y comportamientos. La IA puede contribuir a la creación de una "huella digital policial" muy detallada de los individuos, lo que amplía el alcance para el escrutinio gubernamental y potencialmente erosiona la privacidad civil (Cohen, 2019). Un caso ilustrativo es el uso de sistemas de reconocimiento facial basados en IA en espacios públicos. Estas herramientas pueden identificar a individuos en tiempo real comparando imágenes capturadas con bases de datos de fotos previamente almacenadas. En una ciudad donde estas cámaras estén ubicadas en lugares estratégicos, como plazas, estaciones de transporte y centros comerciales, las autoridades podrían rastrear los movimientos de cualquier ciudadano a lo largo del día. Supongamos que una persona sin antecedentes penales asiste a una manifestación pacífica. La IA podría identificar y registrar su presencia allí, asociando su imagen con el evento. Días después, esta misma persona podría ser identificado nuevamente al visitar un lugar de interés turístico. Si estas informaciones se cruzan, es posible que se cree un perfil sobre esta persona, sus hábitos y lugares que frecuenta, sin que haya cometido ningún delito. Esto no solo constituye una invasión a su privacidad, sino que también podría dar lugar a interpretaciones erróneas o sesgadas sobre sus actividades, poniendo en peligro su libertad y derechos. Por tanto, mientras que el reconocimiento facial puede ser útil para identificar sospechosos o personas desaparecidas, también puede ser mal utilizado para vigilar y registrar la vida de ciudadanos inocentes, erosionando su privacidad y libertades civiles.

Por otra parte, como vimos más arriba, los algoritmos de aprendizaje automático tienen el potencial de inferir datos extremadamente sensibles que podrían no haber sido explícitamente recopilados por las autoridades. Como es el caso del análisis de interacciones en redes sociales, registros de detenciones

y otras fuentes de datos públicos podría usarse para inferir aspectos como afiliaciones políticas, orientación sexual o incluso predisposiciones a ciertos comportamientos, lo que plantea serias preocupaciones éticas, además, de atentar contra los derechos fundamentales en nuestra Constitución. Por ejemplo, tomemos el caso de una persona, que es activa en varios foros de discusión en línea y redes sociales y ha compartido artículos y comentarios críticos sobre la política gubernamental en el ámbito de seguridad. Aunque esta persona simplemente está ejerciendo su derecho a la libertad de expresión y no tiene intenciones de involucrarse en actividades extremistas, el algoritmo podría malinterpretar la frecuencia y naturaleza de sus interacciones en línea, y etiquetarla como una persona de "alto riesgo" para la radicalización. La capacidad de la IA para inferir características como afiliaciones políticas a partir de datos no explícitamente relacionados con ese aspecto es problemática por varias razones. En primer lugar, es una violación de la privacidad de esta persona, quien nunca brindó consentimiento para tal análisis. En segundo lugar, esto podría resultar en consecuencias adversas para ella, como una mayor vigilancia o incluso investigaciones innecesarias por parte de las autoridades.

Otro de los más grandes peligros es la posibilidad de sesgo algorítmico, que podría resultar en la vigilancia o el acoso desproporcionado de comunidades marginadas. Si los algoritmos se entrenan con datos que reflejan prejuicios raciales, económicos o de género, estos sesgos pueden ser perpetuados e incluso amplificados por el sistema de IA, que podría llevar a la estigmatización y marginalización de comunidades o individuos basadas en interpretaciones erróneas o sesgadas. Por ejemplo, en una ciudad, la jefatura local puede implementar un sistema avanzado de IA para analizar patrones de criminalidad y predecir "zonas de alto riesgo", con la esperanza de prevenir delitos antes de que ocurran. Utilizando datos históricos de criminalidad o de otros contextos, la IA identifica áreas en la ciudad donde es probable que se cometan delitos y permite a la policía aumentar la vigilancia en esas áreas. Sin embargo, estos datos históricos también reflejan prácticas pasadas de vigilancia policial o de entornos diferentes, que estaban influenciadas por prejuicios raciales y socioeconómicos. Como resultado, la IA etiqueta de manera desproporcionada barrios de bajos ingresos y comunidades minoritarias como "zonas de alto riesgo", a pesar de que las tasas de criminalidad reales no justifiquen esta designación. Los residentes de estas áreas pueden experimentar un aumento en los controles policiales y en la vigilancia, intensificando la desconfianza hacia las autoridades y perpetuando estigmas. No solo eso, sino que el aumentar la vigilancia en un zona, la posibilidades de detectar delitos aumenta, con lo que intensificaría el sesgo en estas zonas. Esta situación ilustra cómo un algoritmo, aunque neutral en apariencia, puede heredar y perpetuar los prejuicios presentes en los datos con los que fue entrenado, afectando negativamente a comunidades ya marginadas.

Por lo tanto, el uso de perfiles detallados sin el conocimiento o consentimiento de los individuos perfilados amenaza seriamente las libertades civiles. Esto

es especialmente problemático en situaciones donde la recopilación de datos es opaca o donde no se notifica a los individuos afectados. En escenarios más extremos, el perfilamiento podría ser usado de manera indebida para fines de vigilancia estatal o control social, comprometiendo gravemente la privacidad y la libertad individual (Pasquale, 2015). Es imperativo que tanto los desarrolladores de IA como los responsables de las políticas trabajen en conjunto para garantizar que los sistemas de perfilamiento en el ámbito policial se desarrollen y apliquen de una manera que maximice la utilidad pública y la eficiencia, al mismo tiempo que minimiza los riesgos de discriminación, invasión a la privacidad y otros problemas éticos. Aquí también es vital considerar enfoques como la transparencia, la rendición de cuentas y la regulación efectiva, para equilibrar los complejos intereses en juego.

3.4. Aplicaciones y riesgos de la IA en la vigilancia policial y la predicción del comportamiento delictivo

La *Ley Orgánica 7/2021* aborda la captación y tratamiento de datos personales por las Fuerzas y Cuerpos de Seguridad en el ámbito de la videovigilancia. Según el *artículo 15*, la grabación de imágenes y sonidos por las autoridades no se considera una intromisión ilegítima en derechos como el honor y la intimidad si se sigue el principio de proporcionalidad. El *artículo 16* aborda la instalación de sistemas de videocámaras fijas en lugares públicos, requiriendo un análisis de riesgo y de impacto. El *artículo 17* permite el uso de dispositivos móviles para la grabación en situaciones específicas y con aprobación gubernamental. Finalmente, el *artículo 18* establece las pautas para el tratamiento y conservación de las grabaciones. Este marco legal presenta una intersección interesante con los desafíos éticos y de privacidad asociados al uso de la Inteligencia Artificial (IA) en la vigilancia policial. La IA puede potenciar la eficiencia de las operaciones de vigilancia, pero también suscita preocupaciones sobre la privacidad, discriminación y abuso de poder. Por ejemplo, la IA podría realizar reconocimiento facial y de voz mucho más eficientemente que los sistemas tradicionales de vigilancia, pero esto podría llevar a la vigilancia masiva o al perfilamiento de ciertas comunidades.

En este sentido, aunque las capacidades de vigilancia y predicción de comportamiento en el ámbito policial aumentan con el uso de la IA, su uso conlleva una serie de desafíos éticos y de privacidad que no pueden pasarse por alto. En el contexto de la vigilancia policial, la IA puede emplear reconocimiento facial para rastrear a individuos en espacios públicos con un alto grado de precisión. Este avance tecnológico, aunque tiene el potencial de ayudar en la identificación de sospechosos o personas desaparecidas, con la salvedad de aquellas que han desaparecido voluntariamente y ven su imagen difundida en los medios de comunicación o redes sociales, genera preocupaciones significativas sobre la privacidad y las libertades civiles. Por ejemplo, se ha documentado que en

ciertos países se usa de forma extensiva esta tecnología para la vigilancia de la población, abriendo debates éticos sobre la privacidad y el control gubernamental (Fussey y Murray, 2019). Además, tecnologías de reconocimiento de voz y procesamiento de lenguaje natural pueden ser utilizadas para monitorear las comunicaciones. En el ámbito policial, esto podría traducirse en la escucha y análisis automatizados de llamadas o conversaciones en línea para identificar posibles amenazas o actividades delictivas.

En el ámbito de la predicción del comportamiento delictivo, hemos señalado que los algoritmos de aprendizaje automático tienen la capacidad de analizar patrones en registros criminales, informes policiales y otros conjuntos de datos para anticipar dónde y cuándo es más probable que se cometan delitos. Esta forma de "policía predictiva" promete ser una herramienta potente en la lucha contra el crimen, pero no está exenta de polémica y preocupaciones. Como vimos, una de las cuestiones más críticas es cómo la IA puede perpetuar y, en algunos casos, amplificar los sesgos presentes en los datos con los que se alimenta. Un caso notable en los EE.UU. ilustra este problema. Se ha documentado que ciertos sistemas de predicción policial en el país, al ser entrenados con datos históricos que ya reflejaban discriminación racial, tendían a sobrepatrullar y focalizar sus predicciones en barrios predominantemente afroamericanos y latinos. Esto no solo intensificó la vigilancia en estas áreas, sino que también aumentó las interacciones negativas entre la policía y los residentes, exacerbando la desconfianza y tensiones ya existentes. Es decir, la tecnología, lejos de ser una solución neutral, replicaba y amplificaba las desigualdades y prejuicios presentes en el sistema. Por tanto, la cuestión principal radica no solo en la eficacia técnica de la IA, sino también en las implicaciones éticas de su aplicación. Las advertencias sobre la privacidad y la discriminación, como señala Ferguson (2017), resaltan la necesidad de abordar estas tecnologías con precaución, transparencia y un firme compromiso con la justicia y la equidad. Por otra parte, estas herramientas de IA podrían ser utilizadas para reprimir la disidencia política, realizar vigilancia masiva sin salvaguardas adecuadas o perpetuar prejuicios y desigualdades sistémicas (Tene y Polonetsky, 2013; Zuboff, 2019).

Además, estos sistemas no son inmunes a los ataques cibernéticos. Técnicas como la evasión, la exploración y el envenenamiento de datos pueden ser empleadas por atacantes para manipular o engañar a los sistemas de IA, lo que podría resultar en el acceso no autorizado a información sensible o incluso en decisiones erróneas en investigaciones y procesos judiciales. Por ejemplo, supongamos que la policía de una ciudad implementa un sistema de reconocimiento facial basado en IA para identificar y rastrear a sospechosos de delitos en tiempo real a partir de cámaras de vigilancia ubicadas en espacios públicos. Sin embargo, si un grupo de hackers decide atacar el sistema y comienza a inyectar datos falsos en la base de datos de entrenamiento del algoritmo, un ataque conocido como "envenenamiento de datos". Estos datos adulterados incluyen imágenes de personas inocentes etiquetadas como delincuentes. Con el tiem-

po, el algoritmo comienza a reconocer y etiquetar erróneamente a ciudadanos inocentes como sospechosos de delitos debido a este envenenamiento de datos.

Por lo tanto, la utilización de IA para fines de vigilancia y predicción del comportamiento delictivo necesita ser manejada con extrema cautela, implicando un escrutinio riguroso y la participación activa de expertos en ética, defensores de la privacidad y la comunidad en general para asegurar un enfoque equilibrado y justo, con absoluto respeto a los derechos individuales, en especial, aquellos que se establecen en la *Constitución Española*.

3.5. Los riesgos de la manipulación y el autoritarismo digital

La capacidad avanzada de la inteligencia artificial (IA) trae consigo no sólo oportunidades, sino también riesgos significativos vinculados a la manipulación y el surgimiento de un posible autoritarismo digital. En cuanto a la manipulación, otra de las principales preocupaciones es cómo las herramientas de IA podrían utilizarse para fabricar o distorsionar evidencia en investigaciones criminales. Las "deepfakes", por ejemplo, pueden ser especialmente problemáticas en este contexto. Estos vídeos y audios hiperrealistas generados por IA podrían ser utilizados para falsificar pruebas, difamar a individuos o, en el peor de los casos, erróneamente incriminar a personas (Chesney y Citron, 2018). Por otro lado, la IA permite el "microtargeting" policial, que es la focalización muy precisa de individuos o comunidades para vigilancia o intervención basada en análisis de datos. Esto puede ser especialmente peligroso si se emplea de manera incorrecta o discriminatoria, similar a cómo el microtargeting se ha usado en la esfera política para segmentar y manipular a los votantes (Zuboff, 2019).

Fuera de un ámbito democrático, el autoritarismo digital, la adopción masiva de tecnologías de IA por parte de las fuerzas de seguridad puede resultar en un estado de vigilancia que limite las libertades civiles y viole los derechos humanos. La capacidad de la IA para recopilar, analizar y actuar sobre grandes cantidades de datos policiales puede otorgar a las autoridades un nivel de poder y control sin precedentes sobre los ciudadanos. Esta manifestación tecnológica tiene el potencial de interferir, intencionadamente o no, en derechos fundamentales establecidos en la *Constitución Española*. Tomemos como ejemplo el *artículo 16*, que garantiza la libertad ideológica, religiosa y de culto. Una IA mal empleada o mal diseñada podría, teóricamente, llevar a cabo perfiles basados en ideologías, creencias religiosas o patrones de culto, infringiendo directamente este artículo y potencialmente forzando a individuos a declarar o revelar aspectos de su identidad ideológica o religiosa. Además, su *artículo 18* resalta la protección al derecho al honor, a la intimidad y al secreto de las comunicaciones. Con la creciente digitalización y la capacidad de la IA de procesar vastas cantidades de datos, se potencia el riesgo de invasiones a la privacidad y potenciales violaciones a la intimidad de los individuos. Podría darse el caso de que sistemas de IA monitoricen, registren y analicen conversaciones, comportamientos y patrones

sin el conocimiento o consentimiento del individuo, vulnerando así el secreto de sus comunicaciones y su intimidad personal. Por otro lado, el *artículo 19*, que asegura el derecho a la libre circulación, podría verse amenazado si la IA es utilizada para realizar seguimientos invasivos o controlar movimientos basándose en criterios políticos o ideológicos, limitando así la libertad de movimiento de individuos basados en prejuicios o discriminaciones. Estos ejemplos resaltan la necesidad imperante de que la implementación y uso de la IA esté en consonancia con principios éticos y derechos fundamentales, como los consagrados en la *Constitución Española*, para evitar erosiones en nuestras libertades y garantías básicas.

No hay que olvidar que algunos países ya han comenzado a implementar sistemas de "crédito social" basados en IA para monitorear y regular el comportamiento ciudadano, un escenario que podría extrapolarse a contextos de aplicación de la ley si no se toman las precauciones adecuadas (Levy y Schneier, 2020). El "crédito social" es un enfoque que busca asignar una puntuación o calificación a los ciudadanos basada en su comportamiento, acciones y decisiones en diferentes esferas de la vida diaria. Estas puntuaciones se generan mediante la recolección y análisis de grandes cantidades de datos, que pueden incluir desde transacciones financieras y historiales de crédito, hasta hábitos de consumo, comportamiento en redes sociales y, en algunos casos, incluso interacciones personales y opiniones políticas. Este sistema, al ser alimentado y regulado por algoritmos, puede tener implicaciones serias en términos de privacidad y libertades civiles, ya que un puntaje bajo podría resultar en sanciones o restricciones, mientras que un puntaje alto podría otorgar beneficios y privilegios. Un ejemplo notable de la implementación de un sistema de crédito social es China. En este país, el sistema ha sido promovido como una herramienta para mejorar la confianza y la moral en la sociedad. Las puntuaciones pueden afectar una amplia gama de aspectos de la vida de una persona, desde la capacidad para obtener préstamos o contratos de arrendamiento, hasta la posibilidad de viajar o acceder a determinados trabajos. Ciudadanos con puntajes bajos debido a comportamientos considerados no deseados, como evadir tarifas de transporte o difundir información falsa en línea, pueden encontrar restricciones en servicios como viajar en tren o avión. Por otro lado, aquellos con puntuaciones altas pueden recibir beneficios como descuentos en servicios públicos o prioridad en listas de espera para servicios de salud. La preocupación con sistemas como estos radica en el potencial abuso y en las implicaciones éticas relacionadas con la privacidad y la autonomía personal. Además, la posibilidad de que estos sistemas se implementen en contextos de aplicación de la ley añade una capa adicional de complejidad al debate sobre su uso y regulación.

Estos riesgos subrayan la necesidad urgente de regulaciones efectivas y prácticas éticas en el uso policial de la IA. Es imperativo adoptar un enfoque basado en los derechos humanos para garantizar que la aplicación de la IA en la Seguridad Pública respete la privacidad, la autonomía y la dignidad de las personas

(Fjeld et al., 2020). Las fuerzas de seguridad, los encargados de formular políticas y la comunidad en general deben colaborar estrechamente para establecer salvaguardias que mitiguen estos riesgos sin socavar la eficacia de las operaciones policiales.

4. EL EQUILIBRIO ENTRE LA PRIVACIDAD Y EL INTERÉS COLECTIVO

La garantía de derechos y libertades en una sociedad democrática y constitucional depende en gran medida de la existencia y las actuaciones de las fuerzas de seguridad pública que estén comprometidas con el bienestar y la seguridad de todos los ciudadanos. Estas fuerzas, al ser el brazo ejecutor del Estado, debe operar bajo principios éticos y legales que salvaguarden los derechos fundamentales de las personas y que, al mismo tiempo, busquen el interés colectivo. El *artículo* 12 de los *Derechos del Hombre y del Ciudadano de 1789* es un testimonio clave de esta visión, estableciendo que la garantía de los derechos del Hombre y del Ciudadano necesita de una fuerza pública. Por tanto, esta fuerza ha sido instituida en beneficio de todos y no para provecho de aquellos a los que ha sido encomendada. Este precepto refleja la esencia de una fuerza pública que actúa como garantista de derechos, y no como instrumento represor. Esta visión se extiende a otras normas, como la *Resolución 34/169, de 17 de diciembre de 1979, de la Asamblea General de las Naciones Unidas sobre el Código de Conducta para los funcionarios encargados de hacer cumplir la ley*, que resalta la responsabilidad global de garantizar que aquellos en posiciones de poder y autoridad, como los funcionarios encargados de hacer cumplir la ley, actúen con el más alto grado de integridad y respeto hacia los derechos humanos. Con este marco ético y legal en mente, nos adentramos en una era donde la tecnología y la inteligencia artificial plantean desafíos y oportunidades sin precedentes en la relación entre privacidad, la seguridad pública y el interés colectivo.

En el equilibrio entre la privacidad y el interés colectivo radica una de las más delicadas tensiones en el desarrollo de estas tecnologías en el ámbito policial: ¿Hasta qué punto debe el interés colectivo en la seguridad y la prevención del delito prevalecen sobre los derechos individuales a la privacidad y la protección de datos? ¿Es posible hallar un punto de equilibrio entre estas dos demandas aparentemente en conflicto? Los temas aquí tratados plantean preguntas esenciales: ¿Cómo navegar entre la ética deontológica y utilitarista en la toma de decisiones sobre privacidad y datos? ¿En qué condiciones específicas puede el interés público superar el derecho individual a la privacidad? Y, de forma más amplia, ¿cómo pueden las sociedades democráticas mantener un compromiso con la privacidad mientras se aprovecha la capacidad de la IA para mejorar la Seguridad Pública? Para adentrarnos en estas cuestiones cruciales, examinaremos cómo las corrientes éticas de la deontología y el utilitarismo guían nuestras decisiones sobre privacidad y protección de datos en el ámbito policial. Estas

dos corrientes éticas toman relevancia especial cuando se trata de la utilización de la IA en el ámbito policial, donde se plantean complejos dilemas morales y éticos en torno a la privacidad y la protección de datos (Baquero Pérez, 2023).

Desde una perspectiva deontológica, ciertos principios, como el derecho a la privacidad y el control de los datos personales, son intrínsecamente valiosos y deben ser respetados, independientemente de las posibles consecuencias de su aplicación. Immanuel Kant (1724-1804), uno de los filósofos deontológicos más destacados, sostenía que los individuos deben ser tratados como fines en sí mismos y no como medios para lograr otros objetivos. En el contexto policial, esto podría implicar que los individuos tienen un derecho inalienable a no ser sujetos de vigilancia o recolección de datos sin su consentimiento explícito, incluso si tal recolección de datos pudiera tener beneficios, como una mayor Seguridad Pública (Bok, 1983). En contraste, el utilitarismo evalúa la ética de una acción en función de sus consecuencias, buscando maximizar la felicidad o el bienestar general. Según esta escuela de pensamiento, popularizada por filósofos como Jeremy Bentham (1748-1832) y John Stuart Mill (1806-1873), podría considerarse ético utilizar la IA para analizar datos policiales si esta acción resulta en un bien mayor, como la prevención del crimen o el aumento de la Seguridad Pública. Sin embargo, este enfoque podría justificar ciertos grados de violación a la privacidad individual en aras de beneficios sociales más amplios, como podría ser el uso de algoritmos de IA para prevenir actividades delictivas antes de que sucedan, incluso a costa de la privacidad de los individuos (Nissenbaum, 2010).

Navegar entre estos dos enfoques éticos constituye un desafío significativo en el desarrollo y la implementación de tecnologías de IA en el ámbito policial. Es crucial encontrar un equilibrio que respete los derechos individuales a la privacidad y la protección de datos, mientras se buscan formas de maximizar los beneficios potenciales de la IA en la mejora de la Seguridad Pública y la eficacia de la aplicación de la ley. Este delicado equilibrio obliga a un diálogo constante entre las autoridades, los desarrolladores de IA, los defensores de la privacidad y la comunidad en general, para asegurar que la tecnología se utilice de una manera que sea tanto ética como eficaz. En este sentido, para tomar decisiones informadas y equilibradas en contextos que enfrentan dilemas éticos, como el equilibrio entre el derecho individual a la privacidad y la seguridad pública, es esencial seguir un proceso reflexivo y consultivo. Primero, es crucial reconocer y comprender el dilema en cuestión. Luego, se debe recopilar información relevante sobre la tecnología propuesta, considerando su eficacia, riesgos y datos históricos relacionados. Es fundamental involucrar a todas las partes interesadas en el proceso, incluidos expertos, comunidad y proveedores tecnológicos. Al evaluar las alternativas, se deben buscar soluciones que logren objetivos similares sin comprometer demasiado la privacidad. Además, cualquier medida adoptada debe ser proporcional al problema y garantizar la transparencia y el consentimiento de las partes afectadas. Una vez en marcha, es vital revisar periódicamente la medida, establecer protocolos de uso de datos claros, educar

al público y prepararse para futuras adaptaciones. Este enfoque centrado en la ética asegura que se considere tanto la seguridad pública como los derechos fundamentales de los individuos en cualquier decisión tomada.

Además de las perspectivas deontológica y utilitarista, es esencial considerar la ética de la virtud, que pone énfasis en el carácter y las virtudes morales de las personas involucradas. Basada en las enseñanzas de Aristóteles, la ética de la virtud sostiene que las decisiones éticas no dependen únicamente de reglas o de la evaluación de consecuencias, sino en las virtudes y el carácter moral de aquellos que toman las decisiones. En el escenario de la IA en el ámbito policial, esto implica un enfoque especial en las personas que diseñan e implementan estos sistemas. Es esencial que estas personas reciban formación adecuada no solo en aspectos técnicos, sino también en ética y derechos humanos. Deberían ser alentados a reflexionar sobre su papel y responsabilidad en la creación de tecnologías que pueden afectar profundamente los derechos y libertades individuales. La ética de la virtud, en este contexto, promovería el desarrollo de sistemas de IA que sean producto de individuos y equipos que busquen constantemente la integridad, la prudencia y el respeto hacia los derechos de los ciudadanos. Estas medidas, centradas en las personas, se convierten en un pilar crucial para garantizar que la tecnología se utilice de manera ética y responsable.

Para aplicar estos enfoques, el deontológico y el utilitarismo, es indudable que hay tener en cuenta y valorar el interés público en la seguridad y la prevención del crimen puede justificar ciertas limitaciones a la privacidad individual. En el contexto policial, esto puede manifestarse de múltiples formas. Por ejemplo, la recopilación y análisis de datos mediante el uso de tecnologías como el reconocimiento facial o la telemetría vehicular pueden ser herramientas esenciales para las fuerzas del orden en la identificación de sospechosos y en la prevención o resolución de crímenes (Solove, 2002). Sin embargo, como en el caso de las aplicaciones de rastreo de contactos usadas en la pandemia de COVID-19, la recolección y el uso de estos datos deben ser proporcionales a la amenaza en cuestión y contar con salvaguardias que aseguren la mínima invasión a la privacidad (Ferretti et al., 2020). Es decir, la cantidad de información personal recopilada debe ser la estrictamente necesaria para alcanzar los objetivos de Seguridad Pública y prevención del delito.

También, hay que recalcar que la privacidad es un componente esencial en una sociedad democrática, permitiendo a las personas actuar y pensar libremente sin interferencias externas indebidas (Cohen, 2012). Sin embargo, hemos visto que la adopción de la IA en el ámbito policial introduce dilemas éticos y riesgos para la privacidad que son particularmente sensibles y polémicos. Uno de los desafíos más grandes en este ámbito se origina en la recopilación y análisis de grandes conjuntos de datos, o Big Data, en investigaciones policiales y de seguridad. Estas prácticas pueden resultar en intrusiones a la privacidad al descubrir detalles íntimos y comportamientos de los individuos que de otro modo serían privados. Por ejemplo, si utilizamos la recopilación de metadatos

de comunicaciones por parte de las agencias de seguridad puede revelar patrones de comportamiento y relaciones personales que la mayoría de las personas consideraría privadas (Mayer-Schönberger y Cukier, 2013). Las herramientas de IA, como el reconocimiento facial y el análisis de comportamiento, elevan estos riesgos, permitiendo un grado de vigilancia y perfilado nunca antes posible.

Dado que este tipo de tecnologías están siendo cada vez más empleadas por las fuerzas de seguridad, generando preocupaciones serias sobre la erosión de libertades civiles y la posibilidad de acercarnos a una sociedad de vigilancia masiva. Adicionalmente, las transgresiones en el ámbito de la privacidad pueden erosionar la confianza pública en las instituciones policiales, algo vital en cualquier sociedad democrática. Si las personas comienzan a sentir que sus datos pueden ser utilizados de forma indebida o discriminatoria por las fuerzas de seguridad, podrían volverse reacias a cooperar en investigaciones o incluso a denunciar crímenes. Por tanto, es clave que las políticas y regulaciones de privacidad y protección de datos sean robustas y transparentes. Dichas políticas deben establecer reglas claras sobre qué datos pueden ser recolectados, cómo deben ser usados y almacenados, y bajo qué circunstancias pueden ser compartidos. Además, deberían proporcionar mecanismos de transparencia y consentimiento informado para los individuos afectados (Richards y King, 2014).

Es crucial destacar que, aunque el interés público pueda a veces superar el derecho a la privacidad individual, cualquier excepción a este derecho debe ser específica, justificada y acompañada de medidas de mitigación de riesgos. En este sentido se vuelve a recalcar la necesidad de un constante diálogo entre todas las partes implicadas, desde las autoridades policiales y los ingenieros de IA a los defensores de los derechos humanos y la comunidad en general, para asegurarse de que la tecnología se utilice de manera que maximice la utilidad pública sin erosionar los fundamentos éticos y los derechos individuales. Como un caso ilustrativo, supongamos que en una ciudad se ha registrado un aumento preocupante en los casos de secuestros. Las autoridades, en su esfuerzo por combatir esta ola delictiva y garantizar la seguridad de sus ciudadanos, proponen el uso de la telemetría vehicular para rastrear y localizar rápidamente vehículos asociados con actividades sospechosas. Cuando sucede un caso de secuestro, las autoridades pueden utilizar datos de telemetría vehicular para identificar y seguir en tiempo real a vehículos que hayan estado cerca del lugar del incidente o que se desplacen de manera inusual. Así, con esta tecnología podría la policía localizar y detener un vehículo sospechoso poco después de un secuestro. Sin embargo, esta herramienta también recopila datos de telemetría de miles de vehículos inocentes. Para abordar las preocupaciones de privacidad, las autoridades pueden implementar protocolos estrictos. Por ejemplo, solo se accedería a los datos cuando hay una amenaza inmediata y justificada, y la información se retiene solo por un corto período de tiempo, tras el cual se elimina automáticamente. Además, se podría establecer un comité de supervisión independiente para auditar y revisar regularmente el uso de la herramienta y garantizar que

se utilice únicamente en circunstancias excepcionales y justificadas. A través de foros públicos, las autoridades también podrían informar a la comunidad sobre cómo funciona la herramienta, las medidas de salvaguardia en su lugar y sus derechos en relación con los datos recopilados. De esta manera, la ciudad puede abordar la necesidad urgente de responder al problema de los secuestros, aprovechando la tecnología para mejorar la Seguridad Pública, mientras también establece medidas para proteger la privacidad y garantizar la transparencia y la rendición de cuentas.

En definitiva, el uso de la IA en el ámbito policial, la aplicación de los principios deontológicos y utilitaristas tienen su relevancia. Ya se ha dicho que los algoritmos de aprendizaje automático pueden ser empleados, por ejemplo, en la predicción de crímenes o en el análisis de patrones de comportamiento sospechoso y, aunque, estas aplicaciones pueden ser útiles para la Seguridad Pública, su diseño y uso deben ser cuidadosamente gestionados para minimizar las violaciones a la privacidad. No solo se trata de maximizar la efectividad en la prevención y solución de crímenes, sino también de preservar los principios democráticos y la confianza pública que son fundamentales para la cohesión y estabilidad de nuestras sociedades. En este sentido, aparte de que es importante que estos sistemas sean transparentes, auditables y sujetos a revisión judicial para evitar abusos y asegurar que su aplicación esté en línea con los principios éticos y deontológicos, son medidas fundamentales la aplicación de métodos que mitigen los riesgos.

5. MITIGACIÓN DE LOS RIESGOS: MÉTODOS PARA PROTEGER LA PRIVACIDAD Y LOS DATOS EN APLICACIONES DE LA IA

La adopción de la IA nos plantea preguntas ineludibles sobre la privacidad, la ética y la seguridad de los datos recopilados y procesados. ¿Cómo pueden las fuerzas de seguridad aprovechar el poder de la IA sin comprometer la privacidad y los derechos de los ciudadanos? ¿Qué métodos existen para proteger datos sensibles y al mismo tiempo mantener la utilidad de los sistemas de IA? ¿Cómo podemos garantizar que estos métodos sean éticamente sólidos y socialmente aceptables? Está claro que la aplicación de las medidas normativas, fundamentalmente las específicas que garantizan la protección de los datos personales, es una herramienta básica para mitigar los riesgos. Aunque en este trabajo se busca ir más allá de estas medidas normativas, por lo que se abordará estos desafíos complejos explorando varios métodos y herramientas que se pueden emplear para mitigar los riesgos asociados y así facilitar que se logre un mejor equilibrio entre la privacidad, la utilidad y la ética en el uso de IA en el ámbito policial.

En primer lugar, examinaremos las técnicas de anonimización y sus limitaciones. La anonimización de datos ha sido una estrategia común para proteger la identidad de los individuos en conjuntos de datos, pero no está exenta de desafíos, especialmente en el contexto policial. Exploraremos cómo las técnicas de

anonimización pueden ser tanto una bendición como una maldición, ofreciendo protección, pero también limitando la utilidad de los datos. A continuación, se abordan los problemas de consentimiento y notificación en la recopilación y procesamiento de datos policiales. El consentimiento y la notificación son conceptos fundamentales en la ética de la privacidad de datos, pero enfrentan desafíos únicos en el ámbito policial, donde la relación de poder entre las autoridades y los ciudadanos es inherentemente desigual. Luego, se tratará la limitación del almacenamiento de los datos. Por último, analizaremos métodos y herramientas adicionales para proteger la privacidad y los datos en el ámbito policial. Estos métodos incluyen innovaciones como el aprendizaje diferencialmente privado, el aprendizaje federado y el cifrado homomórfico, cada uno con sus propias ventajas y desventajas en el contexto de la Seguridad Pública. En este artículo, nos centraremos en el aprendizaje diferencialmente privado dado que es actualmente el que parece que tiene un desarrollo más prometedor.

Juntas, estas secciones ofrecen una visión panorámica de las estrategias y métodos que pueden ayudar a mitigar los riesgos inherentes al uso de la IA en el ámbito policial. Sin embargo, como veremos, no hay soluciones perfectas, en muchos casos sujeto a deliberaciones entre las partes implicadas. Cada método presenta su propio conjunto de desafíos éticos y técnicos que deben abordarse de manera cuidadosa y considerada.

5.1. Técnicas de anonimización y sus limitaciones

La *Ley Orgánica 7/2021*, en su *artículo 28*, se ocupa de la importancia de la protección de datos desde el diseño y por defecto en el tratamiento de datos personales. Dentro de las técnicas que sugiere para lograr esto está la "seudonimización", que consiste en despersonalizar los datos de tal forma que no puedan atribuirse a una persona sin información adicional. En el ámbito de la protección de datos personales, tenemos tanto la seudonimización como la anonimización, que comparten objetivos fundamentales. Primero, ambas técnicas están diseñadas para proteger la privacidad del individuo minimizando los riesgos asociados con el uso indebido de su información. Se buscan medidas que salvaguarden los derechos y libertades de las personas, como se enfatiza en el *artículo 28* de la *Ley Orgánica 7/2021*. En segundo lugar, tanto la seudonimización como la anonimización se adhieren al principio de "minimización de datos personales". Este principio, también destacado en el *artículo 28*, implica que solo deben tratarse los datos estrictamente necesarios para alcanzar los objetivos específicos del tratamiento. Esto se traduce en un esfuerzo consciente por limitar el alcance y la cantidad de información personal manipulada.

Aunque similares en intención, las técnicas de seudonimización y anonimización difieren en varios aspectos clave. Por un lado, la seudonimización, tal como la define la *Ley Orgánica 7/2021*, es un proceso reversible si se dispone de información adicional. La anonimización, en cambio, aspira a hacer irreversible

la identificación de la persona. Además, el alcance de estas técnicas varía. El *artículo 28* sugiere la seudonimización como una de las posibles medidas a adoptar. Sin embargo, la anonimización va más allá, empleando diversas técnicas como la supresión, la perturbación y la generalización de datos, con el objetivo de hacer casi imposible o completamente imposible la identificación de individuos. Otra diferencia reside en la complejidad técnica y el costo asociado a cada técnica. La anonimización suele requerir una manipulación más extensa de los datos y, por lo tanto, podría ser más costosa y compleja. En contrapartida, la seudonimización, que la Ley considera apropiada conforme al estado de la técnica y el coste de la aplicación, podría resultar más accesible en ciertos contextos. Finalmente, en términos de aplicabilidad, la seudonimización podría ser más apropiada cuando se requiere cierto nivel de reversibilidad en el tratamiento de los datos. En contraposición, la anonimización se prefiere cuando no hay necesidad alguna de reidentificar la información en el futuro. La elección entre una u otra dependerá de diversos factores como el contexto en el que se aplicarán, el propósito específico del tratamiento y los riesgos asociados a la información manejada.

En cualquier caso, la anomización protege más la privacidad de las personas, por lo que se considera que debería ser la primera opción cuando no haya una necesidad clara de reindentificar. Es una estrategia comúnmente empleada para proteger la privacidad y los datos personales en el uso de la IA. Esta técnica consiste en la eliminación o modificación de información que podría usarse para identificar a individuos específicos dentro de un conjunto de datos, como registros de arrestos o informes de incidentes (Sweeney, 2002). Entre las técnicas de anonimización más utilizadas en este contexto se encuentran la supresión de datos, que elimina información como nombres y números de identificación; la perturbación de datos, que altera detalles como ubicaciones exactas de incidentes; y la generalización de datos, que sustituye datos específicos por categorías más amplias, como cambiar el tipo de delito por una categoría más general. Por ejemplo, en una base de datos de detenidos, la supresión de datos podría implicar la eliminación de nombres, números de identificación y huellas dactilares. La perturbación de datos podría alterar las fechas y horas exactas de los arrestos, mientras que la generalización de datos podría consistir en cambiar el barrio exacto donde ocurrió un delito por una región más amplia.

Sin embargo, la anonimización en datos policiales también tiene sus desafíos. El más importante, es evitar que se pueda llegar a conseguir la reidentificación, donde individuos pueden ser nuevamente identificados a partir de datos aparentemente anónimos. Este riesgo es especialmente elevado cuando estos datos se combinan con otros conjuntos de datos, como registros públicos o bases de datos de redes sociales (Narayanan y Shmatikov, 2010). Un ejemplo ilustrativo de esto es el caso estado de Massachusetts en 2006, donde registros de hospital supuestamente anónimos fueron cruzados con registros públicos de votantes, permitiendo reidentificar al gobernador a partir de su historial médico

(Sweeney, 2002). Este suceso pone en evidencia cómo la interacción de diferentes bases de datos, incluso cuando uno de ellos está anonimizado, puede llevar a la identificación de individuos concretos, poniendo en riesgo su privacidad y seguridad. Es vital tener en cuenta estos riesgos cuando se trabaja con datos sensibles en contextos como el policial. Además, la anonimización puede comprometer la utilidad de los datos para aplicaciones de IA en el ámbito policial. Por ejemplo, la alteración de ubicaciones y tiempos específicos podría dificultar el análisis predictivo de delitos o la evaluación precisa de la efectividad de las estrategias de patrullaje (Machanavajjhala et al., 2007).

Por tanto, aunque la anonimización es un método valioso para la protección de la privacidad en el contexto de la IA y la Seguridad Pública, no es una panacea. Se necesitan enfoques complementarios como políticas de privacidad más estrictas, regulaciones de uso de datos específicas para el ámbito policial y técnicas más avanzadas como la privacidad diferencial, que veremos más abajo, que permiten el análisis de datos manteniendo al mismo tiempo la privacidad de los individuos involucrados (Dwork et al., 2006).

5.2. Problemas de consentimiento y notificación en la recopilación y procesamiento de datos policiales

El consentimiento y la notificación son elementos clave en la recopilación y procesamiento de datos en el ámbito policial, especialmente cuando se incorporan tecnologías de IA. El consentimiento implica un acuerdo explícito del individuo para permitir el procesamiento de sus datos personales, mientras que la notificación se refiere a la información proporcionada a los individuos sobre cómo se recolectarán y utilizarán sus datos. Estos dos conceptos enfrentan desafíos únicos y significativos en el contexto policial.

En primer lugar, el consentimiento en el ámbito policial rara vez es voluntario debido a la relación de poder asimétrica entre la policía y los ciudadanos. Este hecho se complica aún más cuando consideramos las disposiciones legales que permiten el acceso a información personal sin el consentimiento del individuo. Por ejemplo, según la *Ley Orgánica 7/2021, Disposición adicional cuarta*, las autoridades competentes pueden solicitar al Instituto Nacional de Estadística y a los órganos estadísticos de ámbito autonómico, sin necesidad del consentimiento del interesado, una copia actualizada de ficheros que contienen datos personales como documento de identidad, nombre, apellidos, domicilio, sexo y fecha de nacimiento. Estos ficheros están formados con los datos que constan en el padrón municipal de habitantes y en el censo electoral. Además, los sistemas policiales se pueden nutrir de bases de datos donde no se requiere el consentimiento del ciudadano. Por tanto, en el contexto español, la *Ley Orgánica 7/2021* permite que las autoridades tengan acceso a dichos datos para fines específicos de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, así como para la protección y prevención

frente a las amenazas contra la Seguridad Pública. Estas disposiciones legales crean un escenario en el que las autoridades tienen un acceso considerable a información personal sin requerir la aprobación directa del individuo afectado, exacerbando la ya de por sí asimétrica relación de poder entre las instituciones de la ley y los ciudadanos.

Por otra parte, en muchos casos, las personas no tienen opción de negarse cuando la policía recopila datos para fines de investigación. Incluso si se solicita el consentimiento, como en el caso de la toma de muestras de ADN, la percepción de coacción o la falta de alternativas viables puede hacer que el consentimiento sea menos que genuino (Solove, 2013). Además, el proceso de consentimiento se complica aún más por políticas de privacidad que pueden ser largas y difíciles de entender. Este problema se agrava en el contexto policial, donde la recopilación de datos a menudo es urgente y no hay tiempo para explicaciones detalladas. La llamada "fatiga de privacidad" puede ser aún más pertinente aquí, dada la naturaleza sensible de los datos recopilados (Obar y Oeldorf-Hirsch, 2018). La "fatiga de privacidad" es un concepto que se refiere al agotamiento y la indiferencia que pueden experimentar los individuos al enfrentar decisiones constantes relacionadas con la privacidad y la protección de datos. En un mundo cada vez más digital, se les pide a las personas que revisen y acepten términos de servicio y políticas de privacidad con regularidad, muchas veces sin leer o comprender completamente las implicaciones de lo que están aceptando. En el contexto policial, la fatiga de privacidad puede ser particularmente problemática debido a la urgencia y la sensibilidad de las situaciones. Cuando la recopilación de datos es inmediata y hay poco tiempo para detenerse a considerar las implicaciones de la privacidad, la fatiga de privacidad puede llevar a los individuos a ceder sus datos personales sin entender completamente las consecuencias de hacerlo. Dada la naturaleza sensible de los datos que se manejan en este ámbito (como información biométrica, historiales criminales o ubicaciones geográficas) el riesgo asociado con la fatiga de privacidad es especialmente alto. Obar y Oeldorf-Hirsch (2018) exploran cómo esta fatiga de privacidad puede llevar a decisiones apresuradas o indiferentes que pueden tener graves consecuencias para la protección de datos personales. Las personas pueden, por ejemplo, aceptar rápidamente términos y condiciones sin leerlos o podrían optar por ignorar notificaciones de seguridad, lo que podría resultar en el uso indebido o la exposición de datos sensibles. En definitiva, la fatiga de privacidad es un fenómeno creciente que tiene importantes implicaciones para la toma de decisiones consciente y bien informada en relación con la privacidad y la protección de datos, especialmente en contextos de alta urgencia y sensibilidad como la aplicación de la ley.

En cuanto a la notificación, su eficacia se ve comprometida cuando las tecnologías de IA que se utilizan para procesar datos policiales son opacas o complejas. Las técnicas avanzadas de aprendizaje automático, como el "aprendizaje profundo", son particularmente difíciles de entender, lo que amplifica el problema de la "caja negra" en el contexto policial (Pasquale, 2015). Los ciudadanos

pueden no estar al tanto de cómo se están utilizando sus datos, cuánto tiempo se almacenarán, qué algoritmos se están aplicando para analizarlos o cómo estos algoritmos analizan sus datos. Por ejemplo, en una ciudad donde se implemente un sistema de cámaras de vigilancia con reconocimiento facial basado en aprendizaje profundo, los residentes pueden ser notificados de la recopilación de imágenes, pero no se les explica detalladamente cómo funcionaba el algoritmo ni cómo se toman las decisiones a partir del análisis de esas imágenes. Este desconocimiento puede llevar a preocupaciones y sospechas por parte de la comunidad, que se puede sentir incomprendida y en cierto modo vigilada sin un consentimiento claro sobre cómo exactamente se procesaban sus datos. Este tipo de incidentes subraya la importancia de una comunicación clara y transparente acerca de las complejas tecnologías de IA, para que los ciudadanos puedan tomar decisiones informadas y confiar en las autoridades.

Por lo tanto, aunque el consentimiento y la notificación son conceptos críticos en la protección de la privacidad y los datos personales, se enfrentan con desafíos particulares en el contexto policial y la utilización de IA. Estos desafíos hacen más apremiante la necesidad de enfoques múltiples para abordar la privacidad y la protección de datos en este ámbito. Estos pueden incluir una mayor transparencia en los métodos de recopilación y procesamiento, rendición de cuentas por parte de las agencias de aplicación de la ley, y una regulación más efectiva que vaya más allá de los enfoques tradicionales de consentimiento y notificación (Mittelstadt et al., 2016).

5.3. Eliminación periódica de datos

En la era de la acumulación masiva de datos y el aprendizaje automático avanzado, la conservación indefinida de datos se ha convertido en una práctica común en muchos ámbitos, incluido el policial. No obstante, la retención prolongada de datos personales plantea serios riesgos para la privacidad y la protección de datos. Es aquí donde la eliminación periódica de datos se presenta como una medida esencial para mitigar estos riesgos. La retención indefinida de datos no sólo amplía el potencial de abuso y mal uso de la información, sino que también aumenta las posibilidades de que los datos se filtren, se corrompan o se utilicen de manera no ética. Implementar un protocolo de eliminación periódica puede reducir estos riesgos y alinear la práctica policial con los principios de minimización de datos y limitación de la conservación, consagrados en regulaciones de protección de datos como el RGPD en Europa y en la *Ley Orgánica 7/2021*. De acuerdo con la *Ley Orgánica 7/2021*, se establece una estructura clara sobre los plazos de conservación y revisión de datos personales en el ámbito policial en su *artículo 8*. El responsable del tratamiento debe asegurarse de que los datos se conserven solo por el tiempo necesario para cumplir con los fines previstos, y, además, está obligado a revisar la necesidad de conservación de estos datos, al menos, cada tres años. Esta revisión debe considerar diversos factores, como la

edad del afectado, el tipo de datos y el estado de cualquier investigación o procedimiento penal relacionado. La Ley también establece un plazo máximo general para la eliminación de datos de veinte años, aunque este plazo puede extenderse bajo ciertas circunstancias, como investigaciones abiertas, delitos no prescritos o la necesidad de proteger a las víctimas. Este enfoque legislativo reconoce los riesgos asociados con la retención prolongada de datos y busca equilibrar la necesidad de conservar información para fines policiales con los derechos de privacidad de los individuos. Es un recordatorio crucial de que, mientras las tecnologías avanzan y la capacidad de almacenar datos aumenta, las consideraciones éticas y legales deben seguir siendo primordiales para garantizar la protección de los derechos individuales y la confianza pública en las instituciones. Sin embargo, la eliminación periódica de datos no está exenta de desafíos. Uno de los principales obstáculos es determinar qué datos deben conservarse y por cuánto tiempo, especialmente cuando la utilidad potencial de los datos para investigaciones futuras es incierta. Además, la eliminación de datos debe llevarse a cabo de una manera que sea irrecuperable para garantizar que los datos eliminados no puedan ser restaurados o accedidos posteriormente.

Una posible solución es establecer políticas claras y protocolos rigurosos para la eliminación de datos, que incluyan auditorías regulares y la capacitación de personal encargado de la gestión de datos. Las herramientas de automatización pueden programarse para eliminar datos que ya no sean necesarios o relevantes, según criterios predefinidos. Además, es crucial que la eliminación de datos sea parte integral del diseño de los sistemas de información en el ámbito policial. Esto es coherente con el concepto de "protección de datos desde el diseño". Este concepto es un enfoque que aboga por integrar medidas de privacidad y protección de datos desde las fases iniciales de diseño y desarrollo de cualquier proyecto, producto o servicio que implique el manejo de datos personales. En lugar de añadir características de privacidad y seguridad como un complemento posterior, este principio insiste en que deben ser componentes fundamentales que se incorporan en cada etapa del ciclo de vida del desarrollo. La idea es que, al considerar los aspectos de privacidad desde el inicio, se pueden identificar y mitigar proactivamente los riesgos potenciales para la privacidad y la protección de datos. Esto implica desde el diseño de la arquitectura del sistema y la selección de tecnologías empleadas, hasta la implementación de políticas y prácticas operacionales. También puede incluir medidas como la minimización de datos (recopilación de solo los datos estrictamente necesarios para el objetivo previsto), el uso de tecnologías de encriptación y la implementación de controles de acceso robustos. Este enfoque es especialmente relevante dada la complejidad y la naturaleza cambiante de las tecnologías de la información, donde las amenazas a la privacidad y la seguridad de los datos pueden ser difíciles de prever. Adoptar la protección de datos desde el diseño ayuda a construir una base sólida en materia de privacidad, facilitando el cumplimiento de la *Ley Orgánica 7/2021* y fortaleciendo la confianza del usuario en el producto o servicio en cuestión.

Por lo tanto, la eliminación periódica de datos se presenta como una necesidad imperante en el ámbito policial, especialmente cuando se aplican tecnologías de IA para la recopilación y el procesamiento de datos. Si bien la implementación de esta medida trae consigo varios desafíos, las soluciones y buenas prácticas emergentes ofrecen un camino viable para equilibrar las necesidades de las investigaciones policiales con los derechos de privacidad de los individuos.

5.4. Métodos y herramientas adicionales para proteger la privacidad y los datos en el ámbito policial

Además de las herramientas anteriores, hay varios otros métodos que pueden emplearse para proteger la privacidad y los datos en aplicaciones de IA en el contexto policial. Uno de estos métodos es el aprendizaje diferencialmente privado o privacidad diferencial. Este enfoque puede ser particularmente útil en situaciones como el análisis de grandes bases de datos de antecedentes penales o patrones de criminalidad. Este método garantiza que el análisis de dichas bases de datos no revelará información identificable de un individuo, sin sacrificar el valor general del análisis para las investigaciones o políticas públicas (Dwork y Roth, 2014). Este enfoque es el que se considera más prometedor, por lo que se tratará en un subapartado específico.

Por otro lado, el aprendizaje automático seguro multi-partes es otro enfoque para preservar la privacidad que permite a varias partes entrenar conjuntamente un modelo de aprendizaje automático sobre sus conjuntos de datos combinados sin compartir los datos en sí. A través de esta técnica, cada participante puede mantener la privacidad de sus propios datos mientras contribuye a un esfuerzo cooperativo de aprendizaje automático (Lindell y Pinkas, 2009). Un método basado en este enfoque es el aprendizaje federado (Federated Learning). Imaginemos, por ejemplo, que diferentes departamentos de policía quieren colaborar en el entrenamiento de un modelo de IA para predecir el crimen. El aprendizaje federado permitiría que cada departamento entrenara el modelo en sus propios datos localmente. Solo los resúmenes del modelo se comparten y se combinan para crear un modelo más robusto, sin compartir datos sensibles entre departamentos (Konečný et al., 2016). El aprendizaje automático federado es una técnica que permite el entrenamiento de modelos de IA sin la necesidad de compartir directamente los datos personales. Esencialmente, este enfoque consiste en entrenar algoritmos de IA en local, es decir, en el mismo dispositivo donde se encuentran los datos (por ejemplo, un teléfono móvil o una computadora), en lugar de hacerlo en un servidor centralizado. Este proceso implica que solo los parámetros del modelo, y no los datos brutos, se comparten y se agregan para mejorar el modelo global. De esta manera, se puede mejorar la precisión de los modelos de IA a la vez que se protege la privacidad de los datos de los usuarios (Yang et al., 2019).

Por último, el cifrado homomórfico (Homomorphic Encryption) es otra herramienta que puede tener aplicaciones significativas en el ámbito policial. Este tipo de cifrado permitiría, por ejemplo, que los datos recolectados por cámaras corporales o drones sean procesados en un estado cifrado. Así, se podrían realizar análisis útiles sin comprometer la privacidad de las personas captadas en el material de video (Gentry, 2009). La encriptación homomórfica representa otra estrategia esencial para la protección de la privacidad en el ámbito de la IA. Esta técnica de encriptación avanzada permite el procesamiento de datos mientras estos permanecen encriptados, lo que significa que los algoritmos de IA pueden realizar operaciones en los datos sin necesidad de desencriptarlos, protegiendo así la privacidad de los datos (Gentry, 2009). En la mayoría de los esquemas de encriptación, los datos deben desencriptarse antes de poder procesarlos. Sin embargo, con la encriptación homomórfica, se puede realizar una gama de operaciones aritméticas (como suma y multiplicación) directamente sobre datos encriptados. Esto es particularmente útil en situaciones en las que los datos son demasiado sensibles para ser compartidos en forma no encriptada o cuando los datos deben ser procesados por una tercera parte que no debería tener acceso a la información sin encriptar. El primer esquema de encriptación homomórfica completamente funcional fue propuesto por Gentry. Desde entonces, la encriptación homomórfica ha encontrado aplicaciones en una variedad de campos, incluyendo servicios en la nube, aprendizaje automático privado, y más. Su utilización en IA permite el desarrollo y despliegue de modelos de aprendizaje automático que pueden operar directamente con datos encriptados, aumentando significativamente la privacidad y seguridad de los datos (Bos et al., 2014). Por supuesto, aún existen desafíos asociados con la encriptación homomórfica, incluyendo la complejidad computacional y el tiempo de procesamiento. Sin embargo, los avances continuos en esta área sugieren que la encriptación homomórfica jugará un papel cada vez más importante en la protección de la privacidad en el campo de la IA.

Es importante señalar que mientras estos métodos pueden ofrecer soluciones para mitigar los riesgos asociados con el uso de IA en la policía, aunque también añaden capas de complejidad técnica. Por otra parte, también implica consideraciones éticas. Por ejemplo, aunque estos métodos pueden proteger la identidad de los individuos, podría ser menos preciso en la identificación de patrones delictivos a nivel micro. Además, cada uno de estos métodos tiene sus propias limitaciones y desafíos que deben considerarse cuidadosamente en el contexto policial.

Tenemos, por tanto, métodos y herramientas adicionales para proteger la privacidad y los datos que pueden complementar a las técnicas de anonimización, a los enfoques basados en el consentimiento y la notificación, y a la limitación de los tiempos de almacenamiento de los datos. Sin embargo, por su complejidad técnica, la implementación efectiva de estos métodos requiere un equilibrio

cuidadoso entre la eficiencia, privacidad y utilidad, especialmente en un campo tan delicado como el policial.

5.5. Privacidad diferencial en el contexto de los datos policiales

De estos métodos, la privacidad diferencial se presenta como un modelo prometedor para abordar los desafíos éticos y de privacidad en el uso de la inteligencia artificial en el manejo de datos policiales. Esta teoría matemática, propuesta inicialmente por Dwork et al. (2006), tiene el potencial de proteger información sensible en investigaciones criminales y otros procesos policiales. Aunque tradicionalmente la privacidad diferencial se ha aplicado en áreas como el IoT o las tecnologías de la información, la privacidad diferencial tiene un potencial significativo para mejorar la ética y la privacidad en el uso de la IA en el ámbito policial. Al igual que empresas como Google y Apple han adoptado esta técnica para proteger la privacidad del usuario en sus respectivos ámbitos (Erlingsson, Pihur, y Korolova, 2014; Apple Inc., 2017), los sistemas policiales podrían beneficiarse enormemente de su implementación para mantener un equilibrio delicado entre la privacidad, la utilidad y la ética en sus operaciones. En el marco de la privacidad diferencial, se puede añadir un "ruido" calculado a las bases de datos policiales o a las consultas que se efectúan en ellas. Este ruido está diseñado para garantizar que el resultado de un análisis estadístico sea casi idéntico, con o sin la inclusión de datos de un individuo en particular. De esta forma, sería sumamente difícil para alguien inferir información sobre un individuo específico a partir de los datos agregados. Esto resulta particularmente relevante en el contexto policial, donde la divulgación de información sobre sospechosos, testigos o víctimas podría tener consecuencias severas (Dwork y Roth, 2014).

Por tanto, vemos que la privacidad diferencial ofrece un marco robusto para proteger la privacidad en aplicaciones de IA, pero su uso en el ámbito de datos policiales viene con su propio conjunto de desafíos y dilemas éticos. Uno de los dilemas más prominentes es el balance entre la preservación de la privacidad y la exactitud y utilidad de los datos en investigaciones y procedimientos policiales. En el contexto de la aplicación de la ley, donde las decisiones pueden tener consecuencias graves como el encarcelamiento o la absolución, la adición de "ruido" para proteger la privacidad puede comprometer la calidad de los datos y, por lo tanto, la eficacia de las investigaciones. En investigaciones criminales, la precisión de la información es crítica, y la introducción de ruido para proteger la privacidad puede en ocasiones comprometer la calidad de los datos para la toma de decisiones (Abadi et al., 2016). Aquí, el equilibrio entre la privacidad y la utilidad se vuelve crítico y delicado, y requiere una consideración ética minuciosa para alcanzar un balance adecuado (Dwork y Roth, 2014). Aún más, la privacidad diferencial puede introducir sesgos en los conjuntos de datos policiales y, por ende, en los modelos de IA que se alimentan de estos datos. Dicho sesgo es especialmente preocupante en el contexto policial debido al riesgo de que

afecte de manera desproporcionada a comunidades vulnerables o marginadas. En escenarios donde la aplicación de la ley ya está sujeta a críticas por prácticas injustas o discriminación, la introducción de sesgos adicionales por medio de la privacidad diferencial puede exacerbar estos problemas y socavar la confianza pública en las instituciones de aplicación de la ley (Bagdasaryan, Poursaeed, y Shmatikov, 2019).

En definitiva, es esencial que los encargados de la implementación de IA en contextos policiales sean plenamente conscientes de estos dilemas éticos. Esto podría implicar establecer robustas políticas de gobernanza de datos, realizar análisis de equidad para identificar y corregir sesgos en los datos y los modelos resultantes, y capacitar a los analistas policiales y otros actores clave en las implicancias éticas de las tecnologías de privacidad. La privacidad diferencial requiere además una comprensión técnica profunda y una implementación cuidadosa para ser efectiva. En el ámbito policial, esto podría requerir formación especializada para los analistas, asegurando que comprendan tanto las capacidades como las limitaciones de esta técnica. De este modo, aunque la privacidad diferencial ofrece un método prometedor para abordar cuestiones de privacidad en el uso de la IA en el ámbito policial, su implementación debe hacerse con un enfoque ético y consciente de los riesgos y desafíos inherentes, especialmente en lo que se refiere a la precisión de los datos y la equidad en la toma de decisiones.

6. CONCLUSIONES

La implementación de IA para mejorar la eficacia y eficiencia de las fuerzas de seguridad ya hemos visto que suscita serios dilemas éticos y conflictos de valor, particularmente en lo que respecta a la privacidad y la libertad individual. Un conflicto de valor palpable es la tensión entre la eficiencia en la aplicación de la ley y la privacidad de los ciudadanos. Por ejemplo, la IA puede procesar y analizar enormes cantidades de datos (desde registros de localización hasta registros de conversaciones en redes sociales) para identificar actividades delictivas o prevenir actos de terrorismo. Aunque estas aplicaciones pueden ser tremendamente efectivas en la mejora de la Seguridad Pública, también implican un riesgo significativo para la privacidad, ya que requieren la recopilación y análisis de datos sumamente sensibles (Mittelstadt et al., 2016).

Además, estos conflictos de valor pueden no ser claramente evidentes. Las tecnologías de IA pueden ser intrincadas y opacas, lo que dificulta que tanto el público como los reguladores comprendan plenamente su impacto en la privacidad y otros derechos fundamentales (Burrell, 2016). Esto es especialmente problemático en un entorno policial, donde las decisiones basadas en IA pueden tener consecuencias muy serias, como la detención o el enjuiciamiento de individuos. Por tanto, es crucial que tanto los diseñadores de estos sistemas de IA como los reguladores y la sociedad en su conjunto consideren cuidadosamente estos conflictos de valores. Las estrategias para abordar estos desafíos pueden

incluir la realización de evaluaciones de impacto en la privacidad específicas para el ámbito policial, la incorporación de principios éticos en el diseño de estas tecnologías y la insistencia en niveles más altos de transparencia y rendición de cuentas en las prácticas de uso de IA por parte de las fuerzas de seguridad (Floridi et al., 2018).

El estado actual de la privacidad diferencial y otras técnicas de mitigación de riesgos en el contexto de datos policiales ilustra un delicado balance entre la explotación del potencial de la IA y la salvaguardia de los derechos individuales y la privacidad. En el ámbito de la aplicación de la ley, la privacidad diferencial se destaca como una solución viable para mantener la confidencialidad de los datos. Sin embargo, esta técnica también enfrenta desafíos significativos, especialmente en lo que respecta a la precisión de los datos y el riesgo de sesgos, asi como, su complejedidad en su aplicación (Dwork y Roth, 2014; Bagdasaryan, Poursaeed, y Shmatikov, 2019).

A medida que la tecnología avanza, las capacidades para recopilar, almacenar y analizar grandes volúmenes de datos en el contexto policial crecerán, ampliando tanto las oportunidades como los riesgos asociados. Esto plantea desafíos cada vez más complejos para el campo de la IA y la privacidad de los datos. La creciente adopción de la IA en la vigilancia, el análisis de redes sociales y otros aspectos del trabajo policial demanda técnicas de mitigación de riesgos más efectivas y éticas. El desarrollo futuro en este ámbito debe enfrentar estos desafíos de manera proactiva. Se necesitan más investigaciones para mejorar la precisión de los datos en investigaciones criminales sin comprometer la privacidad. También es imperativo abordar los sesgos potenciales que podrían surgir al aplicar técnicas como la privacidad diferencial, especialmente porque estos sesgos pueden tener consecuencias reales y graves en la vida de las personas.

Por último, mientras que la normativa específica, como la *Ley Orgánica 7/2021* en España, proporcionan un marco legal para el manejo de datos personales en contextos específicos, como la prevención y enjuiciamiento de crímenes, estas leyes pueden quedarse cortas en abordar las complejidades éticas y de privacidad que surgen en el ámbito de la IA aplicada a la Seguridad Pública. Dada la capacidad de la IA para analizar y sintetizar enormes conjuntos de datos en una escala sin precedentes, el alcance de la información que se puede recopilar y utilizar para fines de vigilancia y aplicación de la ley se expande más allá de lo que la legislación actual podría haber anticipado. Además, la naturaleza a menudo opaca de los algoritmos de IA plantea cuestiones de responsabilidad y transparencia que no son completamente abordadas por las normativas legales existentes. Por lo tanto, es imperativo que los marcos legales evolucionen para mantenerse a la par con los avances tecnológicos, incorporando evaluaciones éticas más rigurosas y salvaguardias de privacidad específicas para las aplicaciones de IA en la Seguridad Pública.

A modo de conclusión, se puede afirmar que la IA tiene el potencial de transformar la forma en que la ley se aplica y se mantiene la Seguridad Pública, pero

esto no debe hacerse a expensas de la privacidad y los derechos civiles de los ciudadanos. Un enfoque equilibrado y éticamente informado es esencial para garantizar que se maximicen los beneficios de estas tecnologías, mientras se minimizan sus riesgos y desafíos éticos.

7. REFERENCIAS

Abadi, M., Chu, A., Goodfellow, I., McMahan, H. B., Mironov, I., Talwar, K., y Zhang, L. (2016). *Deep Learning with Differential Privacy*. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security.

Apple Inc. (2017). iOS Security Guide. https://www.apple.com/business/docs/iOS_Security_Guide.pdf

Babuta, A., Oswald, M., y Rinik, C. (2018). *Machine learning algorithms and police decision-making: legal, ethical and regulatory challenges*. Whitehall Report, núm. 3. Royal United Services Institute for Defense and Security Studies.

Bagdasaryan, E., Poursaeed, O., y Shmatikov, V. (2019). *Differential Privacy Has Disparate Impact on Model Accuracy*. In NeurIPS 2019: 33rd Conference on Neural Information Processing Systems. https://arxiv.org/pdf/1905.12101.pdf

Baquero Pérez, P.J. (2023). *Cuestiones éticas sobre la implantación de la inteligencia artificial en la administración pública*. Revista Canaria de Administración Pública, (1), 243–282.

Bok, S. (1983). *Secrets: On the Ethics of Concealment and Revelation*. Vintage Books.

Bos, J. W., Lauter, K., y Naehrig, M. (2014). *Private predictive analysis on encrypted medical data*. Journal of biomedical informatics, 50, 234-243.

Burrell, J. (2016). *How the machine 'thinks': Understanding opacity in machine learning algorithms*. Big data & society, 3(1).

Chen, M., Mao, S., y Liu, Y. (2014). *Big data: A survey. Mobile Networks and Applications*, 19(2), 171-209.

Chesney, R., y Citron, D. (2018). *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*. California Law Review, 107, 1753-1819.

Cohen, J. E. (2012). *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice*. Yale University Press.

Cohen, J. E. (2019). *Between Truth and Power: The Legal Constructions of Informational Capitalism*. Oxford University Press.

Comisión Europea. (2016a). *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)*.

Comisión Europea (2016b). *Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo*

Crawford, K. (2016). *Can an Algorithm Be Agonistic? Ten Scenes from Life in Calculated Publics*. Science, Technology, y Human Values, 41(1), 77-92.

Dhar, V. (2013). *Data science and prediction*. Communications of the ACM, 56(12), 64-73.

Dwork, C., McSherry, F., Nissim, K., y Smith, A. (2006). *Calibrating Noise to Sensitivity in Private Data Analysis*. In Proceedings of the Third Theory of Cryptography Conference.

Dwork, C., y Roth, A. (2014). *The Algorithmic Foundations of Differential Privacy*. Foundations and Trends in Theoretical Computer Science, 9(3–4), 211–407.

Erlingsson, Ú., Pihur, V., y Korolova, A. (2014). *RAPPOR: Randomized Aggregatable Privacy-Preserving Ordinal Response*. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security.

España (2018). *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*. Boletín Oficial del Estado, número 294, de 6 de diciembre de 2018.

España (2021). *Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales*. Boletín Oficial del Estado, número 128, de 27 de mayo de 2021.

Ferguson, A. G. (2017). *The rise of big data policing: surveillance, race, and the future of law enforcement*. NYU Press.

Ferretti, L., Wymant, C., Kendall, M., Zhao, L., Nurtay, A., Abeler-Dörner, L., Parker, M., Bonsall, D. y Fraser, C. (2020). *Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. science*, 368(6491), eabb6936.

Fjeld, J., Achten, N., Hilligoss, H., Nagy, A., y Srikumar, M. (2020). *Principled artificial intelligence: Mapping consensus in ethical and rights-based approaches to principles for AI*. Berkman Klein Center Research Publication, (2020-1).

Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Robert Madelin, R., Pagallo, U., Rossi, F., Schafer; B., Valcke, P. y Vayena, E. (2018). *AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations*. Minds and Machines, 28(4), 689-707.

Fussey, P., y Murray, D. (2019). Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology. University of Essex Human Rights Centre.

Gentry, C. (2009). *A fully homomorphic encryption scheme*. Stanford University. https://crypto.stanford.edu/craig/craig-thesis.pdf

Joh, E. E. (2017). *Artificial intelligence and policing: First questions*. Seattle UL Rev., 41, 1139.

Jordan, M. I., y Mitchell, T. M. (2015). Machine learning: Trends, perspectives, and prospects. Science, 349(6245), 255-260.

Konečný, J., McMahan, H. B., Yu, F. X., Richtárik, P., Suresh, A. T., y Bacon, D. (2016). *Federated Learning: Strategies for Improving Communication Efficiency*. arXiv preprint arXiv:1610.05492.

Levy, K., y Schneier, B. (2020). *Privacy threats in intimate relationships*. Journal of Cybersecurity, 6(1), tyaa006.

Lindell, Y. (2005). *Secure multiparty computation for privacy preserving data mining. In Encyclopedia of Data Warehousing and Mining* (pp. 1005-1009). IGI global.

Machanavajjhala, A., Kifer, D., Gehrke, J., y Venkitasubramaniam, M. (2007). *l-diversity: Privacy beyond k-anonymity*. ACM Transactions on Knowledge Discovery from Data (TKDD), 1(1), 3-es.

Mayer-Schönberger, V., y Cukier, K. (2013). *Big Data: A revolution that will transform how we live, work, and think*. Eamon Dolan/Houghton Mifflin Harcourt.

Mittelstadt, B., Allo, P., Taddeo, M., Wachter, S., y Floridi, L. (2016). *The ethics of algorithms: Mapping the debate*. Big Data y Society.

Narayanan, A., y Shmatikov, V. (2010). *De-anonymizing social networks*. In 2009 30th IEEE Symposium on Security and Privacy (pp. 173-187). IEEE.

Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

Obar, J. A., y Oeldorf-Hirsch, A. (2018). *The biggest lie on the Internet: Ignoring the privacy policies and terms of service policies of social networking services*. Information, Communication y Society, 23(1), 128-147.

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press.

Richards, N. M., y King, J. H. (2014). *Big Data Ethics*. Wake Forest Law Review, 49, 393–432.

Roman, R., Zhou, J., y Lopez, J. (2013). *On the features and challenges of security and privacy in distributed internet of things*. Computer Networks, 57(10), 2266-2279.

Sicari, S., Rizzardi, A., Grieco, L. A., y Coen-Porisini, A. (2015). *Security, privacy and trust in Internet of Things: The road ahead*. Computer Networks, 76, 146-164.

Solove, D.J. (2002). *Conceptualizing Privacy*. California Law Review, 90(4), 1087-1155.

Solove, D. J. (2008). *Understanding Privacy*. Harvard University Press.

Solove, D. J. (2013). *Privacy self-management and the consent dilemma*. Harvard Law Review, 126, 1880.

Sweeney, L. (2002). *k-anonymity: A model for protecting privacy*. International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 10(05), 557-570.

Tene, O., y Polonetsky, J. (2012). *Big data for all: Privacy and user control in the age of analytics*. Nw. J. Tech. y Intell. Prop., 11, 239.

Thompson, A., Stringfellow, L., Maclean, M., y Nazzal, A. (2021). *Ethical considerations and challenges for using digital ethnography to research vulnerable populations*. Journal of Business Research, 124, 676-683.

Yang, Q., Liu, Y., Chen, T., y Tong, Y. (2019). *Federated machine learning: Concept and applications*. ACM Transactions on Intelligent Systems and Technology (TIST), 10(2), 1-19. https://doi.org/10.1145/3284422

Ziegeldorf, J. H., Morchon, O. G., y Wehrle, K. (2014). *Privacy in the Internet of Things: threats and challenges*. Security and Communication Networks, 7(12), 2728-2742.

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.