Tipo de artículo: Artículo de revisión

El lado oscuro del Big Data como un problema social

The dark side of Big Data as a social problem

Mario González Arencibia[1*], https://orcid.org/0000-0001-9947-7762

[1] Centro de Estudios de Gestión de Proyectos y Toma de Decisiones, Universidad de las Ciencias Informáticas. Habana, Cuba. Correo electrónico: mgarencibia@uci.cu

*** Autor para correspondencia: mgarencibia@uci.cu**

Resumen

El lado oscuro del Big Data representa un problema social que cuestiona la ética en el uso de datos personales a gran escala. El objetivo es investigar el lado oscuro del Big Data como un problema social que afecta la privacidad, la soberanía nacional, la seguridad, los derechos de gobiernos, empresas, ciudadanos, la economía y la política global en su conjunto. La metodología se identifica con el paradigma de investigación cualitativa, basada en el análisis documental, que implicó el análisis de 70 documentos y 38 casos asociados al uso indebido del Big Data por parte de empresas y gobiernos. Los hallazgos relevantes incluyen la violación de datos personales, la discriminación y el sesgo en los algoritmos de inteligencia artificial, así como la influencia en la opinión pública en campañas políticas: Si los datos personales no son manejados con cuidado, pueden ser robados o utilizados de manera inapropiada, lo que puede llevar a la pérdida de la privacidad y la seguridad de los individuos. Por otro lado, los algoritmos de Inteligencia Artificial se basan en datos para tomar decisiones y, si los datos utilizados para entrenarlos son sesgados, los resultados también pueden ser sesgados y discriminatorios. Se sostiene que la influencia en la opinión pública en campañas políticas es otro riesgo asociado con el uso indebido del Big Data: Las campañas políticas pueden utilizar los datos personales de los ciudadanos para personalizar los mensajes y la publicidad, lo que puede influir en la opinión pública y afectar los resultados de las elecciones. Las conclusiones sugieren la necesidad de una regulación rigurosa y ética del uso del Big Data, que proteja los derechos de los ciudadanos y fomente la innovación responsable.

Palabras clave: Big Data, ética, privacidad, regulación, seguridad.

Abstract

The dark side of Big Data represents a social problem that questions the ethics of using personal data on a large scale. The objective is to investigate the dark side of Big Data as a social problem that affects privacy, national sovereignty, security, the rights of governments, companies, citizens, the economy, and global politics as a whole. The methodology is identified with the qualitative research paradigm, based on documentary analysis, which involved the analysis of 70 documents and 38 cases associated with the misuse of Big Data by companies and governments. The relevant findings include the violation of personal data, discrimination and bias in artificial intelligence algorithms, as well as influence on public opinion in political campaigns: If personal data is not handled carefully, it can be stolen or used inappropriately, leading to the loss of privacy and security for individuals. On the other hand, artificial intelligence algorithms rely on data to make decisions, and if the data used to train them is biased, the results can also be biased and discriminatory. It is argued that the influence on public opinion in political campaigns is another risk associated with the misuse of Big Data: Political campaigns can use citizens' personal data to personalize messages and advertising, which can influence public opinion and affect election results. The conclusions suggest the need for rigorous and ethical regulation of Big Data use, which protects citizen's rights and fosters responsible innovation

Keywords: *Big Data, ethics, privacy, regulation, security. Keywords: Big Data, ethics, privacy, regulation, security.*

Recibido: 18/06/2023
Aceptado: 20/08/2023
En línea: 01/09/2023

Introducción

En la actualidad, el Big Data se ha convertido en una herramienta clave para empresas, gobiernos y organizaciones en todo el mundo, ya que permite el análisis de grandes cantidades de información para obtener conocimientos y tomar decisiones informadas. Sin embargo, el uso del Big Data también tiene un lado oscuro que es perjudicial para la sociedad y la soberanía nacional (Crawford, 2016). Por ejemplo, la tesis principal de Safiya Umoja Noble en su libro "Algorithms of Oppression: How Search Engines Reinforce Racism" es que los algoritmos de los motores de búsqueda en Internet pueden reproducir y amplificar los prejuicios y la discriminación racial en las sociedades contemporáneas.

Noble sostiene que los motores de búsqueda, al estar diseñados por seres humanos con prejuicios y estereotipos, reflejan y refuerzan esas concepciones erróneas al mostrar resultados sesgados y discriminatorios. Este autor argumenta que estas prácticas tienen consecuencias negativas para la democracia y la justicia social, ya que limitan el acceso a la información y restringen la participación de grupos marginados en el debate público. Su tesis central de Noble es que los algoritmos de los motores de búsqueda tienen una responsabilidad ética y social en la eliminación de los prejuicios y la discriminación racial en la sociedad.

De lo anterior se deriva, que el lado oscuro del Big Data se refiere a la manipulación o mal uso de grandes cantidades de datos para fines que son contraproducentes o dañinos para la sociedad. Esto incluye la discriminación, la exclusión, la vigilancia excesiva, el control social, la invasión de la privacidad, entre otros (Eubanks, 2018). Su uso dañino tiene implicaciones significativas en la soberanía nacional, ya que con su inadecuado empleo se logra la manipulación de la opinión pública y la interferencia en los procesos políticos y electorales de un país (Tufekci, 2018).

Hasta aquí la pregunta de investigación que sigue este examen es la siguiente: ¿Cómo afecta el uso dañino del Big Data a las organizaciones, los gobiernos, derechos humanos y civiles de las personas, y cuáles son las posibles soluciones para abordar este problema desde una perspectiva social? En esta línea, este artículo tiene como objetivo analizar el lado oscuro del Big Data como un problema social que afecta la privacidad, la soberanía nacional, la seguridad, los derechos de gobiernos, empresas, ciudadanos, la economía y la política global en su conjunto.

Por lo tanto, es importante abordar el lado oscuro del Big Data como un problema social que afecta la soberanía nacional porque su uso dañino tiene implicaciones significativas en la vida de las personas y en la sociedad en general. Este examen contribuye a prevenir el uso dañino de los datos; incluyendo la identificación de prácticas

discriminatorias o invasivas que están afectando a la sociedad en su conjunto. Por otro lado, este análisis permite promover la transparencia y la responsabilidad en el uso de los datos, lo que puede contribuir a la protección de los derechos humanos y civiles. Por ejemplo, el análisis del lado oscuro del Big Data ayuda a identificar patrones de vigilancia o control social que puedan estar limitando la libertad de expresión o afectando la privacidad de las personas.

Materiales **y métodos**

El examen que se presenta se realiza desde la metodología de la investigación cualitativa, enfocada en comprender los problemas sociales, que genera el uso indebido del Big Data. La selección de la muestra, se realiza de manera no aleatoria, basada en criterios específicos como la relevancia del tema, la disponibilidad de la información, La recopilación y análisis de datos, incluye la revisión de informes, libros y artículos, con una muestra de 70 documentos y 38 casos, cuyo análisis de datos permitió incluir la identificación de prácticas dañinas y tendencias que afectan a la sociedad y la soberanía nacional, en diferentes ámbitos sociales. Finalmente, la interpretación de los resultados permite la identificación de enfoques y tácticas factibles para hacer frente a los desafíos encontrados. Este examen facilitó la caracterización de patrones y tendencias en la literatura, así como la exploración de brechas o lagunas en la investigación que requieren una mayor atención en el futuro. En este sentido, los hallazgos y conclusiones del estudio son respaldados por la literatura existente sobre el tema. Es importante señalar que los casos presentados, aunque caracterizan la práctica del uso abusivo del Big Data en la sociedad norteamericana en general, no son exclusivos de Estados Unidos, sino que se han presentado en múltiples países también.

¿Qué es un problema social?

Metodológicamente resulta factible, comenzar este análisis situando, ¿qué se entiende como problema social? El concepto de problema social ha sido debatido por diversos autores en el campo de la sociología y la teoría social. Un problema social es una situación o fenómeno que afecta a un número significativo de personas y que es considerado indeseable o injusto por la sociedad en general. Y para su solución requiere una respuesta colectiva de la sociedad (Mooney, et al, 2017). Estos pueden ser causados por factores económicos, políticos, culturales o psicológicos, y tienen consecuencias negativas para la calidad de vida y el bienestar de las personas afectadas.

Según el sociólogo francés Émile Durkheim, los problemas sociales son situaciones que generan un desequilibrio entre las normas y valores de la sociedad y las condiciones materiales que la hacen posible, lo que provoca un conflicto de intereses entre diferentes grupos (Durkheim, 1982). El sociólogo estadounidense Robert Merton sostiene

que los problemas sociales se originan cuando hay una disfunción en las estructuras sociales que impide que se alcancen los objetivos previstos, produciendo una tensión entre las expectativas y la realidad (Merton, 1968).

Para la socióloga estadounidense Frances Fox Piven, los problemas sociales son situaciones que desafían la capacidad de la sociedad para mantener sus propias normas y valores, y que requieren una respuesta colectiva para su solución (Piven, 1971). El sociólogo alemán Niklas Luhmann define los problemas sociales como situaciones que desestabilizan el sistema social y ponen en riesgo su capacidad para mantener su propia complejidad y diferenciación (Luhmann, 1977).

En su libro "Modern Social Work Theory", Payne (2017) plantea que los problemas sociales son complejos y multidimensionales, y que requieren una comprensión profunda de los factores individuales, sociales y estructurales que los originan. Payne sostiene que los problemas sociales son el resultado de la interacción entre las personas y las estructuras sociales, y que para abordarlos de manera efectiva es necesario tener en cuenta tanto los factores individuales como los factores estructurales que los subyacen.

Mooney, Knox y Schacht (2017), plantean que la comprensión de los problemas sociales implica ir más allá de la mera identificación de los síntomas de los problemas y buscar las causas subyacentes que los originan. Los autores argumentan que la comprensión de los problemas sociales debe ser holística, tomando en cuenta no solo los aspectos individuales, sino también los contextos sociales y estructurales que los rodean. Por otro lado, sugieren que la comprensión de los problemas sociales debe ser crítica y reflexiva, cuestionando los supuestos y prejuicios que subyacen en las explicaciones comunes de los problemas. Esto implica examinar las diversas perspectivas y experiencias de las personas afectadas por los problemas sociales, y buscar soluciones que sean justas y equitativas para todos.

Ejemplos de problemas sociales incluyen la pobreza, la desigualdad de género, la discriminación racial, la violencia doméstica, la exclusión social, la falta de acceso a la educación o a la atención médica. En su libro "Sociology: A Global Perspective", Ferrante (2017) plantea una visión amplia y global de la sociología, enfatizando la importancia de entender los fenómenos sociales en un contexto histórico, cultural y geográfico más amplio.

Macionis y Plummer (2017) plantean una introducción global y rigurosa a la sociología, enfatizando la importancia del enfoque crítico y reflexivo en el análisis de los fenómenos sociales. Su obra es una invitación a comprender y analizar la sociedad en su complejidad y diversidad, y a buscar soluciones efectivas a los problemas sociales que enfrentamos como seres humanos. De esto se deriva la importancia de abordar los problemas sociales de manera efectiva, mediante políticas y programas que promuevan la justicia, la igualdad y el bienestar de las personas

afectadas. Esto requiere una comprensión profunda de las causas subyacentes de los problemas sociales y un compromiso para abordarlos de manera colaborativa y sostenible.

Del análisis realizado por los diversos autores presentados se deriva lo siguiente:

Los problemas sociales son situaciones complejas que surgen cuando hay un desequilibrio entre las normas y valores de la sociedad y las condiciones materiales que la hacen posible. Po otro lado, son el resultado de la interacción entre las personas y las estructuras sociales. Su comprensión debe ser crítica y reflexiva, cuestionando los supuestos y prejuicios que subyacen en las explicaciones comunes de los problemas. El examen que se realice de los problemas sociales debe ser holístico, tomando en cuenta no solo los aspectos individuales, sino también los contextos sociales y estructurales que los rodean; al ser fenómenos complejos y multidimensionales requieren un enfoque integral para su comprensión y solución. Por consiguiente, la solución de los problemas sociales requiere de un esfuerzo colectivo y comprometido por parte de toda la sociedad, mediante políticas y programas que promuevan la justicia, la igualdad y el bienestar de las personas afectadas.

Resultados y discusión

Problemas e impactos del uso dañino del Big Data

Existen numerosos ejemplos de desafíos e impactos del uso dañino del Big Data cuya, amplitud, impactos y relevancia para la sociedad, los hacen clasificar como un problema social. Por ejemplo:

1. Discriminación basada en algoritmos utilizados en la contratación laboral

La discriminación basada en algoritmos utilizados en la contratación laboral es un problema cada vez más preocupante, ya que estos algoritmos pueden estar sesgados y perpetuar la discriminación de género, raza o edad. Amazon: En 2018, se descubrió que el algoritmo utilizado por Amazon para seleccionar currículums vitae en su proceso de contratación estaba discriminando a las mujeres. El algoritmo había sido entrenado con datos históricos de contratación de Amazon, que incluían una mayoría de candidatos masculinos. Como resultado, el algoritmo aprendió a penalizar automáticamente los currículums vitae que incluían palabras o frases que se asociaban más con mujeres. Este caso fue reportado por el medio de comunicación (Reuters, 2018)

McDonald's: En 2019, la compañía de comida rápida fue demandada por discriminación al utilizar un algoritmo para contratar empleados en su sede en Estados Unidos. Según la demanda, el algoritmo favorecía a los candidatos masculinos en detrimento de las mujeres. La demanda alegó que el algoritmo se basaba en los datos históricos de contratación de la empresa, que habían sido sesgados a favor de los hombres (The Guardian, 2019). En el caso de Unilever: En 2016, la empresa de productos de consumo fue criticada por utilizar un algoritmo para seleccionar

candidatos en su proceso de contratación. La crítica se centró en que el algoritmo había sido entrenado con datos de candidatos exitosos en la empresa, que incluían una mayoría de hombres blancos. Como resultado, el algoritmo favorecía a estos candidatos en detrimento de otros (The Guardian, 2016).

La discriminación basada en algoritmos en la contratación laboral tiene un carácter dañino, ya que perpetua y amplifica la discriminación histórica y estructural que ya existe en la sociedad. Los algoritmos pueden estar diseñados para identificar características que podrían estar correlacionadas con el éxito laboral, pero que también están correlacionadas con características que históricamente han sido asociadas con la discriminación, como la edad, el género, la etnia, y la orientación sexual. Como resultado, los algoritmos pueden perpetuar y amplificar la discriminación hacia ciertos grupos, incluso sin que los empleadores sean conscientes de ello.

Los autores Kentaro Toyama y Nicki Kindersley, (2018) en su artículo "The Human Cost of Automated Hiring Practices", señalan que los algoritmos de contratación tienden a perpetuar la discriminación de género, raza y edad, destacando que esto tiene un impacto significativo en las personas afectadas. Los autores afirman que los algoritmos de contratación son especialmente perjudiciales para las mujeres, ya que los algoritmos pueden ser entrenados para identificar características que se consideran "masculinas", como la agresividad o la competencia, y excluir a mujeres que no se ajusten a estos estereotipos.

Además, los autores Cathy O'Neil y Kate Crawford, (2016) en su libro "Weapons of Math Destruction", argumentan que los algoritmos de contratación pueden perpetuar la discriminación racial y socioeconómica, ya que pueden estar diseñados para identificar características que históricamente han sido asociadas con la discriminación, como la educación y el historial de empleo. Los autores señalan que los algoritmos de contratación pueden excluir a personas que tienen habilidades y experiencia valiosas, pero que no se ajustan a los estereotipos que han sido históricamente asociados con el éxito laboral.

2. Violación de la privacidad

El uso ilegítimo del Big Data tiene consecuencias graves en cuanto a la privacidad de los usuarios. Cambridge Analytica: En 2018, se descubrió que la consultora política Cambridge Analytica había obtenido datos de millones de usuarios de Facebook sin su consentimiento. La compañía utilizó estos datos para crear perfiles psicológicos de los usuarios y dirigir publicidad política personalizada. El caso generó un gran escándalo y llevó a Facebook a cambiar sus políticas de privacidad (The Guardian, 2018).

Equifax: En 2017, la agencia de crédito Equifax sufrió una violación de seguridad masiva que afectó a más de 147 millones de personas. Los hackers obtuvieron información personal de los usuarios, incluyendo nombres, direcciones, números de seguridad social y fechas de nacimiento. La violación de seguridad llevó a una investigación del

Congreso de Estados Unidos y a una multa de $700 millones para Equifax (The New York Times. (2017). Yahoo: En 2016, Yahoo reveló que había sufrido una violación de seguridad que afectó a más de mil millones de cuentas de usuario. La violación de seguridad incluyó información personal de los usuarios, como nombres, direcciones de correo electrónico, números de teléfono y contraseñas. La violación de seguridad llevó a una investigación del Congreso de Estados Unidos y a una multa de $35 millones para Yahoo (BBC News, 2016).

Por otro lado, el informe de Privacy International (2018) titulado "Teach 'em to Phish: The Growing Sophistication of Malicious Phishing", destaca cómo la violación de la privacidad también puede ser llevada a cabo por actores maliciosos, como los hackers y los delincuentes cibernéticos, quienes utilizan la información personal de las víctimas para cometer fraude y otros delitos. En cuanto a las consecuencias negativas de la violación de la privacidad, el informe "Mass Surveillance: The Case Against", publicado por la organización Privacy International (2018), señala que la vigilancia masiva y la recopilación de datos pueden tener un impacto negativo en la libertad de expresión, la privacidad y otros derechos humanos, socavando la confianza en las instituciones gubernamentales y la democracia.

En relación al monitoreo de la navegación en línea, los autores Shoshana Zuboff (2019) y Privacy International (2018), en sus publicaciones, han puesto en evidencia cómo las empresas tecnológicas pueden utilizar el Big Data para recopilar información sobre los usuarios y crear perfiles detallados para la publicidad personalizada. En cuanto a la vigilancia en el lugar de trabajo, el informe de la Unión Americana de Libertades Civiles (ACLU) (2018) titulado "The Boss Is Watching: How Workplace Surveillance Is Changing American Life" alerta sobre la invasividad de la vigilancia en el lugar de trabajo y el impacto en la privacidad de los empleados.

Respecto al uso de datos de salud, el informe "Big Data and Health" de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) (2015) destaca la importancia de proteger la privacidad de los usuarios en el manejo de datos de salud, ya que son extremadamente sensibles y pueden tener implicaciones para la seguridad y el bienestar de las personas.

El informe de Privacy International (2019) sobre el uso de datos personales en aplicaciones móviles es preocupante y demuestra cómo las empresas están obteniendo y compartiendo datos personales de los usuarios sin su conocimiento o consentimiento. Según el informe, el 86% de las aplicaciones móviles analizadas compartían datos personales con terceros, y el 43% de estas aplicaciones no proporcionaban información clara sobre cómo se compartían estos datos. Esta práctica viola los derechos humanos, incluyendo el derecho a la privacidad y la protección de datos personales.

Como se señala en el Informe de la Relatora Especial sobre el derecho a la privacidad en la era digital, la recopilación y el uso de datos personales deben ser transparentes, legítimos y proporcionales, y deben estar sujetos a controles y salvaguardias adecuados para proteger los derechos humanos (United Nations General Assembly, 2019). El hecho de

que muchas aplicaciones móviles no proporcionen información clara sobre cómo se usan y comparten los datos personales de los usuarios es especialmente preocupante, ya que esto puede permitir que las empresas compartan estos datos con terceros para fines ilegítimos, como la publicidad personalizada o la manipulación de la opinión pública.

El resultado del análisis anterior es que la violación de la privacidad es un problema social que afecta a personas, instituciones y gobiernos, y tiene consecuencias negativas para los derechos humanos y civiles de las personas, así como para la soberanía de un país. La autora Shoshana Zuboff (2019), en su libro "The Age of Surveillance Capitalism", argumenta que la violación de la privacidad se ha convertido en una práctica común en la era digital, y que las empresas tecnológicas han creado un modelo de negocio basado en la recopilación masiva de datos personales. Este modelo de negocio, según la autora, ha dado lugar a una nueva forma de capitalismo que utiliza la información personal de las personas como materia prima para el beneficio económico, de esta manera el capitalismo de la vigilancia y control de la información, constituye un nuevo factor para la obtención de plusvalía.

3. Uso dañino del Big Data puede contribuir a la creciente desigualdad social de varias maneras

En relación a la discriminación algorítmica, la autora Cathy O'Neil (2016), en su libro "Weapons of Math Destruction", pone en evidencia cómo los algoritmos están sesgados en contra de ciertos grupos de personas, lo que profundizar la discriminación y la desigualdad social.Por otro lado, el informe "Digital Redlining, Access, and Privacy", publicado por la organización Upturn (2016), destaca cómo las empresas que utilizan Big Data para la publicidad personalizada pueden estar discriminando a ciertos grupos de personas.

En el artículo "Machine Bias: There's software used across the country to predict future criminals. And it's biased against blacks", los autores plantean que existen programas informáticos utilizados en todo el país para predecir el comportamiento criminal futuro de los acusados, y que estos programas están sesgados contra las personas de raza negra. Los autores presentan un análisis de los algoritmos de evaluación de riesgos utilizados en el sistema de justicia penal en los Estados Unidos y los datos sugieren que estos algoritmos están sesgados racialmente, lo que puede llevar a una mayor discriminación contra las personas de raza negra en el sistema de justicia penal. Los autores argumentan que estos algoritmos no deberían ser utilizados sin una evaluación y revisión rigurosa para garantizar que sean justos e imparciales para todos los acusados, independientemente de su raza.

Estos algoritmos contribuyen a la discriminación y la desigualdad social. Sesgo que puede llevar a decisiones injustas y al mismo tiempo, afectar la vida de las personas de manera significativa. En este sentido, el informe "Artificial Intelligence and Life in 2030" (2016), publicado por la Universidad de Stanford, destaca cómo la discriminación algorítmica tiene un impacto negativo en la capacidad de las personas para acceder a oportunidades laborales,

educativas y económicas. El informe señala que los algoritmos pueden perpetuar la discriminación y la desigualdad al utilizar información sesgada o incompleta para tomar decisiones.

4. Big Data utilizado para manipular procesos democráticos

La manipulación de la opinión pública y la elección de candidatos a través del uso ilegítimo del Big Data es un tema cada vez más relevante y preocupante en la política contemporánea. La publicidad personalizada y la propagación de noticias falsas pueden influir en la opinión pública y afectar negativamente a la calidad del debate democrático. Como señala Sunstein (2017), la propagación de información falsa y la polarización de la opinión pública socava la democracia al impedir la deliberación y el diálogo constructivo. Como argumentan Kirschner y Tufekci (2018), el uso ilegítimo del Big Data en la política reduce la confianza de los ciudadanos en las instituciones democráticas y aumentar la polarización política. Esto tiene un impacto negativo en la capacidad de las sociedades para resolver problemas importantes y tomar decisiones cruciales.

La manipulación del Big Data también constituye una amenaza para la soberanía nacional, especialmente en el contexto de las elecciones internacionales. Como señala Nye (2018), la interferencia extranjera en las elecciones debilita la democracia al socavar la confianza de los ciudadanos en su sistema político y aumentar la tensión entre los países. El hecho es que, el uso ilegítimo del Big Data en la manipulación de los procesos democráticos es un problema social importante que contribuye a la violación de la soberanía nacional y de los derechos humanos (Cadwalladr, et al, 2018, Rosenbach, 2018).

La manipulación de la opinión pública y la elección de candidatos a través del uso ilegítimo del Big Data tiene graves consecuencias en la capacidad de los ciudadanos para elegir a sus líderes democráticamente. También tiene un impacto negativo en la confianza de los ciudadanos en el proceso democrático en sí mismo. Si los ciudadanos sienten que el proceso electoral está siendo manipulado o que los resultados son injustos, pierden la confianza en sus líderes políticos y en el sistema político en general. Esto socava la estabilidad política y pone en riesgo la soberanía nacional.

Por otra parte, la publicidad personalizada y la propagación de noticias falsas persuade a los ciudadanos para que apoyen a un candidato o partido político, sin tener en cuenta las cuestiones importantes o las plataformas políticas, lo que compromete la calidad del debate democrático. En este sentido, las noticias falsas son diseñadas para desacreditar a los candidatos o partidos políticos y distorsionar la percepción pública de los problemas políticos.

Es importante tener en cuenta que la manipulación de la opinión pública y la elección de candidatos a través del uso ilegítimo del Big Data no es solo un problema en los procesos electorales nacionales, sino que también tiene un impacto en las elecciones internacionales y en las relaciones internacionales en general. Es fundamental que se establezcan regulaciones y controles rigurosos para garantizar que el uso del Big Data en la política y la democracia

sea justo y transparente. Como señala Mayer-Schönberger y Cukier (2013), es necesario desarrollar nuevas formas de regulación y gobernanza para abordar los desafíos éticos y políticos que plantea el Big Data en la política.

5. Capitalización y vigilancia de datos personales de usuarios

La capitalización y vigilancia de datos es un tema que ha sido abordado por diversos autores y expertos en el tema de privacidad y seguridad de datos. La capitalización se refiere a la recopilación, análisis y uso de datos personales por parte de empresas y organizaciones con el fin de obtener beneficios económicos o políticos. La capitalización de datos implica que las empresas recopilan grandes cantidades de datos personales de los usuarios y los utilizan para desarrollar productos, servicios o campañas publicitarias personalizadas.

La vigilancia de datos se refiere a la recolección y análisis de datos personales para monitorear el comportamiento de los usuarios y obtener información sobre sus hábitos, preferencias y opiniones. Por ejemplo, Shoshana Zuboff (2019), en su libro "The Age of Surveillance Capitalism", describe cómo las empresas utilizan la recopilación de datos para obtener ganancias económicas y políticas, y cómo esto puede tener consecuencias negativas para la privacidad y los derechos humanos de los usuarios. Las empresas que se dedican a la capitalización y vigilancia de datos incluyen a las grandes compañías tecnológicas como Google, Facebook y Amazon, así como a empresas especializadas en publicidad en línea y análisis de datos como Acxiom y Experian. Estas empresas utilizan técnicas de seguimiento en línea, como cookies y píxeles de seguimiento, para recopilar información sobre el comportamiento en línea de los usuarios. También utilizan técnicas de minería de datos para analizar los datos recopilados y crear perfiles detallados de los usuarios.

La capitalización y vigilancia de datos es un problema social importante, que tiene consecuencias negativas para la privacidad y los derechos humanos de los usuarios. Por ejemplo, la recolección de datos personales permite la discriminación en la publicidad, el empleo y el acceso a servicios básicos, lo que perpetúa las desigualdades sociales existentes. La vigilancia de datos es utilizada por gobiernos autoritarios para monitorear y reprimir la disidencia política y la libertad de expresión. Por su parte, la Comisión Europea (2018) ha reconocido que la recopilación y uso de datos personales plantea importantes desafíos en términos de privacidad y seguridad.

En su informe "La protección de los datos personales en la economía digital", la Comisión Europea destaca la necesidad de establecer regulaciones y controles rigurosos para garantizar que las empresas respeten los derechos humanos y protejan la privacidad y los datos personales de los usuarios. El informe "No Place to Hide" de Privacy International (2019) muestra cómo muchas empresas utilizan técnicas de seguimiento y minería de datos para recopilar información personal de los usuarios sin su conocimiento o consentimiento, lo que puede tener consecuencias negativas para la privacidad y los derechos humanos. En conclusión, la capitalización y vigilancia de

datos es un tema de gran importancia en la actualidad, ya que tiene consecuencias negativas para la privacidad y los derechos humanos de los usuarios.

6. Big Data para manipular y propagar información falsa

La propagación de información falsa y engañosa a través de medios tecnológicos como Cambridge Analytica, bots y trolls en redes sociales y deepfakes es un problema social grave que tiene consecuencias negativas para la democracia, la privacidad y los derechos humanos. Estas prácticas violan los derechos humanos y civiles de cualquier país, incluyendo la soberanía nacional. En el caso de Cambridge Analytica, la utilización de datos de Facebook para influir en las elecciones presidenciales de Estados Unidos en 2016 ha sido considerada como una amenaza a la integridad del proceso democrático y a la privacidad de los usuarios (Cadwalladr, 2018).

La manipulación psicológica y la propagación de información falsa a través de bots y trolls en redes sociales socava la confianza en las instituciones democráticas y fomentar la polarización política (Woolley, & Howard, 2016). La utilización de bots y trolls en redes sociales para difundir información falsa o engañosa también puede tener consecuencias negativas para la democracia y los derechos humanos. Estos programas informáticos son utilizados para influir en la opinión pública y crear una falsa sensación de apoyo o oposición a ciertas ideas o personas, lo que puede contribuir a la polarización y la desinformación (Bessi, & Ferrara, 2016).

En el caso de los deepfakes, la utilización de esta tecnología para manipular la imagen de personas tiene graves consecuencias para la privacidad y los derechos humanos. Los deepfakes son utilizados para difundir información falsa o engañosa y para socavar la confianza en las instituciones democráticas. Además, la utilización de deepfakes para difundir imágenes falsas de personas tiene consecuencias negativas para la privacidad y la reputación de las personas afectadas (Brundage, et al, 2018). Los ejemplos del Brexit y la pandemia de COVID-19 ilustran cómo el Big Data puede ser utilizado para manipular la información y difundir campañas de desinformación para influir en la opinión pública y en la toma de decisiones. Estas prácticas violan los derechos humanos y civiles al socavar la democracia y la libertad de expresión, y pueden tener consecuencias negativas para la salud y el bienestar de la población.

En el proceso del referéndum del Brexit en el Reino Unido en 2016, se informó que se utilizaron técnicas de manipulación psicológica y campañas de desinformación para influir en el resultado del referéndum (Cadwalladr, 2018). La utilización de información falsa o engañosa en las redes sociales y otros medios limita la confianza en las instituciones democráticas y fomenta la polarización política, lo que tiene consecuencias negativas para la estabilidad y la cohesión social. Durante la pandemia de COVID-19, se difundieron varias campañas de desinformación sobre la enfermedad y las vacunas (Kouzy, et al, 2020). La utilización de información falsa o engañosa tiene consecuencias

graves para la salud y el bienestar de la población, y obstaculiza la confianza en la ciencia y en las autoridades de salud. Además, la difusión de información falsa o engañosa contribuye a la propagación del virus y al agravamiento de la crisis sanitaria.

7. Inadecuado uso del Big Data también socava la transparencia y dificulta la rendición de cuentas

El inadecuado uso del Big Data socava la transparencia y dificultar la rendición de cuentas, lo que tiene consecuencias negativas para los derechos humanos y civiles, y para las relaciones con otros países. Por ejemplo, en cuanto a la opacidad de los algoritmos, Accenture, (2018) encontró que el 56% de las empresas que utilizan inteligencia artificial no explican cómo funcionan sus algoritmos. Esto puede llevar a decisiones injustas o perjudiciales sin que los individuos puedan impugnarlas o entender cómo se llegó a ellas.

En cuanto a la falta de transparencia de las empresas, un informe de la Comisión Europea encontró que solo el 25% de los usuarios de Internet confían en las empresas que recopilan y utilizan sus datos personales (Comisión Europea, 2017). Pew Research Center, (2016) mostró que el 70% de los usuarios de Internet cree que las empresas recopilan demasiada información sobre ellos Esto indica que la falta de transparencia y control sobre el uso de los datos personales puede socavar la confianza de los usuarios en las empresas y en las instituciones que deberían proteger sus datos.

En relación con las dificultades para la rendición de cuentas, Pega, (2017) demostró que el 70% de los consumidores cree que las empresas que utilizan inteligencia artificial deberían ser responsables de los resultados de sus algoritmos, Sin embargo, la opacidad de los algoritmos puede dificultar la rendición de cuentas y la responsabilidad, lo que puede afectar la justicia y la equidad.

El inadecuado uso del Big Data es un problema social porque puede afectar los derechos humanos y civiles, como el derecho a la privacidad y la protección de datos personales. Además, puede socavar la confianza en las instituciones democráticas y afectar las relaciones con otros países, especialmente en el ámbito de la privacidad y la seguridad de los datos. Parcialmente se puede concluir que, la falta de transparencia, las dificultades en la rendición de cuentas y la opacidad de los algoritmos tienen consecuencias negativas para la sociedad en diferentes ámbitos, como el socioeconómico, político y cultural. En el ámbito socio-económico, la opacidad de los algoritmos lleva a decisiones injustas o discriminatorias, lo que afecta la equidad y la justicia social. Un estudio de ProPublica descubrió que un algoritmo utilizado por el sistema de justicia de los Estados Unidos para predecir la reincidencia tenía una tasa de falsos positivos más alta para los afroamericanos que para los blancos (Angwin, et al, 2016). Esto indica que el uso de algoritmos opacos profundiza la discriminación y la desigualdad.

En el ámbito político, la falta de transparencia y rendición de cuentas socava la confianza en las instituciones democráticas y afecta la participación ciudadana. (Pew Research Center, 2016), detectó que el 67% de los estadounidenses cree que las instituciones políticas y económicas de su país no son transparentes. Otro ejemplo es, como un informe de Transparencia Internacional señaló que el 80% de los ciudadanos de América Latina y el Caribe cree que la corrupción es un problema grave en su país (Transparencia Internacional, 2019). Esto indica que la falta de transparencia y rendición de cuentas pone en crisis la confianza en las instituciones públicas y afecta la gobernanza democrática.

En el ámbito cultural, la opacidad de los algoritmos perpetua estereotipos y prejuicios. (Zeynep Tufekci, 2018), observó que los algoritmos de recomendación de videos de YouTube propagan contenidos extremistas y polarizados. Por su parte, Informe de Amnesty International (2018) indicó que el algoritmo de Twitter para recomendar cuentas a seguir tenía tendencias sexistas y raciales. Esto es señal que la opacidad de los algoritmos conduce a la discriminación y los prejuicios culturales.

8. Afectaciones que produce el uso dañino del Big Data en las relaciones entre países para la economía y el comercio global

El inadecuado uso del Big Data tiene consecuencias negativas para las relaciones con otros países en términos de privacidad y seguridad de los datos, afectando la confianza y las relaciones diplomáticas entre los países. Además, reproduce la discriminación y el sesgo cultural en la toma de decisiones automatizadas. Estudio realizado por la Universidad de Harvard (2014) evidenció que la recopilación de datos personales por parte del gobierno de los Estados Unidos y su uso para la vigilancia masiva afectó negativamente la confianza de los ciudadanos de otros países en la democracia estadounidense. Según The Guardian (2013), la Agencia de Seguridad Nacional de los Estados Unidos (NSA) utilizó el Big Data para vigilar a líderes mundiales y ciudadanos de otros países, lo que afectó negativamente las relaciones diplomáticas entre los Estados Unidos y otros países.

Dastin, (2018) mostró que el uso de algoritmos opacos en la toma de decisiones automatizadas incrementa la discriminación y el sesgo cultural. En este estudio se analizó el algoritmo utilizado por Amazon para seleccionar candidatos para puestos de trabajo y se descubrió que el algoritmo discriminaba a las mujeres. Esto indica que el uso dañino del Big Data afecta negativamente la equidad y la justicia social.

La falta de regulaciones y controles rigurosos en el uso del Big Data también afecta las relaciones comerciales entre países. Un estudio realizado por la Comisión Europea (2017), demostró que la falta de confianza de los ciudadanos europeos en la privacidad y seguridad de sus datos personales afectó negativamente el comercio electrónico en

Europa. Esto indica que la falta de regulaciones y controles en el uso del Big Data afecta negativamente la economía y el comercio.

El uso dañino del Big Data puede afectar negativamente la economía y el comercio global de varias maneras:

En primer lugar, puede generar una disminución de la confianza de los consumidores en las empresas que utilizan el Big Data de manera inadecuada. Si los consumidores no confían en la privacidad y seguridad de sus datos personales, es menos probable que realicen compras en línea o compartan información con las empresas. Esto afecta negativamente las ventas y el crecimiento de las empresas, lo que a su vez afecta la economía en general.

En segundo lugar, las empresas que tienen acceso a grandes cantidades de datos y tienen la capacidad de analizarlos y utilizarlos de manera efectiva tienen una ventaja competitiva sobre las empresas más pequeñas que no tienen acceso a la misma cantidad de datos. Esto indudablemente genera desigualdades en el mercado y afecta negativamente a las empresas más pequeñas, lo que a su vez afecta la economía en general.

En tercer lugar, la Comisión Europea (2017) enfatizó que la falta de confianza de los ciudadanos europeos en la privacidad y seguridad de sus datos personales afectó negativamente el comercio electrónico en Europa. Según este estudio, el 72% de los ciudadanos europeos expresó preocupación por la privacidad de sus datos personales en línea, y el 67% de ellos afirmó haber evitado proporcionar información personal en línea debido a estas preocupaciones. Esta falta de confianza en la privacidad y seguridad de los datos personales tiende a reducir el número de transacciones en línea realizadas por los consumidores europeos, lo que a su vez puede afectar negativamente el comercio electrónico en Europa. Además, esta falta de confianza afecta negativamente la competitividad de las empresas europeas que dependen del comercio electrónico para su crecimiento y éxito en los mercados internacionales (European Parliament, 2018).

En cuarto lugar, la falta de regulaciones y controles en el uso del Big Data afecta negativamente la competitividad de las empresas, al reducir la confianza de los consumidores en ellas. Un ejemplo de esto es el caso de la compañía de tecnología Equifax, que en 2017 sufrió una violación de datos que expuso información personal de más de 143 millones de consumidores estadounidenses. La compañía fue criticada por su respuesta lenta y poco efectiva a la violación de datos, y su falta de transparencia en el manejo de la información personal de los consumidores (The New York Times, 2017). Esta falta de transparencia y responsabilidad afectó negativamente la confianza de los consumidores en las empresas y reducir su disposición a compartir información personal en línea. Accenture (2019), enfatizó que el 41% de los consumidores estadounidenses no confiaba en las empresas para proteger su información personal en línea. Esto reduce la capacidad de las empresas para recopilar y utilizar datos de manera efectiva para mejorar sus productos y servicios y competir en el mercado.

Consecuentemente, la falta de regulaciones y controles en el uso del Big Data genera desigualdades entre las empresas. Las grandes empresas que tienen acceso a grandes cantidades de datos y tienen la capacidad de analizarlos y utilizarlos de manera efectiva tienen una ventaja competitiva sobre las empresas más pequeñas que no tienen acceso a la misma cantidad de datos. La consultora McKinsey & Company en 2018 observó que el 1% de las empresas que más utilizan el Big Data tienen un retorno sobre la inversión de hasta un 20% mayor que el promedio de las empresas. Esta desigualdad afecta negativamente la competitividad de las empresas más pequeñas y reduce la innovación y el crecimiento en el mercado.

El lado oscuro del Big Data tiene un impacto significativo en la economía global, ya que el manejo inadecuado del Big Data afecta la competitividad de las empresas, la inversión en tecnología y la innovación, así como la estabilidad financiera y los flujos comerciales. Algunos de los impactos específicos incluyen: ***a) Pérdida de confianza:*** el uso indebido del Big Data erosiona la confianza de los usuarios en las empresas y organizaciones que manejan el Big Data, lo que afecta su reputación y su capacidad para atraer clientes y socios comerciales; ***b) Competencia desleal:*** el uso dañino del Big Data puede dar a algunas empresas una ventaja competitiva injusta al permitirles obtener información sobre sus competidores o clientes que no están disponibles para otros actores en el mercado; ***c) Riesgo financiero:*** el manejo inadecuado del Big Data aumenta el riesgo financiero al permitir la filtración o el robo de información financiera confidencial, lo que tiene implicaciones negativas para la estabilidad financiera y los flujos comerciales.

9. ¿Qué posibles soluciones se pudieran manejar frente al uso dañino del Big Data como un problema social?

Existen diversas posibles soluciones para abordar el lado oscuro del uso indebido del Big Data desde una perspectiva social:

El ***fortalecimiento de la legislación:*** El Reglamento General de Protección de Datos de la Unión Europea (RGPD) es un ejemplo de una ley que establece reglas claras para el manejo de datos personales y establece sanciones significativas para las empresas que no cumplan con estas reglas. Desde su entrada en vigor en mayo de 2018, el RGPD ha tenido un impacto significativo en la forma en que las empresas y los gobiernos manejan los datos personales.

Según un informe de la Comisión Europea, el RGPD ha aumentado la conciencia sobre la privacidad de los datos y ha llevado a un mayor cumplimiento de las normas. Por ejemplo, en mayo de 2021, la Comisión Europea anunció una multa de 746 millones de euros contra Amazon por violaciones del RGPD relacionadas con el uso indebido de datos personales. En el Reino Unido, se han impuesto multas a empresas por un total de 42 millones de libras esterlinas desde la entrada en vigor del RGPD (Comisión Europea, 2019).

Además del RGPD, otros países y regiones han implementado leyes para proteger la privacidad de los datos personales. Por ejemplo, en los Estados Unidos, la Ley de Privacidad del Consumidor de California establece reglas para la recopilación, uso y divulgación de datos personales de los consumidores en California. En China, la Ley de Seguridad de la Información establece reglas para la recopilación, uso y divulgación de información personal y datos sensibles. Sin embargo, aún hay desafíos en la implementación efectiva de estas leyes: Las empresas presentan dificultades para cumplir con las normas debido a la falta de recursos o conocimientos técnicos. Existe todavía, falta de supervisión o sanciones efectivas para las empresas que violan las normas.

La ***transparencia y la responsabilidad:*** Estas ayudan a garantizar que las empresas y los gobiernos actúen de manera ética y responsable en el uso de los datos. En este sentido, podrían ser relevantes en la solución del problema planteado las siguientes medidas:

Las empresas pueden realizar auditorías de sus algoritmos de inteligencia artificial para identificar y abordar cualquier sesgo o discriminación en los resultados. Por ejemplo, en 2018, Amazon realizó una auditoría de su sistema de contratación basado en inteligencia artificial, después de descubrir, que estaba discriminando a las mujeres. La auditoría reveló que el sistema se había entrenado con datos sesgados y Amazon decidió dejar de usarlo (Dastin, 2018).

Las empresas pueden publicar informes de transparencia que detallen cómo utilizan los datos y cómo se toman las decisiones. Por ejemplo, Google publica informes anuales de transparencia que detallan la cantidad de solicitudes de información gubernamental que recibe y cómo responde a ellas (Sitio web de Google, 2023).

Los gobiernos pueden establecer organismos reguladores independientes para supervisar el uso del Big Data y garantizar que se cumplan las normas éticas y legales. Por ejemplo, la Autoridad de Protección de Datos de Irlanda es el organismo regulador encargado de hacer cumplir el RGPD en Irlanda (Autoridad de Protección de Datos de Irlanda, 2023).

La ***participación ciudadana:*** Al involucrar a los ciudadanos en estas decisiones, se puede garantizar que se tomen en cuenta sus preocupaciones y se promuevan los valores éticos en el uso del Big Data. El gobierno de Finlandia ha sido un líder en este campo, creando un grupo de trabajo de ciudadanos para asesorar sobre la ética y el uso responsable de la inteligencia artificial. Este grupo, llamado "Inteligencia Artificial participativa", está compuesto por ciudadanos seleccionados al azar que representan a diferentes sectores y regiones del país. El grupo se reúne regularmente para discutir temas relacionados con la ética y la responsabilidad del uso de la inteligencia artificial, y sus recomendaciones son consideradas por el gobierno finlandés en la toma de decisiones relacionadas con el uso de la inteligencia artificial.

La participación ciudadana en la toma de decisiones sobre el uso del Big Data también ha sido promovida por autores como Boyd, (2014), investigadora en el campo de los medios sociales y la tecnología. Esta autora ha argumentado la urgencia de involucrar a los ciudadanos en la toma de decisiones sobre el uso del Big Data, ya que esto puede ayudar a garantizar que se aborden las preocupaciones éticas y sociales relacionadas con el uso del Big Data.

La ***educación y la conciencia pública:*** Es un imperativo al educar al público sobre los riesgos asociados con el uso indebido del Big Data y fomentar una mayor conciencia sobre la importancia de la privacidad y la protección de datos personales. La educación y la conciencia pública son esenciales para abordar los riesgos del capitalismo de vigilancia porque permiten que los ciudadanos comprendan los riesgos asociados con el uso indebido del Big Data y tomen medidas para protegerse.

El capitalismo de vigilancia es un modelo económico en el que las empresas utilizan el Big Data para controlar y manipular a los consumidores (Zuboff, 2019). Las empresas recopilan enormes cantidades de datos sobre los usuarios y los utilizan para personalizar la publicidad, el contenido y los servicios en línea. Si bien este modelo económico puede ser rentable para las empresas, también plantea graves riesgos para la privacidad y la libertad de los consumidores.

La educación y la conciencia pública son esenciales para abordar los riesgos del capitalismo de vigilancia porque permiten que los ciudadanos comprendan cómo se utilizan sus datos y se sientan capacitados tomando medidas para protegerse. Por ejemplo, la educación sobre la privacidad en línea puede enseñar a los ciudadanos cómo ajustar las configuraciones de privacidad en las redes sociales y utilizar herramientas de privacidad en línea para proteger sus datos personales. Por consiguiente, la conciencia pública puede impulsar cambios en la regulación y la legislación para proteger la privacidad y la libertad de los consumidores. Si los ciudadanos comprenden los riesgos asociados con el capitalismo de vigilancia, pueden presionar a los legisladores para que promulguen leyes y regulaciones que protejan sus derechos de privacidad y libertad.

El resultado es, que los ciudadanos están en el deber de tomar medidas para proteger sus datos personales, así como, ajustar las configuraciones de privacidad en las redes sociales y utilizar herramientas de privacidad en línea. Por ejemplo, la Electronic Frontier Foundation es una organización sin fines de lucro que proporciona herramientas y recursos para ayudar a las personas a proteger su privacidad en línea.

Desarrollo de tecnologías éticas: Las tecnologías éticas son aquellas que se desarrollan con el propósito de abordar los riesgos asociados con el uso indebido del Big Data y promover un uso responsable de la tecnología. En general, las tecnologías éticas se centran en la promoción de prácticas justas, inclusivas y transparentes en el diseño, desarrollo y uso de la tecnología (O'Neil, 2016, Dwork, & Roth, 2014 y OCDE, 2018).

Un ejemplo de tecnología ética es el desarrollo de algoritmos de inteligencia artificial que sean más precisos y menos sesgados. Los algoritmos de inteligencia artificial a menudo se basan en datos históricos, lo que puede llevar a la reproducción de sesgos y prejuicios en los resultados. Los investigadores y las empresas están trabajando para desarrollar algoritmos de inteligencia artificial que sean más precisos y justos, utilizando técnicas como para propicia el aprendizaje y la eliminación de variables irrelevantes. Otro ejemplo de tecnología ética es la utilización de la criptografía y la privacidad diferencial para proteger la privacidad de los usuarios. La criptografía puede ser utilizada para proteger la privacidad de los datos personales, mientras que la privacidad diferencial puede ser implementada para proteger la privacidad de los datos estadísticos. Estas tecnologías pueden ser utilizadas en conjunto para proteger la privacidad de los usuarios sin comprometer la calidad de los datos.

Según un informe de la Organización para la Cooperación y el Desarrollo Económicos (OCDE), el desarrollo de tecnologías éticas contribuye a promover la innovación responsable y a proteger los derechos humanos. El informe de la OCDE señala que las tecnologías éticas pueden ayudar a garantizar que la tecnología se utilice para el bien común, en lugar de para fines perjudiciales [OCDE, 2018). Por lo tanto, los investigadores y las empresas pueden desarrollar tecnologías éticas que aborden los riesgos asociados con el uso indebido del Big Data, como algoritmos de inteligencia artificial que sean más precisos y menos sesgados. Según un informe de la Organización para la Cooperación y el Desarrollo Económicos (OCDE), el desarrollo de tecnologías éticas puede ayudar a promover la innovación responsable y a proteger los derechos humanos (OCDE, 2018).

Ejemplos de tecnologías éticas

Existen varios ejemplos concretos de tecnologías éticas que se han empleado en diferentes esferas y países y que han demostrado tener impactos positivos en la promoción de la privacidad, la justicia y la transparencia:

- Un ejemplo de tecnología ética es la herramienta "Fairness Indicators" de Google, que ayuda a los desarrolladores a evaluar y mitigar el sesgo en sus modelos de aprendizaje automático. Esta tecnología ha sido empleada en la esfera de la publicidad en línea para garantizar que los anuncios se muestren de manera justa e inclusiva. Según un estudio realizado por Google, el uso de Fairness Indicators ha ayudado a reducir el sesgo en los modelos de aprendizaje automático y mejorar la precisión y la calidad de los resultados (Google AI Blog, 2021).
- Otro ejemplo de tecnología ética es la plataforma de inteligencia artificial "Project Debater" de IBM, que utiliza técnicas de procesamiento del lenguaje natural para debatir con seres humanos sobre temas complejos. Esta tecnología ha sido empleada en debates públicos en países como Israel y Japón, y ha demostrado tener impactos positivos en la promoción del pensamiento crítico y la toma de decisiones informadas (IBM Research 2021).

- En la esfera de la privacidad, la tecnología de privacidad diferencial se ha utilizado en países como Estados Unidos y Suecia para proteger la privacidad de los datos estadísticos. Un estudio realizado por el Instituto Tecnológico de Massachusetts (MIT) (2019) demostró que la privacidad diferencial puede proteger la privacidad de los usuarios sin comprometer la calidad de los datos, lo que permite a los investigadores y las empresas utilizar los datos de manera más responsable y ética (Institute for Data, Systems, and Society at MIT, 2019).

Existe la preocupación sobre el impacto que han tenido los usos de las tecnologías éticas en la transparencia. En este sentido, un impacto positivo lo tiene la plataforma "OpenAI GPT-3", que utiliza métodos de aprendizaje automático para generar texto de manera autónoma. OpenAI ha desarrollado una política de transparencia, que incluye la publicación de detalles técnicos sobre la tecnología y la divulgación de cualquier uso potencialmente dañino de la misma. Además, OpenAI ha creado un panel de supervisión independiente para garantizar que la tecnología se utilice de manera responsable y ética (OpenAI, 2021).

Otro ejemplo de tecnología ética que promueve la transparencia es la plataforma "Data.gov", creada por el gobierno de los Estados Unidos para facilitar el acceso a los datos gubernamentales. La plataforma permite a los ciudadanos acceder a información sobre temas como la salud, la educación y el medio ambiente, lo que promueve la transparencia y la rendición de cuentas del gobierno (Data.gov., 2021).

Medidas para el uso responsable de las tecnologías éticas

En cuanto a la garantía de que las tecnologías éticas se utilicen de manera responsable, existen varias medidas que pueden tomar los desarrolladores, investigadores y usuarios: a) Los desarrolladores y los investigadores adoptarán prácticas éticas en el diseño y la implementación de la tecnología, como la evaluación de impacto ético y la inclusión de la diversidad en el equipo de desarrollo; b) Por otro lado, los desarrolladores y los investigadores, podrían, regular adecuadamente el uso de las tecnologías éticas para prevenir su uso indebido. Esto puede incluir la creación de leyes y regulaciones que promuevan prácticas éticas en el diseño y uso de la tecnología, así como la implementación de sistemas de monitoreo y evaluación para garantizar el cumplimiento de estas regulaciones; c) La realidad indica que los usuarios deben ser conscientes de los posibles riesgos y beneficios de la tecnología y tomar decisiones informadas sobre su uso.

Existen diversas estrategias para que los usuarios adquieran una mayor conciencia sobre el uso de la tecnología, planteadas por diferentes autores:

- Leer y estudiar la información disponible: esta estrategia ha sido enfatizada por autores como Luciano Floridi, (2010), argumenta que los usuarios deben ser conscientes de las implicaciones éticas y sociales de la tecnología para

tomar decisiones informadas sobre su uso. Organizaciones como la Electronic Frontier Foundation (EFF) (2021) han creado recursos educativos para ayudar a los usuarios a comprender la tecnología y sus implicaciones éticas y legales.

- Participar en grupos de discusión y comunidades en línea: esta estrategia ha sido promovida por organizaciones como la Asociación para el Progreso de la Inteligencia Artificial (AAAI), que ha organizado foros de discusión para fomentar el diálogo sobre temas éticos y sociales relacionados con la tecnología (Association for the Advancement of Artificial Intelligence, 2021). Autores como Cathy O'Neil (2016) han enfatizado la importancia de escuchar y considerar múltiples perspectivas para comprender los posibles impactos de la tecnología.
- Asistir a conferencias y eventos: esta estrategia ha sido promovida por organizaciones como la Asociación para la Maquinaria Computacional (ACM) (2021), que organiza conferencias y talleres sobre temas relacionados con la ética de la tecnología. Sherry Turkle (2015) ha argumentado que los eventos en vivo pueden proporcionar una oportunidad para reflexionar y discutir los impactos de la tecnología en la sociedad.

La garantía de que las tecnologías éticas se utilicen de manera responsable implica la necesidad de establecer medidas de regulación y supervisión para prevenir su uso indebido. Esto es importante debido a que, aunque las tecnologías éticas se desarrollan con el objetivo de promover la justicia, la transparencia y la privacidad, existe el riesgo de que se utilicen para fines discriminatorios o dañinos.

Para garantizar el uso responsable de las tecnologías éticas, se pueden establecer regulaciones que promuevan prácticas éticas en el diseño y uso de la tecnología. Estas regulaciones pueden incluir la evaluación de impacto ético, la inclusión de la diversidad en el equipo de desarrollo y la transparencia en la toma de decisiones. Además, se pueden implementar sistemas de monitoreo y evaluación para garantizar el cumplimiento de estas regulaciones y para detectar y corregir cualquier posible uso indebido de la tecnología.

Discusión

La discusión sobre el uso indebido del Big Data como un problema social es un tema que ha sido abordado por varios investigadores. En este debate se destaca lo siguiente:

La discriminación y exclusión que puede resultar del uso indebido del Big Data ha sido discutido por autores como Safiya Noble (2018), quien ha argumentado que los algoritmos de búsqueda pueden perpetuar la discriminación y la exclusión de ciertos grupos. Cathy O'Neil (2016), ha enfatizado la necesidad de abordar la falta de diversidad en la industria de la tecnología para prevenir la discriminación y la exclusión.

La falta de transparencia y responsabilidad en el manejo del Big Data ha sido discutida por autores como Danah Boyd (2014), quien ha argumentado que las empresas y organizaciones que manejan el Big Data deben ser más

transparentes sobre cómo se utiliza el Big Data (O'Neil, 2016). Kate Crawford, (2016) ha enfatizado la necesidad de evaluar el impacto ético de las tecnologías de inteligencia artificial para garantizar su uso responsable.

La amenaza a la privacidad y la seguridad que puede resultar del uso indebido del Big Data ha sido discutida por Shoshana Zuboff, (2019) quien ha argumentado que la vigilancia empresarial puede erosionar la privacidad y la autonomía individual. Bruce Schneier (2015) sostiene la necesidad de fortalecer la seguridad del Big Data para prevenir la filtración y el robo de datos.

El presente estudio tiene implicaciones teóricas, metodológicas y prácticas importantes para la investigación y el manejo del Big Data:

Implicaciones teóricas: el estudio destaca la importancia de abordar el uso indebido del Big Data como un problema social complejo que afecta a diferentes grupos y sectores de la sociedad. Este enfoque reconoce la necesidad de considerar las implicaciones sociales, éticas y legales del uso del Big Data y promueve la adopción de enfoques críticos y reflexivos en la investigación y el manejo del Big Data. En otro sentido, el estudio enfatiza la necesidad de desarrollar enfoques metodológicos y prácticas éticas para el manejo del Big Data que puedan prevenir su uso indebido y proteger los derechos y la privacidad de los usuarios. Esto implica la necesidad de establecer regulaciones claras y supervisión efectiva para garantizar que las empresas y organizaciones manejen el Big Data de manera responsable. Además, el estudio destaca la necesidad de evaluar el impacto ético de las tecnologías de inteligencia artificial para garantizar su uso responsable.

Finalmente se puede advertir, que el estudio tiene implicaciones prácticas importantes para el manejo del Big Data en diferentes sectores y contextos. Por ejemplo, las empresas y organizaciones que manejan el Big Data pueden utilizar los hallazgos de este estudio para desarrollar políticas y prácticas éticas en función del manejo del Big Data. Además, los usuarios pueden utilizar los hallazgos de este estudio para comprender mejor los riesgos y las implicaciones del uso del Big Data y tomar decisiones informadas sobre su uso.

Limitaciones: A pesar de los avances en la investigación sobre el uso indebido del Big Data, aún hay mucho por investigar en este campo. Por ejemplo, es necesario investigar más a fondo los impactos específicos del uso indebido del Big Data en diferentes grupos sociales, así como las implicaciones a largo plazo de este fenómeno para la sociedad. Por lo que, es necesario desarrollar enfoques metodológicos y prácticas éticas para el manejo del Big Data que puedan prevenir su uso indebido y proteger los derechos y la privacidad de los usuarios.

Conclusiones

La investigación sobre el lado oscuro del Big Data revela que el uso dañino del Big Data tiene implicaciones significativas para la privacidad de los usuarios. Esto se debe a que el Big Data permite la recopilación de grandes cantidades de información personal y sensible que es utilizada para fines no autorizados, como la segmentación de mercado y la publicidad dirigida. Además, el manejo inadecuado del Big Data también lleva a la discriminación y la exclusión de ciertos grupos sociales, como las minorías étnicas o las personas con discapacidad, al permitir la creación de perfiles basados en características personales.

La falta de transparencia y responsabilidad en el manejo del Big Data también tiene influencias significativas para la soberanía nacional y la seguridad. Esto se debe a que la recopilación y el manejo del Big Data pueden ser utilizados para la investigación y el espionaje de gobiernos y empresas, lo que tiene un impacto negativo para la seguridad nacional y la economía global.

La investigación ha destacado la amenaza a la privacidad y la seguridad de los usuarios debido al riesgo de filtración o robo de información personal y financiera confidencial. Esto tiene efectos negativos para los gobiernos, empresas y usuarios, incluyendo la pérdida de confianza y la exposición a riesgos financieros.

Por último, el examen ha enfatizado en la importancia de establecer regulaciones claras y supervisión efectiva para garantizar que las empresas y organizaciones manejen el Big Data de manera responsable y ética. La situación de uso indebido del Big Data, sugiere desarrollar enfoques teóricos, metodológicos y prácticas éticas para el manejo del Big Data que puedan prevenir su empleo malicioso y proteger los derechos y la privacidad de los usuarios.

Conflictos de intereses

No se poseen conflictos de intereses.

Contribución de los autores

1. Conceptualización: Mario González Arencibia.
2. Curación de datos: Mario González Arencibia.
3. Análisis formal: Mario González Arencibia.
4. Investigación: Mario González Arencibia.
5. Metodología: Mario González Arencibia.
6. Recursos: Mario González Arencibia.
7. Software: Mario González Arencibia.
8. Validación: Mario González Arencibia.

9. Visualización: Mario González Arencibia.
10. Redacción – borrador original: Mario González Arencibia.
11. Redacción – revisión y edición: Mario González Arencibia.

Financiamiento

La investigación no requirió fuente de financiamiento.

Referencias

Accenture. (2018). AI: Built to Scale. https://www.accenture.com/us-en/insights/artificial-intelligence/ai-built-to-scale.

Accenture. (2019). Global Consumer Pulse Research: Security. https://www.accenture.com/us-en/insights/security/consumer-pulse-research.

Amnesty International. (2018). Twitter's Toxic Algorithm. https://www.amnesty.org/en/latest/research/2018/04/twitter-toxic-algorithm/.

Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016). Machine Bias: There's software used across the country to predict future criminals. And it's biased against blacks. ProPublica. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

Artificial Intelligence and Life in 2030 (2016). One Hundred Year Study on Artificial Intelligence: Report of the 2015-2016 Study Panel, Stanford University, Stanford, CA, September 2016.

Association for Computing Machinery. (2021). Conferences. https://www.acm.org/conferences.

Association for the Advancement of Artificial Intelligence. (2021). AAAI Symposium on Ethics of Artificial Intelligence. https://www.aaai.org/Symposia/Spring/sss11.php.

Autoridad de Protección de Datos de Irlanda (2023). https://www.dataprotection.ie/.

BBC News. "Yahoo hit by Big gest data breach in history." (2016). https://www.bbc.com/news/technology-38301594.

Bessi, A., & Ferrara, E. (2016). Social bots distort the 2016 US Presidential election online discussion. First Monday, 21(11).

Boyd, d. (2014). It's Complicated: The Social Lives of Networked Teens. Yale University Press.

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B. & Scharre, P. (2018). The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. Oxford University Press.

Cadwalladr, C. (2018). The Cambridge Analytica Files. The Guardian. https://www.theguardian.com/news/series/cambridge-analytica-files.

Cadwalladr, C., & Graham-Harrison, E. (2018). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The Guardian. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

Comisión Europea. (2017). Special Eurobarometer 460: Data Protection. https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/special/surveyky/2178.

Comisión Europea. (2018). La protección de los datos personales en la economía digital. https://ec.europa.eu/info/sites/info/files/communication-data-protection-digital-world-201801_en.pdf

Comisión Europea. (2019). Informe de evaluación sobre el Reglamento General de Protección de Datos. https://ec.europa.eu/commission/presscorner/detail/es/ip_19_6008.

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

Dastin, J. (2018). Amazon scraps secret AI recruiting tool that showed bias against women. Reuters. https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G.

Data.gov. (2021). About. https://www.data.gov/about/.

Durkheim, E. (1982). The Rules of Sociological Method. Free Press.

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

Electronic Frontier Foundation. (2021). Surveillance Self-Defense. https://ssd.eff.org/.

Eubanks, V. (2018). Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor. St. Martin's Press.

Ferrante, J. (2017). Sociology: A Global Perspective. Cengage Learning.

Floridi, L. (2010). Information ethics: On the philosophical foundation of computer ethics. In Information technology and moral philosophy (pp. 33-65). Cambridge University Press.

Google AI Blog. (2021). Evaluating Fairness in Machine Learning with Fairness Indicators. https://ai.googleblog.com/2021/08/evaluating-fairness-in-machine-learning.html.

IBM Research. (2021.). Project Debater. https://www.research.ibm.com/artificial-intelligence/project-debater/

Institute for Data, Systems, and Society at MIT. (2019). Differential Privacy. https://idss.mit.edu/research/differential-privacy/.

Kirschner, S., & Tufekci, Z. (2018). Old politics needs new technology. Nature, 560(7720), 427-428.

Kouzy, R., Abi Jaoude, J., Kraitem, A., El Alam, M. B., Karam, B., Adib, E., & Zaraket, F. (2020). Coronavirus Goes Viral: Quantifying the COVID-19 Misinformation Epidemic on Twitter. Cureus, 12(3).

Luhmann, N. (1977). The Differentiation of Society. Columbia University Press.

Macionis, J. J., & Plummer, K. (2017). Sociology: A Global Introduction. Pearson.

Mayer-Schönberger, V., & Cukier, K. (2013). Big Data: A Revolution That Will Transform How We Live, Work, and Think. Houghton Mifflin Harcourt.

McKinsey & Company. (2018). Breaking away: The secrets to scaling analytics. https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/breaking-away-the-secrets-to-scaling-analytics.

Merton, R. K. (1968). Social Theory and Social Structure. Free Press.

Mooney, L. A., Knox, D., & Schacht, C. (2017). Understanding Social Problems. Cengage Learning.

Noble, S. U. (2018). Algorithms of Oppression: How Search Engines Reinforce Racism. NYU Press.

Nye Jr., J. S. (2018). The case for democratic geopolitics. Foreign Affairs, 97(1), 22-30.

OCDE (2018). Responsible Innovation in Action: Enabling Responsible Business Conduct in Emerging Technologies. OECD Publishing.

OCDE. (2018). Perspectivas de la OCDE sobre el desarrollo de la inteligencia artificial. https://www.oecd.org/going-digital/ai/ai-policy-observatory.htm.

O'Neil, C. (2016). Weapons of math destruction: How big data increases inequality and threatens democracy. Broadway Books.

OpenAI. (2021). Transparency & Safety. https://openai.com/about/transparency-safety/

Organización para la Cooperación y el Desarrollo Económicos. (2018). Responsible Innovation in Action: Enabling Responsible Business Conduct in Emerging Technologies. OECD Publishing.

Payne, M. (2017). Modern Social Work Theory. Oxford University Press.

Pega. (2017). The Future of AI in CX. https://www.pega.com/sites/default/files/whitepapers/future-of-artificial-intelligence-in-cx.pdf.

Pew Research Center. (2016). The State of Privacy in America. https://www.pewresearch.org/internet/2016/09/21/the-state-of-privacy-in-america/.

Piven, F. F., & Cloward, R. A. (1971). Regulating the Poor: The Functions of Public Welfare. Vintage Books.

Privacy International (2019). To hide: Exposing the sources of risks to your rights online. https://privacyinternational.org/report/2647/no-place-hide-exposing-sources-risks-your-rights-online.

Privacy International. (2018). Mass Surveillance: The Case Against. https://privacyinternational.org/advocacy-briefing/1742/mass-surveillance-case-against.

Privacy International. (2018). Teach 'em to Phish: The Growing Sophistication of Malicious Phishing. https://privacyinternational.org/advocacy-briefing/2015/04/teach-em-phish-growing-sophistication-malicious-phishing.

Privacy International. (2019). No place to hide: Exposing the sources of risks to your rights online. https://privacyinternational.org/report/2647/no-place-hide-exposing-sources-risks-your-rights-online.

Reuters. "Amazon scraps secret AI recruiting tool that showed bias against women." (2018). https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G.

Rosenbach, M. (2018). How the Trump campaign built an identity database and used Facebook ads to win the election. Harvard Business Review. https://hbr.org/2018/03/how-the-trump-campaign-built-an-identity-database-and-used-facebook-ads-to-win-the-election.

Schneier, B. (2015). Data and Goliath: The hidden battles to collect your data and control your world. WW Norton & Company.

Sitio web de Google, (2023). Específicamente su sección de Informes de Transparencia: https://transparencyreport.google.com/.

Sunstein, C. R. (2017). #Republic: Divided Democracy in the Age of Social Media. Princeton University Press. Kirschner, S., & Tufekci, Z. (2018). Old politics needs new technology. Nature, 560(7720), 427-428.

The Guardian. "McDonald's hit with #MeToo class action over sexual harassment." (2019). https://www.theguardian.com/business/2019/may/21/mcdonalds-hit-with-metoo-class-action-over-sexual-harassment.

The Guardian. "The Cambridge Analytica scandal, in 3 paragraphs." (2018). https://www.theguardian.com/news/2018/mar/21/the-cambridge-analytica-scandal-in-3-paragraphs

The Guardian. "Unilever's use of AI hiring tool condemned as 'fundamentally flawed'." (2016). https://www.theguardian.com/technology/2016/oct/13/unilevers-use-of-ai-hiring-tool-condemned-as-fundamentally-flawed.

The Leadership Conference on Civil and Human Rights & Upturn. (2016). Digital Redlining, Access, and Privacy: An Overview. https://www.civilrights.org/wp-content/uploads/2016/04/Digital-Redlining-and-Privacy-Report.pdf.

The New York Times. (2017). Equifax Says Cyberattack May Have Affected 143 Million in the U.S. https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html.

Toyama, K., & Kindersley, N. (2018). The Human Cost of Automated Hiring Practices. Communications of the ACM, 61(11), 34-36. doi: 10.1145/3272139.

Transparencia Internacional. (2019). Barómetro Global de la Corrupción: América Latina y el Caribe 2019. https://www.transparency.org/es/gcba2019/latin-america-and-the-caribbean

Tufekci, Z. (2018). Twitter and Tear Gas: The Power and Fragility of Networked Protest. Yale University Press.

Turkle, S. (2015). Reclaiming conversation: The power of talk in a digital age. Penguin.

United Nations General Assembly (2019). Report of the Special Rapporteur on the right to privacy. https://undocs.org/A/74/188.

Woolley, S. C., & Howard, P. N. (2016). Political Communication, Computational Propaganda, and Autonomous Agents—Introduction. International Journal of Communication, 10, 4882-4890.

Zeynep Tufekci. (2018). YouTube, the Great Radicalizer. The New York Times. https://www.nytimes.com/2018/03/10/opinion/sunday/youtube-politics-radical.html.

Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs.