UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS

FACULTAD DE NEGOCIOS

PROGRAMA ACADÉMICO DE ADMINISTRACIÓN DE EMPRESAS

La Privacidad en el uso de los datos en la ciencia de datos

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el título profesional de Licenciado en Administración de Empresas

AUTOR(ES)

Aravena Nina, Dilcia Kelly (0000-0002-4346-6631)

Tapia Quispe, Higuey Edson (0000-0001-9530-7774)

ASESOR

Alcántara Gavidia, Luis Alberto (0000-0001-8072-3476)

Lima, 15 de Agosto de 2022

DEDICATORIA

Este trabajo está dedicado a nuestros familiares por su apoyo incondicional y fortaleza para terminar con éxito nuestro artículo.

AGRADECIMIENTOS

A Dios por brindarnos la fortaleza y la sabiduría para concluir con el trabajo. Del mismo modo, agradecemos a la Universidad Peruana de Ciencias Aplicadas - UPC por brindarnos la formación académica y todos los recursos para desarrollar el artículo con éxito. También, agradecemos de manera especial a todos los autores que han aportado con sus posturas e investigaciones, haciendo posible el desarrollo de este trabajo de suficiencia profesional.

RESUMEN

La investigación tiene como propósito contrastar las posturas de los autores sobre quién es el responsable de la privacidad de los datos en la ciencia de datos, dado que no está clara, ya que permite identificar a los actores responsables que deben gestionar el uso de los datos, valorando el derecho a la privacidad que tienen las personas. El estudio es de enfoque cualitativo que busca analizar los argumentos de los autores, cuyo alcance académico de referencias consultadas corresponden a artículos científicos indexados a revistas de cuartiles 1 y 2.

Como resultado, se identifica que, cada vez más se usan los algoritmos para analizar grandes conjuntos de datos complejos con el fin de generar conocimientos a partir de los datos, como es: descubrir patrones de comportamientos, saber si alguien es contratado o promovido, si alguien accede a un préstamo o es provisto de vivienda, etc. (martín, 2019; Someh et al., 2019). Los hallazgos demuestran que la ciencia de datos puede afectar a las partes interesadas, estos son: los propietarios que contribuyen con sus datos, las empresas que usan *Big Data*, los constructores que desarrollan los algoritmos, las instituciones del Estado que regulan el uso de los datos y las sociedades que tienen la responsabilidad de gobernar, controlar y dar forma a este fenómeno sociotécnico cambiante, entre otros actores. Asimismo, la investigación establece una responsabilidad compartida entre el grupo de interés antes mencionado y todos aquellos que pueden verse afectado por el análisis de sus datos en la ciencia de datos.

Palabras clave: Privacidad de datos en la ciencia de datos; Responsabilidad de la privacidad de datos; Ética de datos; Ética en el desarrollo de los algoritmos; Ética de la investigación.

Privacy in the Use of Data in Data Science

ABSTRACT

The purpose of the research is to contrast the authors' positions on who is responsible for data privacy in data science, given that it is not clear, since it allows identifying the responsible actors who must manage the use of data, valuing the right to privacy that people have. The study has a qualitative approach that seeks to analyze the arguments of the authors, whose academic scope of consulted references correspond to scientific articles indexed in journals of quartiles 1 and 2.

As a result, it is identified that algorithms are increasingly used to analyze large complex data sets in order to generate knowledge from the data, such as: discovering behavior patterns, knowing if someone is hired or promoted, if someone accesses a loan or is provided with housing, etc. (Martin, 2019; Someh et al., 2019). The findings show that data science can affect the stakeholders, these are: the owners who contribute their data, the companies that use Big Data, the builders that develop the algorithms, the State institutions that regulate the use of data and the societies that have the responsibility to govern, control and shape this changing socio-technical phenomenon, among other actors. Likewise, the research establishes a shared responsibility between the aforementioned interest group and all those who may be affected by the analysis of their data in data science.

Keywords*:* Data privacy in data science; Responsibility for data privacy; data ethics; Ethics in the development of algorithms; Research ethics.

N°1078_La privacidad en el uso de los datos en la ciencia de datos

INFORME DE ORIGINALIDAD

7%	7%	2%	0%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	repositorioacademico.upc.edu.pe Fuente de Internet	2%
2	www.scielo.org.co Fuente de Internet	1%
3	www.itconsultors.com Fuente de Internet	1%
4	www.totalmateria.com Fuente de Internet	<1%
5	www.mold-tech.com Fuente de Internet	<1%
6	www.scielo.org.pe Fuente de Internet	<1%
7	www.informatica-juridica.com Fuente de Internet	<1%
8	idus.us.es Fuente de Internet	<1%
9	repository.udistrital.edu.co Fuente de Internet	

		<1 %
10	inba.info Fuente de Internet	<1 %
11	www.ironmountain.es Fuente de Internet	<1 %
12	Submitted to Harrisburg University of Science and Technology Trabajo del estudiante	<1 %
13	aisel.aisnet.org Fuente de Internet	<1 %
14	www.acambiode.com Fuente de Internet	<1 %
15	www.dykinson.com Fuente de Internet	<1 %
16	europa.eu Fuente de Internet	<1 %
17	revistaparadigma.online Fuente de Internet	<1 %
18	Jorge Alberto Álvarez Díaz, Eduardo Alfredo Duro, Ida Cristina Gubert, Carmen Alicia Cardozo de Martínez et al. "Entre Huxley y Orwell: Big Data y salud", Revista Latina de Sociología, 2018 Publicación	<1 %

19	www.criptonoticias.com Fuente de Internet	<1 %
20	www.oecd-ilibrary.org Fuente de Internet	<1 %
21	www.slideshare.net Fuente de Internet	<1 %
22	diposit.ub.edu Fuente de Internet	<1 %
23	repositorio.ucv.edu.pe Fuente de Internet	<1 %
24	oa.upm.es Fuente de Internet	<1 %
25	www.workday.com Fuente de Internet	<1 %
26	doku.pub Fuente de Internet	<1 %
27	prezi.com Fuente de Internet	<1 %
28	protecciondatos-lopd.com Fuente de Internet	<1 %
29	reader.digitalbooks.pro Fuente de Internet	<1 %

TABLA DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

Introducción

Con la creciente innovación en los tipos de dispositivos para la medición (sensores y satélites), el uso diario y personal de celulares móviles inteligentes (internet de las cosas, wearables, etc.), la interacción social en páginas webs (Twitter, blogs, WhatsApp, Facebook, etc.) y el registro de transacciones comerciales por medios digitales (pago con tarjeta de crédito, dinero móvil, transacciones electrónicas, etc.), todos ellos han generado la explosión de datos que se recopilan automáticamente en grandes volúmenes, a lo que se llama *Big Data* (Rathinam et al., 2021). Este análisis de volúmenes de datos utiliza algoritmos para analizar conjuntos de datos grandes y complejos con el fin de descubrir patrones de comportamiento, correlaciones y otros conocimientos a partir de los datos recabados (Someh et al., 2019), ya que, aún es muy limitada la literatura existente sobre la privacidad en el análisis de datos y sus implicaciones inherentes para los usuarios, organizaciones y grupos interesados (Nnamdi et al., 2022). Esta situación, ha generado en la actualidad importantes desafíos y cuestionamientos sobre quién es el responsable de la privacidad de los datos en las decisiones algorítmicas, ya que no está claro (Martín, 2019). Por ello, se plantea la siguiente pregunta, ¿Cuáles son las posturas acerca de quién es el responsable de la privacidad de los datos en la ciencia de datos?

Dar respuesta a esta pregunta, ha generado una controversia, ya que un grupo de autores consideran que (i) la responsabilidad de la privacidad recae en los propietarios de los datos, (ii) otros mencionan que recae en las empresas que gestionan esa información, también están aquellos que dicen que (iii) los constructores de los algoritmos son los responsables, incluso otros argumentan que (iv) la normativa es la que debe actuar como guía para el manejo de la privacidad, entre otras posturas menos mencionadas en los artículos revisados. Por ese

motivo, la presente investigación se desarrolla de manera selectiva, mediante la búsqueda de los artículos en bases de datos confiables y de prestigio, reconocidas a nivel internacional, como son: Web of Science, Scopus y Proquest, en los cuales se hicieron la búsqueda.

Los artículos que fueron consultados se hayan entre los años 2017 y 2022. La revisión bibliográfica fue orientado principalmente al área de la administración y negocios, multidisciplinario, aplicaciones informáticas y comunicaciones. Las palabras clave usadas para la búsqueda fueron: privacidad de datos en la ciencia de datos, ética de datos, ética en los algoritmos. A partir de la búsqueda fue necesario encontrar palabras claves adicionales como: privacidad y *Big Data*, responsabilidad de la privacidad de datos, uso responsable de los datos y ética de la investigación.

Todas las referencias consultadas corresponden a artículos científicos indexados a revistas internacionales con factor de impacto ubicado entre los cuartiles 1 y 2 de acuerdo a la consulta en la plataforma web de SCImago Journal Rank (SJR) y apoyados en la página web de Journal Citation Report (JCR). Entre las revistas más consultadas están: *Ethics and Information Technology, Journal of Business Ethics, Ethics and Information Technology, Journal of Service Management, Risk Management, Social Science Computer Review y Heliyon*. Todos los artículos fueron seleccionados de acuerdo con el objetivo de estudio y su relevancia para el desarrollo de la investigación, pues cada artículo tenía que confirmar o no la controversia, de esta forma contribuir y fortalecer más el estudio.

Posterior a la obtención de la información contenida en las referencias y los argumentos de los autores consultados, se planteó como objetivo general “contrastar las posturas de los autores sobre quién es el responsable de la privacidad de los datos en la ciencia de datos”, ya que permite identificar a los actores responsables que deben gestionar el uso de los datos, valorando el derecho a la privacidad que tienen las personas. En ese sentido, los objetivos

específicos de la investigación fueron: (i) evaluar las posturas sobre la responsabilidad de los propietarios en la privacidad de sus datos en la ciencia de datos, (ii) evaluar de qué manera la normativa en el uso de datos influye en la privacidad de datos en la ciencia de datos, (iii) evaluar las posturas sobre la responsabilidad de las empresas en la privacidad de los datos en la ciencia de datos, (iv) evaluar las posturas sobre la responsabilidad de los constructores que hacen el procesamiento en la privacidad de los datos en la ciencia de datos.

Al final de la presente investigación, también se considera necesario realizar nuevas investigaciones futuras para determinar si los estudios realizados desde 2017 hasta la actualidad, sobre la cual se sustenta este artículo de controversia, son suficientes para contestar a la pregunta de estudio, aún más considerando el entorno del análisis de *Big Data* que puede cambiar con los años. Asimismo, es importante realizar nuevas investigaciones para explorar en mayor profundidad sobre la responsabilidad que tiene cada uno de los actores, ya que en los artículos no se precisan las funciones que tienen ellos, ni los límites de sus responsabilidades, ni tampoco hay un consenso sobre lo que se entiende con análisis de datos, así también se requieren nuevas investigaciones futuras para probar si los hallazgos encontrados funcionan en las prácticas de ética de datos responsable.

Hay que precisar que la investigación se justifica por varios motivos, uno de ellos, en términos de conveniencia, ya que este estudio tiene valor académico para los interesados que buscan conocer quién es el responsable de la privacidad de los datos en las prácticas de ciencia de datos y, de esta manera, ampliar sus conocimientos. Además, la investigación puede ser usada como consulta para todos los actores analizados (los propietarios, las empresas, los constructores) y, en general, puede ser útil para todas las instituciones, Gobierno y la sociedad que quieran revisar un documento que reúne las diferentes posturas examinadas para un análisis propio de los interesados.

La investigación también tiene relevancia social, ya que los empresarios requieren comprender cómo sus prácticas de ciencia de datos pueden afectar o vulnerar en gran medida a la privacidad de los datos del grupo de interés (los clientes, usuarios, sociedad en general, otros), ya que todas las personas tienen el derecho de saber quiénes tendrán acceso a sus datos para poder cuestionar y reclamar cuando surjan problemas éticos, logrando así una mejor experiencia y satisfacción en el uso de los datos, de esta manera se enmarca el alcance y proyección social.

En cuanto a sus implicancias prácticas, la presente investigación permite resolver un problema real que actualmente existe y que todavía no se ha podido resolver, se trata de conocer quién es el responsable de la privacidad en la ciencia de datos y las decisiones algorítmicas en el escenario de un mundo cada vez más digitalizado, en la cual la tecnología y la creciente innovación genera volúmenes de datos grandes y complejos que luego serán analizados utilizando algoritmos con el fin de descubrir patrones de comportamientos, correlaciones y otros conocimientos generados a partir de los datos de los individuos. Por tanto, es realmente trascendental conocer la responsabilidad que tiene cada uno de los actores en este estudio para afrontar todos los problemas éticos principalmente cuando se invade la privacidad o se hace una asociación algorítmica poco conveniente para el usuario (por ejemplo, cuando califica para un crédito bancario, cuando se buscan otorgar beneficios a personas con cierto tipo de perfil, etc.).

En este documento, se analiza los diferentes puntos de vista de los autores, agrupados en cuatro subtemas, cada uno de ellos explica la controversia. También, hay que precisar que dichos subtemas agrupan a las principales posturas que más se repiten en los artículos consultados. La primera controversia (o subtema) se relaciona con la necesidad de analizar el grado de responsabilidad que tienen los propietarios de los datos, la segunda se asocia con

la normativa como guía para el manejo de la privacidad en el uso de los datos, la tercera enfocada en las empresas como responsables de la privacidad de datos en los algoritmos y, en cuarto lugar, se presentan a los constructores de los algoritmos como responsables de este derecho de la privacidad, ya que son los que entienden mejor la lógica matemática en el análisis algorítmico frente a los gerentes y directivos de las empresas.

Método

La investigación se basa en el enfoque cualitativo, dado que "se enfoca en comprender los fenómenos, explorándolos desde la perspectiva de los participantes" (Hernández et al., 2014, p. 358), dado que permite profundizar en los puntos de vista de los estudios revisados por los autores, cuyo alcance académico de referencias consultadas corresponden a artículos científicos indexados a revistas que tienen un factor de impacto entre los cuartiles 1 y 2. Además, los artículos de los autores que sustentan esta investigación aplicaron diferentes métodos de estudio, como son: métodos exploratorios, análisis de casos, método Delphi, revisión sistemática de la literatura, método Gioia, entre otros que les permitía analizar el enfoque cualitativo. Con esta base, en este documento, se analizaron a las empresas que hacen uso de la tecnología de *Data Science* y *Big Data,* caracterizado por el uso constante de algoritmos y distintas formas de aprendizaje automático, así como las empresas que han adquirido *frameworks* y *clusters* dedicados al procesamiento y almacenamiento de datos, y herramientas de almacenamiento en la nube, siendo publicaciones de diferentes países desarrollados y subdesarrollados, tales como: Asia, África, Europa, América del Norte, América Latina y el Caribe.

Este documento aborda las posturas de los autores sobre la controversia de quién es el responsable de la privacidad de datos en la ciencia de datos, como consecuencia del uso de algoritmos para analizar los grandes volúmenes de datos (*Big Data*) y más complejos cada vez, con el fin de descubrir patrones de comportamientos, correlaciones y otros conocimientos a partir de los datos a analizar, encontrándose vacíos en cuanto a los verdaderos responsables de gestionar el riesgo para garantizar que estas actividades de análisis de datos no invadan la privacidad de las personas.

En la elaboración de este artículo, se ha trabajado cuatro matrices en un archivo Excel para ordenar, resumir y extraer la información más relevante de todos los artículos revisados:

Con respecto a la primera matriz (M-1), ahí se encuentra una lista de todas las referencias consultadas que fueron fundamentales para el desarrollo de este estudio, además de un sucinto resumen de cada documento, las posturas de cada autor, las ideas principales y la relevancia de cada artículo con relación al tema de investigación. También es preciso indicar que todas las referencias en esta matriz se colocaron según la relevancia alta, moderada, baja. Así también, se detallaron las posturas de cada autor, en la cual se puedo distinguir los cuatro subtemas.

Posteriormente, se elaboró la segunda matriz (M-2) que define a cada uno de los cuatro subtemas para comprenderlos mejor, tomando en consideración la información recabada de la primera matriz; dichos subtemas se encontraron como base de análisis en las referencias consultadas. También, se incluyen las justificaciones que sostienen la relevancia de la investigación; asimismo, en esta matriz, se definieron los objetivos específicos enfocadas a cada uno de los subtemas.

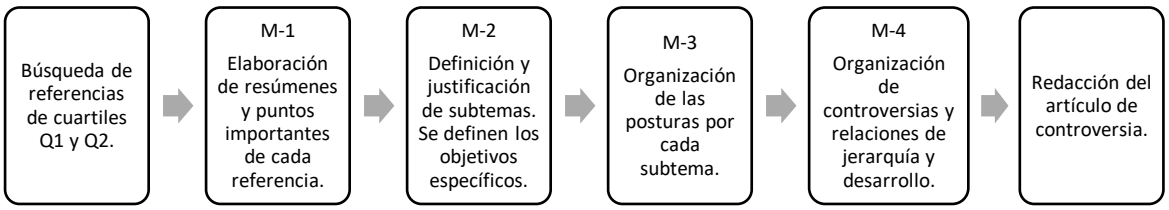
Luego, en la tercera matriz (M-3) se presentan los artículos agrupados por cada subtema, colocando en primer lugar al que se relaciona con los propietarios que generan los datos, luego la normativa que guía del derecho de la privacidad, seguido de las empresas que usan los algoritmos para analizar los datos de estas personas para tomar decisiones; por último, están los constructores que desarrollan los algoritmos guiados por su ética profesional. Sumado a ello, en esta matriz también se colocaron una síntesis de las posturas de cada autor con respecto a la controversia, manteniendo el orden de agrupación.

Finalmente, en la cuarta matriz (M-4), se realizan las relaciones de jerarquía por cada subtema y se precisan las controversias; además, se precisan las relaciones de comparación

entre las posturas de los autores, en la cual se indican las semejanzas y contraposiciones que cada autor defiende con argumentos y que luego servirán para el análisis con explicación más detallada en las relaciones de desarrollo. Esta matriz es muy importante, porque permite distinguir la controversia en la investigación, la misma que se analiza desde la óptica de varios autores, dando respuesta a la pregunta que se plantea en la investigación.

Figura 1

Método de investigación



Desarrollo

Los Propietarios de los Datos como Responsables de la Privacidad de los Datos en la Ciencia de Datos

En principio, se define a los propietarios como las personas o individuos quienes generan los datos que se usan en la ciencia de datos (Rathinam et al., 2021), es decir, son quienes hacen uso diario de celulares inteligentes, Internet de las Cosas, wearables, etc.; así como, interactúan constantemente con las redes sociales, blogs, etc. y realizan transacciones electrónicas comerciales con tarjeta de crédito, dinero móvil, etc.; todas estas transacciones del día a día del usuario han dado lugar a la explosión de los datos recopilados automáticamente que se usan en la ciencia de ciencia (Rathinam et al., 2021).

A partir de lo mencionado, se presenta la primera controversia relacionada con los propietarios como responsables de la privacidad de los datos. En ese sentido, esta controversia presenta dos puntos de vista para el análisis, el primer grupo de autores que plantea que los propietarios tienen la responsabilidad total de la privacidad de sus datos, mientras que el segundo grupo sostiene que los propietarios tienen, en realidad, la responsabilidad parcial de la privacidad de sus datos en la ciencia de datos.

En el siguiente apartado se precisan los detalles de estas posiciones.

Responsabilidad Total de los Propietarios en la Privacidad de sus Datos

La responsabilidad de la privacidad de los datos es un valor que estudia la Ética sobre la base de la moral y que está presente en la conciencia humana concebida como el derecho a la inviolabilidad de la personalidad y de controlar los datos sobre uno mismo (Mittelstadt, 2017). En ese sentido, la responsabilidad total de la privacidad de datos es, por tanto, la capacidad de aceptar y reconocer las consecuencias del derecho de la inviolabilidad de la

personalidad y de controlar los datos, mientras que la responsabilidad parcial de la privacidad de los datos se asocia con la responsabilidad de una parte del todo que representa el derecho a la inviolabilidad de la personalidad y de controlar los datos (Mittelstadt, 2017; RAE, 2022).

En ese sentido, los propietarios requieren comprender el nivel de responsabilidad que tienen ellos cuando otros individuos utilizan sus datos para prácticas de ciencia de datos creando conflictos en torno a la privacidad de los datos (Martín, 2019).

Al respecto, al hablar de responsabilidad total de los propietarios, Rathinam et al. (2021) argumentan que los propietarios deben tener conocimiento de la aplicación de sus datos y no deben dar su información detallada sin su conocimiento. Por ello, sugieren que el consentimiento informado debe estar completamente presente en el análisis de datos de las empresas, quienes deberían solicitar el permiso a los usuarios cuando realizan sus investigaciones. Además, los usuarios pueden tener la opción de activar y configurar sus propios perfiles, así como tener la capacidad de desarrollarlos y actualizarlos constantemente. Incluso cuando los datos se anonimizan, aun así, existen preocupaciones sobre el consentimiento y la ética que implica saber hasta qué punto se respeta la privacidad de las personas.

Entre los exponentes más importantes se encuentran Jayachandran et al., 2016, como se citó en Rathinam et al., 2021 quienes complementaron la idea de la privacidad de los datos, manifestando que los modelos de predicción de *Big Data* también generan estimaciones indirectas que el usuario puede desconocer cuando se obtienen resultados para efectos de políticas, programas de gobierno y monitoreo de indicadores de progreso del desarrollo, tales como: la riqueza, el desarrollo humano, la calidad de la infraestructura, la cubierta forestal y más. Otro autor relevante fue Hammer et al., 2017, como se citó en

Rathinam et al., 2021 quienes indicaron que la mayoría de los datos de *Big Data* se produce como un subproducto ocasionado por el sector privado y puede ser posible que, en el futuro no se pueda garantizar la sostenibilidad de los datos, ya que es probable que los datos públicos impliquen tener licencias para poder utilizarlos, por ende, el suministro de los datos de las personas o máquinas no está garantizada en el mercado que evoluciona y se comprometen los recursos y la privacidad.

El estudio de Rathinam et al. (2021) proporciona un mapa de revisión sistemática sobre *Big Data*. El 50% de las publicaciones fueron de Asia, el 30% de África subsahariana, 15% de América Latina y el Caribe, entre otras publicaciones. De ellos, alrededor del 70% son de países de ingresos bajos y medianos. Entre los hallazgos, los autores encontraron que la utilidad *Big Data* representa un potencial evidente para abordar temas de relevancia para el desarrollo internacional, así como son más relevantes para la sostenibilidad ambiental, el desarrollo urbano, el bienestar y la salud, el desarrollo económico y los medios de vida. Desde este punto de vista, los resultados también revelan la existen varios desafíos analíticos, éticos y logísticos que pueden dificultar el uso de macrodatos en las evaluaciones (calidad de datos, transparencia, intercambio de datos, privacidad, validez de construcción y generalización). Además, destaca el potencial de los grandes datos en contextos frágiles: como la propagación de enfermedades, la violencia, las calamidades naturales y los terrenos difíciles. Finalmente, el estudio concluye que es imperativo que los investigadores mejoren su información sobre la calidad, la ética y la transparencia de los datos para dirigir sus esfuerzos hacia la determinación de las mejores prácticas y estándares en materia de privacidad de datos y ética en general que facilite una mayor interacción entre los científicos de “teledetección” (detección a distancia de información que se realiza mediante satélites), los analistas de *Big Data* y los investigadores o evaluadores del desarrollo.

En la misma posición, Mittelstadt (2017) también argumenta que los individuos y los miembros del grupo deben dar su consentimiento ante los cambios de su identidad para ver si se acepta o no la clasificación algorítmica (al evaluar la aceptabilidad ética de las plataformas de análisis), sino se viola el derecho a la privacidad.

Entre los exponentes más importantes se encuentra Floridi, 2014, como se citó en Mittelstadt, 2017 quien indicaba que la clasificación algorítmica informa algo sobre los individuos a través de sus asociaciones con grupos *ad hoc* por ser personas supuestamente similares, estas personas pueden ser agrupados de acuerdo a sus comportamientos, preferencias y otras características sin ser identificados, estos métodos pueden resultar interesantes a los individuos solo cuando pueden correlacionarse con otros hacia un beneficio común, por ejemplo cuando califica para un crédito bancario, pero, dichas conexiones entre individuos también pueden revelar riesgos para las personas, por ejemplo, cuando se invade su privacidad o se hace una asociación poco conveniente para el usuario.

En relación con el estudio de Mittelstadt (2017), este abordó los sistemas analíticos que involucran la clasificación algorítmica o la agrupación de individuos en grupos *Ad hoc* para impulsar la toma de decisiones, la cual consiste en las clasificaciones y reglas construidas por un sistema de clasificación algorítmica, junto con predicciones de preferencias y comportamientos colectivos que no necesariamente se alinean con los atributos ya protegidos por la ley de privacidad. Entre los hallazgos, los autores encontraron que estos grupos *Ad hoc* construidos algorítmicamente también deberían tener sus intereses en la privacidad al administrar la identidad del grupo, por lo que es necesario centrar un derecho de privacidad en la integridad de la identidad compuesta (privacidad individual y grupal), ya que producen brechas. Los resultados también revela que la privacidad grupal es

un tercer interés a equilibrar junto con la privacidad individual con los beneficios de clasificación, ya que el derecho de un individuo, como el de un grupo están expuestos a ser violados cuando la identidad del propietario se elabora sin el consentimiento, ni la conciencia del individuo, ni del grupo; es por ello que los autores proponen la implementación de mecanismos para proteger los intereses de la privacidad de los grupos al margen de los intereses de cada miembro, esto como una forma de corregir el desequilibrio creado por el aumento de análisis de datos, por ende, proponen que los miembros del grupo deberían poder supervisar si se acepta o no la clasificación algorítmica.

Al igual que Mittelstadt, Ravn et al. (2020) también argumentan que antes de reproducir y representar el contenido de las personas se debe pedir el consentimiento al usuario para proponer un enfoque más considerado en las personas para reproducir y usar datos en dichas plataformas. En ese sentido, el autor considera que los datos disponibles públicamente en Instagram (por ejemplo, imágenes), no por ser públicos, pueden ser usados para tomar decisiones sin consentimiento de las personas.

Entre los exponentes más importantes se encuentran Boyd, 2016, como se citó en Ravn et al., 2020 quien complementó esta posición, cuestionando la lógica binaria que incorpora las plataformas como Facebook que piensan en la privacidad de los datos en términos técnicos simples, manifestando que "los datos están expuestos o no" (Ravn et al., 2020, p. 3), por lo que considera que la privacidad se trata más bien del sentido de control que deben tener los usuarios sobre qué tipo de datos se comparten con otros y bajo qué contexto, pero, dicho control se puede perder frente a los problemas o dilemas éticos dependiendo de cómo el usuario haya interpretado las nociones de privacidad, no aislados

solo a Facebook, sino que también son aplicables a todas las plataformas de redes sociales y al mismo usuario.

En el estudio de Ravn et al. (2020), este estudio de caso cuestionó la simple noción de "datos disponibles públicamente" en Instagram y explora las situaciones éticas en las redes sociales con respecto a los momentos familiares y que pueden estar presente en otras plataformas digitales como Facebook, al igual que otras plataformas, Instagram tiene configuraciones que permiten a los usuarios controlar su audiencia y, por lo tanto, decidir activamente lo que se coloca a disposición del público. Estos tipos de configuraciones se han desarrollado con el paso de los años para permitir a los usuarios tener más opciones de privacidad en el manejo de sus redes sociales. Entre los hallazgos, se encontró que dichas plataformas de redes sociales deben comprometerse con los principios de consentimiento, privacidad y propiedad. Así como descartar cualquier forma de consentimiento basado en simples nociones técnicos de que los datos están 'disponibles públicamente y, por lo tanto, de esta manera están siendo transparentes y justos con los usuarios en materia de privacidad, más aún cuando se habla de publicaciones que incluyen a niños. Por ello, los autores encontraron que los padres, así como los propietarios de los datos, deben asumir la responsabilidad del uso que se le dan a sus publicaciones en las plataformas de redes sociales, argumentando que estas empresas deben considerar más a los usuarios para pedir su consentimiento antes de reproducir y representar su contenido. En línea con esto, los autores sugieren pensar más en la relación socio-tecno-ético de las plataformas, es decir, aprovechar activamente las funciones integradas en las aplicaciones y plataformas, tales como mensajería directa, filtros y hashtags para respaldar el comportamiento más ético.

De manera similar, Arriagada et al. (2020) también argumentan que es importante que las personas estén enteradas del uso que les dan a sus datos, aún más complementan la idea mencionando que dichos datos tienen que estar protegidos incluso los datos "seudonimizados" (procedimiento de gestión de datos en la cual se reemplazan los campos de datos personales por un pseudónimo o identificador artificial dentro de un registro), estos también deben estar protegido por ser información personal, ya que pueden tener elementos de riesgos para la reidentificación, un ejemplo de ello, es una dirección IP, la cual puede actuar como un identificador de perfil y constituye, por lo tanto, una información personal.

Entre los exponentes más importantes se encuentran Seng Ah Lee, 2016, como se citó en Arriagada et al., 2020 quienes complementaron la idea de datos "seudonimizados", manifestando que, en la mayoría de los países occidentales, el uso de los datos personales es una violación de las normas de privacidad de datos, frente a esta situación, indican que los riesgos se "mantienen bajo control" (Arriagada et al., 2020, p. 15) mediante la anonimización de los datos o la utilización de nuevos datos agregados para evitar problemas de privacidad que afectan a sus propietarios, pero lo cierto es que estas afirmaciones tranquilizan erróneamente al público en relación a su derecho a la privacidad.

Continuando con el estudio de Arriagada et al. (2020), este abordó una revisión de la literatura que evalúa los imperativos éticos identificados en la pandemia de COVID-19 desde la perspectiva de la ética de los datos. Como hallazgo, los autores revelan las preocupaciones a nivel social preexistentes sobre los problemas éticos y sus implicancias en las empresas basadas en datos, incluida la privacidad, la vigilancia, la transparencia y la responsabilidad. Además, demuestra que los problemas actuales se han magnificado debido a la pandemia del COVID-19. Estos problemas éticos presentan dos áreas principales de desarrollo, uno relacionado con cuestiones de confianza y responsabilidad, así como la privacidad, manejo

de datos y transparencia; la otra área relacionada con temas de justicia, del trato justo, la discriminación y la desigualdad social. Bajo este escenario, la ética de los datos revela la necesidad de un papel normativo que aborde la necesidad de soluciones basadas en datos y la implementación de su uso alineado a la ética para el desarrollo de sociedades técnicas, inclusivas y pluralistas.

Luego de revisar los argumentos expuestos, se encuentra que los autores consultados que respaldan esta posición creen que los propietarios tienen la responsabilidad total de la privacidad de los datos en la ciencia de datos, ya que son ellos los que deben tener conocimiento total de la aplicación de sus datos, así como deben tener la capacidad de desarrollarlos y poder actualizarlos, configurando sus propios perfiles; en esa línea, no deben dar su información a nadie sin su conocimiento, haciendo valer su derecho de aceptar o no la clasificación algorítmica, sino se viola el derecho a su privacidad, incluso deben cuidar sus datos disponibles públicamente en Instagram, ya que, no por ser públicos, pueden ser usados en la clasificación algorítmica sin consentimiento de ellos, inclusive deben de cuidar sus datos "seudonimizados", ya que pueden tener elementos de riesgos para la re identificación.

Responsabilidad Parcial de los Propietarios en la Privacidad de sus Datos

Continuando con la controversia, en este apartado se discute la posición de los autores con respecto a su punto de vista de que los propietarios solo tienen una responsabilidad parcial en la privacidad de sus datos en la ciencia de datos, cuyo sustento se detalla en las siguientes líneas.

Al respecto, al hablar de responsabilidad parcial, Someh et al. (2019) defiende la idea de que los propietarios no tienen toda la responsabilidad de la privacidad de sus datos, a partir del cual argumentan que todas las partes interesadas son los que deben poder participar por igual en un discurso ético, cuestionar y reclamar cuando surgen problemas éticos y son las personas quienes deben poder controlar qué datos recopilan y agregan las organizaciones sobre ellos, así como deben saber quiénes tendrán acceso a sus datos, incluso deben poder hacer lo dicho después de haber dado su consentimiento a las organizaciones para que recopilen y compartan sus datos.

Entre sus exponentes más relevantes se encuentran Spiekermann y Korunovska, 2017, como se citó en Someh et al., 2019 quienes complementaron la idea mencionando que el poder de los algoritmos radica en generar nueva información, pero el enfoque tecnológico (volumen, variedad y velocidad) limita la comprensión de *Big Data* como un fenómeno sociotécnico que afecta a diferentes partes interesadas, identificando tres procesos sociales dirigidos a los individuos: (i) obtención de datos, (ii) intercambio de datos, (iii) toma de decisiones algorítmicas; este enfoque cuantifica la vida diaria de las personas para beneficiar a las organizaciones que realizan el análisis de los macrodatos. Otro de exponente importante fue Freeman, 1984, como se citó en Someh et al., 2019, quien explica que las partes interesadas puede ser cualquier grupo o individuo que puede afectar o verse afectado por el análisis de *Big Data*. En ese sentido, Markus y Topi, 2015, como se citó en Someh et al., 2019 identificaron tres grupos principales de partes interesadas en el análisis de *Big Data*, estos son: los individuos, las organizaciones y la sociedad.

En relación con el estudio de Someh et al. (2019), este estudio empleó el método Delphi para solicitar la opinión de expertos y el método Gioia para analizar el método cualitativo. Esta investigación utiliza la teoría de las partes interesadas para analizar cada

parte involucrada en el análisis de *Big Data* y revisa las cuestiones éticas desde las tres perspectivas de las partes interesadas (personas, organizaciones y sociedad). Estas partes interesadas incluyen individuos o propietarios que contribuyen con sus datos, organizaciones que usan *Big Data* y las sociedades que tienen la responsabilidad de gobernar, controlar y dar forma a este fenómeno sociotécnico cambiante. Entre los hallazgos, los autores encontraron que los individuos como las sociedades necesitan aumentar su importancia en las interacciones con las organizaciones, en ese caso, las personas deben participar activamente en el desarrollo de principios y lineamientos para asegurar que las sociedades establezcan regulaciones y leyes con sanciones efectivas cuando se vulneran los derechos de las personas sobre la privacidad de los datos. En ese sentido, el análisis de *Big Data* influye en la sociedad, pero, también es la sociedad misma quien puede controlarla y moldearla de una manera que beneficie a todas las partes interesadas y de una forma justa y equilibrada. Por ese motivo, el estudio propone basarse en la ética del discurso y la teoría de las partes interesadas para abordar los problemas éticos que surgen cuando las organizaciones recopilan, analizan, comparten o venden datos de individuos sin el consentimiento o conocimiento genuino de los individuos. De esta manera, sugiere formas de equilibrar las interacciones entre individuos, organizaciones y la sociedad para promover el uso ético del análisis de *Big Data*.

De manera similar, Legewie y Nassauer (2018) argumentan que los usuarios deben elegir la opción de participar o no en la investigación de videos en línea desde una perspectiva ética, pero su responsabilidad también es parcial, ya que es posible que estas personas no sean conscientes de que su comportamiento será analizado por los investigadores y, por lo tanto, no existe el consentimiento informado, por ejemplo, es posible

que las personas representadas en un video no sepan o no den su consentimiento para que se publique un video en línea en las plataformas para compartir videos (Instagram, YouTube, GeoCam, etc.).

Entre los exponentes más importantes se encuentran Gebel et al., 2015, como se citó en Legewie y Nassauer, 2018 quienes mencionaron que la privacidad corresponde a la información personal recopilada durante la investigación que no se vuelve pública ni accesible para las personas que no estaban destinadas y, este es el derecho a la privacidad que tienen todos los propietarios. Otro autor importante es Summer, 2006, como se citó en Legewie y Nassauer, 2018, quien complementó los argumentos de Gebel et al., al decir que, en la práctica esto significa que las personas deben saber que están siendo investigadas, por lo que deben recibir información relevante sobre la investigación planificada en un formato simple y comprensible para aceptar voluntariamente participar o negarse a hacerlo.

Continuando con la investigación de Legewie y Nassauer (2018), el foco de análisis estuvo dirigido al estudio de videos en línea en las plataformas como YouTube, LiveLeaks, Instagram, Facebook, entre otros, los cuales pueden ser publicados sin consentimiento de los usuarios. Como resultado de la investigación, se presentan cinco áreas (consentimiento informado, oportunidades analíticas, privacidad, transparencia y minimización de daños a los participantes) que ayudarán a los investigadores, lectores y revisores a identificar las características relevantes para la ética de la investigación y evaluar los desafíos, riesgos y beneficios, los cuales pueden servir como base para una discusión informada y transparente sobre temas éticos como la violación de la privacidad en la investigación. Otro hallazgo revela que los datos de video en línea serán accesibles como *Big Data* (conjuntos de datos masivos y complejos) se utilizará más ampliamente en los próximos años, posiblemente con la tecnología de *web scraping*, la minería de datos y el análisis de video automatizado, los

cuales permiten recolectar cada vez más datos en línea sobre un evento dado, permitiendo analizar la información tanto textuales como visuales y de forma automática. Los hallazgos también indicaron que, en la actualidad, es difícil lograr el anonimato porque *pixelar* caras y técnicas similares son todavía difíciles de implementar efectivamente, por ende, los autores consideran importante encontrar formas de hacer que los usuarios conozcan que están siendo investigados en las plataformas de internet y de diseñar mecanismos para darles una manera de optar por participar o no. De igual manera, estas opciones que se diseñen, no reemplazan el verdadero consentimiento informado y no libera a los investigadores de su responsabilidad de evaluar cuidadosamente su investigación desde una perspectiva ética, cuando los propietarios no son conscientes de que su comportamiento será analizado por los investigadores o porque los usuarios no tienen forma de marcar sus videos como prohibidos por el momento.

Luego de revisar los argumentos expuestos, se encontró que los autores consultados que respaldan esta posición creen que los propietarios no tienen toda la responsabilidad de la privacidad de sus datos, ya que la responsabilidad recae en todos los grupos interesados que deben poder participar por igual en un discurso ético, cuestionar y reclamar cuando surgen problemas éticos y, por lo tanto, la responsabilidad no es solo del propietario. Además, argumentan que la responsabilidad es parcial, porque las personas no son conscientes de que su comportamiento será analizado por los investigadores probablemente por desconocimiento sobre las implicancias ética de sus datos, de ahí que, no existiría el consentimiento informado. Tampoco es suficiente de que las personas brinden su consentimiento a las empresas para protegerse de los daños del análisis de *Big Data*, sino que las organizaciones también deben ser responsables de la privacidad de los datos, al

margen de la supervisión y control de los usuarios. Asimismo, dichas empresas deben gestionar el riesgo, ya que en la actualidad estas organizaciones no pueden proteger totalmente a las personas con solo cumplir con la ley de privacidad de datos.

Resumen Comparativo de la Controversia Relacionada con los Propietarios de los Datos como Responsable de la Privacidad de sus Datos

La primera controversia examinó el punto de vista de que los propietarios son los responsables de la privacidad de sus datos en la ciencia de datos. Al respecto, se presentaron dos posiciones, (i) quienes mencionaron que los propietarios tienen la responsabilidad total y (ii) quienes mencionaron que los propietarios tienen una responsabilidad parcial en la privacidad de sus datos en la ciencia de datos. En tal sentido, la mayoría de los autores consultados respaldaron la primera posición, indicando que los propietarios son los que tienen la responsabilidad total de la privacidad de sus datos. En ese sentido, se presenta un comparativo entre ambas posiciones (ver Tabla 1).

Tabla 1

Comparativo de la controversia relacionada con los propietarios como responsables de la privacidad de sus datos

Responsabilidad Total de los Propietarios de los Datos	Responsabilidad Parcial de los Propietarios de los Datos
Los propietarios son responsables de la privacidad de sus datos, por ende, deben tener conocimiento del uso que le dan a sus datos	Su responsabilidad no es total porque también está presente la responsabilidad de todas las partes interesadas
El consentimiento informado debe estar completamente presente en todo el análisis de datos para ver si aceptan o no la clasificación algorítmica	Además, porque estas personas no son conscientes de que su comportamiento será analizado por los investigadores
No deben dar su información detallada si no tienen conocimiento en qué se usará	En la situación de personas no conscientes, tampoco no existiría el consentimiento informado
Deben tener la opción de actualizar y configurar sus propios perfiles	Incluso, los propietarios deben poder controlar sus datos después de haber dado su consentimiento
Incluso, los datos "seudonimizados" deben estar protegidos por ser información personal, ya que pueden tener elementos de riesgos para la re identificación	Las empresas también deben gestionar el riesgo, ya que actualmente no pueden proteger a las personas con solo cumplir con las leyes de privacidad

Nota. Resumen comparativo de la responsabilidad de los propietarios en la privacidad de sus datos. Adaptado de Rathinam et al., 2021 (http://dx.doi.org/10.1002/cl2.1149); Mittelstadt, 2017 (http://dx.doi.org/10.1007/s13347-017-0253-7); Ravn et al., 2020 (http://dx.doi.org/10.1177/1556264619850736); Arriagada et al., 2020 (https://doi.org/10.4067/S0718-92732020000200013); Someh et al., 2019 (http://dx.doi.org/10.17705/1CAIS.04434); Legewie & Nassauer, 2018 (http://dx.doi.org/10.17169/fqs-19.3.3130).

La Normativa en el Uso de Datos como Guía de la Privacidad de los Datos en la Ciencia de Datos

Esta segunda controversia se relaciona con la idea de la normativa como guía para la privacidad de los datos en el uso de algoritmos. Con relación a eso, también se presentan dos perspectivas que discuten los autores, la primero relacionada con (i) la normativa en el uso de datos que genera un manejo eficaz de la privacidad de los datos en la ciencia de datos y, la segunda, relacionada con (ii) la normativa en el uso de los datos que es efectiva parcialmente como guía en la privacidad de los datos en la ciencia de datos.

En el siguiente apartado se precisan los detalles de esta postura.

La Normativa en el Uso de Datos es Efectiva como Guía en la Privacidad de Datos

Al hablar de un manejo eficaz, es cuando se consiguen los resultados esperados de manera satisfactoria independientemente de los recursos que se usan (Franzke et al., 2021). En ese sentido, un manejo eficaz en entorno a la privacidad de los datos es cuando se logra proteger y respetar el derecho de la privacidad de las personas de manera satisfactoria e independientemente de los recursos utilizados (Franzke et al., 2021; RAE, 2022).

En tal sentido, se requiere comprender si la responsabilidad de la privacidad de los datos depende de la normativa como guía eficaz de la privacidad de los datos en la ciencia de datos (Franzke et al., 2021).

Al respecto, al hablar de normativa también se hace referencia a las regulaciones, leyes y legislaciones sobre la privacidad de datos para el manejo eficaz. En ese sentido, Mühlhoff (2021) argumenta que una normativa “efectiva” en el análisis predictivo puede ser una guía muy eficaz para la administración de los desafíos éticos (relacionados con la privacidad), ya que actúa como guía hacia la puesta en práctica del pensamiento ético en implementaciones responsables de las empresas, permitiendo que la privacidad predictiva se

relacione con el principio ético fundamental de la dignidad humana. Estos hechos, otorgan al autor buenas razones para mencionar que las organizaciones deben abandonar completamente el uso del análisis predictivo, ya que los medios tecnológicos actualmente son bastante limitados para hacerlo éticamente viable.

Entre los exponentes más importantes se encuentran Zarsky, 2016, como se citó en Mühlhoff, 2021 quien mencionó que la protección de datos ha destacado que el análisis predictivo y desafía los marcos de privacidad contemporáneos, como el Reglamento General de Protección de Datos de la Unión Europea (GDPR), por ende, la protección de la privacidad predictiva requiere un debate ético y una regulación que debe actualizarse frente a los desafíos que se originan en el análisis de *Big Data*, ya que la privacidad predictiva puede impactar en la generación de nuevos enfoques para la regulación y la legislación. De hecho, una regulación más estricta de la tecnología *Big Data* es necesario, ya que los marcos existentes como el RGPD de la Unión Europea son insuficientes para prevenir los efectos tóxicos de los datos masivos anónimos.

Continuando con el estudio de Mühlhoff (2021), este abordó la evaluación ética de los sistemas predictivos a lo que llama "privacidad predictiva" y lo conceptualiza como principio ético que está siendo amenazada por el análisis predictivo. Se analizó el ciclo de procesamiento de datos de los sistemas predictivos para proporcionar una evaluación paso a paso de las implicaciones éticas, identificando las ocurrencias de violaciones de privacidad predictivas. Para el autor la privacidad predictiva, no se refiere a una violación que se comete al robar o filtrar información privada de alguien, sino deriva de una predicción sobre individuos o grupos de perfiles de datos que se recopilan de servicios digitales en internet. Entre los hallazgos, se demostró que la preservación de la privacidad predictiva no está garantizada actualmente por los marcos legales existentes de protección de datos y requiere

de una regulación efectiva y más estricta para prevenirlos, así como es necesaria una concepción colectivista de la privacidad, dado que la privacidad de las personas se viola al usar datos recopilados de otros individuos (puesto que se analiza en grupos), y son la sociedades democráticas los que deben definir si la tecnología se usa en absolutamente todo o no. Por ello, en línea con la normativa, la privacidad predictiva se encuentra entre los límites de la ética, la protección de datos y la antidiscriminación, ya que las personas son perjudicadas si son juzgadas por comparaciones de comportamiento con otros sobre hechos que no desearían revelar sobre ellos mismos, por lo que se necesita de manera urgente una conciencia ética de la privacidad predictiva como un valor fundamental y una condición previa para cualquier regulación exitosa. Asimismo, la evaluación ética de los sistemas predictivos determinó que las predicciones individuales ocasionan que los individuos están siendo juzgados por comparaciones de comportamiento, es decir, por las coincidencias de patrones con el resto de individuos dentro del grupo de sujetos, creando un sesgo injusto. Otro hallazgo fue, que el análisis predictivo desafía los principios éticos como la dignidad humana y la privacidad individual, por lo que sugiere abandonar el uso de dicho análisis, ya que los medios tecnológicos son bastante limitados para abordar los principios éticos (como la dignidad humana y la privacidad individual), dado que los individuos son despojados de su autonomía y dignidad.

De la misma manera, Franzke et al. (2021) argumentan que un marco regulatorio de ayuda para la toma de decisiones de ética de datos es un proceso útil para la evaluación ética de proyectos. Por esa razón, plantea un marco de ayuda para la toma de decisiones de ética de datos (DEDA), la cual es una herramienta eficaz y útil para la evaluación ética de proyectos de datos y para la creación de conciencia sobre cuestiones éticas en las prácticas

de datos como un proceso efectivo para moderar la identificación de casos no éticos y avanzar en el desarrollo de prácticas responsables en la ciencia de datos.

Entre los exponentes más importantes se encuentran Floridi y Taddeo, 2016, como se citó en Franzke et al., 2021 quienes afirmaron que la ética de los datos tiene tres ejes: (i) la ética de los datos, (ii) la ética de los algoritmos y (iii) la ética de las prácticas. Estos tres ejes pueden convergen en el desarrollo del marco DEDA al observar prácticas concretas en el contexto de proyectos municipales, ya que permiten examinar todo el ciclo de vida de los datos para saber cómo se usan, recopilan, almacenan y procesan, lo que incluye saber cómo se usan los algoritmos. Además, estos exponentes indicaron que la ética de los datos viene a ser una rama de la ética enfocada en estudiar los problemas morales asociados con (i) los datos, lo cual incluye: la generación, el registro, la conservación, el procesamiento, la difusión, el intercambio y el uso de los mismos; así como lo relacionado con (ii) los algoritmos que incluye la inteligencia artificial, el aprendizaje automático, los agentes artificiales y los robots; asimismo, en una siguiente instancia, se evalúan los problemas relacionados con (iii) las prácticas correspondientes con los algoritmos.

En esa línea, el estudio de Franzke et al. (2021) abordó una investigación cualitativa en el contexto gubernamental holandés. La muestra para la entrevista se conformó por ocho expertos del municipio de Utrecht como servidores públicos con experiencia profesional en el campo de la gestión basada en datos para los municipios de los Países Bajos y 137 encuestados para medir la efectividad del marco DEDA. La evaluación de la eficacia de dicho marco se desarrolló mediante varios talleres dirigidos a múltiples organizaciones, a saber, municipios, ministerios o la Dirección General de Servicios Públicos, organismos educativos y otros. Los resultados demostraron que las prácticas de datos están ganando relevancia, no solo en el campo del aprendizaje automático y la inteligencia artificial (IA),

sino también en la gobernanza pública, ya que cada vez más se implementan en los gobiernos locales, lo que potencialmente tiene un impacto ético significativo en la sociedad y los ciudadanos individuales. Como hallazgo, se ha demostrado que el marco DEDA se usa de manera efectiva en varios municipios y organizaciones educativas, ya que aumenta la conciencia ética de los datos, a diferencia de otras pautas. Dicho marco DEDA realmente propone no solo un conjunto de reglas estrictas y valores fundamentales, sino que comienza por hacer explícitos los valores que deben regir en la organización donde se desarrollan las prácticas de datos. Además, proporciona un proceso aplicable para adaptar el diseño, adherirse a los valores, documentar las decisiones de diseño e implementar cambios organizacionales para constituir prácticas éticas de datos centrados en la privacidad y responsabilidad.

Así también, Chen y Quan-Haase (2020) argumentan que las corporaciones, el gobierno y las instituciones deben manejar políticas y fuentes claras en torno a la ética de los datos para evitar las controversias en relación a la privacidad de datos.

Entre los exponentes más importantes se encuentra Reuters, 2018, como se citó en Chen y Quan-Haase, 2020 consideró que la ética y la política de los grandes datos requieren de nuevos conocimientos que abarque la recopilación de datos, conservación y el consentimiento informado, al igual que O'Neil, 2016, como se citó en Chen y Quan-Haase, 2020, quienes reforzaron esta idea, sosteniendo que los grandes datos todavía no han resuelto por completo los problemas como la objetividad, la precisión, la veracidad y la inclusión, más bien han introducido nuevos sesgos, subjetividades y formas de opresión; lo que demuestra la necesidad de incorporar nuevas políticas y conocimientos en el uso de datos. Otro exponente importante fue Popham et al., 2018, como se citó en Chen y Quan-Haase,

2020 quienes identificaron que los marcos regulatorios de las iniciativas de Big Data presentan cuatro preocupaciones: (i) ética de datos examinada de manera pública, (ii) marcos regulatorios, (iii) prácticas de consulta y alfabetización, (iv) y colaboración entre agencias, ya que es preocupación de las partes interesadas identificar la desinformación y deformación que genera el uso de *Big Data*, así como sus implicancias en los sesgos inherentes en el análisis de los datos que pueden excluir las necesidades de algunos ciudadanos, por ejemplo, los sesgos a los datos de las redes sociales pueden reflejar las necesidades y deseos de algunos grupos sociales de la población, pero pueden ocasionar que otros grupos sean invisibles en gran medida, lo que puede conducir a datos sesgados y, por lo tanto, a una prestación de servicios desigual.

A partir del estudio de Chen y Quan-Haase (2020), se analizaron en mayor profundidad a todos los actores principales tecnológicos, ya sea Facebook, Google, Apple o Uber e incluso van más allá del mundo corporativo, considerando gobiernos, municipios e instituciones educativas y de salud. El estudio se centró en la revisión de artículos de diferentes regiones del mundo (Estados Unidos, Canadá, India y China) donde usan los sitios de redes sociales: Facebook, LinkedIn, Twitter, Tumblr y Reddit. Entre los hallazgos, los autores encontraron controversias en torno a la política y la ética de los datos, encontrando que la capacidad de los académicos para investigar estos temas se ve obstaculizada debido a la falta de pautas que les guíe y de fuentes de datos sobre el manejo de *Big Data* en la práctica diaria, lo que podría ser proporcionado por parte de las corporaciones, el gobierno y las instituciones; en la práctica, eso ha generado un mayor uso del acuerdo de confidencialidad en más países a través de contratos legales diseñado para brindar protección de datos y privacidad corporativa centradas en los usuarios y sus necesidades de privacidad. Otro hallazgo fue, que los algoritmos sesgados pueden distorsionar la formulación de políticas urbanas, ya que los datos recopilados pueden violar el acuerdo de confidencialidad y las

respuestas políticas basadas en datos, incluida la aplicación de la ley, pueden ser preocupantes con respecto a los algoritmos, ya que carecen de conocimiento local, lo que pueden dar lugar a interpretaciones erróneas e intervenciones equivocadas en comunidades marginadas; por ende, los autores determinaron que los algoritmos que extraen datos de las redes sociales (de miembros de comunidades marginadas) rara vez integran el conocimiento local que ofrece una mejor interpretación y comprensión de los pobladores, habiéndose identificado la necesidad de desarrollar algoritmos culturalmente apropiados y socialmente sensibles para crear un conocimiento local que contemple a la comunidades marginadas.

En la misma línea, Parti y Szigeti (2021) sostienen que es importante desarrollar lineamientos y prácticas éticas, que tomen en cuenta las características del *Big Data*, así como es importante la colaboración interdisciplinaria para analizar, sintetizar y armonizar los vínculos entre disciplinas en un todo coordinado y coherente para trabajar juntos en equipos interdisciplinarios y mapear los obstáculos de la colaboración en torno a las decisiones éticas de datos.

Entre los exponentes más importantes se encuentran Toelch y Ostwald, 2018, como se citó en Parti y Szigeti, 2021 quienes mencionaron que existen muy pocos proyectos de investigación en los que la documentación y normas disponibles cubra todo, desde la idea hasta los datos sin procesar y los resultados; esta idea también lo sostuvieron Srnicek, 2017, como se citó en Parti y Szigeti, 2021 quienes comentaron que esto se debe la falta de regulaciones de privacidad de datos, de patentes pendientes y de una falta de conocimientos técnicos.

Continuando con el estudio de Parti y Szigeti (2021), esta investigación ha explorado en profundidad las ciencias de datos y las ciencias sociales para conformar los equipos

interdisciplinarios. La muestra estuvo conformada por 126 profesionales en la investigación de las ciencias sociales a nivel académico quienes completaron la encuesta. Además, se efectuaron 22 entrevistas a expertos en el campo de las ciencias sociales y de datos mediante muestreo intencional. Entre los hallazgos, los autores identificaron la necesidad de desarrollar lineamientos y prácticas éticas que tomen en cuenta las características del *Big Data* y de las redes sociales, así como los desafíos en la ética de datos. Asimismo, se identificaron problemas como: (i) la educación que está rezagada con respecto a los requisitos de la investigación en el campo digital, (ii) los equipos interdisciplinarios que necesitan de intérpretes para comprender las terminologías, (iii) los datos digitales que presentan problemas de validez, confiabilidad y desafíos éticos, y (iv) la falta de confianza académica que dificulta la ciencia abierta (la transparencia de la ciencia de datos, garantizar la reproducibilidad de los hallazgos, compartir y publicar datos, descripción de los métodos de estudio y la verificabilidad de los hallazgos). Estos hallazgos destacan la importancia de la apertura de los investigadores para establecer colaboraciones interdisciplinarias entre las ciencias sociales y la ciencia de datos para analizar, sintetizar y armonizar los vínculos entre disciplinas en un todo coordinado y coherente que identifiquen los obstáculos y trabajen juntos en ello.

Luego de revisar los argumentos expuestos, se encuentra que los autores consultados que respaldan esta posición creen que la normativa en el uso de datos genera un manejo eficaz de la privacidad de los datos en la ciencia de datos, ya que actúa como guía en la práctica responsable y ética en el manejo de los datos, relacionando la privacidad con el principio ético de la dignidad humana. Asimismo, argumentan que, si bien la normativa es efectiva en el uso de los datos, también indican que es insuficiente, siendo esto un obstáculo

debido a la falta de pautas que guíe a las corporaciones, el gobierno y las instituciones con respecto al manejo de los datos en la práctica diaria para evitar las controversias.

La Normativa en el Uso de Datos es Efectiva Parcialmente como Guía en la Privacidad de datos

Continuando con la controversia, en este apartado se discute la posición de los autores con respecto al punto de vista de que la normativa en el uso de los datos es efectiva parcialmente como guía en la privacidad de los datos en la ciencia de datos, cuyo sustento se detalla en las siguientes líneas.

Al respecto, al hablar de normativa, regulaciones y leyes como efectiva parcialmente en la privacidad de datos, Lang et al. (2021) sostienen que ciertamente se deben implementarse marcos de políticas para administrar las funciones de los portales que gestionan la información con respecto a la privacidad de datos, pero todavía no se han adoptado ampliamente para hablar de una efectividad completa, pese a que otros autores respaldan la opinión de que estos tipos de portales pueden ser muy útiles para compartir los datos en el campo de la salud. Bajo ese escenario, los autores determinaron cinco desafíos legales y éticos para el uso de los portales web en la atención clínica, a saber, privacidad y confidencialidad, capacitación, equidad, alfabetización y toma de decisiones.

Entre los exponentes más importantes se encuentran Melchart et al., 2016, como se citó en Lang et al., 2021, quienes informaron que se debe mantener el avance de la investigación de la salud, así como el tratamiento general de los problemas de privacidad y confidencialidad teniendo como centro al usuario frente a los problemas de ética de datos, especialmente cuando dicha información interactúa con herramientas habilitadas para

internet, por lo que exalta la importancia de la gobernanza del proyecto y los sólidos principios de protección de la privacidad de los datos.

En el estudio de Lang et al. (2021), se analizaron los casos de portales web que compartieron información de pacientes entre investigadores, médicos y el público. Entre los hallazgos sustentados en una revisión de la literatura, los autores encontraron que el desarrollo de los portales terapéuticos plantea una serie de cuestiones legales, éticas y sociales, incluidas las relacionadas con la privacidad y la confidencialidad, por lo tanto, se debe prestar especial atención a cada una de estas consideraciones mediante la implementación de marcos de políticas sólidas para administrar las funciones de los portales web. Como resultado, también se determinaron cinco desafíos legales y éticos para el uso de estos portales en la atención clínica: privacidad y confidencialidad, capacitación, equidad, alfabetización y toma de decisiones.

Al igual que el autor anterior, Markham et al. (2018) sostienen que las normas de la ética de la investigación y los marcos conceptuales del conocimiento algorítmico deben ajustarse para que sea efectiva y para definir y hacer operativa una ciencia de datos basada en la responsabilidad. Por ello, la posición de los autores es adoptar un marco metodológico de ética, ya que permite realizar discusiones productivas en todos los dominios, lo que implica que la ética de los datos pueda evaluarse desde el enfoque del agente moral que origina la acción (evaluación basada en la responsabilidad) o desde el enfoque del paciente (evaluación basada en los derechos).

Entre los exponentes más importantes se encuentran Metcalf et al., 2016, como se citó en Markham et al., 2018, quienes manifestaron que no existe un consenso fácil sobre si los métodos de investigación de *Big Data* deben ser excluidos o forzados a cumplir con las

normas existentes, por lo que también indicaron que las normas existentes deben efectuarse adaptándose a las circunstancias especiales de *Big Data* o complementándose con una nueva norma, de ser el caso. Otro autor relevante fue Buchanan, 2015, como se citó en Markham et al., 2018, quien sostuvo que los diseños tecnológicos tienen impactos negativos potenciales, debido a las actualizaciones extremadamente lentas de las pautas conceptuales y regulatorias.

Entre los hallazgos, los autores encontraron que los regímenes de ética estarán desajustados en la medida que las normas de ética de la investigación y los marcos conceptuales respondan a las condiciones de generación de conocimiento algorítmico y la investigación existente de *Big Data*. Además, los resultados arrojaron que la visualización de los datos tiene su propia política y amplios problemas éticos, muy a pesar de que el almacenamiento de datos y el intercambio de códigos en la ciencia de datos sean bien aceptados en la investigación social como una herramienta de mayor validez y confiabilidad, por eso, los autores sostuvieron que no todos los datos a recolectar se deben de hacer solo por ser válidos.

De manera similar, Forgó et al. (2020) argumentaron que los valores éticos como la privacidad deben complementarse con los requisitos y restricciones legales en la ciencia de datos para generar una confianza garantizada por parte de los usuarios y, de esta manera, resolver los problemas sociales que son el foco para la legitimidad de la ciencia de *Big Data*, así como también lo es el cumplimiento de los valores morales fundamentales para que las personas puedan depositar toda su confianza en la ciencia de datos y en las aplicaciones de la investigación de *Big Data*. En ese sentido, infieren que la normativa no es totalmente efectiva como guía en la privacidad de datos, porque los valores éticos no se complementan

con los requisitos y restricciones legales, más bien sostienen que el uso y la utilización de *Big Data* solo pueden utilizarse si se tratan adecuadamente los valores morales como: la confidencialidad, la privacidad, la exactitud, la transparencia, la autonomía, la equidad y la igualdad de acceso.

Entre los exponentes más importantes se encuentran Inkpen, et al., 2018, como se citó en Forgó et al., 2020 quienes introdujeron la información del controlador de datos como responsable de cualquier daño causado por el procesamiento ilegal y de velar para que el procesamiento de datos personales cumpla con las disposiciones de protección de datos y la normativa; el controlador de datos es la persona jurídica, agencia, autoridad pública o cualquier otro organismo que determinan los medios y los propósitos del procesamiento de datos. Asimismo, indicaron que el controlador será el responsable de demostrar el cumplimiento del principio de la privacidad desde el diseño y todo el desarrollo del análisis de datos.

En su investigación, Forgó et al. (2020) plantearon un marco de investigación que permiten una ciencia de datos éticamente sensible y legalmente compatible en Europa que puede replicarse por instituciones públicas y empresas privadas que tengan acceso a los datos sociales utilizados en procesos analíticos. Entre los hallazgos, los autores revelaron la importancia de complementar los requisitos y restricciones legales con un sólido entendimiento de los puntos de vista de la junta ética operativa con respecto a los valores éticos y los temas legales del procesamiento de los datos (como la privacidad y la protección de datos). Otro hallazgo estuvo enfocado en la investigación e innovación responsable y la aplicación del diseño sensible en el campo de los datos masivos, la cual fomenta el desarrollo de la ciencia y las herramientas que permitan a los usuarios hacer uso de las funcionalidades y capacidades para resolver los problemas, al mismo tiempo les permite respetar los derechos

fundamentales y los valores compartidos, como: la privacidad, la equidad, la seguridad, la igualdad, la autonomía, la dignidad humana; lo que es fundamental para lograr una confianza garantizada en la ciencia de datos y las aplicaciones de la investigación de *Big Data* por parte de los ciudadanos.

Al igual que Forgó et al., los autores Ibiricu y Marja (2020) también argumentaron que la legislación de protección de datos se debe alinear con un marco ético para que sea totalmente efectiva, integrando la ética en las primeras etapas del diseño de procesos y tecnologías, ya que puede garantizar que los empleados involucrados respeten el código de conducta; además, indican que las empresas son quienes deben desarrollar sistemas de valores y código de conducta para que el comportamiento ético se aplique en la tecnología. Por ese motivo, sostienen que la legislación y las normas son esenciales para proteger y respetar las normas éticas, los derechos humanos, la libertad y la privacidad. Al mismo tiempo, comentan que la tecnología, la ley y la ética deben coordinar para generar confianza en los individuos ante los problemas éticos.

Entre los exponentes más importantes se encuentran Renucci et al., 2016, como se citó en Ibiricu y Marja, 2020 quienes manifestaron que el aumento de datos, la velocidad y tecnología plantea la necesidad de gestionar los riesgos éticos y de equilibrar estas demandas con la ética de la normativa, así como de una mejor definición de responsabilidades y roles, nuevas leyes y conciencia ética, ya que, en muchos casos la relación entre la ética y la ley no está muy clara.

En la investigación de Ibiricu y Marja (2020) se abordaron el marco ético relacionado con la legislación de protección de datos de la Unión Europea (UE). Se analizaron las empresas tecnológicas de diferentes países: EE.UU. (Google, Microsoft, Amazon,

Facebook, IBM y Apple), China (Baidu, Alibaba y Tencent). Entre los hallazgos, los autores demostraron que un marco ético breve y fácil de comprender en la empresa debe estar alineado con la legislación de protección de datos de la Unión Europea (UE) para garantizar que los empleados involucrados en la ética de datos respeten el código de conducta integrado. En la investigación, el código de ética de datos ha planteado diez pasos secuenciales: (i) nombrar un patrocinador de alto nivel para promover una política de ética, (ii) tener respaldo del presidente y la junta general, (iii) comunicar al personal e identificar los temas éticos que requieran asesoramiento, (iv) generar participación y utilizar marcos que aborden los problemas éticos, (v) elaborar un código de conducta, (vi) experimentar y probar el código de ética, (vii) publicar el código de ética, (viii) promover el código de ética, (ix) proporcionar ejemplos prácticos del código e (x) implementar mecanismos de revisión. Los resultados también revelaron que establecer reglas claras para el comportamiento ético permite generar confianza y transparencia frente al incremento rápido de los dispositivos, la interconectividad, la velocidad de transmisión, la inteligencia y dependencia de la tecnología; por ese motivo, plantearon integrar la ética de los datos desde las primeras etapas del diseño de procesos y tecnologías en proyecto de datos.

También, Nersessian (2018) argumentaron que un marco de derechos humanos proporciona una guía clara y consistente cuando las leyes nacionales y los mecanismos de aplicación en un país en particular puede ser débiles o poco efectivas con respecto a las decisiones éticas en el contexto de *Big Data*. Por ello, consideraron que el uso de la ley de derechos humanos podría ayudar a las organizaciones a mantener el equilibrio correcto en cuestiones de macrodatos, ya que garantiza que ciertos valores importantes estén profundamente arraigados y, al menos, considerados en la recopilación de información, el

desarrollo de algoritmos, el procesamiento de datos y la interpretación de los resultados. Por ello, los autores sugieren que las corporaciones adopten políticas y procedimientos corporativos relacionados con lo humano en sus actividades comerciales de datos.

Entre los exponentes más importantes se encuentra Massad, 2010, como se citó en Nersessian, 2018, cuando manifestaron que la naturaleza propia a nivel global de los grandes datos dificulta la regulación efectiva a nivel nacional; además, muchas leyes y políticas nacionales están atrasadas incluso en las economías avanzadas, es por ello que Nersessian, 2015, como se citó en Nersessian, 2018 manifestó que los actores corporativos tienen que cumplir obligaciones legales para respetar los derechos humanos en sus actividades comerciales que incluyen actividades con Big Data.

En esa línea, el estudio de Nersessian (2018) abordó temas relacionados con el derecho internacional de los derechos humanos como restricción legal y ética sobre el uso comercial de *Big Data*. Entre los hallazgos, los autores encontraron que existe poco consenso internacional sobre los estándares que deben regir en el uso de la tecnología de *Big Data* que llenen el vacío con respecto a los derechos humanos, ya que una empresa que incorpora un marco de derechos humanos dentro de su sistema de toma de decisiones al menos consideraría las consecuencias de respetar o no el derecho a la privacidad de datos y de involucrarse con la identificación y resolución ética de los problemas de datos y las reparaciones de las violaciones de los derechos humanos que produzcan sus actos. En ese sentido, los principios del derecho internacional de los derechos humanos brindan un marco útil para ayudar a las empresas con principios que restringen su comportamiento comercial para la toma de decisiones éticas en el contexto de *Big Data*.

Luego de revisar los argumentos anteriores, se encuentra que los autores que respaldan esta posición creen que la normativa es efectiva parcialmente como guía en la privacidad de datos, ya que la mayoría de los autores consideran que todavía no existen los marcos legales aplicables a todas las etapas de análisis y de desarrollo de los algoritmos para hablar de una efectividad completa. Asimismo, los valores éticos todavía no se complementan con los requisitos y restricciones legales para ser efectiva totalmente. Inclusive, consideran que la efectividad es parcial porque las normas y los marcos conceptuales del conocimiento algorítmico se tienen que ajustar para hacer operativa una ciencia de datos basada en la responsabilidad.

Resumen Comparativo de la Controversia Relacionada con la Normativa como Guía en la Privacidad de Datos

Después de lo expuesto en este subtema, se encuentra que la mayoría de los autores revisados respaldan esta segunda posición, por ende, se puede considerar que la normativa en el uso de datos es efectiva parcialmente como guía en la privacidad de datos en la ciencia de datos, ya que la mayoría de los autores consideran que todavía no existen los marcos legales aplicables a todas las etapas de análisis de datos y de desarrollo de los algoritmos para hablar de una efectividad completa que permita gestionar la privacidad de los datos. Los argumentos se resumen en el siguiente cuadro comparativo (ver Tabla 2).

Tabla 2

Comparativo de la controversia relacionada con la normativa como guía en la privacidad de los datos

La normativa genera un manejo eficaz de la privacidad de los datos	La normativa es efectiva parcialmente como guía en la privacidad de los datos
La normativa en el uso de datos puede ser efectiva, ya que actúa como guía en la práctica responsable y ética.	No hay efectividad completa, porque no existen marcos legales que apliquen a toda la ciencia de datos.
Un marco regulatorio de ayuda para la toma de decisiones ética es un proceso útil para la evaluación ética de proyectos.	La efectividad es parcial porque las normas y marcos conceptuales tienen que ajustarse para hacer operativa una ciencia de datos responsable.
La normativa puede ser efectiva, pero existe obstáculos debido a la falta de pautas que guíe a las corporaciones, el gobierno y las instituciones.	La normativa no es efectiva porque los valores éticos no se complementan con los requisitos y restricciones legales para generar una confianza garantizada.
Un marco para la toma de decisiones ayuda con la creación de conciencia sobre cuestiones éticas en las prácticas de datos como un proceso efectivo.	La legislación de protección de datos actual debe alinearse con un marco ético para que sea efectiva .
La colaboración interdisciplinaria también es importante para analizar, sintetizar y armonizar las disciplinas y normas en torno a las decisiones éticas de datos.	Las empresas deben desarrollar sistemas de valores y código de conducta para cubrir los vacíos debido a la falta de normativas.
	También se puede usar la ley de derechos humanos como guía clara y consistente para mejorar en cuestiones de macrodatos.

Nota. Resumen comparativo de la normativa como guía en la privacidad de los datos en la ciencia de datos. Adaptado de Mühlhoff, 2021 (http://dx.doi.org/10.1007/s10676-021-09606-x); Franzke et al., 2021 (http://dx.doi.org/10.1007/s10676-020-09577-5); Chen y Quan-Haase, 2020 (http://dx.doi.org/10.1177/0894439318810734); Parti y Szigeti, 2021 (http://dx.doi.org/10.1080/23311886.2021.1970880); Lang et al., 2021 (http://dx.doi.org/10.2196/26450); Markham et al., 2018 (http://dx.doi.org/10.1177/2056305118784502); Forgó et al., 2020

(https://doi.org/10.1007/s41060-020-00211-7); Ibiricu & Marja, 2020 (http://dx.doi.org/10.1108/RMJ-08-2019-0044); Nersessian, D., 2018 (https://doi.org/10.1016/j.bushor.2018.07.006).

La Empresa como Responsable de la Privacidad de los Datos en la Ciencia de Datos

Esta tercera controversia se relaciona con el subtema de la empresa como responsable de la privacidad en el uso de los datos. En cuanto a eso, se encuentran dos posiciones que discuten los autores, el primero relacionado con (i) la responsabilidad total que tienen las empresas en torno a la privacidad de los datos de sus clientes la ciencia de datos; y, la segunda, relacionada con (ii) la responsabilidad parcial que tienen las empresas en torno a la privacidad de los datos de sus clientes en la ciencia de datos.

En el siguiente apartado se precisan los detalles de estas dos posiciones.

Responsabilidad Total de la Empresa en la Privacidad de los Datos de sus Clientes

Esta posición permite comprender a las empresas sobre el grado de responsabilidad que tienen sobre el manejo de la privacidad de los datos de sus clientes cuando se realizan prácticas de ciencia de datos que generan conflictos de privacidad de datos.

Al respecto, al hablar de responsabilidad total de las empresas, Martín (2019) manifestó que las empresas son los responsables de la privacidad de los datos en los algoritmos, ya que en el actor principal en las decisiones éticas que influyen en la delegación de roles y la responsabilidad del algoritmo, incluso cuando la organización afirma que los algoritmos son muy complicados y difíciles de comprender, aun así, son responsables de las implicancias éticas. Por ello, declara que las empresas son responsables no solo de la carga de valor y desarrollo de un algoritmo, sino también del diseño dentro de la decisión

algorítmica, ya que la responsabilidad por la toma de decisiones algorítmicas se construye en el diseño y desarrollo del algoritmo.

Entre los exponentes más importantes se encuentran Barocas et al., 2013, como se citó en Martín, 2019, quienes complementaron la idea, considerando ineficaz e incluso imposible atribuir la responsabilidad al desarrollador o al usuario que genera los datos, pues los usuarios consideran que los algoritmos son complicados y difíciles de comprender y mucho más de identificar, por ende, estos autores excluyeron a los usuarios de cualquier culpabilidad por las implicaciones éticas en los algoritmos. Otro exponente importante es Helbing et al., 2017, como se citó en Martín, 2019, quienes sostuvieron que las empresas podrían usar los algoritmos para inducir a los consumidores hacia una dirección preferida afectando su autonomía en la toma de decisiones.

En esa línea, el estudio de Martín (2019) demostró que las empresas tienen la responsabilidad total de la privacidad de los datos, para lo cual hizo uso de un algoritmo denominado COMPAS de Northpointe para ilustrar que los algoritmos no son neutrales, sino cargados de valor porque (i) crean consecuencias morales, (ii) refuerzan o debilitan los principios éticos, o (iii) disminuyen o afectan los derechos y la dignidad de las partes interesadas. Entre los hallazgos, los autores demostraron que las empresas tienen la responsabilidad de las implicancias éticas en el desarrollo de los algoritmos utilizados en la toma de decisiones con base en la obligación que tienen estas organizaciones cuando diseñan y desarrollan el algoritmo. Entre los resultados, se probó que los algoritmos están cargados de valor en lugar de ser neutrales, lo que demuestra que las empresas tienen implicaciones éticas de los algoritmos. Esto es, las organizaciones hacen una elección moral en cuanto a la delegación de tareas y responsabilidades de los participantes en el diseño de los algoritmos, por ente, también son responsables del diseño de sesgos cargados de valor. Reconocer los

sesgos cargados de valor no solo es importante para asegurar de que los algoritmos sean los más justos posibles (según los principios y normas de la decisión), sino también porque los algoritmos son una parte importante de una decisión más amplia en la delegación de roles y responsabilidades dentro de las decisiones éticas. En ese sentido, las empresas tienen implicaciones éticas de un algoritmo porque conoce las decisiones de diseño del algoritmo y está en la única posición de incorporar los sesgos cargados de valor en el algoritmo para influir en otros, así como los roles y las responsabilidades de la decisión algorítmica. Un ejemplo de los sesgos cargados de valor es, si a un grupo de personas que no se representó en los datos, le negaron sistemáticamente las admisiones de salud, en ese caso se dice que el algoritmo aprendió del conjunto de datos sesgado. Es por ello que la empresa debería asumir la responsabilidad de los actos, los sesgos y la influencia de su tecnología. En consecuencia, los algoritmos deben diseñarse comprendiendo la importancia de la delegación de roles y responsabilidades del sistema de decisión para desarrollar algoritmos responsables que permitan incorporar los principios y normas en la toma de decisiones.

Al igual que Martín, Nnamdi et al. (2022) argumentaron que los dueños de negocios tienen la responsabilidad del cumplimiento del deber percibido de cuidar a sus clientes en la recopilación y síntesis de datos en una economía global interconectada y digital, y que el análisis de *Big Data* en la cadena de suministro se extiende mucho más allá que la simple reinvención del área de la empresa.

Entre los exponentes más importantes se encuentran Kshetri et al., 2014, como se citó en Nnamdi et al., 2022, quienes manifestaron que las características de los grandes datos están estrechamente relacionadas con los efectos de privacidad, éticos y de seguridad en el bienestar del cliente, lo que han llamado la atención de académicos, empresas, sociedad,

industrias y legisladores, ya que la gran cantidad de datos puede producir infracciones de seguridad y violaciones de la privacidad. Otro exponente importante es Mikalef et al., 2019, como se citó en Nnamdi et al., 2022, quienes compartieron la idea de la responsabilidad que tiene la empresa en la privacidad de los datos, recordando el abuso de los datos por parte de Facebook al ignorar el cuidado que debió tener con sus usuarios. Por ese motivo, Kache y Seuring, 2015, como se citó en Nnamdi et al., 2022, coincidieron que las empresas tienen la responsabilidad de asegurar de que los datos de los usuarios y los productos no se compartan sin el consentimiento del propietario.

La investigación de Nnamdi et al. (2022) abordó un proceso de revisión sistemática de la literatura enfocado en el análisis de la cadena de suministro de *Big Data*, cuestiones éticas, de seguridad y privacidad por parte de las empresas con el fin de obtener una ventaja competitiva, así como las implicaciones para la sociedad, las empresas y la industria. Entre los hallazgos, los autores encontraron que las empresas no solo deben cumplir con la legislación, sino también con las normas éticas durante la recopilación, la gestión y el análisis de los datos, por ello existe la necesidad urgente de que las empresas construyan una imagen más confiable para sus clientes, mejorando la seguridad y obteniendo el consentimiento de parte de los clientes para el desarrollo de una arquitectura de seguridad mucho más confiable y segura para evitar la violación de la privacidad del cliente y garantizar el acceso controlado. Otro hallazgo fue, la falta de esfuerzos significativos por parte del gobierno para introducir leyes nuevas y efectivas que reemplacen el marco regulatorio y la infraestructura de seguridad regulatoria, así mismo, falta una creación de conciencia adecuada por parte de la sociedad.

De igual modo, Breidbach y Maglio (2020) argumentaron que las empresas solo deben implementar herramientas de toma de decisiones algorítmicas siempre que el resultado de sus decisiones no afecte de manera ética a los clientes u otras partes interesadas y con el fin de garantizar la responsabilidad ética de las operaciones del servicio que brinda la empresa. Por lo tanto, consideran que también deben desarrollar modelos más responsables y éticos, ya que los conjuntos de datos que son intrínsecamente sesgados o de origen poco éticos deben convertirse en una responsabilidad para las empresas. En ese sentido, es importante la presencia de normas, reglas o procedimientos éticos para prevenir la explotación de los datos para el propio beneficio económico de la empresa.

Entre los exponentes más importantes se encuentra Martín, 2015, como se citó en Breidbach y Maglio, 2020, quien manifestó que las organizaciones utilizan análisis de *Big Data* para reducir costos y generar ingresos adicionales, a menudo sin considerar las implicaciones éticas para otros actores económicos dentro de sus redes de valor. Otros exponentes destacados son Wixom y Ross, 2017, como se citó en Breidbach y Maglio, 2020, quienes también manifestaron que los datos son activos que pueden compartirse y comercializarse como cualquier otro producto, estando expuesto a prácticas poco éticos. También, se menciona a Someh et al., 2019, como se citó en Breidbach y Maglio, 2020, quienes manifestaron que los problemas poco éticos asociados con la toma de decisiones algorítmicas contemplan (i) la confiabilidad limitada de los algoritmos que puede afectar el derecho de la privacidad de las personas, (ii) la falta de participación humana y (iii) la incapacidad de garantizar la responsabilidad de las decisiones algorítmicas tomadas.

En la investigación de Breidbach y Maglio (2020), se abordó el marco de la literatura en el contexto de las compañías de servicios de seguros de Estados Unidos como Deere & Company, John Hancock y Allstate. Entre los hallazgos, los autores demostraron que el

algoritmo, la inteligencia artificial y el conjunto de datos grandes pueden ser poco éticos, afectando a la privacidad de los usuarios, manipulación directa, entre otros. La importancia de la propuesta de valor a través de los modelos comerciales basados en datos ayuda a comprender a las empresas de servicios a dar un mejor uso al aprendizaje automático o la inteligencia artificial, tales intentos pueden tener implicaciones poco éticos, ya que el verdadero propósito de las propuestas de valor basadas en datos a menudo se oculta y se obliga a las personas a usarlas, por ejemplo, se obligan a las personas aceptar los términos y condiciones normalmente antes de usar cualquier servicio digital, lo que es inútil, porque los clientes no los leen ni los entienden, por lo que también vieron conveniente alejarse del modelo de "términos y condiciones". En ese sentido, el estudio reveló que un modelo novedoso centrado en modelos comerciales que redefine el valor basado en datos, lo que puede ser eficaz, ya que permite la aparición de nuevos modelos y alternativas de valor. En consecuencia, desde la perspectiva de una organización, no se trata de usar, o no usar el aprendizaje automático avanzado o inteligencia artificial, sino de comprender los medios para monetizarlos, especialmente porque este proceso puede conducir a problemas poco éticos.

También, Nersessian (2018) argumentaron que los actores corporativos tienen obligaciones legales de respetar los derechos humanos en sus actividades comerciales que necesariamente se relacionan con *Big Data*. Por ello, consideraron que las corporaciones tienen que adoptar políticas y procedimientos corporativos relacionados con los derechos humanos y proporcionar una reparación para las violaciones de los derechos humanos que se produzcan. Dicho marco de derechos humanos también podría proporcionar una guía clara

y consistente a las empresas cuando las leyes del país y los mecanismos de implementación sean débiles.

Entre los exponentes más importantes se encuentra Nersessian, 2015, como se citó en Nersessian, 2018, quien manifestó que los actores corporativos tienen algunas obligaciones legales de respetar los derechos humanos en sus actividades comerciales que incluyen actividades con *Big Data*, particularmente cuando las violaciones de los derechos humanos constituyen crímenes internacionales, en cuyo caso la empresa criminal puede ser considerada responsable del delito mismo o cualquiera que sea cómplice de ella.

En el estudio de Nersessian (2018) principalmente se abordaron temas relacionados con el derecho internacional de los derechos humanos que opera como una restricción legal y ética sobre el uso comercial global de las tecnologías de *Big Data*. Entre los hallazgos, se determinó que existe poco consenso internacional sobre los estándares que deben regir el uso de la tecnología de *Big Data*, por eso los autores explicaron que el derecho internacional de los derechos humanos podría usarse para llenar el vacío que existe actualmente en la normativa en *Big Data* y los algoritmos. En general, encontraron que estas normas internacionales podrían proporcionar un marco coherente para analizar las obligaciones del sector privado y su respeto por los derechos humanos a medida que desarrollan e implementan servicios de macrodatos, ya que, una empresa que incorpora dicho marco de derechos humanos dentro de su ecosistema de toma de decisiones, al menos consideraría el impacto en la privacidad antes de involucrarse con alguna falta en la recopilación de la información, así como en el desarrollo de algoritmos, el procesamiento de datos y la interpretación de los resultados. En ese sentido, el sector empresarial, como principal creador y usuario de la tecnología de *Big Data*, tiene una responsabilidad fundamental para garantizar su uso y desarrollo responsable.

En la misma línea, Hirsch (2019) sostuvo que las empresas son los responsables de gestionar el riesgo continuo principalmente mediante el cumplimiento de las leyes de privacidad para garantizar que sus actividades de análisis de datos no manipulen a las personas o invadan su privacidad, pues no basta solo que las personas brinden su consentimiento para protegerse de los daños que ocasione el análisis de *Big Data*, sino que las empresas tampoco pueden protegerlos simplemente cumpliendo con las leyes de privacidad por los riesgos derivados del uso y análisis de datos que hacen. Inclusive, los tecnólogos pueden decidir abandonar a las empresas cuando sus valores o acciones les parezcan ofensivos, dando más razones a las empresas para no dejar que suceda una falta. Por ello, el autor infiere que las empresas deben actuar de manera responsable en la ética de los datos, de esta manera también podrán adelantarse a las futuras regulaciones en el análisis de *Big Data.*

En el estudio de Hirsch (2019) se analizaron las amenazas para los consumidores individuales en el análisis de *Big Data* por parte de las empresas de tecnología, *retail*, farmacéutica, salud y otras industrias que analizan grandes datos. Entre los hallazgos, los autores sostuvieron que el análisis de *Big Data* puede dañar a las personas en al menos tres formas importantes: invasión de la privacidad, manipulación y sesgo. Además, el análisis *Big Data* representa un riesgo continuo de invasión a la privacidad, pero muchas empresas no conocen completamente estos riesgos comerciales, por ejemplo, las personas ya no pueden solo aceptar las políticas de consentimiento a la privacidad para protegerse, pues las empresas tampoco pueden protegerlas simplemente con cumplir la ley de privacidad de datos, sino que exige ir más allá de la ley. Los hallazgos también revelaron que el uso irresponsable del análisis de *Big Data* puede perjudicar a las personas e infligir un daño

importante a la reputación corporativa y al valor de los accionistas. Como resultado, algunas empresas han comenzado a administrar estos riesgos de invasión de la privacidad de manera proactiva para inferir las vulnerabilidades psicológicas de las personas y aprovecharlas, bajo el enfoque de "ética de datos", ya que el uso irresponsable del análisis de *Big Data* puede perjudicar a las personas y dañar la reputación corporativa y al valor de los accionistas. Asimismo, la ética de datos también sugiere que las empresas deben educarse sobre los marcos de derechos humanos y otras filosofías éticas, y luego hacer un esfuerzo para ajustarse a sus prácticas comerciales.

Igual que Keren y Owen (2019) consideran que son las empresas las que deben comprometerse con las cuestiones de privacidad del usuario, consentimiento y uso secundario de los datos como impulsores de un comportamiento responsable, por lo que las compañías deben tener como objetivo (i) fomentar este comportamiento responsable mediante la construcción de una cultura de transparencia, (ii) la internalización de los valores y principios en sus propias políticas y operaciones, teniendo como foco la innovación y su gobierno, así como (iii) una definición clara de los roles y tareas de las partes interesadas internas para fomentar el comportamiento responsable y ético por parte de los empleados.

Entre los exponentes más importantes se encuentran Bollier et al., 2010, como se citó en Keren y Owen, 2019, quienes indicaron que el manejo de los datos, la privacidad, la seguridad y la integración de estos datos con los procesos comerciales han pasado a primer plano a medida que las organizaciones de la industria consolidan las mejores prácticas destinadas a permitir que maximicen constantemente el valor de los datos dentro del sector financiero. Otro exponente importante es Martín, 2015, como se citó en Keren y Owen, 2019, quien indicó que las empresas investigadas han exhibido un grado considerable de

innovación tecnológica a lo largo del tiempo para permitir la explotación de grandes datos y análisis asociados; por lo que se ha posicionado como un intermediario clave en la administración de suministro de información y de relaciones con las partes interesadas.

En el estudio de Keren y Owen (2019), se abordó una investigación etnográfica empírica dentro de las organizaciones del sector financiero que innova con plataformas y servicios disruptivos relacionados con la tecnología que respaldan el análisis comercial en los sectores bancario y minorista. Entre los hallazgos, se determinó que las innovaciones basadas en *Big Data* pueden tener vacíos de gobernanza, los que pueden ser sustentados con valores y principios relativos a la privacidad y seguridad de los datos, es por eso que las empresas del sector financiero han internalizado estos temas en sus propias políticas y operaciones. También, se demostró que la empresa ha tenido que ser adaptable y receptiva, particularmente a las necesidades de sus partes interesadas y específicamente en el manejo de principios en las prácticas operativas. Otro hallazgo también fue descubrir que la empresa emplea un enfoque de gobernanza de la innovación de varios niveles, respaldado por una estrategia ética basada en un principio de beneficio mutuo con respecto a las partes interesadas. La gobernanza en las empresas también debe incluir la legislación de protección de datos contextuales, los estándares de uso cuando se aceptan tarjetas de pago y los controles corporativos internos, presentados como prácticas organizacionales relacionadas con la seguridad y privacidad de los datos.

Luego de revisar los argumentos expuestos, se pudo encontrar que los autores consultados que respaldan esta posición creen que las empresas tienen la responsabilidad total en la privacidad de los datos de sus clientes en la ciencia de datos, ya que las empresas son los responsables directos en el diseño de los algoritmos como un actor importante en las

decisiones éticas que influyen en la delegación de roles y las decisiones algorítmicas, sobre todo cuando los conjuntos de datos estén expuestos al riesgo de estar sesgados o tener un origen poco ético, además deben incorporar en sus políticas y procedimientos corporativos para proporcionar una guía clara y consistente cuando las leyes del país y los mecanismos de implementación sean débiles. Asimismo, son los responsables de gestionar el riesgo continuo, ya que no basta solo con cumplir con la ley de privacidad de datos, sino también de comprometerse con las cuestiones del consentimiento y uso secundario de los datos para un comportamiento más responsable.

Responsabilidad Parcial de la Empresa en la Privacidad de los Datos de sus Clientes

Continuando con el subtema, en este apartado se discute la posición de los autores con respecto a su punto de vista de que las empresas tienen la responsabilidad parcial de la privacidad de los datos de sus clientes en la ciencia de datos.

Al respecto, al hablar de responsabilidad parcial que tienen las empresas en la privacidad de los datos, Saltz y Dewar (2019) argumentan que las empresas no siempre tienen toda la responsabilidad, ya que dentro del modelado de ciencia de datos existe subjetividad, pero que puede ser gestionado por las organizaciones para implementar mecanismos de gestión que les permitan enfrentar los desafíos éticos en la ciencia de datos; además, las empresas deben centrarse en evitar la discriminación y el sesgo que ocurren, sin saberlo, en el uso de un modelo de ciencia de datos.

Entre los exponentes más importantes se encuentra Crawford, 2013, como se citó en Saltz y Dewar, 2019, quienes complementaron la idea al considerar que los modelos de ciencia de datos se pueden construir utilizando datos que registran un sesgo y, por consiguiente, el modelo también podría tener ese sesgo que podría perjudicar

sistemáticamente a un subgrupo social. Al respecto, Butrymowicz y Garland, 2012, como se citó en Saltz y Dewar, 2019, indicaron que, a pesar de que la base de datos real tiene las puntuaciones correctas o precisas almacenadas en la base de datos, aun así, los datos de una prueba no son precisos y no deben usarse como entrada clave para el modelo analítico de ciencia de datos. En ese sentido, Fuller, 2017, como se citó en Saltz y Dewar, 2019, sostuvo que el científico de datos también tiene el deber de explicar sus modelos y las implicaciones de usar un modelo, usando un lenguaje que los "no científicos de datos", como los gerentes, puedan entender claramente y conocer su impacto.

El estudio de Saltz y Dewar (2019) abordó una revisión sistemática de la literatura. Entre los hallazgos los autores identificaron los desafíos éticos clave en la ciencia de datos, a saber, la necesidad de un marco ético, la novedad del campo, los desafíos relacionados con los datos y los desafíos relacionados con el modelo de análisis. Los resultados demostraron que dichos desafíos éticos relacionados con los datos del sujeto, el almacenamiento, la preparación y la difusión de los mismos podrían afectar la privacidad, el anonimato o causar sesgos en los análisis resultantes. Debido a estos desafíos, el modelo de ciencia de datos podría funcionar incorrectamente y llegar a causar daños, pudiendo ser injusto para algunos sujetos. En ese sentido, si bien la ciencia de datos puede aportar objetividad a la toma de decisiones y funcionar correctamente, de todas maneras, existe subjetividad dentro del modelado de ciencia de datos sobre qué algoritmo usar, qué datos usar, cómo interpretar los resultados u otros. Esto proporciona un marco para que un equipo de profesionales de ciencia de datos podría usar para ayudar a garantizar que la ética se haya considerado adecuadamente dentro del proyecto. En ese sentido, los científicos de datos deben poder dar cuenta de los sesgos en su interpretación de los datos que pueden encontrarse no solo en las herramientas que utiliza el científico, sino también en el propio científico de datos que la empresa contrata,

quienes tienen el deber de explicar sus modelos y las implicaciones de usar el modelo a los gerentes para que puedan entender con explicaciones simples.

En la misma posición, Wiener et al. (2020) sostienen que en entornos organizacionales los modelos de negocio de *Big Data* integran entornos más amplios que incluyen varios grupos de partes interesadas que van desde individuos hasta gobierno y la sociedad. Un ejemplo de ello, es la influencia legislativa que puede permitir o restringir los usos de *Big Data* en materia de privacidad.

Entre los exponentes más importantes se encuentran Hartmann et al., 2016, como se citó en Wiener et al., 2020, quienes indicaron que las partes interesadas son importantes para la investigación del modelo de negocio de grandes datos (BDBM) en al menos dos motivos. En principio, la influencia legislativa que puede normar el uso de grandes datos (BD). En segundo lugar, se encuentran los gobiernos que intentan usar los BD para ayudar cada vez más a sus ciudadanos, principalmente para fines de control y seguridad.

Continuando con el estudio de Wiener et al. (2020), en el documento se revisó la literatura relacionada con los modelos comerciales de negocios y el análisis de *Big Data*. Se analizaron los modelos de negocios de organizaciones europeas y estadounidenses. Entre los hallazgos, los autores encontraron que *Big Data* ofrece a las organizaciones la oportunidad de obtener y mantener una ventaja competitiva, haciendo uso de los modelos comerciales de grandes datos para generar una integración vertical dentro de la cadena de suministros en la medida que recopilan, almacenan, administran y procesan los datos. Los resultados concluyeron que los BDBM no funcionan de forma aislada; más bien, están integrados en un entorno organizacional más amplio que incluyen varias partes interesadas, que van desde individuos hasta gobierno y la sociedad. También, se espera que la consideración de estos

grupos de partes interesadas adicionales genere mayor información para crear y capturar valor, incluso más allá del valor organizacional. De ahí que, muchas organizaciones, al tratar de explotar el potencial comercial estratégico integrado en los grandes datos, han comenzado a renovar sus modelos comerciales o desarrollar otros nuevos, dando lugar al fenómeno de los modelos comerciales de grandes datos para mantener una ventaja competitiva.

En la misma línea, Chalcraft (2018) argumentaron que las organizaciones que se dedican al análisis de datos deben gestionar su responsabilidad en el análisis de datos y sus limitaciones éticas para establecer políticas y procedimientos sobre el desarrollo y la utilización de los datos, incluso cualquier persona puede responsabilizar a la empresa si considera que su derecho a la intimidad está siendo vulnerada, más aún cuando las leyes de privacidad no contempla la información personal de dominio público, por ejemplo, no aplica a la información compartida en redes sociales. En esa situación, las empresas no son los únicos responsables, ya que también están los profesionales de la información quienes deben hacer comprender a las organizaciones sobre las implicaciones y los riesgos relacionados con la información y el análisis de datos, ayudándolos a lidiar con estas preocupaciones éticas relacionadas con la privacidad de los datos.

Entre los exponentes más importantes se encuentran Chessel, 2014, como se citó en Chalcraft, 2018, quienes sugirieron que las organizaciones podrían desarrollar una política de análisis de datos más restringida en consulta con las partes interesadas. Se trata de respetar no solo la información personal contemplado en la legislación de privacidad, sino ir más allá, realizando prácticas de protección adicional contra el uso indebido y la difusión inadecuada de los datos confidenciales que se comparten con todas las partes interesadas.

Siguiendo con el estudio, Chalcraft (2018) buscó establecer límites éticos en el análisis de datos. Las empresas que se analizaron estuvieron dedicadas a generar valor a través de sus recursos de datos comerciales. En tal sentido, los hallazgos demostraron que las organizaciones que participan en el análisis de datos deben decidir la mejor manera de equilibrar las responsabilidades y establecer políticas y procedimientos que ayuden a lograr ese equilibrio frente a sus diferentes partes interesadas. Las leyes y regulaciones de privacidad también existen para proteger el derecho a la privacidad de las personas, limitando la forma en que las empresas recopilan, usan o divulgan los datos de los sujetos. Incluso, los estándares y códigos de práctica pueden guiar a las organizaciones en el establecimiento de sus políticas de análisis de datos. Asimismo, los profesionales de la información pueden ayudar a las organizaciones a lidiar con estas preocupaciones éticas, ya que tienen la perspectiva y las habilidades para abordar los desafíos prácticos de la gestión de datos. También, se consideró apropiado elaborar políticas de privacidad de datos más legibles para brindar más opciones sobre el consentimiento para permitir que las personas opten por participar (o no) en los usos de sus datos o solicitar explícitamente el consentimiento para usos de análisis de datos, específicamente cuando los datos se reutilizan.

De la misma manera, Herschel y Virginia (2017) argumentaron que las empresas deben definir y hacer cumplir las reglas sobre el uso de los datos, ya que no están respetando la autonomía de las personas cuando recopilan y analizan de forma rutinaria la información para evaluar a las personas sin su consentimiento, por eso, plantean las teorías éticas para tomar en consideración a otras personas muy a pesar de quienes toman las decisiones, ya que asume que el bien moral y los principios morales se basan en el razonamiento objetivo a partir de hechos y valores comunes. Además, esta postura sostiene que se debe examinar

los sentimientos, el carácter y las acciones de las personas que implementan y analizan *Big Data*, así como los efectos intencionados y no intencionados de sus acciones en los demás más allá que solo considerar a la empresa como responsable. En otras palabras, se tiene que evaluar a aquellos individuos que emplean *Big Data* y determinar si el uso que hacen de él y sus intenciones son consistentes con las acciones de un sujeto virtuoso (que sea escrupuloso).

Entre los exponentes más importantes se encuentran King y Richards, 2014, como se citó en Herschel y Virginia, 2017, quienes informaron que las empresas deben definir y hacer cumplir las reglas sobre el uso y manejo de los datos; además, revelaron que las personas deberían tener la capacidad de administrar el flujo de su información privada a través de sistemas analíticos masivos porque los usos secundarios de *Big Data* producen nuevas predicciones e inferencias; esto genera que los datos sean un negocio para las empresas.

En esa línea, Herschel y Virginia (2017) discutieron cuatro teorías éticas (el kantianismo, la teoría del contrato social, el utilitarismo y la teoría de la virtud) para enmarcar la comprensión de las cuestiones morales en los problemas de *Big Data* utilizando argumentos lógicos y racionales. Entre los hallazgos, los autores revelaron que el uso de las teorías éticas ayuda a articular mejor los problemas con *Big Data* en función de un conjunto de valores morales. Además, se encontró que el responsable del tratamiento de los datos debe tomar todas las medidas razonables para eliminar los elementos que identifican a las personas cuando esto se ha hecho público sin justificación. En ese sentido, las empresas también pueden informar a los consumidores cuando sus datos se usan para identificar patrones de comportamiento en línea, inclusive pueden crear mecanismos para brindan a los clientes la opción de excluirse de los registros.

Luego de revisar todos los argumentos expuestos en este apartado, se encontró que los autores que respaldan esta posición creen que las empresas no siempre tienen toda la responsabilidad en la privacidad de los datos, porque los modelos de negocio de *Big Data* integran entornos más amplios que incluyen a varias partes interesadas que van desde individuos hasta gobiernos y la sociedad; además, porque en el modelado de ciencia de datos existe subjetividad que puede conducir a la discriminación y el sesgo; en esa línea, también existe una responsabilidad de parte de los profesionales de la información quienes tienen el deber importante de hacer comprender a los gerentes sobre las implicaciones y los riesgos éticos, además, porque están inmersos los sentimientos, acciones y carácter del profesional.

Resumen Comparativo de la Controversia Relacionada con la Empresa como Responsable de la Privacidad de los Datos

Después de lo expuesto en este subtema, se encuentra que la mayoría de los autores revisados respaldan la primera posición, por ende, se puede considerar que las empresas tienen la responsabilidad total de la privacidad de los datos de sus clientes en la ciencia de datos, ya que son los responsables de desarrollar modelos más responsables y éticos. Los argumentos se resumen en el siguiente cuadro comparativo (ver Tabla 3).

Tabla 3

Comparativo de la controversia relacionada con la empresa como responsable de la privacidad de los datos

Responsabilidad Total de la Empresa en la Privacidad de Datos	Responsabilidad Parcial de la Empresa en la Privacidad de Datos
Las empresas son responsables de la privacidad de los datos en los algoritmos, porque deben desarrollar modelos más responsables y éticos.	Las empresas no siempre tienen toda la responsabilidad en la privacidad de datos, porque en el modelado de ciencia de datos existe subjetividad.
Además, son responsables de (i) la delegación de roles, (ii) la decisión algorítmica y (ii) de implementar herramientas éticas que no afecten a sus clientes u otras partes interesadas.	La subjetividad debe ser gestionado por las organizaciones mediante la implementación de mecanismos de gestión para evitar la discriminación y el sesgo en el modelo de ciencia de datos.
Tienen obligaciones legales que deben considerar como son los derechos humanos que deben incorporar en sus políticas y procedimientos corporativos como guía clara y consistente.	Los modelos de negocio de *Big Data* integran entornos más amplios que solo el de la empresa, ya que incluyen las partes interesadas que van desde individuos, gobiernos y la sociedad.
Deben comprometerse con las cuestiones de consentimiento y uso secundario de los datos para un comportamiento más responsable de los datos.	Los profesionales de la información también son responsables porque deben hacer comprender a los gerentes sobre los riesgos éticos en el análisis de datos.
También, son responsables de gestionar el riesgo que se genera cuando la Ley de privacidad de datos no es suficiente.	Las empresas tampoco son los únicos responsables porque el análisis de los datos también depende de las acciones intencionadas y los sentimientos de los profesionales que analizan los datos.

Nota. Resumen comparativo de la normativa como guía en la privacidad de los datos en la ciencia de datos. Adaptado de Martín, 2019 (http://dx.doi.org/10.1007/s10551-018-3921-3). Nnamdi et al., 2022 (http://dx.doi.org/10.1080/09537287.2020.1810764); Breidbach y Maglio, 2020 (http://dx.doi.org/10.1108/JOSM-03-2019-0073); Nersessian, 2018 (https://doi.org/10.1016/j.bushor.2018.07.006); Hirsch, 2019 (https://www.proquest.com/scholarly-journals/data-ethics-risk-management-algorithmic-

age/docview/2344525577/se-2?accountid=28391); Keren y Owen, 2019 (http://dx.doi.org/10.1007/s10551-019-04203-x); Saltz y Dewar, 2019 (http://dx.doi.org/10.1007/s10676-019-09502-5); Wiener et al., 2020 (http://dx.doi.org/10.1177/0268396219896811); Chalcraft, 2018 (); Herschel y Virginia, 2017 (https://doi.org/10.1016/j.techsoc.2017.03.003).

Los Constructores de los Algoritmos como Responsables de la Privacidad de los Datos en la Ciencia de Datos

Los constructores de los algoritmos son los investigadores quienes aportan sus habilidades como profesionales para analizar los volúmenes de datos de los usuarios (Hesse et al., 2019). Estos datos son accesibles para los investigadores profesionales de disciplinas como la física, la ingeniería y la informática, pero, también se encuentran los investigadores cualitativos aficionados, quienes se forman a sí mismos como investigadores cualitativos simplemente al obtener acceso a las transcripciones (Hesse et al., 2019). En la actualidad, este hecho ha generado que algunas las personas se formen a sí mismas como investigadores simplemente al obtener acceso a las transcripciones de los datos (Hesse et al., 2019).

Esta cuarta controversia se relaciona con el punto de vista de que los constructores de los algoritmos son los responsables de la privacidad en el uso de los datos. Con relación a eso, se encuentran dos posiciones que discuten los autores, el primero relacionado con que (i) los constructores de los algoritmos tienen la responsabilidad total de la privacidad de los datos en la ciencia de datos y, la segunda, relacionada con (ii) la responsabilidad parcial que tienen los constructores de los algoritmos en la privacidad de los datos.

Responsabilidad Total de los Constructores de los Algoritmos en la Privacidad de los Datos

Esta posición permite a los constructores comprender el grado de responsabilidad que tienen con respecto al manejo de la privacidad de los datos cuando realizan prácticas de ciencia de datos.

Al respecto, al hablar de responsabilidad total que tienen los constructores en la privacidad de los datos, Hesse et al. (2019) argumentaron que los investigadores deben proteger la privacidad de los datos de las personas al margen de las exigencias institucionales por normas profesionales, incluso deben proteger la privacidad cuando los usuarios se den cuenta o no de cómo las empresas o los mismos investigadores pretenden utilizar su información, de hecho, otros autores han descubierto que los acuerdos de usuario para el manejo de los datos confidenciales se leen muy escasa vez, un ejemplo de ello, es cuando los usuarios de las redes sociales pueden no darse cuenta completamente de cómo son investigados, aunque es ese caso, también puede ser poco razonable solicitar a los investigadores que obtengan el consentimiento de todas las personas que publican un tuit en redes sociales por ejemplo.

Entre los exponentes más importantes se encuentran Metcalf y Crawford, 2016, como se citó en Hesse et al., 2019 quienes opinaron sobre los problemas de consentimiento y privacidad en las redes sociales, considerando que los usuarios normalmente no son totalmente conscientes que proporcionan datos sobre su ubicación y movilidad. Aunque es posible que las medidas institucionales no requieran una revisión ética para estos datos que normalmente se consideran públicos, así, los estándares profesionales obligan a los investigadores a proteger a las personas fuera de las demandas institucionales.

En la investigación de Hesse et al. (2019) efectuaron una revisión de la literatura enfocada en los estudios sociales de la ciencia y la tecnología. Entre los hallazgos, los autores consideraron que las tecnologías y los enfoques de *Big Data* han cambiado las normas y la ética de las prácticas de investigación, de ahí que los académicos de muchas disciplinas y perspectivas metodológicas no deben permanecer pasivos a medida que se desarrollan los proyectos, sino que necesitan participar activamente en estos debates. Por ello, la investigación demostró la necesidad de considerar a los investigadores cualitativos para dar forma a las condiciones en la investigación ética y significativa. Otro hallazgo fue la consideración de cinco principios rectores para que los investigadores cualitativos y sus instituciones los consideren al realizar sus prácticas, estos fueron: i) valorar la diversidad metodológica; (ii) fomentar la investigación para que tengan en cuenta el contexto, la especificidad y las poblaciones marginadas; (iii) abordar dilemas éticos y no solo ver las preocupaciones legales; (iv) mayor atención a las diferencias regionales y disciplinarias; y (v) considerar todo el ciclo de vida de la investigación, incluyendo su vida futura en los archivos o instalaciones de datos abiertos.

Así también, Utts (2021) sostuvo que estos profesionales (estadísticos y científicos de datos) son quienes deben asumir la responsabilidad de las cuestiones éticas en los proyectos, siendo ellos quienes pueden ayudar a crear conciencia y promover las mejores prácticas ante los problemas éticos relacionados con la privacidad de datos que afectan a la ciencia de datos. Incluso, las pautas éticas profesionales o códigos de conducta se tienen que actualizar cada pocos años, ya que en la actualidad se han limitado a los roles que tradicionalmente desempeñaban los estadísticos, por lo que deben extenderse más allá de los

trabajos tradicionales en estadística para desarrollar algoritmos de aprendizaje automático e inteligencia artificial.

Entre los exponentes más importantes se encuentran Gibson, 2019, como se citó en Utts, 2021, quienes consideraron que el rápido crecimiento de los grandes datos genera nuevas oportunidades para que los estadísticos colaboren en cuestiones relacionadas con el falso descubrimiento, la disminución del sesgo y la generalización de los resultados a partir de datos que no son muestras.

Con respecto al estudio de Utts (2021), se abordaron temas relacionados con los estadísticos y lo que pueden hacer ellos para mejorar la ética en la práctica de la ciencia de datos y cómo los educadores de estadística pueden inculcar un comportamiento ético sólido en los estudiantes. Entre los hallazgos, los autores señalaron que los estadísticos son quienes pueden ayudar a crear conciencia y fomentar las mejores prácticas éticas ante los abusos de algoritmos y análisis de datos complejos que impacta en la sociedad. Además, se encontró que muchos usuarios no entienden el concepto de "multicolinealidad" para el análisis (multicolinealidad viene a ser la relación fuerte de dependencia lineal entre dos o más variables explicativas en una regresión múltiple) y pueden necesitar la guía de un estadístico con mayor conocimiento para interpretar correctamente los coeficientes en la regresión múltiple. En ese caso, los educadores estadísticos que enseñan regresión múltiple deben indicar hasta qué punto la multicolinealidad puede conducir a resultados engañosos. Además, estos educadores tienen la responsabilidad ética de promover la alfabetización estadística en todas las etapas de la educación profesional, así como orientar a los estadísticos y científicos de datos sobre los métodos que pueden incorporar en su trabajo para mejorar la práctica ética de la profesión. En ese sentido, los resultados indicaron que los estadísticos tienen la responsabilidad de desempeñar un papel importante para garantizar que el futuro

de la ciencia de datos incluya la ética y, por lo tanto, los estadísticos deben poder hablar sobre el tema como miembros de equipos multidisciplinarios y asumir, muchas veces, el papel de liderazgo al plantear cuestiones de ética.

De modo similar, Arrojo (2019) argumentan que los agentes de la comunicación y tecnología (los profesionales) no tienen por qué guiarse por sus intuiciones individuales o por las socialmente aceptadas, sino que deben guiarse de los códigos deontológicos, es decir de la práctica profesional y del conocimiento científico en el mercado de los valores éticos, en otras palabras, estos códigos deontológicos resuelven los problemas relacionados con la privacidad, buena imagen, derecho a la intimidad, etc. Esto exige atender a las dimensiones habitualmente no contempladas como endógenas y exógenas, ya que tienen que ver con la ética, siendo la segunda dimensión la más visible y que necesita mayor atención. Por ello, consideran que el uso de las innovaciones tecnológicas tiene efectos internos (del acto comunicativo) y externos (en la sociedad en la que circulan).

Uno de los exponentes más importantes es Arroyo, 2015, como se citó en Arrojo, 2019, quien indicó que los dos componentes de valores éticos, endógeno (interno) y exógeno (externo), están presentes en la ciencia en general. Como componente endógeno, se representa a la ciencia como una carga de valores internos dentro de la actividad propietaria, presentes en el proceso humano de hacer ciencia (honor, confiabilidad, responsabilidad de los científicos). El componente exógeno se refiere los aspectos externos de la ciencia científica que conecta a la ciencia con el resto de experiencias humanas: económicas, sociales, culturales, tecnológicas, etc. González, 2015, como se citó en Arrojo, 2019, también consideró que los componentes endógenos y exógenos son aspectos de los valores éticos en la tecnología que justifica la existencia de los valores éticos en la ciencia de la

comunicación en la que se basa la tecnología. Otro de los exponentes relevante es Arroyo, 2013, como se citó en Arrojo, 2019, quien indicó que estos valores en la aplicación de la ciencia, es lo que puede servir de base para los códigos deontológicos profesionales.

En la investigación de Arrojo (2019) se abordaron los valores éticos en las ciencias de la comunicación audiovisual. Entre los hallazgos los autores encontraron que, en la ciencia de la comunicación se transforma lo real y se lleva al mundo creativo usando la tecnología, lo cual debe ser muy bien pensada y alineada a la ética para no dañar los valores intangibles que son valorados (la imagen pública, la familia, el prestigio, la honestidad, etc.). Esto exige atender a las dimensiones habitualmente no contempladas como endógenas y exógenas, ya que tienen que ver con la ética. En la actualidad todo el énfasis está puesto en la ética como estudio de la faceta extrínseca de los fenómenos comunicativos. Asimismo, las innovaciones tecnológicas importantes en sociedades avanzadas pueden provocar nuevos valores desde un punto de vista económico, por ejemplo, los desarrollos tecnológicos de la empresa (como Apple) que hacen uso de las Tecnologías de la Información y la Comunicación (TIC) pueden sugerir nuevos valores éticos. Además, los temas éticos en la aplicación de la ciencia de datos actualmente se relacionan con los códigos deontológicos, ya que permiten regular el comportamiento de estos profesionales de la comunicación. En este sentido, los códigos deontológicos requieren necesariamente una actualización urgente para que consideran los nuevos contextos de uso de los datos enfocados en los valores éticos relacionados con la aplicación de las ciencias de la comunicación. Como tal, la interrelación de la comunicación audiovisual con las TIC, requieren que los códigos deontológicos introduzcan nuevos criterios éticos en el uso de nuevas tecnologías.

Asimismo, Monkman et al. (2018) sostienen que los investigadores tienen el deber profesional de manejar la ética en su investigación frente al riesgo de causar daño a los agentes involucrados, ya que las juntas de revisión ética actualmente pueden ser limitadas y toda la actividad de extracción de contenido de internet debe realizarse de manera responsable para que los datos personales no se vean comprometidos.

Entre los exponentes más importantes se encuentra Walther, 2002, como se citó en Monkman et al., 2018 quien sostuvo que los avances tecnológicos en el análisis de macrodatos han permitido la identificación de las personas, lo que significa que el investigador debe considerar minuciosamente los datos que publican frente a las situaciones de riesgo. A esto se suma un ejemplo de, Narayanan y Shmatikov, 2009, como se citó en Monkman et al., 2018 cuando demostraron que solo se pueden usar algunos datos de información personal (identificadores indirectos) para eliminar el anonimato de un usuario. Entre los identificadores indirectos están: el lugar de trabajo, la ocupación y la ciudad de residencia actual, siendo estos algunos ejemplos que pueden hacer posible la identificación del autor del contenido.

En la investigación de Monkman et al. (2018) se abordó a la ética del uso de datos publicados en las redes sociales en la investigación pesquera. Entre los hallazgos, los autores encontraron que la industria pesquera debe reevaluar constantemente la ética de su investigación en las redes sociales, ya que la orientación de las juntas de revisión ética puede ser limitadas y la extracción de contenido de internet debe realizarse de manera responsable para que los datos no se vean comprometidos. En cuanto a las redes sociales, los investigadores saben que el uso de datos públicos para fines de investigación está protegido por derogaciones en la ley de derechos de autor, aunque las leyes pueden variar en cada país. Por eso, los investigadores son los que deben asegurar de que la minería de texto y de datos

(TDM) estén permitidos en la legislación de derechos de autor de uso de acuerdo a cada país. Además, las políticas de privacidad de los sitios web no deben infringir las leyes de privacidad, protección de datos u otras leyes de derechos humanos. En ese sentido, cuando el investigador hace uso de las redes sociales para generar resultados de investigación, debe asegurar que se ajuste a estos criterios, en especial cuando el consentimiento informado puede estar ausente, en cuyo caso, los científicos deben evaluar la ética de su investigación y determinar la necesidad de una reevaluación regular durante el proceso de investigación y a medida que los sitios de redes sociales evolucionan con el tiempo.

Luego de revisar los argumentos expuestos, se pudo encontrar que los autores consultados que respaldan esta posición creen que los constructores de los algoritmos tienen la responsabilidad total de la privacidad de los datos en la ciencia de datos, ya que estos profesionales deben asumir la responsabilidad de las cuestiones éticas en los proyectos de datos; además, deben proteger la privacidad de los datos de las personas al margen de las exigencias institucionales por normas profesionales; así como deben colaborar con la creación de conciencia en las empresas para promover las mejores prácticas éticas; también, consideran que los profesionales deben guiarse de los códigos deontológicos, es decir de la práctica profesional y conocimiento científico en el contexto de valores éticos y no por qué guiarse de sus intuiciones individuales.

Responsabilidad Parcial de los Constructores de los Algoritmos en la Privacidad de los Datos

En este apartado se discute la postura de los autores que argumentan que los constructores de los algoritmos tienen la responsabilidad parcial de la privacidad de los datos en la ciencia de datos.

Al respecto, Kitto y Knight (2019) sostuvieron que los constructores técnicos de sistemas tienen una responsabilidad parcial en la privacidad de los datos, ya que estos profesionales también interactúan con otros especialistas interesados en políticas, leyes y ética para informar su práctica cuando requieran apoyo. En ese sentido, los autores consideraron que un enfoque basado en virtudes podría guiar a los profesionales que construyen herramientas de análisis de aprendizaje a partir de la responsabilidad para trabajar en una implementación más aplicada en herramientas y enfoques, lo que puede ser usado para cambiar la óptica hacia la acción práctica y la razón al tomar las decisiones en el análisis de aprendizaje por parte de los constructores de sistemas.

Entre los exponentes más importantes se encuentran Drachsler y Greller, 2016, como se citó en Kitto y Knight, 2019, quienes identificaron una lista de verificación *delicate* que tiene un enfoque ético para facilitar una implementación confiable de *Learning Analytics* confiable que puede ser aplicado por investigadores, formuladores de políticas y gerentes institucionales para el análisis de aprendizaje (LA), estos son: enfoque de determinación, explicación, legítimo, involucramiento, consentimiento, anonimizar, técnico y externo.

En el estudio de Kitto y Knight (2019) se diseñó una base de datos piloto para implementar la ética práctica en el análisis de aprendizaje. Entre los hallazgos, los autores indicaron que existe una baja utilización de inteligencia artificial y el análisis de datos cuando los administradores buscan evitar el riesgo, por ende, proponen una base de datos

abierta (piloto) que enumera los casos extremos que enfrentan los constructores de sistemas de o *analytics* como método para guiar en ética a los especialistas que trabajan en el campo de la ciencia de datos para informar su práctica y abordar los problemas, lo cual sería un espacio intermedio en el que los constructores técnicos de sistemas podrían interactuar más con los expertos interesados en políticas, leyes y ética.

En la misma línea, Chalcraft (2018) argumenta que los profesionales de la información son los que deben hacer comprender a las organizaciones sobre las implicaciones y los riesgos relacionados con la información y el análisis de datos, además, las organizaciones deben establecer nuevas políticas y procedimientos de análisis de datos más limitada en "consulta" con las partes interesadas para aprovechar el valor potencial de los datos recopilados.

Entre los exponentes más importantes se encuentran Chessel, 2014, como se citó en Chalcraft, 2018, quienes establecieron los límites éticos (i) técnicos, (ii) legales e (iii) impuestos al análisis de datos. Esto viene a ser una serie de límites superpuestos donde la zona más estrecha es el límite ético. Es ahí donde los profesionales de la información, en particular, deben ayudar a las organizaciones a comprender las implicancias de los riesgos éticos en el análisis de datos.

En ese aspecto, Chalcraft (2018) buscó establecer límites éticos en el análisis de datos que se recopilan y analizan con herramientas y técnicas analíticas más sofisticadas por las organizaciones, los cuales generan valor a través de sus recursos de datos comerciales. Los hallazgos de la investigación revelaron que los profesionales de la información tienen un papel potencialmente importante en las organizaciones, ya que (i) pueden ayudar a las organizaciones a comprender las implicaciones y los riesgos relacionados con el análisis de

datos, (ii) realizar las buenas prácticas profesionales, (iii) crear y cumplir con el el cumplimiento de las políticas y procedimientos relevantes, (iv) colaborar con todas las partes interesadas para brindar respuesta a los problemas éticos. Los resultados también indicaron que los profesionales de la información son los administradores de los activos (de datos) de la empresa y quienes ejercen funciones en las áreas de gestión y gobierno de la información (IM). Por eso, también deben estar comprometidos en ayudar a las organizaciones para extraer valor de los datos como recurso comercial, maximizando la eficiencia de su uso y mitigando los riesgos asociados, incluidos con los riesgos relacionados con la implementación de análisis de datos.

En la misma posición, Morán (2022) también argumentaron que la privacidad de los datos depende de la subjetividad moral de los profesionales dentro de las organizaciones, por lo tanto, su responsabilidad no es total, ya que, por sus condiciones psicológicas subjetivas, dependerían de las afirmaciones que hacen como "robar datos personales es moralmente incorrecto" (Morán, 2022, p. 3). En ese sentido, se valora la privacidad porque las actitudes subjetivas pueden creer que es valiosa, un ejemplo de ello es la identidad individual que representa una información de valor para los usuarios, lo que genera que cuiden la privacidad de su identidad.

Entre los exponentes más importantes se encuentran Hesse et al., 2016, como se citó en Morán, 2022 quienes introdujeron el concepto de responsabilidad moral en los campos de *Big Data* y ciencia de datos frente a los problemas éticos, y los analiza desde una perspectiva metaética (trata los problemas considerando si los valores morales son objetivos o subjetivos), lo que permite repensar quiénes son los responsables en torno a la privacidad. Otro autor importante es Tadeo y Floridi, 2017, como se citó en Morán, 2022, quienes

justifican estos argumentos al mencionar que la responsabilidad moral será efectiva solo en la medida es que esté sustentado en un marco ético capaz de conciliar los diferentes enfoques éticos y el interés de las partes interesadas por mantener la privacidad.

En tal sentido, el estudio de Morán (2022) involucró el uso de tecnologías de Data *Science* y *Big Data*, caracterizado por el uso constante de algoritmos y distintas formas de aprendizaje automático. En el documento, se analizaron a las empresas que han adquirido *frameworks* y *clusters* dedicados al procesamiento y almacenamiento de datos y herramientas de almacenamiento en la nube. Entre los hallazgos, los autores encontraron que los principales problemas están relacionados con la responsabilidad moral, especialmente desde una perspectiva metaética, ya que los principales retos de las ciencias de la información en la era del *Big Data* son básicamente de tipo ético. En ese sentido, los retos de *Big Data* se extiende más allá de la responsabilidad individual de los profesionales de la información, siendo un problema de ética grupal; por lo tanto, requieren enfoques que permitan formular principios morales consistentes como la articulación entre su reflexión axiológica (disciplina de la filosofía que investiga los valores de las cosas), el análisis "meta ético" (analiza el origen de los principios éticos) y las prescripciones deontológicas de sus códigos de ética. Los hallazgos también permiten inferir que una estrategia más integral podría ayudar al desarrollo moral de los profesionales en las organizaciones que incluyan aspectos que van más allá de solo crear un código de ética para combatir la falta de valores morales dentro de la institución; esta estrategia integral puede considerar: cursos de formación o desarrollo moral, la figura de un consultor en temas de ética, la creación de comité de ética autónoma, la posibilidad de denunciar irregularidades de forma anónima, entre otros.

Luego de revisar los argumentos expuestos, se encontró que los autores consultados que respaldan esta posición creen que los constructores de los algoritmos tienen la responsabilidad parcial de la privacidad de los datos en la ciencia de datos, ya que consideran que los investigadores deben asumir la responsabilidad de las cuestiones éticas en los proyectos; además, tienen el deber de proteger la privacidad de los datos de las personas al margen de las exigencias institucionales por normas profesionales; así como, pueden ayudar a crear conciencia en las empresas para promover las mejores prácticas éticas. De igual manera, los profesionales no tienen por qué guiarse de sus intuiciones individuales, sino que deben guiarse de su práctica profesional y su conocimiento científico en el contexto de valores éticos (códigos deontológicos). Del mismo modo, tienen el deber profesional de manejar la ética en su investigación frente al riesgo de causar daño a los agentes involucrados; igualmente, son ellos quienes deben de explicar y hacer comprender a los gerentes sobre los modelos de ciencia de datos.

Resumen Comparativo de la Controversia Relacionada con los Constructores de los Algoritmos como Responsables de la Privacidad de los Datos

Después de lo expuesto en el presente subtema, se encuentra que la mayoría de los autores revisados respaldan la primera posición, por lo tanto, se puede considerar que los constructores de los algoritmos tienen la responsabilidad total de la privacidad de los datos en la ciencia de datos, ya que son los responsables de las cuestiones éticas de los proyectos que desarrollan y porque tienen el deber de proteger la privacidad de los datos de los propietarios al margen de las exigencias institucionales por normas profesionales. Los argumentos que justifican cada postura, se resumen en el siguiente cuadro comparativo (ver Tabla 4).

Tabla 4

Comparativo de la controversia relacionada con los constructores de los algoritmos como responsable de la privacidad de los datos

1. Responsabilidad Total de los Constructores en la Privacidad de Datos	2. Responsabilidad Parcial de los Constructores en la Privacidad de Datos
Estos profesionales deben asumir la responsabilidad de las cuestiones éticas en los proyectos.	No pueden ser totalmente responsables porque la privacidad de los datos depende de la subjetividad moral los investigadores.
Tienen el deber de proteger la privacidad de los datos de las personas al margen de las exigencias institucionales por normas profesionales.	Por sus condiciones psicológicas subjetivas, lo que puede ser privado para los constructores de los algoritmos no necesariamente lo es para otras personas.
Deben ayudar a crear conciencia en las empresas para promover las mejores prácticas éticas, explicar y hacer comprender a los gerentes sobre sus trabajos y los riesgos.	la responsabilidad no es completa porque los constructores técnicos tienen que interactuar con otros especialistas en ética, políticas y leyes para hacer definiciones de valores morales y alinear su práctica.
Los autores consideran que las pautas éticas profesionales y los códigos de conducta deben actualizarse, ya que solo contemplan los trabajos tradicionales.	Las empresas también son los responsables porque deben establecer nuevas políticas y procedimientos de análisis de datos considerando a las partes interesadas.
Los profesionales no deben guiarse de sus intuiciones individuales, sino de los códigos deontológicos en el contexto de los valores éticos.	Incluso, las empresas y sus gerentes comparten la responsabilidad en la privacidad de los datos.
Tienen el deber profesional de manejar la ética en su análisis frente al riesgo de causar daño a los involucrados y porque la junta de revisión ética no es suficiente.	Además, un enfoque basado en virtudes podría guiar a los profesionales que construyen herramienta de análisis de datos en una práctica más ética.

Nota. Resumen comparativo de la normativa como guía en la privacidad de los datos en la ciencia de datos. Adaptado de Hesse et al., 2019 (https://doi.org/10.1177/0002764218805806); Utts, 2021 (http://dx.doi.org/10.1111/insr.12446); Arrojo, 2019 (http://dx.doi.org/10.5294/pacla.2019.22.1.8); Monkman et al., 2018 (http://dx.doi.org/10.1080/23308249.2017.1389854); Kitto y Knight, 2019

(http://dx.doi.org/10.1111/bjet.12868); Chalcraft, 2018 (https://www.proquest.com/scholarly-journals/drawing-ethical-boundaries-data-analytics/docview/2015723271/se-2?accountid=28391); Morán, 2022 (https://doi.org/10.1016/j.heliyon.2022.e08926).

Conclusiones

Luego de revisar las cuatro posturas, se concluye que las empresas son los responsables de la privacidad en la ciencia de datos, ya que la mayoría de los autores revisados respaldan esta posición (ver Tabla 5), argumentando que (i) las empresas son los responsables de desarrollar modelos más responsables y éticos frente al riesgo de causar daño a los agentes involucrados, además son (ii) los encargados de la delegación de roles y las decisiones algorítmicas, igualmente (iii) son lo que deben incorporar políticas, herramientas y procedimientos para mantener una guía clara y firme cuando la normativa del país sea débil.

Tabla 5

Autores que Respaldan cada una de las Cuatro Posturas

Los propietarios de los datos como responsables de la privacidad de los datos en la ciencia de datos	La normativa como guía para la privacidad de los datos en la ciencia de datos	La empresa como responsable de la privacidad de los datos en la ciencia de datos	Los constructores de los algoritmos como responsables de la privacidad en la ciencia de datos
Rathinam et al. (2021)	Mühlhoff (2021)	Martín (2019)	Hesse et al. (2019)
Mittelstadt (2017)	Franzke et al. (2021)	Nnamdi et al. (2022)	Utts (2021)
Ravn et al. (2020)	Chen y Quan-Haase (2020)	Breidbach y Maglio (2020)	Arrojo (2019)
Arriagada et al. (2020)	Parti y Szigeti (2021)	Nersessian (2018)	Monkman et al. (2018)
Someh et al. (2019)	Lang et al. (2021)	Hirsch, D. (2019)	Kitto y Knight (2019)
Legewie y Nassauer (2018)	Markham et al. (2018)	Keren y Owen (2019)	Chalcraft (2018)
	Forgó et al. (2020)	Saltz y Dewar (2019)	Morán (2022)
	Ibiricu y Marja (2020)	Wiener et al. (2020)	
	Nersessian (2018)	Chalcraft (2018)	
		Herschel y Virginia (2017)	

En segundo lugar, la postura que tiene más adeptos se relaciona con la normativa en el uso de los datos, ya que sostienen que dicha normativa puede ser utilizada como guía eficaz de la privacidad en la ciencia de datos; la tercera postura, con una cantidad menor de adeptos, argumentan que los constructores de los algoritmos son los responsables de la privacidad en la ciencia de datos, ya que, por normas profesionales, estos constructores tienen el deber de proteger la privacidad de los datos de los usuarios al margen de las exigencias institucionales; en último lugar, se encuentra que los propietarios de los datos son los responsables de la privacidad en la ciencia de datos, ya que son los dueños de su información y, por lo tanto, deben tener el control de sus datos (ver Tabla 6).

Tabla 6

Resumen de las Cuatro Posturas Presentadas

Los propietarios de los datos como responsables de la privacidad en la ciencia de datos	La normativa como guía para la privacidad de los datos en la ciencia de datos	La empresa como responsable de la privacidad de los datos en la ciencia de datos	Los constructores de los algoritmos como responsables de la privacidad en la ciencia de datos
Los propietarios deben poder controlar sus datos incluso después de haber dado su consentimiento	La normativa en el uso de datos puede ser efectiva, ya que actúa como guía en la práctica responsable y ética	Las empresas son responsables de la privacidad de los datos frente al riesgo de causar daño a los agentes involucrados.	Los constructores son los responsables de la ética en la ciencia de datos, al margen de las exigencias institucionales por normas profesionales
No deben dar su información si no tienen conocimiento del uso que darán a sus datos	La normativa puede ser efectiva, pero no existen marcos legales que apliquen a toda la ciencia de datos	Son responsables de (i) la delegación de roles, (ii) la decisión algorítmica y (ii) de implementar herramientas éticas	Los constructores no deben guiarse de sus intuiciones, sino de los códigos deontológicos. Deben ayudar a crear conciencia a las empresas
Las personas pueden no ser conscientes de que será analizado su comportamiento, en cuyo caso no existiría el consentimiento informado	La normativa es efectiva cuando los valores éticos se complementan y alinean con los requisitos y restricciones legales	Dado que existe subjetividad en el modelado de ciencia de datos, las empresas deben implementar mecanismos de gestión para evitar el sesgo	Un enfoque basado en virtudes podría guiar a los profesionales que construyen herramientas de análisis de datos en una práctica más ética

Sin embargo, luego del análisis, se encuentra que la empresa no es el único responsable de la privacidad de los datos. Si bien, se determinó que la responsabilidad recae en la empresa en mayor medida, lo cierto es que se debe considerar también a las partes interesadas que van desde individuos hasta gobiernos y la sociedad, así como la normativa que tiene que ser respetada por las organizaciones para la regulación de la privacidad de los datos y los propietarios que tienen el rol determinante de gestionar y controlar su información, igualmente los constructores de los algoritmos tienen el deber de explicar y hacer comprender a los gerentes sobre los riesgos del análisis y sus consecuencias, razones por las cuales también son responsables en parte de la privacidad de los datos.

En síntesis, los autores coinciden que la privacidad de los datos es un derecho humano que tiene que ser protegido frente al riesgo de ser vulnerado en el análisis de los datos. De la misma manera, concuerdan que la normativa tiene que estar presente en todas las etapas del análisis y desarrollo de los algoritmos en la ciencia de datos; sin embargo, todavía no existen los marcos legales suficientes que apliquen a toda la ciencia de datos para que guíe a las corporaciones, el gobierno y las instituciones en sus investigaciones.

Por otro lado, también se encontraron ideas muy contrarias, ya que, en un extremo están los autores que consideran que el análisis de *Big Data* y el desarrollo de los algoritmos se pueden aprovechar para crear beneficios mutuos con todas las partes interesadas para lograr el desarrollo de la sociedad; y, en el otro extremo, están los autores que sostienen que las organizaciones deben pensar en abandonar completamente el uso del análisis, ya que no pueden proteger a las personas totalmente frente a los problemas éticos, porque los medios tecnológicos de análisis de datos pueden ser limitados para hacerlo éticamente viable.

Aun así, existen aspectos comunes en los argumentos de los autores cuando mencionan que (i) existe subjetividad en el modelado de los datos, los que deben ser

gestionados por las empresas para implementar mecanismos de gestión que les permitan enfrentar los desafíos éticos; además, cuando indican que (ii) la privacidad de los datos depende de la subjetividad moral de las personas y los constructores creando actitudes subjetivas que pueden sesgar y discriminar los datos o inclusive pueden valorar a la información de diferente forma dependiendo de sus actitudes psicológicas de valoración; asimismo, hay una similitud entre los autores cuando mencionan que (iii) las organizaciones que hacen estas investigaciones necesitan fortalecer la capacidad del personal para realizar una ciencia de datos más responsables y éticos; así como (iv) la normativa la cual presenta vacíos, lo que puede ser gestionado por las empresas creando nuevas políticas y procedimientos para el manejo de la privacidad de los datos.

Finalmente, se requieren estudios futuros para explorar en mayor profundidad sobre la responsabilidad que tiene cada uno de los actores, ya que en los artículos no se precisan las funciones que tiene cada uno ni los límites de sus responsabilidades y tampoco hay un consenso sobre lo que se entiende respecto al análisis de datos, así también se requieren nuevas investigaciones futuras para probar si los hallazgos encontrados funcionan realmente en la práctica de datos responsable.

Referencias

Arriagada, G., Gilthorpe, M., & Müller, V. (2020). The ethical imperatives of the COVID-19 pandemic: An analysis from the ethics of data. *Veritas*, (46), pp. 13-35. https://doi.org/10.4067/S0718-92732020000200013

Arrojo, M. J. (2019). Valores éticos y cambio tecnológico en la comunicación audiovisual: De la ciencia a la tecnología. *Palabra Clave, 22*(1), 171-203. http://dx.doi.org/10.5294/pacla.2019.22.1.8

Breidbach, C. F., & Maglio, P. (2020). Accountable algorithms? the ethical implications of data-driven business models. *Journal of Service Management, 31*(2), 163-185. http://dx.doi.org/10.1108/JOSM-03-2019-0073

Chalcraft, C.A. (2018). Drawing ethical boundaries for data analytics. *Information and Management, 52*(1), 18-25. Retrieved from https://www.proquest.com/scholarly-journals/drawing-ethical-boundaries-data-analytics/docview/2015723271/se-2?accountid=28391

Chen, W., & Quan-Haase Anabel. (2020). Big Data Ethics and Politics: Toward New Understandings. *Social Science Computer Review, 38*(1), 3-9. http://dx.doi.org/10.1177/0894439318810734

Herschel, R., & Virginia, M. (2017). Ethics & Big Data. *Technology in Society, 49*, 31-36. https://doi.org/10.1016/j.techsoc.2017.03.003

Hesse, A., Glenna, L., Hinrichs, C., Chiles, R., & Sachs, C. (2019). Qualitative Research Ethics in the Big Data Era. *American Behavioral Scientist, 63*(5), 560–583. https://doi.org/10.1177/0002764218805806

Hernández, R., Fernández, C., y Baptista, P. (2014). *Metodología de Investigación*. México: Mc. Graw Hill.

Hirsch, D. (2019). Data Ethics: Risk management for the algorithmic age. *Risk Management, 66*(10), 24-29. Retrieved from https://www.proquest.com/scholarly-journals/data-ethics-risk-management-algorithmic-age/docview/2344525577/se-2?accountid=28391

Forgó, N., Hänold, S., van den Hoven, J., Krügel, T., Lishchuk, I., Mahieu, R., Monreale, A., Pedreschi, D., Pratesi, F., & van Putten, D. (2020). An ethico-legal framework for social data science. *International Journal of Data Science and Analytics, 11*(4), 377-390. https://doi.org/10.1007/s41060-020-00211-7

Franzke, A. S., Iris, M., & Schäfer, M. T. (2021). Data Ethics Decision Aid (DEDA): a dialogical framework for ethical inquiry of AI and data projects in the Netherlands. *Ethics and Information Technology, 23*(3), 551-567. http://dx.doi.org/10.1007/s10676-020-09577-5

Ibiricu, B., & Marja Leena van, d. M. (2020). Ethics by design: A code of ethics for the digital age. *Records Management Journal, 30*(3), 395-414. http://dx.doi.org/10.1108/RMJ-08-2019-0044

Keren Naa, A. A., & Owen, R. (2019). A micro-ethnographic study of Big Data-based innovation in the financial services sector: Governance, ethics and organisational practices: JBE. *Journal of Business Ethics, 160*(2), 363-375. http://dx.doi.org/10.1007/s10551-019-04203-x

Kitto, K., & Knight, S. (2019). Practical ethics for building learning analytics. *British Journal of Educational Technology, 50*(6), 2855-2870. http://dx.doi.org/10.1111/bjet.12868

Lang, M., Lemieux, S., Hébert, J., Sauvageau, G., & Zawati, M. H. (2021). Legal and Ethical Considerations for the Design and Use of Web Portals for Researchers, Clinicians, and Patients: Scoping Literature Review. *Journal of Medical Internet Research*. http://dx.doi.org/10.2196/26450

Legewie, N., & Nassauer, A. (2018). YouTube, google, facebook: 21st century online video research and research ethics. *Forum Qualitative Sozialforschung, 19*(3). http://dx.doi.org/10.17169/fqs-19.3.3130

Markham, A. N., Katrin, T., & Herman, A. (2018). Ethics as Methods: Doing Ethics in the Era of Big Data Research—Introduction. *Social Media + Society, 4*(3). http://dx.doi.org/10.1177/2056305118784502

Martin, K. (2019). Ethical Implications and Accountability of Algorithms: JBE. *Journal of Business Ethics, 160*(4), 835-850. http://dx.doi.org/10.1007/s10551-018-3921-3

Mittelstadt, B. (2017). From Individual to Group Privacy in Big Data Analytics. *Philosophy & Technology, 30*(4), 475-494. http://dx.doi.org/10.1007/s13347-017-0253-7

Monkman, G. G., Kaiser, M., & Hyder, K. (2018). The Ethics of Using Social Media in Fisheries Research. *Reviews in Fisheries Science & Aquaculture, 26*(2), 235-242. http://dx.doi.org/10.1080/23308249.2017.1389854

Morán, A. (2022). Towards an ethical framework about Big Data era: metaethical, normative ethical and hermeneutical approaches. *Heliyon, 8*. https://doi.org/10.1016/j.heliyon.2022.e08926

Mühlhoff Rainer. (2021). Predictive privacy: Towards an applied ethics of data analytics. *Ethics and Information Technology, 23*(4), 675-690. http://dx.doi.org/10.1007/s10676-021-09606-x

Nnamdi, J. O., Yusuf, Y. Y., Dharma, K., & Mercangoz, B. A. (2022). Big Data supply chain analytics: ethical, privacy and security challenges posed to business, industries and society. *Production Planning & Control, 33*(2-3), 123-137. http://dx.doi.org/10.1080/09537287.2020.1810764

Nersessian, D. (2018). The law and ethics of Big Data analytics: A new role for international human rights in the search for global standards. *Business Horizons, 61*(6), pp. 845-854. https://doi.org/10.1016/j.bushor.2018.07.006

Parti, K., & Szigeti, A. (2021). The Future of Interdisciplinary Research in the Digital Era: Obstacles and Perspectives of Collaboration in Social and Data Sciences - An Empirical Study. *Cogent Social Sciences, 7*(1). http://dx.doi.org/10.1080/23311886.2021.1970880

Rathinam, F., Khatua, S., Siddiqui, Z., Malik, M., Duggal, P., Watson, S., & Vollenweider, X. (2021). Using Big Data for evaluating development outcomes: A systematic map. *Campbell Systematic Reviews, 17*(3). http://dx.doi.org/10.1002/cl2.1149

Ravn, S., Barnwell, A., & Barbara, B. N. (2020). What is "Publicly available data"? exploring blurred Public–Private boundaries and ethical practices through a case study on instagram. *Journal of Empirical Research on Human Research Ethics, 15*(1-2), 40-45. http://dx.doi.org/10.1177/1556264619850736

Real Academia Española. (2022). *Responsabilidad*. RAE. https://dle.rae.es/responsabilidad?m=form

Saltz, J. S., & Dewar, N. (2019). Data science ethical considerations: A systematic literature review and proposed project framework. *Ethics and Information Technology, 21*(3), 197-208. http://dx.doi.org/10.1007/s10676-019-09502-5

Someh, I., Davern, M., Breidbach, C. F., & Shanks, G. (2019). Ethical Issues in Big Data Analytics: A Stakeholder Perspective. *Communications of the Association for Information Systems, 44*, 34. http://dx.doi.org/10.17705/1CAIS.04434

Utts, J. (2021). Enhancing data science ethics through statistical education and practice. *International Statistical Review = Revue Internationale De Statistique, 89*(1), 1-17. http://dx.doi.org/10.1111/insr.12446

Wiener, M., Saunders, C., & Marabelli, M. (2020). Big-data business models: A critical literature review and multiperspective research framework. *Journal of Information Technology, 35*(1), 66-91. http://dx.doi.org/10.1177/0268396219896811

Anexos

Anexo 1. Entregable 1

MATRIZ 1 - RESUMEN POR FUENTE SELECCIONADA

#	TÍTULO	REFERENCIA	RESUMEN	IDEAS PRINCIPALES	POSTURA	RELEVANCIA
1	Using big data for evaluating development outcomes: A systematic map	Rathinam, F., Khatua, S., Siddiqui, Z., Malik, M., Duggal, P., Watson, S., & Vollenweider, X. (2021). Using big data for evaluating development outcomes: A systematic map. Campbell Systematic Reviews, 17(3)http://dx.doi.org/10.1002/cl2.1149	Big data tiene utilidad para abordar temas de relevancia para el desarrollo internacional, así como son más relevantes para la sostenibilidad ambiental, el desarrollo urbano, el bienestar y la salud, el desarrollo económico y los medios de vida. Desde este punto de vista, los resultados también revelan la existen varios desafíos analíticos, éticos y logísticos que pueden dificultar el uso de macrodatos en las evaluaciones (calidad de datos, transparencia, intercambio de datos, privacidad, validez de construcción y generalización). Además, destaca el potencial de los grandes datos en contextos frágiles: como la propagación de enfermedades, la violencia, las calamidades naturales y los terrenos difíciles. Finalmente, el estudio concluye que los investigadores deben mejorar su información sobre la calidad, la ética y la transparencia de los datos, los que deben dirigir mayores esfuerzos para establecer las mejores prácticas y estándares en materia de privacidad de datos y ética en general para facilitar una mayor interacción entre los científicos de teledetección, los analistas de big data y los investigadores o evaluadores del desarrollo.	1. Big data. 2. Privacidad de datos.	Las personas deben tener conocimiento de la aplicación de sus datos y no deben dar su información detallada sin su conocimiento, en cuyo caso, los usuarios pueden activar y configurar sus propios perfiles, tener la capacidad de desarrollarlos y actualizarlos constantemente. Este tipo de consentimiento informado puede estar completamente presente en la investigación para solicitar el permiso de los usuarios.	ALTO
2	From Individual to Group Privacy in Big Data Analytics	Mittelstadt, B. (2017). From Individual to Group Privacy in Big Data Analytics. Philosophy & Technology, 30(4), 475-494. http://dx.doi.org/10.1007/s13347-017-0253-7	El texto habla sobre la identidad de los grupos ad hoc la cual consiste en las clasificaciones y reglas construidas por un sistema de clasificación algorítmica, junto con predicciones de preferencias y comportamientos colectivos que no necesariamente se alinea con atributos ya protegidos por la ley de privacidad. Estos grupos ad hoc construidos algorítmicamente también deberían tener sus intereses en la privacidad al administrar la identidad del grupo, por lo tanto, es necesario centrar un derecho de privacidad en la integridad de la identidad compuesta (así como la privacidad individual), ya que producen brechas. La privacidad grupal se propone como un tercer interés a equilibrar junto con la privacidad individual y los beneficios de clasificación, ya que el derecho de un individuo como el de un grupo pueden verse violados cuando la identidad del sujeto se elabora sin el consentimiento ni la conciencia del individuo ni del grupo, por lo tanto, los miembros del grupo deberían poder supervisar si se acepta o no la clasificación algorítmica. En conclusión, se debe implementar mecanismos para proteger los intereses de privacidad de los grupos independientemente de los intereses de los miembros individuales, esto como una forma de corregir el desequilibrio creado por el aumento de análisis de datos.	1. Privacidad de datos. 2. Big Data. 3. Análisis de grandes datos. 4. Ética de la información. 5. Grupos ad hoc (son grupos creados por un tercero que vincula a un conjunto de individuos de acuerdo con las similitudes percibida)	El autor considera que los individuos y los miembros del grupo deben dar su consentimiento ante los cambios de su identidad para ver si se acepta o no la clasificación algorítmica (al evaluar la aceptabilidad ética de las plataformas de análisis), sino se viola el derecho a la privacidad.	ALTO
3	What Is "Publicly Available Data"? Exploring Blurred Public–Private Boundaries and Ethical Practices Through a Case Study on Instagram	Ravn, S., Barnwell, A., & Barbara, B. N. (2020). What is "Publicly available data"? exploring blurred Public–Private boundaries and ethical practices through a case study on instagram. Journal of Empirical Research on Human Research Ethics, 15(1-2), 40-45. doi: http://dx.doi.org/10.1177/1556264619850736	Analizan los datos disponibles públicamente en las redes sociales y los casos donde los enfoques éticos con limitantes para proponer un enfoque más considerado en las personas para reproducir y usar datos en dichas plataformas. En ese sentido, el autor considera que los datos disponibles públicamente en instagram (por ejemplo, imágenes), no por ser públicos, pueden ser usados para tomar decisiones sin consentimiento de las personas.	1. La ética en las redes sociales. 2. Privacidad de datos	El autor considera que antes de reproducir y representar el contenido de las personas se debe pedir el consentimiento al usuario para proponer un enfoque más considerado en las personas para reproducir y usar datos en dichas plataformas. En ese sentido, el autor considera que los datos disponibles públicamente en instagram (por ejemplo, imágenes), no por ser públicos, pueden ser usados para tomar decisiones sin consentimiento de las personas.	MODERADO
4	The ethical imperatives of the COVID-19 pandemic: An analysis from the ethics of data	Arriagada, G., Gilthorpe, M., & Müller, V. (2020). The ethical imperatives of the COVID-19 pandemic: An analysis from the ethics of data. Veritas, (46), pp. 13-35. https://doi.org/10.4067/S0718-92732020000200013	El estudio revela las preocupaciones a nivel social preexistentes sobre los problemas éticos y sus implicancias en las empresas basadas en datos, incluida la privacidad, la vigilancia, la transparencia y la responsabilidad. Además, demuestra que los problemas actuales se han magnificados debido a la pandemia del COVID-19. Estos imperativos éticos presentan dos áreas principales de desarrollo, uno relacionado con cuestiones de confianza y responsabilidad, así como la privacidad, manejo de datos y transparencia; la otra área considera temas de justicia, del trato justo, la discriminación y la desigualdad social. Bajo este escenario, la ética de los datos revela la necesidad de un papel normativo que aborde la necesidad de soluciones basadas en datos y la implementación de su uso alineado a la ética para el desarrollo de sociedades técnicas, inclusivas y pluralistas	1. Ética en el uso de datos. 2. Privacidad de datos. 3. Normativa en el uso de datos	Los autores mencionan que es importante que las personas estén enteradas del uso que les dan a sus datos y estos tienen que estar protegidos, incluso los datos seudonimizados es información personal, ya que puede tener elementos de riesgos para la reidentificación como es una dirección IP, dado que actúa como un identificador de perfil y, por lo tanto, constituye como información personal.	ALTO
5	Ethical Issues in Big Data Analytics: A Stakeholder Perspective	Someh, I., Davern, M., Breidbach, C. F., & Shanks, G. (2019). Ethical Issues in Big Data Analytics: A Stakeholder Perspective. Communications of the Association for Information Systems, 44, 34. http://dx.doi.org/10.17705/1CAIS.04434	Proporciona una perspectiva de las partes interesadas sobre el análisis de big data y lo define como un proceso social que surge de las interacciones entre múltiples partes interesadas (individuos, organizaciones y sociedad). Se usa la ética del discurso como guía para analizar la ética del análisis de big data. En tanto, de acuerdo con la teoría de las partes interesadas, los individuos como las sociedades necesitan aumentar su importancia en las interacciones con las organizaciones, en ese caso, las personas deben participar activamente en el desarrollo de principios y lineamientos para asegurar que las sociedades establezcan regulaciones y leyes con sanciones efectivas cuando se vulneran los derechos de las personas sobre la privacidad de los datos. En ese sentido, el análisis de big data influye en la sociedad y la sociedad misma puede controlarla y moldearla de una manera que beneficie a todas las partes interesadas de una forma justa y equilibrada. En resumen, el estudio propone basarse en la ética del discurso y la teoría de las partes interesadas para abordar los problemas éticos que surgen cuando las organizaciones recopilan, analizan, comparten o venden "datos" de individuos sin el consentimiento o conocimiento genuino de los individuos.	1. Big Data. 2. Algoritmos. 3. Estudio Delphi. 4. Privacidad de datos. 5. Teoría de las partes interesadas. 6. Éticas en el análisis de big data.	Los autores consideran que todas las partes interesadas deben poder participar por igual en un discurso ético, cuestionar y reclamar cuando surgen problemas éticos y son las personas quienes deben poder controlar qué datos recopilan y agregan las organizaciones sobre ellos y quiénes tendrán acceso a sus datos, incluso deben poder hacer esto después de haber dado su consentimiento para que las organizaciones recopilen y compartan sus datos.	ALTO
6	YouTube, Google, Facebook: 21st Century Online Video Research and Research Ethics	Legewie, N., & Nassauer, A. (2018). YouTube, google, facebook: 21st century online video research and research ethics. Forum Qualitative Sozialforschung, 19(3) doi:http://dx.doi.org/10.17169/fqs-19.3.3130	Las personas no son conscientes de que su comportamiento será analizado por los investigadores y, por lo tanto, no existe el consentimiento informado, ya que es posible que las personas representadas en un video no sepan o no den su consentimiento para que se publique un video en línea en las plataformas para compartir videos (Instagram, YouTube, GeoCam, etc.)	1. Privacidad de datos, 2. Aspectos legales.	Los autores consideran que los usuarios deben elegir la opción de participar o no en la investigación de videos en línea desde una perspectiva ética, ya que es posible que estas personas no sean conscientes de que su comportamiento será analizado por los investigadores y, por lo tanto, no existe el consentimiento informado, ya que es posible que las personas representadas en un video no sepan o no den su consentimiento para que se publique un video en línea en las plataformas para compartir videos (Instagram, YouTube, GeoCam, etc.)	MODERADO
7	Predictive privacy: towards an applied ethics of data analytics	Mühlhoff Rainer. (2021). Predictive privacy: Towards an applied ethics of data analytics. Ethics and Information Technology, 23(4), 675-690. doi: http://dx.doi.org/10.1007/s10676-021-09606-x	Se explora el análisis predictivo que desafía los principios éticos como la dignidad humana y la privacidad individual. Además, introduce el concepto de "privacidad predictiva" como principio ético que está siendo amenazado por el análisis predictivo, por lo que sugiere abandonar el uso de dicho análisis, ya que los medios tecnológicos son limitados para abordar los principios éticos; en consecuencia, considera que los individuos son despojados de su autonomía y dignidad.	1. La ética en los sistemas predictivos. 2. Privacidad predictiva.	El autor considera que una regulación efectiva y más estricta centradas en los principios éticos puede ser más adecuada para la gestión de la privacidad de datos en los análisis predictivos, incluso si no se cumple con ello, se debería abandonar el uso del análisis predictivo, ya que los medios tecnológicos son limitados para poder abordar el tema ético en el análisis de datos.	ALTO
8	Data Ethics Decision Aid (DEDA): a dialogical framework for ethical inquiry of AI and data projects in the Netherlands	Franzke, A. S., Iris, M., & Schäfer, M. T. (2021). Data Ethics Decision Aid (DEDA): a dialogical framework for ethical inquiry of AI and data projects in the Netherlands. Ethics and Information Technology, 23(3), 551-567. http://dx.doi.org/10.1007/s10676-020-09577-5	El estudio se enfoca en un marco de ayuda para la toma de decisiones de ética de datos (DEDA), la cual es una herramienta eficaz y útil para la evaluación ética de proyectos de datos y para la creación de conciencia sobre cuestiones éticas en las prácticas de datos como un proceso efectivo para moderar la deliberación de casos y avanzar en el desarrollo de prácticas responsables en la ciencia de datos.	1. Ética de datos para la toma de decisiones. 2. El marco DEDA. 3. Ley de privacidad y las regulaciones de gestión de datos.	El autor argumenta que un marco regulatorio de ayuda para la toma de decisiones de ética de datos (DEDA) es un proceso útil para la evaluación ética de proyectos de datos, ya que ayuda crear conciencia sobre cuestiones éticas en las prácticas de datos.	ALTO
9	Big Data Ethics and Politics: Toward New Understandings	Chen, W., & Quan-Haase Anabel. (2020). Big Data Ethics and Politics: Toward New Understandings. Social Science Computer Review, 38(1), 3-9. http://dx.doi.org/10.1177/0894439318810734	Los investigadores encuentran controversias en torno a la política y la ética de los datos, eso ha generado que, la práctica de usar un acuerdo de confidencialidad sea aplicado en muchos países a través de contratos legales diseñado para brindar protección de datos y privacidad corporativa centradas en los usuarios y sus necesidades de privacidad. Asimismo, en el estudio se detecta la necesidad de desarrollar algoritmos culturalmente apropiados y socialmente sensibles para crear un conocimiento local en comunidades marginadas.	1. Big Data. 2. Política en el manejo de datos. 3. Ética de los datos	El autor sugiere que las corporaciones, el gobierno y las instituciones deben manejar políticas y fuentes claras en torno a la ética de los datos para evitar las controversias.	ALTO

#	TÍTULO	REFERENCIA	RESUMEN	IDEAS PRINCIPALES	POSTURA	RELEVANCIA
10	The Future of Interdisciplinary Research in the Digital Era: Obstacles and Perspectives of Collaboration in Social and Data Sciences - An Empirical Study	Parti, K., & Szigeti, A. (2021). The Future of Interdisciplinary Research in the Digital Era: Obstacles and Perspectives of Collaboration in Social and Data Sciences - An Empirical Study. Cogent Social Sciences, 7(1)http://dx.doi.org/10.1080/23311886.2021.1970880	En resumen, es importante la colaboración interdisciplinaria para analizar, sintetizar y armonizar los vínculos entre disciplinas en un todo coordinado y coherente para trabajar juntos en equipos interdisciplinarios y mapear los obstáculos de la colaboración.	1. Ciencia abierta y transparencia de la investigación. 2. Big Data. 3. Equipos multidisciplinarios.	El autor considera importante desarrollar lineamientos y prácticas éticas, que tomen en cuenta las características del big data, así como es importante la colaboración interdisciplinaria para analizar, sintetizar y armonizar los vínculos entre disciplinas en un todo coordinado y coherente para trabajar juntos en equipos interdisciplinarios y mapear los obstáculos de la colaboración.	MODERADO
11	Legal and Ethical Considerations for the Design and Use of Web Portals for Researchers, Clinicians, and Patients: Scoping Literature Review	Lang, M., Lemieux, S., Hébert, J., Sauvageau, G., & Zawati, M. H. (2021). Legal and Ethical Considerations for the Design and Use of Web Portals for Researchers, Clinicians, and Patients: Scoping Literature Review. Journal of Medical Internet Research, http://dx.doi.org/10.2196/26450	El artículo brinda un alcance sobre el potencial de desarrollo y la implementación de los portales terapéuticos, que son webs para compartir hallazgos de investigación en salud entre médicos, investigadores y pacientes. Estos portales podrían ayudar a promover el crecimiento de la medicina de precisión. Para el uso de estos portales se determinaron cinco desafíos legales y éticos (privacidad y confidencialidad, capacitación, equidad, alfabetización y toma de decisiones) para el uso de los portales web en la atención clínica.	1. Portales Web. 2. Ética médica. 3. Privacidad y confidencialidad.	Consideran que deben implementarse marcos de políticas para administrar las funciones de los portales con respecto a la privacidad, pero todavía no se han adoptado ampliamente, pese a que otros autores respaldan la opinión de que estos tipos de portales son muy prometedores para compartir hallazgos de investigación en salud entre médicos, investigadores y pacientes.	MODERADO
12	Ethics as Methods: Doing Ethics in the Era of Big Data Research—Introduction	Markham, A. N., Katrin, T., & Herman, A. (2018). Ethics as Methods: Doing Ethics in the Era of Big Data Research—Introduction. Social Media + Society, 4(3)http://dx.doi.org/10.1177/2056305118784502	Los autores encontraron que los regímenes de ética estarán desajustados en la medida que las normas de ética de la investigación y los marcos conceptuales respondan a las condiciones de generación de conocimiento algorítmico, la investigación de big data y la investigación existente. Además, resaltaron que no todo lo que se puede recolectar debe de serlo y que la visualización de datos tiene su propia política y amplios problemas éticos, muy a pesar de que el almacenamiento de datos y el intercambio de códigos son bien aceptados en la investigación social como una herramienta de mayor validez y confiabilidad	1. Responsabilidad y sostenibilidad de la ciencia de datos. 2. Privacidad y protección de datos. 3. Política y marco regulatorio y legal. 4. Algoritmos	El autor considera que las normas de la ética de la investigación y los marcos conceptuales del conocimiento algorítmico deben ajustarse para definir y hacer operativa una ciencia de datos basada en la responsabilidad y sostenibilidad.	MODERADO
13	An ethico-legal framework for social data science	Forgó, N., Hänold, S., van den Hoven, J., Krügel, T., Lishchuk, I., Mahieu, R., Monreale, A., Pedreschi, D., Pratesi, F., & van Putten, D. (2020). An ethico-legal framework for social data science. International Journal of Data Science and Analytics, 11(4), 377-390. https://doi.org/10.1007/s41060-020-00211-7	Los autores concluyen que los requisitos y restricciones legales se deben complementar con los valores éticos y legales. Se concluye que, resolver problemas sociales es el foco para la legitimidad de la ciencia de big data, pero también lo es el cumplimiento de los valores morales fundamentales para que las personas puedan depositar en la ciencia de datos y en las aplicaciones de la investigación de big data, toda su confianza (confianza garantizada) si se llegan a complementar estas dos condiciones (valores éticos y requisitos y restricciones legales).	1. Privacidad de datos, tales como: la privacidad, la seguridad, la equidad, la igualdad, la dignidad humana y la autonomía. 2. Normativa de los datos	Los autores consideran que los valores morales como la privacidad deben complementarse con los requisitos y restricciones legales en la ciencia de datos, lo que puede generar una confianza garantizada por parte de los usuarios.	MODERADO
14	Ethics by design: a code of ethics for the digital age	Ibiricu, B., & Marja Leena van, d. M. (2020). Ethics by design: A code of ethics for the digital age. Records Management Journal, 30(3), 395-414. http://dx.doi.org/10.1108/RMJ-08-2019-0044	Se considera que un marco ético alineado con la legislación de protección de datos, fácil de aplicar y conciso garantiza que los empleados involucrados respeten el código de conducta. Por ello, se busca integrar la ética en las primeras etapas del diseño de procesos y tecnologías.	1. Normativa y legislación de protección de datos. 2. Ética empresarial por diseño en la era tecnológica. 3. Privacidad y gobierno de datos:	El autor considera que la legislación de protección de datos se debe alinear con un marco ético. Asimismo, indica que son las empresas quienes deben desarrollar sistemas de valores y código de conducta para que el comportamiento ético se aplique en la tecnología. Además, indica que la legislación y las normas son esenciales para proteger y respetar las normas éticas, los derechos humanos, la libertad y la privacidad. Por último, la tecnología, la ley y la ética deben coordinar para generar confianza en los individuos.	ALTO
15	The law and ethics of big data analytics: A new role for international human rights in the search for global standards	Nersessian, D. (2018). The law and ethics of big data analytics: A new role for international human rights in the search for global standards. Business Horizons, 61(6), pp. 845-854. https://doi.org/10.1016/j.bushor.2018.07.006	Existe poco consenso internacional sobre qué estándares deben regir el uso de la tecnología de Big data que beneficien y que llenen el vacío con respecto al derecho internacional de los derechos humanos.	1. Big data. 2. Privacidad de datos. 3. Cultura corporativa. 4. Derechos humanos.	Los actores corporativos tienen obligaciones legales de respetar los derechos humanos en sus actividades comerciales que necesariamente se relacionan con big data.	ALTO
16	Ethical Implications and Accountability of Algorithms: JBE	Martin, K. (2019). Ethical Implications and Accountability of Algorithms: JBE. Journal of Business Ethics, 160(4), 835-850. http://dx.doi.org/10.1007/s10551-018-3921-3	El estudio se enfoca en los algoritmos como un actor importante en las decisiones éticas que influyen en la delegación de roles y la responsabilidad dentro de las organizaciones. En ese sentido, las empresas son los responsables del diseño y desarrollo del algoritmo y los desarrolladores tienen la obligación de seguir la normativa que tiene implicaciones éticas de los algoritmos.	1. Algoritmos como actor de decisiones éticas. 2. Big Data.	El autor responsabiliza a las empresas por los actos de un algoritmo incluso cuando esta organización afirma que el algoritmo es muy complicado y difícil de comprender. Por ello, declaran que las empresas son los responsables no solo de la carga y desarrollo de un algoritmo, sino también del diseño dentro de la decisión algorítmica y los desarrolladores tienen la obligación de seguir la normativa que tiene implicaciones éticas de los algoritmos.	ALTO
17	Big data supply chain analytics: ethical, privacy and security challenges posed to business, industries and society	Nnamdi, J. O., Yusuf, Y. Y., Dharma, K., & Mercangoz, B. A. (2022). Big data supply chain analytics: ethical, privacy and security challenges posed to business, industries and society. Production Planning & Control, 33(2-3), 123-137. http://dx.doi.org/10.1080/09537287.2020.1810764	Existen buenas perpectivas basadas en datos en la cadena de suministros. Además, la mayoría de los datos de la cadena de suministro no son útiles debido a su estado sin procesar y al hecho de que a menudo se mantienen cautivos dentro de los silos organizacionales.	1. Privacidad de datos. 2. Análisis de la cadena de suministro de big data (BDSCA). 3. Big Data.	Los dueños de negocios tienen la responsabilidad del cumplimiento del deber percibido de cuidar a sus clientes en una economía global ciberfísica interconectada en la recopilación y síntesis de datos.	ALTO
18	Accountable algorithms? The ethical implications of data-driven business models	Breidbach, C. F., & Maglio, P. (2020). Accountable algorithms? the ethical implications of data-driven business models. Journal of Service Management, 31(2), 163-185. doi: http://dx.doi.org/10.1108/JOSM-03-2019-0073	La investigación integra las perspectivas desconectadas sobre los servicios de tecnología, la ética en los datos, la ética comercial y los modelos comerciales basado en datos. A partir de dicho enfoque, el autor presenta un marco analítico novedoso sustentado en los modelos comerciales. Demuestra que el algoritmo, la inteligencia artificial (IA) y los conjuntos de datos grandes pueden ser poco éticos, pudiendo generar pérdidas de privacidad, manipulación directa, entre otros indicados por el autor. En ese sentido, el modelo novedoso centrado en modelos comerciales redefine el valor, ya que conllevan la aparición de nuevos modelos y alternativas de valor en base a los datos.	1. Algoritmos: el uso sin restricciones, incorrecto o no regulado de la IA, el aprendizaje automático, entre otros análisis de datos avanzados pueden generar comportamientos poco éticos en las organizaciones. 2. Modelos comerciales propuesto por los autores para el uso efectivo y ético de los datos.	Las empresas solo deben implementar herramientas de toma de decisiones algorítmicas siempre que el resultado de sus decisiones no afecte de manera ética a los clientes u otras partes interesadas. Por lo tanto, también deben desarrollar modelos más responsables y éticos.	MODERADO
19	Data Ethics: Risk Management for the Algorithmic Age	Hirsch, D. (2019). Data Ethics: Risk management for the algorithmic age. Risk Management, 66(10), 24-29. Retrieved from https://www.proquest.com/scholarly-journals/data-ethics-risk-management-algorithmic-age/docview/2344525577/se-2?accountid=28391	El análisis de big data puede dañar a las personas en al menos tres formas importantes: invasión de la privacidad, manipulación y sesgo; además, el análisis big data representa un riesgo continuo de invasión a la privacidad, pero muchas empresas no conocen completamente estos riesgos comerciales. Por ejemplo, las personas ya no pueden solo aceptar las políticas de consentimiento a la privacidad para protegerse, puesto que las empresas no pueden protegerlas simplemente cumpliendo con las leyes de privacidad, sino que exige ir más allá de la ley.	1. Riesgo de privacidad. 2. Uso de análisis de big data. Aprendizaje automático - Algoritmo.	El autor sugiere que las empresas son los responsables de gestionar el riesgo para garantizar que sus actividades de análisis de datos no invadan la privacidad o manipulen a las personas.	ALTO
20	A Micro-ethnographic Study of Big Data-Based Innovation in the Financial Services Sector: Governance, Ethics and Organisational Practices: JBE	Keren Naa, A. A., & Owen, R. (2019). A micro-ethnographic study of big data-based innovation in the financial services sector: Governance, ethics and organisational practices: JBE. Journal of Business Ethics, 160(2), 363-375. doi: http://dx.doi.org/10.1007/s10551-019-04203-x	Las innovaciones basadas en Big Data pueden tener vacíos de gobernanza , en cuyo caso se sustentan en valores y principios relativos a la privacidad y seguridad de los datos que las empresas del sector financiero han internalizado en sus propias políticas y operaciones.	1. Big data. 2. Normativa de datos y legislación. 3. Privacidad de datos.	Considera que son las empresas las que deben comprometerse con las cuestiones de privacidad del usuario, consentimiento y uso secundario de los datos, en cuyo caso han internalizado en sus propias políticas y operaciones.	ALTO
21	Data science ethical considerations: a systematic literature review and proposed project framework	Saltz, J. S., & Dewar, N. (2019). Data science ethical considerations: A systematic literature review and proposed project framework. Ethics and Information Technology, 21(3), 197-208. http://dx.doi.org/10.1007/s10676-019-09502-5	El estudio describe los principales temas éticos a partir de la revisión sistemática de la literatura y propone una posible estructura para integrar dichos temas dentro de un proyecto de ciencia de datos. Como resultado, el estudio identificó los desafíos éticos clave en la ciencia de datos, los cuales son: la necesidad de un marco ético, la novedad del campo, los desafíos relacionados con los datos y los desafíos relacionados con el modelo de análisis.	1. Ciencia de datos para la toma de decisiones. 2. Uso de algoritmo.	Sostiene que dentro del modelado de ciencia de datos existe subjetividad, esto puede ser gestionado por las empresas para implementar mecanismos de gestión que les permitan enfrentar los desafíos éticos en la ciencia de datos.	ALTO

#	TÍTULO	REFERENCIA	RESUMEN	IDEAS PRINCIPALES	POSTURA	RELEVANCIA
22	Big-data business models: A critical literature review and multiperspective research framework	Wiener, M., Saunders, C., & Marabelli, M. (2020). Big-data business models: A critical literature review and multiperspective research framework. Journal of Information Technology, 35(1), 66-91. http://dx.doi.org/10.1177/0268396219896811	El big data ofrece a las organizaciones la oportunidad de obtener y mantener una ventaja competitiva, haciendo uso de los modelos comerciales de grandes datos para generar una integración vertical dentro de la cadena de suministros en la medida que recopilan, almacenan, administran y procesan los datos.	1. Big data. 2. Modelos comerciales de big data.	El autor considera que entornos organizacionales los modelos de negocio de big data integran entornos más amplios que incluyen varios grupos de partes interesadas que van desde individuos hasta gobiernos y la sociedad. Un ejemplo de ello, es la influencia legislativa que puede permitir o restringir los usos de big data en materia de privacidad.	MODERADO
23	Ethics & Big Data	Herschel, R., & Virginia, M. (2017). Ethics & Big Data. Technology in Society, 49, 31-36. https://doi.org/10.1016/j.techsoc.2017.03.003	Se revisan cuatro teorías éticas: el kantianismo, el utilitarismo, la teoría del contrato social y la teoría de la virtud, y se examina cada teoría para mostrar cómo podría emplearse para examinar los problemas de Big Data.	1. Big data. 2. Privacidad de datos. 3. Teoría de la virtud.	Las empresas deben asegurar la privacidad de los datos de las personas. Algunas organizaciones brindan a sus clientes la opción de excluir su información para que no sea compartida con los socios comerciales de la empresa.	ALTO
24	Qualitative Research Ethics in the Big Data Era	Hesse, A., Glenna, L., Hinrichs, C., Chiles, R., & Sachs, C. (2019). Qualitative Research Ethics in the Big Data Era. American Behavioral Scientist, 63(5), 560–583. https://doi.org/10.1177/0002764218805806	El estudio considera que el Big Data ha cambiado el panorama de la investigación y las ciencias sociales, por ese motivo, presenta cinco principios rectores para que los investigadores cualitativos y sus instituciones consideren al visualizar prácticas y pautas futuras dentro de esta investigación cambiante y emergente, siendo: i) valorar la diversidad metodológica; (ii) fomentar la investigación para que tengan en cuenta el contexto, la especificidad y las poblaciones marginadas; (iii) abordar dilemas éticos y no solo ver las preocupaciones legales; (iv) atención a las diferencias regionales y disciplinarias; y (v) considerar todo el ciclo de vida de la investigación, incluyendo su vida futura en los archivos o instalaciones de datos abiertos.	1. Big Data. 2. Investigación cualitativa. 3. Privacidad de los datos. 4. Ética de la investigación.	Los autores mencionan que los investigadores deben proteger la privacidad de los datos de las personas al margen de las exigencias institucionales por normas profesionales. Un ejemplo de ello, es cuando los usuarios de las redes sociales pueden no darse cuenta completamente de cómo las empresas o los mismos investigadores pretenden utilizar su información, de hecho, otros autores han descubierto que los acuerdos de usuario para datos confidenciales muy escasa vez se leen. En ese aspecto, también puede ser poco razonable solicitar a los investigadores que obtengan el consentimiento de todas las personas que publican un tuit en redes sociales, por ejemplo.	ALTO
25	Enhancing data science ethics through statistical education and practice	Utts, J. (2021). Enhancing data science ethics through statistical education and practice. International Statistical Review = Revue Internationale De Statistique, 89(1), 1-17. doi:http://dx.doi.org/10.1111/insr.12446	Se analizan los problemas que afectan a la ciencia de datos éticos, bajo el enfoque de los estadísticos, quienes pueden ayudar a crear conciencia y fomentar las mejores prácticas éticas ante los abusos de algoritmos y análisis de datos complejos que impacta en la sociedad.	1. Privacidad de los datos ante los problemas éticos. 2. Algoritmos y análisis de datos complejos	Corresponde a los estadísticos y los científicos de datos asumir la responsabilidad de las cuestiones éticas en los proyectos, siendo ellos quienes pueden ayudar a crear conciencia y promover las mejores prácticas ante los problemas éticos relacionados con la privacidad de datos que afectan a la ciencia de datos.	ALTO
26	Valores éticos y cambio tecnológico en la comunicación audiovisual: De la ciencia a la tecnología	Arrojo, M. J. (2019). Valores éticos y cambio tecnológico en la comunicación audiovisual: De la ciencia a la tecnología. Palabra Clave, 22(1), 171-203. http://dx.doi.org/10.5294/pacla.2019.22.1.8	Explora la dimensión científica de la ciencia de la comunicación audiovisual y la faceta tecnológica de apoyo para posibilitar la transmisión de la comunicación en razón de la ciencia, con el fin de diferenciar la tecnología de la realidad, es que aquí se transforma lo real y se lleva al mundo creativo usando la tecnología lo cual debe ser cuidadosamente pensada aplicando la ética para no dañar los valores intangibles (la imagen pública, la familia, el prestigio, la honestidad, etc.). Esto exige atender a las dimensiones habitualmente no contempladas como endógenas y exógenas, ya que tienen que ver con la ética, siendo la segunda dimensión más visible y tiene la mayor atención. Es decir, en la actualidad todo el énfasis está puesto en la ética de la información como estudio de la faceta extrínseca de los fenómenos comunicativos.	1. Valores éticos en la tecnología y como aplicación de la ciencia de la comunicación. 2. Dimensiones endógenas y exógenas. 3. Los componentes éticos de la tecnología en la comunicación.	Indican que los agentes de la comunicación y tecnología (los profesionales) no tienen por qué guiarse por sus intuiciones individuales o por las socialmente aceptadas, sino que deben guiarse de los códigos deontológicos, es decir de una práctica profesional y conocimiento científico en el mercado de los valores éticos. Estos códigos deontológicos resuelven problemas de respeto de licencia de privacidad, de buena imagen, derecho a la intimidad, etc.	MODERADO
27	The Ethics of Using Social Media in Fisheries Research.	Monkman, G. G., Kaiser, M., & Hyder, K. (2018). The Ethics of Using Social Media in Fisheries Research. Reviews in Fisheries Science & Aquaculture, 26(2), 235-242. http://dx.doi.org/10.1080/23308249.2017.1389854	La industria pesquera debe reevaluar continuamente la ética de su investigación en las redes sociales, ya que la orientación de las juntas de revisión ética actualmente puede ser limitadas y toda la actividad de extracción de contenido de Internet debe realizarse de manera responsable para que los datos personales no se vean comprometidos.	1. Uso de datos de las redes sociales. 2. Ética de la investigación en las redes sociales.	El autor cree que los investigadores tienen el deber profesional de manejar la ética en su investigación frente al riesgo de causar daño a los agentes involucrados, ya que las juntas de revisión ética actualmente pueden ser limitadas y toda la actividad de extracción de contenido de Internet debe realizarse de manera responsable para que los datos personales no se vean comprometidos.	MODERADO
28	Practical ethics for building learning analytics.	Kitto, K., & Knight, S. (2019). Practical ethics for building learning analytics. British Journal of Educational Technology, 50(6), 2855-2870. http://dx.doi.org/10.1111/bjet.12868	Existe baja utilización de inteligencia artificial y el análisis de datos cuando los administradores buscan evitar el riesgo, como al uso indebido de los datos. Por lo tanto, se propone una base de datos abierta (piloto) que enumera los casos extremos que enfrentan los constructores de sistemas de "Analytics" como método para guiar en ética a los especialistas que trabajan en el campo de la ciencia de datos para informar su práctica. Sería un espacio intermedio en el que los constructores técnicos de sistemas podrían interactuar más con los interesados en políticas, leyes y ética.	1. Privacidad de datos . 2. Legislación en el uso de los datos.	El autor considera que los constructores técnicos de sistemas podrían interactuar más con los especialistas en ética para informar su práctica cuando requieran apoyo. Sería un espacio intermedio en el que los constructores técnicos de sistemas podrían interactuar más con los interesados en políticas, leyes y ética.	ALTO
29	Drawing Ethical Boundaries for Data Analytics	Chalcraft, Jennette,C.P.A., C.A. (2018). Drawing ethical boundaries for data analytics. Information and Management, 52(1), 18-25. Retrieved from https://www.proquest.com/scholarly-journals/drawing-ethical-boundaries-data-analytics/docview/2015723271/se-2?accountid=28391	El estudio se enfoca a establecer límites éticos en el análisis de datos que se recopilan y analizan con herramientas y técnicas analíticas más sofisticadas, por lo que el autor sugiere a las organizaciones establecer nuevas políticas y procedimientos de análisis de datos más limitada en "consulta" con las partes interesada para aprovechar el valor potencial de los datos recopilados.	1. Aprendizaje automático (algoritmo) y Big data. 2. Leyes y regulaciones. 3. Derechos de las personas a la privacidad.	Los profesionales de la información son los que deben hacer comprender a las organizaciones sobre las implicaciones y los riesgos relacionados con la información y el análisis de datos, además, las organizaciones deben establecer nuevas políticas y procedimientos de análisis de datos más limitada en "consulta" con las partes interesada para aprovechar el valor potencial de los datos recopilados.	ALTO
30	Towards an ethical framework about Big Data era: metaethical, normative ethical and hermeneutical approaches	Morán, A. (2022). Towards an ethical framework about Big Data era: metaethical, normative ethical and hermeneutical approaches. Heliyon, 8. https://doi.org/10.1016/j.heliyon.2022.e08926	A partir del uso diario de Big data y sus aplicaciones en diferentes ámbitos, se presentan retos éticos que se plantean a la Ciencia de la Información y no son sobre la fiabilidad de sus profesionales para realizar tareas de forma imparcial en las empresas o sobre la obligación de formarse tecnológicamente en el área de ciencia de datos. Los problemas más importantes son los que se relacionan con el concepto de responsabilidad moral, a partir de una perspectiva metaética y los retos del Big Data. El estudio indica que los desafíos del Big Data se extienden más allá que la responsabilidad individual de un profesional de las Ciencias de la Información, dado que los cambios que provocan los conjuntos masivos de datos son fundamentalmente problemas de una ética de grupo. Además, los desafíos morales en el manejo de Big Data que normalmente se suelen abordar desde la ética aplicada, los autores lo abordan como un problema de metaética y ética normativa como fundamento para su aplicación en códigos profesionales.	1. Metaética. 2. Big data. 3. Ética de la información. 4. Privacidad de datos.	Los autores mencionan que la privacidad de datos depende de la subjetividad moral de la persona que analizan los datos, de alguna manera, ya que, a través de nuestras condiciones psicológicas subjetivas, dependerían las afirmaciones como "robar datos personales es moralmente incorrecto". En ese sentido, valoramos a la privacidad porque nuestras actitudes subjetivas nos llevan a pensar que es valiosa, por ejemplo, la identidad individual representa una información valiosa para los usuarios.	ALTO

Anexo 2. Entregable 2

MATRIZ 2 – SUBTEMAS – JUSTIFICACIÓN – OBJETIVOS ESPECÍFICOS

SUBTEMA	DEFINICION / JUSTIFICACION DEL SUBTEMA	OBJETIVO
LOS PROPIETARIOS DE LOS DATOS COMO RESPONSABLES DE LA PRIVACIDAD DE LOS DATOS EN EL USO DE ALGORITMOS	Son los usuarios o grupo de usuarios quienes son dueños de los datos que se usan en la ciencia de datos. Estos individuos hacen uso personal diario (móviles, wearables, Internet de las Cosas, etc.), además constante tienen interacción social (blogs, Facebook, Twitter, WhatsApp, etc.) y en mantienen un registro digital de transacciones comerciales (transacciones electrónicas, dinero móvil, pago con tarjeta de crédito, etc.); todas estas operaciones diarias que realizan los usuarios han dado lugar a una explosión de datos recopilados automáticamente (Rathinam et al., 2021). Justificación: Las personas requieren comprender el nivel de responsabilidad que tienen ellos cuando se realizan prácticas de desarrollo de modelos analíticos que generan problemas en torno a la privacidad de sus datos. Someh et al. (2019) consideran que las personas deben poder controlar los datos que las empresas recopilan y agregan sobre ellos, además deben saber quiénes tendrán acceso a sus datos, incluso deben poder hacer esto después de haber dado su consentimiento para que las organizaciones recopilen y compartan sus datos, por ende, deberían cuestionar y reclamar cuando surgen problemas éticos. Asimismo, Ravn et al. (2020) y Mittelstadt (2017) consideran que antes de reproducir y representar el contenido de las personas se debe pedir el consentimiento al usuario para proponer un enfoque más considerado con ellos al reproducir y usar sus datos. Es por ello que este estudio permite evaluar si los propietarios de los datos son los responsables de la privacidad de su información en la ciencia de datos enfocados en los proyectos de investigación de las empresas.	Evaluar las posturas sobre la responsabilidad de los propietarios en la privacidad de sus datos en la ciencia de datos.
LA NORMATIVA COMO GUIA PARA LA PRIVACIDAD DE LOS DATOS EN EL USO DE ALGORITMOS	Se refiere a la legislación y las normas para garantizar y hacer las cumplir las normas éticas, escencialmente enfocadas a proteger y respetar los derechos humanos, la libertad y la privacidad de datos. El Reglamento General de Protección de Datos (RGPD) es actualmente la fuente de derecho mundial más importante y completa de codificar las normas de ética digital en un marco legal. El objetivo general del Reglamento es proteger a las personas en sus derechos y libertades fundamentales y, en particular, en su derecho a la protección de sus datos personales, así como de las cuestiones morales y éticas planteadas por la era de los grandes datos en el campo de la investigación (Forgó et al., 2020). Justificación: Se requiere comprender hasta qué punto la normativa, leyes y regulaciones sirven de guia o referencia para los problemas éticos en las prácticas de diseño y desarrollo de modelos analíticos cuando se ve afectado la privacidad de datos de las personas. Esta posición indica que la legislación y las normas son esenciales para proteger y respetar las normas éticas, los derechos humanos, la libertad y la privacidad (biricu & Marja, 2020). Es por ello que este estudio permite evaluar de qué manera la normativa en el uso de los datos influye en la privacidad de los datos cuando se realizan proyectos de investigación.	Evaluar de qué manera la normativa en el uso de datos influye en la privacidad de datos en la ciencia de datos.
LA EMPRESA COMO RESPONSABLE DE LA PRIVACIDAD EN EL USO DE LOS DATOS EN LOS ALGORITMOS	Esta posición plantea que las empresas son responsables de los algoritmos que desarrollan, venden y utilizan. Por lo tanto, deben ser responsables no solo de la carga de un algoritmo, sino también del diseño de la decisión algorítmica. Como tal, las empresas que desarrollan algoritmos son responsables de las implicaciones éticas de los algoritmos utilizados en la toma de decisiones y de la elección en cuanto a la delegación de tareas y responsabilidades de individuos que asignan para realizar el diseño (Martin, 2019). Justificación: Los empresarios requieren comprender cómo sus prácticas de desarrollo de modelos analíticos pueden afectar en gran medida a la privacidad de datos de las personas. Keren & Owen (2019) consideran que las deben comprometerse con las cuestiones de privacidad del usuario, consentimiento y uso secundario de los datos, en cuyo caso deben internalizar políticas y operaciones en sus decisiones de ciencia de datos. Wiener et al. (2020) creen que las organizaciones deben aprovechar los beneficios de los modelos de negocio de big data para generar una ventaja competitiva haciendo uso de los modelos comerciales de grandes datos, pero también deben hacerse responsables de gestionar el riesgo de problemas éticos para garantizar que sus actividades de análisis de datos no invadan la privacidad o manipulen a las personas (Hirsch, 2019). Es por ello que este enfoque permite evaluar en qué forma las empresas son responsables de la privacidad de datos en la ciencia de datos enfocados en proyectos de investigación.	Evaluar las posturas sobre la responsabilidad de las empresas en la privacidad de los datos en la ciencia de datos.
LOS CONSTRUCTORES DE LOS ALGORITMOS COMO RESPONSABLES DE LA PRIVACIDAD EN EL USO DE LOS DATOS	Son todas aquellas personas responsables de analizar, manejar y manipular los datos, puede ser un investigador profesional, estadístico, diseñador o desarrollador del algoritmo. Esta postura propone que estas personas deben ser responsables de las implicaciones éticas del algoritmo en uso, dado que este diseñador es el dueño de la decisión algorítmica, por lo que tiene una responsabilidad mayor cuando se habla de privacidad de los datos. En este grupo también se encuentran las personas no profesionales, quienes se están formando a sí mismas como investigadores simplemente al obtener acceso a las transcripciones, aunque estos últimos todavía son pocos, ya que gran parte de los datos todavía son accesibles solo para investigadores profesionales (Martin, 2019; Hesse et al., 2019). Justificación: Se requiere comprender cómo las prácticas del analista responsable del procesamiento de los datos para el desarrollo de modelos analíticos, pueden afectar en gran medida la privacidad de los datos de las personas. Hesse et al. (2019) argumentan que estos analistas deben proteger la privacidad de las personas al margen de las exigencias institucionales por normas profesionales. Así también, Chalcraft (2018) indica que estos profesionales son los que deben hacer comprender a las organizaciones sobre las implicaciones y los riesgos relacionados con la información y el análisis de datos, siendo ellos (los analistas, investigadores, profesionales, estadísticos o científicos de datos) los que deben asumir la responsabilidad de las cuestiones éticas en los proyectos. Es por ello que este estudio permite evaluar si los analistas son los responsables del manejo de la privacidad de datos en el desarrollo de modelos analíticos en la ciencia de datos.	Evaluar las posturas sobre la responsabilidad de los constructores, que hacen el procesamiento, en la privacidad de datos en la ciencia de datos.

Anexo 3. Entregable 3

MATRIZ 3 - SÍNTESIS POR SUBTEMA

	REFERENCIA	LOS PROPIETARIOS DE LOS DATOS COMO RESPONSABLES DE LA PRIVACIDAD DE LOS DATOS	LA NORMATIVA COMO GUIA PARA LA PRIVACIDAD DE LOS DATOS EN EL USO DE ALGORITMOS	LA EMPRESA COMO RESPONSABLE DE LA PRIVACIDAD EN EL USO DE LOS DATOS	LOS CONSTRUCTORES DE LOS ALGORITMOS COMO RESPONSABLES DE LA PRIVACIDAD EN EL USO DE LOS DATOS
1	Rathinam, F., Khatua, S., Siddiqui, Z., Malik, M., Duggal, P., Watson, S., & Vollenweider, X. (2021). Using big data for evaluating development outcomes: A systematic map. Campbell Systematic Reviews, 17(3)http://dx.doi.org/10.1002/cl2.1149	Las personas deben tener conocimiento de la aplicación de sus datos y no deben dar su información detallada sin su conocimiento, en cuyo caso, los usuarios pueden activar y configurar sus propios perfiles, tener la capacidad de desarrollarlos y actualizarlos constantemente. Este tipo de consentimiento informado puede estar completamente presente en la investigación para solicitar el permiso de los usuarios.			
2	Mittelstadt, B. (2017). From Individual to Group Privacy in Big Data Analytics. Philosophy & Technology, 30(4), 475-494. http://dx.doi.org/10.1007/s13347-017-0253-7	El autor considera que los individuos y los miembros del grupo deben dar su consentimiento ante los cambios de su identidad para ver si se acepta o no la clasificación algoritmica (al evaluar la aceptabilidad ética de las plataformas de análisis), sino se viola el derecho a la privacidad.			
3	Ravn, S., Barnwell, A., & Barbara, B. N. (2020). What is "Publicly available data"? exploring blurred Public–Private boundaries and ethical practices through a case study on instagram. Journal of Empirical Research on Human Research Ethics, 15(1-2), 40-45. doi: http://dx.doi.org/10.1177/1556264619850736	El autor considera que antes de reproducir y representar el contenido de las personas se debe pedir el consentimiento al usuario para proponer un enfoque más considerado en las personas para reproducir y usar datos en dichas plataformas. En ese sentido, el autor considera que los datos disponibles públicamente en instagram (por ejemplo, imágenes), no por ser públicos, pueden ser usados para tomar decisiones sin consentimiento de las personas.			
4	Arriagada, G., Gilthorpe, M., & Müller, V. (2020). The ethical imperatives of the COVID-19 pandemic: An analysis from the ethics of data. Veritas, (46), pp. 13-35. https://doi.org/10.4067/S0718-92732020000200013	Los autores mencionan que es importante que las personas estén enteradas del uso que les dan a sus datos y estos tienen que estar protegidos, incluso los datos seudonimizados es información personal, ya que puede tener elementos de riesgos para la reidentificación como es una dirección IP, dado que actúa como un identificador de perfil y, por lo tanto, constituye como información personal.			
5	Someh, I., Davern, M., Breidbach, C. F., & Shanks, G. (2019). Ethical Issues in Big Data Analytics: A Stakeholder Perspective. Communications of the Association for Information Systems, 44, 34. http://dx.doi.org/10.17705/1CAIS.04434	Los autores consideran que todas las partes interesadas deben poder participar por igual en un discurso ético, cuestionar y reclamar cuando surgen problemas éticos y son las personas quienes deben poder controlar qué datos recopilan y agregan las organizaciones sobre ellos y quiénes tendrán acceso a sus datos, incluso deben poder hacer esto después de haber dado su consentimiento para que las organizaciones recopilen y compartan sus datos.			
6	Legewie, N., & Nassauer, A. (2018). YouTube, google, facebook: 21st century online video research and research ethics. Forum Qualitative Sozialforschung, 19(3) doi:http://dx.doi.org/10.17169/fqs-19.3.3130	Los autores consideran que los usuarios deben elegir la opción de participar o no en la investigación de videos en línea desde una perspectiva ética, ya que es posible que estas personas no sean conscientes de que su comportamiento será analizado por los investigadores y, por lo tanto, no existe el consentimiento informado, ya que es posible que las personas representadas en un video no sepan o no den su consentimiento para que se publique un video en línea en las plataformas para compartir videos (Instagram, YouTube, GeoCam, etc.)			
7	Chen, Y., Chen, C., & Li, S. (2022). Determining factors of participants' attitudes toward the ethics of social media data research. Online Information Review, 46(1), 164-181. doi:http://dx.doi.org/10.1108/OIR-11-2020-0514		El autor considera que una regulación efectiva y más estricta centradas en los principios éticos puede ser más adecuada para la gestión de la privacidad de datos en los análisis predictivos, incluso si no se cumple con ello, se debería abandonar el uso del análisis predictivo, ya que los medios tecnológicos son limitados para poder abordar el tema ético en el análisis de datos.		
8	Franzke, A. S., Iris, M., & Schäfer, M. T. (2021). Data Ethics Decision Aid (DEDA): a dialogical framework for ethical inquiry of AI and data projects in the Netherlands. Ethics and Information Technology, 23(3), 551-567. http://dx.doi.org/10.1007/s10676-020-09577-5		El autor argumenta que un marco regulatorio de ayuda para la toma de decisiones de ética de datos (DEDA) es un proceso útil para la evaluación ética de proyectos de datos, ya que ayuda crear conciencia sobre cuestiones éticas en las prácticas de datos.		
9	Chen, W., & Quan-Haase Anabel. (2020). Big Data Ethics and Politics: Toward New Understandings. Social Science Computer Review, 38(1), 3-9. http://dx.doi.org/10.1177/0894439318810734		El autor sugiere que las corporaciones, el gobierno y las instituciones deben manejar políticas y fuentes claras en torno a la ética de los datos para evitar las controversias.		
10	Parti, K., & Szigeti, A. (2021). The Future of Interdisciplinary Research in the Digital Era: Obstacles and Perspectives of Collaboration in Social and Data Sciences - An Empirical Study. Cogent Social Sciences, 7(1)http://dx.doi.org/10.1080/23311886.2021.1970880		El autor considera importante desarrollar lineamientos y prácticas éticas, que tomen en cuenta las características del big data, así como es importante la colaboración interdisciplinaria para analizar, sintetizar y armonizar los vínculos entre disciplinas en un todo coordinado y coherente para trabajar juntos en equipos interdisciplinarios y mapear los obstáculos de la colaboración.		
11	Lang, M., Lemieux, S., Hébert, J., Sauvageau, G., & Zawati, M. H. (2021). Legal and Ethical Considerations for the Design and Use of Web Portals for Researchers, Clinicians, and Patients: Scoping Literature Review. Journal of Medical Internet Research, http://dx.doi.org/10.2196/26450		Consideran que deben implementarse marcos de políticas para administrar las funciones de los portales con respecto a la privacidad, pero todavía no se han adoptado ampliamente, pese a que otros autores respaldan la opinión de que estos tipos de portales son muy prometedores para compartir hallazgos de investigación en salud entre médicos, investigadores y pacientes.		
12	Markham, A. N., Katrin, T., & Herman, A. (2018). Ethics as Methods: Doing Ethics in the Era of Big Data Research—Introduction. Social Media + Society, 4(3)http://dx.doi.org/10.1177/2056305118784502		El autor considera que las normas de la ética de la investigación y los marcos conceptuales del conocimiento algorítmico deben ajustarse para definir y hacer operativa una ciencia de datos basada en la responsabilidad y sostenibilidad.		
13	Forgó, N., Hänold, S., van den Hoven, J., Krügel, T., Lishchuk, I., Mahieu, R., Monreale, A., Pedreschi, D., Pratesi, F., & van Putten, D. (2020). An ethico-legal framework for social data science. International Journal of Data Science and Analytics, 11(4), 377-390. https://doi.org/10.1007/s41060-020-00211-7		Los autores consideran que los valores morales como la privacidad deben complementarse con los requisitos y restricciones legales en la ciencia de datos, lo que puede generar una confianza garantizada por parte de los usuarios.		
14	Ibiricu, B., & Marja Leena van, d. M. (2020). Ethics by design: A code of ethics for the digital age. Records Management Journal, 30(3), 395-414. http://dx.doi.org/10.1108/RMJ-08-2019-0044		El autor considera que la legislación de protección de datos se debe alinear con un marco ético. Asimismo, indica que son las empresas quienes deben desarrollar sistemas de valores y código de conducta para que el comportamiento ético se aplique en la tecnología. Además, indica que la legislación y las normas son esenciales para proteger y respetar las normas éticas, los derechos humanos, la libertad y la privacidad. Por último, la tecnología, la ley y la ética deben coordinar para generar confianza en los individuos.		
15	Nersessian, D. (2018). The law and ethics of big data analytics: A new role for international human rights in the search for global standards. Business Horizons, 61(6), pp. 845-854. https://doi.org/10.1016/j.bushor.2018.07.006		Los actores corporativos tienen obligaciones legales de respetar los derechos humanos en sus actividades comerciales que necesariamente se relacionan con big data.	El autor comenta que los actores corporativos tienen obligaciones legales de respetar los derechos humanos en sus actividades comerciales que necesariamente se relacionan con Big Data.	
16	Martin, K. (2019). Ethical Implications and Accountability of Algorithms: JBE. Journal of Business Ethics, 160(4), 835-850. http://dx.doi.org/10.1007/s10551-018-3921-3			El autor responsabiliza a las empresas por los actos de un algoritmo incluso cuando esta organización afirma que el algoritmo es muy complicado y difícil de comprender. Por ello, declaran que las empresas son los responsables no solo de la carga y desarrollo de un algoritmo, sino también del diseño dentro de la decisión algorítmica y los desarrolladores tienen la obligación de seguir la normativa que tiene implicaciones éticas de los algoritmos.	

	REFERENCIA	LOS PROPIETARIOS DE LOS DATOS COMO RESPONSABLES DE LA PRIVACIDAD DE LOS DATOS	LA NORMATIVA COMO GUIA PARA LA PRIVACIDAD DE LOS DATOS EN EL USO DE ALGORITMOS	LA EMPRESA COMO RESPONSABLE DE LA PRIVACIDAD EN EL USO DE LOS DATOS	LOS CONSTRUCTORES DE LOS ALGORITMOS COMO RESPONSABLES DE LA PRIVACIDAD EN EL USO DE LOS DATOS
17	Nnamdi, J. O., Yusuf, Y. Y., Dharma, K., & Mercangoz, B. A. (2022). Big data supply chain analytics: ethical, privacy and security challenges posed to business, industries and society. Production Planning & Control, 33(2-3), 123-137. http://dx.doi.org/10.1080/09537287.2020.1810764			Los dueños de negocios tienen la responsabilidad del cumplimiento del deber percibido de cuidar a sus clientes en una economía global ciberfísica interconectada en la recopilación y síntesis de datos.	
18	Breidbach, C. F., & Maglio, P. (2020). Accountable algorithms? the ethical implications of data-driven business models. Journal of Service Management, 31(2), 163-185. doi: http://dx.doi.org/10.1108/JOSM-03-2019-0073			Las empresas solo deben implementar herramientas de toma de decisiones algorítmicas siempre que el resultado de sus decisiones no afecte de manera ética a los clientes u otras partes interesadas. Por lo tanto, también deben desarrollar modelos más responsables y éticos.	
19	Hirsch, D. (2019). Data Ethics: Risk management for the algorithmic age. Risk Management, 66(10), 24-29. Retrieved from https://www.proquest.com/scholarly-journals/data-ethics-risk-management-algorithmic-age/docview/2344525577/se-2?accountid=28391			El autor sugiere que las empresas son los responsables de gestionar el riesgo para garantizar que sus actividades de análisis de datos no invadan la privacidad o manipulen a las personas.	
20	Keren Naa, A. A., & Owen, R. (2019). A micro-ethnographic study of big data-based innovation in the financial services sector: Governance, ethics and organisational practices: JBE. Journal of Business Ethics, 160(2), 363-375. doi: http://dx.doi.org/10.1007/s10551-019-04203-x			Considera que son las empresas las que deben comprometerse con las cuestiones de privacidad del usuario, consentimiento y uso secundario de los datos, en cuyo caso han internalizado en sus propias políticas y operaciones.	
21	Saltz, J. S., & Dewar, N. (2019). Data science ethical considerations: A systematic literature review and proposed project framework. Ethics and Information Technology, 21(3), 197-208. http://dx.doi.org/10.1007/s10676-019-09502-5			Sostiene que dentro del modelado de ciencia de datos existe subjetividad, esto puede ser gestionado por las empresas para implementar mecanismos de gestión que les permitan enfrentar los desafíos éticos en la ciencia de datos.	
22	Wiener, M., Saunders, C., & Marabelli, M. (2020). Big-data business models: A critical literature review and multiperspective research framework. Journal of Information Technology, 35(1), 66-91. http://dx.doi.org/10.1177/0268396219896811			El autor considera que entornos organizacionales los modelos de negocio de big data integran entornos más amplios que incluyen varios grupos de partes interesadas que van desde individuos hasta gobiernos y la sociedad. Un ejemplo de ello, es la influencia legislativa que puede permitir o restringir los usos de big data en materia de privacidad.	
23	Herschel, R., & Virginia, M. (2017). Ethics & Big Data. Technology in Society, 49, 31-36. https://doi.org/10.1016/j.techsoc.2017.03.003			Las empresas deben asegurar la privacidad de los datos de las personas. Algunas organizaciones brindan a sus clientes la opción de excluir su información para que no sea compartida con los socios comerciales de la empresa.	
24	Hesse, A., Glenna, L., Hinrichs, C., Chiles, R., & Sachs, C. (2019). Qualitative Research Ethics in the Big Data Era. American Behavioral Scientist, 63(5), 560–583. https://doi.org/10.1177/0002764218805806				Los autores mencionan que los investigadores deben proteger la privacidad de los datos de las personas al margen de las exigencias institucionales por normas profesionales. Un ejemplo de ello, es cuando los usuarios de las redes sociales pueden no darse cuenta completamente de cómo las empresas o los mismos investigadores pretenden utilizar su información, de hecho, otros autores han descubierto que los acuerdos de usuario para datos confidenciales muy escasa vez se leen. En ese aspecto, también puede ser poco razonable solicitar a los investigadores que obtengan el consentimiento de todas las personas que publican un tuit en redes sociales, por ejemplo.
25	Utts, J. (2021). Enhancing data science ethics through statistical education and practice. International Statistical Review = Revue Internationale De Statistique, 89(1), 1-17. doi:http://dx.doi.org/10.1111/insr.12446				Corresponde a los estadísticos y los científicos de datos asumir la responsabilidad de las cuestiones éticas en los proyectos, siendo ellos quienes pueden ayudar a crear conciencia y promover las mejores prácticas ante los problemas éticos relacionados con la privacidad de datos que afectan a la ciencia de datos.
26	Arrojo, M. J. (2019). Valores éticos y cambio tecnológico en la comunicación audiovisual: De la ciencia a la tecnología. Palabra Clave, 22(1), 171-203. http://dx.doi.org/10.5294/pacla.2019.22.1.8				Indican que los agentes de la comunicación y tecnología (los profesionales) no tienen por qué guiarse por sus intuiciones individuales o por las socialmente aceptadas, sino que deben guiarse de los códigos deontológicos, es decir de una práctica profesional y conocimiento científico en el mercado de los valores éticos. Estos códigos deontológicos resuelven problemas de respeto de licencia de privacidad, de buena imagen, derecho a la intimidad, etc.
27	Monkman, G. G., Kaiser, M., & Hyder, K. (2018). The Ethics of Using Social Media in Fisheries Research. Reviews in Fisheries Science & Aquaculture, 26(2), 235-242. http://dx.doi.org/10.1080/23308249.2017.1389854				El autor cree que los investigadores tienen el deber profesional de manejar la ética en su investigación frente al riesgo de causar daño a los agentes involucrados, ya que las juntas de revisión ética actualmente pueden ser limitadas y toda la actividad de extracción de contenido de Internet debe realizarse de manera responsable para que los datos personales no se vean comprometidos.
28	Kitto, K., & Knight, S. (2019). Practical ethics for building learning analytics. British Journal of Educational Technology, 50(6), 2855-2870. http://dx.doi.org/10.1111/bjet.12868				El autor considera que los constructores técnicos de sistemas podrían interactuar más con los especialistas en ética para informar su práctica cuando requieran apoyo. Sería un espacio intermedio en el que los constructores técnicos de sistemas podrían interactuar más con los interesados en políticas, leyes y ética.
29	Chalcraft, Jennette,C.P.A., C.A. (2018). Drawing ethical boundaries for data analytics. Information and Management, 52(1), 18-25. Retrieved from https://www.proquest.com/scholarly-journals/drawing-ethical-boundaries-data-analytics/docview/2015723271/se-2?accountid=28391			EL autor menciona que las organizaciones que se dedican al análisis de datos deben gestionar su responsabilidad en el análisis de datos y sus limitaciones éticas para establecer políticas y procedimientos sobre el desarrollo y la utilización de los datos, aunque no los únicos responsables, ya que también están los profesionales de la información que tienen responsabilidad de hacer comprender a las organizaciones sobre las implicaciones y los riesgos éticos en el análisis de los datos.	Los profesionales de la información son los que deben hacer comprender a las organizaciones sobre las implicaciones y los riesgos relacionados con la información y el análisis de datos, además, las organizaciones deben establecer nuevas políticas y procedimientos de análisis de datos más limitada en "consulta" con las partes interesada para aprovechar el valor potencial de los datos recopilados.
30	Morán, A. (2022). Towards an ethical framework about Big Data era: metaethical, normative ethical and hermeneutical approaches. Heliyon, 8. https://doi.org/10.1016/j.heliyon.2022.e08926				Los autores mencionan que la privacidad de datos depende de la subjetividad moral de la persona que analizan los datos, de alguna manera, ya que, a través de nuestras condiciones psicológicas subjetivas, dependerían las afirmaciones como "robar datos personales es moralmente incorrecto". En ese sentido, valoramos a la privacidad porque nuestras actitudes subjetivas nos llevan a pensar que es valiosa, por ejemplo, la identidad individual representa una información valiosa para los usuarios.

Anexo 4. Entregable 4

MATRIZ 4 ORGANIZACIÓN DE RELACIONES DE JERARQUÍA, COMPARACION Y DESARROLLO

SUBTEMA	CONTROVERSIA	RELACIONES DE JERARQUIA	RELACIONES DE COMPARACIÓN	RELACIONES DE DESARROLLO
LOS PROPIETARIOS DE LOS DATOS COMO RESPONSABLES DE LA PRIVACIDAD DE LOS DATOS EN EL USO DE ALGORITMOS	**Los propietarios tienen la responsabilidad total de la privacidad de sus datos en la ciencia de datos.**	Rathinam et al. (2021) Mittelstadt (2017) Ravn et al. (2020) Arriagada et al. (2020)	Rathinam et al. (2021) quienes indican que las personas deben tener conocimiento de la aplicación de sus datos y no deben dar su información detallada sin su conocimiento, en cuyo caso, los usuarios pueden activar y configurar sus propios perfiles, tener la capacidad de desarrollarlos y actualizarlos constantemente, dicho de otro modo, deben ser responsables de la privacidad de sus datos. De manera similar, Mittelstadt (2017) argumenta que los individuos y los miembros del grupo deben dar su consentimiento ante los cambios de su identidad para ver si se aceptan o no la clasificación algorítmica (al evaluar la aceptabilidad ética de las plataformas de análisis), sino se viola el derecho a la privacidad. La misma posición tiene Ravn et al. (2020) quienes consideran que antes de reproducir y representar el contenido de las personas se debe pedir el consentimiento al usuario para proponer un enfoque más considerado en las personas para reproducir y usar sus datos en dichas plataformas. Incluso, las imágenes de Instagram, no por ser públicos, pueden ser usados para tomar decisiones sin consentimiento de las personas. De manera similar, Arriagada et al. (2020) también argumentaron que es importante que las personas estén enteradas del uso que les dan a sus datos, aún más complementan la idea mencionando que dichos datos tienen que estar protegidos, incluso los datos seudonimizados es información personal, ya que puede tener elementos de riesgos para la reidentificación, por lo tanto, se constituye como información personal.	Rathinam et al. (2021) argumentan que los datos de los usuarios de teléfonos móviles y de las redes sociales son solo algunas de las fuentes de origen de big data que más se usa en la actualidad con el análisis algorítmico y que pueden informar a los investigadores sobre el comportamiento de sus propietarios. Incluso cuando los datos se anonimizan, aun así, existen preocupaciones sobre el consentimiento y la ética que implica saber hasta qué punto se respeta la privacidad de las personas. Por ello, consideran que los propietarios deben tener conocimiento de la aplicación de sus datos y no deben dar su información detallada sin su conocimiento. Por consiguiente, sugieren que el consentimiento informado puede estar completamente presente en la investigación para solicitar el permiso de los usuarios. Incluso, los usuarios pueden tener la opción de activar y configurar sus propios perfiles, así como tener la capacidad de desarrollarlos y actualizarlos constantemente. De manera similar, Mittelstadt (2017) argumenta que los individuos y los miembros del grupo deben dar su consentimiento ante los cambios de su identidad para ver si se aceptan o no la clasificación algorítmica (al evaluar la aceptabilidad ética de las plataformas de análisis), sino se viola el derecho a la privacidad. La misma posición tiene Ravn et al. (2020) quienes consideran que antes de reproducir y representar el contenido de las personas se debe pedir el consentimiento al usuario para proponer un enfoque más considerado en las personas para reproducir y usar sus datos en dichas plataformas. Incluso, las imágenes de Instagram, no por ser públicos, pueden ser usados para tomar decisiones sin consentimiento de las personas. De manera similar, Arriagada et al. (2020) también argumentaron que es importante que las personas estén enteradas del uso que les dan a sus datos, aún más complementan la idea mencionando que dichos datos tienen que estar protegidos, incluso los datos seudonimizados, ya que puede tener elementos de riesgos para la reidentificación, por lo tanto, se constituye como información personal, un ejemplo de ello, es una dirección IP, la cual puede actuar como un identificador de perfil y constituye, por lo tanto, una información personal.
	Los propietarios tienen la responsabilidad parcial de la privacidad de sus datos en la ciencia de datos.	Someh et al. (2019) Legewie & Nassauer (2018)	Someh et al. (2019) indican que todas las partes interesadas deben poder participar por igual en un discurso ético, cuestionar y reclamar cuando surgen problemas éticos, pero son las personas quienes deben poder controlar qué datos recopilan y agregan las organizaciones sobre ellos y quiénes tendrán acceso a sus datos. En esa misma línea, Legewie y Nassauer (2018) detallan que los usuarios deben poder elegir la opción de participar o no en la investigación de videos en línea desde una perspectiva ética, ya que es posible que estas personas no sean conscientes de que su comportamiento será analizado por los investigadores y, por lo tanto, no existe el consentimiento informado, ni existe responsabilidad.	Someh et al. (2019) indican que todas las partes interesadas deben poder participar por igual en un discurso ético, cuestionar y reclamar cuando surgen problemas éticos, pero son las personas quienes deben poder controlar qué datos recopilan y agregan las organizaciones sobre ellos y quiénes tendrán acceso a sus datos. En su estudio Someh et al. (2019) usa la ética del discurso como guía para analizar la ética del análisis de big data y concluye que los individuos como las sociedades necesitan aumentar su importancia en las interacciones con las organizaciones, en ese caso, las personas deben participar activamente en el desarrollo de principios y lineamientos para asegurar que las sociedades establezcan regulaciones y leyes con sanciones efectivas cuando se vulneran sus derechos sobre la privacidad de los datos. En ese sentido, el análisis de big data influye en la sociedad y, por tanto, la sociedad misma debe controlarla y moldearla de una manera que beneficie a todas las partes interesadas de una forma justa y equilibrada. Es por ello que argumentan que las personas y las partes interesadas deben abordar los problemas éticos que surgen cuando las organizaciones recopilan, analizan, comparten o venden "datos" de individuos sin el consentimiento o conocimiento genuino de ellos (Someh et al., 2019). En esa misma línea, Legewie & Nassauer (2018) tienen una posición similar con otros autores cuando indican que los usuarios deben elegir la opción de participar o no en la investigación desde una perspectiva ética, ya que es posible que estas personas no sean conscientes de que su comportamiento será analizado por los investigadores y, por lo tanto, no existe el consentimiento informado, por ejemplo, es posible que las personas representadas en un video (por ejemplo) no sepan o no den su consentimiento para que se publique dicho video, pero aun así se hacen públicos. Morán (2022) también indican que la privacidad de datos depende de la subjetividad moral de la persona, es por ello que valoramos a la privacidad según cómo nuestras actitudes subjetivas nos llevan a pensar que es valioso, o lo es simplemente porque reconocemos que es valioso. De alguna forma, a través de nuestras condiciones psicológicas subjetivas, dependerían las afirmaciones como "robar datos personales es moralmente incorrecto" (Morán, 2022, p.3). Dicho de otra manera, los problemas más importantes son los que se relacionan con el concepto de responsabilidad moral, a partir de una perspectiva metaética y los retos del Big Data. En ese sentido, Morán (2022) también concluye que los desafíos del Big Data se extienden más allá que la responsabilidad individual de un profesional de las Ciencias de la Información, dado que los cambios que provocan los conjuntos masivos de datos son fundamentalmente problemas de una ética de grupo.
LA NORMATIVA COMO GUIA PARA LA PRIVACIDAD DE LOS DATOS EN EL USO DE ALGORITMOS	**La normativa en el uso de datos es efectiva como guía en la privacidad de los datos en la ciencia de datos.**	Mühlhoff (2021) Franzke et al. (2021) Chen & Quan-Haase (2020) Parti & Szigeti (2021)	Mühlhoff (2021) consideran que una regulación efectiva y más estricta centradas en los principios éticos puede ser más adecuada para la gestión de la privacidad de datos en los análisis predictivos. De la misma manera, Franzke et al. (2021) argumentan que un marco regulatorio de ayuda para la toma de decisiones de ética de datos es un proceso útil para la evaluación ética de proyectos. Así también, Chen y Quan-Haase (2020) sugieren que las corporaciones, el gobierno y las instituciones deben manejar políticas y fuentes claras en torno a la ética de los datos para evitar las controversias, lo cual concuerda con la opinión de Parti y Szigeti (2021) quienes consideran importante desarrollar lineamientos y prácticas éticas que tomen en cuenta las características del big data.	Mühlhoff (2021) consideran que una regulación efectiva y más estricta centradas en los principios éticos puede ser más adecuada para la gestión de la privacidad de datos en los análisis predictivos, ya que actúa como guía hacia la puesta en práctica del pensamiento ético en proyectos responsables de las empresas, incluso si no se cumple con ello, se debería abandonar el uso del análisis predictivo, ya que los medios tecnológicos son limitados para poder abordar el tema ético en el análisis de datos. De la misma manera, Franzke et al. (2021) argumentan que un marco regulatorio de ayuda para la toma de decisiones de ética de datos es un proceso útil para la evaluación ética de proyectos. Por esa razón, plantea un marco de ayuda para la toma de decisiones de ética de datos (DEDA), la cual es una herramienta eficaz y útil para la evaluación ética de proyectos de datos y para la creación de conciencia sobre cuestiones éticas en las prácticas de datos como un proceso efectivo para moderar la deliberación de casos y avanzar en el desarrollo de prácticas responsables en la ciencia de datos. Así también, Chen y Quan-Haase (2020) sugieren que las corporaciones, el gobierno y las instituciones deben manejar políticas y fuentes claras en torno a la ética de los datos para evitar las controversias, lo cual concuerda con la opinión de Parti y Szigeti (2021) quienes consideran importante desarrollar lineamientos y prácticas éticas que tomen en cuenta las características del big data, a la vez introduce la idea de colaboración interdisciplinaria como hecho importante para analizar, sintetizar y armonizar los vínculos en un todo coordinado y coherente para trabajar juntos en equipos interdisciplinarios y mapear los obstáculos de la colaboración en torno a las decisiones éticas de datos.
	La normativa en el uso de datos es efectiva parcialmente como guía en la privacidad de los datos en la ciencia de datos.	Lang et al. (2021) Markham et al. (2018) Forgó et al. (2020) Ibiricu & Marja (2020) Nersessian (2018)	Lang et al. (2021) consideran que deben implementarse marcos de políticas para administrar las funciones de los portales que gestionan la información con respecto a la privacidad de datos, pero todavía no se han adoptado ampliamente para hablar de una efectividad completa. En esa misma línea, Markham et al. (2018) indican que las normas de la ética de la investigación y los marcos conceptuales del conocimiento algorítmico deben ajustarse para definir y hacer operativa una ciencia de datos basada en la responsabilidad y sostenibilidad. Al igual que Markham et al, en Forgó et al. (2020) se detalla que los valores morales como la privacidad deben complementarse con los requisitos y restricciones legales en la ciencia de datos para generar una confianza garantizada por parte de los usuarios. Esta posición también lo comparte Ibiricu y Marja (2020) quienes consideran que la legislación de protección de datos se debe alinear con un marco ético para ser efectiva; además, indican que son las empresas quienes deben desarrollar sistemas de valores y código de conducta para que el comportamiento ético se aplique en la tecnología. Nersessian (2018) también menciona que un marco de derechos humanos puede proporcionar una guía clara y consistente cuando las leyes nacionales y los mecanismos de aplicación en un país en particular puede ser débiles o poco efectivas con respecto a las decisiones éticas en el contexto de Big Data.	Lang et al. (2021) consideran que deben implementarse marcos de políticas para administrar las funciones de los portales que gestionan la información con respecto a la privacidad de datos, pero todavía no se han adoptado ampliamente para hablar de una efectividad completa. Por eso, determinaron cinco desafíos legales y éticos (privacidad y confidencialidad, capacitación, equidad, alfabetización y toma de decisiones) para el uso de los portales web en la atención clínica. En esa misma línea, Markham et al. (2018) también indican que las normas de la ética de la investigación y los marcos conceptuales del conocimiento algorítmico deben ajustarse para definir y hacer operativa una ciencia de datos basada en la responsabilidad y sostenibilidad. Al igual que Markham et al, en Forgó et al. (2020) se detalla que los valores éticos como la privacidad deben complementarse con los requisitos y restricciones legales en la ciencia de datos para generar una confianza garantizada por parte de los usuarios y, de esta manera, resolver los problemas sociales que son el foco para la legitimidad de la ciencia de big data , así como lo es el cumplimiento de los valores morales fundamentales para que las personas puedan depositar en la ciencia de datos y en las aplicaciones de la investigación de big data, toda su confianza. Esta posición también lo comparte Ibiricu y Marja (2020) quienes consideran que la legislación de protección de datos se debe alinear con un marco ético para ser efectiva, integrando la ética en las primeras etapas del diseño de procesos y tecnologías, ya que garantiza que los empleados involucrados respeten el código de conducta; además, indican que son las empresas quienes deben desarrollar sistemas de valores y código de conducta para que el comportamiento ético se aplique en la tecnología. Nersessian (2018) también menciona que un marco de derechos humanos puede proporcionar una guía clara y consistente cuando las leyes nacionales y los mecanismos de aplicación en un país en particular puede ser débiles o poco efectivas con respecto a las decisiones éticas en el contexto de Big Data.

SUBTEMA	CONTROVERSIA	RELACIONES DE JERARQUIA	RELACIONES DE COMPARACIÓN	RELACIONES DE DESARROLLO
LA EMPRESA COMO RESPONSABLE DE LA PRIVACIDAD EN EL USO DE LOS DATOS EN LOS ALGORITMOS	**Las empresas tienen la responsabilidad total de la privacidad de los datos de sus clientes en la ciencia de datos.**	Martin, K. (2019) Nnamdi et al. (2022) Breidbach & Maglio (2020) Nersessian, D. (2018) Hirsch, D. (2019) Keren & Owen (2019)	Martin (2019) menciona que las empresas son los responsables de la privacidad de datos en el uso de los algoritmos, incluso cuando la organización afirma que el algoritmo es muy complicado y difícil de comprender. En la misma línea, Nnamdi et al. (2022) también mencionan que los dueños de los negocios tienen la responsabilidad del cumplimiento del deber percibido de cuidar a sus clientes, al igual que Breidbach y Maglio (2020) quienes además indican que las empresas solo deben implementar herramientas de toma de decisiones algorítmicas siempre que el resultado de sus decisiones no afecten de manera ética a los clientes u otras partes interesadas. En ese entido, Nersessian (2018) también precisa que las organizaciones tienen obligaciones legales para respetar los derechos humanos en sus actividades comerciales que necesariamente se relacionan con big data. Del mismo modo, Hirsch (2019) complementa esta posición, mencionando que las empresas son los responsables de gestionar el riesgo para garantizar que sus actividades de análisis de datos no invadan la privacidad o manipulen a las personas, así como Keren Naa y Owen (2019) que argumentan que son las empresas las que deben comprometerse con las cuestiones de privacidad del usuario, consentimiento y uso secundario de los datos.	En una economía global digitalizada e interconectada para la recopilación de datos, análisis de big data y decisiones algorítmicas, Martin (2019) menciona que las empresas son los responsables de la privacidad de datos en el uso de los algoritmos no solo de la carga y desarrollo de un algoritmo, sino también del diseño dentro de la decisión algorítmica, incluso cuando la organización afirma que el algoritmo es muy complicado y difícil de comprender. En la misma línea, Nnamdi et al. (2022) también mencionan que los dueños de los negocios tienen la responsabilidad del cumplimiento del deber percibido de cuidar a sus clientes frente a los problemas éticos relacionados a la privacidad de sus datos, al igual que Breidbach y Maglio (2020) quienes además indican que las empresas solo deben implementar herramientas de toma de decisiones algorítmicas siempre que el resultado de sus decisiones no afecten de manera ética a los clientes u otras partes interesadas, en su investigación, estos autores también demuestran que el algoritmo, la inteligencia artificial (IA) y los conjuntos de datos grandes pueden ser poco éticos, pudiendo generar pérdidas de privacidad, manipulación directa, entre otros. En ese entido, Nersessian (2018) precisan que las organizaciones tienen obligaciones legales para respetar los derechos humanos en sus actividades comerciales que necesariamente se relacionan con big data; al respecto, existe poco consenso internacional sobre qué estándares deben regir en el uso de la tecnología de Big data que beneficien y que llenen el vacío con respecto al derecho internacional de los derechos humanos. Del mismo modo, Hirsch (2019) complementa esta posición, mencionando que las empresas son los responsables de gestionar el riesgo para garantizar que sus actividades de análisis de datos no invadan la privacidad o manipulen a las personas, ya que en su estudio demuestra que el análisis de big data puede dañar a las personas en al menos tres formas importantes: invasión de la privacidad, manipulación y sesgo; pese al riesgo continuo de invasión a la privacidad, muchas empresas no conocen completamente estos riesgos comerciales, por lo que las personas ya no pueden solo aceptar las políticas de consentimiento a la privacidad para protegerse, ya que las empresas no pueden protegerlas simplemente cumpliendo con las leyes de privacidad, sino que exige ir más allá de la ley; en ese aspecto, las organizaciones deben gestionar el riesgo de invasión a la privacidad. Asimismo, Keren Naa y Owen (2019) que argumentan que son las empresas las que deben comprometerse con las cuestiones de privacidad del usuario, consentimiento y uso secundario de los datos.
	Las empresas tienen una responsabilidad parcial de la privacidad de datos de sus clientes en la ciencia de datos.	Saltz & Dewar (2019) Wiener et al. (2020) Chalcraft (2018) Herschel & Virginia (2017)	Saltz y Dewar (2019) cuestionan el nivel de responsabilidad de la empresa, ya que dentro del modelado de ciencia de datos puede existir subjetividad, aunque esto puede ser gestionado por las empresas para implementar mecanismos de gestión que les permitan enfrentar los desafíos éticos en la ciencia de datos, ya que lo que es ético para unos no necesariamente es ético para otros. De forma similar, Wiener et al. (2020) también argumentan sobre la responsabilidad parcial de las empresas, manifestando que en entornos organizacionales, los modelos de negocio de big data integran entornos más amplios que las empresas consideran, ya que incluyen varios grupos de partes interesadas que van desde individuos hasta gobiernos y la sociedad, un ejemplo de ello es el caso de la influencia legislativa, la cual puede restringir o permitir los usos de big data en materia de privacidad. Del mismo modo, Chalcraft (2018) las empresas no son los únicos responsables, ya que también están los profesionales de la información quienes deben hacer comprender a las organizaciones sobre las implicaciones y los riesgos relacionados con la información y el análisis de datos. Así también, Herschel y Virginia (2017) encuentran que las empresas deben asegurar la privacidad de los datos de las personas.	Saltz y Dewar (2019) cuestionan el nivel de responsabilidad de la empresa, ya que dentro del modelado de ciencia de datos puede existir subjetividad, aunque esto puede ser gestionado por las empresas para implementar mecanismos de gestión que les permitan enfrentar los desafíos éticos en la ciencia de datos, ya que lo que es ético para unos no necesariamente es ético para otros, esto sin duda genera desafíos éticos en la ciencia de datos, los cuales son: la necesidad de un marco ético, la novedad del campo, los desafíos relacionados con los datos y los desafíos relacionados con el modelo de análisis. De forma similar, Wiener et al. (2020) también argumentan sobre la responsabilidad parcial de las empresas, ya que, en entornos organizacionales, los modelos de negocio de big data integran entornos más amplios que las empresas consideran, lo que incluyen varios grupos de partes interesadas que van desde individuos hasta gobiernos y la sociedad, un ejemplo de ello es el caso de la influencia legislativa, la cual puede restringir o permitir los usos de big data en materia de privacidad. En ese sentido, Wiener et al. (2020) también consideran que las organizaciones deben aprovechar los beneficios de los modelos de negocio de big data para generar una ventaja competitiva haciendo uso de los modelos comerciales de grandes datos para generar una integración vertical dentro de la cadena de suministros en la medida que recopilan, almacenan, administran y procesan los datos. De igual manera, Chalcraft (2018) las empresas no son los únicos responsables, ya que también están los profesionales de la información quienes deben hacer comprender a las organizaciones sobre las implicaciones y los riesgos relacionados con la información y el análisis de datos. Del mismo modo, Herschel y Virginia (2017) encuentran que las empresas deben asegurar la privacidad de los datos de las personas
LOS CONSTRUCTORES DE LOS ALGORITMOS COMO RESPONSABLES DE LA PRIVACIDAD EN EL USO DE LOS DATOS	**Los constructores de los algoritmos tienen la responsabilidad total de la privacidad de los datos en la ciencia de datos.**	Hesse et al. (2019) Utts (2021) Arrojo (2019) Monkman et al. (2018)	Hesse et al. (2019) mencionan que los investigadores deben proteger la privacidad de los datos de las personas al margen de las exigencias institucionales por normas profesionales, incluso cuando los usuarios pueden no darse cuenta completamente de cómo las empresas o los mismos investigadores pretenden utilizar su información. Así también, Utts (2021) argumentan que los estadísticos y los científicos de datos deben asumir la responsabilidad de las cuestiones éticas en los proyectos, ya que son ellos quienes pueden ayudar a crear conciencia y promover las mejores prácticas ante los problemas éticos relacionados con la privacidad de datos en la ciencia de datos. Del mismo modo, Arrojo (2019) Indica que los agentes de la comunicación y tecnología (los profesionales) no tienen por qué guiarse por sus intuiciones individuales o por las socialmente aceptadas, sino que deben guiarse de los códigos deontológicos, es decir de una práctica profesional y conocimiento científico en el mercado de los valores éticos. Asimismo, Monkman et al. (2018) consideran que los investigadores tienen el deber profesional de manejar la ética en su investigación frente al riesgo de causar daño a los agentes involucrados.	Hesse et al. (2019) mencionan que los investigadores deben proteger la privacidad de los datos de las personas al margen de las exigencias institucionales por normas profesionales, incluso cuando los usuarios pueden no darse cuenta completamente de cómo las empresas o los mismos investigadores pretenden utilizar su información, de hecho, otros autores han descubierto que los acuerdos de usuario para el manejo de los datos confidenciales se leen muy escasa vez, un ejemplo de ello, es cuando los usuarios de las redes sociales pueden no darse cuenta completamente de cómo las empresas o los mismos investigadores pretenden utilizar su información, aunque es ese caso, también puede ser poco razonable solicitar a los investigadores que obtengan el consentimiento de todas las personas que publican un tuit en redes sociales por ejemplo. Por ese motivo, presenta cinco principios rectores para que los investigadores cualitativos y sus instituciones consideren al visualizar prácticas y pautas futuras dentro de esta investigación cambiante y emergente, siendo: i) valorar la diversidad metodológica; (ii) fomentar la investigación para que tengan en cuenta el contexto, la especificidad y las poblaciones marginadas; (iii) abordar dilemas éticos y no solo ver las preocupaciones legales; (iv) atención a las diferencias regionales y disciplinarias; y (v) considerar todo el ciclo de vida de la investigación, incluyendo su vida futura en los archivos o instalaciones de datos abiertos. Así también, Utts (2021) argumentan que los estadísticos y los científicos de datos deben asumir la responsabilidad de las cuestiones éticas en los proyectos, ya que son ellos quienes pueden ayudar a crear conciencia y promover las mejores prácticas ante los problemas éticos relacionados con la privacidad de datos en la ciencia de datos. Del mismo modo, Arrojo (2019) Indica que los agentes de la comunicación y tecnología (los profesionales) no tienen por qué guiarse por sus intuiciones individuales o por las socialmente aceptadas, sino que deben guiarse de los códigos deontológicos, es decir de una práctica profesional y conocimiento científico en el mercado de los valores éticos. Asimismo, Monkman et al. (2018) consideran que los investigadores tienen el deber profesional de manejar la ética en su investigación frente al riesgo de causar daño a los agentes involucrados, incluso considera que las juntas de revisión ética actualmente pueden ser limitadas y toda la actividad de extracción de contenido de Internet debe realizarse de manera responsable para que los datos personales no se vean comprometidos.
	Los constructores de los algoritmos tienen la responsabilidad parcial de la privacidad de los datos en la ciencia de datos.	Kitto & Knight (2019) Chalcraft (2018) Morán (2022)	Kitto y Knight (2019) considera que los constructores técnicos de sistemas podrían interactuar más con los especialistas en ética para informar su práctica cuando requieran apoyo, existiendo una responsabilidad compartida. Sería un espacio intermedio en el que los constructores técnicos de sistemas podrían interactuar más con los interesados en políticas, leyes y ética. Así mismo, Chalcraft (2018) menciona que los profesionales de la información son los que deben hacer comprender a las organizaciones sobre las implicaciones y los riesgos relacionados con la información y el análisis de datos. Morán (2022) también indica que la privacidad de datos depende de la subjetividad moral de la persona, ya que, a través de nuestras condiciones psicológicas subjetivas, dependerán las afirmaciones como "robar datos personales es moralmente incorrecto".	Kitto y Knight (2019) considera que los constructores técnicos de sistemas podrían interactuar más con los especialistas en ética para informar su práctica cuando requieran apoyo, existiendo una responsabilidad compartida. Sería un espacio intermedio en el que los constructores técnicos de sistemas podrían interactuar más con los interesados en políticas, leyes y ética. En ese sentido, Kitto & Knight (2019) también menciona que existe baja utilización de inteligencia artificial y el análisis de datos cuando los administradores buscan evitar el riesgo, como al uso indebido de los datos. Por ello, en su investigación propone una base de datos abierta (piloto) que enumera los casos extremos que enfrentan los constructores de sistemas de "Analytics" como método para guiar en ética a los especialistas que trabajan en el campo de la ciencia de datos para informar su práctica. Así mismo, Chalcraft (2018) menciona que los profesionales de la información son los que deben hacer comprender a las organizaciones sobre las implicaciones y los riesgos relacionados con la información y el análisis de datos; además, las organizaciones deben establecer nuevas políticas y procedimientos de análisis de datos más limitada en "consulta" con las partes interesada para aprovechar el valor potencial de los datos recopilados. Por eso, en su estudio Chalcraft (2018) se enfoca a establecer los límites éticos en el análisis de datos que se recopilan y analizan con herramientas y técnicas analíticas más sofisticadas, por lo que el autor sugiere a las organizaciones establecer nuevas políticas y procedimientos de análisis de datos más limitada en "consulta" con las partes interesada para aprovechar el valor potencial de los datos recopilados. Morán (2022) también indica que la privacidad de datos depende de la subjetividad moral de la persona, ya que, a través de nuestras condiciones psicológicas subjetivas, dependerán las afirmaciones como "robar datos personales es moralmente incorrecto".