

## **GUIA DOCENTE**

### **MÁSTER UNIVERSITARIO EN DATA ANALYTICS FOR BUSINESS**

2ª Edición

Curso 2024-2025

#### **GRUPO 1**

#### **ASIGNATURA**

- **Nombre: Aspectos éticos y legales del análisis de datos**
- **Tipo de asignatura: Obligatoria (Modulo 3. Gestión de Proyectos)**
- **Trimestre: Segundo**
- **Créditos: Tres**
- **Idioma de docencia: Castellano**
- **Coordinador de la asignatura: Rodrigo Cetina Presuel**
- **Profesor/es de la asignatura: Rodrigo Cetina Presuel**

#### **PRESENTACIÓN DE LA ASIGNATURA**

##### **Objetivos de la asignatura**

Las tecnologías de la información y la comunicación, particularmente en su vertiente digital, parecen haber alterado radicalmente dinámicas de poder, modelos de negocio e incluso la estructura cultural de todo tipo de organizaciones públicas y privadas. La vertiginosa velocidad del avance de las tecnologías de la información y para el análisis de datos así como la ubicuidad en el uso de datos personales en todos los aspectos de la vida pública y privada de la sociedad actual hacen más necesario que nunca el conocer los retos éticos y legales relacionados con estas prácticas y poder entender qué derechos fundamentales están en juego, qué beneficios y qué perjuicios existen para los individuos y la sociedad y por qué.

Este curso permitirá al estudiante explorar las implicaciones éticas y legales de uso de los datos personales, los riesgos y recompensas de la recolección, procesamiento y uso de datos y de una sociedad en constante vigilancia. Esto permitirá al estudiante comprender el por qué de la necesidad de contar con políticas y leyes que protejan a la privacidad y el por qué de la importancia de la defensa de los derechos de las personas y de conducirse guiados por valores éticos sólidos.

En particular la clase permitirá al estudiante identificar las áreas de la práctica del análisis de datos en donde surgen dilemas éticos y le permitirá crecer en la capacidad analítica de los debates éticos y en las consecuencias legales y sociales del uso de datos personales en distintas áreas como el comercio, el empleo, las finanzas, la sanidad, la educación, la seguridad ciudadana, las prestaciones públicas y otras.

Uno de los objetivos principales de este curso es contribuir a hacer al estudiante un ciudadano mejor informado y consciente de que ha de contribuir a la vigilancia y uso ético de los datos y a la construcción de una sociedad en donde la privacidad y la protección de datos son valores y derechos muy presentes. A través de las reflexiones en clase y los casos de estudio propuestos se busca formar ciudadanos críticos que no den por sentada la realidad fáctica del capitalismo de los datos que explota los mismos, y a las personas, sin reparar en los daños que se pueden causar para que dichos ciudadanos puedan influir en

las prácticas éticas y legales relacionadas con los datos dentro de las organizaciones públicas y privadas.

La clase, además, mira hacia el futuro y pretende que el estudiante aproveche esta visión crítica para reflexionar y desarrollar la capacidad de anticipar los retos futuros para los derechos fundamentales y la ética en relación con el uso de los datos personales.

Al final del curso el estudiante será capaz de:

- Manejar con solvencia conceptos como la protección de datos personales, la privacidad y su regulación, la distinción entre datos personales confidenciales, anónimos y abiertos, datos públicos y datos privados, la propiedad y control de los datos y los derechos digitales y la propiedad intelectual.
- Identificar y distinguir con solvencia los distintos retos que son pertinentes al manejo de la información personal, su análisis y las consecuencias que esto puede tener para la sociedad y para las personas, incluyendo mediante el uso de métodos computacionales como el machine learning y la inteligencia artificial.
- Distinguir entre las faltas éticas relacionadas con el manejo de datos y las posibles violaciones a la legislación vigente teniendo en cuenta los potenciales daños que pueden causarse a la sociedad y los individuos, particularmente siendo sensible a los posibles daños que emergen según el contexto del manejo de los datos y los métodos que se utilizan para su análisis y procesamiento.
- Obtener conocimientos fundamentales sobre el marco legal existente, las reglas, prohibiciones y procedimientos legales para acceder y utilizar datos y de las reglas encaminadas a proteger los derechos de las personas de los efectos indeseados o nocivos del uso de ciertas tecnologías.
- Realizar análisis teóricos, filosóficos y críticos acerca de las implicaciones del uso de datos personales y las distintas tecnologías y su relación con la ciencia, la empresa y la política pública.
- Articular de manera cohesiva (tanto de manera oral como escrita) análisis críticos y posiciones argumentativas sólidas respecto de retos éticos y legales relacionados con la recolección y el manejo de los datos así como de las perspectivas de futuro del sector y del avance de la ciencia y tecnología de los datos.

## Contenidos

<p><b>Primera sesión</b> 19 de febrero de 2025</p>	<ol style="list-style-type: none"> <li><b>1. La ética y el manejo de datos: imaginando futuros</b></li> <li><b>2. ¿De qué hablamos cuando hablamos de ética de los datos?</b> <ul style="list-style-type: none"> <li>• Viejos conceptos y nuevas tecnologías: privacidad, consentimiento, vigilancia, poder, justicia, rendición de cuentas y responsabilidad social corporativa.</li> <li>• La ética de los datos en la sociedad de la vigilancia.</li> <li>• El uso de los datos y el deber de mitigar daños.</li> </ul> </li> <li><b>3. Derechos y libertades fundamentales y el manejo de los datos:</b> <ul style="list-style-type: none"> <li>• La dignidad humana.</li> <li>• La privacidad y los derechos al honor y la intimidad.</li> <li>• Del habeas data a al derecho fundamental a la protección de datos personales.</li> <li>• La libertad de expresión, el derecho a la información y el acceso a la información.</li> <li>• El derecho y la inteligencia artificial.</li> </ul> </li> </ol>
--	---

<p><b>Segunda sesión</b> 26 de febrero de 2025</p>	<p><b>1. Los dilemas éticos en la gestión de los datos</b></p> <ul style="list-style-type: none"> <li>• ¿Es el ser humano cuantificable? Una teoría defectuosa del tú.</li> <li>• Recolección de datos y privacidad.</li> <li>• El uso de los datos y los límites del consentimiento informado.</li> <li>• La reutilización de los datos y la vida más allá de los datos.</li> </ul> <p><b>2. Marco regulatorio básico: el corpus de la protección de datos personales</b></p> <ul style="list-style-type: none"> <li>• El marco regulatorio europeo y el marco regulatorio español.</li> <li>• El Reglamento General de Protección de Datos Personales</li> <li>• El Reglamento Europeo de Inteligencia Artificial</li> </ul> <p>Estudio de caso 1. <a href="#">Google Teachable Machine.</a></p> <p>Estudio de caso 2. <a href="#">GEDMatch: el uso de información genética ¿qué pasa cuando se roban nuestro ADN?</a></p>
<p><b>Tercera sesión</b> 4 de marzo de 2025</p>	<p><b>1. Del origen de los datos al fin de la privacidad: anonimización, derecho al olvido, transparencia y acceso público</b></p> <ul style="list-style-type: none"> <li>• En internet nadie sabe que eres un perro: ¿tenemos un derecho al anonimato?</li> <li>• ¿Son los datos realmente anónimos? Re-identificación y los límites de la tecnología.</li> <li>• Videovigilancia, privacidad y protección de datos.</li> <li>• Privacidad sónica.</li> <li>• Transparencia vs. Privacidad: El acceso a la información como amigo y enemigo.</li> <li>• El derecho al olvido: la máquina y la memoria infinita.</li> <li>• Privacidad por diseño y por defecto.</li> </ul> <p>Estudio de caso 3. <a href="#">Reconsiderando el anonimato: técnicas para la re-identificación de datos.</a></p> <p>Estudio de caso 4. <a href="#">El censo poblacional: Implementación de la privacidad diferencial.</a></p>
<p><b>Cuarta sesión</b> 11 de marzo de 2025</p>	<p><b>1. El capitalismo de vigilancia: la privacidad tiene un precio</b></p> <ul style="list-style-type: none"> <li>• La industria de los datos como industria extractiva.</li> <li>• Confundir valor con precio: ¿Debemos tener un derecho a vender nuestros datos?</li> <li>• El mercado de la publicidad microsegmentada: Los costes de la categorización</li> <li>• Personalización a través de los datos: silos de información y democracia.</li> </ul> <p>Estudio de caso 5. <a href="#">Sesgos algorítmicos en la publicidad en redes sociales: Los anuncios microsegmentados como herramienta de exclusión.</a></p> <p>Estudio de caso 6. (1) <a href="#">Gonzalez v. Google.</a> (2) <a href="#">Radicalización algorítmica y extremismo.</a></p> <p>Estudios de caso 7. (1) <a href="#">Moderation Mayhem.</a> (2) <a href="#">Trust and Safety Tycoon.</a></p>
<p><b>Quinta sesión</b> 18 de marzo de 2025</p>	<p><b>1. Retos presentes y futuros del uso y análisis de datos:</b></p> <ul style="list-style-type: none"> <li>• La soberanía y el colonialismo de datos.</li> <li>• Datos, administración pública y decisiones automatizadas.</li> <li>• La inteligencia artificial y las implicaciones éticas para la sociedad: de la IA generativa al</li> </ul>

	<p>machine learning y las decisiones automáticas.</p> <ul style="list-style-type: none"> <li>• La justicia algorítmica.</li> </ul> <p><b>Estudio de caso 8.</b> <a href="#">La máquina de las sospechas: algoritmos en la administración pública, acceso a derechos y discriminación.</a></p> <p><b>Estudio de caso 9.</b> <a href="#">Deepfakes. Dilemas para un futuro cercano.</a></p>
<p><b>Sexta sesión</b> 25 de marzo de 2025</p>	<p><b>1. Presentación de trabajos finales</b></p>

## Metodología docente

La asignatura se estructura en **6 sesiones presenciales**, en horario normal del máster, en las que se combinan la exposición magistral de conceptos, el debate en clase en base a lecturas obligatorias y el desarrollo de 8 estudios de caso que se analizarán y estudiarán a lo largo de las primeras cinco sesiones en las cuales la asistencia a clase y la participación oral activa serán esenciales para poder aprobar el curso y ser evaluados de manera individual. Además, entre la primera y la quinta sesión los estudiantes se dividirán en grupos de trabajo y escogerán libremente un tema relacionado con los retos de futuro para la ética y el derecho a la privacidad y la protección de los datos personales y desarrollarán un ensayo sobre el mismo, analizando las implicaciones de nuevos desarrollos tecnológicos en la materia y sus consecuencias para la sociedad. Dicho trabajo deberá ser presentado de manera oral por cada grupo durante la última sesión de la asignatura y con la retroalimentación dada por el profesor y compañeros durante la ronda de presentaciones, entregarán en fecha posterior la versión final de dicho ensayo. Esto permitirá completar la evaluación de competencias de trabajo en grupo tanto orales como escritas.

## Evaluación

Para evaluar la adquisición de las competencias y objetivos de aprendizaje se plantea un sistema de evaluación continua obligatoria con componentes individuales y grupales.

**Evaluación continua** (obligatoria, individual y en grupo):

- **A nivel individual** (10%): asistencia y participación en la discusión en clase a partir de los temas expuestos, los debates propuestos e interacción valiosa entre compañeros y con el profesorado de la asignatura, incluyendo estar presente y participar activamente en la retroalimentación para los trabajos presentados de manera oral el último día de clase y descrito más abajo.
- **A nivel individual** (10%): demostrar dentro de la discusión en clase y el análisis de los casos de estudio la realización de las lecturas obligatorias marcadas en la guía docente. En cualquier momento, el profesor podrá preguntar a cualquiera de los estudiantes por temas o conceptos específicos contenidos en las lecturas asignadas o en los casos de estudio propuestos.
- **A nivel grupal** (30%). Presentación oral de un trabajo en grupo (descrito a continuación durante la última sesión de clase. La presentación deberá estar acompañada de una presentación en power point que deberá contener los puntos clave del trabajo realizado incluyendo la introducción, los argumentos centrales y las conclusiones del mismo. La retroalimentación obtenida a través de las intervenciones del profesor y los compañeros de clase resultará en puntos de mejora que deberán entregarse en el trabajo final por escrito descrito a continuación.  
Los grupos deberán realizar la presentación horal el día de la última sesión de clase, el **25 de marzo de 2025** en horario normal de clase. El plazo es único e improrrogable y no estar presente en la sesión implicará la pérdida de toda la nota correspondiente a este ejercicio.
- **A nivel grupal** (50%): Elaboración y entrega de un trabajo en grupo (3 a 5 personas). los estudiantes se dividirán en grupos de trabajo y escogerán libremente un tema a desarrollar a través de un ensayo. El tema deberá consensuarse entre los miembros del grupo. Dicho ensayo deberá estar relacionado con los retos de futuro para la ética y los derechos a la privacidad y la protección de los

datos personales y/o de la inteligencia artificial y en el mismo analizarán las implicaciones de nuevos desarrollos tecnológicos en la materia y sus consecuencias para la sociedad.

Se invita a los estudiantes a desarrollar temas que exploren o estén en consonancia con los objetivos de desarrollo sostenible (ODS): <https://www.un.org/sustainabledevelopment/es/development-agenda/> Además, se invita de manera especial a que los estudiantes incorporen la perspectiva de género en el análisis objeto del ensayo o bien a que el tema central del mismo gire en torno a la perspectiva y/o equidad de género.

El tema, además, podrá tener como punto de partida cualquiera de los temas, lecturas, casos de estudio que formen parte de esta asignatura y podrá surgir también de cualesquiera de los temas de debate que se generen en clase.

Herramientas de IA generativa, como por ejemplo ChatGPT, podrán ser objeto del tema a analizar en el ensayo pero su uso queda prohibido salvo que se comunique expresamente y que cualquier parte del trabajo compuesta, producida o creada directamente o con ayuda de estas herramientas sea plenamente identificada en el cuerpo del trabajo y cualesquiera fuentes secundarias utilizadas queden plenamente identificadas. Cualquier otro uso u ocultación del uso de estas herramientas será tratada como plagio y como tal, estará sujeta a las medidas disciplinarias previstas en las normas de convivencia de la UPF-BSM. Además, los estudiantes han de ser conscientes que para la Agencia Catalana de Protección de Datos, el uso de herramientas de IA generativa comportan riesgos para la privacidad y la protección de datos personales y por ello, no recomienda su utilización debido, a entre otras cuestiones, la imposibilidad práctica de ejercer los derechos de autodeterminación informativa (acceso, rectificación, supresión, etc.). y por el claro desconocimiento de las condiciones de seguridad, los plazos de conservación de los datos o la comunicación de datos a terceros. Más información en [https://apdcat.gencat.cat/es/sala\\_de\\_prensa/notes\\_prensa/noticia/Recomanacio-ChatGPT](https://apdcat.gencat.cat/es/sala_de_prensa/notes_prensa/noticia/Recomanacio-ChatGPT)

El ensayo deberá tener una extensión de entre 5.000 y 7.000 palabras (10 a 14 páginas) sin contar anexos y lista de bibliografía. Es imperativo citar apropiadamente las fuentes utilizadas en el ensayo utilizando el formato APA.

**ENTREGA FINAL:** La versión definitiva ensayo para su evaluación final será entregada a más tardar el día **25 de abril de 2025 a las 16h** a través del espacio habilitado a tal efecto en el **aula virtual** de la asignatura. El plazo es único e improrrogable.

Se recuerda a los estudiantes que tendrá a su disposición una sesión optativa de tutoría el día (para la cual será necesaria cita previa) para discutir cualquier contenido o tema relacionado con la elaboración del ejercicio de *policy brief* y sobre la entrega final del *policy paper* de la asignatura. Los alumnos podrán plantear cualquier duda o cuestión o recibir feedback preliminar sobre los trabajos en preparación y que deberán entregarse en la fecha indicada en el apartado **evaluación** de la presente guía

#### **Sistema de recuperación:**

Para los participantes que no hubieran entregado uno de los dos trabajos planteados o la puntuación obtenida en la combinación de métodos de evaluación no fuera suficiente para aprobar la asignatura, se establecerá una prueba selectiva basada en un estudio de caso que incluirá una parte conceptual y una parte práctica y que se ofrecerá durante el siguiente período lectivo.

#### **Reglas de citación**

Todos los trabajos deberán incluir referencias bibliográficas y una bibliografía final en formato APA: <https://www.mendeley.com/guides/apa-citation-guide/>

#### **Integridad y honestidad académica**

La honestidad académica es uno de los valores más importantes de la **UPF Barcelona School of Management**. Saber elaborar una opinión propia a partir de referencias bibliográficas, dando el crédito que merecen sus creadores, es una oportunidad de aprendizaje que nos hace mejorar como profesionales y como personas y por lo tanto es una experiencia fundamental en nuestra formación.

El **plagio** es la **reproducción del contenido sustancial de otra obra haciéndolo pasar como propio**. El plagio se produce cuando se traspasan contenidos de otras fuentes sin especificar su referencia o citando la procedencia de la fuente de forma incompleta, impidiendo su recuperación.

El **plagio** está terminantemente prohibido y como tal, cualquier instancia detectada de plagio estará sujeta

a las medidas disciplinarias previstas en las normas de convivencia de la UPF-BSM que están disponibles en el siguiente enlace: [https://www.bsm.upf.edu/documents/transparencia/2023\\_24-upf-bsm-normes-convivencia.pdf](https://www.bsm.upf.edu/documents/transparencia/2023_24-upf-bsm-normes-convivencia.pdf)

Aquí tienes una sencilla guía sobre qué es la honestidad académica y cómo evitar incurrir en plagio: <https://slides.com/marianhervaslobo/honestidadacademica/fullscreen>

#### **Uso de la IA en las actividades de aprendizaje**

Utilizar **herramientas de inteligencia artificial** en la elaboración de tus trabajos, requiere referenciarlos e incluirlos en la bibliografía final **para evitar el plagio**. Las herramientas de IA generativa, como por ejemplo ChatGPT, podrán ser objeto del tema a analizar en el trabajo, pero su uso solo estará permitido si se comunica expresamente y que cualquier parte del trabajo compuesta, producida o creada directamente o con ayuda de estas herramientas sea plenamente identificada en el cuerpo del trabajo y cualesquiera fuentes secundarias utilizadas queden plenamente identificadas. **Cualquier ocultación del uso de estas herramientas será tratada como plagio** y como tal, estará sujeta a las medidas disciplinarias previstas en las normas de convivencia de la UPF-BSM.

La Universitat Pompeu Fabra pone a disposición de los estudiantes lineamientos sobre integridad académica y el uso de IA generativa:

<https://seuelectronica.upf.edu/documents/107805936/112656436/Instrucci%C3%B3+avaluaci%C3%B3+IAG+%281%29.pdf/908e2fbe-c8eb-f08b-6c62-22ce2b3c26be?t=1690367251359>

Además, el servicio de bibliotecas UPF ha elaborado una guía para el uso de herramientas de IA para la docencia y el aprendizaje:

[https://guiesbibtic.upf.edu/iag?\\_ga=2.12746238.878192489.1727788375-563707063.1643458903&\\_gl=1\\*99nie3\\*\\_ga\\*NTYzNzA3MDYzLjE2NDM0NTg5MDM.\\*\\_ga\\_WD336R1B7H\\*MTcyNzgxMjY0Ny4xNDMuMS4xNzI3ODEyNjQ4LjU5LjAuMA.#](https://guiesbibtic.upf.edu/iag?_ga=2.12746238.878192489.1727788375-563707063.1643458903&_gl=1*99nie3*_ga*NTYzNzA3MDYzLjE2NDM0NTg5MDM.*_ga_WD336R1B7H*MTcyNzgxMjY0Ny4xNDMuMS4xNzI3ODEyNjQ4LjU5LjAuMA.#)

Dicha guía incluye una sección específica **sobre el uso de la IA generativa en trabajos académicos** y que contiene prescripciones sobre **como citar** fuentes de IA generativa de manera adecuada para evitar caer en plagio: <https://guiesbibtic.upf.edu/iag/treballs-academics>

Finalmente, los estudiantes han de ser conscientes que, para la Agencia Catalana de Protección de Datos, el uso de herramientas de IA generativa comporta **riesgos para la privacidad y la protección de datos personales** entre otras razones, por la imposibilidad práctica de ejercer los derechos de autodeterminación informativa (acceso, rectificación, supresión, etc.) y por el claro desconocimiento de las condiciones de seguridad, los plazos de conservación de los datos o la comunicación de datos a terceros en el contexto de estas herramientas. Más información en

[https://apdcat.gencat.cat/es/sala\\_de\\_prensa/notes\\_prensa/noticia/Recomanacio-ChatGPT](https://apdcat.gencat.cat/es/sala_de_prensa/notes_prensa/noticia/Recomanacio-ChatGPT)

#### **Actividades formativas**

- Sesiones magistrales
- Lectura de textos para adquirir conocimientos, propiciar la discusión en clase y expandir lo discutido en las mismas
- Debate abierto en clase
- Presentación oral de un trabajo
- Presentación escrita de un trabajo

#### **PROFESORADO**

**Rodrigo Cetina Presuel**. Decado Asociado de Educación y Asuntos Académicos de la UPF Barcelona School of Management y Senior Lecturer in Law Public Policy de esta casa así como coordinador del Máster Universitario en Políticas Públicas y Sociales. Doctor en Derecho y Ciencias de la

Información por la Universidad Complutense de Madrid, ha sido profesor e investigador en diversas universidades de Estados Unidos durante más de una década, trabajando en instituciones como New York University, la City University of New York, Emerson College, Lasell University y la Universidad de Harvard, en donde ha sido investigador en el Institute for Global Law and Policy de la Harvard Law School. Es autor de dos volúmenes editados y de dos docenas de artículos académicos publicados en revistas especializadas y es experto en temas relacionados con el derecho de la información, la regulación de plataformas digitales, la protección de los procesos electorales y el combate a la desinformación, la protección de datos personales y el derecho de autor así como de la adopción e implantación de inteligencia artificial en la administración pública.

## BIBLIOGRAFIA

En esta asignatura, y dado que no se espera que la mayoría de los participantes sean abogados o tengan un background legal, se han habilitado dos recursos a través de NotebookLM que permite a los estudiantes acceder al contenido de las leyes más relevantes en materia de protección de datos personales y respecto de la regulación de la inteligencia artificial en la Unión Europea:

- Notebook sobre [Protección de datos](#).
- Notebook sobre [Regulación de Inteligencia Artificial](#).

### Primera sesión.

- Solon Barocas, danah boyd (2017) [Engaging the Ethics of Data Science in Practice](#), Communications of the ACM.
- Ethan Zuckerman (2016) [The Perils of Using Technology to Solve Other People's Problems](#), The Atlantic.
- Eric Horvitz, Deirdre Mulligan (2015) [Data, privacy, and the greater good](#), Science.
- Fernando Batista (2016). [La dignidad de la persona en la Constitución española: naturaleza jurídica y funciones](#). Cuest. Const. no.14 Ciudad de México ene./jun. 2006
- Victor Salgado (2010). [Intimidad, privacidad y honor en Internet: nuestros derechos en riesgo](#). Telos 85, págs. 69-79.
- Comisión Europea. [¿Qué son los datos personales?](#)
- Cristina Pauner. (2015). [La libertad de expresión e información como límite al derecho de protección de datos: la excepción periodística](#). Teoría y realidad constitucional, 36, 377–398.
- Evgeny Morozov. (2023). [The True Threat of Artificial Intelligence](#). The New York Times.
- **Vídeo:** Harris, S. [‘Can we build AI without losing control over it?’](#), TED talk, October 2016.
- **Vídeo:** Bostrom, N. [‘What happens when our computers get smarter than we are?’](#), TED talk, April 2015

### Segunda sesión.

- Hildebrandt, Mireille. (2019). [Privacy As Protection of the Incomputable Self: From Agnostic to Agonistic Machine Learning](#). Theoretical Inquiries of Law.19(1).
- Nicholas Carr. (2014). [The Limits of Social Engineering](#). MIT Technology Review.
- Solove, Daniel J. (2013). [Introduction: Privacy Self-Management and the Consent Dilemma](#). Harvard Law Review 126(7):1880–1903. Solo leer pp. 1882 – 1893.
- Agencia Española de Protección de Datos. [Guía del Reglamento General de Protección de datos](#).
- Roselló Mallol. [El RGPD y los difuntos](#).
- L. T. Liu, S. Dean, E. Rolf, M. Simchowitz, M. Hardt, [Delayed Impact of Fair Machine Learning](#), blogpost on Berkeley Artificial Intelligence Research, 17 May 2018
- **Vídeo:** Tufekci, Z. [‘Machine intelligence makes human morals more important’](#), TED talk, 11

### Tercera sesión.

- Ian Ramos González, I. (2021). [Del anonimato a la hiper visualización: ver y ser vistos en la época de internet](#). Hastapenak, 1(1), 144–157.
- Robert Bodle. (2013). [The ethics of online anonymity or Zuckerberg vs. "Moot"](#). ACM SIGCAS Computers and Society, Volume 43, Issue 1, pp. 22-35.
- Latanya Sweeney (2000) [Simple Demographics Often Identify People Uniquely](#). CMU Data Privacy Working Paper 3.
- Scott Berinato (2015) [There's No Such Thing as Anonymous Data](#). Harvard Business Review.
- Brian X. Chen. (2022). [Security Cameras Make Us Feel Safe, but Are They Worth the Invasion?](#) The New York Times.
- Jasmine McNealy (2022). [Sonic Privacy](#). Yale Journal of Law & Technology, vol. 24, pp. 1-26.
- Matt Burgess. (2023). [How Your New Car Tracks You](#). Wired.
- Cécile de Terwangne. (2012). [Privacidad en Internet y el derecho a ser olvidado/derecho al olvido](#). IDP. Revista de Internet, Derecho y Política, núm. 13, febrero, 2012, pp. 53-66
- Laura Silderleib. (2016). [El Derecho al olvido y la persistencia de la memoria](#). Inf. cult. soc. no.35 Ciudad Autónoma de Buenos Aires dic. 2016.
- Yadira Nieves-Lahaba & Gloria Ponjuan-Dante. (2021). [Tratamiento de datos personales y acceso a la información. Visiones a partir de la academia](#). Universitas (Quito, Ecuador), 35, 167–185. <https://doi.org/10.17163/uni.n35.2021.08>
- Lawrence Lessig (2009). [Against Transparency](#). The New Republic.
- Cynthia Dwork & Aaron Roth (2014) The Promise of Differential Privacy (Solo leer Capítulo 1, el resto del libro es opcional), [The Algorithmic Foundations of Differential Privacy](#), NOW Publishers.

### Cuarta Sesión.

- Shoshana Zuboff, Shoshana (2015). [Big Other: Surveillance Capitalism and the Prospects of an Information Civilization](#). Journal of Information Technology 30, 75–89.
- Shoshana Zuboff (2022). [Surveillance Capitalism or Democracy? The Death Match of Institutional Orders and the Politics of Knowledge in Our Information Civilization](#) Organization Theory, 3(3).
- Eduardo Porter (2018). [Your Data Is Crucial to a Robotic Age. Shouldn't You Be Paid for It?](#) The New York Times.
- Aleksandra Korolova (2011) [Privacy Violations Using Microtargeted Ads: A Case Study](#), Journal of Privacy and Confidentiality.
- Piotr Sapiezynski, Avijit Ghosh, Levi Kaplan, Alan Mislove, Aaron Rieke (2019) [Algorithms that "Don't See Color": Comparing Biases in Lookalike and Special Ad Audiences](#), Working paper.
- CBC Marketplace (2017). [How companies use personal data to charge different people different prices for the same product](#).
- A. Chander, [the Racist Algorithm](#), 115 Michigan Law Review 1023, 1046 (2017).
- Rodrigo Cetina Presuel & José Manuel Martínez Sierra (2019). [Algorithms and the News: Social Media Platforms as News Publishers and Distributors](#), Revista de Comunicación, vol. 18, no. 2, pp. 261-285.

### Quinta Sesión.

- Nick Couldry & Ulises A. Mejias. (2019). [Data Colonialism: Rethinking Big Data's Relation to the](#)



[Contemporary Subject](#). Television & new media 20, no. 4, pp. 336–349.

- Stefano Calzati, S. (2021). [Decolonising “Data Colonialism” Propositions for Investigating the Realpolitik of Today’s Networked Ecology](#). Television & New Media, 22(8), 914–929.
- Rodrigo Cetina Presuel & José Manuel Martínez Sierra. (2022). [The Adoption of Artificial Intelligence in Bureaucratic Decision-making: A Weberian Perspective](#). Digital Government Research and Practice. Forthcoming.
- Celeste Kidd & Abeba Birhane, A. (2023). [How AI can distort human beliefs](#). Science (American Association for the Advancement of Science), 380(6651), 1222–1223.
- Dan Bateyko & Muira McCammon. (2019). [After DeepNude, ideas for more conscientious coverage of synthetic media](#). Columbia Journalism Review.
- Adam Satariano & Paul Mozur (2023). [The People Onscreen Are Fake. The Disinformation Is Real](#). The New York Times.
- Huo Jignan. (2023). [AI-generated text is hard to spot. It could play a big role in the 2024 campaign](#). NPR News.
- Waleed Rikab. (2023). [Generative AI Is Enabling Fraud and Misinformation](#). Medium.
- Reuben Binns et al. (2018). “[It’s Reducing a Human Being to a Percentage’: Perceptions of Justice in Algorithmic Decisions](#)”. Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, 1–14.
- Ales Završnik (2021). [Algorithmic justice: Algorithms and big data in criminal justice settings](#). European Journal of Criminology, 18(5), 623–642. <https://doi.org/10.1177/1477370819876762>