

# Seguridad, privacidad y aspectos legales

## Presentación de la asignatura

---

Álvaro López García

Grupo de Computación Avanzada y e-Ciencia  
Instituto de Física de Cantabria (IFCA) - CSIC-UC

Máster universitario en ciencia de datos / Master in Data Science



CONSEJO SUPERIOR DE INVESTIGACIONES CIENTÍFICAS

**CSIC**



## Parte I

### Presentación de la asignatura

# Tabla de contenidos

1. Información, horario, bibliografía

2. Motivación

## Información, horario, bibliografía

---

## Descripción

En esta asignatura el estudiante conocerá los mecanismos básicos para proporcionar un acceso seguro a los recursos en la red, cómo tener en cuenta la debida protección de datos personales, y las condiciones de explotación de datos y software mediante los diferentes tipos de licencias existentes. Asimismo se abordarán aspectos éticos en la ciencia de datos.

# Contenidos

Parte I: Introducción a la seguridad de la información

Información, horario, bibliografía

Motivación

Parte II: Tecnologías para la protección de la información

Parte III: Privacidad y anonimato

Part IV: Aspectos legales

Parte V: Ética en la ciencia de datos

Parte VI: Aplicación en el entorno Open Science

## Profesores.

- Álvaro López García , CSIC (aloga@ifca.unican.es).
- Pablo Orviz Fernández, CSIC (orviz@ifca.unican.es).
- David Rodriguez González, CSIC (drodrig@ifca.unican.es).

## Evaluación.

- Examen: 40 %
- Valoración de informes y trabajos: 60 %

- Clases teóricas + prácticas
- Necesario portátil
- Entregas a lo largo de curso de cuestiones prácticas
- Planificación:

**Feb 02 — 17:30-19:30h** Introducción

**Feb 04 — 17:30-19:30h** Tecnologías

**Feb 09 — 17:30-19:30h** Tecnologías

**Feb 11 — 17:30-19:30h** Aspectos legales

**Feb 16 — 17:30-19:30h** Aspectos legales

**Feb 18 — 17:30-19:30h** Aspectos legales

**Feb 23 — 17:30-19:30h** Anonimato

**Feb 25 — 17:30-19:30h** Anonimato

**Mar 02 — 17:30-19:30h** Anonimato

**Mar 04 — 17:30-19:30h** Etica

**Mar 09 — 17:30-19:30h** Aplicación Open Science

**Mar 11 — 17:30-19:30h** -

**Mar 17 — 17:30-19:30h** Presentación de trabajos

**Mar 19 — 17:30-19:30h** Examen



- KITCHIN, Rob. The data revolution: Big data, open data, data infrastructures and their consequences. Sage, 2014.
- Green, Ben, Gabe Cunningham, Ariel Ekblaw, Paul Kominers, Andrew Linzer, and Susan Crawford. 2017. Open Data Privacy (2017). Berkman Klein Center for Internet & Society Research Publication.
- EC's trustworthy AI
- EC's ethics and data protection
- Commission Report on safety and liability implications of AI, the Internet of Things and Robotics
- White Paper on Artificial Intelligence: a European approach to excellence and trust
- REGLAMENTO (UE) 2016/679
- BOE-A-2018-16673
- Guía protección de datos AEPD
- Google AI Ethics

# Motivación

---

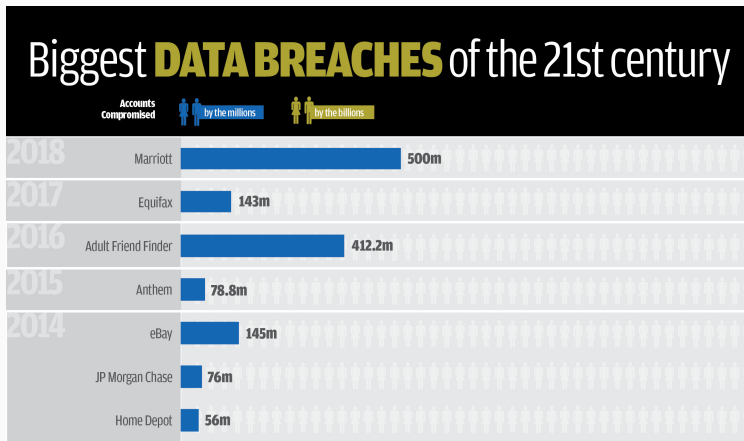
“The World’s most valuable resource is no longer oil, but data” – The Economist<sup>1</sup>

- Los datos tienen un alto valor, según el ámbito:
  - Económico (por ejemplo, transacciones financieras),
  - personal (por ejemplo, datos médicos),
  - político (por ejemplo, sesgo para modificar intención de voto), etc.
- Los datos están en riesgo: pueden ser robados, saboteados, manipulados, divulgados sin permiso, etc.; de forma consciente o no.
- **Responsabilidad:** Los datos pueden ser usados de forma correcta, ética o no.
  - Unas pocas personas pueden tener un tremendo impacto y causar un daño extremadamente grande.
  - Falta de consentimiento en experimentos con nuestros datos.
  - Comportamiento inesperado de los algoritmos implementados.
  - **Las decisiones que se tomen en base a los datos pueden afectar a las personas.**
- Impacto legal, ético, de reputación, etc.

<sup>1</sup>The Economist

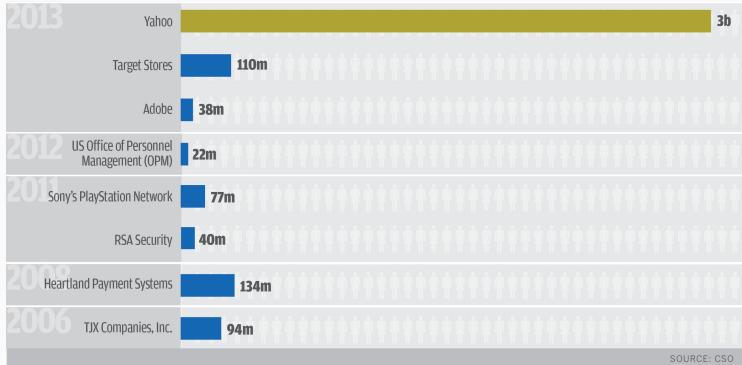
# Seguridad, privacidad, aspectos legales, ética

Motivación: impacto y daño



# Seguridad, privacidad, aspectos legales, ética

Motivación: impacto y daño





## Experimental evidence of massive-scale emotional contagion through social networks

Adam D. I. Kramer<sup>a,1</sup>, Jamie E. Guillory<sup>b,2</sup>, and Jeffrey T. Hancock<sup>b,c</sup>

<sup>a</sup>Core Data Science Team, Facebook, Inc., Menlo Park, CA 94025; and Departments of <sup>b</sup>Communication and <sup>c</sup>Information Science, Cornell University, Ithaca, NY 14853

Edited by Susan T. Fiske, Princeton University, Princeton, NJ, and approved March 25, 2014 (received for review October 23, 2013)

Experimental evidence of massive-scale emotional contagion through social networks



WORKING PAPER SERIES

## On the Rise of the FinTechs—Credit Scoring using Digital Footprints

On the Rise of the FinTechs—Credit Scoring using Digital Footprints

# Seguridad, privacidad, aspectos legales, ética

Motivación: Comportamiento inesperado

- Ejemplo: Análisis de riesgo de criminalidad.
- Método más “objetivo”: basado en un índice de riesgo según datos personales, como por ejemplo
  - Datos de redes sociales (¿es la persona violenta?)
  - Localización (¿dónde vive?, ¿por donde se mueve?)
  - Datos demográficos
- Ejemplo real: Índice de reincidencia en EEUU
  - Crimen + Comportamiento + Datos demográficos -> Libertad condicional sí/no.
  - Problema: Diferencias raciales se ven reflejadas en datos históricos (e.g. individuos negros tienen sentencias más largas por mismos crímenes <sup>2</sup>, mayor violencia policial, etc.)
  - Resultado: El algoritmo está perpetuando los sesgos del pasado.

---

<sup>2</sup>Carson, E. Ann, and William J. Sabol. 2012. “Prisoners in 2011.” NCJ 239808. Washington, DC: US Department of Justice, Office of Justice Programs, Bureau of Justice Statistics.



Preguntas?