Fundació "la Caixa"

PalauMacaya

Computer Vision Center

UNIVERSITAT DE BARCELONA

VIDEOVIGILANCIA Y SEGURIDAD

Sergio Escalera, Catedrático, ICREA Academia
Pau Buch-Cardona
HuPBA Human Behavior Analysis Group
www.sergioescalera.com

PROYECTO SELECCIONADO **CONVOCATORIA** PALAU MACAYA #IAeticaBCN #PalauMacaya

9/12/2020

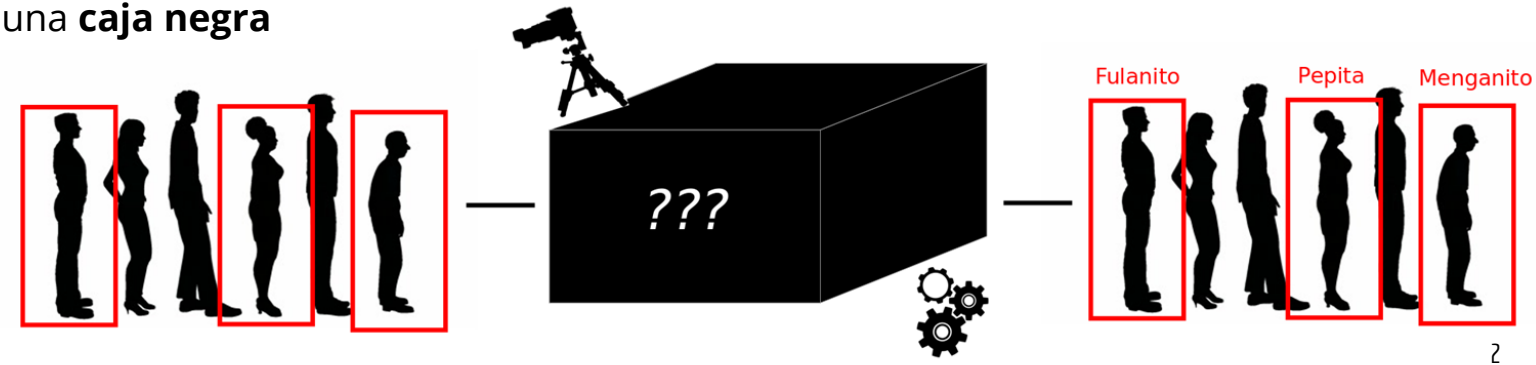
VIDEOVIGILANCIA Y SEGURIDAD

Conceptos:

- Videovigilancia
- Seguridad

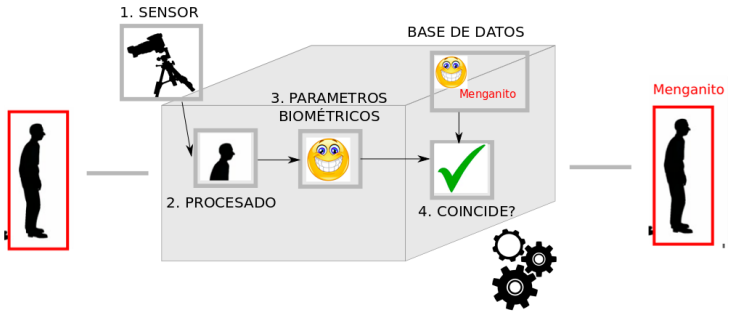
Percepción:

- Nos espían
- Sistema es una **caja negra**



BIOMETRÍA - (dentro de la caja negra)

Bio (biología/cuerpo) - **metría** (medición)
Nos sirve para describir de forma unívoca a una persona.



Ejemplo básico de un sistema biométrico automático

Cualquier sistema que la use debe ser:

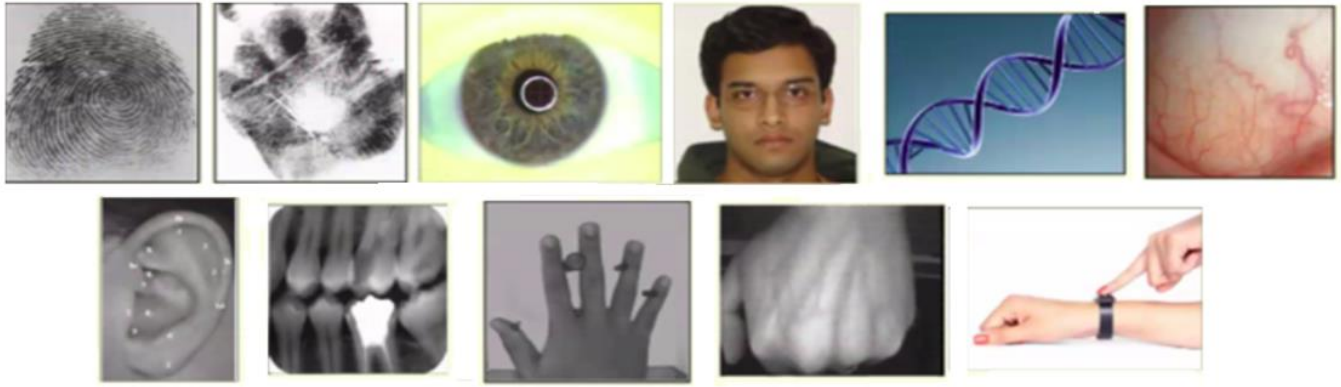
- Universal
- Único
- Permanente
- Rápido de procesar
- Aceptado por la sociedad
- Difícil de reproducir artificialmente

Inicios - Documento de identificación personal - 19XX

SISTEMAS BIOMÉTRICOS - clasificación

Según su naturaleza, los sistemas biométricos se clasifican entre:

- Fisiológicos
  - Huellas dactilares
  - Capilares de la mano
  - Análisis del iris
  - **Reconocimiento facial**
  - ADN
  - Venas oculares
  - Forma de las orejas
  - Estructura dental
  - Estructura de la mano
  - Venas de la mano
  - Datos cardíacos



- Comportamentales
  - Reconocimiento de voz
  - Signatura
  - Ritmo de tecleo
  - Otros comportamentos particulares (el andar)

SISTEMAS BIOMÉTRICOS - aplicaciones (1/2)

Control de Acceso Remoto

PROBLEMA:
usuario y contraseña comprometidos.

SOLUCIÓN:
Huella dactilar e iris.
Rápido y fácil.

Control de Acceso Físico

PROBLEMA:
Llaves y tarjetas (copia, robo, olvido).

SOLUCIÓN:
Huella dactilar y capilares de la mano.

Sistema de biometría por huella dactilar

Control de Fichaje

PROBLEMA:
Múltiples fichajes por parte de 1 trabajador.

SOLUCIÓN:
Huella dactilar y geometría de la mano e iris.

Sistema de biometría por análisis de iris

Seguridad (policía)

PROBLEMA:
Identificación eficaz de criminales reincidentes.

SOLUCIÓN:
Huella dactilar (digital), iris, reconocimiento facial, capilares de la mano.

SISTEMAS BIOMÉTRICOS - aplicaciones (2/2)

Videovigilancia - Mayoritariamente utilizan Tecnología de Reconocimiento Facial (TRF).

Régimen abierto - Población informada. Fines disuasorios

Régimen encubierto - Población NO informada. Control en masa.

Búsqueda de personas - Personas desaparecidas y criminales buscados por la policía.

Rebecca Reid/National Pictures/Reuters

Identificación por conductas y actividades sospechosas - Identificar participantes mediante TRF sobre vídeos guardados.

SISTEMAS de VIDEOVIGILANCIA Y SEGURIDAD - Frequently Asked Questions FAQs -

¿QUÉ TECNOLOGÍA SE UTILIZA EN LOS SISTEMAS DE VIDEOVIGILANCIA?

¿DÓNDE SE IMPLEMENTAN ESTOS SISTEMAS?

¿CÓMO AFECTAN A NUESTRA PRIVACIDAD?

¿QUÉ USO SE LES DA?

¿NOS AFECTAN A TODOS POR IGUAL?

¿CÓMO ES EL FUTURO DE LA TRF?

SISTEMAS de VIDEOVIGILANCIA Y SEGURIDAD - Frequently Asked Questions FAQs -

¿QUÉ TECNOLOGÍA SE UTILIZA EN LOS SISTEMAS DE VIDEOVIGILANCIA?

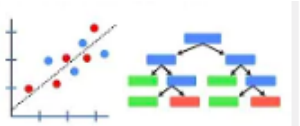
¿DÓNDE SE IMPLEMENTAN ESTOS SISTEMAS?

¿QUÉ USO SE LES DA?

RECONOCIMIENTO FACIAL EN SISTEMAS DE VIDEOVIGILANCIA

¿SE PUEDE AUTOMATIZAR?

Datos digitalizados + patrones geométricos + Big Data. - **Inteligencia Artificial (IA)**



¿POR QUÉ ES INTERESANTE PODER AUTOMATIZAR?

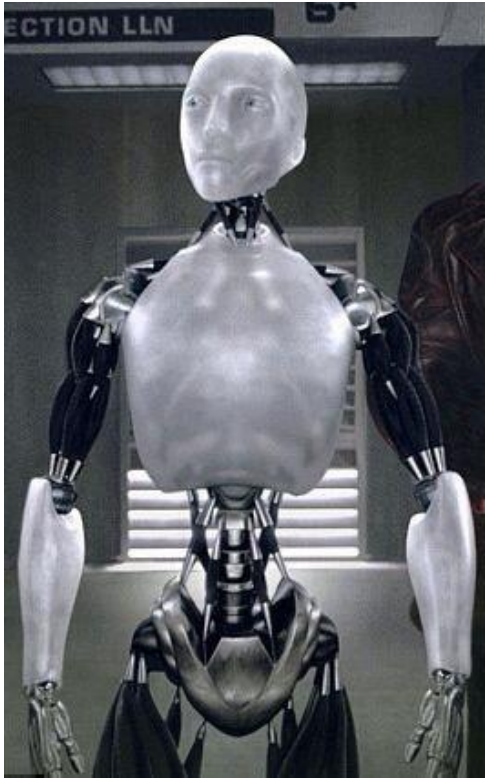
1.

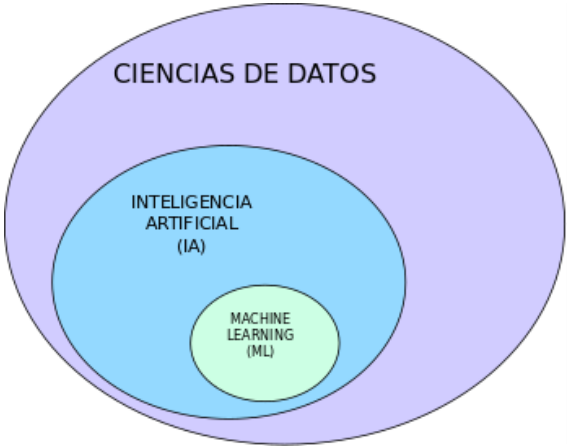
Criterios de identificación objetiva. No se cansa. - **Invariante a la variedad poblacional**

2.

Proceso de grandes cantidades de datos. - **Rápido y en cualquier momento - permite rápida intervención**

INTELIGENCIA ARTIFICIAL - mito vs. realidad





- Subcampo dentro de Data Science.
- Conjunto de herramientas matemáticas y estadísticas en búsqueda de patrones.
- Optimización y predicción mediante experiencia recolectada en los datos (*"razonamiento humano"*).

IMPLEMENTACIÓN BÁSICA DE UN SISTEMA DE IA

Corazón de cualquier sistema de data science - IA:
Programación de <u>algoritmos:</u>

- Conjunto de instrucciones o reglas definidas
- No-ambiguas
- Ordenadas y finitas

OBJETIVO DE UN ALGORITMO:

- Solucionar un problema
- Realizar un cómputo
- Procesar datos

ESTADO INICIAL + INPUT → ESTADO FINAL + SOLUCIÓN

```python
# CONTROL DE CALIDAD DE UNA LÁMPARA

respuesta_1 = input('¿Funciona la lámpara? \n')

if respuesta_1.upper() == 'NO':

    respuesta_2 = input('¿Está enchufada? \n')

    if respuesta_2.upper() == 'NO':
        print('SOLUCIÓN: Enchufe la lámpara')

    elif respuesta_2.upper() == 'SI':

        respuesta_3 = input('¿El foco está quemado? \n')

        if respuesta_3.upper() == 'NO':
            print('SOLUCIÓN: Compre una nueva lámpara')

        elif respuesta_3.upper() == 'SI':
            print('SOLUCIÓN: Reemplazar la bombilla')

        else:
            print('No entiendo su respuesta :(')

    else:
        print('No entiendo su respuesta :(')

elif respuesta_1.upper() == 'SI':
    print('Estupendo! :)')

else:
    print('No entiendo su respuesta :(')
```

DATA SCIENCE - aplicaciones reales

Medicina

ONCORA MEDICAL

Tratamiento personalizado de quimio y radio a partir de resultados de más de 50k pacientes anteriores.

Oncora Medical

Logística

UPS

Cálculo de la ruta óptima de reparto. Variables cómo el tiempo en la ciudad se incorporan.

UPS

Deportes

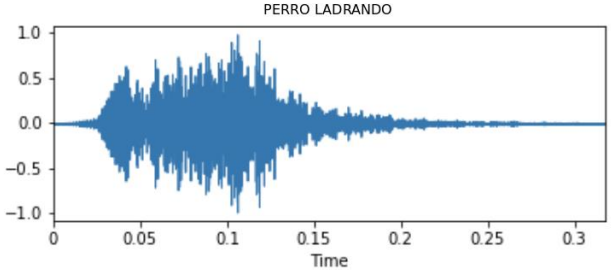
LIVERPOOL

Optimización de plantilla en base al análisis de datos del rendimiento de jugadores disponibles al mercado.

Liverpool F.C.

DATA SCIENCE - TIPOS DE DATOS

DATOS AUDIO

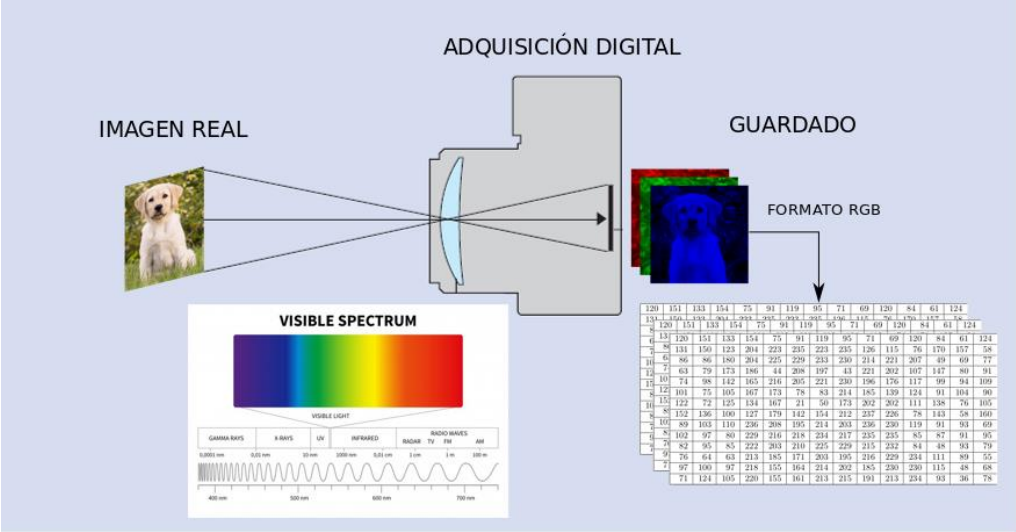


DATOS TEXTO

Lorem Ipsum

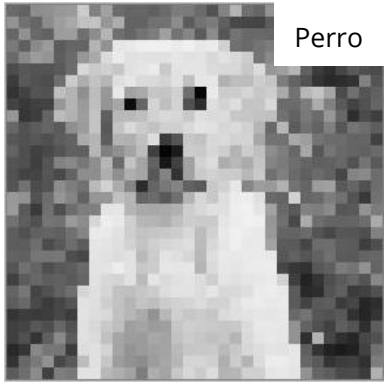
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed eiusmod tempor incidunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquid ex ea commodi consequat. Quis aute iure reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint obcaecat cupiditat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

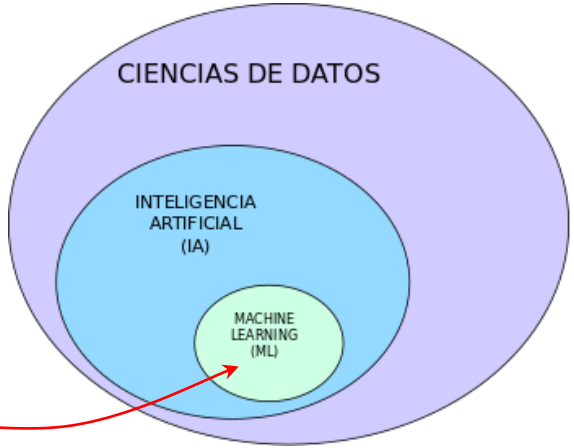
DATOS VISUALES - COMPUTER VISION

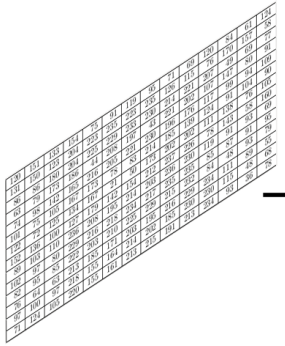


COMPUTER VISION

120	151	133	154	75	91	119	95	71	69	120	8		
131	150	123	204	223	235	223	235	126	115	76	17	???	
86	86	180	204	225	229	233	230	214	221	207	49	69	77
63	79	173	186	44	208	197	43	221	202	107	147	80	91
74	98	142	165	216	205	221	230	196	176	117	99	94	109
101	75	105	167	173	78	83	214	185	139	124	91	104	90
122	72	125	134	167	21	50	173	202	202	111	138	76	105
152	136	100	127	179	142	154	212	237	226	78	143	58	160
89	103	110	236	208	195	214	203	236	230	119	91	93	69
102	97	80	229	216	218	234	217	235	235	85	87	91	95
82	95	85	222	203	210	225	229	215	232	84	48	93	79
76	64	63	213	185	171	203	195	216	229	234	111	89	55
97	100	97	218	155	164	214	202	185	230	230	115	48	68
71	124	105	220	155	161	213	215	191	213	234	93	36	78







Perro

COMPUTER VISION - aplicaciones reales

Automoción

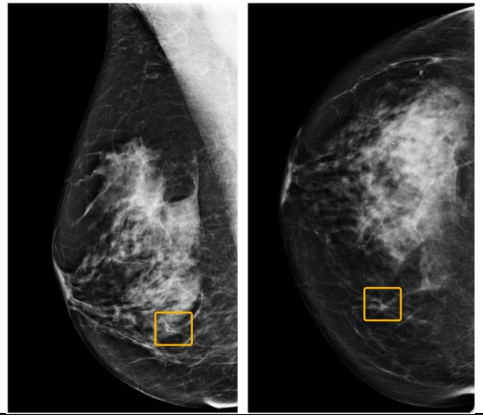
TESLA

Mediante 8 cámaras, se procesa vídeo en tiempo real para detectar objetos y señales en la vía.

Medicina

NATURE

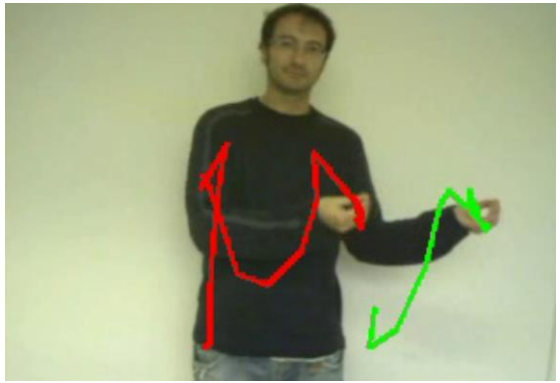
Detección precoz de cáncer de mama a partir del análisis de MRI.



Comunicación

HuPBA

Interpretación en tiempo real del lenguaje de signos.



"NECESITO MÁS INFORMACIÓN"

SISTEMAS DE RECONOCIMIENTO FACIAL (RF)

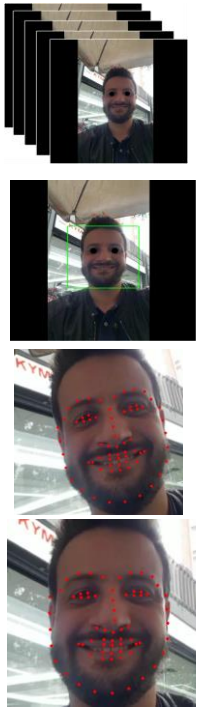
Datos Entrada (Video Frames)

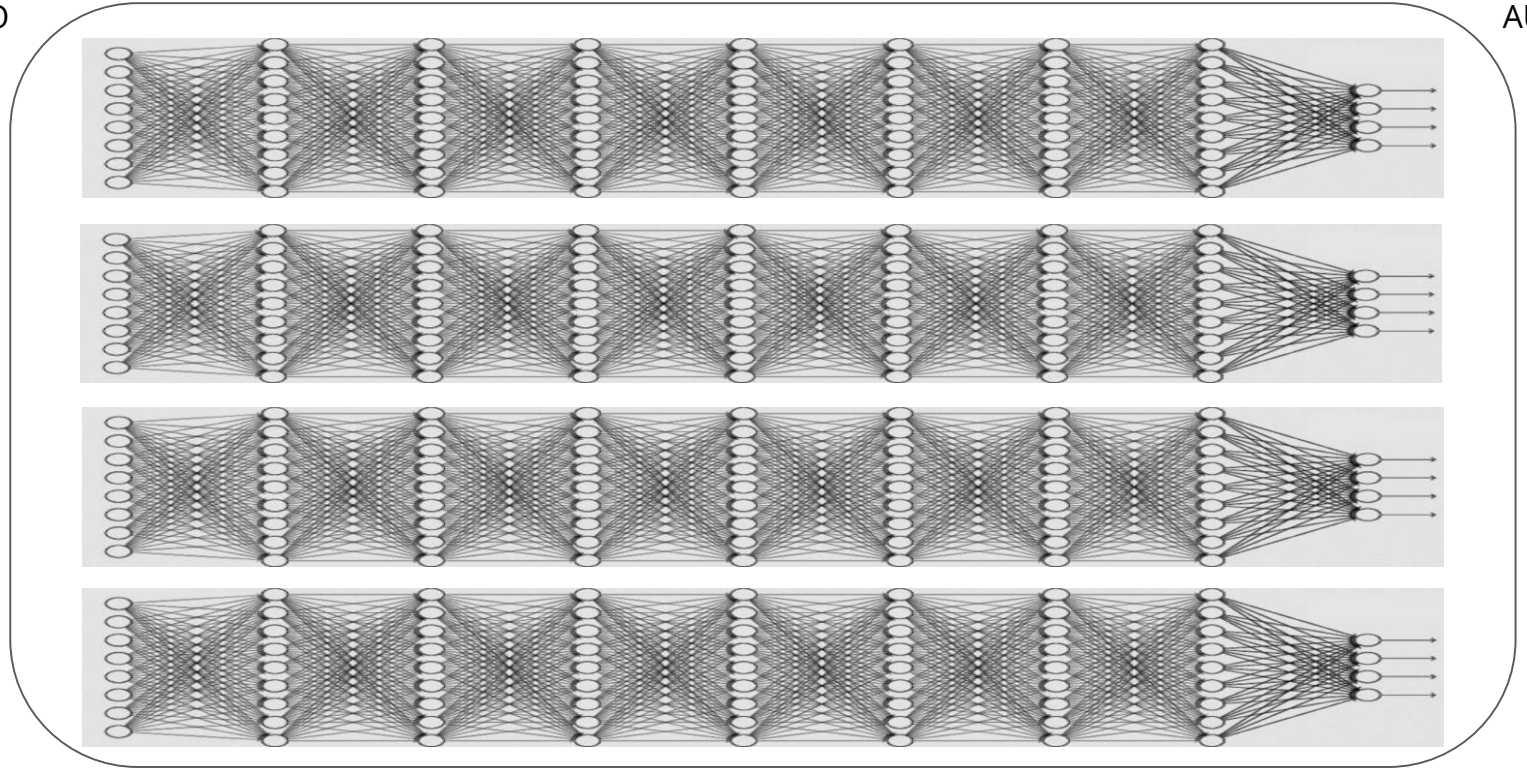
Resultado (ID, probabilidad):
`Sergio, 98,4%`

SISTEMAS DE RECONOCIMIENTO FACIAL (RF)

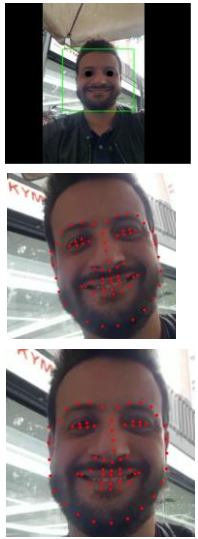
IA EN RF - REDES NEURONALES (deep learning)

ENTRADA AL ALGORITMO





SALIDA AÚTOMÁTICA



(ID, probabilidad):
Sergio, 98,4%

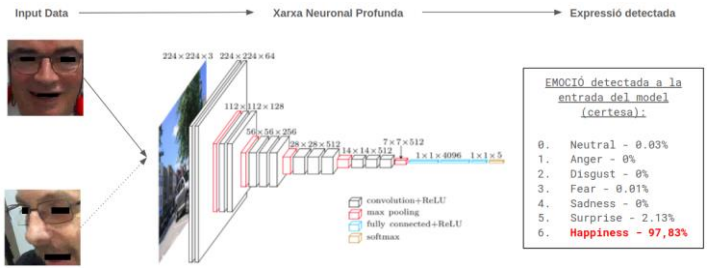
SISTEMAS DE RF - aplicaciones reales

Creativo

FaceApp
Aplicación de filtros (cambios de género, edad, etc.).

Medicina

HuPBA
Detección automática de expresiones faciales en pacientes con parálisis facial en ejercicios de rehabilitación.



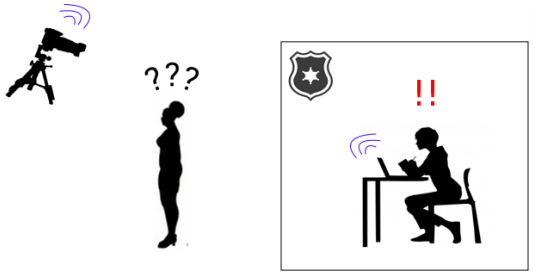
Seguridad

Verificación automática de pasaportes en aeropuertos.

RF en VIDEOVIGILANCIA - usos

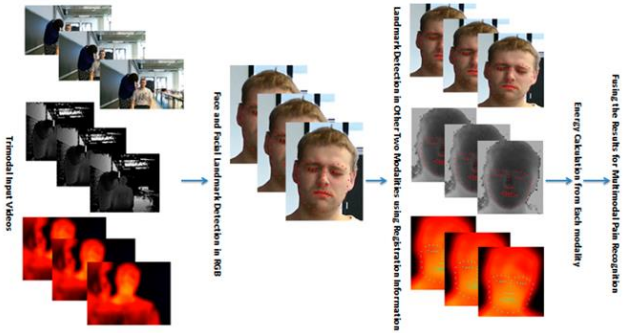
1.

Encontrar persona perdida.



2.

Medicina - control de dolor

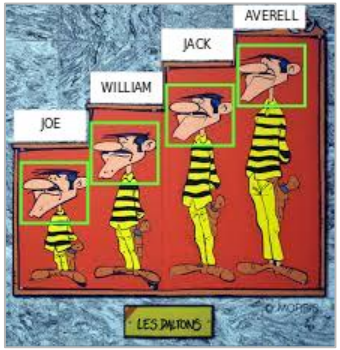


3.

Seguridad en dispositivos personales

4.

Identificar un criminal



5.

Control de fronteras

6.

Seguridad ciudadana

RF en VIDEOVIGILANCIA y SEGURIDAD - ORÍGENES

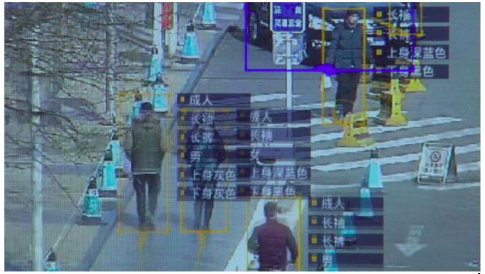
- ESTADOS UNIDOS - FLORIDA 2001
- Partido de la Super Bowl (fútbol americano)
- Antes del 9/11 - TRF inexistente
- Primer sistema de RF de *Régimen Encubierto*
  - ~ 70.000 asistentes al estadio
  - Identificación de criminales entre la multitud
- 19 sospechosos buscados identificados
  - Delitos menores
  - Ninguno de ellos fue arrestado

- Preocupación - privacidad

VIDEOVIGILANCIA y SEGURIDAD - MUNDO

CHINA

- Red de videovigilancia más grande del mundo.
- Base de datos de 20-30 millones de sospechosos.
- El sistema RF es capaz de identificar y seguir a unas 1.400millones de personas.



ESTADOS UNIDOS

- Después de los ataques del 9/11, inversión en sistemas de RF se incrementó.
- Su penetración en habitante / cámara es similar a la de China.
- Enfoque de videovigilancia al sector privado.

VIDEOVIGILANCIA y SEGURIDAD - MUNDO

INDIA

- Sistema de RF automático más extenso del mundo previsto para 2021-2022
- Solución a la escasez de efectivos policiales en el país.

REINO UNIDO

- Es considerado uno de los países con más videovigilancia del mundo.
- Durante muchos años efecto más disuasorio que real.

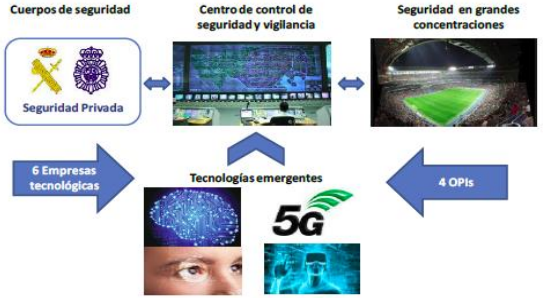
VIDEOVIGILANCIA y SEGURIDAD - ESPAÑA

Control aeropuerto

- Proyecto piloto.
- Sistema de RF para el embarque en el aeropuerto de Barajas, sin presentar documentación.
- Agilidad y seguridad.

Proyecto AI MARS

- Uso de las TRF para control policial (único en Europa). Desarrollo desde 2018. Lanzamiento en 2022. - 5,3M€
- Agentes de policía con gafas de realidad aumentada y IA.
- Identificación de delincuentes y objetos sospechosos entre multitud de gente.



SISTEMAS de VIDEOVIGILANCIA Y SEGURIDAD - Frequently Asked Questions FAQs -

¿CÓMO AFECTAN A NUESTRA PRIVACIDAD?

¿NOS AFECTAN A TODOS POR IGUAL?

¿QUÉ USO SE LES DA?

PRIVACIDAD - DEFINICIONES

- El ámbito de la **vida personal de un individuo**, quien se desarrolla en un espacio reservado, el cual tiene como propósito principal mantenerse **confidencial**. – Wikipedia.
- "Privacidad es el derecho de **permitir estar solo**" - Samuel Warren and Louis Brandeis (1890).
- "Privacidad es el poder de las personas, grupos o instituciones de **poder elegir cuánta información sobre ellos mismos es comunicada** a los demás." - Alan Westin (1970).
- "Privacidad es el **derecho de la gente a guardar información personal**, que otros podrían utilizar en su contra." - Richard Posner (1983).
- A nivel europeo GDPR (**Reglamento General de Protección de Datos**): Asegurar confidencialidad y privacidad de los datos.

CONTROVERSIA - RF & VIDEOVIGILANCIA (1/3)

CONTROL DE MASAS

1.

Abril 2013 - Ataques terroristas en Boston.

- Fallo del sistema - los sospechosos, que figuraban en la base de datos.
- Descrédito, pero abrió posibilidades.

2.

Mayo 2020 - Potencial criminal. Univ. Harrisburg.

- "Precisión del 80%" predecir criminales por sus rasgos faciales.
- Independiente de etnia.
- Polémica. Ya no disponible.

3.

Enero 2020 Detroit - Primer caso conocido de error en sistema RF en América.

- Se culpabilizó el trabajo de la policía.

4.

Julio 2020 Detroit - Segundo caso conocido de error de RF en América.

- Proceso de investigación irregular.

CONTROVERSIA - RF & VIDEOVIGILANCIA (2/3)

DISCRIMINACIÓN ÉTNICA

1.

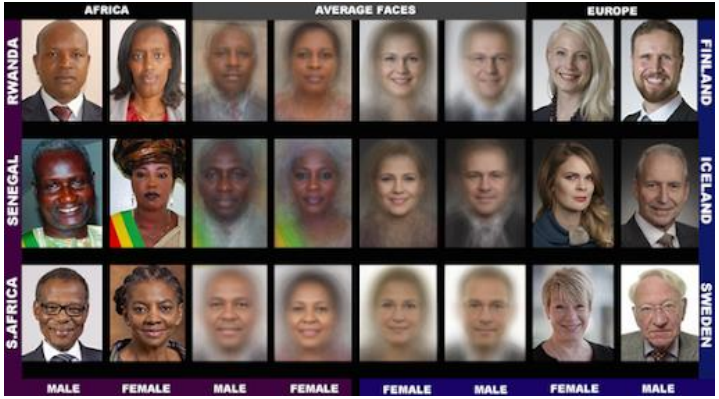
Julio 2015 - Google se disculpa.

- Su software en RF identificó a dos personas negras como gorilas.

2.

Febrero 2018 - Artículo Gender Shades de Joy Buolamwini

- Sesgo étnico y de género de softwares comerciales de RF de Microsoft, IBM y Face ++
- Reconoce mejor hombres caucásicos que mujeres negras.



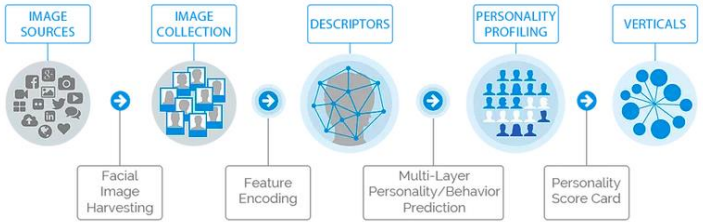
CONTROVERSIA - RF & VIDEOVIGILANCIA (3/3)

VIOLACIÓN DE LA PRIVACIDAD / MALOS USOS

1.

Mayo 2016 - Faception (Israel).

- Con 1 sola foto, su software en RF es capaz de detectar:
  - Criminales
  - Jugadores de poker
  - Pedófilos
  - Terroristas
  - Jugadores de bingo
  - Gente inteligente



2.

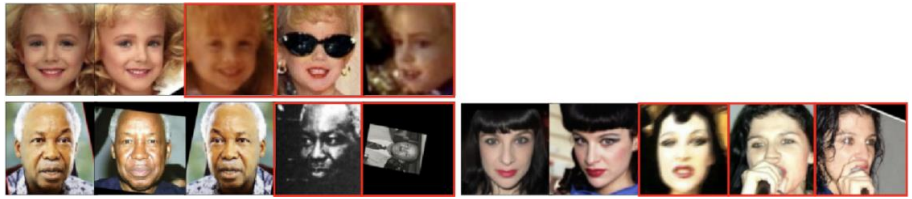
Octubre 2017 - Artículo Gaydar de la Universidad de Stanford.

- Detección de la orientación sexual de una persona a partir de una foto de su rostro con un 80% de precisión (mejor que los humanos).
- Los autores fueron amenazados y también demandados por varios grupos de defensa de derechos humanos.

QUÉ PUEDE ESTAR FALLANDO?

FALLO TÉCNICO

1. Datasets sesgados - Los datos no representan por igual a toda la variedad poblacional - minorías perjudicadas. Pocos datos.
2. Baja resolución, iluminación, orientación cuerpo, partes de la cara ocultas, etc. de los sistemas de adquisición de datos.
3. Condiciones laboratorio - mundo real diferentes (no generalización)



FALLO HUMANO

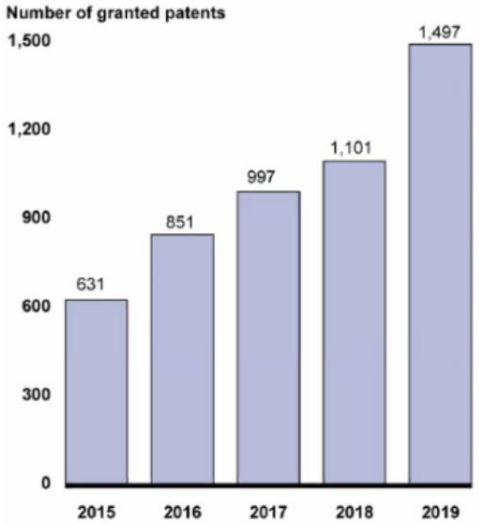
1. Falta de conocimiento de uso de las TRF.
2. Pensar que la máquina sustituye la persona.
3. Malas prácticas/usos de la tecnología.
4. Cuestiones éticas.

CONSECUENCIAS DERIVADAS sobre las TRF (1/2)

RETIRADA DEL MERCADO

Prevención contra posibles malos usos.

- En 2019 Google anunció que no vendería más sistemas de RF hasta no ser regulado.
- En 2020, IBM, Amazon y Microsoft también se sumaron a la iniciativa.
  - IBM retiró su software para RF por parte de la policía.
  - Amazon también hizo lo mismo con su software Rekognition.
  - Microsoft no venderá su sistema a la policía tampoco.
- Estos gestos son simbólicos - hay otras empresas proveedoras
  - Se prevé que el mercado de las TRF crezca casi un 20% hasta 2025.



Número de patentes en sistemas RF ha crecido exponencialmente los últimos años

CONSECUENCIAS DERIVADAS sobre las TRF (2/2)

PERCEPCIÓN DE LA POBLACIÓN

- TFR son racistas
  - Bases de datos retiradas de la comunidad científica
- Efectos psicológicos (ser observado)
- Miedo y criminalización de actos que no lo son (manifestarse).
  - Protestas en Hong Kong
  - Black Lives Matter
- Poder represivo de un gobierno.

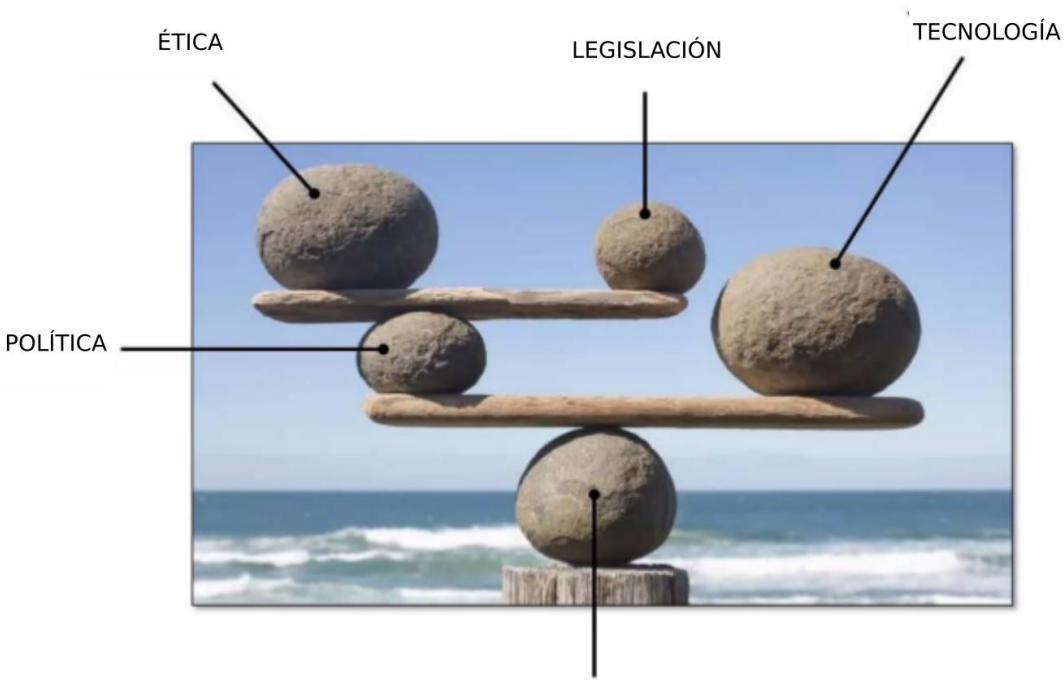
DESINFORMACIÓN

- Los sistemas desplegados son cajas negras para la mayoría de la población.
- Sin transparencia, es lógico sospechar de lo que se desconoce.
- Provoca miedo / repulsión.

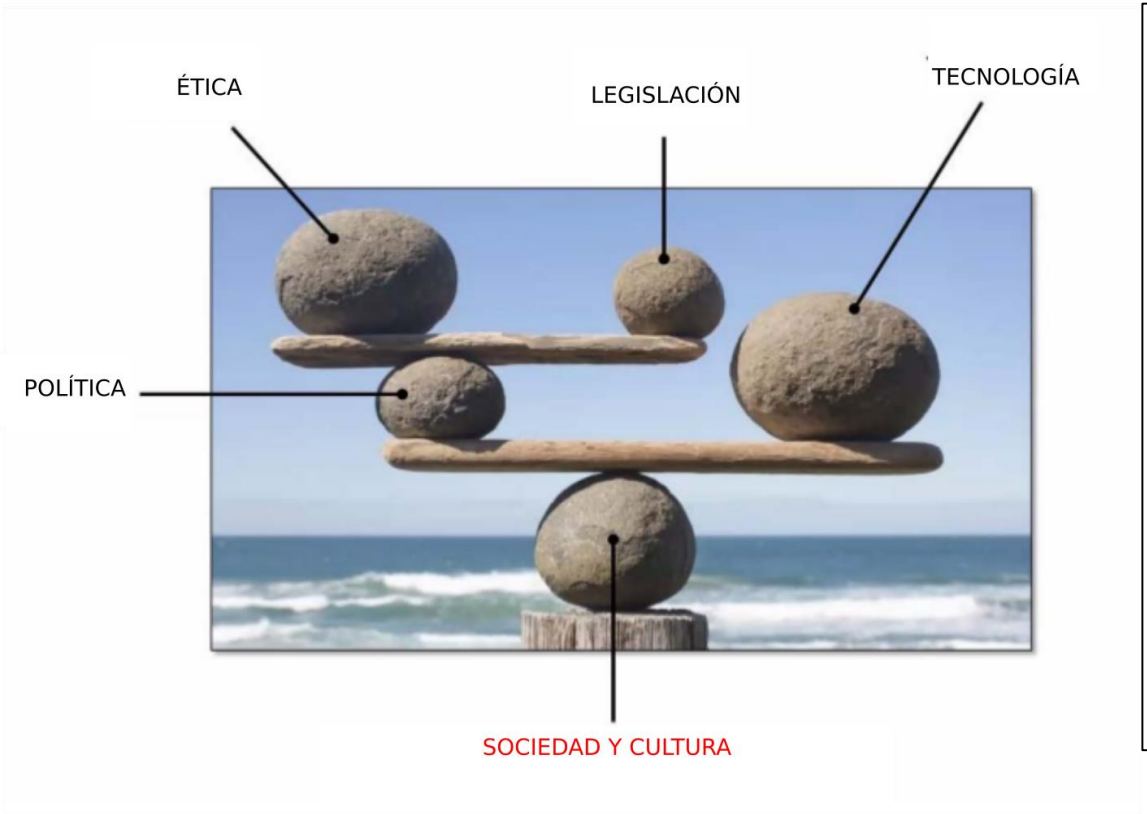
SISTEMAS de VIDEOVIGILANCIA Y SEGURIDAD
- Frequently Asked Questions
FAQs -

¿CÓMO ES EL
FUTURO DE LA TRF?

ES CUESTIÓN DE EQUILIBRIO



ES CUESTIÓN DE EQUILIBRIO - SOCIEDAD

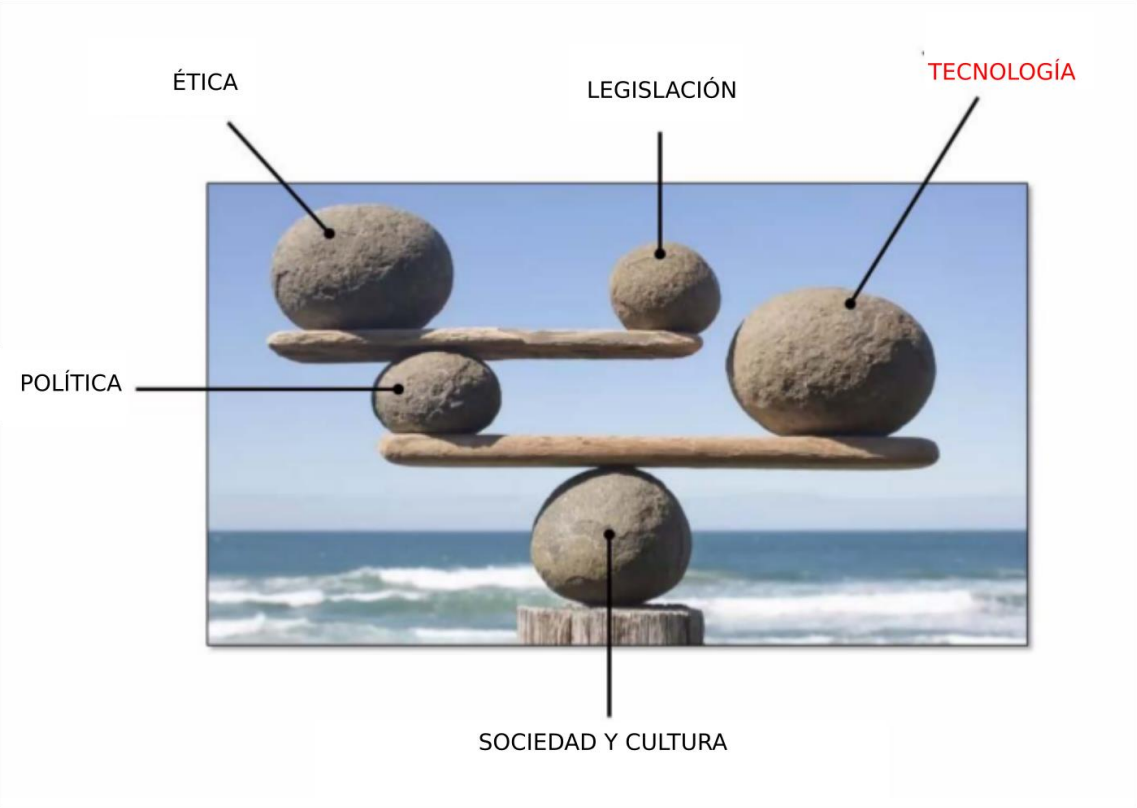


La SOCIEDAD es la base. Necesitamos una sociedad responsable y madura.

- Informar a la población
  - IA
  - Ceder datos personales
- TODOS tenemos responsabilidad
  - Inclusividad
  - Responsabilidad
  - Transparencia
  - Ética

Hay que generar confianza para que la tecnología de RF pueda ser aceptada.

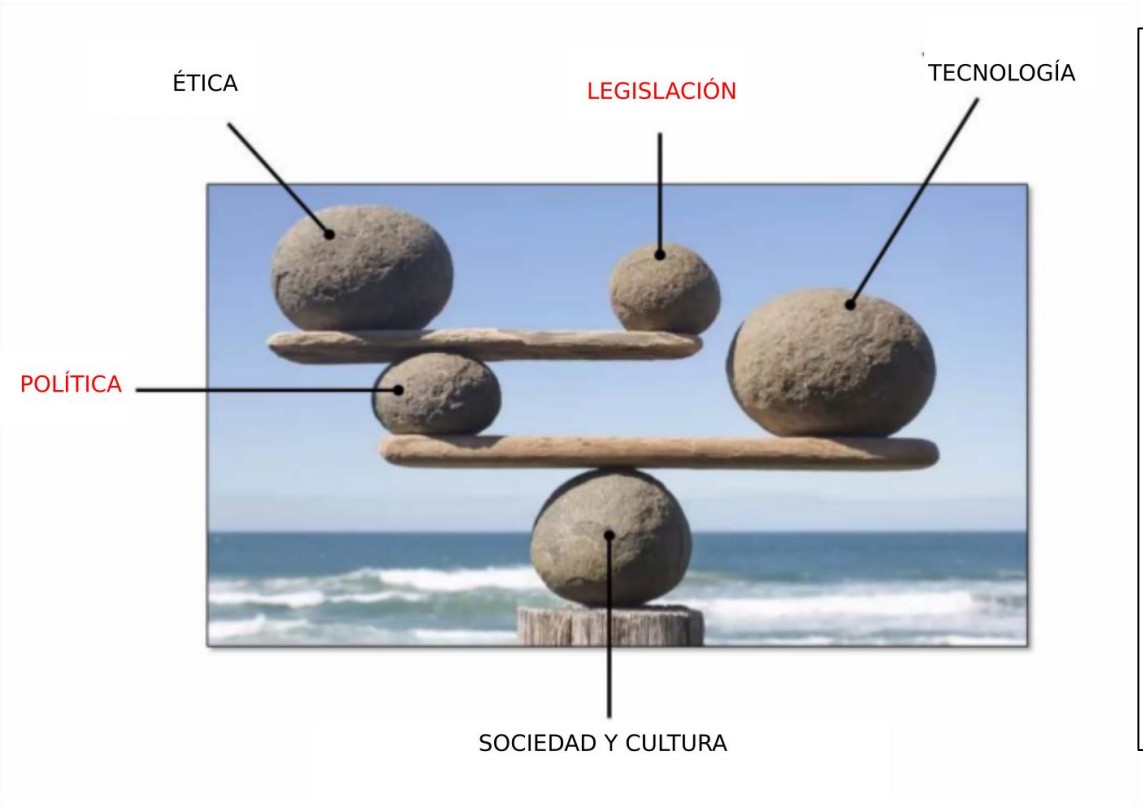
ES CUESTIÓN DE EQUILIBRIO - TECNOLOGÍA



La TECNOLOGÍA puede ser presente pero quizás no madura del todo.

- Utilizar otras técnicas de reconocimiento.
  - Cámaras térmicas, profundidad
  - Sistemas biométricos alternativos / combinados.
- Estrategias de balanceo de datasets y adecuados en entornos reales.
- Sociedad involucrada en el proceso. Formación + supervisión de la tecnología.

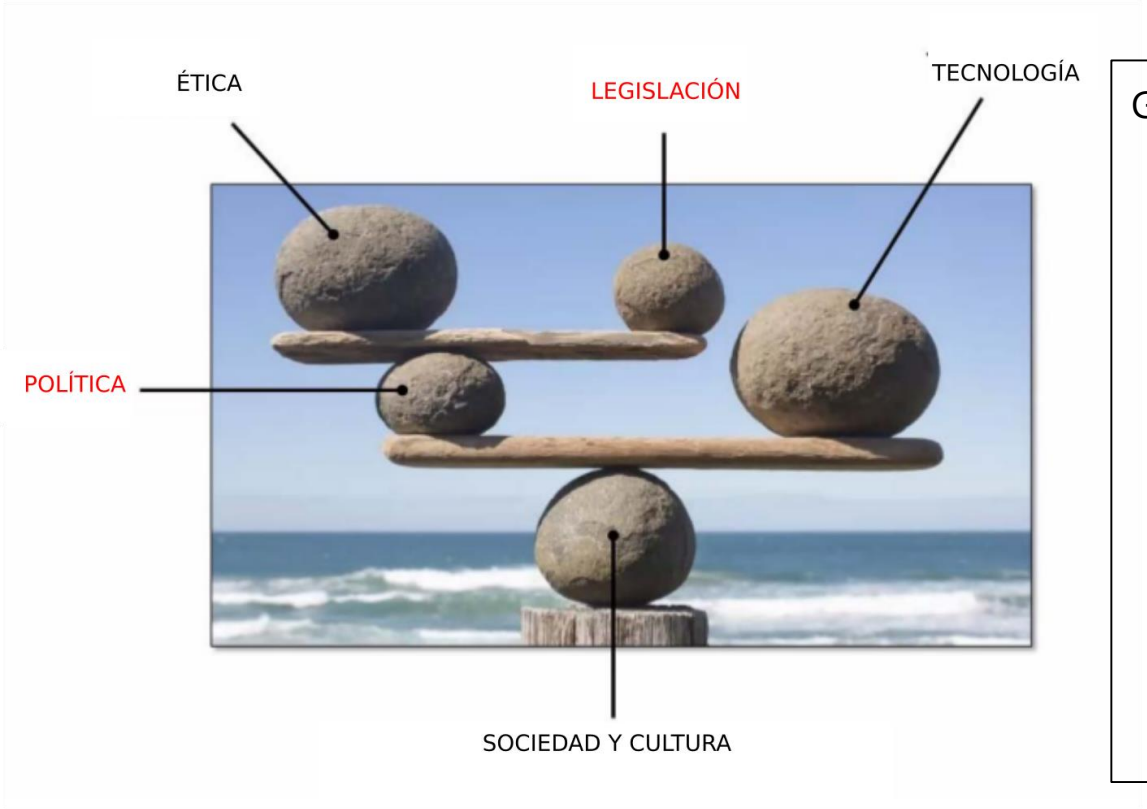
ES CUESTIÓN DE EQUILIBRIO - LEGISLACIÓN



La POLÍTICA tiene un papel fundamental en LEGISLAR el uso adecuado de los sistemas de RF.

- En España estamos amparados por la regulación Europea **GDPR**
  - Privacidad.
  - Protección de datos.
- Necesaria la revisión periódica y auditorías en los países de la Unión.
- Interesante introducir la participación ciudadana.

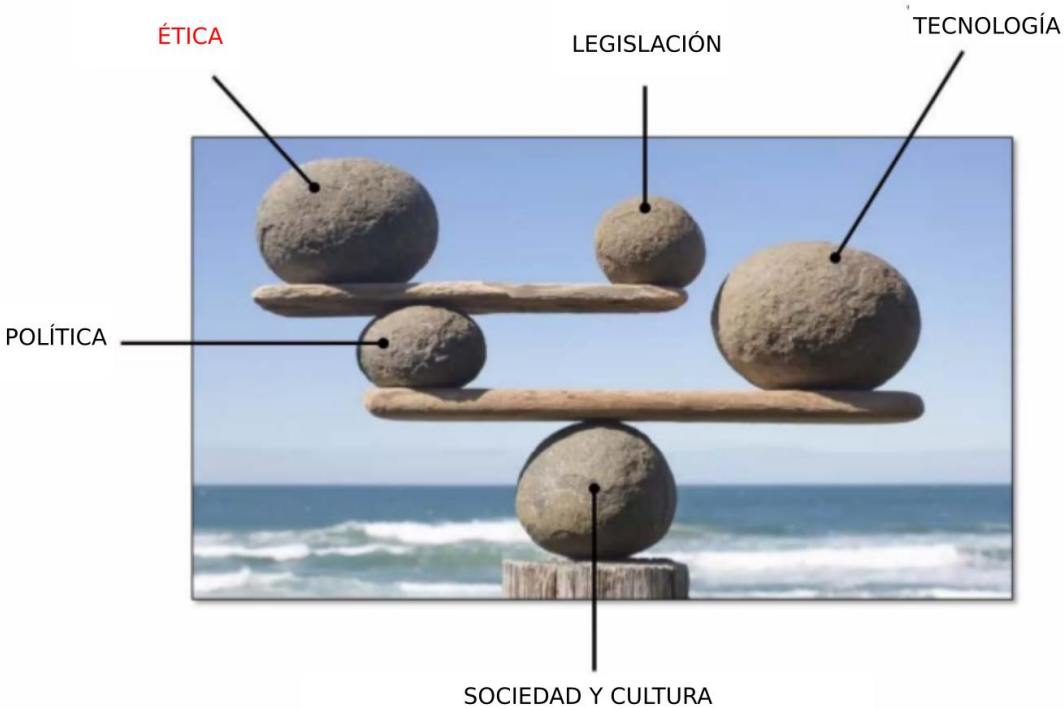
ES CUESTIÓN DE EQUILIBRIO - LEGISLACIÓN



GDPR - Protección de datos.

- Asegurar transparencia e imparcialidad sobre la población.
- Informar y dejar claro el propósito.
- Minimizar los datos recolectados a los necesarios.
- Asegurar datos precisos y actualizados.
- Establecer el tiempo de uso de datos personales al del propósito.
- Asegurar confidencialidad y privacidad de los datos.

ES CUESTIÓN DE EQUILIBRIO - ÉTICA



- Valorar pros vs. contras de utilizar y desarrollar la TRF
  - ¿vale la pena?
  - ¿limitar los usos?
  - ¿impacto deseado?
  - ...

Conclusiones

- La **videovigilancia** analiza vídeos para evitar situaciones de peligro y garantizar **seguridad**.
- La tecnología de **biometría** utilizada es el **reconocimiento facial**, análisis de imágenes. mediante algoritmos de **visión por computador (análisis de datos, IA)** para reconocer las personas que aparecen en una imagen.
- Las técnica de IA recientes más potente que han acelerado el uso del reconocimiento facial a la práctica es la **Red Neuronal Profunda** (Deep Learning).
- La **historia** está llena de ejemplos de **fallos técnicos, fallos humanos, y malos usos** de la tecnología de reconocimiento facial.
- La tecnología de reconocimiento facial no puede funcionar de forma aislada: **el usuario tiene que estar formado y ser partícipe** dentro del ciclo del proceso.
- Las **posibilidades para el bien común** de la tecnología de reconocimiento facial son **innumerables.**
- La **desinformación y la falta de regulación de una tecnología accesible** genera serios problemas en relación a su uso.

Fundació "la Caixa"

PalauMacaya

Computer Vision Center

UNIVERSITAT DE BARCELONA

MUCHAS GRACIAS!

Sergio Escalera, Catedrático, ICREA Academia
Pau Buch-Cardona
HuPBA Human Behavior Analysis Group
www.sergioescalera.com