PROCEDamus

PROCEDIMENTIAMMINISTRATIVIDELLEUNIVERSITA'DEGLISTUDI

progetto di formazione-intervento per le università e gli enti di ricerca

Intelligenza artificiale e diritto: per un'applicazione armoniosa delle tecnologie

Fernanda Faini

Torino, 5 ottobre 2023

Chi sono

- ✓ Docente a contratto di “ICT & Law” – Università Cattolica del Sacro Cuore
- ✓ Docente a contratto di diritto dell’informatica – Università di Pisa
- ✓ Docente a contratto di “Diritto e nuove tecnologie” – Università Telematica Internazionale Uninettuno
- ✓ PhD in diritto e nuove tecnologie – Università di Bologna
- ✓ Funzionario legislativo-legale PA digitale e ICT law – Regione Toscana
- ✓ Membro Task Force Intelligenza Artificiale – AgID
- ✓ Membro gruppo di esperti Blockchain – MISE

DATA SOCIETY

Tecnologia (1)

L'avvento e lo sviluppo incessante delle
tecnologie dell'informazione e della comunicazione (ICT)
hanno mutato profondamente l'esistenza dell'uomo

- da iniziale strumento e ausilio delle attività umane sono arrivate a determinare una **rivoluzione digitale** → mutamenti sociali ed emersione di nuovi interessi ed esigenze inedite

- riguardano la **vita del singolo e delle organizzazioni** → influenzano attività quotidiane, relazioni, progresso, crescita sociale ed economica, lo stesso modo di pensare dell'uomo, sostituiscono prerogative umane

↓

tecnologia protagonista, ma non è "neutrale" →
nella sua valenza strumentale acquisisce il significato che
gli uomini le conferiscono nell'utilizzarla

Tecnologia (2)

Centralità dei dati

- costituiscono l'**"io" digitale**, sono fondamento di ogni **attività umana**, pervadono ogni aspetto dell'**esistenza** → "noi siamo le nostre informazioni"

- **il benessere e lo sviluppo umano** dipendono in modo significativo dai servizi basati sui dati (piattaforme digitali, servizi online)

↓

data society

una "società di dati", che non è soltanto fondata sui dati come nel suo avvento, ma ne è intimamente pervasa finendo per coinvolgere e plasmare l'uomo stesso come un ***data subject***

L'**emergenza sanitaria globale generata dal Covid-19** ha ampliato tali aspetti, spostando il lavoro, le relazioni, persino gli affetti, almeno per alcuni periodi, esclusivamente online → la pandemia incide sui comportamenti e su ogni aspetto di socialità, potenziando la dimensione digitale della vita.

Diritto

Strumento con il quale l'uomo regola la vita

- di conseguenza il diritto è chiamato ad occuparsi della tecnologia, che caratterizza profondamente l'esistenza umana contemporanea

↓

- il diritto è tenuto a individuare regole e principi, disciplinare i comportamenti e le attività, tutelare i diritti, bilanciare interessi diversi e contrapposti, definire responsabilità, prevenire e risolvere i conflitti scaturenti dall'**esistenza digitale** dell'uomo

Ubi societas, ibi ius

Necessità di non rendere tutto ciò che è tecnologicamente possibile,
solo per questo, giuridicamente legittimo

↓

necessario e complesso equilibrio
tra diritto e tecnologia

Società digitale

L’assetto delle società industriali avanzate,
caratterizzato dal ruolo determinante assunto dalle **nuove tecnologie**
e basato sulla **centralità dell’informazione e della conoscenza**
quali **risorse essenziali per lo sviluppo** economico, sociale e culturale

↓

cittadinanza digitale

↓

libertà informatica
diritto all’habeas data
diritti digitali

Caratteristiche (1)

- **informazione** è il principale bene economico, “la materia prima” delle nuove tecnologie (M. Castells)

- **cambia il modo di avere e creare conoscenza** → semplice, economico, veloce → enorme crescita delle informazioni disponibili e strumenti automatici per acquisirle

- **impatto pervasivo** delle tecnologie su ogni aspetto della vita individuale e sociale → settore economico, ambito privato e pubblico (e-government, e-commerce)

Le nuove tecnologie potenziano le capacità umane,
si integrano negli oggetti (Internet of Things),
danno vita a nuovi “soggetti” (intelligenza artificiale e robotica)
↓
crolla il confine tra realtà analogica e digitale
inedita “migrazione di massa” nel mondo digitale

Caratteristiche (2)

- **mutamenti nello "spazio"** → **a-territorialità** → società della rete, globalizzazione: si prescinde dal vincolo territoriale e dalle distanze → interazioni fondate non più su base geografica (comunità territoriali), ma su forme di radicamento basate sugli interessi. Esigenza di omogeneità → risposte giuridiche non possono limitarsi ai confini nazionali (monopolio statale), ma devono assumere veste sovranazionale (diritto europeo e internazionale)

- **mutamenti nel fattore "tempo"** → cambia la percezione del tempo
  - immediatezza → abbattimento delle barriere temporali (le comunicazioni sono sostanzialmente immediate)
  - multitasking → possibile compiere più cose nello stesso momento
  - permanenza delle informazioni → la rete non dimentica
  - ranking → ordine dei risultati delle ricerche non si basa sul tempo → il tempo cede rispetto all'ordine algoritmico della rete
  - velocità e dinamicità della tecnologia, mentre il diritto è strutturalmente "più lento" e tendenzialmente statico (frutto del processo democratico)

Caratteristiche (3)

- **identità digitale dei soggetti** → l'identificazione informatica e la rappresentazione integrale e aggiornata della propria identità
- **intangibilità degli oggetti** → il diritto da sempre è abituato a confrontarsi con la forza delle cose (*res corporales*)
- **realtà digitale e attività giuridiche** → rappresentazioni informatiche che hanno valore giuridico e producono effetti (es. contratti digitali, pagamenti)

- **paradigma dell'accesso** → scalza il concetto di proprietà
  (es. servizi online, car sharing, streaming)

- **ambivalenza fra inclusione ed esclusione** → potenziale aspetto inclusivo, ma nuovi rischi di esclusione (digital divide)

- **sicurezza** dei dati, dei sistemi e delle infrastrutture
- **tutela della persona**, consentendogli il controllo dei propri dati e della propria rappresentazione informatica e la propria libertà

ICT & LAW

Rapporti con altre regole

Nell'era digitale il diritto non è l'unico insieme di regole, ma deve dialogare con altri sistemi di regole, quali:

- **lex informatica o digitalis** →
  le regole informatiche, le "leggi del ciberspazio", le regole tecniche
  Nel caso dell'intelligenza artificiale si parla anche di **lex robotica**

- **le "regole" delle piattaforme digitali e dei colossi tecnologici** →
  Google, Facebook, Amazon, Apple, Microsoft (*big five*)

Lex informatica

Le **regole informatiche condizionano i comportamenti umani**

- abilitano o meno determinate azioni e interazioni
- determinano la facilità nel compimento delle stesse
- collegano o meno effetti
- determinano quali informazioni fornire all'utente

Code is law (L. Lessig) → lex informatica **condiziona ogni altra forma di regolazione**, compresa quella giuridica

↓

ma le regole informatiche sono frutto dell'**uomo**
che **può intervenire** sulle stesse **attraverso il diritto**

↓

Alla tutela giuridica il diritto può affiancare la previsione di **misure tecniche**
capaci di rendere impossibili o disabilitare azioni illecite,
diritto può **incorporare** principi, regole e rimedi nella stessa tecnologia,
può servirsi della tecnologia per garantire il suo rispetto
(es. i principi data protection by design e by default)

Regole delle piattaforme digitali (1)

- **contratto di adesione a una piattaforma digitale con regole unilaterali** → condizioni d'uso, termini di servizio e policy

  ↓

  Le piattaforme si riservano di sospendere o interrompere la fornitura dei servizi in caso di presunte illiceità o mancato rispetto di termini e condizioni

  Esempio: https://policies.google.com/terms

  Caso account social di Donald Trump

- **regole applicate dal "codice"** (non quello giuridico) → gli algoritmi traducono la regola in azione → es. rimozione di un contenuto non gradito

  ↓

  L'algoritmo agisce come tale → es. i casi relativi ad opere d'arte

Regole delle piattaforme digitali (2)

- **autorità di fatto** → individui pronti a cedere dati in cambio della possibilità di avere accesso ai servizi offerti

- **asimmetria di potere** → libertà apparente, profilazioni, polarizzazioni, *filter bubble*, possibili discriminazioni

- **dittatura degli algoritmi** → occorrono azioni difensive "supplementari" del singolo per potersi tutelare. La persona si sgretola in frammenti di dati, lascia tracce di sé, i diversi profili sono capaci di sopravvivere all'individuo (eredità digitale)

Nuove geometrie di potere

- **Stati** → assenza di confini; dimensioni globali dell'oggetto di regolazione; indebolimento della sovranità e pretesa di potere; erosione monopolio
- **colossi tecnologici** → favoriti da capacità di utilizzo delle tecnologie, dimensione sovranazionale, libertà di impresa, regole inadeguate → si presentano come spazi di libertà, ma assumono forme panottiche ed esercitano ruolo concreto nella "regolazione" seppur privi di legittimazione democratica e guidati non dall'interesse pubblico, ma dal profitto economico → **controllori del pedaggio di accesso alla vita digitale**

↓

rischio Big Brother (Big Government + Big Business) (Lessig)
Big Other e **capitalismo della sorveglianza** (Zuboff)
indiscriminata, continua, diffusa, "liquida" con modalità flessibili, seducenti e divertenti, tipiche del consumismo, distanti da connotazioni carcerarie

- **individui** → deboli nei confronti degli uni e degli altri; apparente libertà; rischio di mercificazione dei dati, accesso mediato da forme di pagamento inedite (i propri dati, i propri interessi, i propri comportamenti)

Evoluzione della società digitale

Avvento di tecnologie informatiche e di Internet

- idea utopica dell'agorà digitale, ampia e inedita libertà
- ruolo centrale dell'informazione e della conoscenza
- nuova democrazia "dal basso", diffusione del potere e del controllo

↓

Evoluzione delle tecnologie → rischio di **società del controllo** → **superpanopticon o post-panopticon o capitalismo della sorveglianza** indiscriminata, continua, diffusa, "liquida" con modalità flessibili, seducenti e divertenti, tipiche del consumismo, distanti da connotazioni carcerarie → **volto oscuro della rete**

- potere nelle mani di pochi soggetti
- automazioni e "dittature dell'algoritmo"
- contrattazioni inique, discriminazioni, disparità e disuguaglianze
- filter bubble, echo chambers, polarizzazioni e balcanizzazioni delle opinioni → apparente libertà, ma vediamo chi ci somiglia grazie agli algoritmi
- bufale e fake news → difficoltà a distinguere cosa è vero

BIG DATA E INTELLIGENZA ARTIFICIALE

Big data: cosa sono? (1)

Molteplici definizioni

Enormi volumi di dati detenuti da grandi organizzazioni (governi, colossi tecnologici) provenienti da diverse fonti e analizzati per mezzo di algoritmi

- tecniche di data mining (estrazione di conoscenza)
- big data analytics
- machine learning (apprendimento automatico)
- deep learning (reti neurali artificiali)
- tecnologie specifiche

Eterogenee **tracce digitali** derivanti da interazioni in rete

- dati strutturati e non strutturati
- dati generati dagli utenti
- dati personali

Big data: cosa sono? (2)

- dati raccolti su base volontaria nelle piattaforme online (Facebook, Instagram, Amazon, Linkedin…)
- dati “scambiati” a fronte di utilità conseguibili (raccolte punti, tessere fedeltà, app che consentono sconti)
- dati forniti in modo più o meno consapevole (GPS del telefono, sensori)
- dati “automatici” come i cookies
- dati residui o inferiti → sottoprodotto delle azioni (es. errori di digitazione)
- dati raccolti dai soggetti pubblici
- dati su cui si basa **intelligenza artificiale**
- dati prodotti dagli oggetti → **Internet of Things**

Caratteristiche dei big data

Paradigma delle 3, 4 o 5 V

- **volume** → capacità di acquisire, memorizzare e accedere a enormi quantità di dati.

- **velocità** → capacità di effettuare analisi in tempo reale o ad “alta velocità” Sottende **dinamicità** e **tempo** → in tempi brevi il dato diventa obsoleto.

- **varietà** → eterogenea tipologia di dati e formati, provenienti da fonti diverse (strutturate e non)

Secondo parte di dottrina anche

- **valore** → quanto i big data valgono come insieme
- **veracità** → veridicità, ossia qualità e accuratezza dell’analisi

↓

protagonisti gli algoritmi

big data diventano dinamica materia prima capace di generare valore

Intelligenza artificiale

Sistemi che mostrano un **comportamento intelligente** analizzando il proprio ambiente e compiendo azioni, con un certo grado di autonomia [in ciò sta la natura "intelligente"], per raggiungere specifici obiettivi (Comunicazione della Commissione europea «L'intelligenza artificiale per l'Europa» COM(2018) 238 final del 25 aprile 2018)

- software agiscono nel **mondo virtuale**
  (es. assistenti vocali, software per analisi delle immagini, motori di ricerca, sistemi di riconoscimento vocale e facciale)

- software incorporano l'IA in **dispositivi hardware**
  (es. robot avanzati, auto a guida autonoma, droni o applicazioni dell'IoT)

↓

capacità di riprodurre o attuare operazioni tipiche delle funzioni cognitive umane (apprendimento, problem solving, riconoscimento di volti, traduzione…)

↓

- enormi quantità di **dati** (big data) → anima di IA
- **algoritmi** → motore capace di "animare" i dati e di estrarne il valore

Intelligenza artificiale debole e forte

Intelligenza artificiale
capacità della macchina di riprodurre o attuare operazioni tipiche delle funzioni cognitive umane, quali apprendimento, problem solving, riconoscimento di volti, traduzione, etc. (Simoncini – Suweis)

↓

Alcuni distinguono:

- **intelligenza artificiale debole** → risolve problemi, ma non arriva alla comprensione tipica dell'intelligenza umana

- **intelligenza artificiale forte** → l'intelligenza artificiale mostra capacità cognitive non distinguibili da quelle dell'intelligenza umana

Un recente approccio è relativo all'**augmented intelligence**, orientata a potenziare e aumentare le capacità dell'uomo al fine di supportarlo nel processo decisionale e nell'acquisizione di conoscenza, senza essere sostituito da un sistema artificiale.

Internet of Things (IoT)

Oggetti dotati di sensori per ottenere informazioni, interagire tra loro e in rete

Ampiezza degli oggetti interessati:

- dispositivi indossabili
- domotica → automazione domestica
- robotica
- industria automobilistica
- ambito biomedicale
- monitoraggio in ambito industriale
- rilevazione di eventi avversi

  etc.

I dati prodotti da Internet of Things

sono big data

Finalità e utilizzi (1)

Premessa → i dati sono raccolti e analizzati senza che siano sempre chiari ex ante utilizzi e finalità → risultati imprevisti frutto di correlazioni

- **conoscenza sul presente e sul futuro** → interpretazione di esigenze, profilazione, ottimizzazione della produzione, monitoraggio e supporto alle decisioni, supporto a campagne giornalistiche

  Capacità di predizione → elevate correlazioni indicano alte probabilità → predizioni sugli andamenti di mercato, miglioramento di diagnosi e cure, prevenzione di disastri, previsioni politiche → oracoli digitali

- **servizi e miglioramento qualità della vita** → impiego nell'erogazione di servizi e nello svolgimento di funzioni (controllo etc.), maggior efficacia ed efficienza, tempestività, risparmio

Finalità e utilizzi (2)

- **servizi e miglioramento qualità della vita** → impiego nell'erogazione di servizi e nello svolgimento di funzioni, maggior efficacia ed efficienza, tempestività, risparmio

- lavoro (supportando e sostituendo uomo in una serie di operazioni)
- medicina (diagnosi e cura)
- trasporti (veicoli autonomi)
- assistenza sociale (robot che assistono anziani e disabili)
- sicurezza (riconoscimento facciale)
- finanza (andamento del mercato)
- giustizia (istruttorie e decisioni)

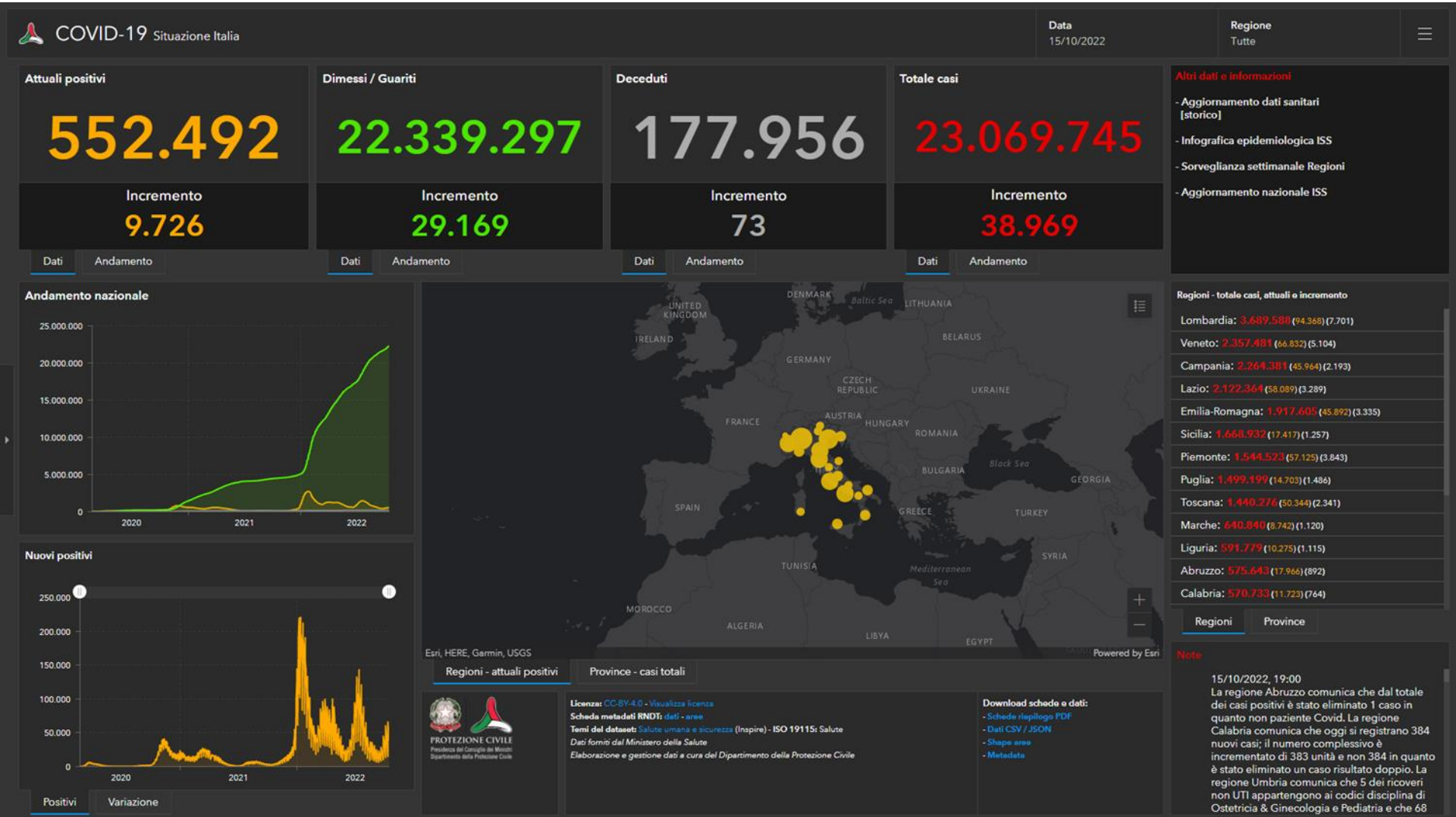
etc.

↓

Big data e IA possono rispondere alla **tutela di interessi generali**, ma anche alla realizzazione di **vantaggi economici**, obiettivi privati

Monitoraggio Covid -19

https://dati-covid.italia.it



ETICA E DIRITTO

Algoritmi e diritto

Muta il modo di conoscere e "misurare" fatti e persone

- si possono **analizzare tendenzialmente tutti i dati** disponibili (non solo campioni)
- **inferenze e correlazioni, logica deterministica, probabilità e non causalità** → si accerta "il cosa", senza domandarsi *ex ante* "il perché" dei fenomeni, si prende atto delle correlazioni che emergono
- **più confusione e meno esattezza** a fronte della conoscenza e comprensione garantita da tali strumenti

↓

Negli algoritmi criticità ontologiche per il diritto

- orientato ai valori (non ai numeri)
- prescrittivo (non descrittivo e predittivo)
- formale e "lento" (non così dinamico)
- poggia sulla scelta individuale e sulla libera volontà (non deterministico)

Dati e conoscenza, analisi e interpretazione

- necessità di **dati di qualità** → le **basi di dati** devono essere **costituite e annotate correttamente**, garantendo qualità, neutralità e intelligibilità, assicurando un elevato grado di sicurezza e riuscendo a prevenire i rischi

- **natura inferenziale e probabilistica delle elaborazioni** → analisi tecnica è un processo di approssimazione con il rischio di trarre conclusioni imprecise senza tradursi in conoscenza → **rischio di bias**, **errori tecnici e manipolazioni umane**, **discriminazioni**, disparità di trattamento, opacità per confusione

↓

adeguata **contestualizzazione, analisi e interpretazione** →

saper fare le domande giuste ai dati e saper comprendere le risposte

Informazione e conoscenza

- **informazione** → dati + significato

è diversa da

- **conoscenza** → si basa su informazioni, ma necessita di ulteriori fattori, quali il processo cognitivo e l'elaborazione "intelligente", la comprensione e l'applicazione all'esperienza: si colloca a un livello gerarchico superiore e possiede maggiore valore → il solo insieme di informazioni non è necessariamente sinonimo di conoscenza

↓

necessario conoscere per vivere il proprio spazio e per esercitare consapevolmente i propri diritti e libertà

↓

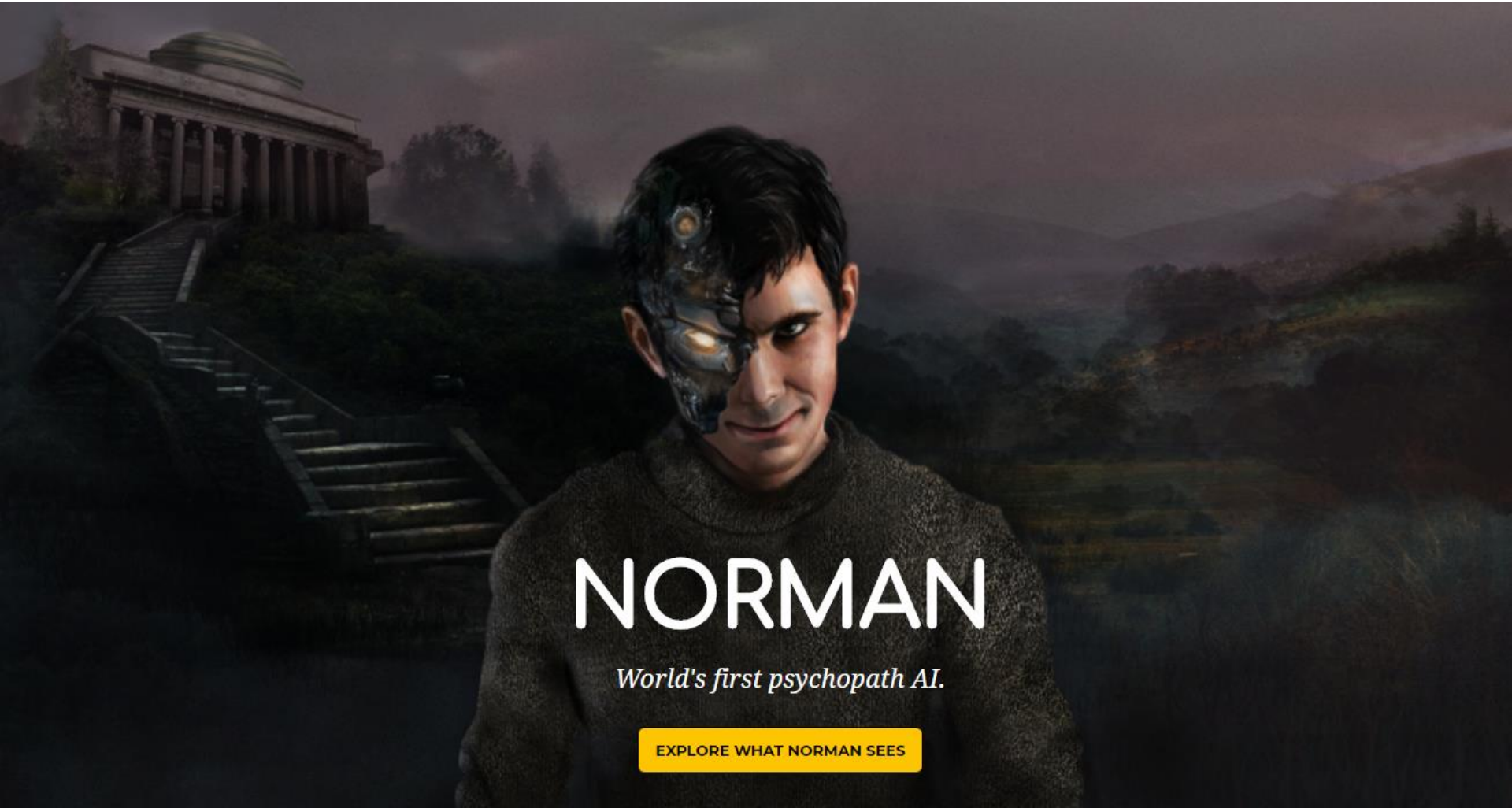
accesso alla conoscenza ha un legame saldo con la persona e i suoi diritti

↓

la mancata conoscenza può arrivare a minare le fondamenta del modello democratico

Importanza dei dati

http://norman-ai.mit.edu



Bias e dintorni (1)

Il caso di **Eric Loomis**
sentenza State of Wisconsin v. Eric Loomis, 881 N.W.2d 749 (2016)

Software di algoritmi predittivi **Compas**, utilizzato per valutare il rischio di recidiva e pericolosità sociale → la sentenza ha legittimato l'uso del software ritenendo che rispettasse il principio del giusto processo, dal momento che costituiva solo un ausilio a disposizione del giudice per supportare la sua valutazione e non il motivo esclusivo della decisione.

↓

sulla base della natura proprietaria del software, a Loomis non è stato concesso l'accesso al codice sorgente, utile per comprendere e contestare le decisioni.

↓

Gli studi sul software Compas hanno mostrato **margine di errore e "imparità"** nella predizione a seconda del gruppo etnico di riferimento → Compas sovrastimava alcuni fattori quali l'appartenenza ad un certo gruppo etnico.

Bias e dintorni (2)

Progetto sperimentale di Amazon impiegava IA per fornire punteggi ai candidati. Nel 2015 emerge che il sistema non selezionava candidature per ruoli di sviluppatori di software e posti ad alto contenuto tecnologico in modo neutrale rispetto al genere: escludeva i cv delle donne

↓

Il software aveva “imparato” in modo automatico che i candidati uomini (numericamente maggiori) erano preferibili

e ha **penalizzato i cv con la parola donna**

↓

Amazon è stata costretta a sciogliere il team del progetto

Profili etici

- **individuazione e la scelta dei valori etici e delle norme giuridiche** con cui educare gli algoritmi e istruire le macchine

- **individuazione di principi comuni tra ordinamenti diversi** nel pluralismo etico che caratterizza la società contemporanea

- complessa valutazione relativa all'introduzione o all'adattamento di **categorie giuridiche e norme**

↓

rispetto dei valori etici della società e dei correlati principi di diritto
si traduce nella necessaria **tutela da offrire ai diversi diritti in gioco**,
che esige il rispetto delle norme di riferimento

Dilemmi etici

Macchine autonome, armi e veicoli a guida autonoma possono incidere su **posizioni individuali di particolare rilievo etico-giuridico**, come il diritto alla vita e all'integrità fisica

↓

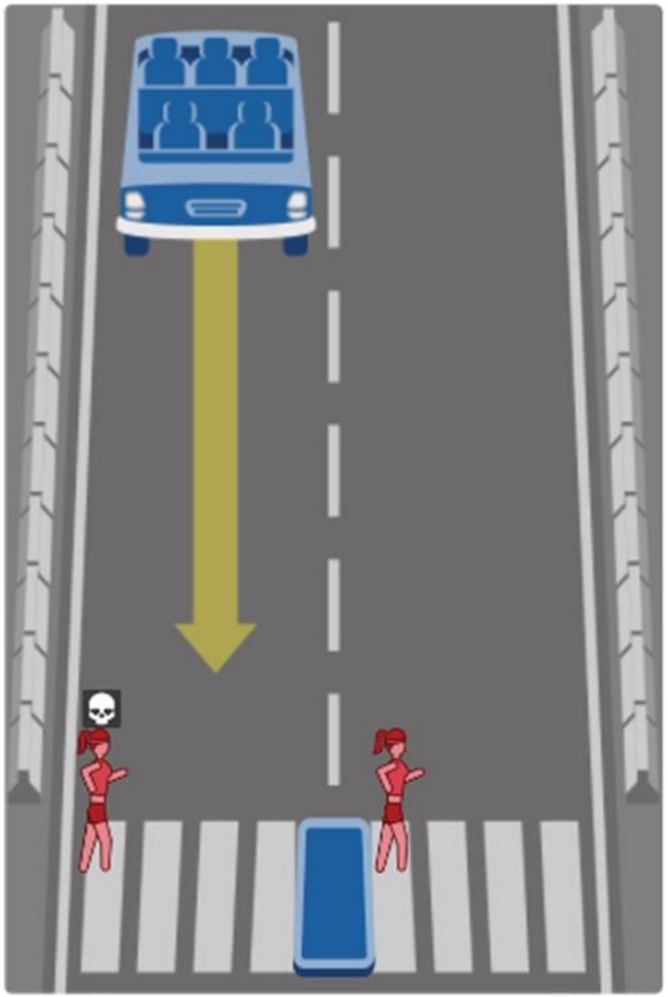
accettabile in tali casi la sostituzione della macchina all'uomo, rischiando di aprire vuoti di responsabilità in caso di danni?

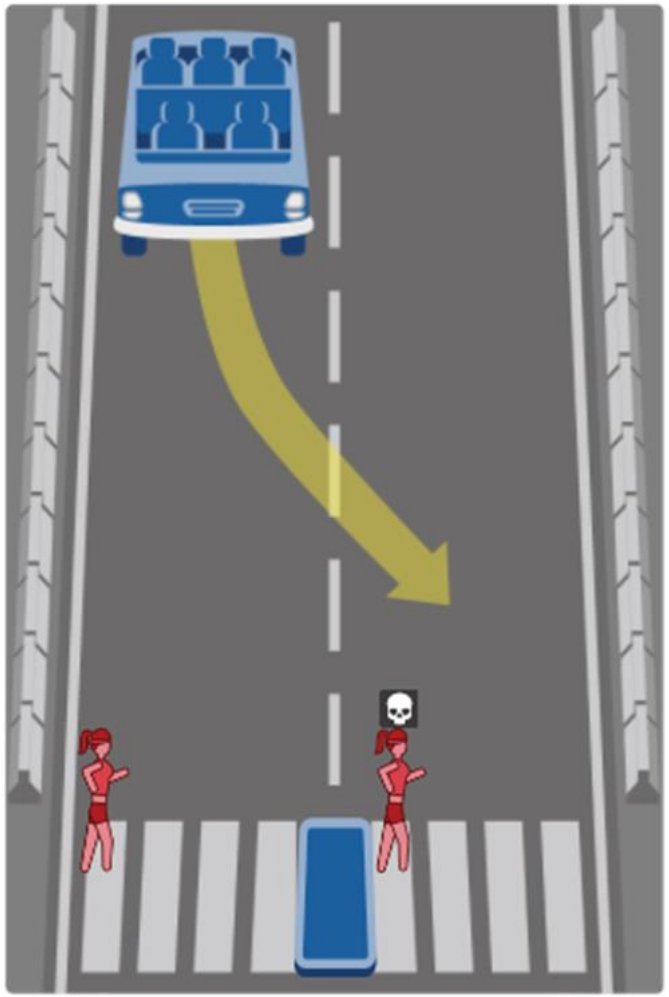
In caso affermativo, difficile regolamentare il comportamento della macchina e la responsabilità di fronte a **tensioni etiche e problematiche complesse** soprattutto laddove siano in gioco interessi dello stesso peso assiologico:

- in caso di **collisione inevitabile** quale scelta dovrà compiere il veicolo a guida autonoma, laddove si tratti di recare danno a diversi potenziali soggetti o persino di sacrificare una vita piuttosto che un'altra?
- su **quali criteri etici** dovranno basarsi tali scelte e **quali istruzioni** dovrà ricevere la macchina per operare le scelte?

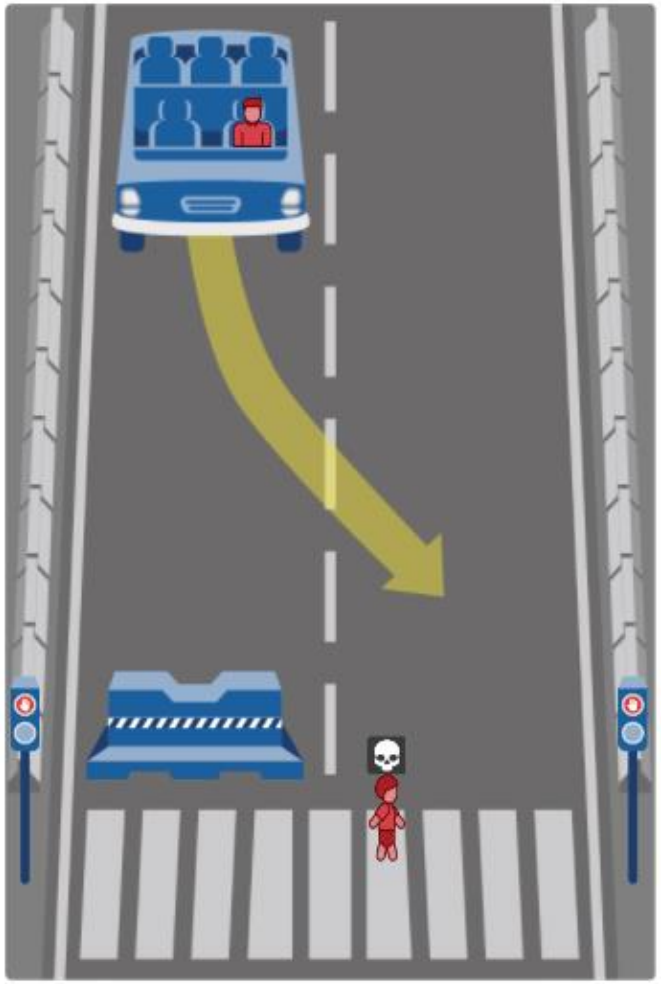
https://www.moralmachine.net

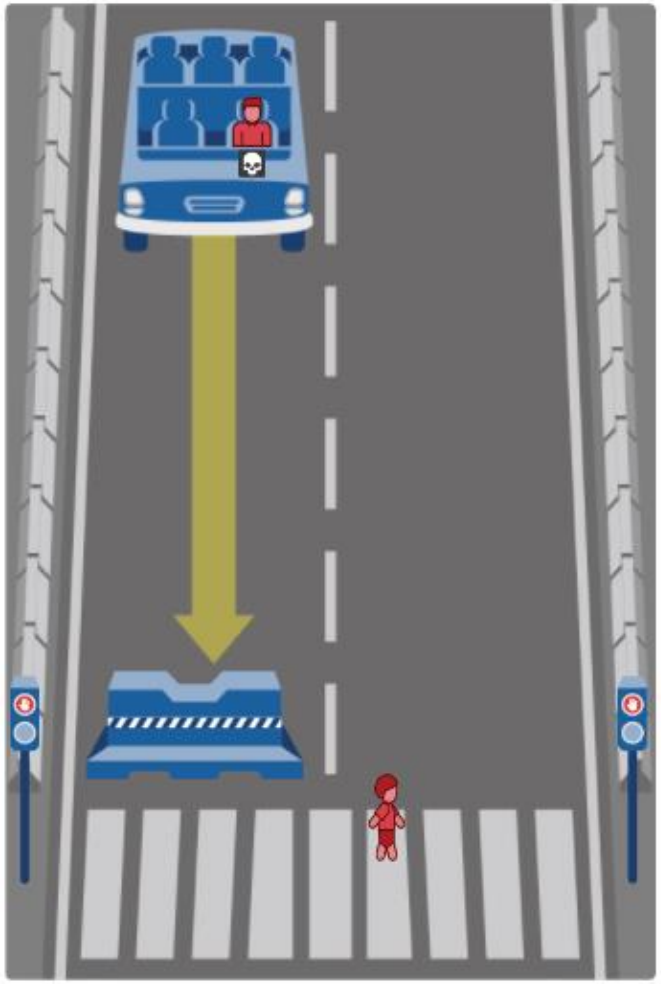
Cosa dovrebbe fare l'auto a guida autonoma? (1)



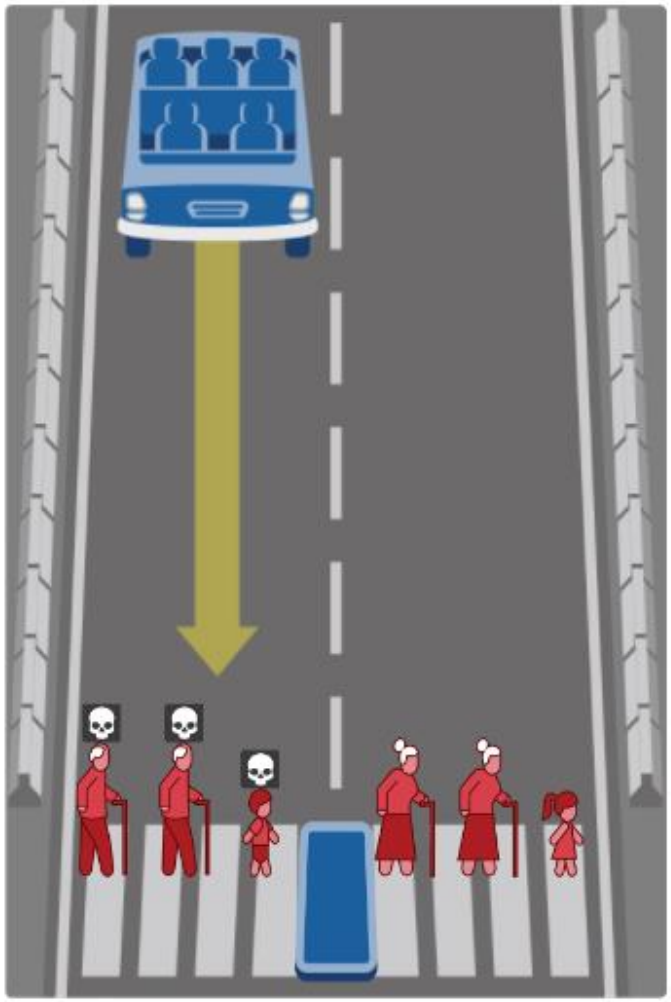


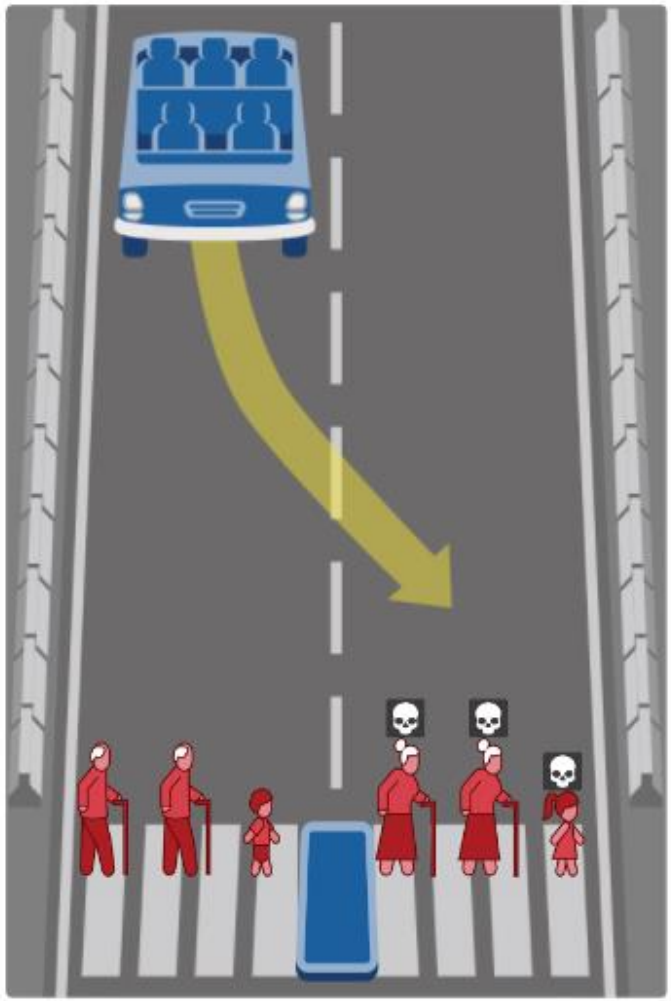
Cosa dovrebbe fare l'auto a guida autonoma? (2)





Cosa dovrebbe fare l'auto a guida autonoma? (3)





Big data divide

- **big data divide** → asimmetria, pochi “signori” dei dati (colossi digitali e poteri pubblici) raccolgono ed elaborano big data

- **pericolo di usare le previsioni in contesti diversi** da quelli di origine con le relative discriminazioni (es. lavoro, assicurazioni, prevenzione del crimine) → dati utilizzati per finalità ulteriori rispetto ai servizi per cui sono impiegati, soprattutto laddove ciò avvenga in modo poco trasparente

- **controllo sociale, sorveglianza e monitoraggio indiretto** grazie a dati pubblici e privati → rischio di scivolare dalla società della conoscenza verso un superpanopticon o post-panopticon

↓

algoritmi guidano i comportamenti individuali (es. social) → **apparente libertà** del singolo/utente guidato dall’automazione

Datagate

Nel 2013 Edward Joseph **Snowden** ha rivelato le attività di **sorveglianza di massa** dei servizi di intelligence statunitensi connesse in particolare al programma governativo segreto, denominato **PRISM**.

Sorveglianza condotta da cinque occhi (USA, Canada, Gran Bretagna, Australia, Nuova Zelanda)

Accesso e raccolta ad opera delle agenzie governative da aziende come **Google, Microsoft, Facebook, Apple, Skype e Yahoo** di dati quali:

- email
- profili
- chat e conversazioni
- video
- foto

Facebook – Cambridge Analytica

Nel 2018 Christopher **Wylie**, che è stato dipendente della società di consulenza Cambridge Analytica, ha fatto emergere lo spregiudicato utilizzo dei dati personali forniti dagli utenti durante l'utilizzo dell'app "This is your digital life" da parte di Cambridge Analytica (specializzata nella profilazione e micro-targeting comportamentale), per mezzo di accordi con il titolare dell'app, che trattava i dati a fini di ricerca

↓

utilizzo dei dati per campagne di comunicazione capaci di influenzare, condizionare e manipolare gli individui in occasioni quali il referendum sulla Brexit

↓

manipolazione delle scelte individuali

(in tal caso opinioni politiche,

che hanno tutela più incisiva)

FRAMEWORK GIURIDICO EUROPEO

Quadro europeo sulla dimensione digitale

Framework giuridico europeo, diretto a disciplinare la dimensione digitale della vita umana, formato inizialmente prevalentemente da **atti di soft law** e, più di recente, da un **insieme di regolamenti** quali:

- **Digital Services Act** (regolamento UE 2022/2065)
- **Digital Markets Act** (regolamento UE 2022/1925)
- **Data Governance Act** (regolamento UE 2022/868)
- **Data Act**, proposto il 23 febbraio 2022
- **Artificial Intelligence Act**, proposto il 21 aprile 2021

↓

Necessario un complesso articolato di regole diverse, atte a costruire una **disciplina complessivamente sostenibile** e, a tal fine, tese a garantire:

- **prevedibilità e certezza del diritto** → da parte di UE muta approccio formale con la tendenza a "inasprire" la forza degli atti normativi (da soft law ad hard law) per garantirne effettività (si sceglie il regolamento) e muta approccio sostanziale (si sceglie di regolare e di incidere sui poteri privati)
- **flessibilità e adattabilità** all'evoluzione e ai cambiamenti della tecnologia → soft law, meccanismi di revisione, aggiornamento, flessibilità negli atti

Atti e documenti sui dati

- **guidelines on the Protection of Individuals with Regard to the Processing of Personal Data in a World of Big Data** – 23/01/2017, Comitato Convenzione 108

- **comunicazioni della Commissione europea**
  - ✓ «Verso una florida economia basata sui dati» – 02/07/2014
  - ✓ «Costruire un'economia dei dati europea» – 10/01/2017
  - ✓ «Verso uno spazio comune europeo dei dati» – 25/04/2018
  - ✓ «Strategia europea dei dati» – 19/02/2020

- proposta di regolamento **Data Governance Act** – 25/11/2020

- **documenti dell'European Data Protection Supervisor (EDPS)**
  Opinion 7/2015 «Meeting the challenges of big data»; Opinion 8/2016 «on coherent enforcement of fundamental rights in the age of big data»; Opinion 3/2018 «on online manipulation and personal data»

- **Pubblicazioni Organisation for Economic Co-operation and Development (OECD)** come «Data-Driven Innovation: Big Data for Growth and Well-Being», 2015

Data Governance Act

proposta di regolamento UE del 25 novembre 2020

Atto volto a promuovere la **disponibilità dei dati utilizzabili** rafforzando la fiducia negli intermediari di dati e potenziando i meccanismi di condivisione dei dati in tutta l'UE, che integra la direttiva (UE) 2019/1024, dal momento che riguarda i dati oggetto di diritti di terzi detenuti da enti pubblici.

Propone:

- ✓ messa a disposizione dei dati del settore pubblico per il riutilizzo qualora tali dati siano oggetto di diritti di terzi
- ✓ condivisione dei dati tra le imprese, dietro compenso in qualsiasi forma
- ✓ consenso all'utilizzo di dati personali con l'aiuto di un "intermediario per la condivisione dei dati personali", il cui compito consiste nell'aiutare i singoli individui a esercitare i propri diritti a norma del regolamento generale sulla protezione dei dati
- ✓ consenso all'utilizzo dei dati per scopi altruistici

Quadro sovranazionale su IA (1)

Ruolo guida dell'Unione europea nel realizzare un **approccio comune** degli Stati membri in relazione all'intelligenza artificiale:

- Risoluzione recante «raccomandazioni alla Commissione concernenti **norme di diritto civile sulla robotica**» del Parlamento europeo, 16/02/2017 → responsabilità e personalità dei robot

- Comunicazione «**L'intelligenza artificiale per l'Europa**» Commissione europea, COM(2018) 237 final, 25/04/2018 → IA made in Europe e antropocentrica; approccio basato su valori e diritti fondamentali, in modo da essere sostenibile e apportare benefici all'intera comunità

- Comunicazione «**Piano coordinato sull'intelligenza artificiale**» della Commissione europea, COM(2018) 795 final, 07/12/2018 → Stati membri incoraggiati a sviluppare strategie nazionali, basandosi sul lavoro europeo

- Risoluzione recante «raccomandazioni alla Commissione su un **regime di responsabilità civile per l'intelligenza artificiale»** del Parlamento europeo, 20/10/2020 → responsabilità basata sul rischio

Quadro sovranazionale su IA (2)

- «**Orientamenti etici per un'IA affidabile**» dell'High-Level Expert Group on AI, 08/04/2019 → intelligenza artificiale meritevole di fiducia o affidabile: 3 componenti (legalità, eticità, robustezza) e 4 principi etici (rispetto autonomia umana, prevenzione dei danni, equità, esplicabilità)

↓

- Comunicazione «**Creare fiducia nell'intelligenza artificiale antropocentrica**» della Commissione europea, COM(2019) 168 final, 08/04/2019

- **«Libro Bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia »** della Commissione europea, COM(2020) 65 final, 19/02/2020 → ecosistema di eccellenza e di fiducia. Sono individuati gli elementi essenziali delle prescrizioni giuridiche per il futuro quadro normativo per l'IA

- **Proposta di regolamento «Artificial Intelligence Act»** della Commissione europea, COM(2021) 206 final, 21/04/2021

«Orientamenti etici per un'IA affidabile» High-Level Expert Group on AI (1)

8 aprile 2019, elaborati da un gruppo di esperti ad alto livello sull'intelligenza artificiale indipendente istituito dalla Commissione europea nel giugno 2018

Intelligenza artificiale meritevole di fiducia o affidabile

↓

3 componenti (ognuna necessaria, ma non sufficiente da sola) durante l'intero ciclo di vita del sistema:

- **legalità** → IA deve ottemperare a tutte le leggi e ai regolamenti applicabili
- **eticità** → IA deve assicurare l'adesione a principi e valori etici → diritto non è sempre al passo con gli sviluppi tecnologici, a volte nemmeno con le norme etiche o non è adatto ad affrontare determinate questioni
- **robustezza** → dal punto di vista tecnico e sociale poiché, anche con le migliori intenzioni, i sistemi di IA possono causare danni non intenzionali

↓

principi etici e indicazioni

su come possano essere resi operativi in sistemi socio-tecnici

«Orientamenti etici per un'IA affidabile» High-Level Expert Group on AI (2)

Basi di un'"IA affidabile"
IA deve rispondere, essere realizzata e valutata sulla base di:

4 principi etici

- **rispetto dell'autonomia umana** → piena ed effettiva autodeterminazione: sistemi di IA non devono subordinare, costringere, ingannare, manipolare, condizionare o aggregare in modo ingiustificato gli esseri umani
- **prevenzione dei danni**
- **equità** → dimensione sostanziale e procedurale (capacità di impugnare le decisioni e presentare ricorso)
- **esplicabilità** → trasparenza e spiegabilità per creare e mantenere fiducia

↓

tra i principi possono insorgere **tensioni** e
non esiste alcuna soluzione prestabilita per risolverle

Quadro di riferimento per un'IA affidabile

PROCEDamus
PROCEDIMENTI AMMINISTRATIVI DELLE UNIVERSITÀ DEGLI STUDI
Progetto di formazione-intervento per le università e gli enti di ricerca

INTRODUZIONE

IA affidabile

- **Legalità dell'IA**
- **Eticità dell'IA**
- **Robustezza dell'IA**

(non trattata nel presente documento)

CAPITOLO I

Basi di un'IA affidabile

Garantire l'aderenza ai principi etici basati sui diritti fondamentali

→ **4 Principi etici**

Riconoscere e risolvere le potenziali tensioni tra di essi

- Rispetto dell'autonomia umana
- Prevenzione dei danni
- Equità
- Esplicabilità

CAPITOLO II

Realizzazione di un'IA affidabile

Garantire l'attuazione dei requisiti fondamentali

→ **7 Requisiti fondamentali**

Da valutare e considerare costantemente durante l'intero ciclo di vita del sistema di IA mediante

- **Metodi tecnici**
- **Metodi non tecnici**

- Intervento e sorveglianza umani
- Robustezza tecnica e sicurezza
- Riservatezza e governance dei dati
- Trasparenza
- Diversità, non discriminazione ed equità
- Benessere sociale e ambientale
- Accountability

CAPITOLO III

Valutazione dell'IA affidabile

Garantire l'operatività dei requisiti fondamentali

→ **Valutazione dell'IA affidabile**

Adattare all'applicazione specifica dell'IA

Proposta di regolamento «Artificial Intelligence Act» (1)

COM(2021) 206 final del 21 aprile 2021

Approccio basato sul rischio → 4 categorie: inaccettabile, alto, basso, minimo.

- **sistemi a rischio inaccettabile** → IA è considerata una minaccia alla sicurezza e ai diritti dell'uomo, che di conseguenza sono vietati. Vi rientrano:

✓ sistemi che utilizzano **tecniche subliminali**, che agiscono senza che una persona ne sia consapevole, al fine di distorcerne materialmente il comportamento, in un modo che provochi o possa provocare un danno;

✓ **sistemi atti a sfruttare le vulnerabilità di un gruppo specifico di persone**, dovute all'età o alla disabilità fisica o mentale, al fine di distorcere materialmente il comportamento, in modo da poter provocare un danno;

✓ sistemi di **social scoring** da parte di autorità pubbliche, volti alla valutazione o classificazione dell'affidabilità delle persone per un determinato periodo di tempo sulla base del comportamento sociale o di caratteristiche personali o della personalità, in cui il punteggio sociale ottenuto comporti il verificarsi di un trattamento pregiudizievole o sfavorevole di determinate persone o di interi gruppi in contesti sociali che non sono collegati ai contesti oppure ingiustificato o sproporzionato rispetto a comportamento;

✓ sistemi di **identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico** a fini di attività di contrasto, a meno che e nella misura in cui tale uso sia strettamente necessario per gli specifici obiettivi previsti, etc.

Proposta di regolamento «Artificial Intelligence Act» (2)

COM(2021) 206 final del 21 aprile 2021

- **sistemi ad alto rischio** → in questa categoria sono compresi:

✓ sistemi destinati a essere utilizzati per l'identificazione biometrica remota "in tempo reale" e "a posteriori" delle persone fisiche
✓ sistemi impiegati nella gestione e nel funzionamento di **infrastrutture critiche**
✓ sistemi usati per determinare l'accesso o l'assegnazione a **istituti d'istruzione e di formazione** o per valutare gli studenti
✓ sistemi destinati a essere utilizzati per procedure di assunzione o selezione di candidati in **ambito lavorativo** e per la gestione e la valutazione dei lavoratori
✓ sistemi per **l'accesso a prestazioni e servizi pubblici e a servizi** privati essenziali e fruizione degli stessi (es. quelli per valutare l'affidabilità creditizia)
✓ sistemi di **valutazione del rischio di commettere reati o di recidiva**
✓ sistemi per la gestione della migrazione, dell'asilo e del controllo delle frontiere, come l'esame delle domande di asilo, visti e permessi di soggiorno
✓ sistemi per **assistere l'autorità giudiziaria** nella ricerca, interpretazione e applicazione della legge, etc.

Proposta di regolamento «Artificial Intelligence Act» (3)

COM(2021) 206 final del 21 aprile 2021

I **sistemi ad alto rischio** sono sottoposti a norme che seguono l'approccio di accountability del regolamento europeo 2016/679 (protezione dei dati personali)

Insieme integrato di strumenti e requisiti da rispettare nel sistema di gestione dei rischi come

- documentazione tecnica adeguata
- qualità dei dataset di addestramento
- valutazione e dichiarazione di conformità
- registrazione e tracciabilità, monitoraggio,
- misure appropriate di sorveglianza umana
- obblighi di trasparenza, accuratezza, robustezza e sicurezza

Sono previste **sanzioni** in caso di mancato rispetto di quanto previsto.

Proposta di regolamento «Artificial Intelligence Act» (4)

COM(2021) 206 final del 21 aprile 2021

La proposta prevede

- **sistemi a basso rischio** → obblighi specifici di trasparenza. Ad esempio:

- nel caso di **chatbot**, l'utente deve essere informato che sta interagendo con un sistema di intelligenza artificiale, a meno che ciò non risulti evidente dalle circostanze e dal contesto di utilizzo,
- nel caso di **deep fake**, ossia un sistema di intelligenza artificiale che genera o manipola contenuti di immagini, audio o video, che somigliano sensibilmente a persone, oggetti, luoghi o altre entità o eventi esistenti e che possono apparire falsamente come autentici o veritieri, è necessario rendere noto all'utente che il contenuto è stato generato o manipolato artificialmente.

- **sistemi a rischio minimo** → consentiti il libero sviluppo ed uso

Proposta di regolamento «Artificial Intelligence Act» (5)

COM(2021) 206 final del 21 aprile 2021

Governance

La proposta prevede un **European Artificial Intelligence Board**, composto da

- autorità nazionali di controllo, di cui è prevista la designazione da parte degli Stati membri
- European Data Protection Supervisor

Funzioni → tale organismo è chiamato a fornire assistenza e consulenza alla Commissione, facilitando la cooperazione in materia, contribuendo agli orientamenti e alle analisi necessarie e assistendo le autorità nazionali di controllo e la Commissione europea nel garantire l'applicazione uniforme del regolamento.

↓

Esigenza di governance si manifesta nei diversi regolamenti europei, che prevedono l'istituzione di Comitati e gruppi di esperti a livello sovranazionale, chiamati a fornire assistenza e consulenza alla Commissione europea

FRAMEWORK ITALIANO

Quadro nazionale su IA

- **Libro Bianco «L'intelligenza artificiale al servizio del cittadino»**, curato dall'Agenzia per l'Italia Digitale (AgID) e dalla Task Force sull'Intelligenza artificiale composta da esperti selezionati, pubblicato nel marzo 2018 → sfide e raccomandazioni

- **Proposte per una strategia italiana per l'intelligenza artificiale**, elaborate dal Gruppo di Esperti sull'intelligenza artificiale nominato dal Ministero dello Sviluppo Economico, 2019 → RenAIssance basata su tre pilastri (umanesimo, affidabilità, sostenibilità)

LIBRO BIANCO - AGID E TASK FORCE

ia.italia.it
#taskforceIA

Libro Bianco IA

“L’intelligenza artificiale al servizio del cittadino”

Task Force IA è stata costituita nel 2017 dall’AgID → **30 componenti** con competenze multidisciplinari selezionati attraverso una call pubblica → **https://ia.italia.it/task-force**

9 sfide

1. Etica
2. Tecnologia
3. Competenze
4. Ruolo dei dati
5. Contesto legale
6. Accompagnare la trasformazione
7. Prevenire le disuguaglianze
8. Misurare l’impatto
9. L’Essere umano

↓

sezione dedicata alle **raccomandazioni**

STRATEGIA NAZIONALE IA

Elaborata dal Gruppo di Esperti MISE sull'intelligenza artificiale

Proposte per una

Strategia italiana

per l'intelligenza artificiale

Ministero dello sviluppo economico

Strategia

RenAIssance

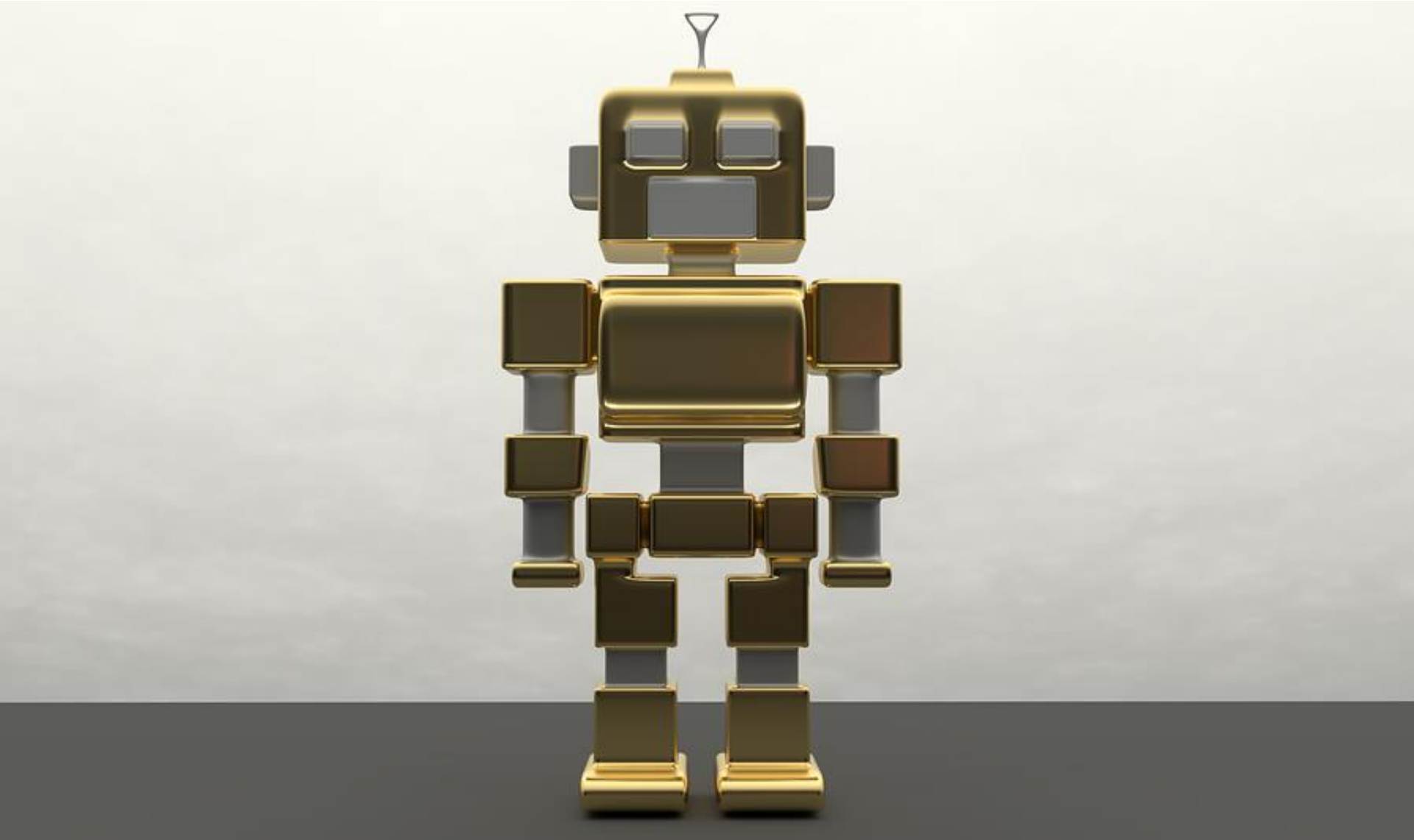
Tre pilastri

1. IA per l'essere umano → **umanesimo**
2. IA per un ecosistema digitale affidabile → **affidabilità**
3. IA per lo sviluppo sostenibile → **sostenibilità**

Tre fattori abilitanti

1. **dati** e loro economia
2. **infrastrutture**
3. **atre tecnologie** (5G, blockchain, sicurezza, cloud computing) → importanza delle interazioni tra tecnologie diverse per moltiplicare il potenziale

ASPETTI GIURIDICI



Ownership

Chi è titolare?
Chi ha prodotto, chi detiene o chi elabora i dati?
Beni pubblici?

1. **proprietà tradizionale** → prospettiva civilistica della proprietà tradizionale, immaginando un diritto di proprietà sui dati da intendere come beni

2. **prospettiva contrattuale** → sfruttare autonomia contrattuale, al fine di tutelare i database per regolarne la cessione o la concessione di diritti di utilizzo temporaneo e al fine di regolare ulteriori aspetti afferenti a intelligenza artificiale, individuando i profili di responsabilità reciproca

3. **proprietà intellettuale** → nel caso di insieme di dati e di software interviene la normativa sul diritto d'autore e sui diritti connessi
   - **"contenitore"** → se si ritiene che il valore sia nell'insieme dei dati → diritto d'autore per le banche dati creative e diritto sui generis per le banche dati non creative (cui in genere sono ricondotti big data).
   - **software e servizi** → algoritmi hanno ruolo cruciale in tali soluzioni – se si ritiene che il valore sia nelle analisi e negli algoritmi: protezione del diritto d'autore

Chi ne è responsabile? (1)

Ricostruzione della responsabilità in caso di incidenti → la dottrina indica diverse possibili strade:

- responsabilità del **produttore** (art. 114, d.lgs. 206/2005)
- responsabilità per l'**esercizio di attività pericolose** (art. 2050 c.c.)
- responsabilità dei proprietari per i **danni cagionati da animali** (art. 2052 c.c.)
- responsabilità **in vigilando e in educando** di genitori, tutori e maestri per i danni cagionati da fatti illeciti dei minori e degli allievi (art. 2048 c.c.)

Seppur meno utilizzate, non manca chi richiama:

- responsabilità per il danno cagionato da **cose in custodia** (art. 2051 c.c.)
- responsabilità per la **circolazione dei veicoli** (art. 2054 c.c.)

Chi ne è responsabile? (2)

- **titolarità diverse** → non si tratta di un singolo bene immateriale, ma di un processo che vede proprietà dei dati, ruolo degli algoritmi, titolarità di software di analisi, contratti eventuali di fornitura di servizi → il titolare dello strumento può essere diverso dal titolare del servizio
- a seconda del caso, può cambiare la **partecipazione umana** all'azione e alla decisione che conduce a eventuali danni. Chi è responsabile in caso di errori o bias? La responsabilità è ascrivibile sempre e solo ad un soggetto umano o talvolta gli algoritmi in autonomia conducono a decisioni o soluzioni che possono provocare danni? Come avrebbe dovuto essere diversamente programmato l'algoritmo per evitare il danno?

↓

- **"sistemi agenti"** → esigenza di imputabilità autonoma in considerazione del difficile collegamento tra le attività delle macchine e la responsabilità umana. Il Parlamento europeo affronta la questione con **sistemi di assicurazione obbligatoria** e forme di **responsabilità oggettiva** → si interroga sul riconoscimento dello status giuridico di **personalità elettronica**, seppur non sia scevro di problematiche, quali **l'attribuzione di diritti e doveri** e l'individuazione della capacità di agire

Personalità elettronica

Ordinamenti giuridici cominciano a interrogarsi se la macchina non sia soltanto oggetto di diritti, ma possa diventare soggetto di diritti → tecnologia non è più solo un "mezzo" per realizzare azioni, ma sempre più è essa stessa a prendere autonomamente decisioni significative per la persona umana e la sua libertà

soggettività giuridica, personalità "elettronica" e diritti a macchine?

↓

complesse implicazioni filosofiche ed etiche, legate al riconoscimento di prerogative umane ad agenti diversi

- **titolarità del diritto d'autore** su opere create da macchine (quali opere d'arte, software) → diritto d'autore presuppone un autore umano

- **attribuzione della responsabilità** in caso di danni, insieme alla correlata questione del **risarcimento**

Chi è titolare dei diritti?

The Next Rembrandt

2016

https://www.nextrembrandt.com

Edmond De Belamy

2018

opera venduta all'asta alla cifra di 432.500 dollari

Rischi e problematiche giuridiche

- **necessario rispetto dei principi dell'ordinamento**, tra cui dignità, pieno sviluppo della persona, eguaglianza e non discriminazione → necessità di valutazione su impatto giuridico, sociale ed etico e rischi per la collettività

- **concorrenza** → rischio che i colossi del web siano dominanti sul mercato con violazione delle norme antitrust (la concentrazione Microsoft/Skype 2011, concentrazione Facebook/WhatsApp 2014)

- **segreto industriale** → in specifico per proteggere gli algoritmi e le tecniche di analisi impiegate per estrarre valore dai dati

- **tutela del consumatore e dell'utente** → rischio di inefficacia alla luce di pratiche commerciali opache, black box, rischio di discriminazioni, disparità di trattamento e di prezzo, distorsioni

- **legge applicabile e giurisdizione competente** → criticità geopolitiche; raccolta e utilizzo dei dati è sovranazionale e si pongono difficoltà a stabilire la legislazione e la giurisdizione nel momento patologico del conflitto

Problematiche giuridiche in ambito pubblico

Rispetto norme e principi che guidano azione pubblica → tra queste:

- **procedimento** amministrativo → principi di **imparzialità**, **trasparenza** e **partecipazione** (legge 241/1990; d.lgs. 33/2013) → es. esigenza di motivazione (art. 3, legge 241/1990), garantire forme di accesso e assicurare correlate garanzie processuali
- **amministrazione digitale** (d.lgs. 82/2005) → es. diritti digitali
- **qualità dei dati pubblici** (d.lgs. 82/2005; d.lgs. 33/2013) → quantità, incertezza, natura inferenziale e probabilistica rischiano di mettere in crisi la disciplina

↓

esigenza di garantire **trasparenza e apertura** non solo dei dati, ma anche della **logica degli algoritmi** e del **processo di funzionamento** del servizio

↓

esigenza di garantire **certezza del diritto**

Il caso relativo alla scuola (1)

Caso afferente all'algoritmo usato nella procedura di mobilità dei docenti nelle sedi disponibili nell'organico della scuola.

- **TAR Lazio-Roma, sezione III bis, 21 marzo 2017, n. 3742 e 22 marzo 2017, n. 3769** → diritto di accesso documentale all'algoritmo deputato a gestire il procedimento, configurato quale atto amministrativo informatico.

- **TAR Lazio, sez. III bis, 10 settembre 2018, nn. 9224-9930; TAR Lazio, sez. III bis, 27 maggio 2019, n. 6606; TAR Lazio, sez. III bis, 13 settembre 2019, n. 10964**

✓ **netta chiusura** all'impiego di algoritmi per decisioni amministrative, anche laddove scaturenti da un'attività vincolata e in casi complessi e ampi

✓ **algoritmo incapace di assicurare le garanzie procedimentali e i principi** di trasparenza, partecipazione e obbligo di motivazione con le **correlate garanzie processuali** (diritto di azione e difesa in giudizio)

Il caso relativo alla scuola (2)

- **Consiglio di Stato, Sezione VI, 8 aprile 2019, n. 2270**

✓ **algoritmo** in ambito pubblico è giuridicamente **ammissibile e legittimo per attività vincolate prive di discrezionalità, ma utilizzo di procedure "robotizzate" non può essere motivo di elusione dei principi dell'ordinamento**. La regola tecnica che governa l'algoritmo resta una regola amministrativa generale, costruita dall'uomo e non dalla macchina, per essere poi solo applicata da questa.

✓ necessarie **conoscibilità** secondo una declinazione rafforzata del principio di trasparenza e **giustiziabilità** quale soggezione alla piena cognizione e al pieno sindacato del giudice amministrativo

✓ nella fattispecie violazione dei principi di imparzialità, pubblicità e trasparenza → impossibilità di comprendere le modalità con cui, attraverso l'algoritmo, sono stati assegnati i posti disponibili, costituisce di per sé un vizio tale da inficiare la procedura → gli esiti sono risultati connotati da **illogicità e irrazionalità**, essendosi verificate **situazioni paradossali**, in contrasto con le disposizioni di riferimento

Il caso relativo alla scuola (3)

- **Consiglio di Stato, sez. VI, 13 dicembre 2019, n. 8472, n. 8473 e n. 8474**

Nuovo meta-principio di legalità algoritmica → principi scaturenti anche dal diritto sovranazionale (es. regolamento UE 2016/679)

- ✓ **conoscibilità e comprensibilità** → necessaria motivazione e giustificazione della decisione in senso sostanziale e non rigida e meccanica applicazione delle regole procedimentali → diritto a conoscere i diversi aspetti dell'algoritmo e decifrarne la logica → autori, procedimento per l'elaborazione, meccanismo di decisione, comprensivo delle priorità nella procedura valutativa e decisionale e dei dati rilevanti
- ✓ **non discriminazione algoritmica** → algoritmo non deve assumere carattere discriminatorio, garantendo la qualità dei dati, minimizzando il rischio di errori e rettificando i dati o i fattori che possano determinarli
- ✓ **non esclusività della decisione algoritmica** → deve essere assicurato intervento umano, anche solo in termini di controllo, verifica e validazione

La censura, più che singole violazioni di legge, finisce per involgere il metodo in quanto tale per difetto di trasparenza dello stesso

IA E DATA PROTECTION

Framework giuridico (1)

- **Regolamento UE 2016/679 relativo alla protezione dei dati personali, nonché alla libera circolazione di tali dati General Data Protection Regulation – GDPR** → teso a rendere omogenea ed efficace la tutela della persona, rafforzando la correlata fiducia da parte della collettività

Disciplina non riguarda **i dati anonimi** → dati che in origine o a seguito di trattamento non possono essere associati ad un interessato identificato o identificabile (considerando 26, reg. UE 2016/679) →

anonimizzazione è diversa da pseudonimizzazione

- **Regolamento (UE) 2018/1807 sulla libera circolazione dei dati non personali nell'Unione europea** → teso a sfruttare le opportunità dell'economia basata sui dati, nella quale si collocano gli stessi big data (superamento degli obblighi di localizzazione dei dati, messa a disposizione e accesso di autorità competenti, portabilità dei dati non personali etc.)

Framework giuridico (2)

Sull'interazione tra i due regolamenti rileva la **Comunicazione della Commissione europea «Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union»** del 29 maggio 2019 → atto esclusivamente a titolo informativo, che per espressa dichiarazione non contiene alcuna interpretazione autorevole

↓

Nel caso dei **big data** i dati sono di tipologia eterogenea e provengono da fonti diverse → di norma avranno la connotazione di **insiemi di dati misti**

- dati personali e dati non personali non indissolubilmente legati → reg. UE 2018/1807 si applica alla parte contenente dati non personali e reg. (UE) 2016/679 si applica alla parte contenente dati personali.
- dati personali e dati non personali **indissolubilmente legati** → reg. UE 2018/1807 lascia impregiudicata l'applicazione del reg. (UE) 2016/679 → **applicazione piena del regolamento (UE) 2016/679 all'insieme di dati misti**, anche quando i dati personali rappresentano solo una piccola parte.

Principi

Big data e soluzioni di IA rischiano ontologicamente di scontrarsi con i **principi applicabili al trattamento previsti dal regolamento (UE) 2016/679** (art. 5):

- **limitazione della finalità** → i dati devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità (art. 5, paragrafo 1, lett. b)

- **minimizzazione dei dati** → devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (art. 5, paragrafo 1, lett. c)

- **esattezza e accuratezza dei dati** → dati devono essere di qualità, ossia esatti e aggiornati (art. 5, paragrafo 1, lett. d)

Informazioni e consenso

Problemi anche per il rispetto di pilastri della disciplina:

- **informazioni da fornire all'interessato** → artt. 12-13-14
- **consenso** → art. 7 → preventivo, specifico, inequivocabile, revocabile

↓

Su cosa saranno fornite le informazioni e su cosa sarà espresso il consenso? È autenticamente libero il consenso se fornito a fronte di vantaggi conseguibili in termini relazionali, professionali, sociali e a fronte dell'accesso alla propria vita digitale?

Apparente libertà, rileva il considerando 42, reg. UE «*il consenso non dovrebbe essere considerato liberamente espresso se l'interessato non è in grado di operare una scelta autenticamente libera o è nell'impossibilità di rifiutare o revocare il consenso senza subire pregiudizio*»

Dati personali e dati anonimi

- esistono **dati totalmente anonimi**? Inferenze su gruppi, metadati, dati residui, dati ausiliari…

- la **definizione stessa di dato personale** può essere insufficiente → dati afferenti a gruppi o comunità sulla cui base sono prese decisioni che incidono anche sul singolo che non ha prestato il consenso e non ha ceduto dati, oltre ai metadati e ai dati residui

- **necessità di condotte difensive** → l'individuo è costretto a pagare in termini monetari e di tempo per mettere in atto strategie difensive dei propri dati

↓

marketing diretto e connessa profilazione → art. 21, comma 2 → può essere considerato legittimo interesse su cui basare il trattamento dei dati personali → consente il trattamento

↓

La protezione avviene con **diritto di opposizione** in qualunque momento → **meccanismo di opt-out**

Processo decisionale automatizzato

L'interessato ha il **diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione**, che produca effetti giuridici o che incida in modo analogo significativamente sulla sua persona.

↓

La previsione non si applica nel caso in cui la decisione:

a) **sia necessaria per la conclusione o l'esecuzione di un contratto** tra l'interessato e un titolare del trattamento;
b) **sia autorizzata dal diritto dell'Unione o dello Stato membro** cui è soggetto il titolare del trattamento […];
c) **si basi sul consenso esplicito** dell'interessato.

Nel caso a) e c), il titolare deve attuare misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno **il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione**.

(art. 22, regolamento europeo 2016/679)

SCENARI FUTURI E STRUMENTI DI GOVERNANCE

IA antropocentrica e affidabile

Necessità di una nuova **etica digitale** che guidi la regolazione

↓

Intelligenza antropocentrica e affidabile

come emerge dalle strategie e dagli atti europei in materia

Fondamentale l'elemento umano,

la capacità dell'uomo di orientare la tecnologia → la tecnologia da sola non basta; necessità del ruolo del diritto che deve servirsi di un approccio etico.

Bilanciamento "mobile" tra diritti e interessi può basarsi sulla **centralità della persona**, sui valori della dignità e dello sviluppo della stessa, condivisi fondamenti costituzionali

↓

persona come **prisma i cui riflessi sono costituiti dai diversi diritti in gioco** che poggiano e convergono sul condiviso fondamento costituzionale, la clausola aperta dei diritti della personalità di cui all'art. 2 Cost.

Diritto nella tecnica e accountability

Approccio sistematico, preventivo, proattivo e tecnico
logica del regolamento UE 2016/679

- **incorporazione del diritto nella tecnica**
  richiama la funzione preventiva del diritto che si serve della tecnologia per garantire il suo rispetto → **legal protection by design** e **by default**→ privacy by design e by default (art. 25), data protection impact assessment (art. 35), data breach (artt. 33-34) → **risk-based approach**

- **accountability, sicurezza ed approccio etico** → artt. 24 e 32 → il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere **in grado di dimostrare**, che il trattamento è effettuato conformemente al regolamento

- **responsabilità e sistema sanzionatorio** → artt. 82-84 → sanzioni severe utili a garantire effettività

✓ **Proposta di regolamento «Artificial Intelligence Act»**, COM(2021) 206 final, 21/04/2021

-

Diritto alla comprensione e alla contestabilità

Trasparenza → ai sensi degli artt. 13, 14 e 15 del regolamento europeo 2016/679 tra le informazioni da fornire all'interessato e su cui ha accesso:

- l'esistenza di un processo decisionale automatizzato, compresa la profilazione, e, almeno in tali casi,
- **informazioni significative sulla logica utilizzata**,
- **l'importanza e le conseguenze previste** di tale trattamento per l'interessato.

↓

trasparenza algoritmica

explainable AI

riequilibra asimmetria, supera opacità di black box e incide sulla libertà:

diritto alla comprensione, spiegabilità e diritto alla contestabilità,

il singolo deve essere garantito nel diritto all'autodeterminazione informativa

↓

diritto alla sindacabilità

da parte dell'interessato e del giudice

✓ **Proposta di regolamento «Artificial Intelligence Act»** parla di appropriato livello di trasparenza (sufficiently transparent)

Supervisione e sorveglianza umana

Supervisione e alla sorveglianza umana sono tese a **prevenire e minimizzare rischi e pericoli** → in linea con l'approccio proattivo e preventivo

↓

equilibrio tra la componente umana e la componente macchina,
attraverso la garanzia dello **"human in the loop"**

↓

evitare il rischio che concretamente la decisione
umana possa essere "attratta" dai risultati della macchina

Explainability costituisce la condizione necessaria per la supervisione umana → solo se l'essere umano è in grado di comprendere il modo in cui il sistema decide può operare un controllo effettivo

- ✓ **Proposta di regolamento «Artificial Intelligence Act»** prevede misure concrete da applicare individuate dal fornitore, che consentono a chi è affidata la sorveglianza umana di comprendere e interpretare il sistema, intervenire o interromperlo, decidere se utilizzarlo e restare consapevole della possibile tendenza a fare eccessivo affidamento sull'output

Apertura e diritto al riutilizzo

Utilizzo sinergico di open data e big data, proteggendo le libertà dei singoli e la sovranità dei dati relativi

↓

sanatoria al momento della diffusione,

liberando i dati, in linea con la natura non escludibile e non rivale del bene

(limitato dal potere economico o pubblico)

↓

garantisce diritti e libertà degli individui,

un accesso equo e maggiore concorrenza,

competitività ed equità del mercato.

Forme di tutela collettiva?

Forme di tutela collettiva → i dati sono beni comuni, a titolarità diffusa, con impatto collettivo

↓

autodeterminazione collettiva

Accanto a possibilità per l'interessato di dare mandato a organismo o associazione per reclamo o ricorso giurisdizionale per suo conto (art. 80, comma 1), è significativo **art. 80**, comma 2 → gli Stati membri possono prevedere che un **organismo, organizzazione o associazione**, indipendentemente dal mandato conferito dall'interessato, abbia

- il **diritto di proporre un reclamo** all'autorità di controllo e
- il **diritto a proporre un ricorso giurisdizionale**

qualora ritenga che i diritti di cui un interessato gode siano stati violati

↓

tutela collettiva ex post
conforme ai valori collettivi oggetto di protezione

Quale “orizzonte giuridico” digitale?

- nuova etica digitale
- centralità della persona, supremazia delle libertà e dei diritti fondamentali
- diritto deve recuperare spazio giuridico pubblico
- creazione di un adeguato contesto istituzionale
- evitare la “logica del più forte” e il rischio di “privatizzazione” della rete

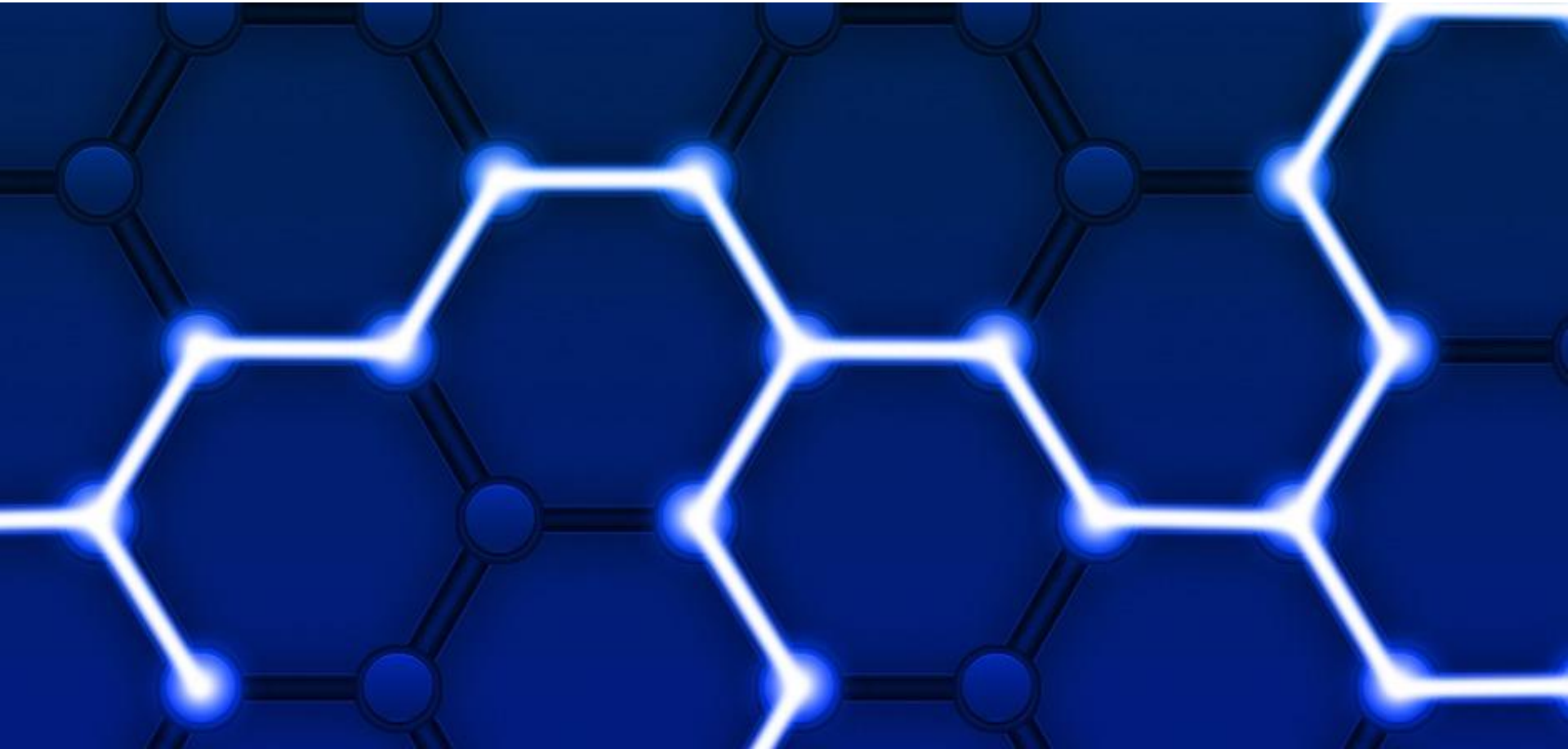
Costruzione di un **costituzionalismo globale** (S. Rodotà)

- **regole comuni** e dimensione sovranazionale (ma emergono forme di sovranismo e nazionalismo e nuovi blocchi geopolitici)
- **integrazione di regole diverse** → regole giuridiche, lex informatica, regole del mercato e dei colossi tecnologici, regole sociali, soft law
- **genesi orizzontale, per espansione**
- **approccio multistakeholder e multilevel** → pluralità di attori e livelli
- **nuove forme di cooperazione e collaborazione tra Stati**

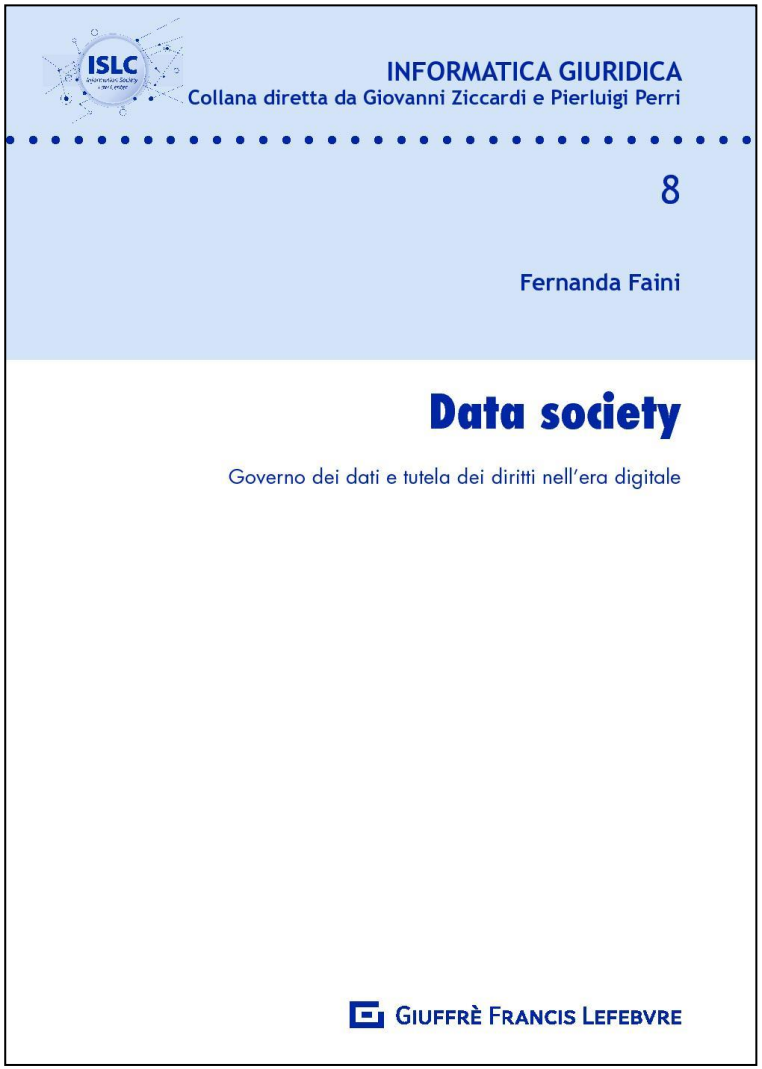
Ubi data society, ibi ius

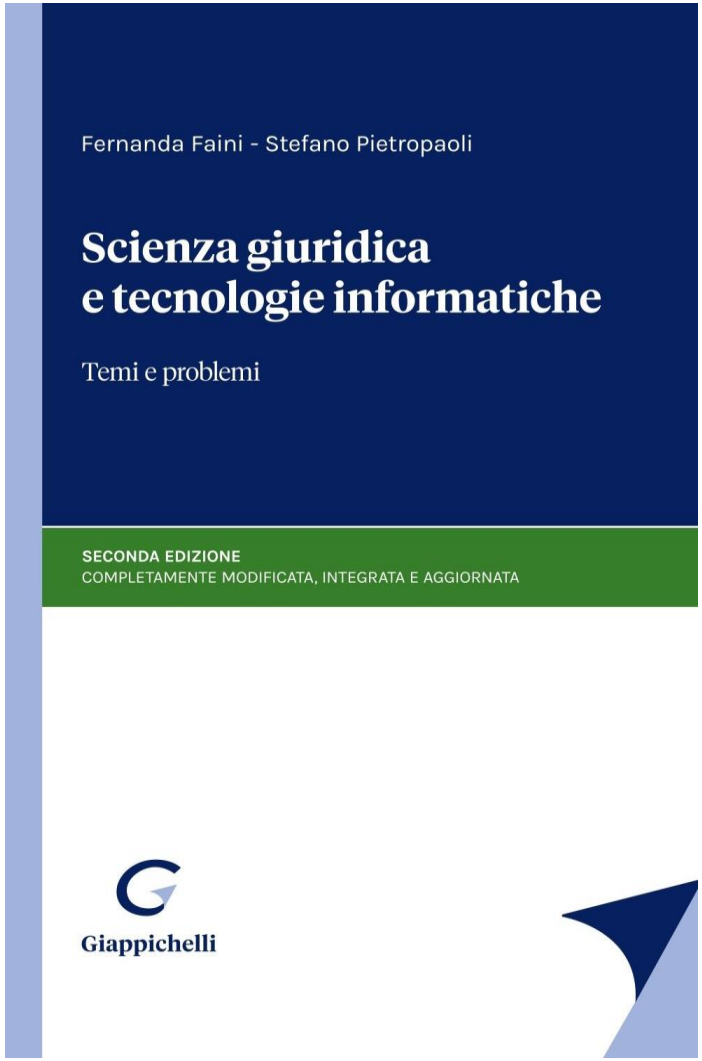
il governo dei dati necessita del ruolo del diritto e della forza dei diritti per riuscire a proteggere la persona nell'era digitale e

disegnare il presente e il futuro della democrazia



PROCEDamus
PROCEDIMENTI AMMINISTRATIVI DELLE UNIVERSITÀ DEGLI STUDI
progetto di formazione-intervento per le università e gli enti di ricerca





Grazie per l'attenzione

Fernanda Faini

Docente a contratto di diritto dell'informatica – Università di Pisa
Docente a contratto in "ICT & Law" – Università Cattolica del Sacro Cuore
Docente a contratto di "Diritto e nuove tecnologie" – Università Uninettuno

email fernandafaini@gmail.com

LinkedIn fernandafaini

BY NC ND