StatCities 2023
TRAVOLTI DA UN INSOLITO DESTINO NEL MARE SMERALDO DEI DATI
15 e 16 giugno 2023 – Museo Archeologico, OLBIA

# La tutela dei dati personali negli ambiti IA

Paola Baldi

Sessione: Intelligenza artificiale e statistica

Comune di Olbia

Unione Statistica Comuni Italiani

# Di che cosa parliamo

❑ Tema dell'intelligenza artificiale (IA):

- Da mesi improvvisamente al centro dell'attenzione dei media, del grande pubblico, ma anche dei Governi di molti paesi, dopo la presentazione e la messa a disposizione di strumenti di dialogo e interrogazione basati su sistemi GPT (*Generative Pre-Trained Transformer, una rete neurale artificiale per modelli di linguaggio di grandi dimensioni*).
- Entusiasmo per le grandi opportunità di utilizzo e le possibili ricadute positive dell'intelligenza artificiale in molti ambiti.
- Preoccupazioni su aspetti etici, giuridici, tecnologici, e sui possibili impatti negativi per gli individui e per la società.

❑ Qui ci limitiamo ad alcune considerazioni sullo sviluppo (*rapido e inarrestabile*) delle tecnologie IA e sulle iniziative in corso da tempo per governarne lo sviluppo e l'applicazione nell'ambito di un quadro normativo condiviso,

❖ con riferimento in particolare alla compatibilità dei sistemi IA che utilizzano dati personali con i principi e la normativa sulla protezione dei dati personali.

# I tempi

| La protezione dei dati personali. | Intelligenza Artificiale | La strategia europea per l'intelligenza artificiale |
|---|---|---|
| • 1995 Direttiva 95/46 (CE)<br>• 2009 Trattato di Lisbona: protezione dati personali è diritto fondamentale dei cittadini<br>• 2016 GDPR: Responsabilizzazione del Titolare del trattamento dei dati personali | • Anni 50-80 del XX secolo: «approccio umano»<br>• Anni 80 del XX secolo ad oggi: «approccio razionale» | • 2018 Comunicazione «Intelligenza artificiale per l'Europa»<br>• 2020 Libro bianco sull'IA<br>• 2021 Proposta di Regolamento UE (AI Act)<br>• 2023 AI Act: In corso l'esame del Parlamento e del Consiglio dell'UE |

# La protezione dei dati personali
# Evoluzione del quadro normativo europeo

- **Direttiva 95/46 (CE),** «relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati»
- **Trattato di Lisbona (2007)**: il diritto alla protezione dei dati personali, già previsto nel 2000 dalla *Carta dei diritti fondamentali dell'Unione europea (Carta di Nizza),* è diventato diritto fondamentale dei cittadini, da garantire allo stesso modo in tutto il territorio dell'Unione.
- **Regolamento (UE) 2016/679** del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali , nonché alla libera circolazione di tali dati, e che abroga la direttiva 95/46/CE (Regolamento Generale sulla Protezione dei Dati – RGPD).
- **Adeguamento delle normative nazionali**

# La protezione dei dati personali
# Evoluzione normativa

- Con il Regolamento UE (2016/679) si è passati da norme prevalentemente prescrittive a regole basate sulla responsabilizzazione del titolare del trattamento dei dati e sulla trasparenza.
- Non solo «tutela della riservatezza», ma «protezione dei diritti e delle libertà fondamentali, in particolare il diritto alla protezione dei dati personali»
- Oltre ai principi applicabili e alle condizioni di liceità del trattamento dei dati personali, il Regolamento stabilisce i diritti degli interessati *(tra cui, ad esempio, il diritto a non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona)* e gli obblighi per il titolare del trattamento *(tra cui in particolare: informazioni agli interessati, analisi dei rischi per i diritti e le libertà, adozione di misure di garanzia e di sicurezza).*

# Intelligenza artificiale - Sviluppo

Anni 50-80 del XX secolo

- Progetti basati su approccio linguistico o logico-simbolico *(approccio umano)*:
  - formalizzare processi informatici che riproducessero i processi umani di comprensione e decisione.
  - Buoni risultati in sistemi a informazione perfetta e/o in ambiti specialistici. Sistemi esperti.

Anni 80 del XX secolo – ad oggi

- Cambio di paradigma tecnologico *(approccio razionale)*:
  - approccio statistico
  - modelli basati su algoritmi e su reti neurali artificiali
  - sistemi di apprendimento automatico (*machine learning*);
    algoritmi «addestrati» su grandi basi di dati e migliorati tramite l'esperienza (*deep learning*) per generare nuovi output (*IA generativa*).

# La strategia europea per l'intelligenza artificiale

- Aprile 2018 – «**L'Intelligenza artificiale per l'Europa**» - Comunicazione della Commissione al Parlamento europeo, al Consiglio europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni.

- *Propone un approccio che pone le persone al centro dello sviluppo dell'intelligenza artificiale (IA antropocentrica) e incoraggia l'uso di questa potente tecnologia per contribuire a risolvere le più importanti sfide mondiali nei settori principali (sanità, trasporti, ambiente, attività produttive…..).*
- *Si basa su tre pilastri:*
  - *Aumentare gli investimenti pubblici e privati nell'IA*
  - *Prepararsi ai cambiamenti socioeconomici*
  - ***Garantire un quadro etico e giuridico adeguato***
- *Propone una prima definizione di Intelligenza Artificiale*

# Cos'è l'intelligenza artificiale? *(2018- AI for Europe)*

- ***Intelligenza artificiale (IA)*** *«indica sistemi che mostrano un comportamento intelligente analizzando il proprio ambiente e compiendo azioni, con un certo grado di autonomia, per raggiungere specifici obiettivi»*

- I sistemi basati sull'IA possono consistere in software che agiscono nel mondo virtuale *(per esempio assistenti vocali, chatbox, software per l'analisi delle immagini, motori di ricerca, sistemi di riconoscimento vocale e facciale*); oppure incorporare l'IA in dispositivi hardware *(per esempio in robot avanzati, auto a guida autonoma, droni o applicazioni dell'Internet delle cose*).
- Utilizziamo l'IA quotidianamente (*per esempio per tradurre le lingue o bloccare lo spam delle email o nei suggerimenti per gli acquisti on line)*.
- **Molte tecnologie di IA richiedono l'uso di dati (anche personali) per migliorare le loro prestazioni** *(dati di addestramento degli algoritmi).*

# Usi quotidiani e possibili dell'IA *(2018 - AI for Europe)*

# La strategia europea per l'intelligenza artificiale - AI Act

- Dicembre 2018 – «Piano coordinato sull'intelligenza artificiale» *(da aggiornare annualmente)*
- Febbraio 2020 – «Libro bianco sull'intelligenza artificiale. Un approccio europeo all'eccellenza e alla fiducia»
- Aprile 2021 – Proposta di Regolamento della Commissione europea che stabilisce regole armonizzate sull'intelligenza artificiale (**Legge sull'intelligenza artificiale** / **AI Act**)
- Dicembre 2022 – Adottata posizione del Consiglio dell'UE in merito all'AI Act
- Maggio 2023 – Le commissioni Mercato Interno e Libertà Civili del Parlamento europeo hanno adottato il testo modificato dell'AI Act
- **14 Giugno 2023 – Approvazione del Parlamento europeo in seduta plenaria**
- *Successiva negoziazione con gli stati membri (Consiglio dell'UE) e rappresentanti della Commissione UE per l'adozione definitiva della nuova legge, che sarà in vigore per tutti gli stati membri (ma si applicherà dopo 24 mesi dall'entrata in vigore)*

# L'AI Act nel contesto delle iniziative UE per l'IA

- L'iter della proposta di regolamento (legge AI Act) procede in parallelo con le altre iniziative dell'approccio europeo all'intelligenza artificiale, che comprende ulteriori atti di regolamentazione *(legge sulla governance dei dati, legge sui servizi digitali e sui mercati digitali, strategia in materia di cyber sicurezza…),* ma anche iniziative per promuovere e sostenere gli sviluppi della tecnologia e la fiducia degli utenti.

- Contemporaneamente alla proposta di AI Act, nel 2021 è stato presentato anche il **piano coordinato aggiornato per l'IA,** *con il quale la Commissione e gli Stati membri intendono promuovere l'eccellenza nell'IA unendo le forze per massimizzare le risorse e coordinare gli investimenti, attraverso i programmi Europa digitale e Orizzonte Europa (che fa seguito a Horizon 2020) e ulteriori investimenti del settore privato e degli Stati membri.*

  - *Sono previsti bandi e finanziamenti per progetti di IA per i settori più rilevanti e per la ricerca scientifica e l'innovazione.*

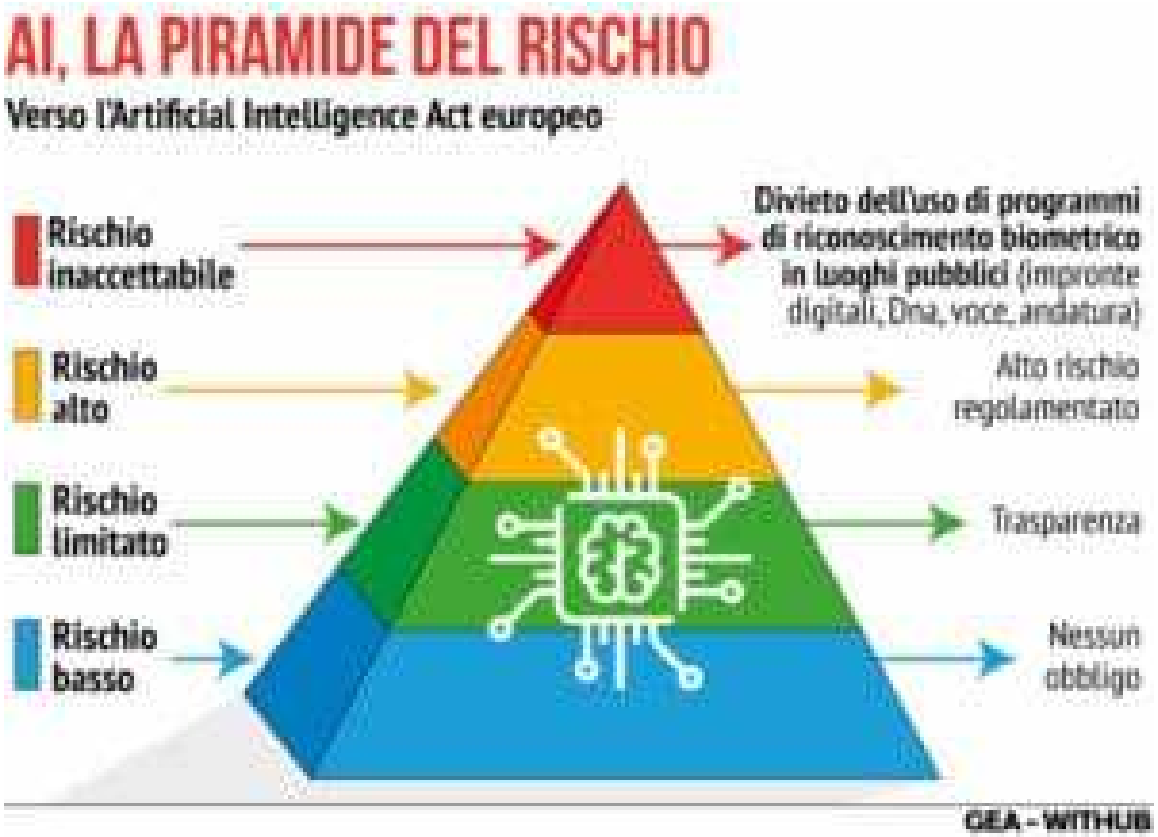
# Progetto TRUSTS

- Particolare rilevanza, per gli aspetti legati alla protezione dei dati personali, riveste il Progetto **TRUSTS** (Trusted Secure Data Sharing Space), finanziato dall'UE e volto a ripristinare la fiducia nel mercato dei dati.
  - Il progetto della durata di tre anni (2020-2022), ha riunito 17 partner di 9 paesi europei, con l'obiettivo di creare un mercato pan-europeo sicuro e affidabile per i dati personali e industriali
- Obiettivo del progetto: sviluppare nuove piattaforme di tipo federativo, che consentano di sperimentare architetture di data sharing *(non trasferimento di dati, ma accesso ai dati controllato*), che
  - siano basate su scambi di dati sicuri e affidabili tra fornitori e consumatori di dati,
  - forniscano servizi informativi utili a chi carica i propri dati sulla piattaforma e ne mantiene il controllo,
  - garantiscano il rispetto dell'anonimato,
  - propongano processi di utilizzo dei dati con soluzioni tecnologiche conformi al GDPR e che pertanto possano essere non limitate ai dati open, ma estendibili anche ai dati personali e ai dati aziendali .

# Intelligenza artificiale – IA *(AI Act - testo modificato 2023)*

- ***Sistema di intelligenza artificiale**: «un sistema basato su macchina progettato per operare con diversi livelli di autonomia e che può, per obiettivi espliciti o impliciti, generare risultati quali previsioni, raccomandazioni o decisioni, che influenzano ambienti fisici o virtuali»*
  - Il riferimento a «previsioni» include «contenuti», che sono considerati una forma di previsioni.
  - Per «ambienti» si intende «i contesti in cui i sistemi IA operano»
  - La nuova definizione comprende i sistemi per impieghi generali (General Purpose AI) e i modelli di base (foundation models), compresi i modelli di linguaggio generativo di grandi dimensioni (IA generativa).
- La proposta di Regolamento suddivide i sistemi IA in base ai **rischi** che pongono **per i diritti fondamentali.**

# Classificazione dei sistemi IA in base al livello di rischio



# Principi generali per tutti i sistemi di IA

Lo sviluppo e l'uso dei sistemi di IA e dei modelli di base (*foundation models*) deve rispettare i **principi generali** dell'approccio europeo umano-centrico *(art. 4 AI Act)* :

- ❑ Sorveglianza e intervento umano
- ❑ Robustezza tecnica e sicurezza
- ❑ **Tutela della privacy e data governance**
- ❑ Trasparenza
- ❑ Diversità, non discriminazione ed equità
- ❑ Benessere sociale e ambientale

*La sfida: adottare definizioni e creare regolamentazione che resista alla prova del tempo (consentendo alle regole di adattarsi ai cambiamenti tecnologici), rappresenti un compromesso accettabile tra le diverse visioni e non sia troppo influenzata dal dibattito sulle «questioni del giorno». Tecnologie in rapida evoluzione.*

# Pratiche di IA vietate

Sono **vietate** le applicazioni dell'IA che **violano i valori dell'Unione Europea** e che pertanto implicano un **rischio inaccettabile**, tra cui:

- Immissione sul mercato o utilizzo di sistemi IA che utilizzano tecniche subliminali o che sfruttano la vulnerabilità delle persone, al fine di distorcerne i comportamenti o creare loro danno
- Pratiche di «social scoring» (*sistemi che classificano le persone in base al loro comportamento sociale, alle loro caratteristiche socio-economiche o personali),* che possono comportare conseguenze ingiustificate per determinate persone fisiche o gruppi di persone
- Sistemi di identificazione biometrica remota in tempo reale o a posteriori in luoghi pubblici, a meno di un'autorizzazione preventiva nell'ambito di attività di indagine su specifici reati gravi
- Sistemi che valutano il rischio di commissione di reati basandosi sulla profilazione dell'individuo o valutando le sue caratteristiche

# Sistemi IA ad alto rischio

È considerato **ad alto rischio** l'uso di una serie di tecnologie che creino **rischi elevati** per la salute, la sicurezza, l'ambiente o **i diritti fondamentali delle persone.**

Questi sistemi devono **rispettare specifici requisiti**: certificazione di conformità, sistema di gestione dei rischi, data governance, trasparenza, sorveglianza umana.

**I requisiti e gli obblighi per i sistemi ad alto rischio integrano quelli previsti dalla normativa privacy già in vigore (GPDR)**.

Sono sistemi IA ad alto rischio:

1) I sistemi per i quali è richiesta una valutazione di conformità ai sensi della normativa di armonizzazione dell'UE indicata nell'Allegato II dell'AI Act *(sicurezza di macchinari, giocattoli, dispositivi medici, trasporti, etc.)*
2) I sistemi elencati nell'Allegato III *(se creano rischi elevati)*. È previsto un periodico aggiornamento, delegato alla Commissione UE. ***Quasi tutti** i sistemi che rientrano in questo elenco prevedono il **trattamento di dati personali.***

# Sistemi ad alto rischio (AI Act - Allegato III)

Sistemi di IA destinati ad essere utilizzati per:

- **Identificazione e categorizzazione biometrica remota delle persone fisiche,** "in tempo reale" e "a posteriori" *(escluse le applicazioni che rientrano tra le pratiche IA vietate)*
- Gestione e funzionamento delle infrastrutture critiche (*componenti di sicurezza nella gestione del traffico stradale e nella fornitura di acqua, gas, riscaldamento, elettricità)*
- **Istruzione e formazione professionale** *(al fine di determinare l'ammissione di persone fisiche agli istituti di istruzione e formazione professionale o per valutare gli studenti)*
- **Occupazione, gestione dei lavoratori e accesso al lavoro autonomo** *(per l'assunzione o la selezione di persone fisiche, in particolare per vagliare o filtrare le candidature, valutare i candidati , oppure per adottare decisioni sulle persone nell'ambito dei rapporti di lavoro)*
- **Accesso a prestazioni e servizi pubblici e a servizi privati essenziali e fruizione degli stessi** *(per l'accesso alle prestazioni e ai servizi di assistenza pubblica, ai servizi di emergenza di primo soccorso, l'accesso al credito, ….)*
- **Attività di contrasto** *(per valutare rischi di reato effettivo o potenziale, anche sulla base della profilazione delle persone, della rilevazione dello stato emotivo, dei tratti e delle caratteristiche delle persone fisiche o di gruppi di persone; per individuare «deep-fake» )*

# Sistemi a rischio limitato e a rischio minimo

- Il **rischio limitato** si riferisce ai sistemi di IA con specifici **obblighi di trasparenza** *(sistemi destinati a interagire con le persone fisiche: chatbot, deep fake, sistemi di riconoscimento delle emozioni)*.

- **Modelli di base (Foundation models).**
  L'AI Act prevede ulteriori obblighi di trasparenza e specifici requisiti di progettazione, documentazione, monitoraggio per i modelli di base.
  Questi sistemi non sono inseriti tra i sistemi ad alto rischio, ma dovranno comunque essere progettati e sviluppati nel rispetto del diritto dell'UE e delle libertà fondamentali.

- La proposta di Regolamento consente l'uso libero dell'**IA a rischio minimo** *(rientra in questa categoria la gran parte dei sistemi di IA utilizzati nell'UE: applicazioni come videogiochi, filtri antispam ...)*

# Norme privacy vigenti (GDPR)

In attesa dell'approvazione e entrata in vigore dell'AI Act, **tutti i sistemi** di intelligenza artificiale **che utilizzano dati personali** (indipendentemente dal loro livello di rischio) **devono comunque rispettare le disposizioni del GDPR**, con riferimento

- ai **principi applicabili** nel trattamento dei dati personali (*liceità, correttezza, trasparenza, limitazione delle finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza, responsabilità)*
- ai **diritti degli interessati** *(diritto di chiedere l'accesso ai dati personali che li riguardano, la rettifica, la cancellazione, la limitazione del trattamento o di opporsi allo stesso, nonché il diritto alla portabilità dei dati)*
- agli **obblighi del titolare del trattamento,** in particolare:

- *progettazione per impostazione predefinita configurando fin dall'inizio le garanzie indispensabili per la sicurezza del trattamento dei dati,*
- *valutazione di impatto su diritti e libertà degli interessati, adozione di misure tecniche e organizzative adeguate per la riduzione o eliminazione del rischio,*
- *informativa agli interessati che specifichi, tra l'altro, la finalità e la base giuridica del trattamento dei dati (consenso, legittimo interesse del titolare, contratto, …)*

# L'iniziativa del Garante italiano su ChatGDP

- La necessità di rispettare le norme vigenti in materia di privacy era già stata evidenziata formalmente da altre autorità *(ad es. Information Commissioner's Office - ICO, il «Garante» inglese, ha pubblicato nel 2021 e aggiornato nel 2023 le proprie linee guida su IA e protezione dati*), ma senza intervenire con provvedimenti diretti su casi specifici.
- 30 Marzo 2023 - Sospensione dell'uso di ChatGPT in Italia fino a presentazione di risposte da OpenAI, per presunte violazioni della normativa GDPR su informative, base giuridica del trattamento dei dati, diritti degli interessati, tutela dei minori.
- 27 aprile 2023 – Fine della sospensione. OpenAI ha presentato le risposte richieste e realizzato gli adattamenti necessari:
  - *pubblicata informativa che illustra quali dati sono trattati (dati conferiti e dati sull'utilizzo dei sistemi), e con quali modalità, per l'addestramento degli algoritmi e che ricorda che chiunque ha diritto di opporsi a tale trattamento,*
  - *implementato modulo che consente di esercitare il diritto di opposizione e di escludere conversazioni e cronologia dal training degli algoritmi,*
  - *richiesta data di nascita per registrazione; da implementare successive misure per verifica età.*
  - *Ulteriore impegno, ancora da realizzare, per una adeguata campagna informativa.*

# Protezione dati personali e IA

- Adeguamenti richiesti dal Garante Privacy: uno standard per il futuro?
  - Non solo CHAT GPT. Molti altri prodotti simili (Bard di Google, Claude di Anthropic, Bing di Microsoft, ….), anche con differenti impostazioni riguardo l'etica dei sistemi IA.
- Iniziative di altri Paesi (Francia, Irlanda, Canada…). L'European Data Protection Board ha lanciato una task force su ChatGPT per promuovere collaborazione tra le autorità europee.
- **Requisiti GDPR**: non ostacoli allo sviluppo delle tecnologie , ma «**vincoli tecnici**» da inserire nella progettazione.
  - Stimoli per l'accelerazione di nuove soluzioni tecnologiche *(uso di dati pseudonimizzati o anonimizzati o di set di dati sintetici per l'addestramento degli algoritmi)* e per strategie dei produttori *(versioni progettate per rendere i sistemi più trasparenti, versioni con maggiore controllo dei dati immessi dagli utenti)*
- Non solo protezione dati personali (persone fisiche), ma anche esigenza di tutelare il patrimonio informativo aziendale *(versioni «personalizzate» con dati di addestramento «aziendali» su server separati, segmentazione dei prodotti ….)*

# Regolamentazione e innovazione

- Preoccupazione per possibile ostacolo a sviluppo tecnologie e ricerca nel settore: non tanto per le norme privacy, già in vigore, ma soprattutto per gli ulteriori requisiti e gli obblighi che saranno introdotti dall'AI Act per i produttori di sistemi *(gestione dei rischi, data governance, rispetto diritti d'autore, etc.)*
- Sviluppi dell'IA generativa: Non solo problemi etici, anche necessità di migliorare gli algoritmi *(sia per evitare la possibilità di aggirare i limiti/divieti, sia per aumentare l'attendibilità dei risultati* ) e la **qualità dei dati usati per addestramento** *(eliminare possibili distorsioni e fattori di discriminazione)*
- AI Act - Misure a sostegno dell'innovazione *(spazi di sperimentazione, misure per i fornitori di piccole dimensioni e gli utenti)*
- Anche le grandi aziende e i portatori di interessi hanno bisogno di standard e regolamentazione, ma chiedono poche regole, chiare e non troppo rigide
- Possibile collaborazione tra aziende e legislatori e iniziative di autoregolamentazione dei produttori di sistemi IA *(anche per anticipare i tempi di entrata in vigore dell'AI Act)*
- In discussione tra UE e Stati Uniti un **Codice di condotta volontario**, da adottare in tempi brevi

# IA, protezione dati personali e statistica

- Possibile uso dei sistemi IA per analisi statistiche con tecniche deep learning: *basi dati enormi, grandi quantità di dati, utilizzo non solo per addestramento sistemi IA, per risposte a richieste utenti chatbot e per utenti sistemi «settoriali»*
- Possibile uso dei sistemi IA per la «stima» di valori mancanti (microdati) delle variabili in archivi statistici? *(Archivi integrati, Registri)*
- Necessità di sviluppare nuovi modelli teorici e/o nuove tecniche di analisi?
- Impatto su aspetti privacy: *Regole simili a quelle previste per statistiche su big data (rispetto principi GPDR, valutazione di impatto, descrizione fonti…). Nuove regole ad hoc?*
- Necessità comunque di tenere separate le variabili prodotte attraverso sistemi IA *(riconoscibilità)* perché si possa tenere conto della loro natura nelle analisi statistiche.
- Rafforzamento della natura solo statistica dei Registri? o possibile ipotizzare sottoinsiemi di un Registro con usi differenziati?

- Per colmare questo lungo vuoto legislativo, l'Unione europea sta già discutendo con gli Stati Uniti un codice di condotta volontario, che dovrebbe vedere la luce nelle prossime settimane.

Grazie per l’attenzione!



*335 1225582*


*paolabaldi49@gmail.com*