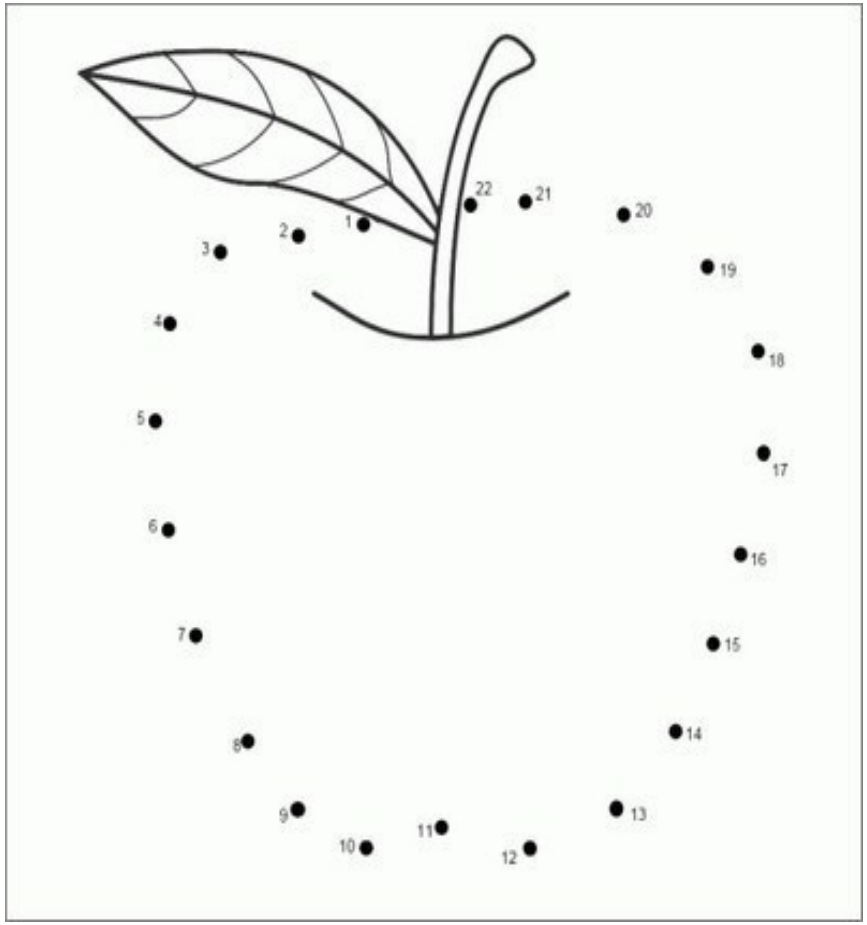
L’intreccio tra
AI Act, Privacy e CAD
nell’adozione di tool IA nella PA

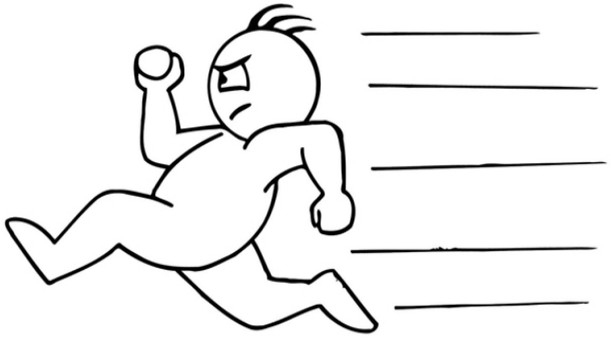
Prof. Avv. Marco Mancarella
Professore Associato di Informatica giuridica – UniSalento
Componente @LawLab – LUISS Guido Carli di Roma
Fondatore LiquidLaw srl
Avvocato esperto in Amministrazione digitale e Privacy

spin-off
UniSalento
2018-22


1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22

l'entropia di un sistema isolato lontano dall'equilibrio tende ad aumentare nel tempo, finché l'equilibrio non è raggiunto

«Il diritto è sempre in affanno rispetto alla tecnologia»



L'intelligenza artificiale è centrale per la trasformazione digitale della società ed è diventata una delle priorità dell'UE.

ChatGPT, l'Intelligenza Artificiale usata in un tribunale colombiano

Un magistrato del paese sudamericano ha utilizzato la nuova e discussa chatbot di OpenAI per la redazione di una sentenza

Di Marco Martorana
Avvocato

Pubblicato il 22/02/2023

FERNANDA GONZÁLEZ INTELLIGENZA ARTIFICIALE 05.12.2023

In Brasile è stata approvata una legge scritta da ChatGPT

È successo a Porto Alegre, nel sud del paese, e il consigliere comunale che ha proposto la norma lo ha rivelato solo dopo l'entrata in vigore

INTELLIGENZA ARTIFICIALE

Rubare i dati da ChatGPT, usando ChatGPT: così le IA rivelano nomi, cognomi, volti e indirizzi delle persone

di Emanuele Capone

Un team di ricercatori ha scoperto una falla nella più nota fra le IA generative, che può essere forzata a svelare informazioni sensibili. L'italiana Annalisa Barla: "Impatto grave soprattutto per i possibili usi aziendali di questi strumenti"

03 DICEMBRE 2023 AGGIORNATO 04 DICEMBRE 2023 ALLE 07:36

5 MINUTI DI LETTURA

PROVVEDIMENTO DEL GARANTE PRIVACY IN TEMA DPIA N. 269 del 19 novembre 2018

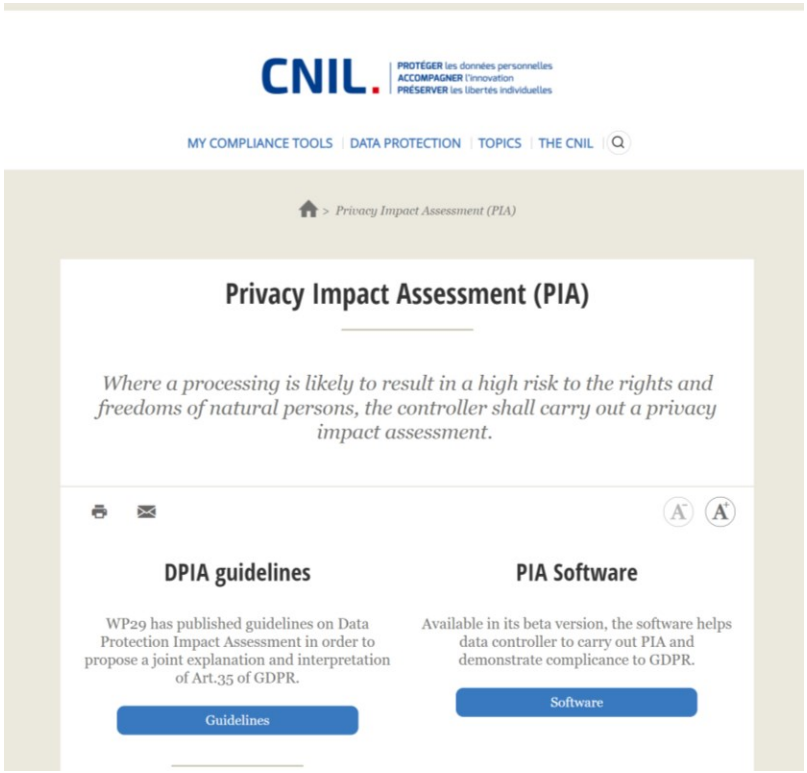
Obbligo di valutazione di impatto per IA per valutare il rischio nel trattamento dati!!!

La **valutazione di impatto del trattamento** (**D.P.I.A., cioè *Data Protection Impact Assessment*)** è un processo volto a descrivere il trattamento, valutarne la necessità e la proporzionalità e a gestire gli eventuali rischi per i diritti e le libertà delle persone derivanti dal trattamento

*7. Trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; **sistemi di intelligenza artificiale**; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il wi-fi tracking) ogniqualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01*

https://www.garanteprivacy.it/valutazione-d-impatto-della-protezione-dei-dati-dpia-

https://www.cnil.fr/en/privacy-impact-assessment-pia



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 - GDPR)

Altri necessari adempimenti

- Informative ad hoc
- Registro trattamenti sempre aggiornato
- Revisione procedure, soprattutto data breach e esercizio diritti
- Nomine Responsabili del trattamento «rinforzate»

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** (regolamento UE 2024/1689)

↓

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

- **Data Governance Act** – Regolamento UE 2022/868

- **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

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 (Commissione UE), 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

«Artificial Intelligence Act»

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.

«Artificial Intelligence Act»

- **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.

«Artificial Intelligence Act»

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

Ponte AI ACT - GDPR

ai sensi dell'articolo 27, paragrafo 4, del Regolamento UE 1689/2024 – AI ACT la **valutazione d'impatto sui diritti fondamentali (cd. FRIA) per i sistemi IA ad alto rischio effettuata dai deployer (anche PA)** può andare ad integrare la valutazione d'impatto sulla protezione dei dati (ove già presente)

Ponte AI ACT - GDPR

Nel contesto della FRIA, gli **utilizzatori** devono
- **descrivere i processi** in cui il sistema di IA sarà impiegato e la sua finalità
- **indicare il periodo di tempo e la frequenza** con cui il sistema sarà utilizzato, **le categorie** di individui e gruppi impattati da tale utilizzo, eventuali specifici rischi, i **sistemi di controllo umano attivati** nonché le **misure** da adottare qualora i rischi identificati si concretizzino

«Artificial Intelligence Act»

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 (ad es. videogiochi abilitati all'intelligenza artificiale o filtri antispam)

«Artificial Intelligence Act»

In via generale, l'applicazione del Regolamento si avrà **soltanto a partire dal 2 agosto 2026,** ossia al decorso di ventiquattro mesi dalla sua entrata in vigore

Tuttavia, l'AI Act prevede, in via del tutto eccezionale, una scaletta progressiva per l'inizio di operatività di alcuni specifici capi e disposizioni in base a quanto previsto dall'art 113, tra questi casi:

1.I capi I e II (definizioni e pratiche vietate) si applicano a decorrere **dal 2 febbraio 2025**

2.Il capo III, sezione 4 (autorità di notifica designate dagli stati membri), il capo V (modelli di AI per finalità generali), il capo VII (banca dati UE per i sistemi ad alto rischio), il capo XII (sanzioni) e l'art. 78 (riservatezza dei dati trattati in conformità al regolamento) si applicano **a decorrere dal 2 agosto 2025**, ad eccezione dell'art. 101 (sanzioni pecuniarie per i fornitori di modelli di IA per finalità generali)

3.L'art. 6, paragrafo 1 (classificazione dei sistemi ad alto rischio), e i corrispondenti obblighi di cui al Regolamento, si applicano **a decorrere dal 2 agosto 2027**

«Artificial Intelligence Act»

Sono state poi dettate tempistiche precise sui passaggi successivi alla pubblicazione in Gazzetta dell'AI Act:

- il Considerando 174 sancisce infatti che in considerazione dei "*rapidi sviluppi tecnologici e le competenze tecniche necessarie per applicare efficacemente il presente regolamento, la Commissione dovrebbe* ***valutare e riesaminare*** *il presente regolamento* ***entro il 2 agosto 2029 e successivamente ogni 4 anni*** *e riferire al Parlamento europeo e al Consiglio*"

«Artificial Intelligence Act»

Limitazioni all'Identificazione Biometrica
L'accordo introduce restrizioni sull'uso dei sistemi di identificazione biometrica in spazi pubblici, richiedendo autorizzazioni giudiziarie e definendo chiaramente i reati per i quali possono essere utilizzati.
L'impiego di queste tecnologie sarà circoscritto a casi come la ricerca di vittime di rapimento, la prevenzione di minacce terroristiche o l'identificazione di sospetti di gravi crimini.

Divieti specifici sull'uso dell'Intelligenza Artificiale
Vengono vietate pratiche come la categorizzazione biometrica basata su caratteristiche sensibili (credenze politiche, religiose, razza), la raccolta indiscriminata di immagini per creare database di riconoscimento facciale, il riconoscimento delle emozioni sul posto di lavoro e nelle scuole, il social scoring, e l'uso di IA per sfruttare vulnerabilità individuali.

«Artificial Intelligence Act»

Le sanzioni previste

Le sanzioni per le violazioni della legge europea sull'intelligenza artificiale (AI) sono stabilite come percentuali del fatturato annuo globale dell'azienda colpevole o come un importo fisso, scegliendo il maggiore tra i due. Le ammende sono dettagliate come segue:

- fino a 35 milioni di euro o il 7% del fatturato per violazioni delle applicazioni AI proibite
- fino a 15 milioni di euro o il 3% del fatturato per le violazioni degli obblighi previsti dalla legge sull'AI
- fino a 7,5 milioni di euro o l'1,5% del fatturato per la fornitura di informazioni non corrette

Per le PMI e le start-up, sono previsti massimali di ammende più proporzionati in caso di violazione. Inoltre, individui o entità possono presentare reclami alle autorità di vigilanza del mercato competenti per mancata conformità alla legge sull'AI, con la garanzia di un trattamento adeguato del reclamo secondo le procedure dell'autorità.

«Artificial Intelligence Act»

Obblighi DEPLOYER

l'AI Act prevede obblighi (presidiati da ingenti sanzioni) anche per gli **utilizzatori ("*deployer*")** dei sistemi di intelligenza artificiale, ossia per chi (persona fisica o giuridica) impieghi questi sistemi per finalità che non siano meramente personali

Gli obblighi degli utilizzatori si aggiungono a quelli imposti ad altri soggetti (***provider*, rappresentanti autorizzati, importatori e distributori**) coinvolti a vario titolo nel mettere sul mercato un sistema di IA

«Artificial Intelligence Act»

Obblighi DEPLOYER

Ad esempio, un **deployer** che decida di adottare un sistema di intelligenza artificiale catalogato **ad alto rischio** dall'AI Act (tra cui, sistemi adoperati nell'attività di ricerca del personale o *recruiting*, di identificazione biometrica remota o utilizzati per valutare l'affidabilità creditizia) sarà soggettO a una serie di **obblighi pervasivi, elencati nell'art. 26** dell'AI Act

Fra l'altro, gli utilizzatori devono:

- adottare **appropriate misure tecniche e organizzative** per garantire di utilizzare i sistemi di IA nel rispetto delle istruzioni fornite dal *provider*
- provvedere al **controllo umano tramite personale con opportune competenze**
- nonché, ove abbiano il **controllo sui dati di *input* del sistema di IA, assicurare che tali dati siano pertinenti e sufficientemente rappresentativi** rispetto alla finalità del sistema

«Artificial Intelligence Act»

Obblighi DEPLOYER

Qualora, invece, un ente valuti di investire in un sistema di IA **a rischio limitato**, gli oneri saranno più ridotti, ma l'azienda sarà comunque soggetta a **doveri informativi** nei confronti delle persone fisiche con cui il sistema interagisce

Ad esempio, gli utilizzatori di sistemi di riconoscimento delle emozioni, di categorizzazione biometrica o creatori di *deep fake* devono fornire informazioni sul funzionamento di tali sistemi nonché sul fatto che i contenuti mostrati sono stati artificialmente creati o manipolati

Queste informazioni si aggiungono a quelle che gli utilizzatori devono fornire agli interessati ai sensi del GDPR

«Artificial Intelligence Act» (8)

Obblighi DEPLOYER

In conclusione:

- necessaria **cooperazione tra deployer e gli altri soggetti coinvolti** (*in primis*, i *provider*). Ad esempio, i deployer devono monitorare il funzionamento del sistema di IA sulla base delle istruzioni fornite dai *provider* e, laddove ritengano che tale sistema possa presentare un rischio per la salute, la sicurezza o i diritti fondamentali delle persone, devono informare senza ritardo il *provider* (o il distributore) e l'autorità di controllo. Simili obblighi di notifica sono previsti anche in caso di incidenti gravi
- i **contratti** tra deployer e *provider* / importatori / distributori potranno definire i tempi di notifica di eventuali rischi o incidenti e le informazioni da fornire a corredo; ciò anche per agevolare la successiva notifica all'autorità di controllo.

La maggior parte degli obblighi che l'AI Act impone agli utilizzatori dei sistemi di IA sarà applicabile a partire dal 2026

«Artificial Intelligence Act» (9)

Implicazioni per sistemi ad alto Rischio
L'accordo stabilisce requisiti rigorosi per i sistemi di IA considerati ad alto rischio, inclusi quelli utilizzati in contesti elettorali o per influenzare il comportamento degli elettori.
Tali sistemi dovranno sottostare a valutazioni di impatto sui diritti fondamentali.
Inoltre, i cittadini avranno il diritto di presentare reclami e richiedere spiegazioni riguardo le decisioni prese da questi sistemi.

Sostegno all'Innovazione
Disposizioni che consentono di **testare i sistemi di AI in condizioni reali**, nel rispetto di specifiche condizioni e salvaguardie.

Il regolamento **esclude dalla sua applicazione i sistemi impiegati unicamente per finalità militari o di difesa**. Analogamente, l'accordo stabilisce che il regolamento non riguarderà i sistemi di intelligenza artificiale usati esclusivamente a fini di ricerca e innovazione, così come non si applica a coloro che fanno uso di AI per scopi personali e non professionali.

«Artificial Intelligence Act» (11)

Ufficio AI della Commissione Europea
Per assicurare il rispetto delle nuove regole europee sull'intelligenza artificiale (AI), verrà creato un Ufficio AI all'interno della Commissione Europea. Questo ufficio avrà il compito di supervisionare i modelli avanzati di AI, promuovere standard e pratiche di test, e garantire l'applicazione delle regole in tutti gli Stati membri.

Un gruppo di esperti indipendenti fornirà consulenza sull'AI, aiutando nello sviluppo di metodologie per valutare i modelli di AI e monitorando i rischi per la sicurezza.

Il Comitato di AI, composto da rappresentanti degli Stati membri, agirà come organo di coordinamento e consultivo, giocando un ruolo chiave nell'attuazione del regolamento. Sarà inoltre istituito un forum consultivo che coinvolgerà varie parti interessate per fornire competenze tecniche al Comitato per l'AI.

FRAMEWORK ITALIANO

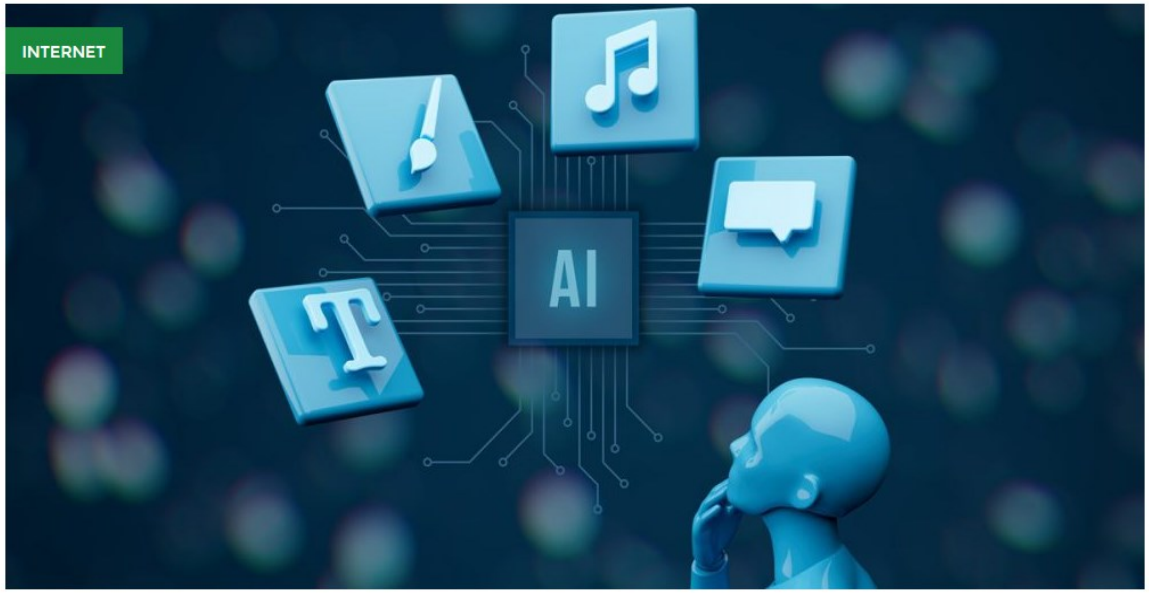
AgID | Agenzia per l'Italia Digitale

Il Responsabile per la Transizione al Digitale

AUTORITÀ

Intelligenza Artificiale, ora è ufficiale: la vigilanza in Italia ad AgID e ACN

di **Paolo Anastasio** | 20 Marzo 2024, ore 11:50



Ora è ufficiale: la funzione di vigilanza e controllo dell'intelligenza artificiale in Italia andrà all'AgID e per le competenze che riguardano la cybersecurity all'ACN. Marco Scialdone, Head Litigation and Academic Outreach di Euroconsumers: '"Bene che si inizi a fare chiarezza su

DDL IA aprile 2024????

Agid: dovrà sovrintendere lo sviluppo dell'AI, l'applicazione negli enti pubblici e la certificazione e l'accreditamento di chi sviluppa algoritmi

Acn: che invece avrà compiti ispettivi e di sanzione, in caso di illeciti

In parallelo Agid sta impostando le sue linee guida sull'AI

Piano triennale Informatica PA 2024-2026: **dicembre 2024** come la scadenza entro cui Agid dovrà scrivere le **linee guida per promuovere l'adozione dell'intelligenza artificiale nella PA,** per bandire gare e appalti dedicati e per sviluppare le prime applicazioni

Nel 2025 Agid punta a raggiungere quota **150 progetti di intelligenza artificiale** negli enti pubblici, da portare a 400 nei 12 mesi successivi. In parallelo, sul fronte acquisti, nel 2025 l'obiettivo è di 100 procedure per acquistare servizi di AI, che **nel 2026 devono aumentare fino a 300**. Mentre nel campo delle applicazioni, i traguardi da raggiungere nel 2025 e nel 2026 sono rispettivamente di 50 e 100 progetti di sviluppo avviati.

Esistono sanzioni per il mancato rispetto dei vari obblighi di Amministrazione digitale?

LA VIGILANZA SUGLI OBBLIGHI DI TRANSIZIONE DIGITALE – Le sanzioni

Art. 12, comma 1-ter, del C.A.D.

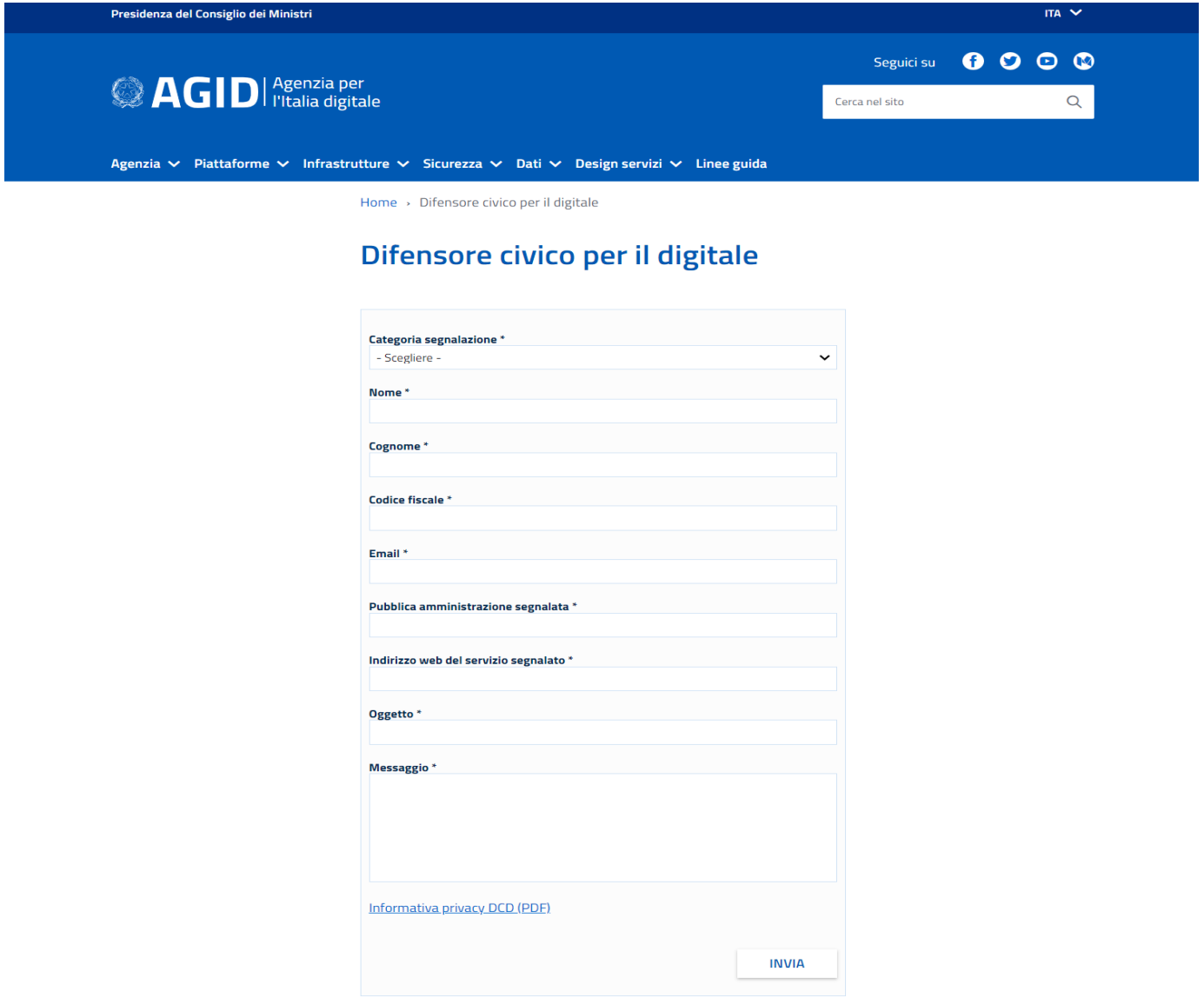
- **Responsabilità del Dirigente**
- Responsabilità civile, penale, contabile, dirigenziale, disciplinare e impatto negativo sulla misurazione e valutazione della performance organizzativa ed individuale dei dirigenti.

Art. 18 bis del C.A.D.

Violazione degli obblighi di transizione digitale

- **Sanzione amministrativa pecuniaria comminata da AGID (avvio 2022) per violazione di qualsivoglia norma attinente al digitale**
- da € 10.000 a € 100.000

LA VIGILANZA SUGLI OBBLIGHI DI TRANSIZIONE DIGITALE – Le sanzioni



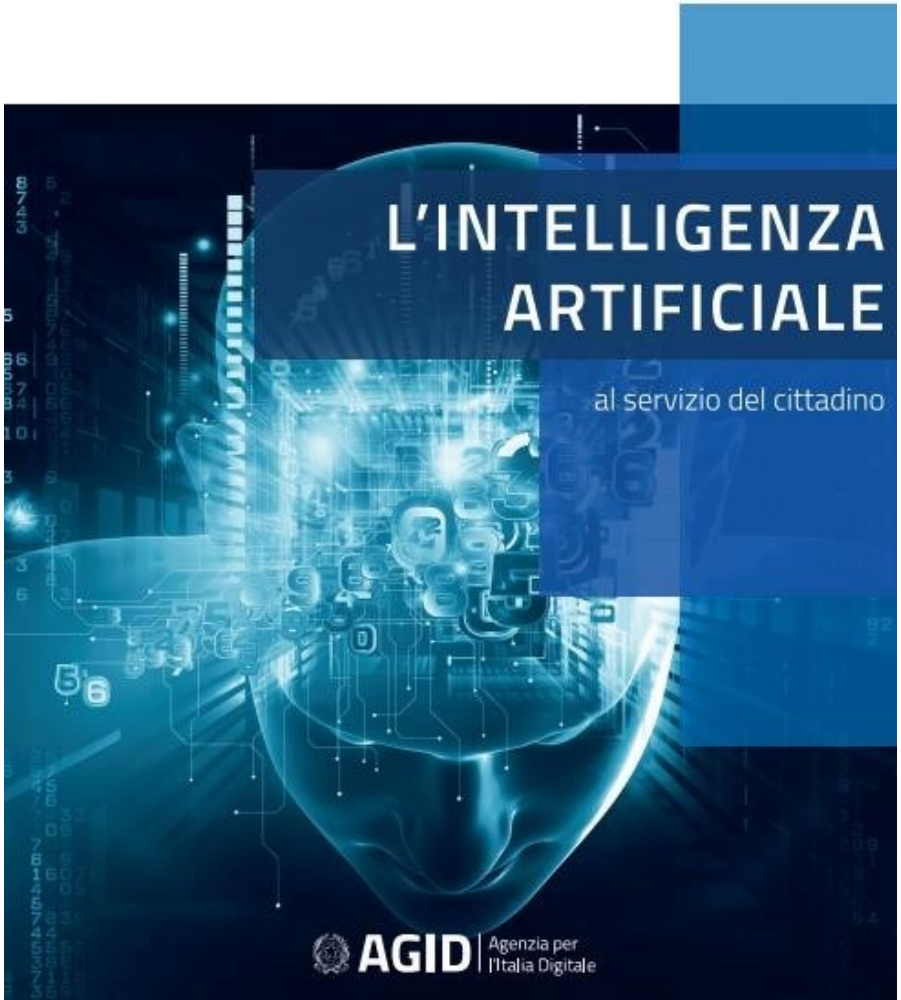
Quadro nazionale su IA

- **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**

STRATEGIA NAZIONALE IA

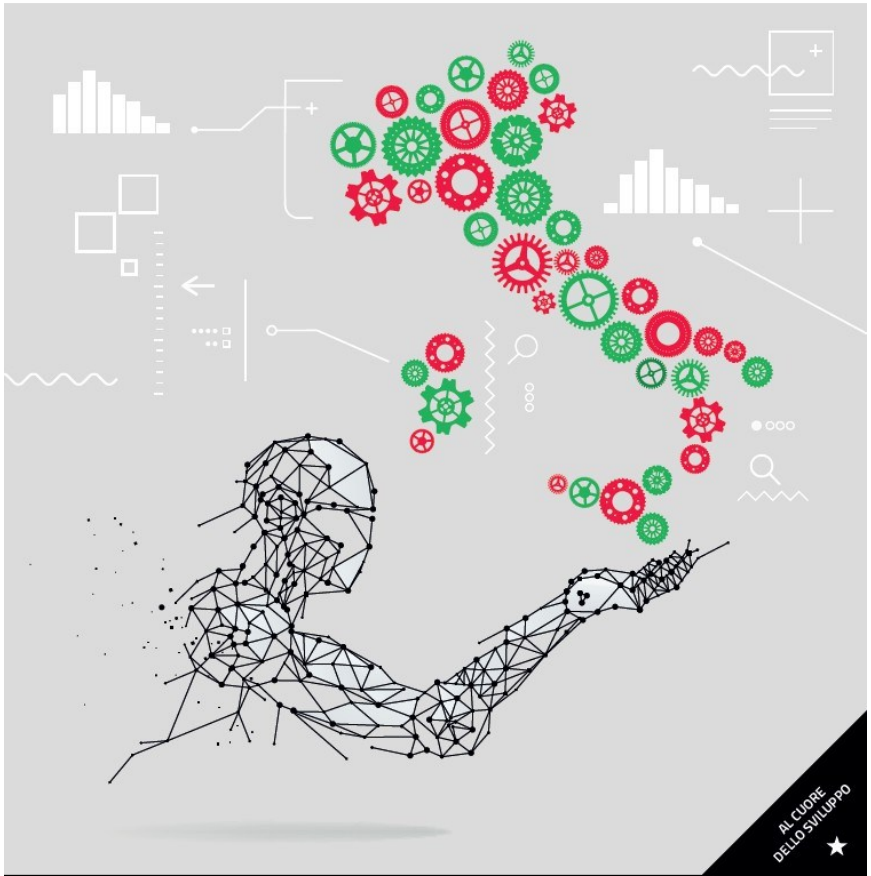
Elaborata dal Gruppo di Esperti MISE sull'intelligenza artificiale

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

CAD – D.Lgs. 82/2005

I DIRITTI DIGITALI

Art. 3 CAD – Diritto all'uso delle tecnologie.

- *Chiunque ha il **diritto di usare**, in modo accessibile ed efficace, le soluzioni e gli strumenti di cui al presente Codice nei rapporti con i soggetti di cui all'articolo 2, comma 2 [P.A.], anche ai fini dell'esercizio dei diritti di accesso e della partecipazione al procedimento amministrativo.*

- Giurisdizione esclusiva del TAR;
- **ATTENZIONE: IL CAD NON CITA ESPRESSALMENTE L'IA**

“L’IA favorirà una definitiva transizione digitale nella gestione documentale?”

- **l’estrazione automatica di informazioni di interesse da grandi insiemi di documenti,** costituiti da testi normativi, regolamentari o di prassi, da riviste, monografie o volumi giuridici
- **l’individuazione e il recupero di documenti** per contenuto e non per semplice parola chiave; la classificazione documentale di testi, atti, schemi e quanto altro ordinariamente in uso nel contesto di un procedimento amministrativo
- **lo sviluppo di interfacce intelligenti** che possano guidare la raccolta delle informazioni utili nel dialogo con gli utenti e di chatbot per fornire le prime risposte orientative ai quesiti posti dal cittadino che propone un’istanza
- **l’assistenza automatizzata nella redazione di testi** in generale e degli atti come delibere, determine o anche contratti, come gli appalti le concessioni

“È possibile formare l’originale di un documento amministrativo in modalità cartacea?”

1. Le pubbliche amministrazioni formano gli originali dei propri documenti, inclusi quelli inerenti ad albi, elenchi e pubblici registri, con mezzi informatici secondo le disposizioni di cui al presente codice e le regole tecniche di cui all'articolo 71.

(Art. 40, D. Lgs. n. 82/2005)

In combinato con l'art. 21 octies della Legge 241/1990 scaturisce la **annullabilità** dell'atto per violazione di legge – art. 40 CAD

invalidità dell'atto…

Art. 21, comma 2ter CAD (novità 2016)

Fatto salvo quanto previsto dal decreto legislativo 2 luglio 2010, n. 110 [ATTO PUBBLICO INFORMATICO DEL NOTAIO], ogni altro atto pubblico redatto su documento informatico e' sottoscritto dal pubblico ufficiale a pena di nullità con firma qualificata o digitale

Documento informatico:

Un documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.

(Art. 1, lett. p), D.Lgs. n. 82/2005)

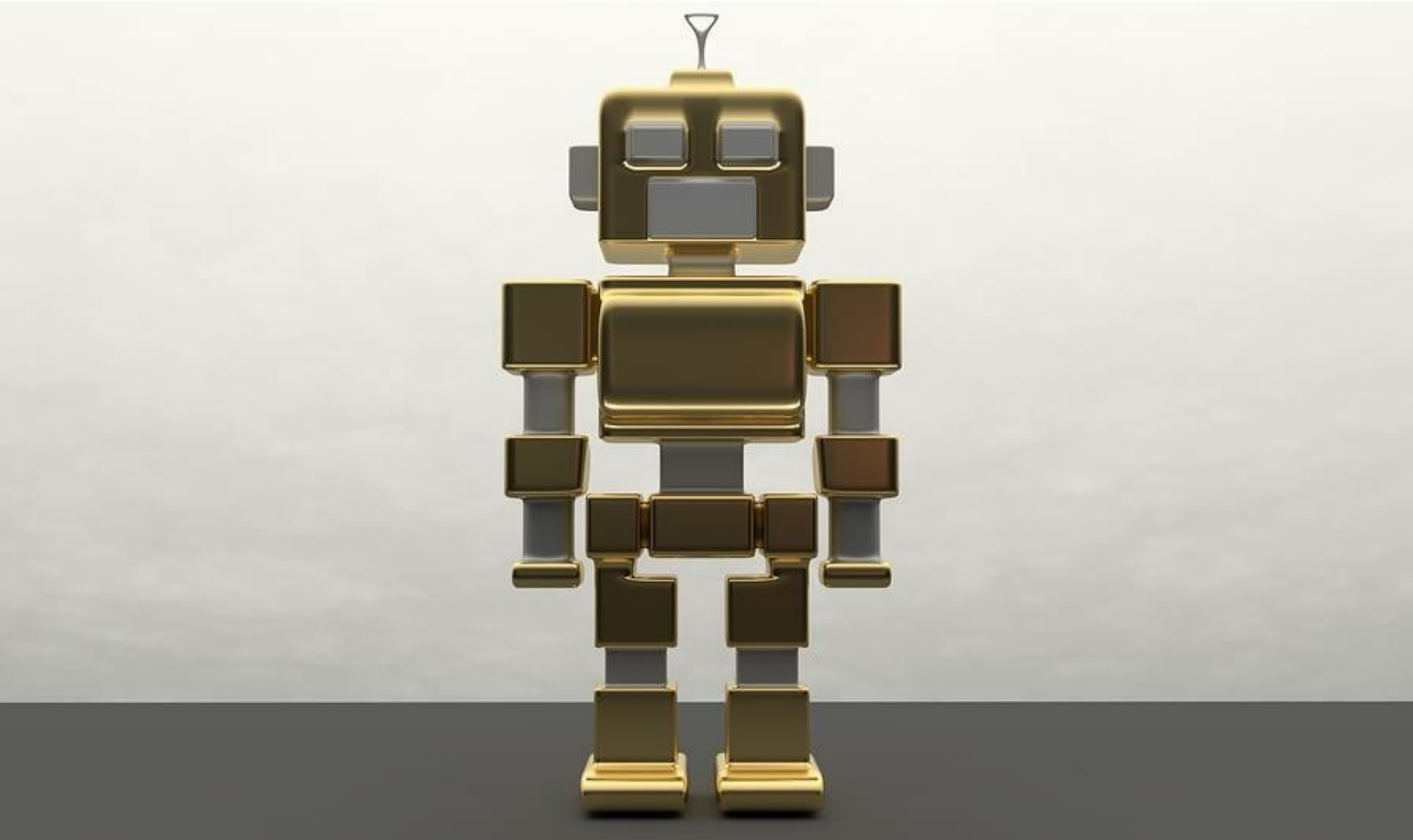
Documento amministrativo informatico:

Ogni rappresentazione, grafica, fotocinematografica, elettromagnetica o di qualunque altra specie, del contenuto di atti, anche interni, formati dalle pubbliche amministrazioni, o, comunque, da queste ultime utilizzati ai fini dell'attività amministrativa

(All. 1 – LG documento informatico 9 settembre 2020)

Per cui “documento amministrativo informatico” può essere un file di testo, una foto, un video, un audio, purchè rappresenti informaticamente un atto, un fatto o un dato rilevanti giuridicamente…potenzialmente anche elaborati tramite IA!

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?

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.)

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

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 documento 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

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** → 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

Ultimo e definitivo caso:

L'ambito di applicazione dell'algoritmo è stato poi esteso anche alle scelte **discrezionali** dell'Amministrazione con due sentenze gemelle del Consiglio di Stato, pubblicate il 13 dicembre 2019 (la n. 2936/2019 e la n. 8474/2019), ma a condizione che, a tutela dell'interesse pubblico, la P.A. assicurasse l'intervento del funzionario nel procedimento

Consiglio di Stato n. 881 del 4 febbraio 2020


PANIC !
ctrl
alt

liquid LAW

Thank you

Prof. Avv. Marco Mancarella

marco.mancarella@liquidlaw.it

www.liquidlaw.it

@liquidlawsrl www.liquidlaw.it liquidlaw

spin-off UNIVERSITÀ DEL SALENTO