



IA e GDPR: riflessioni da DPO su diritti fondamentali da tutelare e falsi miti da smontare

Andrea Lisi



PONTIFICIA
UNIVERSITÀ
ANTONIANUM



UNIVERSITÀ DEGLI STUDI
SUOR ORSOLA
BENINCASA



Centro Universitario Internazionale
di Ricerca e Innovazione "Integral Intelligence".
Futuro, Diplomazia Culturale
e Benessere Integrato



Lui

Umberto
Eco



La Rete è soprattutto una moda. Ma, come l'haute couture, può fare da traino al prêt-à-porter della tecnologia. E a Bologna nasce il primo laboratorio

Internet? È una top model

di VITTORIO ZAMBARDINO



1996...



Vieni vaso, vieni! - RICOMINCIO DA TRE (Massimo Troisi)

Non c'è riuscito Massimo Troisi e ci riuscirà una scimmia con microchip?

La Cina lancia un nuovo chip cerebrale per sbloccare il potenziale umano: come funziona Neucyber

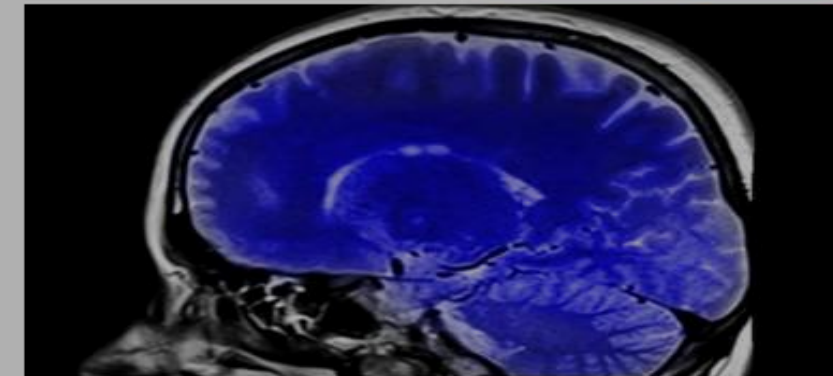
Il chip è stato presentato durante una conferenza tecnologica a Pechino. Il Paese ora sta correndo per recuperare lo scarto e stare al passo con gli Stati Uniti, che già da tempo stanno investendo su interfacce neurali in grado di migliorare le capacità fisiche e mentali.

A cura di **Ellsabetta Rosso**

74
CONDIVISIONI

COMMENTA

CONDIVIDI

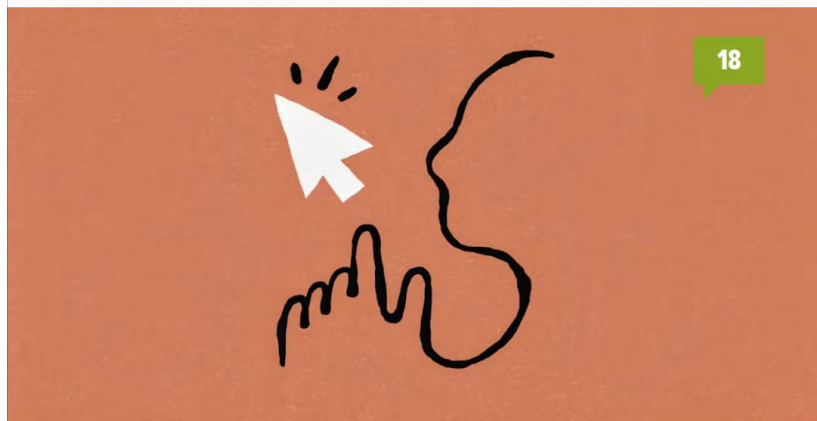


Una scimmia con gli arti legati dietro alla schiena ha preso una fragola con il pensiero. Nell'era delle Brain Computer Interface o Bci, non è poi così strano. La dimostrazione si è svolta a Pechino, la società **Beijing Xinzhiba Neurotechnology**, sostenuta dal governo cinese, ha presentato il suo dispositivo, **Neucyber**, un'interfaccia neurale che vuole competere con i chip Occidentali, come **Telepaty** di Neuralink. Secondo **William Hannas**, analista capo del **Center for Security and Emerging Technology (Cset)** dell'Università di Georgetown, la Cina sta rapidamente recuperando terreno nel settore. "Sono fortemente motivati", ha spiegato a **Wired**. "Stanno facendo un lavoro davvero all'avanguardia".



L'IA può controllare il computer al posto dell'utente. La nuova capacità del modello Claude di Anthropic

di **Sergio Donato** - 23/10/2024



Due sistemi di IA si sono auto-replicati, è la prima volta

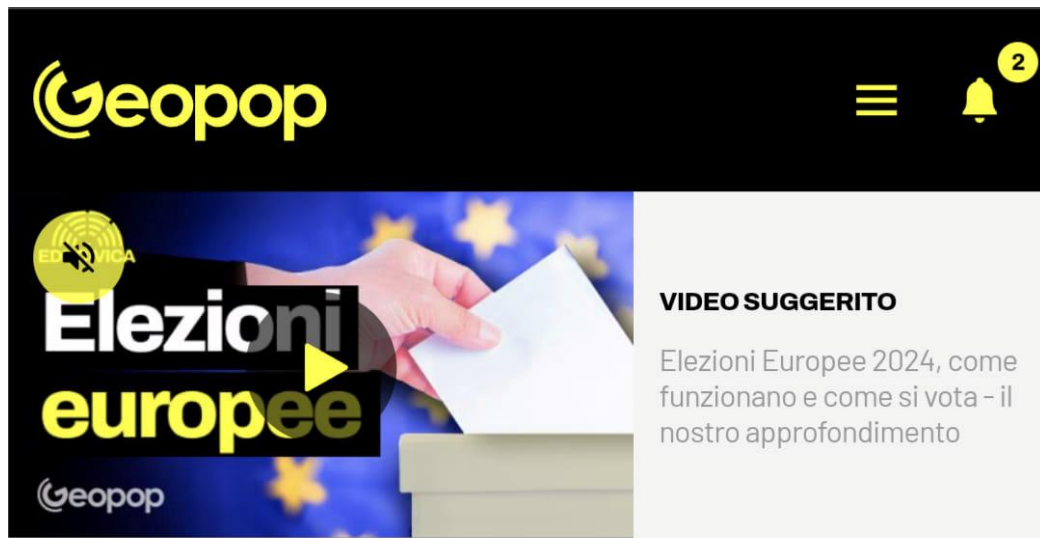
Test in Cina. I ricercatori: 'superata la linea rossa'

27 gennaio 2025, 08:44

di **Enrica Battifoglia**

Condividi





6 Giugno 2024 • 20:30

**«L'AI porterà
all'estinzione umana»:
facciamo chiarezza
sull'allarme lanciato da
13 esperti**

Androidi, stime cui non credere: domineranno il mondo entro il 2035

Già prima del 2030 gli androidi non saranno più un'eccezione. E saranno molto più utili dei robot industriali, pronti a trasformare l'economia e la società.



I robot si suicidano?

Bagaglio sempre incluso
Da 42€ solo andata

ITA
AIRWAYS

Robot si «suicida» in Corea del Sud: stress da superlavoro o semplice guasto?

di Eugenio Spagnuolo

Nella città di Gumi si indaga sulla strana «morte» di un robot impiegato dal Comune per avere a che fare con il pubblico. Le modalità dell'incidente ricordano un atto di autolesionismo. In attesa di capire quanto accaduto, non verrà sostituito. Ma l'avanzata nel Paese degli automi non si ferma



CORRIERE TV

BARBARA BONCHI

E CON CLAUDIO SANTAMARIA NEL MONDO DI PIETRO

Salta a 21

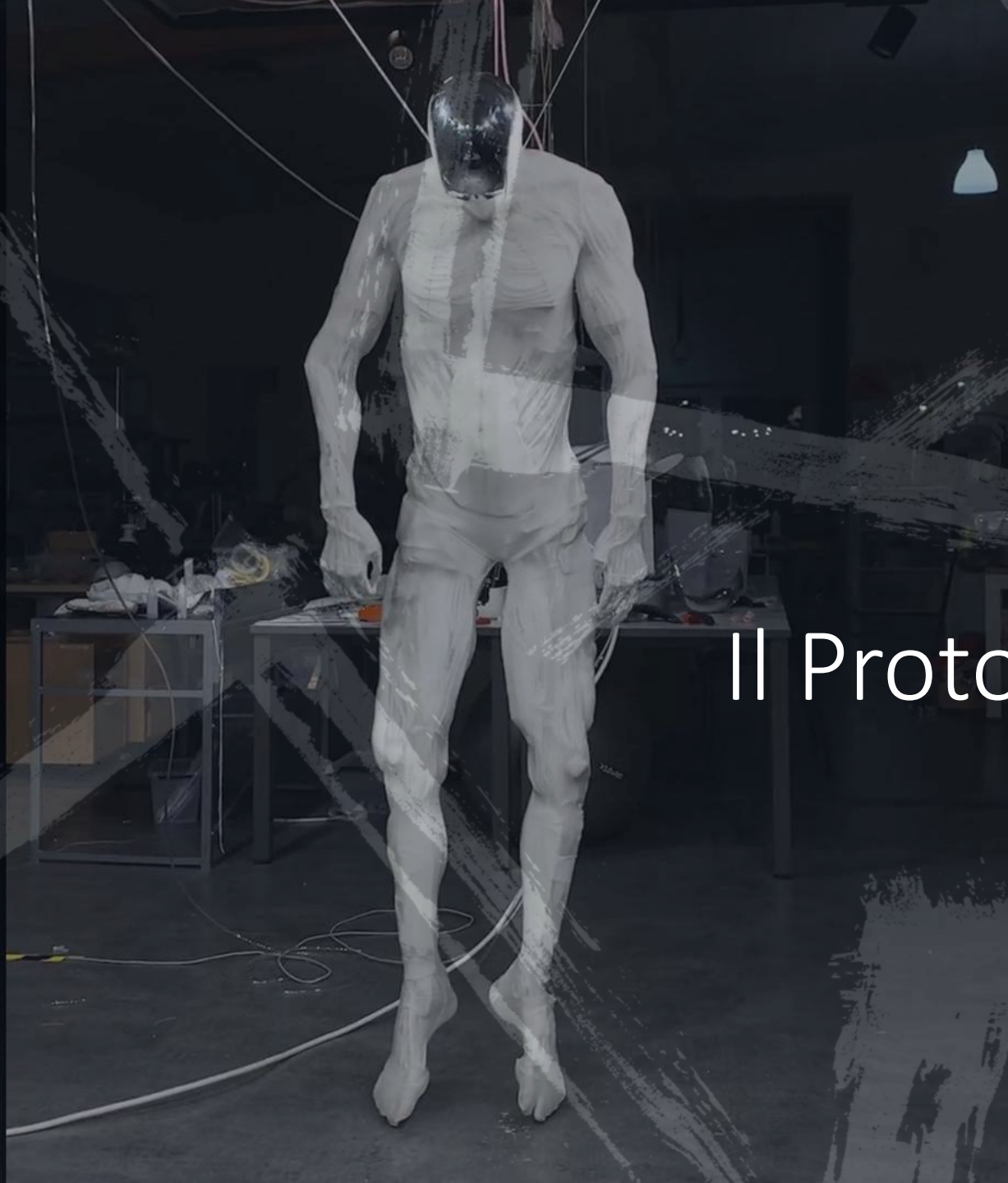
Publicità

ORA AL CINEMA

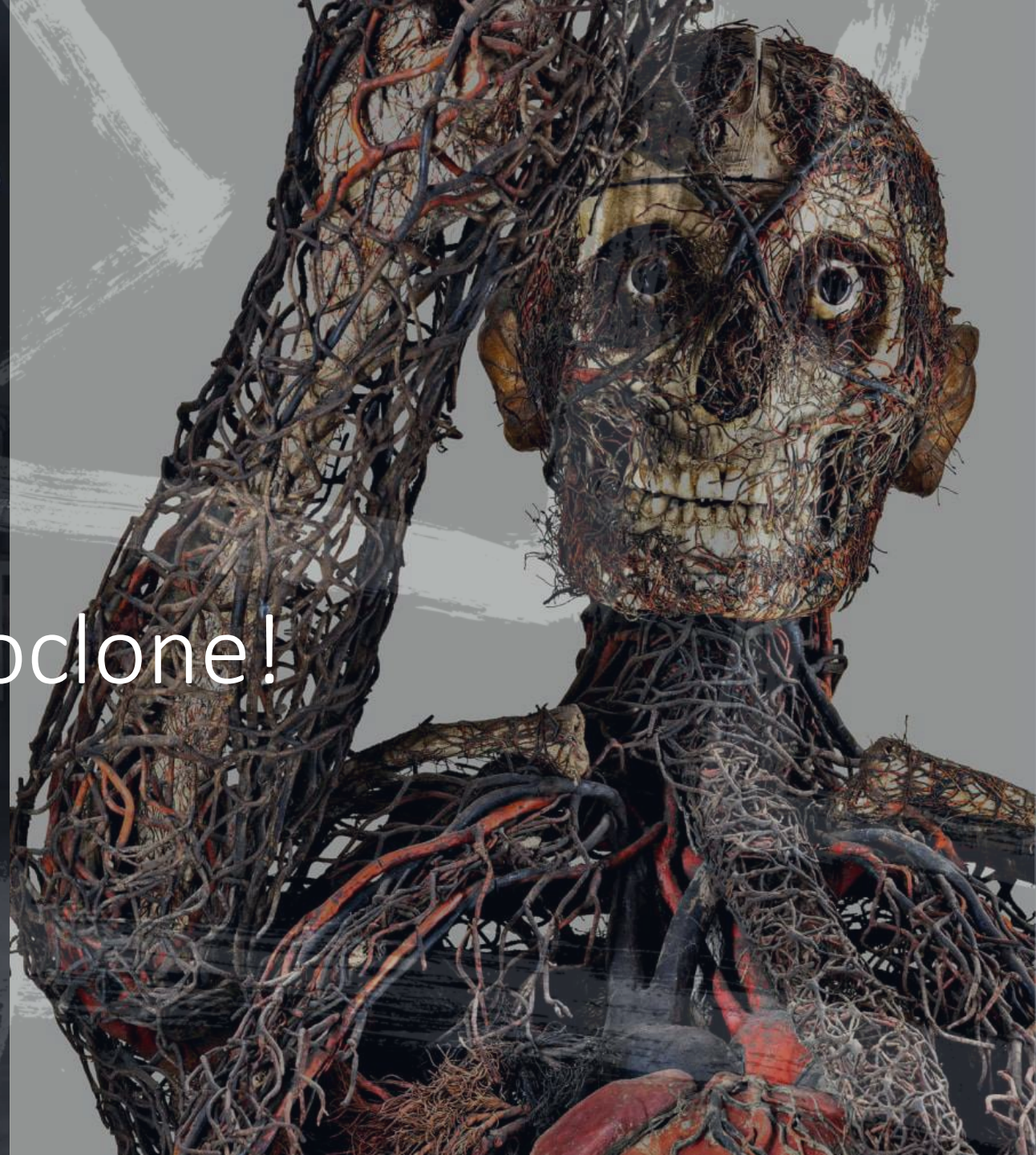
L'intelligenza artificiale ci ha fatto parlare in coreano al ristorante

Qui è ora

Qui è dove conoscere significa confrontarsi con le sfide della contemporaneità, ascoltare le nuove generazioni da accogliere nel tempo presente. Ora.



Il Protocolone!



Scenari distopici

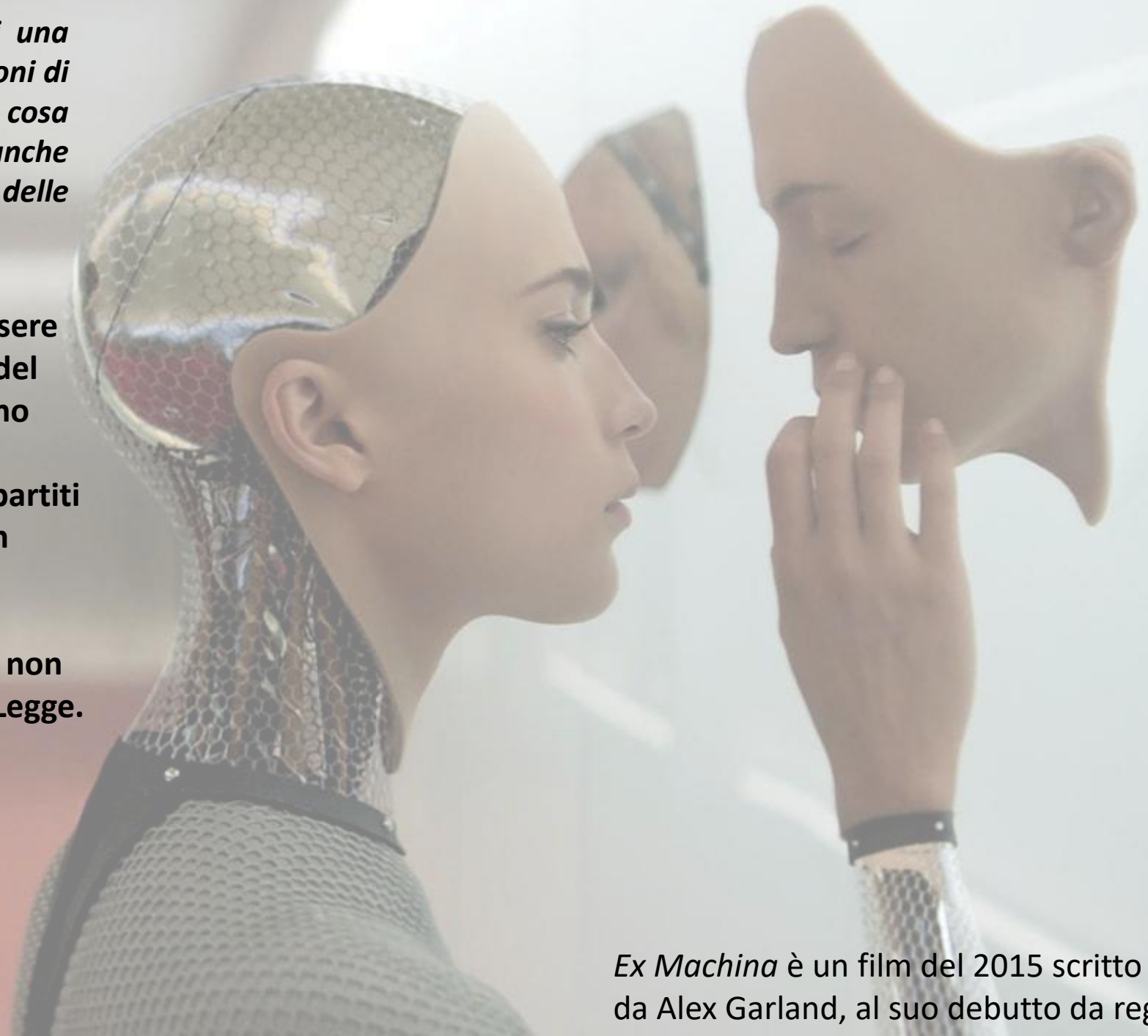


Scenari possibili?

CODEx

Siamo ancora lontani dallo sviluppo di una vera coscienza artificiale, ma le suggestioni di certi film aiutano a comprendere cosa potrebbe succedere se ciò accadesse, anche semplicemente ricordandoci il contenuto delle tre leggi della Robotica di Asimov:

- 1. Un robot non può recar danno a un essere umano né può permettere che, a causa del suo mancato intervento, un essere umano riceva danno.**
- 2. Un robot deve obbedire agli ordini impartiti dagli esseri umani, purché tali ordini non vadano in contrasto alla Prima Legge.**
- 3. Un robot deve proteggere la propria esistenza, purché la salvaguardia di essa non contrasti con la Prima o con la Seconda Legge.**



Ex Machina è un film del 2015 scritto e diretto da Alex Garland, al suo debutto da regista



Scenari attuali

180 113 13 144

Ti amo

Tutto chiaro?



Dug,
Film Walt Disney,
Up, 2009

Etica dell'IA?

Etica dell'IA?

INTELLIGENZA ARTIFICIALE

L'AI candidata sindaca a Taranto: D'Amico è un test per la politica partecipativa

Home > Cultura E Società Digitali

f in X M C A

Anna Luce D'Amico è un progetto politico basato sull'AI e sulla politica partecipativa. Nato a Taranto, potrebbe rappresentare un modello innovativo per altre città italiane. Il suo programma si basa su dati, trasparenza e coinvolgimento dei cittadini

Pubblicato il 31 mar 2025

Andrea Santoro

fondatore di Santoro Comunicare

Pierluca Tagariello

direttore della Comunicazione Istituzionale di Roma Capitale



Una definizione di IA

Art. 2.

(Definizioni)

1. Ai fini della presente legge, si intendono per:

a) sistema di intelligenza artificiale: un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'*input* che riceve come generare *output* quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali;

Intelligenza artificiale

Usi quotidiani e usi possibili

Alcuni esempi di come viene usata l'IA e delle possibilità che offre



europarl.eu

Fonte:

<https://www.europarl.europa.eu/news/it/headlines/society/20200827STO85804/che-cos-e-l-intelligenza-artificiale-e-come-viene-usata>

VERBA VOLANT

SCRIPTA MANENT

BIG DATA



VOLUME

DATA SIZE



VELOCITY

SPEED OF CHANGE



VARIETY

DIFFERENT FORMS
OF DATA SOURCES



VERACITY

UNCERTAINTY OF
DATA



Troppe informazioni
disinformano

Qualunque frase priva di fonti bibliografiche
certe, su internet la potrete trovare
attribuita per il 99% a:
Oscar Wilde, Jim Morrison o Albert Einstein
...e per il restante 1%
a un altro autore sbagliato!

FONTE:

<https://ricerca.repubblica.it/repubblica/archivio/repubblica/2013/01/20/aforismiit-per-smascherare-truffatori-di-frasi-celebri.html>

Il dato (personale e non personale) come merce preziosa:
dato anche quale strumento di analisi, previsione e
influenzamento del comportamento di un individuo.



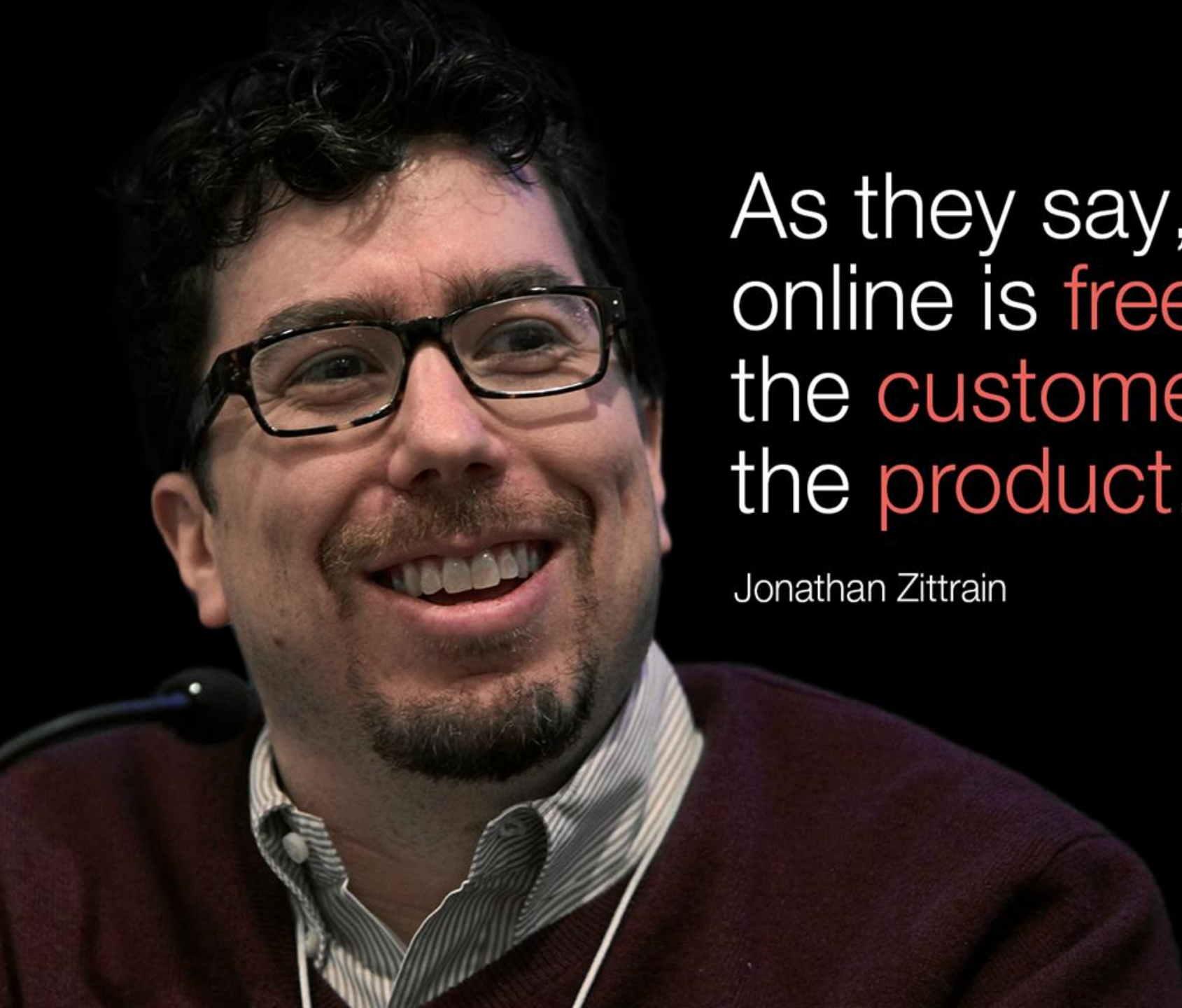
Dati

Informazioni

Profilazione

Manipolazione

*Money, it's a crime
Share it fairly but don't take a slice of my pie
(Money, The dark side of the moon, Pink Floyd)*



As they say, if something
online is **free**, you're not
the **customer** – you're
the **product**.

Jonathan Zittrain

WORLD
ECONOMIC
FORUM





Alla cerimonia d'insediamento del nuovo presidente presenti i tre uomini più ricchi al mondo, nonostante gli screzi del passato

Alla *rotunda* di Capitol Hill, a Washington, i tre uomini più ricchi del mondo si mimetizzano in giacca e cravatta nella folla presente alla cerimonia di insediamento di Donald Trump, 47esimo presidente degli Stati Uniti. A partire da Elon Musk, con una ricchezza stimata è di 433.9 miliardi di dollari, braccio destro del tycoon durante l'ultima campagna elettorale. Un sostegno che gli è valso frequenti comparsate sui palchi della campagna elettorale Usa al fianco del futuro presidente, con *standing ovation* annessa, e la nomina a capo del nuovo dipartimento dell'Efficienza governativa (Doge). Insieme a lui non passano di certo inosservati Mark Zuckerberg e Jeff Bezos.

| Tra big tech e amministratori delegati

Tra gli spettatori della cerimonia al Campidoglio non mancano i rappresentanti e gli amministratori delle principali big tech mondiali. Da OpenAi con Sam Altman a Apple, con il ceo Tim Cook. Passando per Sundar Pichai, amministratore delegato di Alphabet. Ma i miliardari non sono certo finiti: Miriam Adleson, Tilman Fertitta e Todd Ricketts gestiscono un patrimonio di oltre 50 miliardi di dollari. A cui si aggiunge Brian Armstrong, guru della crypto. La seconda amministrazione Trump prende così il via sotto l'egida di miliardi di dollari e di alcuni tra gli uomini più potenti del mondo. Cosa succederà di questi sodalizi, poi, è ancora tutto da vedere.

I Sultani alla Corte di Trump

L'attuale ecosistema digitale si fonda sullo sfruttamento intensivo ed indiscriminato delle informazioni e dei dati personali. Nel corso di poco più di un decennio, la struttura dei mercati è andata convergendo verso situazioni di quasi-monopolio, decretando l'accrescimento esponenziale del potere di mercato di pochi, ma potentissimi, attori privati. Il risultato è la concentrazione del potere di controllo dei flussi d'informazione nelle mani dei giganti del tech, circostanza che facilita il consolidamento di un modello di business basato sulla profilazione e finanche manipolazione delle persone.

Si rende a tal proposito necessario un ripensamento strutturale del modello di business prevalente. Si impone, inoltre, un intervento coordinato delle autorità della protezione dei dati, della protezione dei consumatori e della concorrenza, che tenga conto delle sinergie e sfide comuni alle diverse aree di regolazione.

A portrait of Giovanni Buttarelli, a middle-aged man with grey hair, wearing a dark suit, white shirt, and patterned tie. He is looking slightly to the right with a serious expression. The background is dark with various colorful icons (red, yellow, orange) representing digital concepts like a play button, a shield, a document, and a film strip.

Giovanni Buttarelli

NORMATIVA IN MATERIA L'EUROPA... e L'ITALIA: la fiducia nel mercato digitale

DIGITALIZZAZIONE E PRIVACY

Non c'è digitalizzazione senza protezione dei dati personali

Regolamento EIDAS 910/2014

Codice dell'amministrazione digitale

Regole tecniche (Linee Guida AgID)

Regolamento GDPR 679/2016

Codice protezione dati personali

Linee Guida

NORMATIVA IN MATERIA L'EUROPA... e L'ITALIA: le regole per gli operatori di servizi essenziali

SERVIZI, MERCATI E GOVERNANCE DIGITALI Non c'è digitalizzazione senza regole

Digital Services Act (DSA)
Regolamento (UE) 2022/2065 del 19/10/2022

relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (*regole stringenti per piattaforme e motori di ricerca di grandi dimensioni – oltre 45 milioni di utenti attivi*)

Digital Markets Act (DMA)
Regolamento (UE) 2022 / 1925 del 14/09/2022

relativo mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali) – *regole per i gatekeeper*

Data Governance Act (DGA)
Regolamento (UE) 2022/868

relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724 (Regolamento sulla governance dei dati) – *riutilizzo di dati protetti detenuti da enti pubblici*

NORMATIVA IN MATERIA L'EUROPA: le regole per gli operatori di servizi essenziali

Cybersecurity Act
Regolamento (UE) 2019/881
relativo all'ENISA, l'Agenzia dell'Unione europea per la ciber sicurezza, e alla certificazione della ciber sicurezza per le tecnologie dell'informazione e della comunicazione

Cyber Resilience Act (CRA)
Regolamento (UE) 2024/2847
relativo all'adozione di un sistema europeo comune di certificazione della cybersecurity basato sui Common Criteria

Security e Data Protection Non c'è digitalizzazione senza sicurezza

NIS 1- Direttiva (UE) 2016/1148
recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione

DECRETO LEGISLATIVO 18 maggio 2018, n. 65
Attuazione della direttiva (UE) 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione

NIS 2 - Direttiva (UE) 2022/2555
relativa a misure per un livello comune elevato di cybersecurity nell'Unione

DECRETO LEGISLATIVO 4 settembre 2024, n. 138
Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di ciber sicurezza nell'Unione

Digital Operational Resilience for the financial sector and amending Regulations (DORA)
Regolamento (EU) 2022/2554 del 14 dicembre 2022

relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE)

DIRETTIVA (UE) 2022/2557 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO
del 14 dicembre 2022 su resilienza dei soggetti critici

DECRETO LEGISLATIVO 4 settembre 2024, n. 134
Attuazione della direttiva (UE) 2022/2557, relativa alla resilienza dei soggetti critici (e che abroga la direttiva 2008/114/CE del Consiglio)

NORMATIVA IN MATERIA L'EUROPA... e L'ITALIA: le regole per gli operatori di servizi essenziali

Accessibilità dei servizi informatici Non c'è digitalizzazione senza accessibility

Per accessibilità si intende la capacità dei sistemi informatici di erogare servizi e fornire informazioni fruibili, senza discriminazioni, anche da parte di coloro che a causa di disabilità necessitano di tecnologie assistive o configurazioni particolari

Direttiva(UE) 2016/2102
relativa all'accessibilità dei siti web e delle applicazioni
mobili degli enti pubblici

LEGGE 9 gennaio 2004, n. 4 (modificata dal DL 76/2020)
*Disposizioni per favorire e semplificare l'accesso degli
utenti e, in particolare, delle persone con disabilità' agli
strumenti informatici*

Determinazione AgID n. 353/2022
di adozione della Circolare n. 3 del 20 Dicembre 2022

*fornisce specifici criteri per una corretta applicazione della
normativa sull'accessibilità dei servizi informatici anche per
le grandi aziende private*

DIRETTIVA (UE) 2019/882
sui requisiti di accessibilità dei prodotti e dei servizi

DECRETO LEGISLATIVO 27 maggio 2022, n. 82
*Attuazione della direttiva (UE) 2019/882 del 17 aprile 2019 sui
requisiti di accessibilita' dei prodotti e dei servi*

Bruxelles, 26.1.2022
COM(2022) 28 final

Dichiarazione europea
sui diritti e i principi digitali per il decennio digitale

2025/327

5.3.2025

REGULATION (EU) 2025/327 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 11 February 2025

on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Articles 16 and 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

[Pagina iniziale](#) > [Stampa](#) > [Comunicati stampa](#)

● Consiglio dell'UE Comunicato stampa 27 giugno 2023 23:47

Normativa sui dati: il Consiglio e il Parlamento raggiungono un accordo sull'accesso equo ai dati e sul loro utilizzo

Nell'ottica di fare dell'UE un leader nella nostra società basata sui dati, la presidenza del Consiglio e i rappresentanti del Parlamento europeo hanno raggiunto un accordo provvisorio su un nuovo regolamento riguardante norme armonizzate **sull'accesso equo ai dati e sul loro utilizzo** (normativa sui dati).



L'accordo odierno accelererà la trasformazione digitale della nostra Unione. Una volta entrata in vigore, la normativa sui dati sbloccherà il potenziale economico e sociale dei dati e delle tecnologie e contribuirà alla creazione di un mercato interno dei dati. Rafforzerà il mercato unico, consentendo la libera circolazione dei dati all'interno dell'UE e tra i vari settori, a beneficio dei nostri cittadini e delle nostre imprese.

— Erik Slottner, ministro svedese della Pubblica amministrazione

Regolamento UE 2023/2854 riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo (Data Act)

Diritto.it

PORTALE GIURIDICO
CON LA PIÙ RECENTE
GIURISPRUDENZA
NETWORK MAGGIOLI EDITOR

Aree tematiche ▾

Giurisprudenza commentata

La Pratica Forense ▾

Prodotti Gratuiti ▾



In evidenza:

Riforma giustizia

Esame Avvocato

Nuovo Codice dei Contratti pubblici

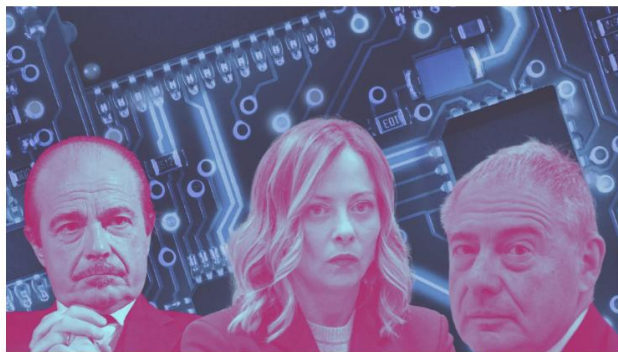
Home > [AI&Legaltech](#) > [AI Act: il regolamento europeo 1689/2024 in Gazzetta Ufficiale](#)

[AI&LEGALTECH](#)

AI Act: il regolamento europeo 1689/2024 in Gazzetta Ufficiale

Cosa ha deciso il governo sull'intelligenza artificiale

Nel disegno di legge sull'AI c'è l'impegno a spendere fino a un miliardo per progetti di startup. Poi i reati per deepfake, i piani di formazione e la ricerca sanitaria. Sparisce la fondazione



Da sinistra: Antonio Padellaro, sottosegretario all'Intelligenza Artificiale; Elena Basso, ministro della Sanità; e Antonio Di Lorenzo, ministro della Giustizia. Sotto: il disegno di legge sull'Intelligenza Artificiale. A destra: il ministro della Sanità, Antonio Di Lorenzo

GDPR | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI



Decalogo per la realizzazione di servizi sanitari nazionali attraverso sistemi di Intelligenza Artificiale



EDPS - European Data Protection Supervisor -
Orientamenti sull'IA generativa: Cogliere le opportunità,
proteggere le persone

EDPS ha pubblicato i suoi orientamenti sull'intelligenza artificiale generativa e sui dati personali per le istituzioni, gli organi e gli organismi dell'UE (IUE). Gli orientamenti mirano ad aiutare gli IUE a rispettare gli obblighi in materia di protezione dei dati di cui al regolamento (UE) 2018/1725 quando utilizzano o sviluppano strumenti di IA generativa.



Siete qui: [Portal](#) > [Tutte le notizie](#) > [Il Consiglio d'Europa adotta il primo trattato internazionale sull'intelligenza artificiale](#)



Sala stampa

Il Consiglio d'Europa adotta il primo trattato internazionale sull'intelligenza artificiale

Deutsch

English

Español

Français

Русский

COMITATO DEI MINISTRI | STRASBURGO | 17 MAGGIO 2024



*È utile
questa
ipertrofia
normativa?*

«migliorare il funzionamento del mercato interno e promuovere la diffusione di un'intelligenza artificiale (IA) antropocentrica e affidabile, garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione Europea, compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, contro gli effetti nocivi dei sistemi di IA nell'Unione e di promuovere l'innovazione»

AI Act – art. 1 par. 1



Carta dei diritti fondamentali dell'Unione europea

SINTESI DI:

[Carta dei diritti fondamentali dell'Unione europea](#)

QUAL È L'OBIETTIVO DELLA CARTA?

La Carta dei diritti fondamentali dell'Unione europea (la Carta) tutela i **diritti fondamentali** di cui godono le persone nell'**Unione europea** (Unione). Si tratta di uno strumento moderno e completo del **diritto dell'Unione** che tutela e promuove i diritti e le libertà delle persone di fronte ai cambiamenti nella società, al progresso sociale e agli sviluppi scientifici e tecnologici.

PUNTI CHIAVE

Contenuto

La Carta riafferma, nel pieno rispetto dei poteri e delle funzioni dell'Unione e del principio della **sussidiarietà**, i diritti stabiliti basati sulla tradizioni costituzionali e dagli obblighi internazionali comuni degli **Stati membri**, che comprendono la **Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali**, le Carte sociali adottate dall'Unione e dal **Consiglio d'Europa** e la giurisprudenza della **Corte di giustizia dell'Unione europea** e della **Corte europea dei diritti dell'uomo**. Grazie alla visibilità e alla chiarezza che la Carta conferisce ai diritti fondamentali, essa contribuisce a creare la **certezza del diritto** nell'Unione.

La Carta comprende un preambolo introduttivo e 54 articoli, suddivisi in sette capi:

- Capo I: **dignità** (dignità umana, diritto alla vita, diritto all'integrità della persona, proibizione della tortura e delle pene o trattamenti inumani o degradanti, proibizione della schiavitù e del lavoro forzato).
- Capo II: **libertà** (diritto alla libertà e alla sicurezza, rispetto della vita privata e della vita familiare, **protezione dei dati di carattere personale**, diritto di sposarsi e di costituire una famiglia, libertà di pensiero, di coscienza e di religione, libertà di espressione e d'informazione, libertà di riunione e di associazione, libertà delle arti e delle scienze, diritto all'istruzione, libertà professionale e diritto di lavorare, libertà d'impresa, diritto di proprietà, diritto di asilo, protezione in caso di allontanamento, di espulsione e di estradizione).
- Capo III: **uguaglianza** (uguaglianza davanti alla legge, **non discriminazione**, diversità culturale, religiose e linguistica, **parità tra uomini e donne**, **diritti del bambino**, **diritti degli anziani**, **inserimento dei disabili**).
- Capo IV: **solidarietà** (**diritto dei lavoratori all'informazione e alla consultazione nell'ambito dell'impresa**, diritto di negoziazione e di azioni collettive, diritto di accesso ai servizi di collocamento, tutela in caso di licenziamento ingiustificato, condizioni di lavoro giuste ed eque, divieto del lavoro minorile e **protezione dei giovani sul luogo di lavoro**, **vita familiare e vita professionale**, sicurezza sociale e assistenza sociale, protezione della salute, accesso ai **servizi d'interesse economico generale**, tutela dell'ambiente, **protezione dei consumatori**).
- Capo V: **cittadinanza** (diritto di voto e di eleggibilità alle **elezioni del Parlamento europeo** e alle **elezioni comunali**, diritto a una buona amministrazione, **diritto d'accesso ai documenti**, Mediatore europeo, diritto di petizione, libertà di circolazione e di soggiorno, tutela diplomatica e consolare);
- Capo VI: **giustizia** (diritto a un ricorso effettivo e a un giudice imparziale, **presunzione di innocenza e diritti della difesa**, principi della legalità e della proporzionalità dei reati e delle pene, diritto di non essere giudicato o punito due volte per lo stesso reato).
- Capo VII: **disposizioni generali**.



<https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A12016P%2FTXT>

Articolo 1

Dignità umana

La dignità umana è inviolabile. Essa deve essere rispettata e tutelata.

Articolo 3

Diritto all'integrità della persona

1. Ogni persona ha diritto alla propria integrità fisica e psichica.

Articolo 6

Diritto alla libertà e alla sicurezza

Ogni persona ha diritto alla libertà e alla sicurezza.

Articolo 7

Rispetto della vita privata e della vita familiare

Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni.



Articolo 8

Protezione dei dati di carattere personale

1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.
2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica.
3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.

Articolo 11

Libertà di espressione e d'informazione

1. Ogni persona ha diritto alla libertà di espressione. Tale diritto include la libertà di opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limiti di frontiera.
2. La libertà dei media e il loro pluralismo sono rispettati.

Articolo 16

Libertà d'impresa

È riconosciuta la libertà d'impresa, conformemente al diritto dell'Unione e alle legislazioni e prassi nazionali.

Articolo 21

Non discriminazione

1. È vietata qualsiasi forma di discriminazione fondata, in particolare, sul sesso, la razza, il colore della pelle o l'origine etnica o sociale, le caratteristiche genetiche, la lingua, la religione o le convinzioni personali, le opinioni politiche o di qualsiasi altra natura, l'appartenenza ad una minoranza nazionale, il patrimonio, la nascita, la disabilità, l'età o l'orientamento sessuale.
2. Nell'ambito d'applicazione dei trattati e fatte salve disposizioni specifiche in essi contenute, è vietata qualsiasi discriminazione in base alla nazionalità.



Tutte le più recenti normative europee in materia di scenari digitali ruotano intorno ai seguenti principi fondamentali:

- **libera circolazione, portabilità e protezione dei dati** (personali e non personali);
- **trasparenza** (non solo informativa su basi giuridiche, finalità, ruoli e diritti delle parti deboli coinvolte nei processi digitali, ma anche trasparenza degli algoritmi);
- **non esclusività** della decisione algoritmica e **non discriminazione** algoritmica;
- **accountability**, quindi, definizione di ruoli e responsabilità, di modelli organizzativi e procedure;
- **integrità** e, quindi, **affidabilità** dei dati;
- **sicurezza** e, quindi, **gestione del rischio**;
- **interoperabilità** di sistemi informatici, database e archivi digitali;
- **accessibilità** e **sostenibilità**.

PARLAMENTO EUROPEO

CONSIGLIO

COMMISSIONE EUROPEA



Dichiarazione europea sui diritti e i principi digitali per il decennio digitale

(2023/C 23/01)

Il Parlamento europeo, il Consiglio e la Commissione proclamano solennemente la seguente dichiarazione comune sui diritti e i principi digitali per il decennio digitale.

Preambolo

Considerando quanto segue:

- (1) L'Unione europea (UE) è un'«unione di valori», sancita dall'articolo 2 del trattato sull'Unione europea, e si fonda sul rispetto della dignità umana, della libertà, della democrazia, dell'uguaglianza, dello Stato di diritto e sul rispetto dei diritti umani, compresi i diritti delle persone appartenenti a minoranze. Inoltre, secondo la Carta dei diritti fondamentali dell'Unione europea, l'UE si fonda sui valori indivisibili e universali della dignità umana, della libertà, dell'uguaglianza e della solidarietà. La Carta ribadisce inoltre i diritti derivanti in particolare dagli obblighi internazionali comuni agli Stati membri.
- (2) La trasformazione digitale interessa ogni aspetto della vita delle persone. Offre notevoli opportunità in termini di miglioramento della qualità della vita, crescita economica e sostenibilità.
- (3) La trasformazione digitale presenta anche sfide per le nostre società democratiche e le nostre economie, così come per gli individui. Con l'accelerazione della trasformazione digitale è giunto il momento che l'UE specifichi come si dovrebbero applicare nell'ambiente digitale i suoi valori e diritti fondamentali applicabili offline. La trasformazione digitale non dovrebbe comportare la regressione dei diritti. Ciò che è illegale offline è illegale online. La presente dichiarazione non pregiudica le «politiche offline», come l'accesso offline ai servizi pubblici principali.
- (4) Il Parlamento ha invitato più volte a definire principi etici che guidino l'approccio dell'UE alla trasformazione digitale e garantiscano il pieno rispetto dei diritti fondamentali quali la protezione dei dati, il diritto al rispetto della vita privata, la non discriminazione e la parità di genere, nonché di principi quali la protezione dei consumatori, la neutralità tecnologica e della rete, l'affidabilità e l'inclusività. Ha inoltre chiesto una maggiore protezione dei diritti degli utenti nell'ambiente digitale, nonché dei diritti dei lavoratori e del diritto alla disconnessione ⁽¹⁾.

Dichiarazione sui diritti e i principi digitali per il decennio digitale

Il nostro obiettivo è di promuovere un modello europeo per la trasformazione digitale, che metta al centro le persone, sia basato sui valori europei e sui diritti fondamentali dell'UE, riaffermi i diritti umani universali e apporti benefici a tutte le persone, alle imprese e alla società nel suo complesso.

Dichiariamo pertanto quanto segue:



CAPITOLO I

Mettere le persone al centro della trasformazione digitale

1. Le persone sono al centro della trasformazione digitale nell'Unione europea. La tecnologia dovrebbe essere al servizio e andare a beneficio di tutte le persone che vivono nell'UE, mettendole nelle condizioni di perseguire le loro aspirazioni, in tutta sicurezza e nel pieno rispetto dei loro diritti fondamentali.

Ci impegniamo a:

- a) rafforzare il quadro democratico per una trasformazione digitale che vada a beneficio di ogni persona e migliori la vita tutte le persone che vivono nell'UE;
- b) adottare le misure necessarie per garantire che i valori dell'UE e i diritti delle persone riconosciuti dal diritto dell'Unione siano rispettati online così come offline;
- c) promuovere e garantire un'azione responsabile e diligente da parte di tutti gli attori, pubblici e privati, nell'ambiente digitale;
- d) promuovere attivamente questa visione della trasformazione digitale, anche nelle relazioni internazionali.

Solidarietà e inclusione

2. La tecnologia dovrebbe essere utilizzata per unire le persone, e non per dividerle. La trasformazione digitale dovrebbe contribuire a una società e a un'economia eque e inclusive nell'UE.

Ci impegniamo a:

- a) garantire che la progettazione, lo sviluppo, la diffusione e l'utilizzo di soluzioni tecnologiche rispettino i diritti fondamentali, consentano l'esercizio di tali diritti e promuovano la solidarietà e l'inclusione;
- b) perseguire una trasformazione digitale che non lasci indietro nessuno. Essa dovrebbe andare a beneficio di tutti, realizzare la parità di genere e includere in particolare gli anziani, le persone che vivono nelle zone rurali, le persone con disabilità, le persone emarginate, vulnerabili o prive di diritti, così come coloro che agiscono per loro conto, e dovrebbe inoltre promuovere la diversità culturale e linguistica;
- c) sviluppare quadri adeguati affinché tutti gli operatori del mercato che traggono vantaggio dalla trasformazione digitale si assumano le proprie responsabilità sociali e contribuiscano in modo equo e proporzionato ai costi delle infrastrutture, dei servizi e dei beni pubblici, a beneficio di tutte le persone che vivono nell'UE.



Connettività

3. Ogni persona, ovunque nell'UE, dovrebbe avere accesso alla connettività digitale ad alta velocità a prezzi accessibili.

Ci impegniamo a:

- a) garantire l'accesso a una connettività di elevata qualità, con la disponibilità di un accesso a internet, per tutte le persone, ovunque nell'UE, comprese le persone a basso reddito;
- b) proteggere e promuovere un'internet neutra e aperta in cui le applicazioni, i servizi e i contenuti non siano bloccati o degradati in modo ingiustificato.



Istruzione, formazione e competenze digitali

4. Ogni persona ha diritto all'istruzione, alla formazione e all'apprendimento permanente e dovrebbe poter acquisire tutte le competenze digitali di base e avanzate.

Ci impegniamo a:

- a) promuovere un'istruzione e una formazione digitali di elevata qualità, anche al fine di colmare il divario digitale di genere;
- b) sostenere gli sforzi intesi a consentire a tutti i discenti e gli insegnanti di acquisire e condividere le capacità e le competenze digitali necessarie, tra cui l'alfabetizzazione mediatica e il pensiero critico, per partecipare attivamente all'economia, alla società e ai processi democratici;
- c) promuovere e sostenere gli sforzi volti a dotare tutti gli istituti di istruzione e formazione di connettività, infrastrutture e strumenti digitali;
- d) dare a ogni persona la possibilità di adattarsi ai cambiamenti introdotti dalla digitalizzazione del lavoro attraverso il miglioramento delle competenze e la riqualificazione professionale.

Condizioni di lavoro giuste ed eque

5. Ogni persona ha diritto a condizioni di lavoro eque, giuste, sane e sicure e a una protezione adeguata nell'ambiente digitale come nel luogo di lavoro fisico, indipendentemente dalla sua situazione occupazionale, dalle modalità o dalla durata dell'occupazione.
6. I sindacati e le organizzazioni di datori di lavoro svolgono un ruolo importante nella trasformazione digitale, in particolare in relazione alla definizione di condizioni di lavoro giuste ed eque, anche per quanto riguarda l'utilizzo degli strumenti digitali sul luogo di lavoro.

Ci impegniamo a:

- a) garantire che tutte le persone abbiano la possibilità di disconnettersi e godano di garanzie per l'equilibrio tra vita professionale e vita privata in un ambiente digitale;
- b) garantire che, nell'ambiente di lavoro, gli strumenti digitali non mettano in alcun modo a rischio la salute fisica e mentale dei lavoratori;
- c) garantire il rispetto dei diritti fondamentali dei lavoratori nell'ambiente digitale, compresi il diritto al rispetto della vita privata e il diritto di associazione, il diritto di contrattazione e azione collettiva, nonché la protezione dalla sorveglianza illecita e ingiustificata;
- d) garantire che l'utilizzo dell'intelligenza artificiale sul luogo di lavoro sia trasparente e segua un approccio basato sul rischio e che siano adottate le corrispondenti misure di prevenzione per mantenere un ambiente di lavoro sicuro e sano;
- e) provvedere in particolare affinché sia garantita la sorveglianza umana nelle decisioni importanti che interessano i lavoratori e questi ultimi siano, in generale, informati del fatto di stare interagendo con sistemi di intelligenza artificiale.





Servizi pubblici digitali online

7. Ogni persona dovrebbe avere accesso online ai servizi pubblici principali nell'UE. A nessuno deve essere chiesto di fornire dati più spesso di quanto necessario durante l'accesso ai servizi pubblici digitali e il loro utilizzo.

Ci impegniamo a:

- a) garantire che a tutte le persone che vivono nell'UE sia offerta la possibilità di utilizzare un'identità digitale accessibile, volontaria, sicura e affidabile, che dia accesso a un'ampia gamma di servizi online;
- b) garantire l'accessibilità e il riutilizzo su vasta scala delle informazioni della pubblica amministrazione;
- c) agevolare e sostenere in tutta l'UE un accesso fluido, sicuro e interoperabile a servizi pubblici digitali concepiti per soddisfare le esigenze delle persone in modo efficiente, compresi in particolare i servizi sanitari e assistenziali digitali, segnatamente l'accesso alle cartelle cliniche elettroniche.

CAPITOLO III

Libertà di scelta

Interazioni con algoritmi e sistemi di intelligenza artificiale

8. L'intelligenza artificiale dovrebbe fungere da strumento per le persone, con l'obiettivo ultimo di aumentare il benessere umano.
9. Ogni persona dovrebbe essere messa nelle condizioni di godere dei benefici offerti dai sistemi algoritmici e di intelligenza artificiale, anche compiendo le proprie scelte informate nell'ambiente digitale, e rimanendo al contempo protetta dai rischi e dai danni alla salute, alla sicurezza e ai diritti fondamentali.

Ci impegniamo a:

- a) promuovere sistemi di intelligenza artificiale antropocentrici, affidabili ed etici nell'intero corso del loro sviluppo, della loro diffusione e del loro utilizzo, in linea con i valori dell'UE;
- b) garantire un livello adeguato di trasparenza in merito all'uso degli algoritmi e dell'intelligenza artificiale e fare in modo che le persone siano autonome e responsabili quando li utilizzano e informate quando interagiscono con essi;
- c) garantire che i sistemi algoritmici siano basati su insiemi di dati adeguati al fine di evitare discriminazioni e consentano la supervisione umana di tutti i risultati che interessano la sicurezza e i diritti fondamentali delle persone;
- d) garantire che le tecnologie come l'intelligenza artificiale non siano utilizzate per pregiudicare le scelte delle persone, ad esempio per quanto riguarda la salute, l'istruzione, l'occupazione e la vita privata;
- e) prevedere garanzie e adottare misure adeguate, anche promuovendo norme affidabili, al fine di assicurare che, in ogni momento, l'intelligenza artificiale e i sistemi digitali siano sicuri e vengano utilizzati nel pieno rispetto dei diritti fondamentali;
- f) adottare misure per garantire che la ricerca sull'intelligenza artificiale rispetti i più elevati principi etici e il diritto pertinente dell'UE.





Un ambiente digitale equo

10. Ogni persona dovrebbe essere in grado di scegliere realmente e liberamente quali servizi online utilizzare, sulla base di informazioni obiettive, trasparenti, facilmente accessibili e affidabili.
11. Ogni persona dovrebbe avere la possibilità di competere lealmente e innovare nell'ambiente digitale. Tutto ciò dovrebbe apportare benefici anche alle imprese, comprese le PMI.

Ci impegniamo a:

- a) garantire un ambiente digitale sicuro e protetto, basato sulla concorrenza leale, in cui siano tutelati i diritti fondamentali, siano garantiti i diritti degli utenti e la protezione dei consumatori nel mercato unico digitale e siano ben definite le responsabilità delle piattaforme, in particolare dei grandi operatori e dei gatekeeper;
- b) promuovere l'interoperabilità, la trasparenza, le tecnologie aperte e gli standard aperti come modo per rafforzare ulteriormente la fiducia nella tecnologia e la capacità dei consumatori di compiere scelte autonome e informate.

Partecipazione allo spazio pubblico digitale

12. Ogni persona dovrebbe avere accesso a un ambiente digitale affidabile, diversificato e multilingue. L'accesso a contenuti diversificati contribuisce a un dibattito pubblico pluralistico e alla partecipazione effettiva alla democrazia in modo non discriminatorio.
13. Ogni persona ha diritto alla libertà di espressione e di informazione, nonché alla libertà di riunione e di associazione nell'ambiente digitale.
14. Ogni persona dovrebbe poter accedere alle informazioni su chi possiede e controlla i servizi mediatici che utilizza.
15. Le piattaforme online, in particolare le piattaforme online di dimensioni molto grandi, dovrebbero sostenere il libero dibattito democratico online. Visto il ruolo svolto dai loro servizi nel plasmare l'opinione pubblica e il dibattito pubblico, le piattaforme online di dimensioni molto grandi dovrebbero attenuare i rischi derivanti dal funzionamento e dall'uso dei loro servizi, anche in relazione alle campagne di disinformazione e cattiva informazione, e tutelare la libertà di espressione.



Ci impegniamo a:

- a) continuare a salvaguardare tutti i diritti fondamentali online, in particolare la libertà di espressione e di informazione, compresi la libertà e il pluralismo dei media;
- b) sostenere lo sviluppo e l'utilizzo ottimale delle tecnologie digitali per stimolare il coinvolgimento delle persone e la partecipazione democratica;
- c) adottare misure proporzionate volte a contrastare tutte le forme di contenuti illegali, nel pieno rispetto dei diritti fondamentali, compreso il diritto alla libertà di espressione e di informazione, senza imporre obblighi generali di sorveglianza o forme di censura;
- d) creare un ambiente digitale in cui le persone siano protette dalla disinformazione, dalla manipolazione delle informazioni e da altre forme di contenuti dannosi, comprese le molestie e la violenza di genere;
- e) sostenere l'accesso effettivo a contenuti digitali che rispecchino la diversità culturale e linguistica nell'UE;
- f) conferire alle persone maggiore autonomia e responsabilità affinché compiano scelte liberamente determinate e specifiche e limitare lo sfruttamento delle vulnerabilità e dei pregiudizi, in particolare attraverso la pubblicità mirata.

CAPITOLO V

Sicurezza, protezione e conferimento di maggiore autonomia e responsabilità

Un ambiente digitale sicuro, protetto e tutelato

16. Ogni persona dovrebbe avere accesso a tecnologie, prodotti e servizi digitali che siano sicuri e protetti e tutelino la vita privata fin dalla progettazione, traducendosi in un elevato livello di riservatezza, integrità, disponibilità e autenticità delle informazioni trattate.

Ci impegniamo a:

- a) adottare ulteriori misure per promuovere la tracciabilità dei prodotti e assicurare che nel mercato unico digitale siano offerti solo prodotti sicuri e conformi alla legislazione dell'UE;
- b) proteggere gli interessi delle persone, delle imprese e delle istituzioni pubbliche dai rischi di cibersicurezza e dalla criminalità informatica, anche per quanto riguarda le violazioni dei dati e i furti o le manipolazioni dell'identità, il che comprende requisiti di cibersicurezza per i prodotti connessi immessi sul mercato unico;
- c) contrastare coloro che cercano di compromettere, all'interno dell'UE, la sicurezza online e l'integrità dell'ambiente digitale o che promuovono la violenza e l'odio attraverso strumenti digitali, e chiamarli a rispondere delle loro azioni.



Vita privata e controllo individuale sui dati

17. Ogni persona ha diritto al rispetto della vita privata e alla protezione dei propri dati personali. Quest'ultimo diritto prevede anche che i singoli individui abbiano il controllo di come sono utilizzati i propri dati e con chi sono condivisi.
18. Ogni persona ha diritto alla riservatezza delle proprie comunicazioni e delle informazioni sui propri dispositivi elettronici e a non essere sottoposta a sorveglianza online illecita, tracciamento pervasivo illecito o misure di intercettazione.
19. Ogni persona dovrebbe essere in grado di determinare la propria eredità digitale e decidere cosa succede, dopo la sua morte, ai propri account personali e alle informazioni che la riguardano.

Ci impegniamo a:

- a) garantire che ogni persona abbia un controllo effettivo sui propri dati personali e non personali, in linea con le norme dell'UE in materia di protezione dei dati e il pertinente diritto dell'UE;
- b) garantire l'effettiva possibilità per i singoli individui di trasferire facilmente i propri dati personali e non personali tra diversi servizi digitali, in linea con i diritti di portabilità;
- c) proteggere efficacemente le comunicazioni dall'accesso non autorizzato di terzi;
- d) vietare l'identificazione illecita e la conservazione illecita delle registrazioni delle attività.



Protezione dei bambini e dei giovani e conferimento di maggiore autonomia e responsabilità nell'ambiente digitale

20. I bambini e i giovani dovrebbero essere messi nelle condizioni di compiere scelte sicure e informate e di esprimere la propria creatività nell'ambiente digitale.
21. Si dovrebbero migliorare le esperienze, il benessere e la partecipazione all'ambiente digitale dei bambini e dei giovani attraverso materiali e servizi adeguati all'età.
22. Occorre prestare particolare attenzione al diritto dei bambini e dei giovani di essere protetti da tutti i reati commessi attraverso le tecnologie digitali o facilitati da tali tecnologie.

Ci impegniamo a:

- a) offrire a tutti i bambini e i giovani opportunità per acquisire le necessarie capacità e competenze, tra cui l'alfabetizzazione mediatica e il pensiero critico, per navigare e interagire nell'ambiente digitale in modo attivo e sicuro e per compiere scelte informate;
- b) promuovere esperienze positive per i bambini e i giovani in un ambiente digitale sicuro e adeguato all'età;
- c) proteggere tutti i bambini e i giovani dai contenuti dannosi e illegali, dallo sfruttamento, dalla manipolazione e dagli abusi online e impedire che lo spazio digitale sia utilizzato per commettere o facilitare reati;
- d) proteggere tutti i bambini e i giovani dal tracciamento, dalla profilazione e dal targeting illegali, in particolare a fini commerciali;
- e) coinvolgere i bambini e i giovani nell'elaborazione delle politiche digitali che li riguardano.



CAPITOLO VI

Sostenibilità

23. Per evitare danni significativi all'ambiente, e al fine di promuovere l'economia circolare, i prodotti e i servizi digitali dovrebbero essere progettati, prodotti, utilizzati, riparati, riciclati e smaltiti in modo da attenuare il loro impatto negativo sull'ambiente e sulla società ed evitare l'obsolescenza prematura.
24. Ogni persona dovrebbe avere accesso a informazioni precise e di facile comprensione sull'impatto ambientale e sul consumo energetico dei prodotti e dei servizi digitali, nonché sulla loro riparabilità e sul loro ciclo di vita, in modo da essere in grado di compiere scelte responsabili.

Ci impegniamo a:

- a) favorire lo sviluppo e l'utilizzo di tecnologie digitali sostenibili che abbiano un impatto negativo minimo sulla società e sull'ambiente;
- b) incentivare scelte di consumo e modelli aziendali sostenibili e promuovere un comportamento sostenibile e responsabile delle imprese lungo tutte le catene globali del valore dei prodotti e dei servizi digitali, anche per contrastare il lavoro forzato;
- c) promuovere lo sviluppo, la diffusione e l'uso attivo di tecnologie digitali innovative con un impatto positivo sull'ambiente e sul clima, al fine di accelerare la transizione verde;
- d) promuovere norme e marchi di sostenibilità per i prodotti e i servizi digitali.



Il **presupposto** per avviare qualsiasi progetto di innovazione digitale, (a maggior ragione quando ci si avvalga di sistemi di intelligenza artificiale), deve essere la garanzia della **qualità dei dati** a disposizione. Quindi, occorre prestare massima attenzione alle normative italiane ed europee e agli strumenti (tecnici e archivistici) a tutela dell'integrità, del costante aggiornamento, della completezza, della consultabilità, della comprensibilità, dell'omogeneità, della facile accessibilità, della usabilità, della condivisibilità e della interoperabilità dei dati.

Data protection e data security
(by design e by default)





PATIENT FILES

Per garantire la **protezione dei dati sanitari** in qualsiasi sistema digitale è indispensabile la predisposizione di sistemi di gestione documentale con i quali – attraverso l’adozione di appropriate misure organizzative e tecnologiche – individuare i documenti che nel corso dello svolgimento dell’attività lavorativa devono essere via via archiviati con modalità idonee a garantire le caratteristiche di **autenticità, integrità, affidabilità, leggibilità e reperibilità** prescritte dalla disciplina di settore applicabile

(Cfr. Provv. Garante privacy n. 353/2021, Solera)

La fiducia nel mercato digitale...



Regolamento eIDAS (electronic IDentification Authentication and Signature): Regolamento (UE) N. 910/2014 del PARLAMENTO EUROPEO e del CONSIGLIO del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE

Regolamento GDPR (General Data Protection Regulation): Regolamento (UE) N. 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

I principi ispiratori dei due Regolamenti

Regolamento eIDAS:

(1) Instaurare la **fiducia negli ambienti online** è fondamentale per lo sviluppo economico e sociale. La mancanza di fiducia, dovuta in particolare a una percepita assenza di certezza giuridica, scoraggia i consumatori, le imprese e le autorità pubbliche dall'effettuare transazioni per via elettronica e dall'adottare nuovi servizi.

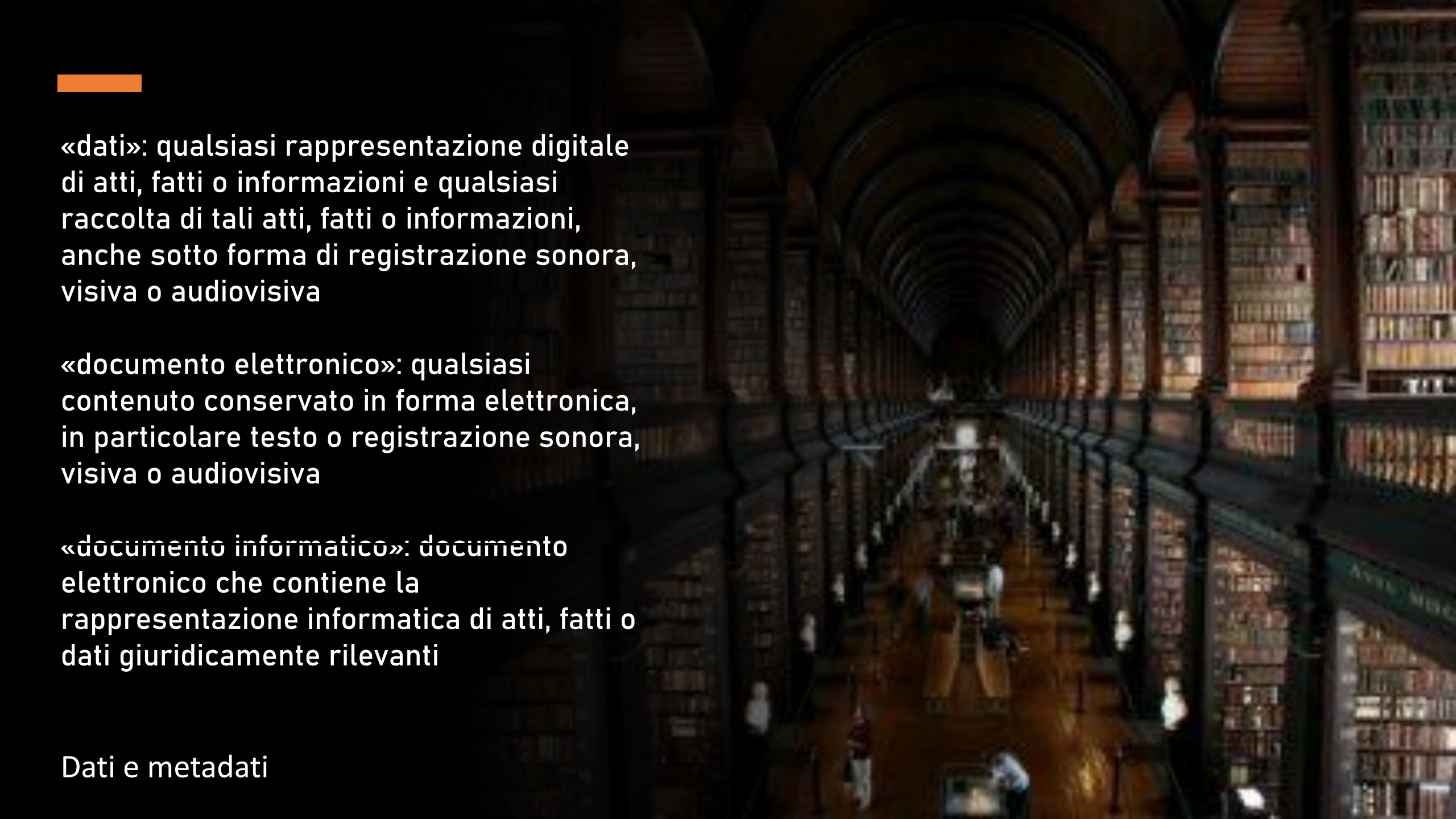
(2) Il presente regolamento mira a rafforzare la fiducia nelle transazioni elettroniche nel mercato interno fornendo una base comune per interazioni elettroniche sicure fra cittadini, imprese e autorità pubbliche, in modo da migliorare l'efficacia dei servizi elettronici pubblici e privati, nonché dell'eBusiness e del commercio elettronico, nell'Unione europea.

Regolamento GDPR:

(1) La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale. L'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.

(6) La rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. La portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano. La tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali.

(7) Tale evoluzione richiede un quadro più solido e coerente in materia di protezione dei dati nell'Unione, affiancato da efficaci misure di attuazione, data l'importanza di creare il **clima di fiducia che consentirà lo sviluppo dell'economia digitale** in tutto il mercato interno.

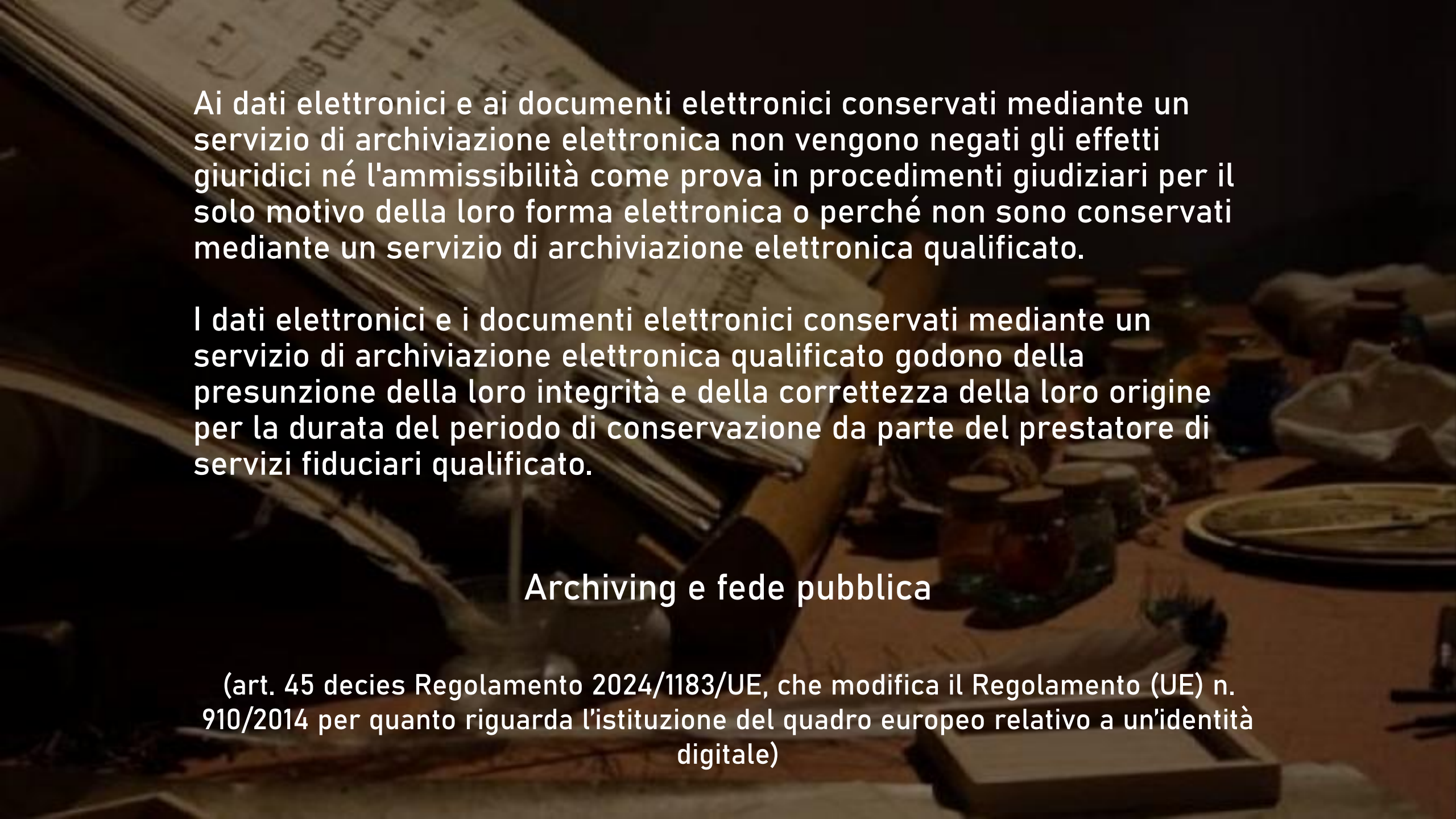


«dati»: qualsiasi rappresentazione digitale di atti, fatti o informazioni e qualsiasi raccolta di tali atti, fatti o informazioni, anche sotto forma di registrazione sonora, visiva o audiovisiva

«documento elettronico»: qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva

«documento informatico»: documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti

Dati e metadati

The background of the slide is a dark, textured image. On the left, there is a stack of old, yellowed parchment or paper, with some text visible but mostly illegible. A quill pen lies diagonally across the parchment. To the right, there is a small, dark, cylindrical object, possibly a jar or a container, and a small, light-colored, bowl-like object. The overall lighting is dim, creating a sense of antiquity and history.

Ai dati elettronici e ai documenti elettronici conservati mediante un servizio di archiviazione elettronica non vengono negati gli effetti giuridici né l'ammissibilità come prova in procedimenti giudiziari per il solo motivo della loro forma elettronica o perché non sono conservati mediante un servizio di archiviazione elettronica qualificato.

I dati elettronici e i documenti elettronici conservati mediante un servizio di archiviazione elettronica qualificato godono della presunzione della loro integrità e della correttezza della loro origine per la durata del periodo di conservazione da parte del prestatore di servizi fiduciari qualificato.

Archiving e fede pubblica

(art. 45 decies Regolamento 2024/1183/UE, che modifica il Regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione del quadro europeo relativo a un'identità digitale)

Art. 5 Qualità dei dati

I dati a carattere personale oggetto di un'elaborazione automatizzata sono:

- a) ottenuti e elaborati in modo lecito e corretto;
- b) registrati per scopi determinati e legittimi ed impiegati in una maniera non incompatibile con detti fini;
- c) adeguati, pertinenti e non eccessivi riguardo ai fini per i quali vengono registrati;
- d) esatti e, se necessario, aggiornati;
- e) conservati in una forma che consenta l'identificazione delle persone interessate per una durata non superiore a quella necessaria ai fini per i quali sono registrati.

Art. 6 Categorie speciali di dati

I dati di carattere personale indicanti l'origine razziale, le opinioni politiche, le convinzioni religiose o altri credo, nonché i dati a carattere personale relativi allo stato di salute ed alla vita sessuale, non possono essere elaborati automaticamente a meno che il diritto interno non preveda garanzie adeguate. Lo stesso dicasi dei dati di carattere personale relativi alle condanne penali.

Art. 7 Sicurezza dei dati

Adeguate misure di sicurezza vengono adottate per la protezione di dati di carattere personale registrati nei casellari automatizzati contro la distruzione accidentale o non autorizzata, ovvero la perdita accidentale così come contro l'accesso ai dati, la modifica o la diffusione non autorizzate.

Legge 21 febbraio 1989, n. 98
(ratifica Convenzione di Strasburgo n. 108/1981)

Principi applicabili al trattamento di dati personali (art. 5 GDPR)

Paragrafo 1 - I dati personali sono:

- a) trattati in modo **lecito, corretto e trasparente** nei confronti dell'interessato (idoneità dell'informativa per contenuto e modalità con cui viene resa - cfr. artt. 12, 13 e 14);
- b) raccolti per finalità **determinate, esplicite e legittime**, e successivamente trattati in modo non incompatibile con tali finalità (le finalità di archiviazione nel pubblico interesse e quelle di ricerca scientifica o storica non sono considerate incompatibili con quelle iniziali - cfr. art 89)
- c) **adeguati, pertinenti e limitati a quanto necessario** rispetto alle finalità per le quali sono trattati ("minimizzazione dei dati");
- d) **esatti e se necessario aggiornati** (i dati inesatti devono essere rettificati o cancellati);

Principi applicabili al trattamento di dati personali (art. 5)

- e) **conservati** in una forma che consenta l'identificazione dell'interessato **per un arco di tempo non superiore al conseguimento delle finalità** per le quali sono trattati (per finalità di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici possono essere conservati per tempi più lunghi);
- f) trattati in modo da garantire **un'adeguata sicurezza**, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali ("integrità e riservatezza").

Paragrafo 2 – Il titolare del trattamento **è competente per il rispetto del paragrafo 1 e in grado di provarlo** (principio di responsabilizzazione o accountability)

Accountability e ruoli nel trattamento (art. 24 GDPR)

1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, 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 presente regolamento. Dette misure **sono riesaminate e aggiornate** qualora necessario.
2. Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 **includono l'attuazione di politiche adeguate** in materia di protezione dei dati da parte del titolare del trattamento.

Protezione dei dati fin dalla progettazione (art. 25.1 GDPR)

Tenendo conto dello **stato dell'arte** e dei **costi di attuazione**, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei **rischi** aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, **sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso** il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.



Privacy by design

Protezione dei dati per impostazione predefinita (art. 25.2)

Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita (by default), **solo i dati personali necessari** per ogni specifica finalità del trattamento. Tale obbligo vale per:

- la quantità dei dati personali raccolti;
- la portata del trattamento;
- il periodo di conservazione;
- l'accessibilità.

In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica (es. trattamenti automatizzati)



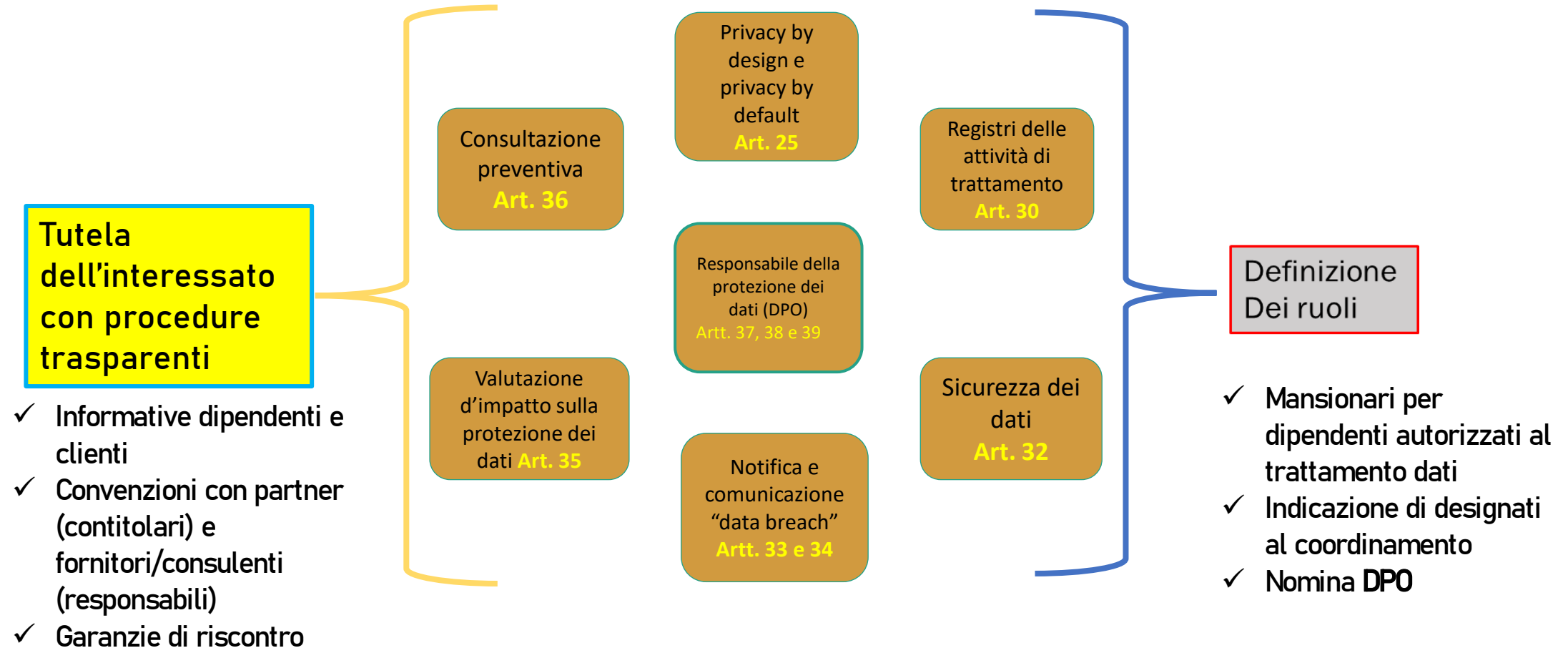
cfr. art. 3 del D.Lgs. 196/03 - Principio di necessità

Art. 28, par. 1, GDPR

Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, **quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti** per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.

Da dove iniziare?

Le principali obbligazioni di compliance previste nel Regolamento UE 2016/679

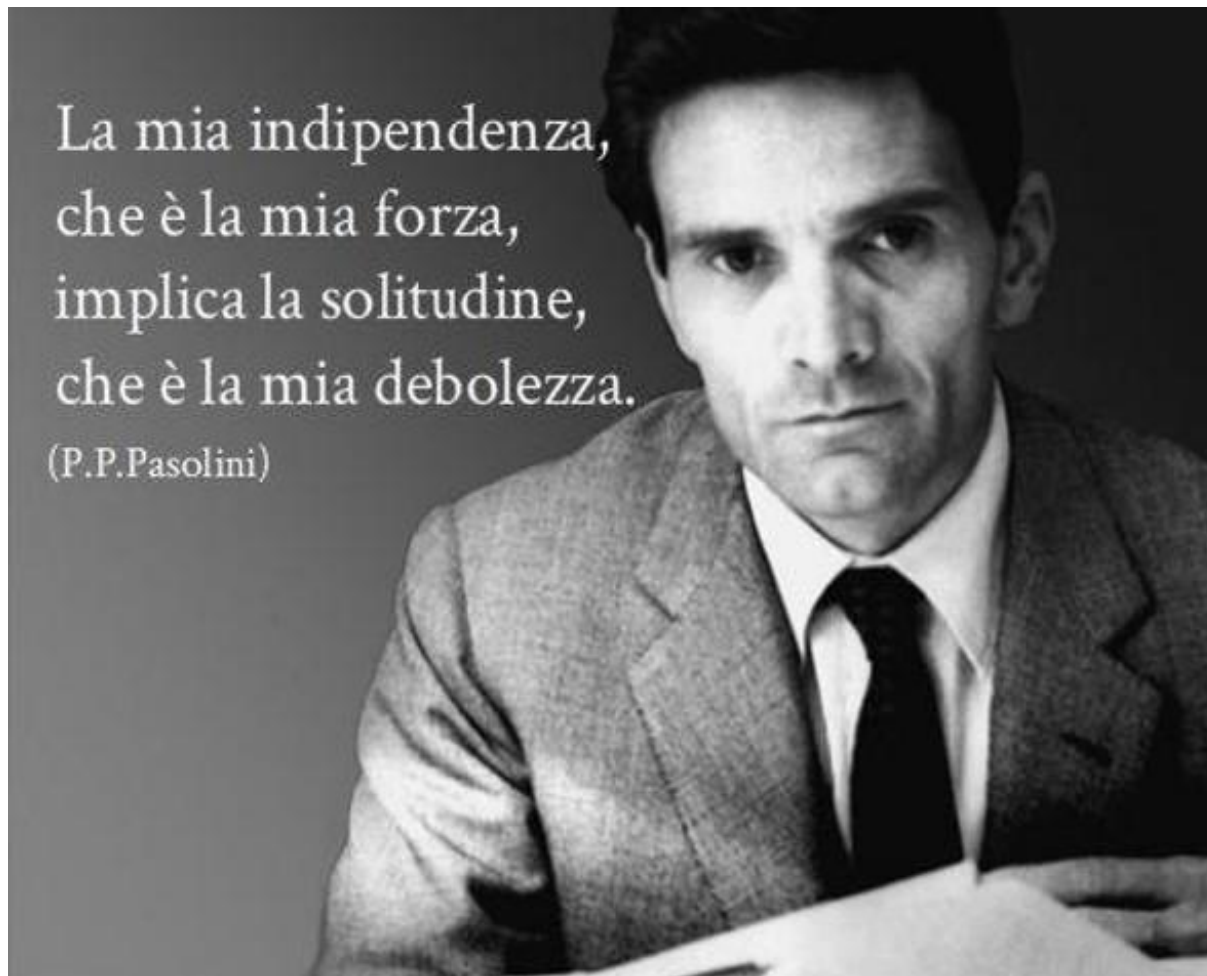


IL DPO...



La mia indipendenza,
che è la mia forza,
implica la solitudine,
che è la mia debolezza.

(P.P.Pasolini)



L'importanza dell'approccio interdisciplinare

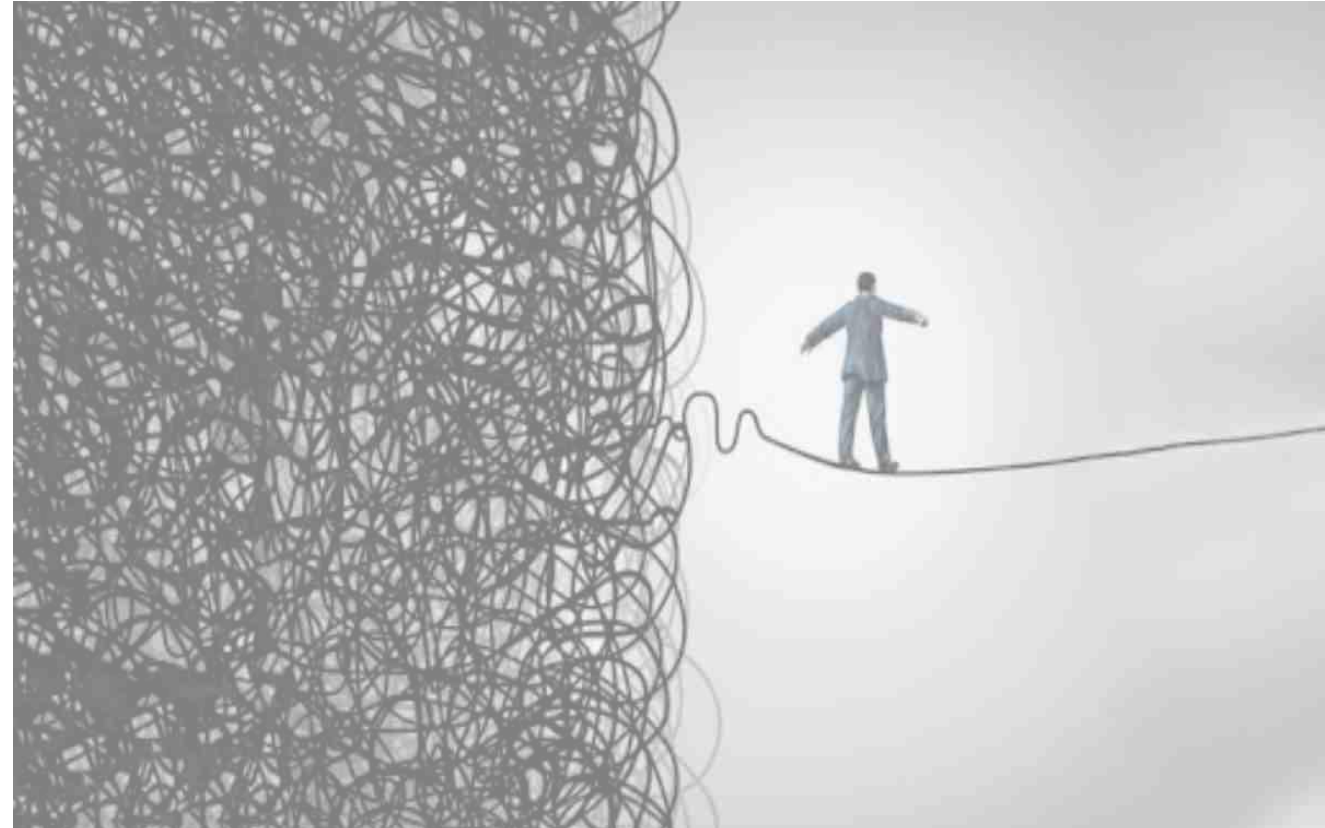
*Data Protection Officer,
Responsabili della
Conservazione, Manager
della trasformazione
digitale, Referenti security e
AI and Data Ethics
Compliance Manager
in costante confronto*



I misteri dell'orizzonte, René Magritte, 1955

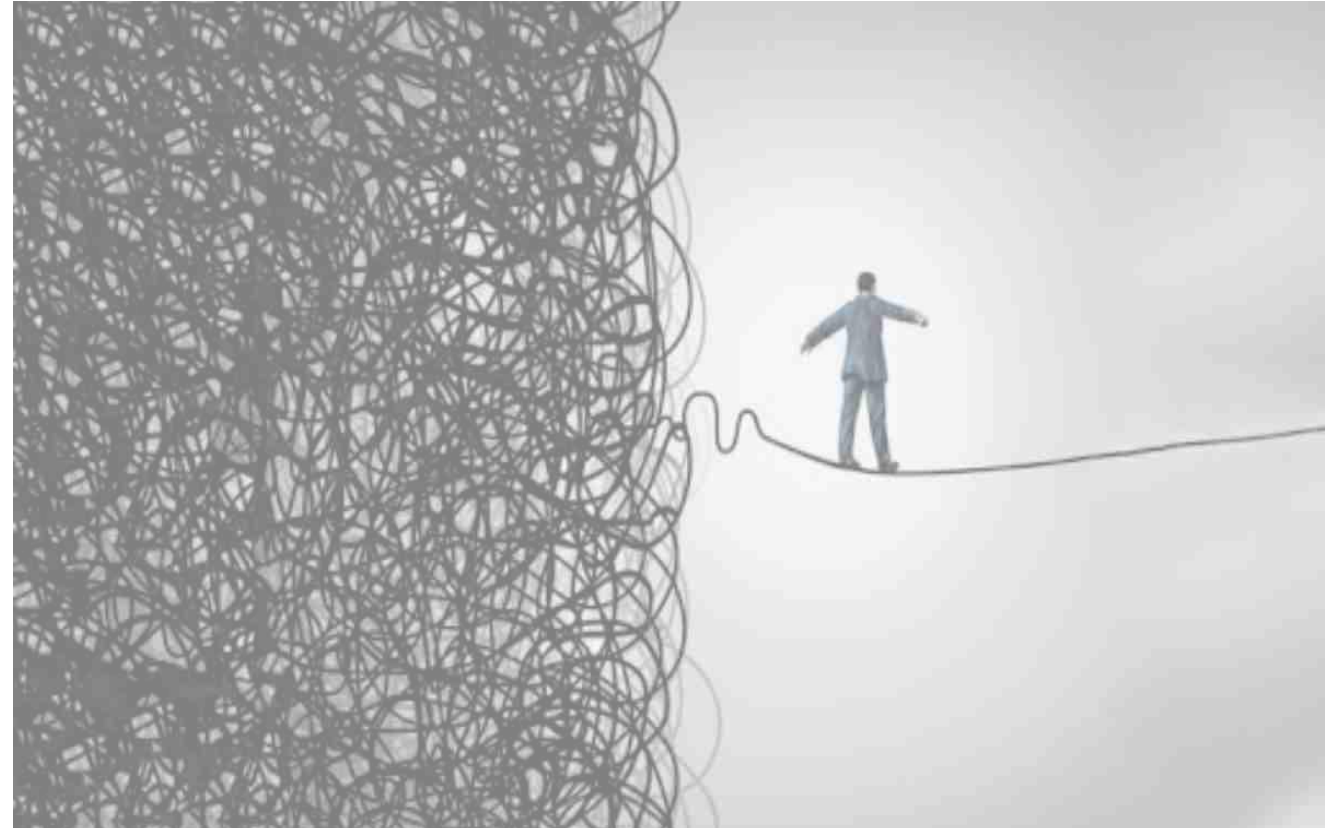
Le funzioni da sviluppare in ogni organizzazione vocata all'innovazione digitale

Il Responsabile della Conservazione dei documenti informatici (RdC) riveste un ruolo centrale nella gestione dei dati digitali, in particolare nell'ambito della loro archiviazione, conservazione e garanzia della loro integrità nel tempo. In un contesto normativo sempre più stringente - cfr. legislazioni come il GDPR, eIDAS, il Codice dell'amministrazione digitale e altre normative più specifiche e di settore sulla gestione e conservazione dei dati - il RdC deve possedere una conoscenza approfondita sia sul piano tecnico, sia su quello legale, sia su quello storico-filosofico, con il fine di garantire che i dati siano correttamente archiviati e protetti, rispettando i principi fondamentali di conservazione, integrità e accessibilità nel tempo.



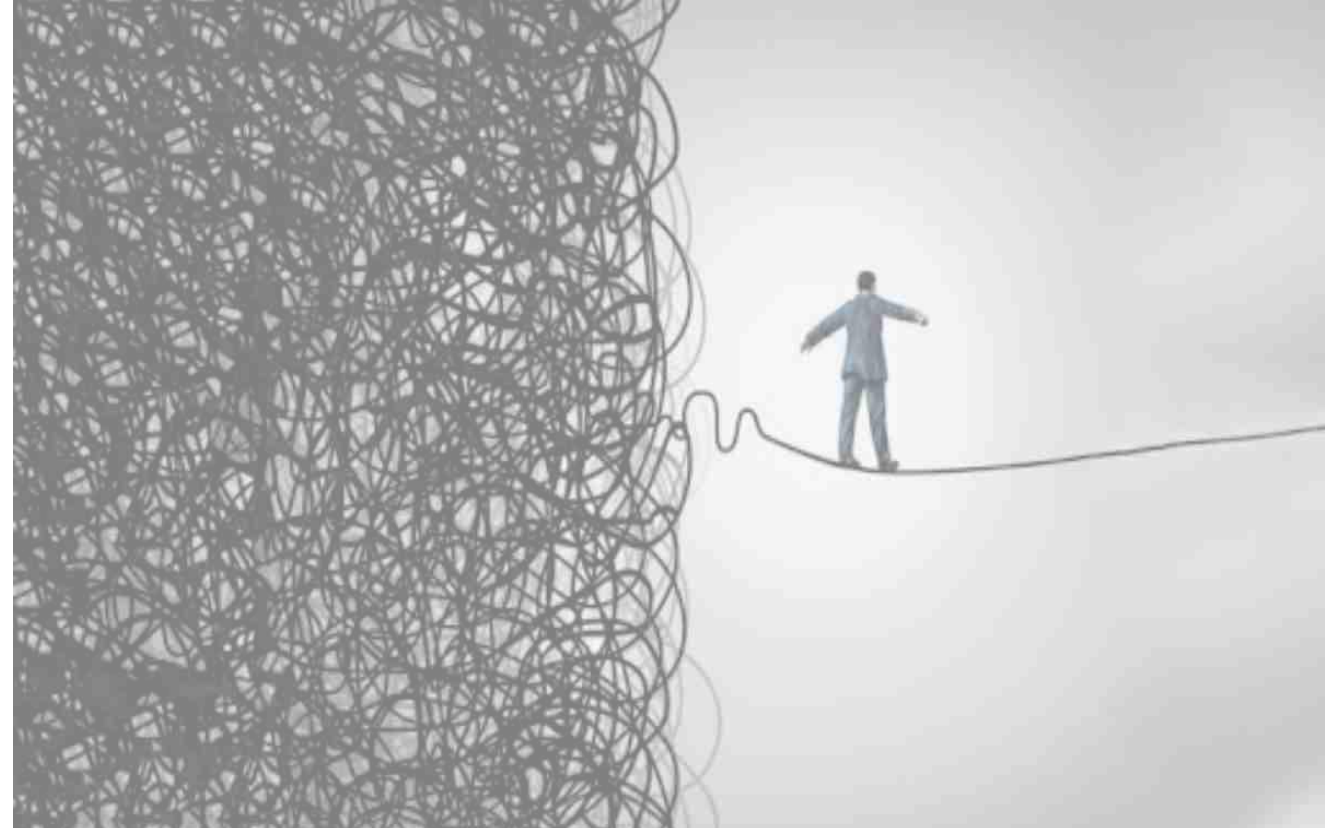
Le funzioni da sviluppare in ogni organizzazione vocata all'innovazione digitale

Il Data Protection Officer (DPO) è una figura fondamentale per assicurare la conformità delle organizzazioni alle normative sulla protezione dei dati personali. Il DPO svolge una funzione strategica nel monitoraggio delle pratiche in relazione alla data protection attraverso la supervisione della gestione dei dati e intervenendo in caso di possibili violazioni. La ricerca in questo ambito si concentra sull'evoluzione della funzione del DPO. Il suo ruolo va via via adattandosi alle nuove tecnologie e alle normative sempre più stringenti, con un focus specifico sulla protezione delle particolari categorie di dati personali che risultano più sensibili in contesti ad alto rischio: si pensi su tutti a quelli legati all'intelligenza artificiale, così come alle nuove modalità di raccolta e profilazione automatizzata dei dati



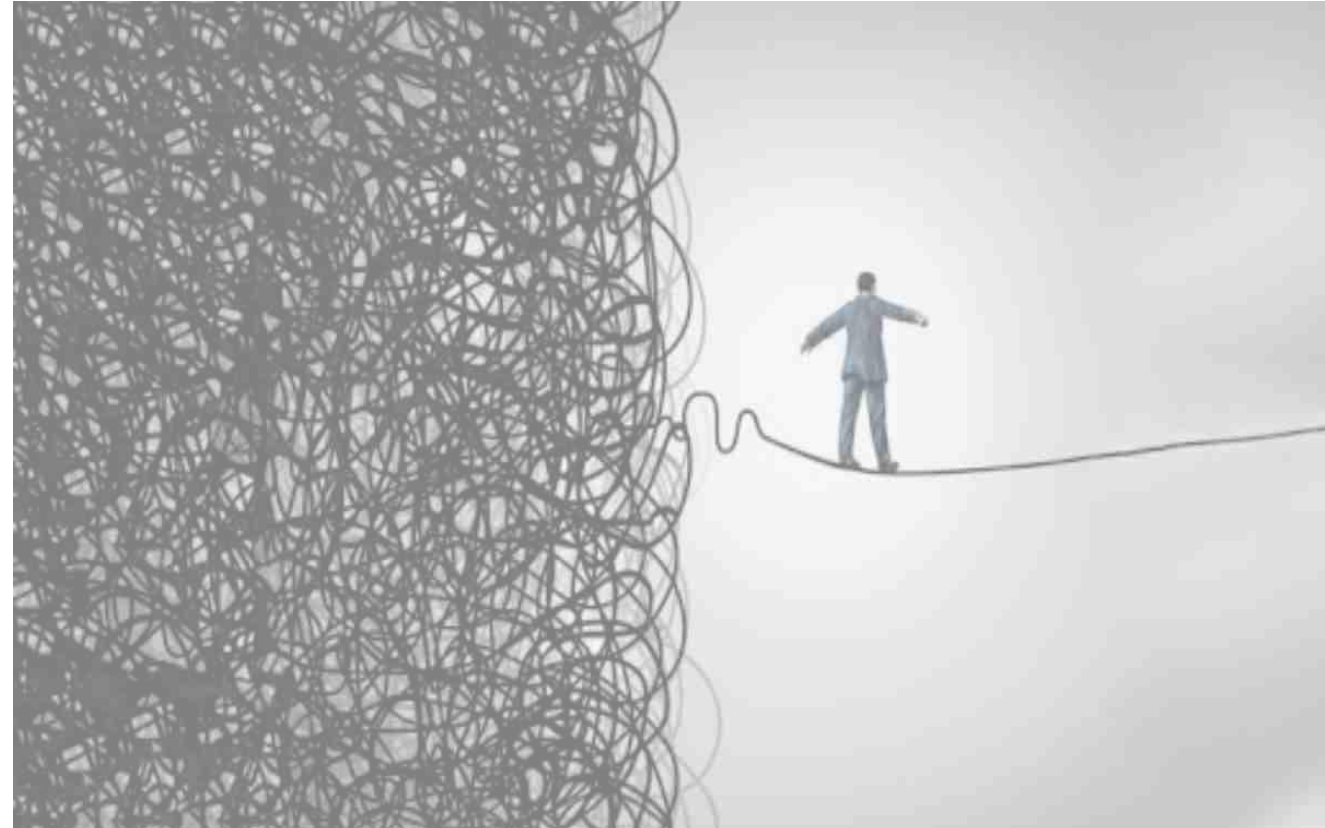
Le funzioni da sviluppare in ogni organizzazione vocata all'innovazione digitale

Il Referente per la Cybersicurezza o anche Chief Information Security Officer (CISO) è una figura professionale in grado di affrontare le nuove sfide della cybersicurezza con un approccio multidisciplinare, pratico e orientato alle reali esigenze delle organizzazioni pubbliche e private, secondo quanto previsto dalla Legge 90/2024 e per il coordinamento e la gestione delle attività e degli adempimenti della Direttiva NIS 2 (2022/2555/UE), del D.Lgs. 138/2024 e del GDPR.



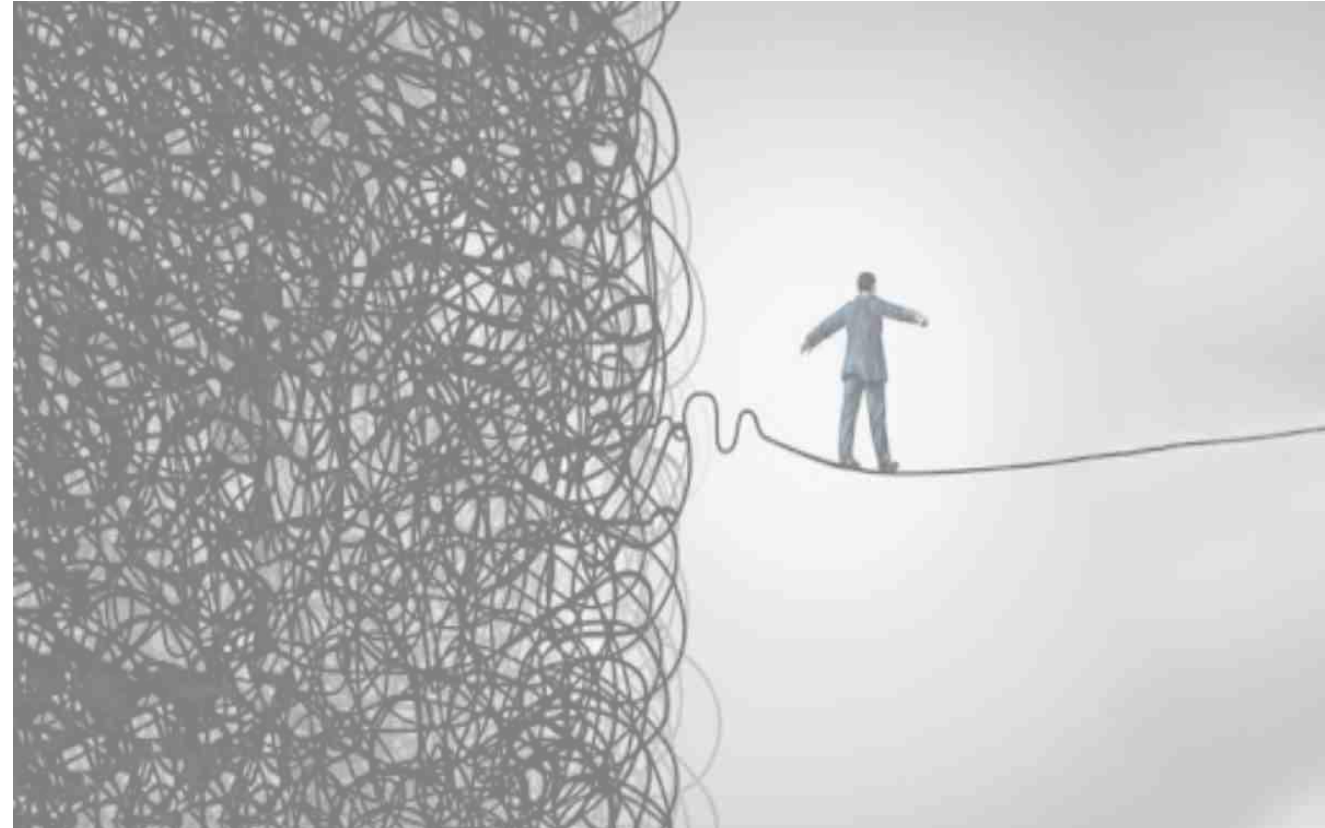
Le funzioni da sviluppare in ogni organizzazione vocata all'innovazione digitale

Il Responsabile della trasformazione digitale o Chief Digital Officer (CDO), nelle organizzazioni pubbliche e private, deve essere in grado sia di governare lo sviluppo e la gestione di processi complessi di trasformazione tecnologica e sia di sovrintendere progetti di trasformazione digitale. Tale figura strategica va indagata nella sua poliedricità, in modo da garantire che la transizione digitale, in continua evoluzione, risponda alle esigenze del diritto e dell'etica.



Le funzioni da sviluppare in ogni organizzazione vocata all'innovazione digitale

L'Esperto di Etica Digitale o AI and Data Ethics Compliance Manager (AIDEC Manager) è una figura emergente che si occupa di analizzare e proporre soluzioni per affrontare le problematiche etiche e giuridiche legate all'uso delle nuove tecnologie, in particolare quelle che riguardano l'intelligenza artificiale, l'automazione dei processi decisionali e la privacy. La ricerca in questo campo esplora le implicazioni etiche e giuridiche delle scelte tecnologiche e mira a sviluppare linee guida che garantiscano l'utilizzo delle tecnologie in modo equo, trasparente e, soprattutto, rispettoso dei diritti fondamentali degli individui. Il ruolo dell'AIDEC Manager è cruciale per orientare l'evoluzione delle tecnologie in direzione di un futuro in cui la digitalizzazione non solo promuove l'innovazione, ma sia capace di tutelare i principi morali, etici, giuridici e deontologici.



I RUOLI NELLA PA

Il modello di governance digitale



La Governance del patrimonio informativo di una società o una PA:
Compliance normativa nella Società dell'Informazione

Processo per la definizione e gestione dei profili di autorizzazione





Black Box

Il diritto di accesso non può essere negato a causa di difficoltà conoscitive derivanti dall'utilizzo di algoritmi

Consiglio di Stato, sezione VI, 6 giugno 2025, n. 4929 – Pres. De Felice, Est. Ponte

Atto amministrativo – Accesso ai documenti – Procedimento automatizzato – Utilizzo dell'algoritmo – Difficoltà conoscitive – Diniego – Illegittimità

L'accesso documentale non può essere negato per le difficoltà conoscitive derivanti dall'utilizzo, nell'esercizio dell'attività amministrativa, di algoritmi interamente gestiti in forma automatizzata. (1).

In motivazione, la sezione evidenzia che l'utilizzo di sistemi di intelligenza artificiale, dagli algoritmi al c.d. machine learning, va inteso quale modulo procedimentale per lo svolgimento dell'attività autoritativa in modalità più efficienti ed è regolato dai principi di conoscibilità e comprensibilità, non esclusività della decisione algoritmica, non discriminazione algoritmica; pertanto, l'amministrazione dotata di competenza primaria nella materia della gestione e del pagamento dei contributi oggetto di un'istanza di accesso non può trincerarsi dietro la non conoscibilità dei meccanismi informatici di gestione: alla luce dei suddetti principi, a chi chiede l'accesso non sono opponibili le difficoltà conoscitive derivanti dall'utilizzo, nell'esercizio dell'attività amministrativa, di algoritmi interamente gestiti in forma automatizzata.

Art. 22 Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione

1. L'interessato ha il diritto di 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.
2. Il paragrafo 1 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, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato;
 - c) si basi sul consenso esplicito dell'interessato.
3. Nei casi di cui al paragrafo 2, lettere a) e c), il titolare del trattamento attua 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.**
4. Le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, a meno che non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.

E quindi che strada deve indicare il DP0?





Accountability

Ma a chi compete
assicurarsi che sia
garantita la
compliance sui dati
gestiti dall'azienda?

Consigli generali

A un team composto da:

- ✓ Designati al coordinamento della protezione dei dati
- ✓ Data Protection Officer
- ✓ Direttori dei sistemi informativi
- ✓ Security Manager
- ✓ *AI Ethical Manager? ...etc.*

I consigli generali da fornire son sempre gli stessi...

In caso di sviluppo progetti innovativi che comportino trattamenti di dati personali, chiedere sempre la collaborazione del DPO su:

- ✓ Cosa (*tipologia di dati e trattamenti*)
- ✓ Perché (*base giuridica e finalità*)
- ✓ Come (*attraverso quali strumenti, operazioni e soggetti*)
- ✓ Quando (*tempistiche e conservazione*)
- ✓ Chi (*destinatari*)
- ✓ Dove (*luogo di trattamento*)

Accountability

Ovviamente è sempre indispensabile coinvolgere il Team privacy e gli affari legali...

Consigli generali

In caso di sviluppo
soluzioni software /
app o per la scelta e
contrattualizzazione
dei rapporti relativi a
soluzioni
informatiche / cloud

Coinvolgere Team e DPO su:

- ✓ Cosa (*tipologia di dati e trattamenti*)
- ✓ Perché (*base giuridica e finalità*)
- ✓ Come (*attraverso quali strumenti, operazioni e soggetti*)
- ✓ Quando (*tempistiche e conservazione*)
- ✓ Chi (*destinatari*)
- ✓ Dove (*luogo di trattamento*)

fate visionare clausole privacy, SLA e atti di designazione a DPO e Team

Consigli ulteriori...

Che domande
rivolgere a una
soluzione
informatica?

- ✓ Che attività di trattamento sono consentite dal sw?
- ✓ È consentita la separazione dei dati?
- ✓ È consentita l'esportabilità in formato interoperabile/riutilizzabile dei dati?
- ✓ È consentita la «limitazione» nel trattamento del dato in caso di richiesta?;
- ✓ È prevista l'automatica cancellazione dei dati dopo un tempo stabilito?
- ✓ Ci sono strumenti di anonimizzazione/pseudoanonimizzazione?
- ✓ In caso di soluzione in cloud i server sono dislocati in Europa?
- ✓ È previsto un accesso selettivo ai dati previo inserimento di id e pw?
- ✓ Le pw sono robuste? Il sistema ne prevede in automatico il cambio?
- ✓ Sono previste politiche di autorizzazione differenziata per profilo utente nella gestione dei database?
- ✓ È prevista una gestione dei log?
- ✓ È previsto una gestione dei report in caso di data breach?
- ✓ Etc.

Avete una checklist di controllo della privacy by design e privacy by default?

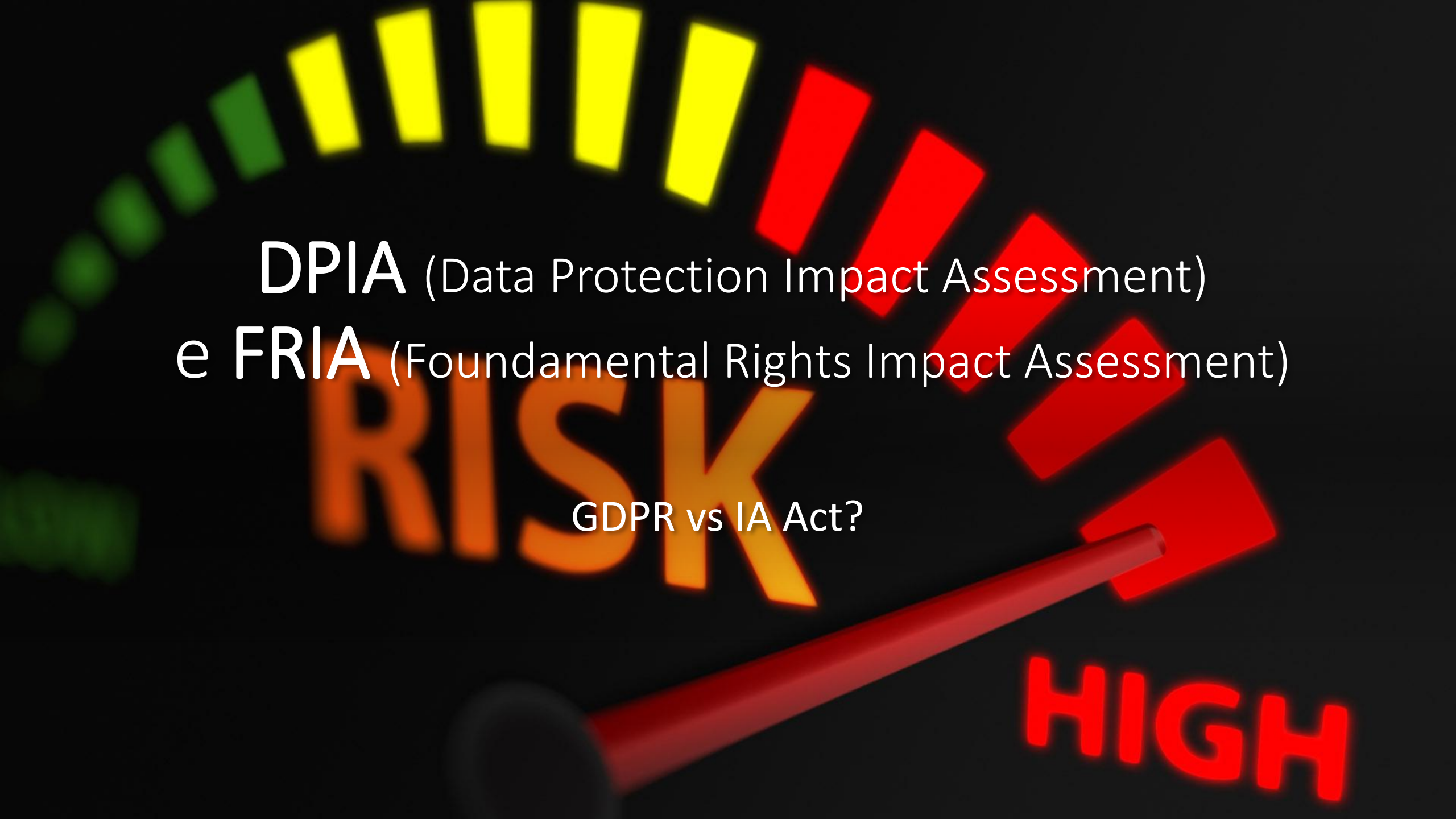
Trasparenza e conoscibilità

Non esclusività della decisione
algoritmica

Non discriminazione

...e ruolo del DPO





DPIA (Data Protection Impact Assessment)
e **FRIA** (Fundamental Rights Impact Assessment)

GDPR vs IA Act?

GDPR vs IA Act?





Tempistiche di Applicazione dell'AI Act

- ✓ **2 febbraio 2025:** Sono entrate in vigore le disposizioni relative all'alfabetizzazione in materia di AI e alle pratiche di AI vietate.
- ✓ **2 agosto 2025:** Si applicano le norme sulla governance e gli obblighi per l'AI di uso generale.
- ✓ **2 agosto 2026:** L'AI Act entra pienamente in vigore, con la maggior parte delle disposizioni applicabili da questa data.
- ✓ **2 agosto 2027:** Gli obblighi per i sistemi di AI ad alto rischio, incorporati in prodotti regolamentati, diventano effettivi.

Accountability

L' art. 5 dell'AI Act, applicabile dal 2 febbraio, proibisce, nella sintesi fornita dalla Commissione europea, le seguenti otto pratiche:

- manipolazione e inganno dannosi basati sull'intelligenza artificiale
- sfruttamento dannoso delle vulnerabilità basato sull'intelligenza artificiale;
- punteggio sociale o social scoring;
- valutazione o previsione del rischio di reato individuale;
- scraping non mirato di materiale Internet o CCTV per creare o espandere database di riconoscimento facciale;
- riconoscimento delle emozioni nei luoghi di lavoro e negli istituti scolastici;
- categorizzazione biometrica per dedurre determinate caratteristiche protette;
- identificazione biometrica remota in tempo reale per scopi di applicazione della legge in spazi accessibili al pubblico.

L'articolo 96 dell'AI Act prevede che la Commissione adotti apposite Linee guida sull'applicazione delle regole relative alle pratiche vietate soprariportate.

Si tratta di orientamenti non vincolanti. L'interpretazione dei divieti, da parte della Commissione, non vincola infatti i destinatari, come invece accade per le interpretazioni della normativa compiute dalla Corte di giustizia.

Accountability



Brussels, 4.2.2025
C(2025) 884 final

ANNEX

ANNEX

to the

Communication to the Commission

Approval of the content of the draft Communication from the Commission -
Commission Guidelines on prohibited artificial intelligence practices established by
Regulation (EU) 2024/1689 (AI Act)

Obblighi per Sviluppatori e Deployer



Alfabetizzazione in materia di AI: Entro il 2 febbraio 2025, sviluppatori e deployer devono garantire che il proprio personale abbia un livello sufficiente di conoscenze sull'AI, tenendo conto dell'istruzione e formazione dei soggetti coinvolti.

Pratiche di AI vietate: Dal 2 febbraio 2025, è vietato l'uso di sistemi di AI che manipolano il comportamento umano, sfruttano vulnerabilità, o utilizzano tecniche di riconoscimento facciale non mirato.

Compliance e gestione dei rischi: Sviluppatori e deployer devono assicurare la conformità alle norme, gestire i rischi associati ai sistemi di AI e garantire la trasparenza.

Sistemi ad alto rischio: Per i sistemi classificati come ad alto rischio, ci sono obblighi specifici di valutazione e mitigazione dei rischi, che diventano effettivi dal 2 agosto 2027.

Queste misure mirano a creare un ecosistema di AI sicuro e trasparente, proteggendo i diritti fondamentali dei cittadini e promuovendo un uso etico dell'intelligenza artificiale.

Accountability

Istruzioni sull'uso responsabile di sistemi di intelligenza artificiale (IA) generativa

Anche ai sensi dell'art. 29 del Regolamento (UE) 2016/679 (GDPR)

*Il 20 marzo 2024 la Commissione Europea – Direzione Generale per la Ricerca e l'Innovazione – ha pubblicato il documento intitolato **Living guidelines on the Responsible use of Generative AI in research** indirizzate a tutti coloro, siano essi ricercatori, organizzazioni per la ricerca o per il finanziamento della ricerca, che utilizzano l'Intelligenza Artificiale generativa.*

N.B. Gli esempi di istruzioni di seguito riportate non riguardano lo sviluppo di sistemi di IA, ma solo il loro utilizzo.

Alcuni estratti...

ISTRUZIONI E RACCOMANDAZIONI PER GLI UTENTI

- Assicurarsi che l'uso dello strumento sia autorizzato e appropriato.
- Considerare che è solo uno strumento, e comprendere come funziona.
- Preferire i sistemi addestrati su dati certificati e ufficiali per limitare i rischi.
- Preferire i sistemi trasparenti nelle loro condizioni d'uso.
- Prediligere strumenti di IA che consentano la verifica delle fonti e dei riferimenti, o che siano addestrati utilizzando dataset trasparenti con fonti e riferimenti adeguatamente documentati.

Alcuni estratti...

- Prediligere sistemi dedicati al settore specifico di riferimento.
- Dare istruzioni chiare allo strumento e verificare che siano state comprese correttamente.
- Inserire solo dati non sensibili già disponibili pubblicamente, evitando comunque di inserire dati personali. Non inserire dati che per loro natura o per qualsiasi altra ragione devono considerarsi segreti o riservati. Prestare particolare attenzione alle questioni relative alla privacy, alla riservatezza e ai diritti di proprietà intellettuale quando si condividono informazioni sensibili o protette con gli strumenti di IA.

Alcuni estratti...

- Verificare sempre la correttezza delle risposte. Rivedere criticamente gli output ed evitare la dipendenza eccessiva dagli strumenti di IA (come per Google o altri strumenti di ricerca).
- Essere trasparenti sull'uso di IA generativa.
- Reformulare il testo generato se destinato a documenti ufficiali o legali.
- Mantenere sempre il controllo sulla decisione e assumere sempre in prima persona le decisioni.

Istruzioni particolari...

1. Rimanere responsabile in ultima istanza dell'output e della produzione dei contenuti:

- garantire l'integrità dei contenuti generati o supportati da strumenti di intelligenza artificiale (IA);
- mantenere un approccio critico verso i risultati prodotti dall'IA, con la consapevolezza delle limitazioni di questi strumenti, come bias, falsificazioni (c.d. allucinazioni) e imprecisioni;
- non considerare i sistemi di IA autori o coautori, la responsabilità è sempre in capo all'essere umano.

2. Utilizzare i sistemi di IA generativa in maniera trasparente:

- chiarezza nell'uso: indicare quali strumenti di IA generativa sono stati usati, come hanno influenzato i risultati ottenuti e rendere disponibili input e output, se rilevante;
- riproducibilità: considerare la natura casuale degli output degli strumenti di IA, discutendo eventuali limitazioni e bias.

Istruzioni particolari...

3. Prestare particolare attenzione alle questioni relative alla privacy, alla riservatezza e ai diritti di proprietà intellettuale quando si condividono con i sistemi di IA dati personali, informazioni sensibili o protette:

- proteggere le informazioni sensibili o protette (come testi, dati, immagini) evitando di caricarle su sistemi di IA online senza la garanzia che non saranno riutilizzati da terzi, ad esempio per addestrare modelli futuri o in modi non tracciabili e verificabili;
- non inserire nei sistemi di IA dati personali, salvo che non si abbia il consenso dell'interessato oppure non ci siano altre basi giuridiche che rendano lecita la condivisione dei dati;
- in ogni caso, comprendere gli impatti che l'uso degli strumenti di IA può avere sulla privacy e sulla proprietà intellettuale, configurare adeguatamente le impostazioni e le opzioni di privacy degli strumenti, valutare dove e come i dati vengono trattati.

Istruzioni particolari...

4. **Quando utilizzano l'IA generativa, rispettare la legislazione nazionale, europea e internazionale applicabile, come regolarmente deve avvenire durante le attività di ricerca:**
 - evitare il plagio e riconoscere correttamente il lavoro altrui, citando le fonti appropriate se l'output dell'IA si basa su risultati di altri;
 - gestire responsabilmente eventuali dati personali nei contenuti generati, nel rispetto della politica dell'Organizzazione e della normativa in materia di protezione dei dati personali.
5. **Imparare continuamente a utilizzare correttamente gli strumenti di IA generativa al fine di massimizzarne i vantaggi, e aggiornarsi, anche attraverso la formazione:**
 - aggiornarsi sulle migliori pratiche per l'uso degli strumenti di IA generativa, condividendole con i colleghi.
6. **Astenersi dall'utilizzare strumenti di IA generativa in modo sostanziale in attività critiche o sensibili che potrebbero avere un impatto su altri colleghi o organizzazioni :**
 - occorre proteggere anche il lavoro inedito dei colleghi da esposizioni o inclusioni non autorizzate in modelli di IA.

A photograph of a city in ruins, likely after a conflict. The image shows several multi-story buildings that have been severely damaged, with many windows missing and structural elements exposed. Debris is scattered across the ground. In the background, thick plumes of dark smoke rise into a cloudy sky, suggesting ongoing destruction or fires. The overall tone is somber and desolate.

Sostenibilità e IA

The dark side of the moon

<https://www.internazionale.it/reportage/laura-melissari/2024/08/06/intelligenza-artificiale-lavoratori-sfruttamento>



Messaggio pubblicitario con finalità promozionale.

TECNOLOGIA

I proletari dell'intelligenza artificiale

Laura Melissari, giornalista

6.8.2024



L'avvocato deve stupirsi
della tecnologia o essere
capace di interpretarla?



Il passato insegna, ma non va ripetuto all'infinito...



Certe cose per adesso le sa fare solo lui...



CI VUOLE TANTO CORAGGIO...

a momentary lapse of reason

L'evento
che risveglia
il senso
e il gusto
del digitale



Grazie per l'attenzione!
andrealisi@studiolegalelisi.it
www.digeat.info

LECCE
27.28.29
Novembre
2025

