

INDICE SOMMARIO

<i>Elenco Autori</i>	XV
<i>Premessa</i>	XVII
<i>Abstract</i>	XIX
<i>Avvertenza</i>	XXI
<i>Prefazione</i>	XXIII

Capitolo 1

TUTELA DELLA PERSONA, DATI E ASIMMETRIE DI POTERE TRA GDPR E AI ACT: IL CREPUSCOLO DELL'AUTODETERMINAZIONE

Emilio Tosi

1. Premessa	4
2. Il dato economico: oltre l'AI <i>hype</i> "en attendant" la <i>tech bubble</i>	9
3. Il ruolo europeo di regolatore globale dell'innovazione digitale: verso un nuovo <i>Bruxelles effect</i> dell'AI Act dopo il GDPR?	11
4. L'orditura normativa dell'AI ACT: una trama complessa tra principi e regole.	15
5. Principali finalità e tutele dell'AI Act	25
6. La classificazione del rischio delle AI: inaccettabile, alto, limitato e minimo	26
7. Prime riflessioni: luci e ombre tra iporegolazione e iperregolazione	30
8. Dati e <i>governance</i> dei dati delle AI ad alto rischio: l'art. 10 dell'AI Act	34
9. Sorveglianza umana delle AI ad alto rischio: art. 14 AI Act e il principio <i>human in the loop</i>	36
10. Vulnerabilità digitale della persona e fragilità del consenso.	38
11. Conclusioni: dal controllo Orwelliano al controllo Kafkiano	43

Capitolo 2

GDPR E AI ACT: DIGNITÀ DELLA PERSONA E PROFILI COSTITUZIONALI OLTRE L'AUTOREGOLAZIONE

Ginevra Cerrina Feroni

1. La dignità al centro della contemporanea regolazione europea del digitale	49
2. La declinazione della dignità umana nella sistematica del GDPR e gli interventi del Garante	52

3.	L'anima <i>fundamental-rights based</i> dell'AI Act nella tassonomia delle pratiche di IA, vietate e ad alto rischio	55
4.	Sfide della <i>governance</i> dell'IA	59
5.	Conclusioni e prospettive future	60

Capitolo 3

DALLA TRAGEDIA DEI BENI COMUNI A QUELLA DEI DATI PERSONALI: L'INSOSTENIBILE LEGGEREZZA DELL'ADDESTRAMENTO DEGLI ALGORITMI

Guido Scorza

1.	Il contesto e la tesi	64
2.	La legittimità del <i>webscraping</i> finalizzato all'addestramento degli algoritmi	68
3.	Le basi giuridiche teoricamente utili	73
4.	Il legittimo interesse come base giuridica per il <i>webscraping</i> strumentale all'addestramento degli algoritmi	74
5.	Gli obblighi del titolare del trattamento che ricorra al legittimo interesse quale base giuridica	80
6.	Il dilemma dell'impossibilità tecnologica di addestrare gli algoritmi se non si considera il legittimo interesse un'idonea base giuridica	82
7.	Una proposta di soluzione imperfetta per mitigare la tragedia dei dati personali senza sbarrare la strada all'innovazione.	84

Capitolo 4

DIRITTI SUL CORPO E DATI SANITARI

Fabrizio Criscuolo

1.	Premessa	88
2.	Identità personale e autodeterminazione informativa: la funzione del consenso	90
3.	Altruismo dei dati e solidarietà	93
4.	Osservazioni conclusive	95

Capitolo 5

DATI BIOMETRICI, WEB SCRAPING E VALUTAZIONE D'IMPATTO

Anna Carla Nazzaro

1.	Dati personali, dati biometrici e riferibilità univoca al soggetto	101
2.	Analisi della Tecnologia e delle Implicazioni per la definizione di dato biometrico	102
3.	Specificazione del concetto di identificazione e ruolo del <i>webscraping</i> nell'AI Act.	105
4.	Ipotesi applicative: criticità nell'utilizzo del <i>webscraping</i>	107

5.	Considerazioni sulle Finalità del Trattamento dei Dati Biometrici	110
6.	Qualità dei dati e Valutazione d'impatto	111

Capitolo 6

AI RESPONSABILE E AFFIDABILE: IL PRINCIPIO DI *ACCOUNTABILITY*

Carmelo Fontana

1.	Premessa	116
2.	Il principio di <i>accountability</i> nel GDPR e nell'AI Act	117
3.	Osservazioni conclusive	120

Capitolo 7

TRASPARENZA E DATI DI ADDESTRAMENTO TRA PROPRIETÀ INTELLETTUALE E *PRIVACY*

Alberto Maria Gambino

1.	Trasparenza e <i>privacy</i>	126
2.	Principio di trasparenza e protezione dei dati personali	129
3.	IA, <i>privacy</i> e diritto d'autore	135

Capitolo 8

NOVE CERTEZZE SU DECISIONI ALGORITMICHE, DIRITTO ALLA SPIEGAZIONE E TUTELA DEI CONSUMATORI

Salvatore Orlando

1.	Le certezze dei dubbi come basi dell'interpretazione	144
2.	Tre certezze sulle « decisioni algoritmiche ».	146
2.1.	I sistemi di IA non hanno personalità giuridica	146
2.2.	Il concetto di 'decisore' in senso giuridico	151
2.3.	Le tre nozioni di 'decisioni', le due nozioni di 'influenza sulle decisioni' e il significato dell'espressione 'pratiche di IA' nell'AI Act	152
3.	Tre certezze sul diritto alla spiegazione	156
3.1.	La distinzione tra 'uso dei sistemi di IA' (funzionamento) e 'uso degli <i>output</i> dei sistemi di IA' (qualunque attività giuridicamente rilevante)	156
3.2.	Differenza tra l'AI Act come disciplina quadro sul prodotto 'sistema di IA' (sviluppo, commercializzazione ed uso, nel senso di funzio- namento) e le innumerevoli e diverse discipline di diritto dell'Unione e nazionale che hanno ad oggetto le attività interessate dall'uso degli <i>output</i> dei sistemi di IA	157
3.3.	Il diritto alla spiegazione di cui all'art. 86 AIA si aggiunge e non soppianta alcuno dei divieti e dei rimedi previsti dal diritto del- l'Unione e nazionale di volta in volta applicabile	161

4.	Tre certezze sulla tutela dei consumatori	164
4.1.	Dalla protezione del consumatore online a quella dell'utente online .	164
4.2.	Centralità della persona.	164
4.3.	Pluriplanarità dell'ordinamento giuridico.	166
	<i>Bibliografia, a cura di Giovanni Maria Tosi</i>	169
	<i>Appendice. Regolamento (UE) 2024/1689 del Parlamento Europeo e del Consiglio del 13 giugno 2024 - AI Act</i>	175

ELENCO AUTORI

GINEVRA CERRINA FERONI

Vice Presidente Garante per la protezione dei dati personali; Professore Ordinario di Diritto Costituzionale nell'Università di Firenze.

FABRIZIO CRISCUOLO

Professore Ordinario di Diritto Civile nell'Università di Roma La Sapienza.

CARMELO FONTANA

Senior Corporate Counsel Google EMEA; Presidente AIRIA.

ALBERTO MARIA GAMBINO

Professore Ordinario di Diritto Privato Università Europea di Roma.

ANNA CARLA NAZZARO

Professore Ordinario di Diritto Privato, Università degli Studi Internazionali di Roma - UNINT.

SALVATORE ORLANDO

Professore Ordinario di Diritto Privato nell'Università di Roma La Sapienza.

GUIDO SCORZA

Componente Garante per la protezione dei dati personali.

EMILIO TOSI

Professore Associato di Diritto Privato nell'Università di Milano Bicocca, Ordinario ASN; Direttore Collana internazionale di studi giuridici privatistici Diritto delle Nuove Tecnologie©; Direttore Centro Studi Diritto Nuove Tecnologie DNT®.

Desidero innanzitutto ringraziare la Fondazione Cesifin nella persona del Presidente Beppe Morbidelli e della Vice Presidente Ginevra Cerrina Feroni per aver ospitato l'XI *Convegno del Centro Studi Diritto Nuove Tecnologie DNT®* dal titolo “*Persona, dati personali e algoritmi tra GDPR e AI Act*” nella suggestiva cornice di Palazzo incontri il 17 giugno 2024 e dedicato a prime ragionate riflessioni in merito alle intersezioni tra *General Data Protection Regulation* e *Artificial Intelligence Act*.

Il 21 maggio 2024, dopo il passaggio in Parlamento, il Consiglio dell'Unione europea ha definitivamente approvato il Regolamento sull'intelligenza artificiale dell'Unione Europea (“AI Act”): non il primo in assoluto come spesso si dice — in quanto preceduto cronologicamente di pochi giorni dal *Colorado Artificial Intelligence Act* (CAIA) il 17 maggio 2024 — ma certamente il primo in termini di tutela dei diritti fondamentali della persona rispetto all'AI.

Dopo essere stato firmato dai presidenti del Parlamento europeo e del Consiglio UE il 13 giugno 2024 il Regolamento n. 1689 è stato pubblicato nella Gazzetta Ufficiale dell'Unione europea il 12 luglio 2024 ed è entrato formalmente in vigore il 1° agosto 2024 venti giorni dopo la sua pubblicazione, ma sarà pienamente applicativo solo dopo due lunghi anni, con alcune eccezioni che vedremo meglio in seguito.

L'UE con l'AI Act pone significativi limiti allo sviluppo delle intelligenze artificiali assicurando impiego e utilizzo antropocentrico, sicuro, trasparente e affidabile oltre al rispetto dei diritti fondamentali della persona: occorre, tuttavia, evitare un eccesso di normazione, ossia l'*iper-regolazione* che potrebbe risultare fatale allo sviluppo del settore.

(*) *Direttore Collana internazionale di studi giuridici privatistici Diritto delle Nuove Tecnologie© e Centro Studi Diritto Nuove Tecnologie DNT®; Professore Associato di Diritto Privato, Ordinario ASN, Università degli studi di Milano-Bicocca.*

In direzione opposta a quella europea, più prudente e protettiva della persona, gli Stati Uniti con il recente Executive Order presidenziale del 23 gennaio 2025 rimuovono, invece, i precedenti limiti statuendo programmaticamente che: *“It is the policy of the United States to sustain and enhance global AI dominance in order to promote human flourishing, economic competitiveness and national security”*.

Il dominio globale nello sviluppo e utilizzo delle intelligenze artificiali costituisce il nuovo orizzonte applicativo federale. Il *purpose* governativo è chiaro: vincere la sfida dell’innovazione tecnologica significa vincere la sfida geopolitica tra le grandi potenze.

In tale nuovo ordine globale che si delinea all’orizzonte la visione europea antropocentrica fondata sulla gestione del rischio si contrappone rispetto a quella americana orientata, innanzitutto, al successo dell’intrapresa tecnologica che, tuttavia, non è esente da rischi, anzi.

Si pensi, innanzitutto, solo per citare i più emblematici, ai rischi per i diritti fondamentali della personalità, i dati personali, l’informazione e la cybersicurezza.

Tali modelli alternativi — tra percezione e realtà effettiva — richiedono, nel dialogo transatlantico, attenta riflessione di carattere non solo etico, rilevante ma non sufficiente di per sé a governare il fenomeno, certamente economico e sociale ma soprattutto giuridico.

Si tratta, dunque, per il giurista di affrontare il tema nuovo e scivoloso, in un contesto globale complesso e in evoluzione come quello attuale, dei complessi rapporti tra protezione della persona, dei dati personali e delle nuove vulnerabilità digitali, da un lato e sviluppo e utilizzo trasparente, affidabile e responsabile di entità artificiali statisticamente “intelligenti”, dall’altro.

ABSTRACT

With the AI Act the EU places significant legal limits on the development of artificial intelligence, ensuring transparent, reliable *anthropocentric* development and use as well as respect for fundamental human rights and personal data. Relevant and deep are the emerging legal intersections between *General Data Protection Regulation*, EU Regulation n. 679/2016 and *AI Act*, EU Regulation n. 1689/2024.

This selection of studies from well known experts — is the result of the 2024 Florence Conference held at Cesifn with Diritto Nuove Tecnologie DNT® Center of legal Studies — deals with key issues of personal fundamental rights, data protection and privacy facing increasing disruptive AI systems deployment and use.

AVVERTENZA

Nel presente volume verranno utilizzati indifferentemente i termini IA e AI per abbreviare rispettivamente Intelligenza Artificiale e Artificial Intelligence.

“Saper guardare negli occhi il destino del proprio tempo” era quanto Max Weber, circa un secolo fa, esortava a fare, superando la condizione di debolezza dell’uomo moderno di fronte a una realtà che, già allora, andava delineandosi come profondamente complessa. È un invito che resta valido, se possibile ancor di più oggi, quando la velocità e la rilevanza dei mutamenti indotti dall’evoluzione tecnologica rischiano di rendere l’uomo sempre meno protagonista della storia e persino della cronaca. La sfida è, allora, rimettere l’uomo al centro di questo cambiamento, perché la tecnica sia al servizio dell’uomo e mai viceversa.

In questo percorso, il diritto — mai come nel caso presente morfologia del sociale — ha un ruolo dirimente: assegnare all’innovazione una direzione e dei limiti, perché essa non sia, con paradossale eterogenesi dei fini, socialmente regressiva. Questo vale soprattutto per l’IA che, per la sua capacità emulativa del ragionamento umano, appare potenzialmente in grado di sostituire la persona in molte funzioni. Il tema non è tanto e non è soltanto quello del rischio che “i robot ci rubino il lavoro” quanto, piuttosto, quello della libertà dell’uomo rispetto alla pervasività di una tecnologia che, come nel caso delle applicazioni di IA in campo neuroscientifico, giunge fino alla soglia, sinora invalicabile, del pensiero umano.

La peculiarità caratterizzante l’IA è, infatti, come ha osservato Eric Sadin, il suo essere una tecnica non tanto e non solamente protesica — volta cioè a compensare carenze dell’uomo — quanto piuttosto mimetica, capace cioè di emulare la razionalità umana e di apprendere autonomamente. Questi elementi rendono l’IA assolutamente innovativa e non realmente paragonabile alle altre tecnologie, anche per l’imprevedibilità che può connotarne talora i processi e per l’autono-

(*) *Presidente Autorità Garante per la Protezione dei Dati Personali; Professore Emerito di Diritto Civile nell’Università di Salerno.*

ma, rispetto alla decisione umana, che spesso può caratterizzarne gli esiti. Quello dello scopo e dei limiti è, dunque, il principale obiettivo da perseguire nel governo della tecnica e soprattutto di quella sua altissima espressione che è l'IA come ben sottolinea questo libro.

L'Europa ha colto questa sfida, delineando (in particolare con lo schema di regolamento sull'IA) una strategia antropocentrica di governo della tecnica, che temperi la *rule of technology*, in tutta la sua autoreferenzialità, con la *rule of law*. Nel promuovere un'innovazione sostenibile sotto il profilo delle garanzie giuridiche, dell'equità sociale, della dignità personale, l'Europa ha investito sul terreno del digitale la propria identità come Comunità di diritto, sottolineando la propria specificità tanto rispetto alla *deregulation* americana quanto rispetto al dirigismo cinese.

Si tratta di una sfida che l'Europa ha colto non da ora, ma già nel 2016 con il GDPR, che regola il fulcro dell'IA: il trattamento di dati personali funzionale a processi decisionali automatizzati e all'addestramento dell'algoritmo.

Rispetto a questo nucleo centrale dell'IA, la disciplina di protezione dei dati offre alcune garanzie essenziali: il principio di conoscibilità (che esclude la legittimità di algoritmi *black-box*, riconoscendo il diritto di ricevere informazioni significative sulla logica utilizzata); quello di non esclusività della decisione algoritmica che impone un intervento umano capace di controllare, validare o smentire la decisione automatizzata; il divieto di discriminazione algoritmica; un generale principio di trasparenza che impone precisi obblighi informativi nei confronti dell'utente; un criterio di qualità ed esattezza dei dati da utilizzare, particolarmente rilevante per evitare i *bias* propri di un addestramento dell'algoritmo sulla base di informazioni inesatte o non sufficientemente rappresentative. Le garanzie particolari accordate nel trattamento dei dati dei minori si sono, inoltre, rivelate determinanti nell'assicurare il doveroso controllo sull'accesso degli infraquattordicenni ad alcuni dei contenuti offerti da questi *chatbot*, ritenuti inadeguati (ad esempio perché sessualmente espliciti) per il loro grado di sviluppo cognitivo, etico, personologico.

L'*Ai Act* rilancia e sviluppa le opzioni di politica del diritto più significative del GDPR, sottendendo alcune scelte importanti, nel metodo e nel merito della normazione, su cui riflettono gli Autori dell'opera, illustrandone alcuni aspetti essenziali.

Da un lato, infatti, è determinante la stessa scelta in favore della regolazione, in un contesto in cui la frequente tendenza alla *deregula-*

tion finisce per delegare alla legge del mercato la definizione del perimetro di diritti e libertà. È una scelta, questa, che caratterizza tutta la politica europea del digitale, dal GDPR sino ai *Data Governance*, *Digital Services* e *Digital Markets Act*, accomunati dall'opzione in favore della fonte regolamentare, che si consolida sempre più come la forma tipica della disciplina europea del digitale. Essa esprime, infatti, quell'aspirazione unitaria ("*one continent, one law*") sottesa a politiche su cui l'Unione investe, anzitutto, la propria identità, proprio come sta facendo sul rapporto tra diritto e tecnica, per imprimere all'innovazione un governo antropocentrico e, di più, personalista (il principio di supervisione umana e le misure volte a contrastare le distorsioni cognitive degli algoritmi sono, in tal senso, significative).

Dall'altro lato, nel merito, l'architettura regolatoria si fonda su di una definizione dell'IA tecnologicamente neutra e lungimirante ("*future proof*") e su di una distinzione (ripresa peraltro dalla direttiva sulla responsabilità civile da IA), dei relativi sistemi sulla base della loro rischiosità secondo una piramide di gravità ascendente.

La stessa tassonomia dei divieti e dei gradi di rischiosità delle applicazioni di IA rievoca i parametri previsti dalla disciplina di protezione dei dati, secondo un'affinità di prospettiva che questo volume analizza in profondità. Il tema centrale, che percorre tutto il libro è, infatti, la sinergia tra regolazione dell'IA e protezione dei dati, funzionale alla promozione di un vero e proprio umanesimo digitale; a una riacquisizione di centralità della persona nel governo della tecnica.

Quest'obiettivo, soprattutto se iscritto all'interno della politica del digitale europea, complessivamente intesa, esprime l'esigenza di rimodulare il perimetro del tecnicamente possibile sulla base di ciò che si ritiene giuridicamente ed eticamente accettabile, temperando — come è stato detto — l'algocrazia con l'algoretica, con effetti anche geopolitici importanti.

Su questo la regolazione europea marca in maniera evidente la propria differenza, qui davvero identitaria rispetto a Stati Uniti e Cina, definiti da Anu Bradford "imperi digitali" per il ruolo a vario titolo svolto nella competizione tecnologica, con l'attitudine (di qui la metafora imperialista) a una proiezione extraterritoriale della propria sfera d'influenza.

Gli Stati Uniti infatti, secondo quest'impostazione, promuovrebbero la tecnologia quale fattore di competitività anche geopolitica, grazie a un approccio regolatorio liberista all'interno e mercantilista all'esterno, in ciò distinguendosi massimamente dal dirigismo cinese.

Quest'ultimo, per parte sua, condizionerebbe i finanziamenti per gli interventi infrastrutturali nei Paesi in via di sviluppo all'acquisto di tecnologie cinesi, "esportando" — con una logica quasi coloniale — non solo tecnologia, ma anche paradigmi normativi (la disciplina cinese dell'IA e dei dati in particolare).

L'Unione europea avrebbe invece tentato, come già con il GDPR, di adeguare l'industria globale al proprio modello di bilanciamento tra innovazione e diritti, attento anche al principio di precauzione e puntando sulla forza del proprio bacino di mercato. Non scevra dall'approccio europeo è, del resto, l'istanza riequilibratrice sottesa al tentativo di responsabilizzazione dei "poteri privati" proprio certamente dell'*Ai Act* ma, già prima, del "pacchetto digitale" complessivamente inteso (*Digital Services* e *Digital Markets Act*, soprattutto), come anche e originariamente del GDPR.

La sfida europea è dunque nel tentare di governare l'innovazione non tanto in maniera astrattamente protezionistica, quanto imprimendole una direzione compatibile con la tutela dei diritti e delle libertà fondamentali, estendendo il proprio modello regolatorio anche oltre i confini del proprio territorio. Come si è detto, se è vero che l'Europa sul piano interno ha fondato la propria identità sul diritto e non sul potere, è altrettanto vero che nelle relazioni internazionali — e nel digitale soprattutto — ha tentato di affermare e costruire il proprio potere sul diritto.

L'Europa persegue, non da ora, quest'obiettivo, nella consapevolezza di come — qui e ora — si delinei (parafrasando Carlo Levi) il "cuore antico" del futuro. Esso, solo, può ancorare — come chiarisce bene il libro — l'innovazione a un limite giuridico, politico, sociale; prima ancora etico, di sostenibilità.