L'intelligenza artificiale, la protezione dei dati e le cooperative di dati e in Argentina

Mauricio BORETTO*

RIASSUNTO: Attraverso il presente documento si cerca di raccogliere e fornire strumenti per coloro che portano avanti progetti di innovazione pubblica attraverso la tecnologia, ma in particolare quelli che importano l'uso dell'intelligenza artificiale. In questo senso, si raccomanda di adottare un approccio multidisciplinare, comprendendo in modo integrale le implicazioni dell'uso, adozione, sviluppo e innovazione pubblica attraverso l'intelligenza artificiale. Il documento è destinato a fornire un quadro per l'adozione tecnologica dell'intelligenza artificiale centrata sul cittadino e sui suoi diritti, concependone l'aspetto sociale e strategico, assicurando un funzionamento ottimale della fornitura di servizi e un approccio etico.

PAROLE-CHIAVE: Intelligenza artificiale; dati personali; cooperative di dati; diritto argentino.

TITLE: *Artificial Intelligence, Data Protection and Data Cooperatives in Argentina*

ABSTRACT: *This document seeks to gather and provide tools for those pursuing public innovation projects through technology, particularly those involving the use of artificial intelligence. In this regard, it is recommended to adopt a multidisciplinary approach, comprehensively understanding the implications of the use, adoption, development, and public innovation through artificial intelligence. The document aims to provide a framework for the technological adoption of artificial intelligence, focusing on citizens and their rights, understanding its social and strategic aspects, ensuring optimal service provision and an ethical approach.*

KEYWORDS: *Artificial intelligence; personal data; data cooperatives; Argentine law.*

* Doctor en Derecho (Universidad Nacional de Córdoba). Profesor titular de la cátedra de Derecho Concursal, Universidad Nacional de Cuyo. Premio de Derecho privado Castán Tobeñas (Academia Aragonesa de Legislación y Jurisprudencia – España). Ganador concurso visiting proffesor/visiting researcher 2022/2023 Universidad de Bari Aldo Moro. Profesor invitado de la Universidad de Salerno. Integrante del Comité Editorial en calidad de redactor de la Revista Italiana "Contrato y Empresa Europa". Director del Seminario "Aprendiendo el Derecho concursal en italiano y en inglés", Facultad de Derecho, Universidad Nacional de Cuyo. Integrante del Instituto de Derecho Empresarial de la Academia de Derecho y Ciencias Sociales en Buenos Aires.

DOI: https://doi.org/10.5281/zenodo.19720753 ISSN: 2316-8374

Prima parte: l'intelligenza artificiale

1. Punto di partenza

L'Argentina non ha una legge sull'intelligenza artificiale.[1]

Tuttavia, il Capo di Gabinetto dei Ministri (attraverso la Segreteria per l'Innovazione Tecnologica) ha elaborato un documento con "Raccomandazioni per un'Intelligenza Artificiale Affidabile".[2]

Nel quadro dell'Agenda Digitale Argentina (2018) e della Strategia Nazionale di Scienza, Tecnologia e Innovazione "Argentina Innovadora 2030" del Ministero della Scienza, Tecnologia e Innovazione, il governo ha emesso a giugno 2019 il *Piano Nazionale di Intelligenza Artificiale ("Plan IA")* con l'obiettivo di posizionare l'Argentina come «leader» regionale nella generazione di politiche che contribuiscano alla crescita sostenibile e al miglioramento delle pari opportunità *attraverso tecnologie di IA* con impatto sulla matrice scientifica, tecnologica, socioeconomica, politica e produttiva.

Nell'aprile 2021, il governo pubblicò il Piano di sviluppo produttivo dell'Argentina 4.0, un'iniziativa del Ministero dello sviluppo produttivo che mirava a promuovere l'incorporazione delle tecnologie 4.0, compresa l'IA, nella catena produttiva nazionale.

L'irruzione dell'Intelligenza Artificiale (AI), che si esprime nella crescente importanza dei dati e degli algoritmi nella vita delle persone, spinge gli Stati a definire strategie per incanalare il potenziale trasformativo di questa tecnologia nella risoluzione di problemi concreti e a favore del bene comune.

Le soluzioni tecnologiche basate sull'IA consentono livelli più elevati di automazione e il passaggio a sistemi decentralizzati e predittivi per il processo decisionale.

Sul piano produttivo, l'IA è promettente per la sua capacità di promuovere l'innovazione, aggiungere valore, aumentare la produttività del lavoro, dare origine a nuovi beni e servizi, potenziare le esportazioni, tra altre possibilità.

Nel settore pubblico, l'IA offre soluzioni che rendono più efficiente la gestione dello Stato e migliorano la progettazione e l'attuazione delle politiche e la fornitura di servizi

[1] F. BONAURA, *Inteligencia artificial, Los desafíos de su regulación en Argentina*, profesional 360, actuación y formación profesional, La Ley, Thomson Reuters, diciembre 2024
[2] Può essere ampliato in servicios.infoleg.gob.ar/infolegInternet/anexos/380000-384999/384656/norma.htm

essenziali in materia di salute, istruzione, sicurezza, trasporti, cura dell'ambiente, ecc. I governi possono anche utilizzare l'IA per migliorare la comunicazione e il coinvolgimento con i cittadini.

In questo senso, lo Stato svolge un ruolo fondamentale non solo promuovendo la ricerca e lo sviluppo di soluzioni IA che siano progettate per soddisfare le reali esigenze delle persone, ma anche garantendo che l'IA sia trasparente, equa e responsabile.

Ciò implica stabilire regole chiare per garantire che i vantaggi di qualsiasi sviluppo tecnologico possano essere sfruttati da tutti i settori della società; promuovere la responsabilità nella raccolta e nell'uso dei dati personali; evitare la discriminazione algoritmica e gestire i rischi dell'uso dell'IA per prevenire il danno.

Attraverso il presente documento si cerca di raccogliere e fornire strumenti per coloro che portano avanti progetti di innovazione pubblica attraverso la tecnologia, ma in particolare quelli che importano l'uso dell'intelligenza artificiale.

In questo senso, si raccomanda di adottare un approccio multidisciplinare, comprendendo in modo integrale le implicazioni dell'uso, adozione, sviluppo e innovazione pubblica attraverso l'intelligenza artificiale.

Il documento è destinato a fornire un quadro per l'adozione tecnologica dell'intelligenza artificiale centrata sul cittadino e sui suoi diritti, concependone l'aspetto sociale e strategico, assicurando un funzionamento ottimale della fornitura di servizi e un approccio etico.

Lo sviluppo e l'implementazione dell'IA può generare sfide, che richiedono che la sua adozione sia progettata seguendo una serie di principi etici in modo tale da mantenere la tutela dei diritti fondamentali, rispettare i valori democratici, prevenire o ridurre i rischi, promuovere l'innovazione e il design incentrato sulle persone.

2. Come è consigliabile concepire l'intelligenza artificiale?

Questo punto è rilevante data la tendenza umana ad antropomorfizzare la tecnologia. In questo senso, un aspetto consigliabile è dato da una chiara distinzione tra i concetti di responsabilità e esecuzione.

Quando si contrattano servizi tecnologici, ciò che viene trasferito al fornitore è l'esecuzione di compiti diversi ma non la responsabilità della loro effettiva realizzazione, con l'intelligenza artificiale accade lo stesso.

Quando si utilizzano algoritmi di intelligenza artificiale, l'esecuzione è trasferita, ma non la responsabilità. Cioè, l'intelligenza artificiale esegue solo un'esecuzione senza intenzione propria e in modo reattivo a una richiesta umana, che ha deciso di programmarla, allenarla e implementarla con un uso specifico al fine di eseguire diverse azioni.

Di conseguenza, un algoritmo non possiede l'autodeterminazione per prendere decisioni liberamente e quindi non può essere considerato responsabile delle azioni che vengono eseguite attraverso tale algoritmo in questione.

In altre parole, affinché una persona umana possa essere legalmente responsabile delle decisioni che prende per compiere una o più azioni, deve esserci discernimento (pieni poteri mentali umani), intenzione (pulsione o desiderio umano) e libertà (per agire in modo calcolato e premeditato).

Pertanto, per evitare di cadere in antropomorfismi che potrebbero ostacolare eventuali regolamentazioni e/o attribuzioni erronee, è importante stabilire la concezione delle intelligenze artificiali come artifici, cioè come tecnologia, una cosa, un mezzo artificiale per raggiungere obiettivi umani ma che non devono essere confusi con una persona umana. Cioè, l'algoritmo può eseguire, ma la decisione deve necessariamente ricadere sulla persona e quindi anche la responsabilità.

3. Principi che tutti gli attori coinvolti devono rispettare

Secondo il governo argentino, nel documento citato – "Raccomandazioni per un'Intelligenza Artificiale Affidabile" – redatto dal Capo di Gabinetto dei Ministri, attraverso la Segreteria per l'Innovazione Tecnologica, sono rilevanti alcuni principi che tutti gli attori coinvolti devono rispettare, e che dovrebbero essere considerati come principi di progettazione, sviluppo, implementazione e utilizzo dell'intelligenza artificiale.

In questo senso, si è tenuto conto che l'Organizzazione delle Nazioni Unite (ONU) attraverso l'Organizzazione delle Nazioni Unite per l'Educazione, la Scienza e la Cultura

(UNESCO) ha emesso la *Raccomandazione sull'Etica dell'Intelligenza Artificiale*, cui hanno aderito tutti i Paesi membri nell'Assemblea generale del novembre 2021, tra cui l'*Argentina*.

Tale raccomandazione contiene una serie di principi che vedremo in seguito.[3]

Proporzionalità e innocuità.
Si dovrebbe riconoscere che le tecnologie IA non garantiscono necessariamente da sole la prosperità degli esseri umani, dell'ambiente e degli ecosistemi. Qualora si possa verificare un danno per gli esseri umani, occorre garantire l'applicazione di procedure di valutazione dei rischi e l'adozione di misure atte a prevenire il verificarsi di tale danno.

Sicurezza e protezione.
Danni indesiderati (rischi per la sicurezza) e vulnerabilità agli attacchi (rischi di protezione) dovrebbero essere evitati e presi in considerazione, prevenirsi ed eliminarsi durante il ciclo di vita dei sistemi IA per garantire la sicurezza e la protezione degli esseri umani, dell'ambiente e degli ecosistemi.

Diritto alla privacy e protezione dei dati.
È importante che i dati per i sistemi di IA siano raccolti, utilizzati, condivisi, archiviati e cancellati in modo coerente con il diritto internazionale e in linea con i valori e i principi enunciati, nel rispetto dei quadri giuridici nazionali, rilevanti a livello regionale e internazionale.

Supervisione e decisione umane.
Può accadere che gli esseri umani scelgano di affidarsi ai sistemi IA per ragioni di efficacia, ma la decisione di cedere il controllo in contesti limitati continuerà a ricadere sugli esseri umani, poiché questi possono ricorrere ai sistemi di IA nel processo decisionale e nell'esecuzione dei compiti, ma un sistema di IA non potrà mai sostituire la responsabilità finale degli esseri umani e il loro obbligo di rendere conto.

Trasparenza e spiegabilità.
La trasparenza e la comprensibilità dei sistemi di IA sono spesso condizioni preliminari fondamentali per garantire il rispetto, la protezione e la promozione dei diritti umani, delle libertà fondamentali e dei principi etici. Le persone dovrebbero avere la possibilità

[3] F. MORANDIN – AHUERMA, *Principios normativos para una ética de la inteligencia artificial*, Consejo de Ciencia y Tecnología de Puebla, ISBN: 978-607-8901-78-4 Primera edición, México, 2023.

di chiedere spiegazioni e informazioni al responsabile dell'IA o alle istituzioni del settore pubblico competenti. Tali responsabili dovrebbero informare gli utenti quando un prodotto o servizio viene fornito direttamente o con l'aiuto di sistemi IA in modo adeguato e tempestivo.

Responsabilità e rendiconto.
Dovrebbero essere sviluppati meccanismi adeguati di monitoraggio, valutazione d'impatto, audit e due diligence, anche per quanto riguarda la protezione degli informatori, per garantire la responsabilità dei sistemi di intelligenza artificiale e del loro impatto lungo tutto il ciclo di vita.

Sensibilizzazione e educazione.
La sensibilizzazione e la comprensione del pubblico riguardo alle tecnologie dell'IA e al valore dei dati dovrebbero essere promosse attraverso un'educazione aperta e accessibile, la partecipazione civica, le competenze digitali e la formazione in materia di etica nell'uso dell'IA, l'alfabetizzazione mediatica e informativa e la formazione gestita congiuntamente da governi, organizzazioni intergovernative, la società civile, le università, i media, i leader comunitari e il settore privato, tenendo conto della diversità linguistica, sociale e culturale esistente, al fine di garantire un'effettiva partecipazione pubblica.

Governance e collaborazione adattative tra più parti interessate.
Il coinvolgimento di diverse parti interessate lungo tutto il ciclo di vita dei sistemi IA è necessario per garantire approcci inclusivi alla governance dell'IA. Tra questi, i governi, le organizzazioni intergovernative, la comunità tecnica, la società civile, i ricercatori e gli ambienti universitari, i media, i responsabili dell'istruzione, responsabili politici, imprese del settore privato, istituzioni per i diritti umani e organismi di promozione della parità, organi di controllo contro la discriminazione e gruppi di giovani e bambini, tra gli altri.

4. Aspetti etici da considerare nel ciclo dell'IA[4]

Allo stesso modo e anche secondo le "Raccomandazioni per un'Intelligenza Artificiale Affidabile" –redatto dal Capo di Gabinetto dei Ministri, attraverso la Segreteria per l'Innovazione Tecnologica– ci sono "*Aspetti etici da considerare nel ciclo dell'IA*".

[4] Può essere ampliato in *Instituto para el futuro de la educación, Observatorio Tecnológico de Monterrey*: https://observatorio.tec.mx/edu-news/principios-eticos-de-la-educacion-con-inteligencia-artificial-ia/; Blog de los Estudios de Informática, Multimedia y Telecomunicación de la Universitat Oberta de Catalunya: https://blogs.uoc.edu/informatica/es/cinco-principios-inteligencia-artificial-etica/

Poiché gli aspetti etici sono specifici per le persone, in ogni fase del ciclo di vita dell'IA si deve garantire che le persone che compongono il team responsabile della progettazione conoscano e comprendano i necessari aspetti etici fondamentali coinvolti.

Fase n° 1: Progettazione e modellazione dei dati

Questa è la prima fase del ciclo di vita dell'IA. Si inizia con la progettazione dei dati e dei modelli coinvolti. È importante che fin da questa prima fase siano inclusi come criteri di progettazione aspetti etici che facilitino il rispetto dei principi definiti e aumentino di conseguenza le probabilità di successo del progetto.

Punto di partenza comune per il team multidisciplinare e diversificato.

Poiché ogni persona in un team multidisciplinare e diversificato ha competenze diverse con esperienze diverse, è consigliabile concordare chiaramente l'obiettivo del progetto. Di conseguenza, ogni singola persona che fa parte del gruppo deve conoscere, comprendere, concordare e impegnarsi a realizzare i seguenti aspetti minimi:

a. I principi di progettazione, sviluppo, implementazione e uso etico dell'intelligenza artificiale definiti dall'UNESCO.
b. L'impatto sulla società in generale e le esigenze da soddisfare nei destinatari in particolare.
c. I rischi potenziali valutati per livello di impatto e probabilità di verificarsi, e i trattamenti definiti per ciascuno di essi.
d. I meccanismi di trasparenza e responsabilità da utilizzare per la tracciabilità e l'audit (sia quello eseguito dalle macchine e/o deciso dalle persone).
e. Il ruolo, la portata delle attività e la ripartizione delle responsabilità di ogni persona che fa parte del team.
f. La definizione e l'assegnazione formale della persona responsabile di garantire la sostenibilità del progetto nel tempo.
g. La comprensione e il rilevamento dei diversi profili di persone destinatarie (contribuenti, dipendenti pubblici, beneficiari di sicurezza sociale, studenti, pazienti, ecc.). Questo include gli aspetti che potrebbero eventualmente portare a diversi pregiudizi. Si raccomanda inoltre che ciascuno di questi profili sia rappresentato da almeno una persona.

h. La rilevazione e comprensione delle dimensioni, implicazioni e impatto della normativa in questione.
i. La documentazione, la registrazione e la socializzazione dell'esperienza per promuovere le buone pratiche e gli insegnamenti necessari per l'apprendimento organizzativo e l'innovazione pubblica.
j. I dati sono la materia prima per costruire il modello addestrato di intelligenza artificiale che verrà utilizzato in modo che, inserendo diversi input, si ottenga una risposta corretta.

In questo senso, i diversi aspetti che seguono devono essere considerati per poter realizzare un disegno etico dei dati.

a. *La classificazione dei dati in base alla loro riservatezza.*

Si raccomanda che tale classificazione sia concordata e che sia elaborata sulla base di norme internazionali relative alla sicurezza delle informazioni. A titolo di esempio, viene delineata una classificazione generale concordata a livello internazionale.

- *Dati riservati*. Si riferisce a quei dati o informazioni sensibili che possono riguardare questioni di intelligence, difesa, sicurezza e simili.
- *Dati personali*. Si riferisce a quei dati o informazioni delle persone che sono state specificamente definite come tali dalla normativa vigente.
- *Dati interni*. Si riferisce a quei dati o informazioni di gestione interna, che non risultano né riservati né personali ma che non catalogano come informazione pubblica
- *Dati pubblici*. Si riferisce a quei dati o informazioni di pubblico dominio che sono generalmente disponibili, sia come set di dati aperti, e/o contenuti in siti web.

b. Le fonti di dati che saranno utilizzate per progettare e costruire il set di dati corrispondente alla formazione del modello.

i. *Dati disponibili su internet*. Il caso meno costoso, tuttavia, si deve tener conto che vi è un alto grado di probabilità che essi siano imprecisi, possiedano pregiudizi di diverso tipo, possano essere oggetto di proprietà

intellettuale, tra vari aspetti che non solo degradano la qualità dei dati, ma impediscono anche di creare dati di allenamento in modo etico.

ii. *Dati esistenti nell'organizzazione.* In questo caso, è necessario dimensionare i costi associati: prima dell'uso si deve prendere in considerazione la classificazione secondo la loro riservatezza, diritti di utilizzo, consenso dei titolari, possibilità di rendere anonimi tali dati e altri aspetti previsti dalla normativa vigente.

iii. *Dati richiesti da terzi.* In questo caso, anche i costi associati devono essere dimensionati, poiché non sono disponibili su internet, e per ottenerli e utilizzarli si deve tener conto della classificazione secondo la loro riservatezza, diritti di utilizzo, consenso del titolare, la tracciabilità di tutto il processo di raccolta e creazione dei dati per la formazione e altri aspetti stabiliti dalla normativa vigente.

c. La qualità dei dati.

In tutti i casi, la qualità dei dati deve essere garantita.

- Ad esempio, evitando l'esistenza di pregiudizi, verificare che siano precisi o riflettano la realtà che intendono rappresentare, tra le altre.
- Questo trattamento deve essere effettuato da professionisti delle scienze dei dati, che devono valutare continuamente i diversi set di dati per garantire che l'addestramento dei modelli IA sia eseguito secondo i principi dell'UNESCO sopra citati.

I modelli devono essere progettati in modo da non introdurre pregiudizi propri della loro concezione. Ad esempio, attraverso una definizione che omette aspetti del contesto che privilegiano o danneggiano le persone rispetto alle altre, oppure utilizzando algoritmi che funzionano meglio con determinate variabili o caratteristiche rispetto ad altre, che potrebbero generare eventuali imprecisioni o distorsioni nei risultati.

In linea con i principi dell'UNESCO, i modelli devono essere trasparenti e spiegabili. Cioè, l'esecuzione che ha portato al risultato deve poter essere compresa dalle persone che gestiscono tali sistemi, affinché queste possano a loro volta prendere decisioni con questi risultati, e inoltre per poter spiegare chiaramente alle persone interessate dalla decisione presa o a terzi come si è giunti a tale risultato.

Fase n° 2: Verifica/Convalida

In una seconda fase, all'interno del ciclo di vita dell'IA, è importante effettuare le verifiche e le validazioni corrispondenti dei progetti realizzati nella prima fase.

Per fare questo, si deve prendere in considerazione la progettazione delle attrezzature, dei dati e dei modelli coinvolti. Queste verifiche e validazioni sono effettuate tenendo conto sia dei principi definiti dall'UNESCO, sia dell'interazione delle persone destinatarie con i prototipi progettati (prime soluzioni concettuali del o dei modelli formati), in condizioni simili a quelle che avrà la sua attuazione definitiva.

Come vengono convalidate le conoscenze etiche specifiche necessarie per il progetto IA? Etica dei dati

Gli insiemi di dati appositamente costruiti per l'addestramento dei modelli di intelligenza artificiale devono essere convalidati prima dell'implementazione sul campo. Il personale del team che è un professionista della scienza dei dati deve essere responsabile della valutazione della qualità dei dati da utilizzare per l'addestramento dei modelli di IA.

Deve essere stabilita una classificazione del rischio (ad esempio, di tre livelli tipo semaforo o con valori da uno a cinque) per quanto riguarda la conformità ai principi dell'UNESCO sopra citati.

Come vengono convalidati gli aspetti etici dei modelli di IA?

Le prove con prototipi devono essere eseguite da professionisti con conoscenze di metodologie agili ed è consigliabile che il team multidisciplinare e diversificato responsabile del progetto sia presente nella realizzazione delle stesse.

In questo caso, i modelli addestrati saranno anche convalidati in condizioni simili a quelle che avranno nella loro attuazione. Per eseguire tali prove si utilizzeranno uno o più prototipi dei modelli addestrati, con un'interfaccia utente minima ma di aspetto simile a quella definitiva.

Per testare i modelli, almeno una persona di ogni profilo definito sarà invitata affinché il team possa osservare come viene utilizzato il modello e sfruttare tale interazione per

verificare diversi aspetti etici del design. Ad esempio, che non vi siano pregiudizi, che la persona responsabile della decisione possa comprendere il risultato dell'esecuzione del modello (nel caso del modello di adozione umano-macchina), che possa essere spiegato in modo semplice alle persone interessate, convalidando che essi comprendano chiaramente il risultato del modello e la conseguente decisione umana.

Cioè, in questo test con prototipi, saranno convalidati diversi aspetti etici quali; la congruenza tra i risultati e le aspettative del progetto; l'assenza di pregiudizi; la spiegabilità del modello; e altri aspetti etici del design che possono essere migliorati.

Deve essere stabilita una classificazione del rischio (ad esempio, tre livelli di semaforo o valori da uno a cinque) rispetto a quanto sono conformi ai principi dell'UNESCO sopra citati.

Come vengono registrate le verifiche/validazioni?

Tutte le azioni e decisioni prese nell'ambito di un progetto di IA, comprese quelle relative alle verifiche e convalide degli aspetti etici effettuate nella fase di progettazione, devono essere registrate.

Questo punto è critico per poter rispettare i principi relativi alla trasparenza e responsabilità delle azioni e decisioni coinvolte in ogni progetto di IA.

Deve essere utilizzato un mezzo di registrazione formale che consenta la tracciabilità e l'audit di tutte le azioni di verifica e convalida.

Fase n° 3: Attuazione

In questa fase entrano in gioco i professionisti delle infrastrutture che fanno parte del team multidisciplinare e diversificato del progetto IA. In questo caso, esistono opzioni di implementazione che possono essere basate sull'acquisto di servizi cloud, sulla distribuzione di infrastrutture proprie o su una soluzione che contempli entrambe le opzioni.

In ogni caso, si dovrà garantire che l'implementazione permetta di: stabilire un adeguato grado di sicurezza delle informazioni; tracciare le azioni e le decisioni avvenute nel progetto identificando le persone che le hanno eseguite; effettuare audit (questo punto è

particolarmente importante quando si acquistano servizi cloud) e offrire all'utente facilità di accessibilità alle tecnologie dell'informazione e della comunicazione (TIC).

Come stabilire un livello adeguato di sicurezza delle informazioni?

È importante che siano adottate le migliori prassi in materia di sicurezza delle informazioni. A tal fine, i responsabili della sicurezza delle informazioni che formano il team di lavoro diversificato e multidisciplinare dovranno tener conto dei seguenti aspetti:

a. La comprensione, conoscenza e portata degli standard internazionali e delle normative e delle migliori pratiche in materia di sicurezza delle informazioni.
b. La rilevazione, conoscenza e comprensione della normativa vigente in materia di sicurezza delle informazioni.
c. L'utilizzo di applicazioni accessorie incaricate della gestione dei registri (*loggings*, eventi, ecc.) dei sistemi coinvolti in modo tale da facilitare il trattamento di eventuali incidenti di sicurezza; automatizzare la creazione di report di audit; e migliorare la trasparenza attraverso il controllo delle persone che accedono ai sistemi, alle applicazioni e alle apparecchiature.
d. Eseguire diversi test per individuare vulnerabilità alla sicurezza che potrebbero causare incidenti indesiderati.
e. La partecipazione dell'area o dell'autorità con responsabilità primaria in materia di sicurezza delle informazioni, che comprende tutti gli aspetti relativi alla cibersicurezza e alla protezione delle infrastrutture critiche dell'informazione, nonché alla generazione di capacità di prevenzione, rilevamento, difesa, risposta e recupero in caso di incidenti di sicurezza informatica. Ciò è particolarmente importante nel caso in cui l'istituzione che adotta lo sviluppo basato sull'IA abbia un'area specifica di sicurezza delle informazioni.

Quali aspetti devono essere presi in considerazione per stabilire la tracciabilità?

I sistemi coinvolti nella realizzazione dell'infrastruttura per l'implementazione del progetto di IA, così come le procedure definite per la loro gestione, devono possedere mezzi adeguati per registrare tutte le azioni eseguite nel sistema (Aumenti, diminuzioni, modifiche alle impostazioni) per tutte le gerarchie e tutti i profili utente (amministratore,

operatore, utenti, ecc.), in modo da poter identificare fedelmente tutte le persone che hanno portato a termine le varie azioni e decisioni nel progetto.

Quali aspetti devono essere presi in considerazione per rendere i sistemi auditabili?

Per garantire il rispetto dei principi etici è necessario sottoporre a audit il modello e la tracciabilità è lo strumento migliore per raggiungere questo obiettivo. È fondamentale essere in grado di identificare e comprendere il record di azioni, decisioni e/o qualsiasi altro evento che influisce sui sistemi coinvolti nel progetto IA.

- Nel caso di implementazione di soluzioni on premise (all'interno dell'infrastruttura dell'organizzazione), è importante garantire, oltre al controllo dell'accesso ai sistemi, il controllo dell'accesso fisico in cui è ospitata l'infrastruttura coinvolta.
- Nel caso di una distribuzione tramite servizi cloud, è importante comprendere le possibilità di audit offerte dai fornitori di servizi cloud prima dell'appalto, per poter comprendere se la portata offerta permette di strumentare i principi etici corrispondenti a tale materia.

Quali aspetti devono essere presi in considerazione per rendere i sistemi accessibili alle TIC?

Le migliori pratiche in materia di accessibilità delle TIC devono essere attuate, sia attraverso siti web che applicazioni mobili. A tal fine, i professionisti responsabili dell'accessibilità delle TIC, che formano il team di lavoro diversificato e multidisciplinare, dovranno tener conto dei seguenti aspetti:

a. La sostituzione, conoscenza e comprensione della portata delle norme internazionali e le migliori pratiche in materia di accessibilità TIC.
b. Il rilievo, la conoscenza e la comprensione della portata delle normative nazionali in materia di accessibilità TIC.
c. La valutazione del sito *web*. Nel caso particolare dell'accessibilità *web*, si raccomanda di utilizzare applicazioni specifiche disponibili per valutare l'accessibilità dei siti *web* che gli utenti utilizzeranno per accedere ai sistemi coinvolti in modo tale da garantire un livello minimo di accessibilità (livello A).

Si raccomanda inoltre di richiedere l'assistenza dell'autorità di applicazione della legge 26.653 (*di acceso alle informazioni pubbliche*) sull'accessibilità del *web*.

Fase n° 4: funzionamento e manutenzione

I progetti di innovazione tecnologica non terminano con l'implementazione; la gestione e la manutenzione rappresentano la fase finale del ciclo di vita dell'IA.

Un problema frequente è che queste due azioni, nonostante la loro importanza, spesso non sono prese in considerazione nella progettazione dei progetti.

Questi compiti sono le operazioni e la manutenzione sia dell'infrastruttura in cui è implementata la soluzione tecnologica basata su IA, sia del modello stesso, dato che, per esempio, spesso i modelli si degradano e smettono di rispondere correttamente.

Tali azioni consentono la disponibilità, la continuità e la sostenibilità del servizio fornito attraverso la soluzione di IA.

Come si potrebbe effettuare un monitoraggio e cosa dovrebbe essere monitorato considerando l'uso etico dell'IA?

Il monitoraggio è un'azione che viene eseguita in questa fase per assicurarsi che tutto funzioni come previsto. Si possono monitorare diverse variabili che saranno scelte in base allo scopo perseguito. Ad esempio, se si cerca di capire se il modello risponde come è stato validato nei test con prototipi, è possibile monitorare le sue prestazioni attraverso la misurazione di diversi parametri in modo automatico e in modo manuale, cioè condotta da persone che ispezionano e valutano il comportamento del modello.

Quali aspetti generali dovrebbero essere considerati per quanto riguarda l'esistenza di Incidenti di natura etica?

Gli incidenti etici possono essere causati da diversi motivi. Ad esempio, possono essere causati da un errore umano involontario in una delle fasi del ciclo di vita che provoca un malfunzionamento in una o più tecnologie coinvolte, un uso intenzionale e improprio di una o più persone all'interno dell'organizzazione, un uso improprio degli utenti finali, un attacco alla sicurezza dell'organizzazione (interno e/o esterno), tra gli altri.

Se i principi e le raccomandazioni contenute nel presente documento sono stati recepiti, si hanno le basi minime per poter dare un corretto trattamento a un eventuale incidente etico qualunque sia la sua causa.

Poiché il verificarsi di incidenti non può essere eliminato, la documentazione corretta e completa degli stessi sarà un input fondamentale per poter tenere conto dei dettagli e delle condizioni in cui si sono verificati.

Successivamente, tali registri saranno utili per compilare i rapporti di rendicontazione necessari e rispettare i principi definiti dall'UNESCO.

Il trattamento degli incidenti permette di imparare da essi per evitare che si ripetano, mettendo in evidenza quegli aspetti che hanno fallito per poterli correggere.

5. Un caso particolare: responsabilità per i danni causati dalla commercializzazione o dall'uso di sistemi di IA

Come abbiamo già spiegato, in Argentina, attualmente non esiste una regolamentazione specifica sull'IA né sulla responsabilità per i danni causati dalla commercializzazione o dall'uso di sistemi di IA.

Per quanto riguarda la responsabilità per i danni causati, in assenza di un quadro normativo specifico, Argentina applica le norme del Codice Civile e Commerciale della Nazione (2015, di seguito CCyC) relative alla responsabilità civile.

In questo senso, gli articoli 1757 e 1758 CCyC stabiliscono la responsabilità derivante dall'intervento di cose ed attività che sono per loro natura rischiose o pericolose.[5]

In base a queste disposizioni:

- sia il proprietario che il custode della cosa (*sistema IA*) sono responsabili per i danni causati dal loro rischio o pericolo, nonché per le attività che sono rischiose o pericolose per natura, per i mezzi utilizzati e per le circostanze della sua esecuzione.

[5] A. KEMELMAJER DE CARLUCCI y M. BORETTO, *Manual de derecho privado*, T II, Bs. As., Eudeba, Rubinzal-Culzoni, 2016, p. 205 y sigtes.

- la responsabilità è oggettiva e l'autorizzazione amministrativa per l'uso della cosa o l'esecuzione dell'attività, o il rispetto delle tecniche di prevenzione, non esonera dalla responsabilità.

Tuttavia, è importante sottolineare che in Argentina l'IA come tecnologia non regolamentata non richiede alcuna autorizzazione amministrativa prima del lancio sul mercato.

D'altra parte, è importante chiarire che il termine "guardiano" di cui all'art. 1758 citato, si riferisce a colui che ha il controllo e direzione di una cosa, sia da sé o attraverso terzi, e chi trae beneficio dal suo uso. Nel caso di attività rischiosa o pericolosa, la responsabilità ricade sulla persona che la svolge, la utilizza o ne trae beneficio, sia essa stessa o tramite terzi.

Pertanto, quando si tratta di un sistema IA che comporta rischi o pericoli intrinseci, si applicano le disposizioni sopra menzionate.[6]

Inoltre, l'art. 1710 CCyC stabilisce un obbligo generale di *prevenire i danni*, il che significa che il controller del sistema IA deve prendere misure ragionevoli per evitare che si verifichi un danno ingiustificato, ridurre la sua entità e non aggravare il danno se è già avvenuto.

Esiste un caso in cui si ritiene che non vi sia alcun dubbio che il fattore di attribuzione è oggettivo. Si tratta del caso degli incidenti stradali provocati da veicoli autonomi, che sono guidati da IA.[7]

La ragione per sostenere questa posizione è la disposizione dell'art. 1769 CCyC in cui si effettua in modo chiaro un riferimento agli arts. 1757 e 1758 del CCyC in caso di danni causati dalla circolazione dei veicoli. Non effettuando questa norma una distinzione tra i veicoli guidati da persone umane e quelli che si spostano in modo autonomo, consideriamo che questi ultimi sono inclusi nella normativa di riferimento, che implica che la base per rispondere in questi casi è il rischio creato. Analogamente, rientrerebbero

[6] I. E. ALTERINI, *La legislación argentina frente a la IA*, columna de opinión diario La Nación, 14 agosto de 2024.
[7] M. F. BLANCO PIGHI y M. MACHADO, *El factor de atribución en la responsabilidad por daños causados por la inteligencia artificial* https://www.austral.edu.ar/wp-content/uploads/2024/09/Comision-3-Derecho-de-danos-1.pdf?x44142&x44142.

nella definizione di automobile e veicolo a motore dell'art. 5 della legge 24.449 (legge di transito nazionale) i veicoli autonomi.

Quindi non ci sono dubbi sull'applicazione di questo regime in Argentina.

Per quanto riguarda gli altri casi, si dovrà specificare nel caso specifico se ci troviamo di fronte ad una situazione che può essere inclusa negli art. 1757 e 1758, che implicherebbe l'esistenza di un rischio creato. Ci possono essere casi in cui la responsabilità è soggettiva. Quindi, dobbiamo fare alcuni chiarimenti.

Il concetto di "cosa rischiosa" si basa su un criterio "statistico". Se il rischio consiste nella potenzialità dannosa della cosa, allora sono tali quelle che producono danni frequentemente, regolarmente, secondo quello che di solito succede secondo l'ordine naturale degli eventi. Dovrebbero essere aggiunti al catalogo anche gli elementi che, pur non causando danni di solito, possono causare danni di grande entità. Allo stesso modo, è stato sostenuto che il rischio dell'attività può essere individuato da un criterio quantitativo o statistico, alla ponderazione di standard stabiliti dal legislatore e ragionevolmente attenendosi alle regole dell'esperienza.

L'esistenza del rischio deve essere valutata secondo gli standard fissati dalla teoria della causalità adeguata.

In questo modo, il caso in esame deve essere esaminato secondo questi parametri.

Per questo motivo, non sarà possibile fornire una risposta generica per specificare quale sia il fattore di attribuzione applicabile in tutte le situazioni in cui è stato causato un danno da parte dell'IA.

Ciò implica che si dovrà analizzare ogni singolo caso specifico in cui si applica questo meccanismo, per determinare, caso per caso, se ci troviamo di fronte a una situazione di responsabilità oggettiva o soggettiva.

Tuttavia, si possono fare alcune precisazioni per inquadrare certe situazioni all'interno o al di fuori dell'ambito del rischio creato.

In effetti, esistono sistemi di IA ad alto rischio in cui il fattore di attribuzione della responsabilità è obiettivo (dalla natura stessa dell'attività). Ad esempio, i sistemi di

identificazione biometrica, quelli relativi all'amministrazione della giustizia e ai processi democratici, ecc.

Al contrario, ci possono essere altri casi in cui la responsabilità è soggettiva nei quali dovrà essere dimostrata l'esistenza di dolo o colpa dell'utente o del titolare del sistema IA. Riteniamo che, nel caso dei secondi, sarà necessario dimostrare l'esistenza di un qualche tipo di controllo o servizio di supporto del bene o servizio per imputare la responsabilità.

Da questo punto di vista, parte della dottrina argentina[8] ha applicato alla responsabilità soggettiva per i danni causati dai sistemi di IA la giurisprudenza del Massimo Tribunale argentino collegata alla responsabilità dei motori di ricerca su internet, nelle situazioni in cui non adottano una condotta diligente dopo essere stati debitamente informati dell'esistenza di contenuti dannosi che sono indicizzati attraverso i loro algoritmi.[9]

In questo modo, l'operatore di IA non sarebbe responsabile per uno dei seguenti motivi:

> a) il sistema IA è stato attivato senza la loro conoscenza, adottando tutte le misure ragionevoli e necessarie per evitare tale attivazione al di fuori del controllo dell'operatore; o
> b) la dovuta diligenza è stata osservata attraverso l'esecuzione delle seguenti azioni: la selezione di un sistema IA appropriato per i compiti e le capacità adeguate, la corretta messa in funzione del sistema IA, il controllo delle attività e la manutenzione dell'affidabilità operativa mediante l'installazione periodica di tutti gli aggiornamenti disponibili.

Finalmente, dal punto di vista della legge *per la tutela dei consumatori No 24.240* (1993), l'art. 40 stabilisce che i produttori, i fabbricanti, gli importatori, i distributori, i fornitori, venditori e chiunque abbia messo il loro marchio sulla cosa o servizio saranno solidalmente responsabili se il consumatore subisce un danno a causa di un difetto o rischio della cosa o prestazione del servizio. Tuttavia, coloro che possono dimostrare che la causa del danno è stata estranea a loro possono essere esonerati in tutto o in parte dalla responsabilità.

---

[8] M. F. BLANCO PIGHI y M. MACHADO, *El factor de atribución en la responsabilidad por daños causados por la inteligencia artificial* https://www.austral.edu.ar/wp-content/uploads/2024/09/Comision-3-Derecho-de-danos-1.pdf?x44142&x44142

[9] Corte Suprema de Justicia Nación (Argentina), "R., M. B. c. Google Inc. s/ daños y perjuicios" 28/10/2014 Cita online: LALEY AR/JUR/50173/2014 y "G., C. V. c. Google Inc. s/ daños y perjuicios 12/09/2017 Cita Online: AR/JUR/60631/2017

Questo è particolarmente rilevante quando si tratta di utilizzare i sistemi IA nel contesto delle relazioni con i consumatori.

Infatti, in Argentina, è chiaro che si può attribuire responsabilità a tutta la catena di commercializzazione di un bene o servizio collegato con meccanismi di intelligenza artificiale, purché il danno sia causato ad un consumatore da parte del fornitore, a motivo del rischio o vizio del servizio o dell'attività (art. 40, legge 24.240).

Bozza di Codice di Difesa del Consumatore (2024).

Anche se non è ancora legge in vigore, è interessante descrivere i principi sanciti nel Progetto di Codice di Difesa del Consumatore presentato nel 2024 al Parlamento argentino, in materia di IA. Va notato che, detto progetto, è in fase di analisi.

- Articolo 3. *Principi negli ambienti digitali*. Fatta salva l'applicazione dei principi indicati nell'articolo precedente, negli ambienti digitali valgono i seguenti principi: a) neutralità tecnologica, affidabilità e inclusione; b) una protezione rafforzata contro le nuove tecnologie, in particolare per quanto riguarda i dati personali del consumatore e *l'uso da parte del fornitore di sistemi di intelligenza artificiale o di contratti autoeseguibili*; c) di trasparenza digitale. Il fornitore deve garantire la tracciabilità, la spiegabilità, la comprensione, la trasparenza e *l'intermediazione umana dei sistemi di intelligenza artificiale* o simili che utilizza nell'ambito del rapporto di consumo; d) *di non essere destinatario di decisioni basate unicamente sul trattamento automatizzato dei dati personali*.

- Articolo 15. Informazioni nell'ambito dell'utilizzo di mezzi tecnologici automatizzati. *Quando si utilizzano sistemi di intelligenza artificiale* o qualsiasi altra tecnologia che determinano un processo decisionale parzialmente automatizzato durante il rapporto con il consumatore, devono essere fornite informazioni chiare, precise, complete, veritiere e comprensibili su:
  a) La realizzazione del trattamento automatizzato dei dati nel rapporto di consumo.
  b) La finalità specifica del trattamento automatizzato dei dati.
  c) Tipi di dati trattati.
  d) Se sono usati per rilevare emozioni, o determinare categorie o profili digitali.
  e) Se il contenuto è generato o manipolato in modo automatizzato durante il rapporto di consumo e lo scopo di esso.

  I fornitori devono predisporre mezzi adeguati a consentire ai consumatori di accedere a informazioni supplementari durante l'intero rapporto di consumo.

- Articolo 27. Attenzione al consumatore. Il *trattamento dignitoso* comprende l'obbligo di attenzione al consumatore, adeguato alle sue condizioni di vulnerabilità o di vulnerabilità aggravata e *il diritto all'intermediazione umana quando si utilizzano sistemi di intelligenza artificiale o equivalenti.*

  - Il fornitore deve disporre di risorse e procedure sufficienti per ricevere le richieste che gli vengono rivolte, ascoltare, informare e consigliare il consumatore, ricevere i suoi reclami e dargli una risposta adeguata e in tempo ragionevole.
  - Non potrà rifiutare di ricevere note di reclami o richieste di informazioni che i consumatori desiderano presentare agli uffici di assistenza, dando prova della loro ricezione.
  - In base alle circostanze, il fornitore deve abilitare centri di assistenza con accesso reale ed effettivo, dotandosi per questo personale qualificato e infrastrutture adeguate.

  Nei casi in cui siano coinvolti sistemi di intelligenza artificiale, il fornitore deve offrire le procedure di informazione e consultazione tramite forma scritta, elettronica o digitale.

- Articolo 34. Responsabilità e sanzioni. *I soggetti raggiunti da questa Sezione godono della tutela preventiva e risarcitoria nei confronti del fornitore a seguito delle pratiche abusive* sopra descritte. La responsabilità è solidale e si proietta anche su chi agisce in suo nome, sia o non un professionista liberale, e non esclude altre sanzioni amministrative. Nell'ambito delle pratiche abusive, la sanzione punitiva prevista dall'articolo 132 del presente Codice dovrà essere particolarmente valutata, attenta all'inficiazione di diritti fondamentali o diritti umani.

Seconda parte: la protezione dei dati e le cooperative di dati

1. Punto di partenza

La disciplina giuridica delle *data cooperatives* è contenuta nel recente regolamento dell'UE dedicato alla *Governance* europea dei dati (Reg. UE 2022/868, *Data Governance Act*), ove tali soggetti sono inquadrati nell'ambito della categoria dei

fornitori di servizi di intermediazione di dati.[10] Si tratta però di intermediari di dati del tutto *sui generis*, in quanto fondano il proprio modello di funzionamento su base mutualistica, aggregano dati di interessati (*data subjects*) o imprese di piccole e medie dimensioni (SMEs), che fanno attivamente parte della cooperativa di dati, contribuendo a decidere democraticamente le modalità di (ri)utilizzo dei dati conferiti a fattor comune.[11]

Il modello emergente in sede europea è innovativo, sia perché ha l'ambizione di creare nuovi *competitors* rispetto ai *big players* operanti nel settore delle nuove tecnologie,[12] sia perché, grazie all'approccio mutualistico, si pone come operatore maggiormente virtuoso, in grado di valorizzare meglio – e con logiche partecipative e democratiche – i dati (personali e non personali) che vengono conferiti dai membri della cooperativa.[13]

Dal confronto con gli studiosi di Paesi extra-UE è sorta l'idea di indagare l'esportabilità del modello europeo di cooperativa di dati anche in altri ordinamenti.

In questa direzione, scopo del presente lavoro è, innanzitutto, quello di verificare se ed in che modo il modello europeo delle cooperative di dati possa essere eventualmente proposto [ed applicato] in ordinamenti extra-UE, con particolare riferimento all'ordinamento argentino. Ci si propone, inoltre, di analizzare, alla luce delle soluzioni emergenti nell'ordinamento argentino, eventuali elementi che possano portare a modifiche migliorative del modello europeo, *de jure condito* in via interpretativa o *de jure condendo*.

L'indagine viene condotta avendo riguardo anche all'esplorazione dei possibili ambiti di applicazione del modello mutualistico delle cooperative di dati, tenendo conto dei differenti contesti applicativi emergenti in Europa e in Argentina.

---

[10] Cfr. artt. 10 ss. del *Data Governance Act*. In generale, sul tema si rinvia a F. BRAVO, *Intermediazione di dati personali e servizi di* data sharing *dal GDPR al* Data Governance Act, in *Contratto e impresa Europa*, 2021, 1, pp. 199-256.

[11] Si veda, *amplius*, *infra*, par. 2, nonché F. BRAVO, *Le cooperative di dati*, in *Contratto e impresa*, 2023, 3, pp. 757-799; ID., *Data Cooperatives*, in F. BRAVO (a cura di), *EU Data Cooperatives*, cit., pp. 1-37.

[12] Ved. COMMISSIONE EUROPEA, *Una strategia europea per i dati*, comunicazione al Parlamento europeo, al Consiglio, al Comitato economico e sociale e al Comittato delle Regioni, Bruxelles, 19 febbraio 2020 [COM(2020)66 final], a cui si aggiunge anche la Risoluzione del Parlamento europeo del 25 marzo 2021, intitolata anch'essa «*Strategia europea per i dati*» [P9_TA(2021)00098] (2021/C 494/04), nella quale, al par. 25, viene riconosciuto «il ruolo fondamentale degli intermediari dei dati in quanto facilitatori strutturali dell'organizzazione dei flussi di dati», accogliendo «favorevolmente i piani della Commissione per la classificazione e la certificazione degli intermediari in vista della creazione di ecosistemi di dati interoperabili e non discriminatori» ed invitando «la Commissione a garantire l'interoperabilità attraverso lo sviluppo di criteri minimi tra intermediari di dati; esorta la Commissione a collaborare con le organizzazioni europee e internazionali di normazione per identificare e colmare le lacune in materia di normazione dei dati».

[13] Sull'approccio mutualistico cfr. F. BRAVO, *Data Cooperatives*, cit., pp. 7 ss., nonché L. PETRONE, *Il mercato digitale europeo e le cooperative di dati*, in F. BRAVO (a cura di), *EU Data Cooperatives*, cit., pp. 38 ss.

2. Le cooperative di dati nell'ordinamento argentino. Una nuova sfida

2.1. Introduzione

In Argentina, il punto di partenza deve essere che, il fenomeno giuridico della cooperativa dei dati, non esiste. Siamo di fronte a un tema assolutamente nuovo.

In questo modo, la premessa da cui dobbiamo partire è il seguente interrogativo: è possibile "importare" questa figura dall'Europa per essere applicata nella Argentina quando, nel quadro del diritto argentino in vigore, la cooperativa *di dati* non è regolata dalla legge sulle cooperative (20337/1973), né da nessun'altra legge.

In altri termini, è possibile disporre di dati in Argentina –*attraverso una cooperativa*– come avviene in Europa (ai sensi del regolamento 2022/868); *assumendo la cooperativa in questione la funzione di intermediario di dati*?

Crediamo che, per trovare una risposta a questo interrogativo, dobbiamo prima analizzare se il diritto argentino in vigore «permette» il *trattamento di dati*, l'*intermediazione di dati* e, in caso affermativo, *sotto quali condizioni*.

Si tratta di sapere, insomma, se una cooperativa regolata dalla legge 20337 può avere come oggetto sociale lo svolgimento delle seguenti attività: *raccolta, gestione, scambio e utilizzo di dati (personali o no) con uno o più obiettivi specifici; in altre parole, se può adottare il profilo di un intermediario dei dati nella misura in cui facilita lo scambio di dati tra un numero indeterminato di titolari e i loro potenziali utenti*.

2.2. Qual è il diritto argentino in vigore?

A tal fine, dobbiamo tenere conto diverse leggi *specifiche* in questo senso:

a. *Legge 20337 (1973) sulle cooperative*

In linea di principio, come struttura giuridica in sé, la figura della cooperativa regolata dalla legge argentina 20337 potrebbe funzionare come cooperativa di dati ogni volta che ha il tipico *scopo mutualistico* di questo tipo di persona giuridica privata nel diritto argentino (art. 141, Codice civile e commerciale, di seguito CCyC).

Infatti, il sistema dell'economia cooperativa mira a soddisfare i bisogni umani di persone organizzate volontariamente sulla base del mutuo aiuto e dello sforzo personale.

Sono entità fondate sullo sforzo proprio e sull'aiuto reciproco per organizzare e fornire servizi, la cui caratteristica intrinseca è l'*atto cooperativo*.

Il art. 4 della Legge 20337 prescrive: *"Sono atti cooperativi quelli realizzati tra le cooperative e i loro associati e da questi stessi tra di loro nel compimento dell'oggetto sociale e nel raggiungimento degli scopi istituzionali. Lo stesso vale, per le cooperative, per gli atti giuridici che con identico scopo compiono con altre persone".*

L'atto cooperativo è, in altre parole, l'attività che partendo dalla solidarietà e dallo scopo dei membri di agire insieme come associati, e in un tutto secondo i principi cooperativi, si concretizza nella prestazione da parte della società, di uno o più servizi (oggetto della cooperativa) per soddisfare bisogni individuali simili dei soci in vista del bene particolare di tutti loro (fine della cooperativa), e per estensione al bene della comunità.

Da questo concetto si deduce che gli atti cooperativi sono atti di speciale natura delle parti coinvolte, specificità del loro oggetto e finalità perseguita; sono limitati alla prestazione di un servizio che la cooperativa offre ai soci allo scopo di eliminare l'intermediazione onerosa, e sono caratterizzati da basi solidali e mutualistiche che escludono il profitto.[14]

b. Legge 25326 (2000) di protezione dei dati personali

La presente legge[15] ha per oggetto la protezione integrale dei dati personali contenuti in archivi, registri, banche di dati o altri mezzi tecnici di trattamento di dati, pubblici o privati destinati a fornire relazioni, per garantire il diritto all'onore e alla vita privata delle persone, nonché l'accesso alle informazioni che su di esse sono registrate, in conformità con quanto stabilito dalla Costituzione nazionale (articolo 43, terzo comma). In nessun caso possono essere compromessi il database o le fonti di informazione giornalistica.

[14] A. KEMELMAJER DE CARLUCCI y M. BORETTO, *"Manual de Introducción al Derecho Privado"*, Mendoza, ed. Facultad Ciencias Económicas de la Universidad Nacional de Cuyo, 2006/2007, t. 4.
[15] O. A. GOZAÍNI, *"Hábeas Data. Protección de Datos Personales"*. 2° Edición Ampliada y Reformada. Editorial Rubinzal-Culzoni. Buenos Aires, 2011. O. A. GOZAÍNI, *"Ley 25.326 de protección de datos personales"*. Sup.Const. Esp.2003 (abril), 61 – LA LEY2003-C, 1139. *"Habeas data y el consentimiento para el tratamiento de datos personales"*. JA 1999-IV-399. P. A. PALAZZI, *"La protección de los datos personales en la Argentina: ley 25.326 de protección de datos personales y hábeas data comentada y anotada con jurisprudencia"*. Editorial Errepar Buenos Aires, 2004.

Va sottolineato, tuttavia, che esiste un progetto di legge[16] per aggiornare questa legislazione, i cui principi sono già stati recepiti dalla dottrina argentina, che prende come punto di partenza il riconoscimento e la protezione dei dati personali come diritto umano ed un elemento essenziale della politica dello Stato argentino.

La proposta di aggiornamento della legge è il risultato di un dibattito di idee partecipative, aperte e trasparenti sui bisogni e la realtà dell'Argentina in materia, contemplando tre idee principali: i) il diritto umano alla protezione dei dati personali e l'autodeterminazione informativa, ii) innovazione tecnologica basata su principi etici che promuove uno sviluppo economico inclusivo e iii) costruzione della fiducia attraverso regole del gioco chiare.

In questo senso, dobbiamo tenere conto anche che il 15 gennaio 2024, l'Unione europea ha ratificato l'Argentina come un paese adatto per lo scambio transfrontaliero di dati personali. Infatti, il Comitato europeo ha analizzato in dettaglio le leggi e i regolamenti argentini, nonché l'operato dell'Agenzia per l'accesso all'informazione pubblica (di seguito, AAIP), autorità di attuazione della legge di protezione integrale dei dati personali.

Il Comitato ha concluso che l'Argentina mantiene una legislazione allineata agli standard internazionali in materia di protezione dei dati, rendendola adatta al trattamento transfrontaliero dei dati personali.

I fattori chiave di questa decisione includevano:

a) il riconoscimento dell'AAIP come entità indipendente (in modo simile a quanto stabilito dal Regolamento generale sulla protezione dei dati personali –GDPR– dell'UE)
b) la sanzione della legge N° 27.483 (2018) che approva la Convenzione 108 del Consiglio d'Europa per la protezione delle persone rispetto al trattamento automatizzato dei dati personali ed, inoltre, la legge 27.699 (2022), che approva il Protocollo di modifica della Convenzione per la protezione delle persone con riguardo al trattamento automatizzato dei dati personali, noto anche come Convenzione 108+.

[16] Consiglio federale per la trasparenza (2022). Rapporto sull'aggiornamento della legge sulla protezione dei dati personali da una prospettiva federale. Agenzia per l'accesso alla informazione pubblica (AAIP).

c) il suddetto progetto di legge per l'aggiornamento della Legge sulla protezione dei dati personali promosso dall'AAIP, presentato al Congresso nazionale nel giugno 2023
d) l'emissione di altre importanti risoluzioni da parte dell'AAIP (ad esempio, secondo il criterio 2 della risoluzione n. 4/2019 dell'AAIP,[17] *il titolare dei dati personali ha il diritto di chiedere al responsabile del trattamento una spiegazione circa la giustificazione della decisione basata unicamente sul trattamento automatizzato dei dati che potrebbe avere un effetto negativo su di lui*).

Questa valutazione positiva ha portato l'UE a reinserire l'Argentina nel gruppo selezionato di paesi con norme adeguate alla protezione dei dati, un gruppo che conta già altri 10 membri, composto da: Andorra, Canada, Isole Faroe, Guernsey, Isola di Man, Israele, Jersey, Nuova Zelanda, Svizzera e Uruguay.

L'AAIP ha sottolineato l'importanza di questo risultato, affermando che non solo migliora le opportunità commerciali e lo sviluppo tecnologico dell'Argentina, ma definisce anche il paese come leader regionale nella protezione dei dati personali.

c. Legge 24766 (1996) sulla riservatezza delle informazioni e dei prodotti legittimamente sotto il controllo di una persona e divulgato in modo contrario agli usi commerciali onesti. Protezione dei dati commerciali e industriali

La sanzione di questa legge ha avuto come obiettivo l'adattamento di questa legislazione ai requisiti dell'art. 39 dell'accordo TRIP.[18]

La sua sigla in spagnolo è ADPIC (Accordo sugli aspetti del diritto di proprietà intellettuale relativi al commercio). Pubblicato come allegato 1 C dell'accordo che istituisce l'Organizzazione mondiale del commercio, fatto a Marrakech il 15/04/1994.

Nel 1995 la legge 24425 approva da parte dell'Argentina l'accettazione dei risultati dell'Uruguay Round del GATT (General Agreement on Tariffs and Trade) e che include il TRIP.

[17] https://servicios.infoleg.gob.ar/infolegInternet/anexos/315000-319999/318874/norma.htm
[18] E. SALIS y C. O. MITELMAN, *"La nueva ley de confidencialidad argentina"*, Portal Internacional de la Universidad de Alicante sobre Propiedad Industrial e Intelectual y Sociedad de la Información, uaipit.com/.

Il suddetto articolo 39, al fine di garantire una protezione efficace contro la concorrenza sleale, mira a proteggere le informazioni non divulgate, il che implica che *ogni persona (umana o giuridica) che ha un segreto industriale o commerciale è autorizzata a impedire l'accesso di terzi alle informazioni e ad impedirne l'uso, senza il loro previo consenso, purché le informazioni soddisfino tre condizioni: che sia segreta, abbia un valore commerciale per tale natura e sia stata oggetto di misure ragionevoli per mantenerla segreta*.

d. *Legge 27078 (2014) sulle tecnologie della comunicazione e informazione (noto come legge digitale argentina)*

L'articolo 5 disciplina *l'inviolabilità delle comunicazioni*, stabilendo che: *"La corrispondenza, intesa come qualsiasi comunicazione effettuata mediante le tecnologie dell'informazione e della comunicazione (TIC), comprese le tradizionali poste, la posta elettronica o qualsiasi altro meccanismo che induca l'utente a presumere la riservatezza della stessa e dei dati di traffico ad essa associati, effettuati attraverso le reti e i servizi di telecomunicazione, è inviolabile. La loro intercettazione, così come la loro successiva perquisizione ed analisi, avverrà solo su richiesta del giudice competente"*.

Altri strumenti giuridici *generici* da prendere in considerazione sono:

a. *Costituzione argentina* (*diritto alla privacy* secondo il suo art. 18, ampliato dall'art. 19[19]);
b. Precedenti della nostra *Corte Suprema di Giustizia della Nazione come "Ponzetti de Balbin vs. Editorial Atlántida"* (1985 – sentenze 306:1892) in cui si definisce il diritto alla privacy come *"il diritto dell'individuo di decidere da solo in che misura condividerà con gli altri i suoi pensieri, sentimenti e fatti della sua vita personale"*;
c. I *Trattati Internazionali* come la Convenzione Americana sui Diritti Umani, il Patto Internazionale sui Diritti Civili e Politici, il proprio *rimedio processuale costituzionale denominato "Habeas Data"*[20] (Const. Nac., art. 43, 3o par.); pilastri fondamentali del Blocco di costituzionalità.

[19] Articolo 19. – *Le azioni private degli uomini che in nessun modo offendano l'ordine e la morale pubblica, né nuocciano a un terzo, sono riservate solo a Dio ed esenti dall'autorità dei magistrati. Nessun abitante della Nazione sarà obbligato a fare ciò che la legge non comanda, né privato di ciò che essa non proibisce.*
[20] A. B. BIANCHI, *"El hábeas data como medio de protección del derecho a la información objetiva en un valioso fallo de la Corte Suprema"*. LA LEY 1998-F, 297. A. B. BIANCHI, *"Hábeas data y derecho a la privacidad"*. ED, 161-866. G. J. BIDART CAMPOS, *"¿Habeas data, o qué? ¿Derecho "a la verdad", o qué?"*. LA LEY 1999-A, 212.

d. L'attuale *Codice civile e commerciale* (art. 52): lesioni alla dignità. *La persona umana lesa nella sua intimità personale o familiare, nell'onore o nella reputazione, nell'immagine o nell'identità, o che in qualsiasi modo sia compromessa nella sua dignità personale, può chiedere la prevenzione e il risarcimento dei danni subiti*

2.3. Una cooperativa di dati nel diritto argentino? Possibili risposte

Facendo come semplice esempio di applicazione pratica in cui la cooperativa di dati può essere uno strumento utile dal punto di vista socio-culturale per il processo decisionale strategico, potremmo ipotizzare lo scenario seguente: in un paese con povertà come l'Argentina, dove la distribuzione razionale delle risorse economiche tra i vari gruppi vulnerabili per soddisfare le diverse esigenze sociali è vitale, a volte con uno Stato assente, potremmo chiederci: *se sia opportuno creare una cooperativa di dati come quella figura nel l'intermediazione dei dati ?*

1. Per servire da strumento giuridico istituzionale non governativo al fine di facilitare la raccolta, la gestione e l'uso razionale dei dati (economici, educativi, sanitari, sociali, culturali, ecc.) corrispondenti a una determinata comunità territoriale (ad esempio un quartiere povero) a beneficio dei propri associati.
2. Con l'obiettivo di ottimizzare l'esecuzione strategica delle politiche pubbliche – da parte del governo –, in questi settori sociali vulnerabili.

Per esempio, a Mendoza, ci sono quartieri vulnerabili – come il «Barrio La Favorita» e il «Barrio 31 de Mayo», Città Capital, tra gli altri – in cui, ad esempio, attraverso una cooperativa di dati che avesse come membri le unioni di quartiere, gli ordini religiosi, i propri abitanti del quartiere e forse lo stesso governo comunale, che fosse anche amministrata dai suoi stessi membri, si potrebbe:

a) raccogliere dati relativi al numero di famiglie in situazione di vulnerabilità, se queste dispongono di aiuti economici statali, se hanno un impiego, se sono persone che vivono di affari propri o sono «cartonieri» (raccolgono cartone), se ci sono istituzioni educative nel territorio, sale di primo soccorso, se esistono microprestiti concessi dallo Stato o da qualche ONG agli abitanti del quartiere per essere applicati ad «imprese» modeste (acquisto di una macchina da cucire, di un forno elettrico, ecc.), se ci sono delle mercatine, ecc.
b) creare un database o *big data* sociale.

c) classificare questi dati secondo criteri razionali.
d) infine, utilizzare e gestire tali dati, che la cooperativa di dati può condividere con il governo, per fare strategicamente una determinata politica pubblica in cui saranno utilizzati fondi pubblici (es., costruire una sala di pronto soccorso dove non c'è, installare un «merendero» –luogo dove può mangiare una persona povera– in un determinato settore dei quartieri, concedere microprestiti ai disoccupati, ecc.).
e) in questo modo, grazie alla cooperativa di dati e ai dati razionalmente gestiti dalla stessa, i membri della cooperativa, compresi gli stessi abitanti del quartiere, possono conoscere meglio "le loro esigenze" e, ad esempio, potranno chiedere istituzionalmente al Comune l'esecuzione delle politiche pubbliche educative, sanitarie, edilizie, ecc. in modo molto più efficiente.

Le ragioni per diventare membro di una cooperativa di dati includono l'altruismo dei dati (condivisione dei dati per aiutare gli altri, spesso nella ricerca sanitaria) e la sovranità dei dati (mantenere il potere e il controllo sui propri dati).

In questo modo, in Argentina siamo convinti che le organizzazioni no profit e le agenzie di servizi sociali potrebbero organizzare i loro sistemi di dati come cooperative di dati, unendosi per condividere tecnologia e infrastrutture, e allo stesso tempo utilizzando la governance collettiva per sviluppare impegni e metriche condivise.

Per raggiungere questo obiettivo è necessario qualcosa di molto importante: risorse economiche che consentano alla cooperativa dei dati di acquisire una tecnologia efficace e assumere risorse umane per classificare e gestire le informazioni raccolte, attraverso la stessa tecnologia, in modo da consentire un uso corretto di tali dati.

Non si possono usare elementi rudimentali come una semplice "tabella di Excell".

La tecnologia è necessaria per ottenere informazioni accurate in tempo reale e tempestiva. Solo così si può progettare una strategia e ottimizzare le decisioni che vengono prese.

Per questo scopo, cioè per fornire fondi alla cooperativa dati, si può attuare un sistema di finanziamento collettivo utilizzato in Italia dalla Fondazione Un Caffè (*https://www.1caffe.org/*) concepita come la prima realtà sociale digitale creata per sostenere le piccole e medie associazioni italiane senza scopo di lucro attraverso la

diffusione della cultura del gesto del dono. Dal 2011, ogni anno, attraverso la sua piattaforma di *crowdfunding*, questa Entità aiuta molte organizzazioni solidali che promuovono progetti di assistenza a diverse cause sociali.

In altre parole, attraverso il *crowdfunding* i terzi interessati ad aiutare la cooperativa di dati possono fare piccole donazioni di fondi che consentano a quest'ultima di avere le risorse finanziarie per affrontare i suoi obiettivi.

A tal fine, occorre tener conto che:

(i) La base del *crowdfunding* è il concetto di economia collaborativa. La traduzione letterale di questa espressione anglosassone significa finanziamento collettiva.
(ii) Può essere utilizzato tramite una piattaforma digitale o *marketplace*
(iii) Una caratteristica centrale del *crowdfunding* è la massiccia unione di investitori che finanziano progetti ad alto potenziale, ognuno con piccole somme di denaro.
(iv) Avantaggi:
  (a) Permette di fare donazioni a persone con diversa capacità economica, democratizzando la partecipazione alla cultura della carità (attraverso la pratica di donare).
  (b) Fornire alla cooperativa dei dati il capitale necessario per il suo progetto (acquisire tecnologia per gestire i dati, pagare il salario delle risorse umane che utilizzano tale tecnologia e progettano schemi per classificare tali informazioni, ecc.), in modo rapido, riducendo drasticamente i costi di finanziamento, dal momento che la cooperativa non è un'entità a scopo di lucro e che ottiene profitti in virtù della sua attività.

In somma, a nostro avviso, una cooperativa di dati sarebbe molto utile in Argentina, potendo fungere da intermediario di dati con diversi obiettivi, per esempio:

- filantropi o di beni comuni, *come abbiamo appena analizzato*, ma non solo con questo obiettivo, infatti, potrebbe anche avere altri obiettivi
- legate ai *big data* possono anche svolgere un ruolo chiave nella collaborazione aziendale tra diverse aziende per la generazione di informazioni abbondanti e di qualità. Si tratta della condivisione e dell'utilizzo dei dati raccolti in una

determinata attività, compilati e gestiti dalla cooperativa di dati per aiutarli a prendere decisioni migliori all'interno di un quadro sicuro. Pensiamo, ad esempio, a diverse aziende agricole –l'Argentina è un paese agricolo per eccellenza (soia, mais, grano, sorgo, girasole, ecc.)– che fanno parte di una cooperativa di dati e che, grazie alle informazioni meteorologiche e sui mercati dei cereali che questa conserva insieme ai dati forniti da fonti esterne (ad esempio, quelli provenienti da satelliti, stazioni meteorologiche e informazioni di mercato), o anche informazioni provenienti dalle stesse aziende partner che utilizzano la tecnologia a tal fine, rende possibile la creazione di modelli di previsione e consulenza avanzati che consentono ai suoi partner di disporre dei dati necessari per conoscere con maggiore precisione quali cereali seminare, in quale periodo dell'anno, adottare misure di prevenzione in caso di siccità o inondazioni, speculare sulla redditività del raccolto, ecc.

Riteniamo che sarebbe legalmente fattibile nel nostro paese una cooperativa di dati come intermediario di dati, purché vengano rispettati alcuni parametri legali inderogabili sotto pena di illegittimità nell'oggetto sociale effettuato dalla persona giuridica, vale a dire:

(i) I dati da trattare dalla cooperativa, siano essi personali o no (commerciali, industriali, ecc.), richiedono il previo consenso del titolare, con le relative eccezioni (conf. art. 5, legge 25326 e artt. 1 e 3, legge 24766).

a. Per quanto riguarda i dati personali, dovrà essere rispettato anche l'obbligo di informazione preventiva dell'art. 6, legge 25326

b. Normalmente la cooperativa non ha bisogno di trattare dati sensibili e non potrebbe farlo. La sua attività sarebbe illecita. Tuttavia, eccezionalmente potrebbe essere necessario compilarli per riferirsi a informazioni sulla salute (ricordiamo, per esempio, il caso della cooperativa di dati come strumento giuridico istituzionale non governativo a fini di bene comune in quartieri poveri nei quali i dati sulla salute possono essere rilevanti) e dovrà rispettare l'art. 7, inc. 2, legge 25326, ovvero trattare i dati in modo dissociato in modo che le informazioni ottenute non possano essere collegate a una persona determinata o determinabile (art. 2, legge 25326). In quest'ultimo caso, bisogna sempre tenere presente che questo tipo di dati può essere trattato solo se vi sono motivi di interesse generale autorizzati dalla legge, per scopi statistici o scientifici e purché non sia possibile identificare i loro titolari (art. 7, legge 25326).

c. Nel caso di dati commerciali o industriali di terzi, purché essi rientrino nella qualifica di informazione segreta ai sensi dell'art. 1, Legge 24766, la cooperativa deve evitare di effettuare pratiche di trattamento dei dati, in particolare l'accesso ad essi, in modo contrario agli usi commerciali onesti. La violazione di contratti, l'abuso della fiducia, l'istigazione alla violazione e l'ottenimento di informazioni non divulgate da parte di terzi che sapessero o meno, per grave negligenza, che l'acquisizione comportava tali pratiche, sono contrari agli usi commerciali onesti (art. 1, legge 24766).

(ii) Comprendiamo che, date le caratteristiche sopra esposte, la cooperativa dati funziona come una sorta di registro dei dati e sarebbe un responsabile del registro, motivo per cui, quando ha per oggetto il trattamento dei dati personali (art. 2, Legge 25326), dovrà essere registrata nel Registro Nazionale delle Basi di Dati Personali (sotto l'orbita della Direzione Nazionale per la Protezione dei Dati Personali, art. 24, Legge 25326).

A tal fine, devono essere soddisfatti anche i requisiti dell'art. 21, legge 25326, tra cui la cooperativa di dati dovrebbe informare: a) Nome e indirizzo del responsabile; b) Caratteristiche e scopo del file; c) Natura dei dati personali contenuti in ogni file; d) Modalità di raccolta e aggiornamento dei dati; e) Destinazione dei dati e persone fisiche o di esistenza ideale a cui possono essere trasmessi; f) Modo di interconnessione delle informazioni registrate; g) Mezzi utilizzati per garantire la sicurezza dei dati, specificando la categoria di persone che hanno accesso al trattamento delle informazioni; h) Durata della conservazione dei dati; i) Modalità e condizioni di accesso alle informazioni personali e procedure per la rettifica o l'aggiornamento delle informazioni

(iii) Inoltre, deve essere compilato con la registrazione che corrisponde come persona giuridica privata secondo la legge sulle cooperative 20337 (presso il registro delle "cooperative" a carico dell'Istituto nazionale di azione cooperativa, art. 10).

(iv) La cooperativa di dati può anche, in questa stessa direzione, elaborare codici di condotta per l'esercizio professionale, stabilire norme per il trattamento dei dati personali che tendano a garantire e migliorare le condizioni di funzionamento dei sistemi informativi in base ai principi stabiliti nella Legge 25326. Tali codici dovrebbero essere iscritti nel registro che l'organismo di controllo ha a tal fine, il quale potrà rifiutare l'iscrizione qualora ritenga che non siano conformi alle disposizioni legislative e regolamentari in materia (arg. art. 30, Legge 25326).

(v) In questo contesto, dal punto di vista dell'intermediazione dei dati, potrebbe esserci cessione di dati personali da parte della cooperativa di dati, che dovrebbe

rispettare determinati parametri legali affinché la sua attività non sia illecita dal momento che non può cedere o condividere i dati a discrezione o secondo criteri di mera convenienza. In tal senso, almeno, si deve tener conto dei seguenti parametri (art. 11, Legge 25326):

a. I dati personali oggetto di trattamento possono essere comunicati solo per l'adempimento delle finalità direttamente connesse all'interesse legittimo del cedente e del cessionario e con il previo consenso del titolare dei dati, a cui deve essere comunicato lo scopo della cessione e identificato il cessionario o gli elementi che consentono di farlo
b. Il consenso alla cessione è revocabile.
c. Il consenso non è richiesto quando, ad esempio: a) una legge lo prevede; b) la cessione avviene tra gli organi dello Stato in forma diretta, nella misura in cui ciò sia conforme alle rispettive competenze; c) si tratta di dati personali relativi alla salute, e se necessario per motivi di sanità pubblica, emergenza o per effettuare studi epidemiologici, purché l'identità dei titolari dei dati sia preservata mediante adeguati meccanismi di dissociazione; d) sia stata applicata una procedura di dissociazione delle informazioni, in modo che i titolari dei dati non siano identificabili.

In ogni caso, si deve anche tener conto che il cessionario sarà soggetto agli stessi obblighi legali e regolamentari del cedente e quest'ultimo risponderà solidale e congiuntamente per l'osservanza degli stessi davanti all'organismo di controllo e al titolare dei dati.

Como citar:

BORETTO, Mauricio. L'intelligenza artificiale, la protezione dei dati e le cooperative di dati e in Argentina. **Civilistica.com**, a. 15, n. 1, 2026. Disponível em: https://civilistica.emnuvens.com.br/redc. Data de acesso.

civilistica.com
Recebido em:
15.10.2025
Aprovado em:
12.1.2026