Studio Legale RICCIARDI – CONTE (SLRC)
Avv. Piero Ricciardi – Avv. Maurizio Conte
INTEGRATED COMPLIANCE MANAGER

ATTIVITÁ
COMPLIANCE NORMATIVA
D.LGS. 231/2001 RESPONSABILITÁ DI IMPRESA
USO DEL SISTEMA FINANZIARIO E ANTIRICICLAGGIO
GDPR GENERAL DATA PROTECTION REGULATION
RATING DI LEGALITÁ E RATING REPUTAZIONALE

SERVIZI
TEMPORARY COMPLIANCE MANAGEMENT (TCM)
DATA PROTECTION OFFICER (DPO)
ORGANISMO DI VIGILANZA (ODV)
CYBER SECURITY E TRASFORMAZIONE DIGITALE

PARERE PRO VERITATE

Allo Studio Legale RICCIARDI – CONTE (di seguito, in breve, "SLRC") è stato richiesto di fornire un parere sull'eticità ed "umanizzazione" dell'algoritmo in uso nel servizio di rating reputazionale digitalizzato, documentato e tracciabile (di seguito, in breve, "rating reputazionale") elaborato dalla società MEVALUTATE HOLDING LTD e pubblicato dal periodico online CROP NEWS – Cronache Reputazionali Oggettive Personalizzate, edito dall'omonima Associazione non ptofit, con cui si attesta che dalle risultanze dei documenti esaminati (1. Report del Gruppo di Ricerca e Sviluppo in Collaborazione Pubblico-Privato MEVALUATE HOLDING – The Bank of Reputation; 2. Codice della Reputazione Universale; 3. RATING MEVALUATE: MISURARE L'IMMISURABILE; 4. Worldwide Ethics Committee MEVALUATE HOLDING; 5. Regolamento CROP NEWS) detto algoritmo si caratterizza per trasparenza, inclusività e imparzialità risultando quindi "umanizzato" oltre che conforme al dettato della bozza di Regolamento europeo sull'intelligenza artificiale pubblicata il 21 aprile 2021.

Per fornire un parere in linea con la normativa europea, non ci si può esimere dal considerare alcuni principi contenuti in detta bozza di Regolamento 2021/0106 che la Commissione Europea ha presentato il 21 aprile 2021 che delinea un quadro armonizzato sull'intelligenza artificiale **(allegato A).**

L'obiettivo della fonte normativa citata è declinare i **vantaggi** derivanti dall'impiego di sistemi di **intelligenza artificiale (IA)** come:

- il miglioramento nella fruizione dei servizi del cittadino
- l'agevolazione dello sviluppo delle imprese
- il conferimento di maggiore efficienza ai servizi di interesse pubblico

con i risvolti negativi che potrebbero concretizzarsi, ove i primi venissero impiegati mediante un uso distorto o abusivo.

Nello specifico, gli **obiettivi** che la bozza di Regolamento si propone di realizzare sono:

- garantire che i sistemi di **IA** immessi sul mercato dell'Unione siano sicuri e rispettino le leggi esistenti sui diritti fondamentali e sui valori dell'unione
- garantire la certezza del diritto per facilitare gli investimenti e l'**innovazione** nell'IA
- migliorare la **governance** e l'effettiva applicazione delle leggi esistenti sui diritti fondamentali e sui requisiti di sicurezza applicabili ai sistemi di IA
- facilitare lo **sviluppo** di un mercato unico delle applicazioni di IA legali, sicure e affidabili, prevenendo la frammentazione del mercato interno.

Anche i rischi insiti nei sistemi di IA sono considerati nella proposta: in effetti, si parte dalla individuazione di un **rischio inaccettabile**; qui si tratta di sistemi IA che mettono a rischio i diritti e le libertà dei cittadini UE e che, pertanto, saranno sostanzialmente banditi.

In tali casi di parla di **IA forte** in quanto questa tecnologia è in grado di riprodurre processi intellettivi analoghi a quelli umani; rientrano in questa classe:

- i sistemi di IA che utilizzino tecniche subliminali che, al di là della consapevolezza di una persona, possa manipolare materialmente il suo comportamento in un modo tale da causare (o è probabile che possa causare a quella persona o a un'altra persona) danni fisici o psicologici;
- i sistemi di IA che sfruttino una qualsiasi delle vulnerabilità di un gruppo specifico di persone a causa della loro età, disabilità fisica o mentale, al fine di manipolare materialmente il comportamento di una persona appartenente a quel gruppo in un modo da causare (o è probabile che possa causare) a quella persona o un'altra persona danni fisici o psicologici;
- i sistemi di IA da parte della pubblica autorità (o per suo conto) per la valutazione o la classificazione dell'affidabilità delle persone fisiche per un determinato periodo di tempo in base al loro comportamento sociale o a caratteristiche personali o di personalità note o previste, con l'attribuzione di un punteggio sociale (c.d. *social scoring*);
- l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico per finalità di *law enforcement* (fatte salve alcune eccezioni relative: alla ricerca mirata di specifiche potenziali vittime di reati, compresi bambini scomparsi; la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o sicurezza fisica delle persone fisiche o di un attacco terroristico; l'individuazione, la localizzazione, l'identificazione o il perseguimento di un autore o sospettato di un reato punibile nel membro Stato interessato da una pena detentiva o un ordine di detenzione per a periodo massimo di almeno tre anni, come determinato dalla legge dello stesso Stato membro).

L'utilizzo dei sistemi di IA vanno considerati come ad uso limitato o gestito, come ad esempio:

- predisporre, implementare e documentare un sistema di gestione del rischio (art. 9); nei sistemi di IA ad alto rischio che utilizzano tecniche che comportano la formazione di modelli con i dati, devono essere sviluppati sulla base di set di dati di addestramento, convalida e test che soddisfano i criteri di qualità specifici (art. 10);
- redigere la documentazione tecnica prima della data di immissione sul mercato o della messa in servizio e deve essere costantemente aggiornata (art. 11)
- essere progettati e sviluppati con capacità che consentano la registrazione automatica degli eventi ("log") durante il loro funzionamento; tali capacità di registrazione devono essere conformi a standard riconosciuti o comuni specifiche (art. 12)
- essere progettati e sviluppati in modo tale da garantire che il loro funzionamento sia sufficientemente trasparente per consentire agli utenti di interpretare il sistema output e utilizzarlo in modo appropriato (art. 13)
- essere progettati e sviluppati in modo tale – (anche con strumenti di interfaccia uomo-macchina appropriati) – da poter essere efficacemente controllati da persone fisiche durante il periodo in cui è in uso il sistema di IA (art. 14);
- i fornitori garantiscono che i sistemi di IA destinati a interagire con le persone fisiche siano progettati e sviluppati in modo tale che le persone fisiche siano informate che stanno interagendo con un sistema di intelligenza artificiale; tale obbligo non si applica ai sistemi di IA autorizzati per legge a individuare, prevenire, indagare e perseguire reati:

- gli utenti di un sistema di riconoscimento delle emozioni o di un sistema di classificazione biometrica devono informare del funzionamento del sistema le persone fisiche ad esso esposte. Questo obbligo non si applica ai sistemi di IA utilizzati per la categorizzazione biometrica, nei casi consentiti, per rilevare, prevenire e indagare sui reati.
- Gli utenti di un sistema IA che genera o manipola contenuti immagine, audio o video che assomiglino sensibilmente a persone, oggetti, luoghi o altre entità o eventi esistenti e che sembrino falsamente una persona reale («deep fake»), deve rivelare che il contenuto è stato generato o manipolato artificialmente.

Esistono poi **sistemi altamente invasivi di IA, come quelli di riconoscimento facciale biometrico** utilizzati dalle forze dell'ordine per ragioni di *law enforcement,* pur rientrando in questa classe, i limiti saranno molto più stringenti. Il loro utilizzo da parte della pubblica autorità sarà consentito solo in casi eccezionali, quali la ricerca di un soggetto smarrito o IA fini di prevenzione di una specifica ed imminente minaccia terroristica.

Per lo sviluppo delle IA è necessario un approccio che prevenga e attenui i potenziali rischi del trattamento dei dati personali e nella valutazione del rischio, ed è necessario, altresì, adottare una prospettiva più ampia che tenga conto non solo dei diritti umani e delle libertà fondamentali ma anche del funzionamento delle democrazie, dei valori sociali ed etici dei Paesi dell'**Unione europea**; le IA devono rispettare pienamente i diritti degli interessati e devono sempre consentire un controllo da parte degli interessati.

Ancora, si deve adottare un approccio preventivo per valutare l'impatto di possibili conseguenze negative derivante dallo sviluppo di applicazioni IA in tutte le fasi del trattamento dei dati personali, avendo un approccio volto a garantire la tutela dei diritti umani dalle fasi di progettazione, evitando così qualsiasi pregiudizio o altri effetti negati sui diritti umani e le **libertà fondamentali** degli interessati; valutare la qualità, la natura, l'origine e la quantità dei dati personali utilizzati, eliminando i dati superflui e utilizzato dati sintetici (rappresentativi dei dati reali originali) quando possibile.

Per ottemperare a tali requisiti è necessario che l'utilizzo di modelli algoritmici siano sempre contestualizzati per non produrre impatti negativi sulle persone e la società.

Sicuramente alle autorità di controllo devono essere forniti i mezzi sufficienti per attuare i programmi di vigilanza sugli algoritmi. L'intervento umano deve essere preservato nei processi decisionali; gli sviluppatori, produttori e fornitori di IA, qualora ritengano che l'applicazione possa incidere in modo significativo sui diritti umani e sulle libertà fondamentali, dovrebbero consultare le preposte autorità di controllo e dovrebbero promuovere la cooperazione tra le diverse autorità competenti in materia di **protezione dei dati personali**, di concorrenza e diritti del consumatore.

Per questo motivo è necessario garantire l'indipendenza dei comitati di esperti.

Al termine di tali riflessioni, possiamo affermare oltre ogni dubbio che l'algoritmo sviluppato da MEVALUATE HOLDING Ltd e il suo uso sono in linea con la regolamentazione europea in quanto rappresentano uno sviluppo etico ed umanizzato di un sistema procedurale non invasivo, rispettoso dei diritti e libertà dei singoli partecipanti al rating e trasparente con regole chiare e precise.

ATTIVITÁ
COMPLIANCE NORMATIVA
D.LGS. 231/2001 RESPONSABILITÁ DI IMPRESA
USO DEL SISTEMA FINANZIARIO E ANTIRICICLAGGIO
GDPR GENERAL DATA PROTECTION REGULATION
RATING DI LEGALITÁ E RATING REPUTAZIONALE

SERVIZI
TEMPORARY COMPLIANCE MANAGEMENT (TCM)
DATA PROTECTION OFFICER (DPO)
ORGANISMO DI VIGILANZA (ODV)
CYBER SECURITY E TRASFORMAZIONE DIGITALE

In effetti, l'umanizzazione degli algoritmi è un tema etico che ha l'obiettivo di elaborare un modello di sviluppo delle società occidentale contemporanee in cui la rigidità dell'algoritmo venga mitigata, quindi, "umanizzata" nel rispetto di principi etici condivisi. La vera natura del problema risiede nella complessità della tematica e nella sua trasversalità, che esige l'associazione della cultura umanistica con quella tecnologica. Le intelligenze artificiali non sono, infatti, soggetti previsti dalla Carta costituzionale ma soggetti nati dal mercato. Decisioni elettroniche, automatiche, informatiche, prevalgono sempre più sul singolo. Ma se gli esiti dei software al servizio del pubblico sono destinati ad incidere in misura sempre maggiore sui diritti dei cittadini, dovremo volgerci verso un "algor-etica", affinché la macchina sia sempre al servizio dell'uomo perché se l'algoritmo deve decidere per noi, è bene che siamo noi a mantenerne il controllo. Nel caso del rating reputazionale l'**algoritmo è umanizzato** perché è **trasparente** (il suo funzionamento è conosciuto o conoscibile dall'utente a cui è illustrato in modo comprensibile con i richiamati documenti 1. Report del Gruppo di Ricerca e Sviluppo in Collaborazione Pubblico-Privato MEVALUATE HOLDING – The Bank of Reputation; 2. Codice della Reputazione Universale; 3. RATING MEVALUATE: MISURARE L'IMMISURABILE; 4. Worldwide Ethics Committee MEVALUATE HOLDING; 5. Regolamento CROP NEWS); **inclusivo** (interculturale, non sessista, non razzista, perchè, ad esempio, prevede che con il decorso del tempo si attenuino gli effetti negativi di una determinata azione compiuta in passato, così consentendo di ottenere risultati più "puliti" di quelli che si possono produrre utilizzando un algoritmo generico); **imparziale** (obbediente a criteri obiettivi di valutazione; immune da inclinazioni o atteggiamenti personalistici).

Napoli, 24 novembre 2021

Avv. Piero Ricciardi