Diritto e Giustizia
IL QUOTIDIANO DI INFORMAZIONE GIURIDICA

La proposta di Regolamento UE sull'Intelligenza Artificiale: i profili operativi del nuovo quadro normativo europeo – Parte Quarta

Prof. Avv. Alessandro del Ninno
Studio Legale Tonucci & Partners

§ 1. Introduzione: le tematiche oggetto di analisi.

Nel primo dei cinque saggi – pubblicato su *Diritto e Giustizia* il 28 aprile scorso - in cui si è scelto di suddividere l'analisi pratica della proposta di *Regolamento del Parlamento europeo e del Consiglio che stabilisce norme armonizzate in materia di intelligenza artificiale (l'Artificial Intelligence Act) e che modifica talune norme legislative dell'Unione* (di seguito, per brevità, il "*Regolamento IA*") abbiamo illustrato e commentato operativamente i profili generali del Regolamento IA, l'oggetto e le finalità delle nuove regole, l'ambito di applicazione, le principali definizioni giuridiche dei concetti e – infine- abbiamo approfondito le scelte legislative circa i divieti imposti a particolari "*pratiche di intelligenza artificiale*".

Nel secondo saggio è stata approfondita l'analisi pratica in merito all'approccio *risk based* che emerge dalla proposta di Regolamento IA (anche comparativamente con l'approccio basato sul rischio adottato dal Regolamento 679/2016), e si è svolto l'esame della classificazione dei sistemi di Intelligenza Artificiale *ad alto rischio*. Il secondo contributo si è concluso con l'avvio della descrizione – per tali sistemi - degli obblighi pratici in capo a chi li immette sul mercato o li mette in uso. I fornitori, difatti, devono "*strutturare, attuare, documentare e mantenere*" (in base a quanto previsto dall'articolo 9 della proposta di Regolamento IA) un complessivo sistema di *risk management* per i sistemi IA ad alto rischio, fatto di requisiti legali, tecnici e documentali.

Nel terzo contributo si è poi concluso l'esame del complessivo sistema di *risk management*, approfondendo gli obblighi di trasparenza, nonché l'impostazione cosiddetta *antropocentrica* dei sistemi IA, con l'obbligo di garantire la sorveglianza umana. Nella terza parte si sono poi analizzati gli ulteriori obblighi organizzativi, tecnici, commerciali e di altro tipo in capo ai fornitori di sistemi IA ad alto rischio, con l'illustrazione – nello specifico – dei loro obblighi inerenti la c.d. *accountability* dell'Intelligenza Artificiale e degli aspetti pratici delle *procedure di conformità* a cui devono sottoporre i sistemi IA ad alto rischio prima di immetterli sul mercato.

Nel presente contributo si procederà all'analisi pratica della parte del Regolamento IA che impone specifici obblighi ai numerosi soggetti che svolgono precisi ruoli nelle varie fasi di sviluppo, produzione, importazione, commercializzazione, distribuzione e utilizzo dei sistemi IA ad alto rischio e si illustrerà la prima disciplina al mondo dei cosiddetti *deepfakes*.

§ 2. Gli obblighi in capo agli altri soggetti coinvolti nella catena del valore dei sistemi di Intelligenza artificiale ad alto rischio.

Come detto in precedenza, nella catena produttiva e commerciale per la immissione sul mercato (o la messa in servizio) di sistemi IA ad alto rischio sono coinvolti numerosi soggetti che svolgono precisi ruoli nelle varie fasi di sviluppo, produzione, importazione, commercializzazione, distribuzione e utilizzo. In capo a ciascuna categoria di questi soggetti sono posti specifici obblighi e - nella modifica di paradigmi giuridici e contrattuali, come vedremo – addirittura gli utenti/acquirenti finali di detti sistemi sono sottoposto ad obblighi gestionali nel corso dell'utilizzo dei sistemi IA acquistati e messi in uso.

Dopo aver approfondito nella Parte Terza gli specifici obblighi dei *fornitori* dei sistemi IA ad alto rischio, ci occuperemo ora – nella rapida rassegna del presente paragrafo – degli obblighi imposti a: produttori di sistemi che si interano con i sistemi IA, rappresentanti autorizzati, importatori, distributori, utenti e altre terze parti.

Qualora un sistema di IA ad alto rischio sia integrato nei prodotti fabbricati a sensi delle normative settoriali elencate al paragrafo A dell'Allegato II al Regolamento IA (si pensi ai produttori di giocattoli, ascensori, sistemi di trasporto, sistemi di comunicazione, dispositivi medici, etc), i *produttori* di tali beni che integrano sistemi IA si assumono la piena responsabilità della conformità e sicurezza anche del sistema IA integrato (cfr. art. 24 del Regolamento IA). Di conseguenza, per quanto riguarda il sistema AI come parte del prodotto da loro immesso sul mercato o messo in servizio, sono soggetti ai medesimi obblighi che il Regolamento IA impone ai fornitori dei sistemi IA in quanto tali.

Quanto al "*rappresentante autorizzato*" si ricorda che esso è definito come "*qualsiasi persona fisica o giuridica stabilita nell'Unione che ha ricevuto un mandato scritto da un fornitore di un sistema di intelligenza artificiale che non sia stabilito nella UE per, rispettivamente, eseguire e svolgere per suo conto gli obblighi e le procedure stabilite dal Regolamento*" (cfr. art. 3.5 Reg. IA). L'articolo 25 del Regolamento IA introduce un obbligo di nomina – mediante "*mandato scritto*" - di un rappresentante nella UE del fornitore ivi non stabilito, laddove sia sconosciuto l'*importatore* del sistema IA e prima che questo venga immesso sul mercato oppure messo in servizio (tale obbligo ricorda quello analogo del rappresentante del titolare del trattamento di cui all'articolo 27 del GPDR). Il mandato/nomina deve conferire al rappresentante autorizzato il potere di:

1. conservare e mettere a disposizione delle autorità nazionali competenti (cfr. art. 63 Reg. IA) una copia della dichiarazione di conformità e della documentazione tecnica inerenti ciascun sistema IA ad alto rischio;
2. fornire a richiesta motivata delle autorità nazionali competenti tutte le informazioni e i documenti necessari a dimostrare (*accounatbility* dell'IA) la conformità dei sistemi IA ad alto rischio a tutti i requisiti previsti dal *sistema di gestione della qualità* e dal

sistema di risk assessment, ivi inclusa la fornitura di accesso ai *logs* generati automaticamente da detti sistemi, nella misura in cui tali *logs* siano sotto il controllo del fornitore in base a un accordo contrattuale con l'utilizzatore (si veda *infra*);
3. cooperare con le autorità nazionali competenti (sul modello di quanto previsto per i fornitori dall'articolo 23 Reg. IA) in base a loro richiesta motivata nell'ambito di qualsiasi azione che dette autorità intraprendano in relazione ai sistemi IA ad alto rischio.

Quanto agli *importatori* (cfr. art. 3.6 Reg. IA, "*importatore*": qualsiasi persona fisica o giuridica stabilita nell'Unione che immette sul mercato o mette in servizio un sistema di IA che reca il nome commerciale o il marchio di una persona fisica o giuridica stabilita al di fuori dell'Unione), questi – prima della immissione dei sistemi IA ad alto rischio (importati) sul mercato - dovranno assicurare, ai sensi dell'articolo 26 Reg. IA, che:

- il fornitore abbia effettuato correttamente la procedura di *conformity assessment*;
- il fornitore abbia redatto la documentazione tecnica in base ai requisiti e ai contenuti prescritti dall'Allegato IV al Regolamento;
- il sistema IA rechi il marchio di conformità e sia accompagnato dalla prescritta documentazione e manualistica d'uso con tutte le istruzioni di utilizzo.

L'importatore, oltre a non poter immettere sul mercato sistemi IA ad alto rischio per i quali abbia verificato (o ritenga ragionevolmente) la non conformità ai requisiti posti dal Regolamento, avrà altresì l'obbligo di informare il fornitore e le autorità competenti per la sorveglianza del mercato ove da detta non conformità possano discendere rischi per la salute o la sicurezza degli utenti o rischi di lesione di diritti fondamentali.

Vi è poi una previsione importante rispetto alla possibile ricostruzione di responsabilità per danno (la cui corretta imputazione ai vari soggetti in gioco appare complicata dalla frammentazione ed articolazione di fasi e soggetti coinvolti nella produzione e immissione sul mercato dei sistemi IA ad alto rischio). L'art. 26.4 Reg. IA prescrive infatti una specifica responsabilità dell'importatore per le fasi di magazzino e trasporto dei sistemi IA, per tutta la durata di tali fasi a cui l'importatore sovrintende. Infine, gli importatori (che dovranno essere specificatamente identificati sul sistema o sul *packaging* mediante indicazione di nome, ragione sociale, marchio e recapito geografico dove possono essere contattati) devono sottostare ai medesimi obblighi che più sopra abbiamo elencato – ai nn. 1-3 – per i rappresentanti autorizzati nell'ambito dei rapporti e della cooperazione con le autorità nazionali competenti.

Quanto ai *distributor*i (cfr. art. 3.7 Reg. IA, "*distributore*": qualsiasi persona fisica o giuridica nella *supply chain*, diversa dal fornitore o dall'importatore, che rende disponibile un sistema di IA sul mercato dell'Unione senza che siano coinvolte o impattate sue proprietà), questi, prima di rendere disponibile sul mercato un sistema IA ad alto rischio (attività commerciale diversa dalla "immissione sul mercato", difatti ai sensi dell'art. 3, per "*messa a disposizione sul mercato*" si intende qualsiasi fornitura di un sistema di IA per la distribuzione o uso sul mercato dell'Unione nel corso di un'attività commerciale,

indipendentemente dal fatto che ciò avvenga verso corrispettivo oppure gratuitamente) dovranno verificare che il sistema rechi il previsto marchio di conformità CE, sia accompagnato dalla documentazione tecnica e dalle istruzioni di utilizzo (che sempre l'articolo 3 definisce come "*le informazioni per informare l'utente, in particolare, dello scopo previsto e dell'uso corretto di un sistema di intelligenza artificiale, incluse le informazioni sulle impostazioni relative al contesto geografico, comportamentale o funzionale specifico all'interno del quale il sistema di IA ad alto rischio è destinato ad operare*") e che tanto il fornitore quanto l'importatore abbiano a loro volta assolto agli adempimenti loro prescritti dal Regolamento.

Anche il distributore, qualora abbia verificato (o ritenga ragionevolmente) la non conformità del sistema IA ad alto rischio, si asterrà dal rendere disponibile il sistema sul mercato e informerà il fornitore e l'importatore ove da detta non conformità possano discendere rischi per la salute o la sicurezza degli utenti o rischi di lesione di diritti fondamentali. Egli è poi responsabile delle fasi di magazzino e trasporto dei sistemi IA ad alto rischio per tutto il periodo durante il quale sovrintende a tali fasi.

Il distributore, quando ritenga o abbia ragione di ritenere che un sistema IA ad alto rischio che egli ha reso disponibile sul mercato non è conforme ai requisiti prescritti dal Regolamento IA, dovrà porre in essere tutte le azioni correttive del caso (o farle intraprendere al fornitore, importatore o altro operatore) per rendere il sistema conforme oppure dovrà predisporre il ritiro o il richiamo del sistema ("*richiamo di un sistema di IA*": qualsiasi misura volta a ottenere il ritorno al fornitore di un sistema di IA messo a disposizione degli utenti; "*ritiro di un sistema di IA*" indica qualsiasi misura volta a prevenire la distribuzione, la visione e l'offerta di un sistema IA). L'obbligo di informare le autorità nazionali competenti (tutte quelle degli Stati Membri ove i sistemi IA sono stati resi disponibili) ove da sistemi IA ad alto rischio non conformi possano discendere rischi per la salute o la sicurezza degli utenti o rischi di lesione di diritti fondamentali è per il distributore ulteriormente dettagliato (rispetto al medesimo obbligo che grava sull'importatore) dalla prescrizione di "*fornire dettagli, in particolare, delle non conformità riscontrate e delle azioni correttive intraprese*" (cfr. art. 27.4 Reg. IA).

Infine, i distributori devono sottostare ai medesimi obblighi che più sopra abbiamo elencato – ai nn. 1-3 – per i rappresentanti autorizzati e per gli importatori nell'ambito dei rapporti e della cooperazione con le autorità nazionali competenti

Vi è infine una rilevante previsione – una sorta di clausola generale – che si applica a tutti i soggetti della filiera: l'articolo 28, rubricato "*Obblighi per i distributori, gli importatori gli utenti e qualsiasi altra terza parte*". Tale norma prevede la "trasformazione" immediata in "*fornitore*" ai sensi e per gli effetti del Regolamento IA (con la immediata sottoposizione ai pesanti obblighi di cui all'articolo 16 per i fornitori di sistemi IA ad alto rischio) per qualsiasi soggetto che:

a) immetta sul mercato o in servizi un sistema IA ad alto rischio identificandolo con il proprio nome o il proprio marchio;
b) modifichi lo "scopo previsto" di un sistema IA ad alto rischio già immesso sul mercato o in servizio;
c) apporti ad un sistema IA ad alto rischio una modifica sostanziale (che l'art. 3.23 Reg. IA definisce come "*una modifica al sistema di intelligenza artificiale in seguito alla sua immissione mercato o messa in servizio che influisce sulla conformità del sistema di IA ai i requisiti di cui al Titolo III, Capitolo 2 del Regolamento o si sostanzia in una modifica dello scopo previsto per il quale il sistema di IA è stato progettato*");

Gli effetti giuridici (anche nella prospettiva della responsabilità sia contrattuale che per fatto illecito) derivanti dall'articolo 28 Reg. IA sono rilevanti poiché laddove – in particolare - un qualsiasi soggetto della filiera modifichi lo "scopo previsto" di un sistema IA ad alto rischio già immesso sul mercato o in servizio o apporti a un sistema IA ad alto rischio una modifica sostanziale, si determinerà la immediata conseguenza che il fornitore originario che aveva immesso sul mercato o in servizio il sistema non sarà più considerato tale (sostituito appunto dal soggetto che ha effettuato le modifiche citate) e non sarà più responsabile ai sensi e per gli effetti del Regolamento IA.

§ 2.1 Segue: il caso particolare degli obblighi imposti agli utenti di sistemi di Intelligenza Artificiale ad alto rischio. Gli obblighi gestionali e informativi e l'impatto sui contratti di fornitura.

L'utente di un sistema IA ad alto rischio è definito dall'art. 3.4 del Regolamento IA come "*qualsiasi persona fisica o giuridica, autorità pubblica, agenzia o altro ente che utilizza un sistema di intelligenza artificiale sotto la sua autorità*"; tale definizione di *utente* non si applica al caso di utilizzo di un sistema di Intelligenza Artificiale nell'ambito di un'attività personale o di un'attività non professionale (va evidenziata l'ampiezza di tale definizione, atta a ricomprendere soggetti e situazioni anche molto diverse tra di loro, oltre alla inapplicabilità della medesima definizione al cosiddetto "*uso domestico*" di un sistema di IA).

Quando pensiamo agli "utenti" di sistemi IA ad alto rischio non dobbiamo porci solo in una prospettiva "consumeristica" dell'acquirente finale (per esempio: di una vettura a guida autonoma), ma pensare altresì a soggetti pubblici (es: persino i governi o una pubblica amministrazione) e privati (es: datori di lavoro rispetto a lavoratori; docenti rispetto a studenti, etc) che impiegano per finalità varie un sistema IA ad alto rischio e che perciò sono soggetti ad obblighi diretti a tutela dei destinatari finali (cittadini, lavoratori, etc) delle possibili conseguenze derivanti dall'impiego di tali sistemi.

Di particolare interesse – dunque - la scelta del Legislatore di prevedere *obblighi attivi* per gli utenti dei sistemi IA ad alto rischio (comunque per qualsiasi utente, anche persona singola, che non impiega il sistema per scopi meramente personali). L'articolo 29 Reg. IA – difatti – prescrive specifici obblighi indirizzati a questa categoria di soggetti, a partire da

quello di rispettare la manualistica e le istruzioni di utilizzo: generalmente questa è una clausola contrattuale che i fornitori impongono – ai fini della responsabilità – nelle condizioni generali di contratto. Qui viene invece assunta quale clausola legale.

Gli utenti dei sistemi IA ad alto rischio sonno soggetti a un duplice ordine di obblighi: quelli derivanti dal Regolamento IA (o da altre norme UE) e quelli che la legislazione nazionale dello Stato Membro può imporre, ferma restando in ogni caso la libertà dell'utente di organizzare le proprie risorse e attività allo scopo di implementare le misure di sorveglianza umana (cfr. art. 14 Reg. IA) indicate dal fornitore.

Quando l'utente è anche la fonte (successiva) dei *dati di input* (cfr. art. 3.32 Reg. IA) nel senso che esercita un controllo sui *dataset* di (ulteriore) addestramento che il sistema acquisisce una volta messo in uso, allora l'utente assumerà anche la responsabilità della qualità complessiva dei dati (completezza, rappresentatività, specificità in ordine al contesto, etc) in rapporto allo "scopo previsto" del sistema IA che utilizza.

Interessante è poi l'art. 29.4 Reg. IA perché introduce uno scenario per il quale la relazione contrattuale tra l'utente di un sistema IA ad alto rischio e il fornitore non si definisce con la stipula dell'accordo commerciale di fornitura o comunque non si caratterizza solo per le successive esigenze di manutenzione, aggiornamento o supporto. L'utente, difatti, è chiamato a tenere costantemente informato il fornitore (e il distributore) che gli ha venduto il sistema IA, "*monitorando continuamente l'operatività del sistema in base alle istruzioni di utilizzo*" e qualora abbia verificato (o ritenga ragionevolmente) la non conformità del sistema IA ad alto rischio, deve sospenderne immediatamente l'uso e informare il fornitore (e il distributore) ove da detta non conformità possano discendere rischi per la salute o la sicurezza o rischi di lesione di diritti e libertà fondamentali. L'obbligo di informare il fornitore e il distributore scatta per l'utente anche quando egli abbia identificato qualsiasi "incidente grave" o qualsiasi "malfunzionamento" del sistema IA (che dovrà disattivare). Si ricordi che l'articolo 3 Reg. IA definisce "incidente grave" "qualsiasi incidente che, direttamente o indirettamente, comporta, potrebbe aver comportato o potrebbe comportare (si noti l'incertezza del "potrebbe aver comportato": in effetti il funzionamento o malfunzionamento di certi sistemi IA – come quelli che utilizzano il deep learning o le reti neurali e possono assumere decisioni autonome – può risultare sconosciuto anche ai suoi operatori, che ad esempio non hanno alcuna possibilità di verificare o controllare cosa avviene nei "nodi" più profondi del sistema IA e come vengono precisamente assunte le decisioni operative…) quanto segue:

(a) la morte di una persona o gravi danni alla salute di una persona, alla proprietà o all'ambiente,
b) un'interruzione grave e irreversibile della gestione e del funzionamento di infrastruttura critica.

Tale obbligo informativo dell'utente verso il fornitore va letto specularmente all'articolo 62 del Regolamento IA che prescrive ai fornitori di sistemi IA ad alto rischio già immessi sul

mercato della UE di notificare ogni "incidente grave" o "malfunzionamento" di detti sistemi alle autorità di sorveglianza del mercato in ciascuno Stato membro "*immediatamente dopo che il fornitore abbia stabilito una connessione causale tra il sistema IA ad alto rischio e il malfunzionamento o il grave incidente o immediatamente dopo che il fornitore abbia ritenuto non irragionevole tale connessione causale e – in ogni caso – non più tardi di 15 giorni dopo che il fornitore è divenuto consapevole* (anche per le informazioni che gli avrà fornito l'utente, n.d.r.) *di tale malfunzionamento o incidente grave*". Come è evidente, riecheggia in questa disposizione (art. 62.2 Reg. IA) il meccanismo della notifica della *data breach* da parte dei Titolari del trattamento nel sistema del Regolamento UE 679/2016 (ed in effetti un malfunzionamento di un sistema IA ad alto rischio può anche comportare una *data breach* nella prospettiva *data protection*).

Ma il coinvolgimento dell'utente, piuttosto pesante dal punto di vista organizzativo e procedurale (si pensi agli utenti aziende), sta nella prescrizione in base alla quale ove egli non riesca a raggiungere il fornitore, si sostituirà automaticamente – come soggetto obbligato – al fornitore medesimo e sarà lui a dover procedere alle sopra citate notifiche alle autorità di sorveglianza del mercato (che a loro volta informeranno gli enti nazionali e le pubbliche autorità menzionate all'art. 64.3 Reg. IA, oltre alla Commissione UE, in base a specifiche linee guida procedurali che la Commissione rilascerà appositamente).

Altro obbligo che impatterà sulle procedure interne delle aziende e sull'organizzazione tecnica e documentale dell'utente è quello di tenere traccia e registrare i *logs* automaticamente generati da sistemi IA ad alto rischio, nella misura in cui essi siano sotto il controllo dell'utente. Difficoltà applicative determinerà la generica e ambigua previsione di "*conservare i logs registrati per un periodo proporzionato rispetto allo scopo previsto di ciascun sistema IA ad alto rischio, ai sensi della normative nazionale o della UE*".

Infine, gli utenti di sistemi IA ad alto rischio dovranno utilizzare le informazioni che ai sensi dell'articolo 13 Reg. IA devono essere loro fornite in maniera trasparente per l'utilizzo corretto e consapevole dei sistemi, onde condurre la valutazione di impatto preventiva sulla protezione dei dati personali obbligatoria ai sensi dell'art. 35 del GDPR o dell'art. 27 della Direttiva 2016/680 sui trattamenti di dati a fini di prevenzione, indagine, accertamento e perseguimento di reati: un interessante punto di contatto – codificato – tra normative che sono casualmente e logicamente intrecciate tra loro.

§ 3. Le procedure di valutazione e certificazione di conformità dei sistemi IA ad alto rischio. Rinvio.

Il Capo IV del Regolamento IA (artt. 30-39) definisce il quadro giuridico per il coinvolgimento degli organismi notificati in qualità di terzi indipendenti nelle procedure di valutazione della conformità dei sistemi IA ad alto rischio.

Il Capo V (artt. 40-51) del Regolamento IA dettaglia la disciplina relativa alle procedure di valutazione e accertamento della conformità dei sistemi IA ad alto rischio. L'approccio utilizzato dal Legislatore per la valutazione di conformità mira a ridurre al minimo gli oneri per gli operatori economici e per organismi notificati.

Le regole ivi identificate prescrivono che i sistemi di Intelligenza Artificiale destinati ad essere integrati nei prodotti fabbricati a sensi delle normative settoriali elencate al paragrafo A dell'Allegato II al Regolamento IA (giocattoli, ascensori, sistemi di trasporto, sistemi di comunicazione, dispositivi medici, etc) siano soggetti agli stessi meccanismi di verifica *ex ante* ed *ex post* della conformità dei prodotti di cui sono componenti alla legislazione di settore (cfr. Allegato II Reg. IA). Il rafforzamento delle garanzie risiede nel fatto che i sistemi IA che siono componenti di tali prodotti dovranno rispettare sia i requisiti di conformità del Regolamento IA che quelli stabiliti dalla legislazione settoriale per i prodotti di cui sono una componente.

Per quanto riguarda i sistemi di IA ad alto rischio *stand alone* di cui all'Allegato III, viene stabilito un nuovo un sistema di *conformity assessment* basato su controlli interni *ex ante* richiesti ai fornitori (ad eccezione dei sistemi di identificazione biometrica a distanza che sono soggetti alla valutazione della conformità da parte di terze parti indipendenti) e controlli *ex post* (sorveglianza successiva alla immissione sul mercato) che detti fornitori devono garantire successivamente alla commercializzazione.

Oltre alle procedure di valutazione della conformità, il Capo V disciplina la procedura di registrazione europea dei sistemi IA ad alto rischio, la costituzione da parte della Commissione UE di un database europeo dei sistemi notificati, le certificazioni, gli standard armonizzati, il marchio CE di conformità, etc: ne abbiamo parlato diffusamente, quanto agli adempimenti pratici da porre in essere, nella precedente parte terza del presente commentario.

§ 4. La regolamentazione sui deepfakes e i nuovi diritti delle persone fisiche nell'ambito dell'interazione con sistemi di Intelligenza Artificiale.

L'articolo 52 del Regolamento introduce per la prima volta al mondo delle norme a contrasto dei cosiddetti *deepfake*. Il *deepfake* (che incrocia la definizione di *deep learning*) è una sofisticata manipolazione di immagini e video già esistenti (con *face-swap*, scambi di viso) che determina la creazione di nuovi contenuti fasulli (appunto: *fake*) ma del tutto realistici e credibili. Più in particolare, immagini corporee e facciali catturate in Internet vengono rielaborate e adattate a un contesto diverso da quello originario tramite un sofisticato algoritmo di Intelligenza Artificiale. Definita come "*l'ultima crisi morale di internet*", la fenomenologia del *deepfake* rappresenta un elevatissimo pericolo democratico, poiché video e immagini falsi (ma perfettamente credibili) di personaggi pubblici (es: politici) che hanno già circolato in rete hanno dimostrato ampiamente tutta la capacità di spostare l'opinione pubblica (e persino le intenzioni di voto) di cittadini non in grado di

riconoscere il *fake*: si pensi ai recenti casi di *deepfakes* che hanno colpito personaggi come la *speaker* ella Camera dei Rappresentanti USA Nancy Pelosi, l'ex Presidente Obama, la candidata alle elezioni Hillary Clinton.

Anche se il Legislatore non ci fornisce una specifica definizione di *deepfake* nel lungo elenco di cui all'articolo 3 del Regolamento IA, nell'articolo 52, comma 3, ci si concentra sui sistemi IA che rendono possibile il fenomeno, definendo i contorni del processo di formazione del *fake* e i suoi risultati: "*sistemi di Intelligenza Artificiale che generano o manipolano immagini, contenuti audio o video che assemblano efficacemente persone, oggetti, luoghi o altre entità o eventi reali ed esistenti onde far sembrare a una persona che siano autentici o affidabili*". Il Legislatore va dunque oltre rispetto alle definizioni di *deepfake* che possiamo trovare nella pratica, visto che i sistemi IA sono in grado (e sempre più lo saranno, con sempre maggiore accuratezza) non solo di *manipolare* contenuti esistenti, ma anche di *generare* ex novo immagini/video/audio di persone (alle quali possiamo far affermare ciò che vogliamo e che possiamo rendere protagonisti di azioni in video che non hanno commesso nella realtà). Il tutto *assemblando* (quasi come in una sceneggiatura cinematografica vera e propria) *persone, oggetti, luoghi* ed *eventi* nella costruzione di un contenuto fasullo ma perfettamente credibile nel suo apparire "*autentico e affidabile*". Si intuisce la estrema pericolosità per i diritti e le libertà fondamentali degli individui: non solo dei soggetti che – loro malgrado – sono i protagonisti dei *deepfakes*, ma anche dei destinatari che sono indotti a ritenere autentico il fasullo, con l'effetto (spesso voluto dagli autori dei *deepfakes*) di condizionarne illecitamente scelte, opinioni e conseguenti comportamenti.

Come risponde il Legislatore UE alle sopra rilevate criticità e rischi connessi ai *deepfakes*?

L'obbligo è solo di tipo informativo poiché l'autore del *deepfake* (o meglio, per citare la norma, gli utilizzatori di un sistema IA che lo genera) deve rendere evidente che i contenuti sono artefatti e generati o manipolati artificialmente. Non vi è dunque un divieto, e anzi, tale (limitato) obbligo di rendere evidente il fasullo nel *deepfake* (comunque sanzionato – in caso di omissione informativa ai terzi - fino a 20 milioni di Euro o fino al 4% del fatturato globale annuo) rischia tuttavia di essere svuotato dalla deroga contenuta al medesimo art. 52.3 dell'impiego lecito dei d*eepfakes* come "*necessari per l'esercizio del diritto alla libertà di espressione e del diritto alla libertà delle arti e delle scienze garantito nella Carta dei diritti fondamentali dell'UE soggetto a garanzie adeguate per i diritti e le libertà di terzi*". Il limite e il superamento di tali diritti fondamentali andranno di volta in volta valutati (anche sulla base della Giurisprudenza della Corte di Giustizia UE). A parere di chi scrive, in ogni, caso, si tratta di una occasione persa nel tentativo di contenere e gestire il preoccupante fenomeno dei *deepfakes*: il Legislatore si è approcciato con una non condivisibile "timidezza regolatoria".

Di deroga all'impiego di "*sistemi di Intelligenza Artificiale che generano o manipolano immagini, contenuti audio o video*" ve ne è anche un'altra e riguarda l'assai interessante

evoluzione che – dalla lettura della norma – può intuirsi rispetto allo scenario delle attività svolte dalle autorità pubbliche che sempre più impiegano la tecnologia nelle attività di ricerca, investigazione, accertamento, prevenzione e perseguimento dei reati: laddove difatti i *deepfakes* siano generati da tali soggetti pubblici e si configurino come strumenti di indagine (al pari, ad esempio, dei *trojan* da lungo tempo utilizzati nelle indagini per le intercettazioni) per l'accertamento, prevenzione e accertamento dei reati, ovviamente non vi è alcun obbligo di disvelare l'artifizio.

L'articolo 52 del Regolamento IA introduce anche nuovi diritti per le persone fisiche, speculari e conseguenti al funzionamento dei sistemi IA e al sorprendente risultato delle tecniche di apprendimento o *deep learning*. Dal momento che – difatti – il livello di sofisticatezza raggiunto da tali sistemi li rende indistinguibili dall'operato umano (si pensi ai *chatbot,* assistenti elettronici sintetici e distanza che dialogano in linguaggio naturale senza che ci si possa accorgere che si tratta di sistemi IA e non di essere umani), viene introdotto l'obbligo (e il corrispondente diritto) che già la Commissione UE – nel *Libro Bianco sull'Intelligenza Artificiale* del Febbraio 2020 – riteneva fondamentale: quello di essere informati che si sta interagendo con un sistema IA e non con un essere umano. Anzi, l'art. 52.1 introduce un obbligo *by design*, poiché fin "*dalla fase di progettazione e sviluppo di sistemi IA destinati ad interagire con persone fisiche*" tanto la progettazione che lo sviluppo dovranno essere condotti in modo tale che le persone siano consapevoli o informate che stanno interagendo con un sistema non umano. Tale obbligo non si applica: (a) quando è evidente ed ovvio dalle circostanze e dal contesto di utilizzo; (b) quando tali sistemi sono autorizzati dalla legge in quanto destinati ad essere impiegati nelle attività di ricerca, investigazione, accertamento, prevenzione e perseguimento dei reati.

Altro diritto ad essere informati (in questo nuovo catalogo di cui all'articolo 52 Reg. IA) riguarda l'impiego di:

- "*sistemi di riconoscimento delle emozioni*"*:* indica un sistema di IA che ha lo scopo di identificare o dedurre emozioni o intenzioni di persone fisiche sulla base dei loro dati biometrici;

- "*sistemi di classificazione biometrica*"*:* un sistema di IA con lo scopo di assegnare persone fisiche a categorie specifiche, come sesso, età, colore dei capelli, colore degli occhi, tatuaggi, origine etnica o orientamento sessuale o politico, sulla base dei loro dati biometrici.

Difatti, che impiega tali sistemi deve informare le persone che vi sono esposte che essi sono operativi (a meno che il sistema di classificazione biometrica non sia autorizzato dalla legge come strumento di ricerca, investigazione, accertamento, prevenzione e perseguimento di un reato).