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 Quinta

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 quarto contributo si è proceduto 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 è illustrata la prima disciplina al mondo dei cosiddetti *deepfakes*.

Nel presente e conclusivo contributo cominceremo ad esaminare la nuova disciplina europea dei cc.dd *regulatory sandboxes*, per poi analizzare compiti e funzioni del nuovo organismo istituito dal Reg. IA, e cioè il *Comitato europeo per l'Intelligenza Artificiale*, che analizzeremo in rapporto a compiti e funzioni delle autorità nazionali competenti e in una prospettiva comparativa anche con l'analogo Comitato previsto dal RGPD nel settore *data protection*. Chiuderemo infine l'analisi della proposta di Regolamento IA illustrando l'impianto sanzionatorio, che si caratterizza – come già fu per il RGPD – per la severità degli importi sanzionatori.

§ 2. I regulatory sandboxes: nuovi strumenti giuridici di sperimentazione anticipata delle soluzioni tecnologiche di IA.

Il Titolo V ("*Misure di supporto all'Innovazione*") del Regolamento IA introduce norme volte a creare un quadro giuridico che la Commissione UE ha presentato come "*innovation-friendly*", "*future-proof*" e resiliente a cambiamenti radicali. A tal fine, si incoraggia l'adozione a livello nazionale dei cosiddetti *regulatory sandboxes*.

Ma cosa sono questi "*recinti sabbiosi regolatori*" (o "*spazi di sperimentazione normativa*" come li chiama la versione italiana del Regolamento IA)?

I "*regulatory sandboxes*" sono sostanzialmente degli strumenti giuridici che consentono la predisposizione di ambienti di prova e sperimentazione per testare anticipatamente – tra gli altri - l'impatto regolatorio e di mercato nel corso dello sviluppo di servizi tecnologici, sotto la guida delle autorità competenti che svolgono attività di supervisione della sperimentazione, in modo da implementare con maggior facilità soluzioni che siano "*legal by design*". Come nell'Informatica esiste il *sandbox* inteso come un ambiente di test, sperimentazione e controllo finalizzato a verificare le funzionalità di un software prima che questo sia messo in produzione (dall'Informatica è difatti mutuata la definizione, che però letteralmente rimanda alla particolare struttura recintata contenente sabbia che permette il gioco dei bambini in un ambiente controllato e sicuro), nel sandbox regolatorio l'azienda ammessa alla sperimentazione può anticipatamente sviluppare soluzioni innovative in un ambiente controllato, a contatto con il mercato reale e con la supervisione di una autorità di controllo. Per comprendere meglio le caratteristiche dei *sandboxes normativi* può farsi riferimento a uno dei modelli meglio sviluppati in Europa: il *Regulatory Sandbox* del Regno Unito, rispetto al quale le aziende ammesse operano sotto la supervisione della *Financial Conduct Authority* (FCA). Come si legge sul sito *web* della FCA, gli obiettivi sono quelli di:

- agevolare la fase di test di beni e servizi tecnologici in un ambiente controllato;
- ridurre il cosiddetto *time-to-market* e ridurne potenzialmente il costo;
- sostenere le aziende nell'identificare i presidi migliori per tutelare gli utenti;

- agevolare l'accesso a risorse finanziarie.

L'azienda che voglia essere ammessa al *sandbox* (o alla "*coorte*", così come sono chiamate in UK, in base al metodo di suddivisione, le aziende partecipanti) deve seguire una procedura di autorizzazione, nella quale vengono valutati preferenzialmente determinati requisiti (es: capacità di innovare un certo segmento di mercato con le proprie soluzioni tecnologiche, destinazione del bene o del servizio al mercato nazionale, etc). Le aziende ammesse fruiscono di una stretta cooperazione dell'autorità di supervisione, la quale monitora da vicino lo sviluppo e l'implementazione dei test, ad esempio collaborando con l'azienda (l'autorità fornisce consulenza e una sorta di *cassetta degli attrezzi* per svolgere i test) e concordando tutele personalizzate per i consumatori (tra l'altro, uno degli obiettivi del *sandbox* è anche quello di ridurre i costi per i consumatori). I test si svolgono per una durata temporale limitata (es: 18 mesi) e con un numero limitato di clienti (ma i test sono reali e svolti – come si diceva - sul mercato e a condizioni di mercato). Una parte rilevante della sperimentazione è appunto quella circa l'impatto regolatorio. Lo sviluppo del bene o servizio tecnologico viene infatti valutato non solo dal punto di vista commerciale, di mercato e tecnico, ma anche nella prospettiva:

- della corretta interpretazione e applicazione delle disposizioni normative vigenti, rispetto alle quali l'autorità di supervisione svolge un compito di chiarimento e supporto, fornendo indicazioni informali sulle potenziali implicazioni normative di un prodotto, servizio o modello di business innovativo che è in una fase iniziale di sviluppo;
- di come il quadro normativo possa influenzare il bene o il servizio una volta definitivamente immesso sul mercato;
- della disapplicazione o modifica di norme e regolamenti settoriali applicabili per sperimentare che effetti avrebbe sul bene o servizio nell'ottica del mercato e dei consumatori (ovviamente la disapplicazione vale per la sola fase di *test*);
- dell'impegno da parte dell'Autorità di supervisione (che sottoscrive una specifica "*no enforcement letter*") a non applicare per tutta la fase di test sanzioni in caso di disallineamento o violazione dei parametri concordati di sperimentazione da parte dell'azienda (con salvezza però delle tutele per i consumatori).

In sostanza, lo strumento giuridico del *regulatory sandbox* è di straordinaria utilità, soprattutto per la sua flessibilità che comporta – all'esito della sperimentazione – vantaggi per tutti: per l'azienda i vantaggi sono tutti quelli sopra indicati nella sintetica descrizione di come funziona lo strumento; ma anche le autorità di sorveglianza e lo stesso legislatore possono tarare meglio i loro interventi regolatori e normativi, poiché possono sfruttare i risultati della sperimentazione anche per migliorare la *qualità* della legislazione settoriale o meno. E' difatti ben presente agli operatori come negli ultimi anni si assista ad un sempre più grave scadimento delle modalità con le quali vengono scritte le norme (chi scrive ha coniato la dizione di "*sciatteria redazionale*" per identificare il fenomeno), leggi che poi sono difficilmente applicabili proprio perché illeggibili e incomprensibili (vuoi per la struttura –

con un unico articolo e centinaia di commi – vuoi proprio per lingua, grammatica e costruzioni sintattiche utilizzate dal Legislatore nell'articolato). Si aggiunga, poi, che regolamentare la tecnologia comporta ulteriori rischi: in passato il Legislatore ha spesso introdotto nell'ordinamento norme che prescindevano tanto da una compiuta conoscenza – in capo a chi legiferava - delle specifiche tecniche, funzionali e operative della tecnologia che si voleva disciplinare, quanto da una (preventiva) valutazione di impatto (sul mercato, sui fornitori, sugli utenti, etc) delle regole emanate, determinandosi situazioni di gravi criticità applicative delle norme, purtroppo emerse *ex post*.

Alla luce di tutto questo, si comprenderà come lo strumento del *regulatory sandbox* potrebbe davvero essere ulteriormente sviluppato nella sua potenzialità di costituire – anche per i legislatori – un nuovo *paradigma* di redazione delle norme, che parta dalle specifiche caratteristiche della tecnologia da regolare (e dagli esiti della sue sperimentazione preventiva), abbandonando la generalità e astrattezza per fondarsi – come qualcuno ha detto – su *norme granulari* ("*granulars norms*") già sperimentate nelle fasi di test nella loro efficacia regolatoria e di *favor* del mercato.

Si diceva più sopra che anche l'Italia ha per la prima volta introdotto nell'ordinamento nazionale lo strumento del *regulatory sandbox*. Già nel documento intitolato *Proposte per una strategia italiana per l'intelligenza artificiale* e rilasciato dal Tavolo di esperti sull'IA istituito dal Ministero dello Sviluppo Economico, si leggeva: "*Verso nuovi strumenti di governo per l'innovazione. Accanto alla piena realizzazione di una strategia nazionale per la qualità della regolazione, in linea con i migliori standard internazionali e con gli obiettivi di sviluppo sostenibile, il Governo deve porre le basi per l'utilizzo di strumenti di regolazione sperimentale (sandboxes), di innovation deal per accelerare il processo di revisione della legislazione in modo compatibile con l'evoluzione tecnologica, e di politiche di innovazione dal lato della domanda, incluso l'avvio di challenges tese a indirizzare l'innovazione verso il soddisfacimento dei bisogni della società italiana*."

La legge 28 giugno 2019, n. 58 di conversione del decreto legge 30 aprile 2019, n. 34 ("*Decreto Crescita*") all'art. 36, comma 2-*octies* ha poi previsto l'istituzione presso il Ministero dell'economia e delle finanze (MEF) del *Comitato FinTech*. Il Comitato ha il compito di individuare gli obiettivi, definire i programmi e porre in essere le azioni per favorire lo sviluppo della tecno-finanza. In base alle nuove norme, e alla luce del crescente ruolo dell'innovazione finanziaria negli ambiti presidiati dalle autorità di vigilanza e controllo, le autorità sono autorizzate, singolarmente o in collaborazione tra loro, a stipulare accordi con università e centri di ricerca ad esse collegati aventi ad oggetto lo studio dell'applicazione alla loro attività istituzionale degli strumenti di intelligenza artificiale, di registri contabili criptati e di registri distribuiti, nonché la formazione del proprio personale.

La legge 28 giugno 2019, n. 58 di conversione del decreto legge 30 aprile, n. 34, ha introdotto anche una disciplina dei *regulatory sandbox* (art. 36, commi da 2-*bis* a 2-*septies*). Con tale intervento legislativo si è introdotto nell'ordinamento nazionale uno strumento finalizzato a consentire sperimentazioni di applicazioni *FinTech* che, mediante nuove

tecnologie, quali l'intelligenza artificiale e i registri distribuiti, possano consentire l'innovazione di servizi e prodotti nei settori finanziario, creditizio, assicurativo e dei mercati regolamentati (prossimamente vedrà la luce con d.m. il regolamento del Ministero dell'Economia e delle Finanze recante norme in materia di *Comitato FinTech* e sperimentazione *FinTech*, in attuazione dell'art. 36, commi 2-bis e 2-octies del Decreto Legge 30 aprile 2019, n. 34, convertito con modificazioni dalla Legge 28 giugno 2019, n. 58).

Se dunque *regulatory sandboxes* specifici già esistono in diversi Stati europei, oltre al Regno Unito (Italia inclusa, come abbiamo visto, ma anche Norvegia, Svizzera e Olanda si sono dotate di tale strumento), con l'adozione del Regolamento IA essi troverebbero un riconoscimento formale e omogeneo a livello UE, creando così le condizioni per creare "*sandboxes*" anche per progetti paneuropei e internazionali. In tale prospettiva, il Considerando 72 della proposta di Regolamento IA prevede:

"*Gli obiettivi dei regulatory sandboxes dovrebbero essere quelli di promuovere l'innovazione dell'IA attraverso la predisposizione di un ambiente controllato di sperimentazione e test nello sviluppo e nella fase di pre-commercializzazione, al fine di garantire la conformità dei sistemi innovativi di Intelligenza Artificiale al presente regolamento e alle altre normative applicabili dell'Unione e degli Stati membri; rafforzare la certezza del diritto per gli innovatori, la supervisione delle autorità competenti, la comprensione delle opportunità, dei rischi emergenti e degli impatti dell'uso dell'IA e accelerare l'accesso ai mercati, anche rimuovendo le barriere per le piccole e medie imprese (PMI) e per le start-up. Per garantire un'attuazione uniforme in tutta l'Unione ed economie di scala, è opportuno stabilire regole comuni per la regolamentazione e l'implementazione dei sandbox e un quadro per la cooperazione tra le autorità competenti coinvolte nella supervisione dei sandbox. Il presente regolamento dovrebbe fornire la base giuridica per l'utilizzo dei dati personali raccolti per altri scopi per lo sviluppo di determinati sistemi di IA nell'interesse pubblico all'interno dei regulatory sandboxes, in linea con l'articolo 6, paragrafo 4, del regolamento (UE) 2016/679 e l'articolo 6 del regolamento (UE) 2018/1725 e fatto salvo l'articolo 4, paragrafo 2, della direttiva (UE) 2016/680. I partecipanti al sandbox dovrebbero prestare garanzie adeguate e cooperare con le autorità competenti, anche seguendo le loro indicazioni e agendo rapidamente e in buona fede per mitigare eventuali rischi elevati per la sicurezza e i diritti fondamentali che potrebbero sorgere durante lo sviluppo e la sperimentazione nel sandbox. Il comportamento dei partecipanti al sandbox dovrebbe essere preso in considerazione quando le autorità competenti decidono se imporre una sanzione amministrativa ai sensi dell'articolo 83, paragrafo 2, del regolamento 2016/679 e dell'articolo 57 della direttiva 2016/680*".

§ 2.1. Gli articoli 53-55 del Regolamento IA sui regulatory sandboxes.

L'articolo 53 del Regolamento IA introduce la disciplina applicabile ai *regulatory sandboxes* sull'IA (che nel testo italiano del Regolamento IA vengono definiti *spazi di sperimentazione normativa dell'IA)* istituiti da una o più autorità competenti degli Stati Membri o dal Garante Europeo per la protezione dei dati personali. Tali strumenti (per i

quali l'art. 55 Reg. IA prevede un accesso prioritario, agevolato - anche dal punto di vista delle tariffe – e tarato sulle specifiche esigenze di *start up* e fornitori di piccole dimensioni) dovranno fornire un ambiente controllato che faciliti - per un periodo limitato di tempo e prima della loro immissione sul mercato o della loro messa in servizio - lo sviluppo, la sperimentazione e la validazione di sistemi innovativi di IA, nell'ambito di uno specifico programma. Tale programma deve essere attuato sotto la diretta supervisione e con la guida delle autorità competenti allo scopo di assicurare la conformità ai requisiti prescritti dal Regolamento IA o dalle altre normative nazionali o dell'Unione, se applicabili (i partecipanti, invece, restano responsabili ai sensi della normativa applicabile dell'Unione e degli Stati membri in materia di responsabilità per eventuali danni arrecati a terzi a seguito della sperimentazione che ha luogo nel *sandbox*).

Una prima considerazione: il legislatore menziona i "*sistemi di intelligenza artificiale innovativi*" quale oggetto e presupposto degli *spazi di sperimentazione normativa* senza tuttavia specificare cosa si intenda con il requisito (che appare specifico) dell'innovazione (e non rinvenendosi nemmeno alcuna specifica definizione tra le 44 elencate all'articolo 3 del Reg. IA). Ciò, in assenza di ulteriori chiarimenti o modifiche nel corso di approvazione del testo, potrebbe portare a difficoltà applicative, ad esempio in sede di ammissione alle sperimentazioni di sistemi IA che debbano qualificarsi come "*innovativi*" ai sensi dell'art. 53, comma 1 Reg. IA. In ogni caso, al di là di tali criticità, è certo che la disciplina sui *regulatory sandboxes* non è limitata ai *sistemi IA ad alto rischio*, ma è applicabile indifferentemente a tutti i sistemi IA.

Lo specifica disciplina sugli *spazi di sperimentazione normativa* mostra inoltre – ancora una volta - la stretta correlazione tra Regolamento IA e normativa sulla protezione dei dati personali nel (intesa ad ampio raggio come insieme delle norme di cui al Regolamento (UE) 2016/679, al Regolamento (UE) 2018/1725 e alla Direttiva (UE) 2016/680). Intanto, gli Stati membri devono assicurare che nella misura in cui i "*sistemi di intelligenza artificiale innovativi*" coinvolgono il trattamento di dati personali o in altro modo ricadono nell'ambito del mandato di vigilanza di altre autorità nazionali o di altre autorità competenti che forniscono o supportano l'accesso ai dati, le autorità nazionali di protezione dei dati e dette autorità dovranno essere associate al funzionamento del *sandbox*. Rispetto alle discipline nazionali su tale strumento giuridico, la proposta di Regolamento IA insiste – giustamente – sulla stretta correlazione tra attività di sperimentazione e trattamento di dati personali (si pensi – solo per fare alcuni esempi - alla profilazione di consumatori o ai dati raccolti durante la sperimentazione in modalità completamente automatica sull'utilizzo da parte degli utenti finali del bene o del servizio in corso di test, etc). Altra stretta correlazione si rinviene all'articolo 54, comma 1, Reg. IA, rubricato *Ulteriore trattamento dei dati personali per lo sviluppo nello spazio di sperimentazione normativa per l'IA di determinati sistemi di IA nell'interesse pubblico.* Ai sensi della citata norma, nello spazio di sperimentazione normativa per l'IA i dati personali legalmente raccolti per altre finalità possono essere trattati ai fini dello sviluppo e delle prove nel *sandbox* nel rispetto delle seguenti condizioni:

a) i sistemi di IA innovativi devono essere sviluppati per salvaguardare un *interesse pubblico rilevante* in uno o più dei seguenti settori (il Reg. IA riecheggia il concetto di *interesse pubblico rilevante* che il RGPD indica quale presupposto specifico per poter trattare dati di particolare natura superando il divieto di cui all'art. 9, comma 1, RGPD e per poter superare il "congelamento" a cui sono soggetti i dati personali oggetto di una istanza di esercizio del diritto di limitazione, ai sensi dell'art. 18, comma 2 RGPD):

i) la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro le minacce alla sicurezza pubblica e la prevenzione delle stesse, sotto il controllo e la responsabilità delle autorità competenti. Il trattamento si basa sul diritto degli Stati membri o dell'Unione;
ii) la sicurezza pubblica e la sanità pubblica, compresi la prevenzione, il controllo e il trattamento delle malattie;
iii) un elevato livello di protezione e di miglioramento della qualità dell'ambiente;

b) i dati trattati sono necessari per il rispetto di uno o più dei requisiti richiesti in materia di: sistema di gestione dei rischi, governance dei dati, conservazione della documentazione tecnica, sorveglianza umana dei sistemi, informazioni e trasparenza agli utenti, robustezza e sicurezza dei sistemi, qualora tali requisiti non possano essere efficacemente soddisfatti mediante il trattamento anonimizzato, sintetico o di altri dati non personali (si noti l'introduzione del concetto di *trattamento sintetico* dei dati; più correttamente, sono *dati sintetici* quelli generati da algoritmi che riproducono in maniera fedele - sotto il profilo matematico e statistico - *dataset* del mondo reale, senza tuttavia rappresentare persone esistenti oppure elementi ad esse riferibili);
c) esistono meccanismi di monitoraggio efficaci per individuare eventuali rischi elevati per i diritti fondamentali degli interessati durante la sperimentazione nel *sandbox* e meccanismi di risposta per attenuare rapidamente tali rischi e, ove necessario, interrompere il trattamento;
d) i dati personali da trattare nel contesto dello spazio di sperimentazione sono in un ambiente di trattamento dei dati funzionalmente separato, isolato e protetto sotto il controllo dei partecipanti e solo le persone autorizzate hanno accesso a tali dati (le cc.dd *misure di segregazione,* accompagnate da idonee misure organizzative, come ad esempio l'accesso ai dati consentito solo alle persone autorizzate, ciò che riecheggia gli obblighi di sicurezza sui dati di cui all'articolo 32, comma 4, RGPD);
e) i dati personali trattati non devono essere trasmessi, trasferiti o altrimenti consultati da terzi 8dovendo appunto rimanere nel perimetro/recinto sicuro della sperimentazione normativa);
f) il trattamento di dati personali nel contesto dello spazio di sperimentazione non comporta misure o decisioni aventi ripercussioni sugli interessati;
g) i dati personali trattati nell'ambito del *regulatory sandbox* sono cancellati una volta terminata la partecipazione allo spazio di sperimentazione o al raggiungimento del termine del periodo di conservazione dei dati personali;
h) i *log* del trattamento dei dati personali nel contesto dello spazio di sperimentazione sono conservati per la durata della partecipazione allo spazio di sperimentazione e per 1

anno dopo la sua cessazione, al solo scopo di adempiere gli obblighi di rendicontazione e documentazione previsti o da altre normative applicabili dell'Unione o degli Stati membri e solo per il tempo necessario per adempiere tali obblighi;
i) una descrizione completa e dettagliata del processo e della logica alla base dell'addestramento, delle prove e della convalida del sistema di IA è conservata insieme ai risultati delle prove nell'ambito della documentazione tecnica;
j) una breve sintesi del progetto di IA sviluppato nello spazio di sperimentazione, dei suoi obiettivi e dei risultati attesi è pubblicata sul sito web delle autorità competenti.

Di interesse appare poi l'articolo 53, comma 3 Reg. IA che lascia impregiudicati i poteri correttivi e di controllo delle autorità nazionali competenti (autorità diverse dalle "*autorità nazionali di protezione dei dati personali*" che – come si diceva – vengono associate alla sperimentazione, insieme alle autorità nazionali competenti, nel caso di trattamento di dati personali). In caso di *qualsiasi* rischio significativo per la salute e la sicurezza e i diritti fondamentali individuato durante lo sviluppo e le prove nel *sandbox*, le autorità nazionali competenti disporranno (in caso di insuccesso di misure di mitigazione del rischio intraprese) la sospensione del processo di sviluppo e di prova della sperimentazione normativa per l'IA. E' da ritenere, anche se la norma non lo specifica, che in questi casi anche le *autorità nazionali di protezione dei dati personali* potranno disporre il *blocco dei trattamenti*, ex art. 58 RGPD.

Infine, le modalità e le condizioni di funzionamento degli spazi di sperimentazione normativa per l'IA, compresi i criteri di ammissibilità e la procedura per la domanda, la selezione, la partecipazione e l'uscita dallo spazio di sperimentazione, nonché i diritti e gli obblighi dei partecipanti saranno stabiliti in appositi atti delegati da emanarsi a cura della Commissione.

§ 3. Il Comitato Europeo per l'Intelligenza Artificiale e il ruolo delle autorità nazionali. I codici di condotta sull'Intelligenza Artificiale.

Il modello europeo di *governance* dell'Intelligenza Artificiale (denominazione del Titolo VI del Regolamento IA) replica quello che si sta già sperimentando con successo nel settore della tutela dei dati personali e che istituisce una struttura di coordinamento europeo per fornisce consulenza e assistenza alla Commissione UE, agli Stati Membri e alle autorità nazionali di controllo. L'articolo 56 Reg. IA. Istituisce difatti il *Comitato europeo per l'Intelligenza Artificiale*, composto dalle autorità nazionali di controllo sull'IA (a loro volta enti di nuova costituzione, di cui abbiamo parlato nei contributi precedenti), rappresentate dal capo di tale autorità o da un alto funzionario di livello equivalente, dal Garante europeo della protezione dei dati ed eventualmente da altre autorità nazionali che possono essere di volta in volta invitate per questioni di loro competenza (non è difficile immaginare la partecipazione di autorità garanti per la protezione dei dati nazionali).

Il *Comitato europeo per l'Intelligenza Artificiale* differisce tuttavia profondamente, se analizziamo comparativamente struttura, compiti e poteri, da quello omologo istituito dall'articolo 68 RGPD: difatti, mentre il *Comitato europeo per la protezione dei dati personali* ha personalità giuridica, è rappresentato dal suo presidente e vede nella Commissione UE un mero partecipante senza diritto di voto, nel caso del *Comitato europeo per l'Intelligenza Artificiale* esso è soprattutto un organo consultivo della Commissione (che lo presiede, convoca le relative riunioni e fissa l'ordine del giorno) ed ha poi compiti di assistenza e coordinamento delle autorità nazionali e della Commissione.

Inoltre, mentre *Comitato europeo per la protezione dei dati personali* è deputato [ai sensi degli articoli 5.1, lettera (a) e 70, comma 1, lettera (a) RGPD] ad assicurare "*l'applicazione corretta*" del RGPD, a tal fine pubblicando anche "*linee guida, raccomandazioni e migliori prassi*", tali compiti non sono analogamente assegnati all'omologo *Comitato europeo per l'Intelligenza Artificiale* (tra l'altro privo delle garanzie di indipendenza che invece sono specificate per l'altro comitato dall'articolo 69 RGPD). Il *Comitato europeo per l'Intelligenza Artificiale,* difatti, formula pareri, raccomandazioni o contributi scritti su questioni relative all'attuazione del Reg. IA (es: sulle specifiche tecniche, sull'uso delle norme armonizzate o delle specifiche comuni, sulla preparazione di documenti di orientamento) e tale attività appare essere ben diversa dal compito di assicurarne e sorvegliare la corretta applicazione o non è assimilabile allo specifico compito di emanazione di linee guida che l'articolo 70 RGPD assegna al Comitato europeo per la protezione dei dati personali. Probabilmente. L'unico caso in cui il *Comitato europeo per l'Intelligenza Artificiale* potrebbe svolgere una attività paragonabile alla emanazione di linee guida, raccomandazioni o prassi è la specifica attribuzione di contribuire all'uniformità delle pratiche amministrative negli Stati membri, anche per il funzionamento dei *regulatory sandboxes.*

Parimenti privo di centralità è il ruolo del *Comitato europeo per l'Intelligenza Artificiale* se rapportato ai compiti delle autorità nazionali di controllo che lo compongono. Le *autorità nazionali di controllo* sull'Intelligenza Artificiale sono una *species* del più ampio *genus* delle *autorità nazionali competenti*. Si ricorderà che ai sensi dell'articolo 3, nn. 42 e 43 Reg. IA, per:

"*autorità nazionale di controllo*": si intende l'autorità alla quale uno Stato membro attribuisce la responsabilità di attuare e applicare il presente regolamento, di coordinare le attività affidate a tale Stato membro, di fungere da punto di contatto unico per la Commissione e di rappresentare lo Stato membro in seno al Comitato europeo per l'intelligenza artificiale;
"*autorità nazionale competente*": si intende l'autorità nazionale di controllo, l'autorità di notifica e l'autorità di vigilanza del mercato.

L'articolo 59 Reg. IA istituisce un assai farraginoso sistema in base al quale, ciascuno Stato membro:

b) istituisce (*ex novo*) oppure designa *autorità nazionali competenti* (di cui non è però dichiarata l'indipendenza, ma è richiesto che esse siano "*organizzate e gestite in modo che sia salvaguardata l'obiettività e l'imparzialità dei loro compiti e attività*");.
c) designa *un'autorità nazionale di controllo* tra le *autorità nazionali competenti*. L'autorità nazionale di controllo agirà poi come *autorità di notifica* e *autorità di vigilanza del mercato*, a meno che uno Stato membro non abbia motivi organizzativi e amministrativi per designare più di un'autorità.

Il Regolamento IA non fissa il numero di componenti delle autorità nazionali competenti ma richiede che il personale sia dotato di "*competenze e conoscenze che comprendono una comprensione approfondita delle tecnologie, dei dati e del calcolo dei dati di intelligenza artificiale, dei diritti fondamentali, dei rischi per la salute e la sicurezza e di una conoscenza delle norme e dei requisiti giuridici esistenti*". Staremo a vedere se requisiti così stringenti saranno ignorati come spesso è accaduto in Italia nelle designazioni di componenti delle autorità amministrative indipendenti.

Si accennava più sopra ad un sistema tra il farraginoso e il burocratico. E' difatti previsto che ogniqualvolta le autorità nazionali competenti intendono fornire orientamenti e consulenza in relazione a un sistema di IA in settori disciplinati da altre normative dell'Unione, esse devono consultare le autorità nazionali competenti a norma di tale normativa dell'Unione, come opportuno (in un proliferare di competenze e meccanismi di consultazione).

E' poi prevista la facoltà per gli Stati membri di istituire un *punto di contatto centrale* per la comunicazione con gli operatori: davvero non si comprende cosa sia tale puto di contatto centrale e come dovrebbe coordinarsi con l'autorità nazionale competente o di controllo (che ben potrebbe fungere anche da punto di contatto centrale).

Infine, nei casi in cui le istituzioni, le agenzie e gli organismi dell'Unione rientrano nell'ambito di applicazione del Regolamento IA, è il Garante europeo della protezione dei dati ad agire in qualità di autorità competente per la loro vigilanza: previsione sorprendente che ancora una volta mostra il favor del Legislatore verso più collaudati meccanismi già sperimentati nel settore *data protection* e applicati all'Intelligenza Artificiale.

Passando all'esame delle norme del Regolamento IA sui codici di condotta, va evidenziato che – ancora una volta – viene replicato un meccanismo che sta da poco prendendo piede operativamente anche nel settore della protezione dei dati personali. L'articolo 69 del reg. IA prevede infatti che la Commissione e gli Stati membri incoraggiano e agevolano (anche tenendo conto degli interessi e delle esigenze specifici dei fornitori di piccole dimensioni e delle *start-up*) l'elaborazione di codici di condotta intesi a promuovere l'applicazione volontaria ai sistemi di IA diversi dai *sistemi di IA ad alto rischio* dei requisiti relativi, ad esempio, alla sostenibilità ambientale, all'accessibilità per le

persone con disabilità, alla partecipazione dei portatori di interessi alla progettazione e allo sviluppo dei sistemi di IA, etc.

I codici di condotta:
a) possono essere elaborati da singoli fornitori di sistemi di IA o da organizzazioni che li rappresentano o da entrambi, anche con la partecipazione degli utenti e di tutti gli altri portatori di interessi e delle loro organizzazioni rappresentative;
b) possono riguardare uno o più sistemi di IA, tenendo conto della similarità della finalità prevista dei sistemi pertinenti.

§ 4. Il sistema sanzionatorio per la violazione del Regolamento sull'Intelligenza Artificiale.

Il sistema sanzionatorio introdotto dal Regolamento IA si snoda attraverso un doppio binario: *nazionale* ed *europeo*.

Quanto alla prima prospettiva, il Reg. IA (art. 71) rinvia alla legislazione degli Stati Membri per la determinazione delle procedure applicative per la corretta ed efficace applicazione di sanzioni amministrative pecuniarie per – in generale – "*la violazione del presente regolamento*", Le sanzioni amministrative pecuniarie nazionali devono essere effettive, proporzionate e dissuasive e devono tener conto degli interessi dei fornitori di piccole dimensioni e delle *start-up* e della loro sostenibilità economica.

Quanto alla prospettiva sanzionatoria *europea*, il Regolamento IA fissa direttamente l'importo delle sanzioni *massime*, in ciò replicando il modello sanzionatorio già istituito dal Regolamento UE sulla protezione dei dati personali, che prevede massimi sanzionatori edittali per la violazione di specifiche norme. Le sanzioni applicabili ai sensi del Regolamento IA colpiscono soprattutto la violazione delle prescrizioni sui *sistemi IA ad alto rischio*. Tuttavia, la sanzione amministrativa più elevata (anche dei massimi previsti dall'omologo Regolamento sulla protezione dei dati) è quella fino a 30 milioni di Euro o fino al 6% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, in caso di violazione dell'articolo 5 Reg. IA sul divieto di pratiche di intelligenza artificiale (che possono essere messe in atto anche nell'ambito della operatività di normali sistemi IA, non necessariamente ad alto rischio).

Saranno dunque soggette alla sanzione indicata fino a 30 milioni di Euro o fino al 6% del fatturato mondiale le seguenti pratiche di Intelligenza Artificiale, ove applicate in violazione del divieto:

- l'immissione sul mercato, la messa in servizio o l'uso di sistemi di IA che utilizzano tecniche subliminali che vanno al di là della consapevolezza di una persona al fine di distorcere materialmente il comportamento di una persona in un modo che causa o è probabile che possa causare a quella persona o a un'altra persona danni fisici o psicologici;

- l'immissione sul mercato, la messa in servizio o l'uso di sistemi di IA che sfruttano una qualsiasi delle vulnerabilità di un gruppo specifico di persone a causa della loro età, disabilità fisica o mentale, al fine di distorcere materialmente il comportamento di una persona appartenente a quel gruppo in un modo che causa o è probabile che possa causare a quella persona o a un'altra persona danni fisici o psicologici;
- l'immissione sul mercato, la messa in servizio o l'uso di sistemi di IA che consentono il cosiddetto *social credit scoring*, e cioè:

(a) l'immissione sul mercato, la messa in servizio o l'uso di sistemi di IA da parte di pubbliche autorità o per loro conto allo scopo di procedere alla valutazione o alla classificazione dell'affidabilità delle persone fisiche in un determinato contesto temporale in base al loro comportamento sociale o a caratteristiche personali o di personalità note o previste, con un punteggio sociale che porti a uno o ad entrambe delle seguenti conseguenze:

(i) trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di interi gruppi di persone fisiche in contesti sociali che non sono correlati ai contesti nei quali i dati sono stati originariamente generati o raccolti;

(ii) trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di interi gruppi di persone fisiche che risulti ingiustificato e sproporzionato rispetto al loro comportamento sociale o alla sua gravità.

- l'immissione sul mercato, la messa in servizio o l'uso di sistemi di identificazione biometrica a distanza in tempo reale in spazi accessibili al pubblico ai fini dell'attività di contrasto, a meno che non vi siano specifiche esigenze di ricerca mirata di specifiche potenziali vittime di reati, compresi bambini scomparsi; di prevenzione di una minaccia specifica, sostanziale e imminente per la vita o sicurezza fisica delle persone fisiche o di un attacco terroristico; etc.

La stessa sanzione fino a 30 milioni di Euro o fino al 6% del fatturato mondiale sarà applicata nel caso di violazione degli specifici requisiti di qualità che l'articolo 10 Reg. IA fissa per i *sistemi IA ad alto rischio* che utilizzano tecniche e set di dati di addestramento, convalida e prova. Questi requisiti di qualità, è bene ricordarlo, riguardano:

1. appropriate pratiche di governance e gestione dei dati di addestramento;
2. pertinenza, rappresentatività, correttezza e completezza dei dati di addestramento;
3. considerazione appropriata delle caratteristiche o degli elementi particolari dello specifico contesto geografico, comportamentale o funzionale all'interno del quale il sistema di IA ad alto rischio è destinato a essere usato;
4. adeguate pratiche di gestione e governance dei dati per lo sviluppo di sistemi di IA ad alto rischio diversi da quelli che utilizzano tecniche e dati di addestramento al fine di garantire che tali sistemi di IA ad alto rischio siano comunque conformi ai requisiti di qualità sopra elencati.

In una scala di gravità, la violazione degli articoli 5 e 10 Reg. IA è considerata dal Legislatore UE come quella più grave. Immediatamente al di sotto, è considerata la "*non*

conformità dei sistemi di IA ai requisiti o agli obblighi previsti dal regolamento, diversi da quelli di cui agli articoli 5 e 10". Per tali ipotesi, generali e residuali e che riguardano ad ampio raggio tutta una serie di caratteristiche che i sistemi IA (anche quelli non ad alto rischio) devono possedere, di procedure e di tecniche è prevista l'applicazione di una sanzione amministrativa pecuniaria fino a 20 milioni di Euro o, se *l'autore del reato* (così viene definito il trasgressore, anche se, rispetto alla natura amministrativa della sanzione pecuniaria, sorgono dubbi sulla correttezza giuridica sia della dizione in lingua italiana che del termine utilizzato nel testo inglese di "*offender*") è una società, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

Per offrire alcuni esempi dei casi in cui potrà trovare applicazione tale sanzione, possono citarsi i seguenti (riferiti comunque ai sistemi IA alto rischio):
- la mancata adozione di un sistema di gestione dei rischi connessi ai sistemi IA;
- la mancata predisposizione della documentazione tecnica dei ai sistemi IA;
- il mancato tracciamento e la mancata registrazione dei log di un sistema IA;
- la mancata sorveglianza umana;
- la mancata adozione di un adeguato livello di accuratezza, robustezza e cybersicurezza dei sistemi IA per tutto il loro ciclo di vita;
- la mancata adozione di un sistema di gestione di qualità;
- la violazione degli obblighi informativi e di trasparenza.

Deve essere ricordato che anche gli utenti di sistemi IA ad alto rischio possono incorrere nella applicazione della sanzione fino a 20 milioni di Euro o fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, nel caso – ad esempio – di violazione degli obblighi specifici che l'art. 29 Reg. IA pone a loro carico: si pensi al caso di una azienda che acquista un sistema IA ad alto rischio di valutazione dei dipendenti ed è responsabile dei dati di input: potrebbe derivarne una "*non conformità*" (dizione tra l'altro assai ambigua e generica quella impiegata nell'articolo 71, comma 4 Reg. IA) del sistema IA sanzionabile con gli importi di cui sopra.

Altra ipotesi sanzionatoria riguarda la fornitura di informazioni inesatte, incomplete o fuorvianti agli organismi notificati e alle autorità nazionali competenti: fino a 10 milioni di Euro o, in caso di società, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

La determinazione in concreto, per ogni singolo caso, dell'importo sanzionatorio specifico (sempre difficile quando i meccanismi prevedono solo massimi edittali, anche per le disomogeneità che si possono determinare da caso a caso e da Stato a Stato) deve tenere nel debito conto alcuni requisiti già noti perché richiamati anche dall'impianto sanzionatorio del RGPD:

a) la natura, la gravità e la durata della violazione e delle sue conseguenze;
b) se altre autorità di vigilanza del mercato hanno già applicato sanzioni amministrative pecuniarie allo stesso operatore per la stessa violazione;

c) le dimensioni e la quota di mercato dell'operatore che ha commesso la violazione.

Chi applica le sanzioni amministrative pecuniarie?

L'articolo 71 Reg. IA non lo specifica (anche se l'indiretto riferimento alle "*altre autorità di vigilanza del mercato che hanno già applicato sanzioni amministrative pecuniarie allo stesso operatore per la stessa violazione*" sembrerebbe incardinare in capo a tali autorità la competenza sanzionatoria). Al comma 8, tuttavia, vi è la specifica indicazione che a seconda dell'ordinamento giuridico degli Stati membri le sanzioni pecuniarie possono essere inflitte dai tribunali nazionali competenti o da altri organismi competenti in tali Stati membri.

Staremo dunque a vedere, visto che in apertura si parlava delle competenze nazionali in materia sanzionatoria, cosa decideranno gli Stati membri, che tra l'altro potranno prevedere anche sanzioni penali vere e proprie, come già accade – in sede nazionale – con l'impianto sanzionatorio penale nel settore *data protection*, deciso a livello di Stati membri (cfr. artt. 167 e ss. Del Codice della privacy italiano).

Certo è che in una prospettiva comparativa con l'impianto sanzionatorio del RGPD, quello strutturato nel Regolamento IA appare molto meno preciso, non legando ad esempio le sanzioni alla violazione di specifiche norme, come previsto ad esempio nell'art 83 del RGPD, ma prevedendo una sorta di macro-sanzione per tutto ciò che non è violazione degli articoli 5 e 10, oppure non prevedendo una competenza specifica a comminare le sanzioni, o – infine – rinviando agli ordinamenti degli Stati membri.

Vi è infine, nell'impianto sanzionatorio del Regolamento UE sull'Intelligenza Artificiale, una sorta di catalogo di sanzioni pecuniarie di tipo – diciamo – *pubblicistico* che il Garante europeo per la protezione dei dati personali può comminare alle istituzioni, alle agenzie e agli organismi dell'Unione Europea che rientrano nell'ambito di applicazione del Regolamento (cfr. art. 72 Reg. IA):

a) sanzioni fino a 500 mila euro per violazione dell'articolo 5 Reg. IA sul divieto di pratiche di intelligenza artificiale o per violazione dell'articolo 10 sui requisiti sopra visti in merito a sistemi IA che usano dati di addestramento;

b) sanzioni fino a 250 mila euro per non conformità dei sistemi IA ai requisiti o agli obblighi previsti dal Regolamento, diversi da quelli di cui agli articoli 5 e 10.