LUISS

Dipartimento di **Giurisprudenza**

Cattedra **Diritto Commerciale Progredito**

Intelligenza artificiale e vigilanza bancaria

Chiar.mo Prof. Gian Domenico Mosco
RELATORE

Chiar.mo Prof. Giorgio Meo
CORRELATORE

Vittorio Del Vecchio

Matricola 161933

CANDIDATO

Anno accademico 2023/2024

INDICE

CAPITOLO I - *SUPTECH*: L'INTELLIGENZA ARTIFICIALE AL SERVIZIO DELLA SUPERVISIONE BANCARIA

1. L'intelligenza artificiale applicata alla vigilanza bancaria: presupposti, contenuti e ragioni dell'indagine

L'avvento dell'intelligenza artificiale rappresenta, sicuramente, il principale prodotto dell'innovazione tecnologica contemporanea; le sue sconfinate possibilità applicative permeeranno ogni settore della società rivoluzionando il modo di operare e di ricercare le soluzioni ai problemi. In uno scenario mondiale, sempre più connesso e digitalizzato, l'esigenza di studiare il fenomeno, comprenderne rischi e benefici, nonché, regolamentarlo è fortemente sentita delle istituzioni mondiali ed europee. Per questo motivo, in un primo momento, i governi e le organizzazioni internazionali hanno orientato la loro attenzione al fenomeno inteso come "oggetto da regolamentare", in quanto, l'utilizzo dell'intelligenza artificiale ha destato numerose preoccupazioni, in particolare, in relazione alle implicazioni etiche. Da tempi recenti a questa parte, però, gli esperti e le istituzioni hanno preso atto dei vantaggi, in termini di miglioramento della qualità della vita e della *governance*, nel concepire il fenomeno anche come strumento di politica normativa, cioè, impiegato "per regolamentare"[1] e per migliorare l'espletamento dei pubblici servizi[2]. Tra le sconfinate potenzialità dell'intelligenza artificiale figurano, certamente, la capacità di dettare delle regole in grado di agire *ex ante* onde prevenire comportamenti illeciti e migliorare significativamente i processi amministrativi, affinché siano sempre più efficienti, efficaci ed economici. Tuttavia, prima dell'utilizzo di tali tecnologie, le istituzioni non potranno prescindere dall'adozione di una metodologia che

[1] LETTIERI N., DONÀ S., *Critical data studies e tecno-regolazione. Paradigmi emergenti di ricerca e tutela nell'era del lavoro data-driven*, su Dirittifondamentali.it - Fascicolo 2/2020, 2020. Si parla di tecno-regolazione. [Online]. Disponibile se: https://dirittifondamentali.it/wp-content/uploads/2020/06/Lettieri-Don%C3%A0-Critical-data-studies-e-tecno-regolazione.-

[2] MISURACA G., VAN NOORDT C., *AI Watch - Artificial Intelligence in public services: Overview of the use and impact of AI in public services in the EU*, EUR 30255 EN, (Ufficio delle pubblicazioni dell'Unione europea, 2020). [Online]. Disponibile su: AI watch, artificial intelligence in public services - Publications Office of the EU (europa.eu)

analizzi, oltre ai fattori trainanti e gli aspetti positivi, i rischi e le barriere all'uso dell'IA nei servizi pubblici[3].

Il presente elaborato è orientato ad approfondire le implicazioni derivanti dall'utilizzo dei sistemi di intelligenza artificiale nell'attività di vigilanza bancaria della BCE. Il fenomeno è noto, più in generale, come *SupTech* (*Supervisory Technology*), cioè, «*l'uso da parte delle autorità finanziarie di strumenti avanzati di raccolta e analisi di dati, consentiti da tecnologie innovative*».[4] Secondo alcuni, sarebbe preferibile parlare di "*SupTech generations*"[5] per descrivere le varie applicazioni, attuali e future, a seconda del grado di coinvolgimento nell'attività. L'impiego dell'IA, infatti, potrebbe esser finalizzato, da un lato, allo svolgimento di attività di raccolta, traduzione e analisi di tipo descrittivo dei dati, nonché, al monitoraggio degli istituiti vigilati e dall'altro, a prender parte all'attività decisionale o assumere, in casi estremi, il ruolo di decisore autonomo. La distinzione tra le varie modalità d'impiego assume rilevanza fondamentale per valutare la compatibilità di tali strumenti con il quadro giuridico ed istituzionale.
Da un punto di vista tecnico, invece, tra gli strumenti suscettibili di esser impiegati dalle autorità, occorre distinguere, in linea generale, quelli basati su algoritmi condizionali da quelli basati sul *Machine Learning* e *Deep Learning*. I sistemi, basati sui primi, producono un dato *output* al realizzarsi o meno della condizione su cui è basato il programma. Questo modo di operare renderebbe l'algoritmo compatibile e utilizzabile in tutti quei casi, molto rari, in cui l'attività di vigilanza si traduce nell'esercizio di un potere totalmente vincolato in capo alla BCE. I sistemi che si avvalgono di tecniche di ML svolgono operazioni, senza istruzioni esplicite, attraverso l'utilizzo di una logica induttiva, quindi, legata ad un modello esperienziale. Per questo motivo la BCE, data la natura discrezionale della sua attività ed avendo a che fare con grandi moli di dati, ha scelto di avvalersi dei secondi e quindi, anche l'elaborato sarà focalizzato sulle sole implicazioni derivanti dall'utilizzo delle tecniche di ML con i diritti fondamentali e con l'assetto istituzionale della stessa BCE. Nonostante l'indiscutibile rilevanza del tema nel

[3] Ivi par. 1.2.
[4] COELHO R., DE SIMONI M., PRENIO J., *N. 14 - Applicazioni suptech per l'antiriciclaggio*, in Quaderni dell'antiriciclaggio, 2019. [Online]. Disponibile su: https://uif.bancaditalia.it/pubblicazioni/quaderni/2019/quaderno-14-2019/index.html
[5] DI CASTRI S. *et al*., "*The suptech generations*", FSI Insights on policy implementation No 19, Bank for International Settlements, 2019. [Online]. Disponibile su: The suptech generations (bis.org)

contesto attuale, stupisce l'assenza di studi accademici[6] volti ad indagare, approfonditamente, questo argomento. Di fronte a questa evidente lacuna, che la presente ricerca mira a colmare, si offrirà una panoramica, da un lato, dello stato attuale delle applicazioni da parte della BCE, illustrandone i vantaggi e le problematiche (comuni a tutte le applicazioni di IA in qualunque campo) e dall'altro, delle prospettive future e delle specifiche problematiche che potrebbero derivare, alla luce del quadro legale ed istituzionale, dall'automazione della vigilanza bancaria.

L'indagine, quindi, è orientata alla trattazione delle problematiche legali, riguardanti qualunque sistema di IA, con il GDPR ed il Regolamento europeo sull'intelligenza artificiale. In particolare, in relazione al GDPR, ci si chiede fino a che punto la restrizione dei diritti dell'interessato può essere consentita per utilizzare l'IA a fini di vigilanza bancaria, considerato che l'incremento della qualità dell'*output* di qualunque sistema di ML passa per la raccolta e il consequenziale *training* su un gran numero di dati (anche personali).

Con riferimento all'entrata in vigore dell'*AI Act*, invece gli interrogativi attengono: al ruolo che quest'ultimo ricopre nello sviluppo di un'IA affidabile; a quale tipo di "rischio" presentano i sistemi di apprendimento automatico impiegati nella vigilanza bancaria; alla possibilità di superare i problemi di trasparenza e di scongiurare i rischi per i diritti fondamentali. A questo proposito, data la novità del Regolamento e la presenza di numerosi interrogativi, si è deciso di dedicarvi l'intero Capitolo II.

In seguito, l'elaborato, fatta la distinzione tra l'*AI-Enhanced* e l'*AI-Driven* nel contesto dell'attività di vigilanza, si sofferma sulle implicazioni che potrebbero derivare in futuro in caso di coinvolgimento della seconda. I principali motivi di attrito derivanti dall'automazione sono legati all'obbligo, in capo alle BCE, di garantire il diritto ad avere una buona amministrazione. Ai sensi dell'art. 41 della Carta dei diritti fondamentali dell'Unione europea e più nello specifico ai sensi degli artt. 19 e 22 del Regolamento SSM, la BCE è tenuta ad operare, in modo indipendente, secondo imparzialità, equità ed in tempi ragionevoli ed allo stesso tempo a garantire, prima di prendere una decisione motivata, il diritto ad ascoltare le ragioni del destinatario del procedimento, nonché, il diritto ad accedere al fascicolo che lo riguarda.

[6] Ad eccezione di RINGE W.G. *et al*., *Navigating the Legal Landscape of AI-Enhanced Banking Supervision: Protecting EU Fundamental Rights and Ensuring Good Administration,* European Banking Institute Working Paper Series 2023 - no. 140, 2023. [Online]. Disponibile su: https://ssrn.com/abstract=4430642

Premesso quanto innanzi, data l'assenza di trasparenza sul funzionamento interno dei sistemi di ML, come può un algoritmo motivare una decisione se non è in grado di dimostrare come sia arrivato ad un determinato *output*?

Inoltre, essendo tali sistemi, basati su un metodo correlazionale e non causale, come possono fornire la prova del nesso causale tra le circostanze di fatto e la decisione?

Ed in ultimo, con riferimento al diritto ad esser ascoltati, che peso ha, ammesso che lo abbia, la versione offerta dal destinatario di un procedimento automatizzato, nella decisione di un algoritmo allenato su una miriade di altri dati?

Questi sono i principali problemi che i sistemi di apprendimento automatico incontreranno ogni qualvolta verranno impiegati, non solo nei procedimenti condotti dalla BCE, in qualunque attività amministrativa rivolta a presone fisiche o giuridiche.

Successivamente, l'elaborato si sofferma sulla responsabilità dei funzionari in caso di danni commessi dall'intelligenza artificiale quando questa riveste il ruolo di decisore. Sarà possibile ritenere responsabili i funzionari, nei casi in cui non abbiano competenze informatiche, per non aver vigilato correttamente sui risultati di un algoritmo di cui non hanno conoscenza e le cui logiche di funzionamento sono, spesso, oscure?

Esaurite le questioni sulle possibili implicazioni con il quadro giuridico, è necessario analizzare il fenomeno *SupTech* anche da un'altra prospettiva: quella istituzionale.

La BCE svolge, in via indipendente, funzioni di politica monetaria e di vigilanza ma, allo stesso tempo, è tenuta a render conto del proprio operato alle altre istituzioni e più in generale all'opinione pubblica (*accountabilty*). Premesso ciò, si intende stimolare una riflessione sull'opportunità circa l'introduzione dell'intelligenza artificiale nelle decisioni di vigilanza. Il rischio è che l'*accountability* della BCE, in caso di concorso dell'IA nelle decisioni di vigilanza, non possa più essere garantita innescando istanze di revisione del regime di indipendenza.

Per concludere, si proverà a fornire una chiave di lettura per risolvere le questioni sollevate e superare gli ostacoli che si frappongono tra l'IA e il suo impiego nella vigilanza bancaria, sia sul piano giuridico che istituzionale, esaminando e confrontando le soluzioni suggerite dagli autori del panorama accademico per situazioni simili ma soprattutto, attraverso delle personali riflessioni.

2. Intelligenza artificiale. Un'analisi generale del fenomeno

L'IA è stata definita in molti modi a causa dell'estrema mutevolezza e capacità di evolversi del fenomeno.[7] La tendenza registrata nel corso del tempo è stata quella di cercare di delimitare i contorni di tale tecnologia sulla base dell'assunto, non fondato, che ciò fosse necessario per affrontare un dibattito sui risvolti e sulle implicazioni sociali, economiche e giuridiche derivanti dall'impiego dell'IA. Quest'ultima, non è un termine scientifico che necessita di esser definito ma, un'espressione generica utilizzata per indicare una serie di prodotti e servizi tra loro diversi[8]. D'altro canto, è sempre stato chiaro l'obiettivo che i ricercatori si sono posti: migliorare i processi cognitivi nelle macchine per riprodurre in tutto o in parte il prodotto del pensiero umano allo scopo di renderle "intelligenti"[9]. Il termine "intelligenza artificiale" è stato coniato da *John McCarty* nel 1956, in quanto, utilizzato in un documento denominato "*Proposta di Dartmouth*" e presentato ad una conferenza al *College* da cui prende il nome. Tuttavia, l'articolo che ha inaugurato la lunga stagione di ricerca sul tema è *Computing Machinery and Intelligence*, scritto da *Alan Turing* e pubblicato sulla rivista *Mind* nel 1950. All'interno dell'articolo l'autore elabora un gioco di imitazione conosciuto come *Test* di *Turing c*he permette di distinguere quando un sistema artificiale possa esser considerato "intelligente". Secondo tale *test* se il comportamento del sistema sarà indistinguibile da quello dell'essere umano secondo una probabilità dell'almeno 30% allora sarà "intelligente". In questo periodo, compaiono i primi studi sull'intelligenza artificiale basati su due modelli di comprensione diversi. Il primo è basato su un ragionamento logico deduttivo. Gli ingegneri, nei primi anni, dotavano l'IA di un sistema predefinito di regole o assiomi per permettere alla macchina di ragionare sui dati ricevuti e giungere a una conclusione. Il secondo modello di comprensione è un modello di tipo induttivo, basato sull'analogia, che grazie all'apprendimento di una serie di informazioni da grandi *dat-set*, giunge a una conclusione basata sull'esperienza. Partendo, quindi, da casi particolari trae una regola

---

[7] LEGG S., HUTTER M, *Universal Intelligence: A Definition of Machine Intelligence*, *Minds and Machines*, 2024, pp 391-444, che indicava nel 2007 già 53 definizioni esistenti di IA. [Online]. Disponibile su: https://philpapers.org/rec/LEGUIA

[8] FLORIDI L., *Etica dell'intelligenza artificiale. Sviluppi, opportunità e sfide*, s.l., Raffaello Cortina Editore, 2022, par. 2.1. [Online]. Disponibile su: https://books.google.it/books?id=kABlEAAAQBAJ&printsec=copyright&hl=it#v=onepage&q&f=false

[9] TESTOLIN A., ZORZI M., *L'approccio moderno all'intelligenza artificiale e la rivoluzione del deep learning*, in "Giornale italiano di psicologia, Rivista trimestrale" 2/2021, pp. 313-334, 2021, p. 315. [Online]. Disponibile su: http://ccnl.psy.unipd.it/publications/l2019approccio-moderno-all2019intelligenza-artificiale-e-la-rivoluzione-del-deep-learning/view

generale da applicare a casi identici o simili. Tuttavia, tra gli anni ’60 e ’70, mentre il modello logico-deduttivo conobbe un rapido sviluppo, il modello induttivo subì una battuta d’arresto per la limitata potenza di calcolo e per l’indisponibilità di grandi moli di dati necessari a far funzionare il suo *software*. Dalla fine degli anni ’80 si assiste ad un’inversione di rotta data, soprattutto, dall’aumento della capacità di calcolo che ha agevolato l’implementazione di modelli induttivi ed una applicazione diffusa di sistemi che nei decenni precedenti erano stati interessati solo da un punto di vista teorico come, ad esempio, le reti neurali. La crescita esponenziale della capacità di calcolo e di conservazione dei dati ha reso possibile l’adozione del metodo induttivo segnando il passaggio dell’IA da branca della logica a quella della statistica[10]. Con il ventunesimo secolo si giugne al culmine di questa evoluzione, ove l’addestramento di modelli sempre più complessi e accurati, reso possibile grazie ai “*big data”* e all’avvento del *deep learning*, ha favorito il progresso in vari settori della vita quotidiana e allo stesso tempo, ha posto la società dinanzi a nuove sfide di carattere etico. Tali sfide sono state accettate da molte organizzazioni internazionali che hanno lanciato un’ampia gamma di iniziative al fine di determinare dei principi etici che governassero l’agire dell’IA[11]. Questa tendenza, se da un lato, ha avuto il merito di porre immediatamente un freno, almeno da un punto di vista teorico, a possibili abusi nell’utilizzo di tali sistemi, dall’altro, ha generato una notevole confusione per via della grande mole di principi enucleati che sono risultati, in certi casi, ridondanti e in altri, contraddittori[12]. In linea generale, dall’analisi dei lavori più significativi[13], si registra un elevato grado di convergenza e delle differenze quasi sempre determinate dalla lingua in cui sono redatti.

[10] FLORIDI L., *Etica dell’intelligenza artificiale. Sviluppi, opportunità e sfide*, s.l., Raffaello Cortina Editore, 2022, par. 1.1. [Online]. Disponibile su: https://books.google.it/books?id=kABlEAAAQBAJ&printsec=copyright&hl=it#v=onepage&q&f=false

[11] Secondo *l’AI Ethics Guidelines Global Inventory* di *AlgorithmWatch* nel 2019 sono più di 160. [Online]. Disponibile su: https://algorithmwatch.org/en/ai-ethics-guidelines-global-inventory/

[12] FLORIDI L., “*Etica dell’intelligenza artificiale. Sviluppi, opportunità e sfide*”, s.l., Raffaello Cortina Editore, 2022, par. 4.1. [Online]. Disponibile su: https://books.google.it/books?id=kABlEAAAQBAJ&printsec=copyright&hl=it#v=onepage&q&f=false

[13] *Ex multis*: Future of Life Institute*, I Principi di Asilomar per l’IA*, gennaio 2017; Università di Montréal, *La dichiarazione di Montréal per l’IA responsabile*, novembre 2017; Parlamento europeo, *Risoluzione del Parlamento europeo recante raccomandazioni alla Commissione concernenti il quadro relativo agli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate*, 2020.

Secondo alcuni[14], il problema della proliferazione incontrollata dei principi è risolvibile partendo dall'assunto che l'IA non sia una nuova forma di intelligenza, bensì, una nuova modalità di agire. Per questo motivo, è possibile superare il problema attraverso l'applicazione dei principi della bioetica in quanto più vicini all'etica digitale e rappresentanti una perfetta sintesi di quelli indicati da *AlghoritmWatch*[15]. Ai principi della bioetica, applicabili all'IA quali la *beneficenza*, la *non maleficenza*, l'*autonomia* e la *giustizia* se ne deve aggiungere un quinto tipico esclusivamente dell'IA: l'*esplicabilità*. La *beneficenza* implica che l'IA debba essere sviluppata al fine di perseguire il bene comune e promuovere il benessere dell'essere umano. La *non maleficenza* si esplica nell'evitare un utilizzo improprio e prevenire comportamenti dannosi. L'*autonomia* di tali sistemi deve essere limitata, reversibile e non deve compromettere le libertà degli esseri umani. La *giustizia* impone di eliminare le iniquità e ogni discriminazione. La garanzia dell'*esplicabilità* sorge dalla necessità di superare il "*black box problem*", cioè, la mancanza di trasparenza nel processo che porta l'algoritmo ad una determinata conclusione. L'IA, soprattutto, se impiegata nell'ambito dell'attività di vigilanza bancaria, deve operare in modo trasparente per permettere ai destinatari di eventuali provvedimenti di esercitare il diritto alla difesa ed eventualmente, contestare l'eventuale decisione attraverso l'analisi del procedimento che ha portato ad un determinato *output*.

2.1. Le tecniche utilizzate dall'intelligenza artificiale

Numerosi sono stati i dibattiti, intercorsi nel tempo, all'interno della comunità scientifica e filosofica attorno al concetto di "macchine intelligenti". In particolare: sulla loro definizione, su sé fosse stato eticamente corretto crearle e sulle loro caratteristiche tecniche. Sin dalla metà del secolo scorso, l'attenzione degli studiosi si è focalizzata sullo studio di modelli di intelligenza artificiale[16]. Date le difficoltà[17] di sviluppare dei modelli sul piano pratico, gli studi si sono concentrati sul concetto di intelligenza artificiale da cui nacquero due teorie che costituiscono una prima, per certi versi, classificazione di tali

[14] FLORIDI L., "*Etica dell'intelligenza artificiale. Sviluppi, opportunità e sfide*", s.l., Raffaello Cortina Editore, 2022, par. 4.2. [Online]. Disponibile su: https://books.google.it/books?id=kABlEAAAQBAJ&printsec=copyright&hl=it#v=onepage&q&f=false
[15] Si veda n. 14.
[16] CHOLLET F., *Deep learning with Python*, II Ed., Manning, Shelther Island, New York, 2021, p.2. [Online]. Disponibile su: https://sourestdeeds.github.io/pdf/Deep%20Learning%20with%20Python.pdf
[17] Sono indicate nel par. 1.

sistemi. Quest'ultime individuano due tipologie di intelligenza artificiale: forte e debole. L'intelligenza artificiale forte mira a replicare le capacità cognitive generali dell'essere umano e a sviluppare una coscienza autonoma tali da permetterle di eseguire qualsiasi compito o risolvere qualsiasi problema con l'obiettivo finale di risultare indistinguibile da un essere umano, ovvero, consapevole dei propri stati mentali ed esser dotata di libero arbitrio[18]. La debole è finalizzata, non già ad avere capacità cognitive generali e una coscienza autonoma, ma a svolgere una o più funzioni umane complesse. Con il progresso tecnologico, alla teoria, sono seguite le prime applicazioni pratiche attraverso l'ideazione di tecniche di computazione e soluzioni collocate alla base dell'IA: gli algoritmi[19]. Dalle prime tipologie di algoritmi (condizionali) basati su «espressioni condizionali» [20] che «*allow a program to execute a diffent code depending on what happens as the programs runs*»[21] agli algoritmi più avanzati che utilizzano sistemi di apprendimento quali il *machine learning* e il *deep learning*[22].

Gli algoritmi condizionali o deterministici hanno la capacità di assumere decisioni sulla base di regole predeterminate in fase di programmazione il cui codice risulta accessibile, consultabile e comprensibile da un essere umano con le specifiche competenze tecniche. Un esempio di algoritmo di tipo condizionale è l'istruzione "*if-else*" presente in molti linguaggi di programmazione. L'algoritmo eseguirà un blocco di codice se la condizione sia vera ed un altro nel caso in cui la condizione sia falsa. Il processo logico alla base di questi algoritmi è simile al ragionamento giuridico[23], in quanto, in presenza di una

---

[18] FERILLI S. *et al*., *L'intelligenza artificiale per lo sviluppo sostenibile*, Consiglio Nazionale delle Ricerche, 2021. [Online]. Disponibile: https://www.cnr.it/sites/default/files/public/media/attivita/editoria/VOLUME%20FULL%2014%20digital%20LIGHT.pdf

[19] *Intelligenza Artificiale, significato e applicazioni dell'AI*: https://blog.osservatori.net/it_it/intelligenza-artificiale-funzionamento-applicazioni

[20] CARULLO G., *Decisione amministrativa e intelligenza artificiale*, in: Diritto dell'informazione e dell'informatica, fasc. 3, 2021, p. 433. [Online]. Disponibile su: https://air.unimi.it/handle/2434/891372

[21] *Ex multis* JOHNSON M. J., *A Concise Introduction to Programming in Python*, CRC Press, 2018, p. 23. [Online]. Disponibile su: https://dokumen.pub/a-concise-introduction-to-programming-in-python-second-edition-2nbsped-9781138082588-1138082589.html

[22] Più precisamente il *deep learning* è un sottoinsieme del *machine learning*. Il *deep learning* combina la statistica e la matematica con l'architettura di una rete neurale per replicare il ragionamento di una mente umana. I sistemi di *machine learning* si servono solo della matematica e della statistica per risolvere certi problemi come spiegato su: https://aws.amazon.com/it/compare/the-difference-between-machine-learning-and-deep-learning/#:~:text=Il%20deep%20learning%20%C3%A8%20ideale,senso%20ai%20dati%20non%20strutturati.&text=Il%20machine%20learning%20risolve%20problemi,un'architettura%20di%20rete%20neurale.

[23] CARULLO G., *Decisione amministrativa e intelligenza artificiale*, in: Diritto dell'informazione e dell'informatica, fasc. 3, 2021, p. 434. [Online]. Disponibile su: https://air.unimi.it/handle/2434/891372

situazione di fatto (il realizzarsi delle condizioni richieste dal programma) sussumibile in una fattispecie astratta (regola predeterminata nel programma), si procede all'applicazione della norma con le annesse conseguenze (*output*). Questo modo di operare rende l'algoritmo compatibile e utilizzabile in tutti i casi in cui l'attività di vigilanza si traduce nell'esercizio di un potere vincolato in capo alla BCE, ossia, ogni volta in cui la norma, al sussistere di determinati requisiti, prescrive una data conseguenza. Secondo alcuni[24], un discorso analogo potrebbe esser fatto anche nei casi in cui, nell'esercizio di un potere vincolato, l'attività sia tecnico-discrezionale e i parametri tecnici, entro i quali la valutazione si debba svolgere, possano essere tradotti in regole informatiche condizionali. Nell'ambito dell'attività di supervisione bancaria, svolta dalla BCE o dall' autorità nazionale competente, i casi in cui il potere è interamente vincolato sono rari, in quanto, i parametri normativi che circoscrivono il loro operato non sono stringenti e lasciano ampia discrezionalità nell'esercizio delle funzioni di vigilanza[25]. Ad esempio, il legislatore italiano nel TUB utilizza espressioni di contenuto astratto come la "sana e prudente gestione" affidando alla Banca d'Italia numerosi poteri di valutazione del caso di specie e permettendogli di valutare, di volta in volta, le finalità da perseguire. Anche i casi in cui la normativa sembra prevedere una determinazione vincolata al realizzarsi di determinate condizioni, come l'art. 14 del TUB, si rinviene un elemento che colora la decisione di una componente discrezionale.

La norma in questione conferisce, alla Banca d'Italia prima e alla BCE poi, il potere di verificare le condizioni indicate al comma uno cioè: la forma giuridica della società, il capitale sociale iniziale, il programma concernente l'attività iniziale, il rispetto dei requisiti degli azionisti e degli esponenti aziendali, insussistenza di particolari legami espressamente indicati[26]. Tra queste, la valutazione della serietà progetto economico è sicuramente discrezionale. Infatti, nonostante le modifiche apportate dalla direttiva 77/780/CEE,[27] l'autorità competente può decidere di rigettare le proposte che non presentino un progetto economico serio, cioè, che non permetterebbe all'intermediario di operare nel mercato in maniera efficiente[28]. È evidente che un algoritmo condizionale

[24] Ibidem.
[25] BRESCIAMORRA C., *Il diritto delle banche*, Il Mulino, Bologna, 2020, par. 8.6.4.
[26] Art. 14, c.1, let. f del TUB.
[27] Prima il potere di concessione dell'autorizzazione veniva valutato sulla base dell'esigenze di mercato, quindi, un potere fortemente discrezionale
[28] BRESCIAMORRA C., *Il diritto delle banche*, Il Mulino, Bologna, 2020, par. 9.1.

risulterebbe inadeguato a svolgere autonomamente l'intera attività, potendo, al più, esser impiegato nello svolgimento della parte che comporta una valutazione non discrezionale. Per concludere, tale tecnica risulta inadeguata quando il numero di condizioni da prendere in considerazione non è predeterminabile o estremamente elevato, come nel caso dell'esercizio del potere discrezionale[29].

L'altra tecnica alla base dell'intelligenza artificiale, sviluppatasi di pari passo con l'aumento delle capacità di elaborazione e conservazione dei dati, è il *machine learning* (di seguito ML). I sistemi di ML sono funzionali ad eseguire delle attività, senza delle istruzioni esplicite, attraverso l'addestramento su *set* di dati e apprendendo da essi i criteri per adottare nuove soluzioni. Tali sistemi sono costituiti da un codice sorgente e da un modello generato attraverso il *training* sui dati. Il primo è la «*versione di un algoritmo scritta in un linguaggio di programmazione ad alto livello (ossia più vicino al linguaggio umano, tipicamente in pseudo inglese), le cui istruzioni sono poi eseguite dalla macchina mediante appositi programmi*»[30]. Il modello, invece, è il risultato delle elaborazioni delle rappresentazioni, cioè, delle astrazioni matematico-numeriche utilizzate per produrre un dato *output*. Distinguiamo due tipologie di apprendimento: supervisionato e non supervisionato[31]. Nell'apprendimento supervisionato il modello si addestra con una serie di dati *input* e i corrispondenti dati di *output*[32]. Tra le varie tipologie dell'apprendimento supervisionato vi sono i modelli di regressione e classificazione che rispettivamente sono utilizzati se le variabili di *output* hanno valori continui e per prevedere tipologie o classi di un oggetto da un numero finito di opzioni[33].

Nell'apprendimento non supervisionato i *set* di dati sono forniti senza valore di *output* e quindi, l'algoritmo procede ad identificarli autonomamente[34]. Tra i modelli di questa

---

[29] CARULLO G., *Decisione amministrativa e intelligenza artificiale*, in: Diritto dell'informazione e dell'informatica, fasc. 3, 2021, p. 436. [Online]. Disponibile su: https://air.unimi.it/handle/2434/891372

[30] CAPELLI M., *Codice sorgente*, Enciclopedia della Scienza e della Tecnica, 2008. [Online]. Disponibile su: https://www.treccani.it/enciclopedia/codice-sorgente_(Enciclopedia-della-Scienza-e-della-Tecnica)/

[31] A cui secondo molti se ne aggiunge un terzo: apprendimento per rinforzo. L'elaborato però tratterà solo ed esclusivamente i tipi di apprendimento utilizzati da sistemi di ML impiegati nell'attività di supervisione bancaria. Cfr. LAVECCHIA V., *Differenza tra Apprendimento supervisionato, non supervisionato e con rinforzo*, Informatica e Ingegneria online. [Online]. Disponibile su: https://vitolavecchia.altervista.org/differenza-tra-apprendimento-supervisionato-non-supervisionato-e-con-rinforzo/

[32] Team I.A. Italia, *Cos'è un modello di Machine Learning o Apprendimento Automatico?* [Online]. Disponibile su: https://www.intelligenzaartificialeitalia.net/post/cos-%C3%A8-un-modello-di-machine-learning-o-apprendimento-automatico

[33] Ibidem.

[34] Ibidem.

seconda tipologia di apprendimento rinveniamo: il *clustering* che consente di individuare elementi simili tra loro; la regola di associazione per trovare relazioni tra variabili in un insieme di dati; la riduzione dimensionale che estrae le informazioni più importanti da una serie di dati; il *deep learning* di cui si è già discusso.

Per concludere, trattasi di sistemi di IA "aperti" e non deterministici che svolgono operazioni attraverso l'utilizzo di una logica induttiva, abduttiva oppure analogica. Appare evidente che tale tecnica meglio si concilia con la natura prevalentemente discrezionale del potere di vigilanza bancaria, in quanto, il ML attraverso il *training*, darà la possibilità, da un lato, di comprendere come l'autorità ha agito in casi analoghi o simili e dall'altro, di prendere in considerazione molte più variabili contemporaneamente. Per questo motivo, le autorità di vigilanza hanno scelto di avvalersi di questa tipologia di sistemi al fine di rendere più efficace la vigilanza e concentrare le risorse umane su attività più complesse e di maggiore importanza.

3. *SupTech*: l'intelligenza artificiale impiegata attualmente nell'attività di vigilanza della BCE

Negli ultimi anni, l'evoluzione tecnologica ha rivoluzionato il modo di operare delle autorità bancarie attraverso l'uso di tecnologie innovative nelle attività delle autorità di vigilanza[35]. Questo fenomeno prende il nome di *SupTech*[36]. Lo sviluppo a fini applicativi degli strumenti *SupTech* è influenzato, dal punto di vista della domanda, dall'esigenza di garantire una risposta celere ed efficace attraverso l'analisi in tempo reale di grandi moli di dati e dal punto di vista dell'offerta, dall'aumento dell'efficienza dei costi e della maggiore capacità di calcolo ed analisi dei dati derivanti dall'utilizzo di tali tecnologie[37]. Nello specifico, i principali *driver* della domanda sono: la necessità di maggiore sorveglianza, anche a seguito della crisi finanziaria globale del 2008, attraverso un monitoraggio in tempo reale; la maggiore attenzione alla prevenzione dei reati finanziari; l'aumento del numero dei soggetti sottoposti a vigilanza[38]. Sebbene l'impiego di questi

[35] DI CASTRI S. *et al*., "*The suptech generations*", FSI Insights on policy implementation No 19, Bank for International Settlements, 2019, sez. 1.
[36] Per un'ulteriore nozione di *SupTech* si veda il par. 1 in cui si cita quella data dalla Banca d'Italia.
[37] Financial Stability Board, "*The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions - Market developments and financial stability implications*", 2020, p. 2. [Online]. Disponibile su: The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions: Market developments and financial stability implications (fsb.org)
[38] Ibidem.

strumenti si stia diffondendo rapidamente, non è pacifico cosa rientri nella nozione di *SupTech* atteso che sia la definizione precedentemente data che quella della Banca d'Italia si riferiscono al concetto di "tecnologia innovativa" senza definirla, portando a differenti interpretazioni, più o meno ampie, di *SupTech*[39].

L'utilizzo della tecnologia, all'interno dell'attività di supervisione bancaria, è stato oggetto di un passaggio generazionale[40] da un'applicazione tecnologica ad un'altra che ha trovato il suo culmine in un'architettura di *big data* funzionale allo sviluppo di IA avanzate. Per questo motivo si suole parlare di *SupTech generations* piuttosto che di *SupTech* inteso come concetto unitario. La prima generazione ha previsto l'utilizzo della tecnologia per lo svolgimento di attività di raccolta di dati e analisi di tipo descrittivo rese, per limiti dell'infrastruttura, in *report* statici[41]. La seconda generazione ha avuto ad oggetto la digitalizzazione di processi amministrativi come portali *web* o *upload* di massa per le presentazioni di documenti con controlli di convalida automatizzati[42]. La terza generazione è stata incentrata sull'architettura dei *big data* che permette di analizzare, ad estrema velocità, enormi volumi di dati con formati destrutturati ed eterogenei. L'automazione della procedura, nonché, le evidenti potenzialità di tali architetture garantiscono l'archiviazione ed il calcolo di un *pool* di dati molto ampio e un'analisi statistica avanzata compresa quella predittiva[43]. L'ultima generazione, che non è stata ancora raggiunta, prevede l'impiego dell'IA nel procedimento di supervisione e nelle azioni delle autorità[44]. Come accennato nel paragrafo precedente, fra le tecniche di IA esistenti, il *machine learning* costituisce quella preferita dalle autorità di vigilanza per perseguire miglioramenti in termini di efficienza nell'ambito dell'attività di supervisione. In particolare, l'applicazione di tali tecnologie trova il suo campo di elezione nel monitoraggio dei rischi connaturati all'attività bancaria quali: il rischio di credito, di controparte, di mercato, operativo, di liquidità e non solo.

Il monitoraggio del rischio di credito, ossia, del rischio di perdita della banca in caso

[39] DI CASTRI S. *et al*., "*The suptech generations*", FSI Insights on policy implementation No 19, Bank for International Settlements, 2019, sez. 1.
[40] Ivi sez. 3.
[41] Ibidem.
[42] Ibidem.
[43] Ibidem.
[44] Ibidem.

d'inadempimento dei debitori consente all'autorità di vigilanza di accertare che gli istituti bancari abbiano delineato un adeguato sistema di controllo e gestione dello stesso.

Il rischio di controparte, sottocategoria del rischio di credito, consiste nel rischio «*che la controparte di una transazione avente a oggetto strumenti finanziari derivati, o altre specifiche operazioni, risulti inadempiente prima del regolamento della stessa*»[45].

I rischi di mercato sono rappresentati dalle possibili passività dovute a movimenti nel livello o nella volatilità dei prezzi di mercato[46].

I rischi operativi riguardano la possibilità che la banca affronti delle perdite a causa di risorse umane, politiche e processi inadeguati o a causa di fattori non prevedibili, come eventi esogeni[47].

Ed in ultimo, il rischio di liquidità rappresentato dai casi in cui una banca «*non è in grado di fare fronte ai propri impegni di pagamento per l'incapacità di reperire fondi sul mercato o smobilizzare i propri attivi*»[48].

In ordine a detto rischio, si è resa necessaria la previsione di regole che obbligano le banche a predisporre piani di emergenza in caso di momentanee carenze di liquidità.

La verifica delle problematiche legate al rischio di liquidità può essere agevolata dall'uso del *Machine Learning*. Ad esempio, le reti neurali artificiali possono essere utilizzate per stimare l'andamento generale del rischio ed individuare i fattori con maggiore grado di incidenza[49].

Le reti *bayesiane* sono, invece, in grado di stimare la probabilità per un dato evento di rischio[50]. Come detto, la principale distinzione tra i metodi di apprendimento di un sistema di ML sono l'apprendimento supervisionato, utilizzato per compiti di classificazione e previsione, e l'apprendimento non supervisionato per il *clustering*. In linea generale, le tecnologie impiegate dalla BCE rientrano all'interno della categoria dell'IA "predittiva", in quanto, volte a classificare un insieme di dati al fine di formulare

---

[45] BRESCIAMORRA C., *Il diritto delle banche*, Il Mulino, Bologna, 2020, par. 9.8.2.

[46] JORION P., *Value at Risk: The New Benchmark for Managing Financial Risk*, New York: McGraw-Hill, 2007, pt. 1. [Online]. Disponibile su: https://www.researchgate.net/publication/243767965_Value_at_Risk_The_New_Benchmark_for_Managing_Financial_Risk

[47] BRESCIAMORRA C., *Il diritto delle banche*, Il Mulino, Bologna, 2020, par. 9.8.2.

[48] Ivi, par. 9.8.3.

[49] LEO M. *et al.*, "Machine *Learning in Banking Risk Management: A Literature Review*" in Risks, 2019, par. 3.3. [Online]. Disponibile su: https://www.mdpi.com/2227-9091/7/1/29

[50] Ibidem.

delle previsioni o ad automatizzare determinate decisioni o fasi delle stesse[51]. Trattandosi di un modello la cui efficacia è subordinata all'attività preliminare di addestramento, risulta fondamentale, per raggiungere qualunque risultato, che si mettano a disposizione una grande quantità di dati veritieri e affidabili, sui quali le autorità di supervisione bancaria dovranno attuare pratiche e controlli per garantirne la qualità[52]. In base ai risultati dell'indagine[53], svolta dal *Financial Stability Board*, la qualità e la completezza dei dati, sia strutturati che non[54], costituiscono un obiettivo essenziale, affinché possa esser garantito il buon funzionamento dell'IA.

L'altra sfida, mira a scongiurare i rischi informatici derivanti dall'elevato utilizzo di tecnologie e soluzioni digitali. Il rischio di attacchi informatici è alto e per questo motivo, le autorità di vigilanza, che impiegheranno sistemi di ML, dovranno adottare misure di protezione e di sicurezza dei dati.

La realizzazione di tali obiettivi e più in generale, l'avvento della *SupTech*, ha comportato, da un lato, un incremento dell'efficienza, in termini di riduzione dei costi, dell'azione amministrativa ma, dall'altro, richiederà certamente l'assunzione di specialisti e la creazione e lo sviluppo di programmi di formazione per il personale già assunto. Tuttavia, il reclutamento di risorse può esser complicato dalla presenza di *competitor* nel settore privato, oltre che oneroso dal punto di vista economico.

Sebbene gli effetti dell'impiego di tali strumenti comportino un significativo miglioramento dell'operato dei supervisori per economicità e garanzia di risultati raggiunti, sarebbe un grave errore trascurare le possibili implicazioni legali con il tessuto normativo europeo. Risulta chiaro che l'utilizzo dell'IA per qualunque attività, dovrà confrontarsi con l'*AI Act* da cui discenderà un consequenziale obbligo in capo al fornitore e all'utente di rispettare i requisiti di sicurezza e trasparenza imposti a seconda del grado di rischio del sistema. Inoltre la BCE, ma più in generale tutte le autorità che ne faranno

---

[51] RINGE W.G. *et al*., *Navigating the Legal Landscape of AI-Enhanced Banking Supervision: Protecting EU Fundamental Rights and Ensuring Good Administration,* European Banking Institute Working Paper Series 2023 - no. 140, 2023, par. B.1.

[52] GUDIVADA V. *et al*., *Data Quality Considerations for Big Data and Machine Learning: Going Beyond Data Cleaning and Transformations*, International Journal on Advances in Software, vol 10 no 1 & 2, 2017, par. Introduction. [Online]. Disponibile su: Soft17v10n12_65040_1497480383_15201.pdf (upv.es)

[53] Financial Stability Board, *The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions - Market developments and financial stability implications*, 2020, par. 3.2.

[54] Può risultare difficile garantire la qualità dei dati quando provengo dai *social media*.

uso, dovrà garantire l'accesso ai dati personali utilizzati per il *training* algoritmico e rispettare i limiti all'uso dei dati personali imposti dal GDPR.

3.1. *AI-Enhanced*

Come illustrato nel paragrafo precedente, il coinvolgimento dell'IA nell'attività di vigilanza bancaria è stato oggetto di passaggi generazionali. I sistemi di IA possono svolgere una funzione "servente" all'autorità di vigilanza, cosiddetti *AI-Enhanced* o svolgere un ruolo attivo nel procedimento decisionale, *AI-Driven*.

Attualmente, in virtù delle limitazioni indicate al par. 4.2.5., la BCE ha scelto di avvalersi esclusivamente dell'*AI-Enhanced*. Una modalità di coinvolgimento, che all'inizio era unicamente finalizzata a sostituire le risorse umane nelle attività di: raccolta, analisi ed elaborazione dei dati, sintesi, traduzione di documenti ed indicazione degli elementi più rilevanti; ma ora trova il suo campo di elezione principale nel monitoraggio dei rischi connaturati all'attività bancaria e nello svolgimento dell'attività d'indagine. Non sembra presentare particolari ostacoli all'adempimento dell'obbligo, in capo alla BCE, di garantire una "buona amministrazione" quando l'IA svolge funzione "servente". La valutazione dell'*output* rimane di competenza della persona fisica ed i risultati raggiunti assumono una valenza esclusivamente interna non esplicando effetti verso i destinatari del provvedimento.

In realtà, l'utilizzo dell'*AI-Enhanced* diviene addirittura essenziale per stare al passo con i tempi e adattarsi alle sfide sempre più complesse dell'attività, nonché, per garantire la "buona amministrazione" attraverso una riduzione della durata dei procedimenti. Un elenco dei risvolti applicativi è offerto al par. 4 del Cap. III.

3.2. *AI-Driven*

Il termine "*AI-Driven*" descrive un processo guidato dall'intelligenza artificiale[55] e coincide con la quarta generazione *SupTech*. Gli strumenti in questione possono assumere la forma di motori di raccomandazione che suggeriscono corsi d'azione o anche di *chatbot* che eseguono compiti di supervisione precedentemente svolti dagli esseri umani[56].

[55] Definizione tratta dall'articolo: *What is AI-driven?* [Online]. Disponibile su: https://evolv.ai/glossary/ai-driven

[56] DI CASTRI S. *et al*., "*The suptech generations*", FSI Insights on policy implementation No 19, Bank for International Settlements, 2019, sez. 1.

Inoltre, sempre in questa direzione, è presumibile che possano essere impiegati per svolgere in modo autonomo talune attività in cui oggi l'IA ricopre un ruolo "servente". Si pensi ad un sistema di valutazione "*fit and proper*" che non si limiti alla sola lettura e valutazione del questionario, come avviene attualmente, ma ad un esame completo sull'idoneità di un determinato soggetto.

A livello tecnico tali sistemi presuppongono un'architettura costituita da big data in quanto la maggior parte di modelli *AI-Driven* richiedono, affinché i risultati siano validi, grandi volumi di dati e una potenza di calcolo significativa[57].

A livello giuridico sono, invece, maggiori gli ostacoli che la vigilanza bancaria "guidata" dall'IA potrebbe incontrare rispetto al quadro legale. Per questo motivo, si dedicherà all'*AI-Driven banking supervision* il par. 4. di questo capitolo.

3.3. Il piano di digitalizzazione dell'MVU: il *SupTech Hub* e la piattaforma *Virtual Lab*

In tempi recenti vi è stata una presa d'atto della BCE circa la necessità di redigere un piano di digitalizzazione del MVU al fine di cercare di integrare l'attività di supervisione bancaria con strumenti *SupTech*. In ragione di ciò, la BCE ha creato un apposito *Supervisory Technology (SupTech) Hub* che riunisce la stessa BCE e le autorità nazionali per facilitare la collaborazione e il coordinamento nella presentazione di progetti che utilizzano strumenti di apprendimento automatico, elaborazione del linguaggio naturale e analisi avanzata per svolgere funzioni di vigilanza quali: prove di stress, segnalatori di rischi e procedure di autorizzazione all'esercizio dell'attività bancaria[58]. La realizzazione del piano di digitalizzazione passerà attraverso cinque obiettivi fondamentali: la costituzione di un modello *hub and spoke* per la vigilanza bancaria; l'incentivo ai supervisori alla formazione di una cultura digitale; la creazione di un ecosistema di innovazione che vada oltre la vigilanza bancaria, l'utilizzo dell'intelligenza artificiale e dei *big data* per fornire ai supervisori tecnologie innovative all'avanguardia; l'automatizzazione e la digitalizzazione dei processi[59]. La collaborazione all'interno del

[57] Ibidem.
[58] Financial Stability Board, "*The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions - Market developments and financial stability implications*", 2020, allegato 1, caso 2. [Online]. Disponibile su: The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions: Market developments and financial stability implications (fsb.org)
[59] Ibidem.

SupTech Hub è supportata da una piattaforma tecnologica, ossia, *Virtual Lab*. Quest'ultima, basata su *cloud computing*[60] permette alle parti del MVU di connettersi tra loro con l'obiettivo di creare nuovi modelli di tecnologie innovative. Un'altra iniziativa è IMAS che agevola il flusso di informazioni sulle procedure di vigilanza e sul loro stato tra autorità di vigilanza e banche significative e non significative e terze parti come soggetti non vigilati e persone fisiche[61]. L'attuazione del piano di digitalizzazione, non può e non deve prescindere da una politica di rinnovamento del personale focalizzata al reclutamento di esperti nel campo delle tecnologie innovative e alla formazione del personale esistente attraverso specifici corsi[62].

3.4. I vantaggi derivanti dall'impiego delle nuove tecnologie nella vigilanza bancaria

Nel contesto bancario europeo, il rispetto delle regole prudenziali, da parte delle istituzioni bancarie, è di vitale importanza per garantire la stabilità bancaria e la fiducia dei clienti. L'introduzione dell'intelligenza artificiale nella vigilanza bancaria ha rivoluzionato il modo in cui le autorità di vigilanza, in particolare la BCE, svolgono l'attività di monitoraggio sugli istituti. Questa innovazione tecnologica ha portato una serie di vantaggi significativi che stanno radicalmente rivoluzionando il settore.

In via preliminare, urge segnalare che, trattandosi di tecnologie in fase di sperimentazione ed il cui utilizzo è diventato parte integrante dell'attività della BCE solo recentemente, non vi sono ancora dati statistici che possono accertare eventuali migliorie in termini di efficienza, efficacia ed economicità dell'azione amministrativa. Per questo motivo, si offriranno al lettore una panoramica dei vantaggi che certamente deriveranno dall'utilizzo dei sistemi di ML, che svolgono funzione "servente", tenuto conto delle caratteristiche intrinseche degli stessi e delle indagini svolte sul tema.

A livello terminologico, ad esser precisi, più che di vantaggi si dovrebbe parlare di approdi obbligatori per l'attività di vigilanza bancaria. Infatti, per vantaggio si intende

---

[60] «*È un termine usato per descrivere una rete globale di server, ognuno con una funzione univoca. Il cloud non è un'entità fisica, ma è una vasta rete di server remoti ubicati in tutto il mondo, che sono collegati tra loro e operano come un unico ecosistema*», si veda il sito di *Microsft Azure*: https://azure.microsoft.com/it-it/resources/cloud-computing-dictionary/what-is-the-cloud/

[61] Una descrizione del portale IMAS è offerta dal sito della BCE: https://www.bankingsupervision.europa.eu/banking/portal/imas/html/index.it.html

[62] Financial Stability Board, "*The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions - Market developments and financial stability implications*", 2020, par. 5. [Online]. Disponibile su: The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions: Market developments and financial stability implications (fsb.org)

una: «*posizione favorevole, (o) condizione favorevole che uno ha, con proprio giovamento, rispetto a un altro o ad altri con cui sussiste una gara o un confronto*»[63]. Nel caso di specie, l'impiego di tali strumenti non permetterebbe di raggiungere alcuna posizione di superiorità rispetto al fenomeno della vigilanza bancaria ma permetterebbe alle autorità di stare al passo con i tempi ed adattarsi alle sfide sempre più complesse della vigilanza, tra cui: l'aumento degli istituti da supervisionare, l'avvento di nuove forme di comunicazione, nuovi rischi e pericoli, l'ottimizzazione delle risorse economiche, la realizzazione di un sistema bancario più solido e capace di attirare più capitali rispetto alle potenze economiche concorrenti etc.

I vantaggi[64] apportati dalle tecnologie innovative riguardano vari settori dell'attività di vigilanza quali: le segnalazioni di vigilanza, la gestione dei dati, l'analisi microprudenziale e più specificamente, sul rispetto delle norme antiriciclaggio e contro il finanziamento del terrorismo[65].

Per quanto riguarda le segnalazioni di vigilanza, l'automatizzazione dell'attività di valutazione delle stesse passa dalla previsione, sul sito[66] della BCE, di una *Whistelblowing platform*. La BCE incentiva i cittadini a segnalare le violazioni, del diritto dell'Unione in materia bancaria, di una banca vigilata che ricade sotto la sua diretta competenza o di un'autorità nazionale. Successivamente, la segnalazione è valutata da un gruppo di esperti, circa la competenza della BCE, per poi essere inoltrata alla struttura competente. Sebbene, attualmente, il sistema sia finalizzato unicamente ad automatizzare la ricezione delle informazioni, in futuro, è probabile che anche la fase di valutazione della competenza dell'autorità, attualmente svolta da un gruppo di esperti, sarà svolta da sistemi di ML. Per quanto riguarda quest'ultimo aspetto, non essendo un'attività discrezionale ma vincolata, anche l'utilizzo di algoritmi condizionali[67] potrebbe esser sufficiente.

---

[63] Definizione tratta dal vocabolario Treccani rinvenibile al sito: https://www.treccani.it/vocabolario/vantaggio/

[64] Per comodità espositiva, d'ora in avanti, si userà il termine vantaggi, nonostante si sottolinea che non si tratta di veri e propri vantaggi.

[65] Financial Stability Board, *The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions - Market developments and financial stability implications*, 2020, par. 7.

[66] Il sito è: https://whistleblowing.bankingsupervision.europa.eu/

[67] Si veda il par. 1.1. per la distinzione tra algoritmi condizionali e quello che si avvalgono di tecniche di ML.

La gestione dei dati è sicuramente il settore dell'attività di vigilanza che potenzialmente è in grado di beneficiare maggiormente dell'avvento dell'intelligenza artificiale. Le applicazioni *Suptech* sono suscettibili di incrementare il valore dei dati attraverso una riduzione della complessità degli stessi[68], nonché, attraverso una loro elaborazione in un tempo nettamente inferiore rispetto all'attività umana o comunque di sistemi che non si avvalgono di ML. Un ulteriore vantaggio è la riduzione dei costi della gestione dei dati ottenuta attraverso la digitalizzazione degli stessi che potrebbe migliorare efficienza ed efficacia dei processi operativi riducendo costi operativi e del personale[69].

L'impatto della *Suptech*, attraverso la centralizzazione di alcuni processi per evitare di svolgere la stessa attività più volte[70], è stato determinante per far fronte all'aumento della complessità dei dati da esaminare.

Le cause dell'aumento della loro complessità sono: l'eterogeneità dei dati degli istituti regolamentati che rende difficile per le autorità dare istruzioni univoche e prive di ambiguità per tutti gli istituti regolamentati; l'eterogeneità delle esigenze delle autorità in materia di dati che essendo destinati a specifiche finalità rendono complicato il riutilizzo; la duplicazione dei processi tra le istituzioni regolamentate[71].

L'attività di gestione dei dati è un'attività complessa, in quanto composta da una serie operazioni quali la comunicazione, la raccolta, la memorizzazione, l'analisi e visualizzazione dei dati.

L'attività di comunicazione e raccolta dei dati è la prima fase dell'attività di gestione dei dati, comprendente l'attività di comunicazione, cioè, di trasmissione dei dati all'autorità di vigilanza nonché la fase di raccolta degli stessi. Le tecnologie *Suptech* sono in grado di ricevere grandi quantità di dati strutturati[72] e non strutturati[73], garantendo efficienze

---

[68] Financial Stability Board, *The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions - Market developments and financial stability implications*, 2020, par. 7.

[69] Ivi par. 3.1.

[70] Molti elementi della produzione dei *report* sono comuni a tutte l'entità vigilate.

[71] Financial Stability Board, *The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions - Market developments and financial stability implications*, 2020, par. 6.

[72] «*I dati strutturati, identificati da tag di metadati, seguono sempre uno schema predefinito, presentando le informazioni che contengono in modo organizzato. I dati strutturati hanno una struttura e un formato standardizzato e ben definito, si conformano allo stesso modello di dati e seguono uno specifico ordine. Ciò li rende facilmente accessibili e particolarmente utili durante i processi di analisi, scienza dei dati e-business intelligence*». Definizione tratta dall'articolo rinvenibile al sito: https://www.it-impresa.it/blog/dati-strutturati-e-non-strutturati/

[73] «*I dati non strutturati si presentano sotto forma di immagine, video, testo o audio. Spesso, infatti sono: in costante movimento, di origine imprevedibile, digitali, interoperabili, misti e multimodali, dislocati*

operative nei processi di raccolta e rendicontazione degli stessi[74]. Nonostante ciò, nell'indagine del *Financial Stability Board*, nel 2020, più di un terzo delle autorità continuavano usare sistemi non innovativi per la raccolta dei dati di *reporting* delle banche, mentre, il resto portali[75]. L'innovazione, al fine di facilitare e automatizzare la comunicazione tra banche e autorità di vigilanza, ha introdotto le interfacce di programmazione delle applicazioni (API)[76]. Tale applicazione ha comportato una riduzione dei costi e la possibilità di modificare, in tempo reale, le informazioni nei casi di eventi economici inattesi[77].

L'attività di raccolta dati deve essere, non solo efficace, sicura ed economica ma, anche eterogenea e tempestiva. Il principio dell'eterogeneità dell'attività è rappresentativo della necessità di non limitare la raccolta dati a quelli presentati dalle banche e richiesti dalla normativa, ma anche a tutte quelle informazioni presenti nei motori ricerca, i cd. dati *open source*[78]. Quest'ultimi, spesso, si caratterizzano per volumi elevati e forme non strutturate che renderebbero, se non coadiuvata da sistemi di elaborazione dei dati basati su IA, difficile e dispendiosa la loro estrazione.

L'attività di memorizzazione è la fase successiva a quella di raccolta dei dati e consiste nell'attività di archiviazione e conservazione dei dati comunicati dagli istituti vigilati. L'incremento dei dati e dei costi di conservazione ha spinto le autorità di vigilanza ad avvalersi di infrastrutture efficienti come la tecnologia *cloud*[79] in grado di garantire: agilità per accedere a più tecnologie per svariati fini; elasticità tale da non dover allocare

---

geograficamente (a beneficio della loro stessa protezione)». Definizione tratta dall'articolo rinvenibile al sito indicato nella nota precedente.

[74] Financial Stability Board, *The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions - Market developments and financial stability implications*, 2020, par. 6.1.

[75] Ibidem.

[76] «*Le API sono intermediari software fondamentali che consentono a varie banche dati e programmi di scambiarsi informazioni*». Definizione tratta dall'articolo rinvenibile al sito: https://www.capterra.it/glossary/884/application-programming-interface#:~:text=Un'interfaccia%20di%20programmazione%20delle,programmi%20software%20comunicano%20tra%20loro.

[77] Financial Stability Board, *The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions - Market developments and financial stability implications*, 2020, par. 6.1.

[78] «*Gli Open Data, o dati aperti, sono dati accessibili a tutti, messi a disposizione da Pubbliche Amministrazioni o aziende private che possono essere riutilizzati per diversi scopi*». Definizione tratta dall'articolo rinvenibile al sito: https://www.forumpa.it/pa-digitale/open-data-cosa-sono-come-sfruttarli-e-stato-dellarte-in-italia/

[79] «*Il cloud computing consiste nella distribuzione on-demand delle risorse IT tramite Internet, con una tariffazione basata sul consumo. Piuttosto che acquistare, possedere e mantenere i data center e i server fisici, è possibile accedere a servizi tecnologici, quali capacità di calcolo, archiviazione e database, sulla base delle proprie necessità affidandosi a un fornitore cloud*». Definizione tratta dall'articolo rinvenibile al sito: https://aws.amazon.com/it/what-is-cloud-computing/

in anticipo una quantità maggiore di risorse di quante siano necessarie, così da gestire i picchi nei livelli di attività in futuro; risparmio sui costi quali *data center* e *server* fisici in favore di una risorsa variabile a seconda dello spazio di archiviazione utilizzato[80]. Tuttavia, l'esternalizzazione, attraverso *cloud*, della fase di memorizzazione è suscettibile di aumentare la vulnerabilità informatica e ridurre la capacità delle autorità di valutare se un dato servizio è conforme al tessuto normativo[81]. La maggior parte delle autorità intervistate dal *Financial Stability Board* ha dichiarato che sta valutando l'adozione di tecniche di memorizzazione dei dati basate su *cloud* [82]. Sebbene la tecnologia *cloud* sia diversa dall'IA, oggi la capacità dell'intelligenza artificiale, basata sull'apprendimento automatico, consente di ricavare interpretazioni imparziali di informazioni basate sui dati accrescendo l'efficienza dei processi, riducendo i costi e migliorando la fase di memorizzazione dei dati[83].

L'ultima fase della gestione dei dati è finalizzata all'analisi e visualizzazione dei dati precedentemente raccolti che consistono rispettivamente nel «*processo con cui si ricavano informazioni da dati che vengono estratti, trasformati e centralizzati per scoprire e analizzare schemi nascosti, relazioni, tendenze, correlazioni e anomalie, oppure per convalidare una teoria o un'ipotesi*»[84] e «*la rappresentazione grafica di informazioni e dati grazie a elementi visivi come diagrammi, grafici e mappe, gli strumenti per la visualizzazione dei dati creano una soluzione accessibile per osservare e comprendere tendenze, valori anomali e ricorrenze presenti nei dati*»[85]. In precedenza, le autorità di vigilanza si affidavano ad *Excel* per funzioni di calcolo ed analisi, ma con l'aumento dell'uso dei dati non strutturati, hanno preso atto dell'incapacità dei sistemi tradizionali ad analizzare dati non strutturati e hanno iniziato ad adottare strumenti

[80] Ibidem.
[81] Financial Stability Board, *The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions - Market developments and financial stability implications*, 2020, par. 6.2.
[82] Ibidem.
[83] BRENNER M., *The Role of AI in Cloud Computing*, in The Forecast by Nutanix, 2023. [Online]. Disponibile su: https://www.nutanix.com/theforecastbynutanix/technology/ai-in-the-cloud
[84] Definizione tratta dall'articolo rinvenibile al sito: https://www.talend.com/it/resources/what-is-data-analytics/#:~:text=L'analisi%20dei%20dati%20%C3%A8,una%20teoria%20o%20un'ipotesi.
[85] Definizione tratta dall'articolo rinvenibile al sito: https://www.tableau.com/it-it/learn/articles/data-visualization#:~:text=La%20visualizzazione%20dei%20dati%20%C3%A8,e%20ricorrenze%20presenti%20nei%20dati.

SupTech[86]. Un esempio è NAVI – *Network Network Analytics and Visualisation*[87], uno strumento impiegato dalla BCE che utilizza l'analisi di rete e le visualizzazioni grafiche come mezzo per ottenere una rappresentazione visiva e intuitiva degli assetti proprietari, nonché, della misura in cui gli azionisti degli enti significativi sono interconnessi[88]. Inoltre, sono state introdotte tecnologie basate su algoritmi di NLP, cioè, «*in grado di analizzare, rappresentare e quindi comprendere il linguaggio naturale*»[89] di estrarre maggiori informazioni dai dati disponibili in minor tempo e risorse rispetto alla supervisione umana. In particolare, la *Federal Reserve* sta adottando delle soluzioni *SupTech* in grado di estrarre ed analizzare informazioni da gradi moli di dati, anche non strutturati, da vari documenti allo scopo di monitorare gli istituti bancari più grandi e scorgere i *trend* emergenti[90].

Per quanto riguarda la vigilanza micropudenziale, le autorità, attraverso la *SupTech*, sono state in grado di codificare alcuni controlli e convalide più semplici, concentrandosi su fasi dell'attività più complesse. Un'applicazione dell'IA, nell'ambito della vigilanza microprudenziale, è il *Early Warning System* (EWS) per le banche *less significant,* ossia un modello di ML in grado di supportare il lavoro, della BCE e delle autorità nazionali competenti, nell'individuazione dei casi di sofferenza finanziaria degli istituti bancari meno significativi[91] [92]. Tutto ciò, presenta numerosi vantaggi in termini di risposta in tempo reale a fenomeni che richiedono celerità e precisione nell'intervento.

Nello stesso modo, anche la vigilanza degli istituti bancari sul rispetto delle norme antiriciclaggio e contro il finanziamento del terrorismo si presta ad esser automatizzata,

---

[86] Financial Stability Board, *The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions - Market developments and financial stability implications*, 2020, par. 6.2.

[87] Le caratteristiche di tale innovazione così come delle altre citate in seguito saranno trattate nello specifico nel capitolo 3.

[88] MCCAUL E., *The impact of suptech on European banking supervision, at the Supervision Innovators Conference*, 2022. [Online]. Disponibile su: https://www.bankingsupervision.europa.eu/press/interviews/date/2024/html/ssm.in240226~c6f7fc9251.en.html

[89] Definizione tratta dall'articolo rinvenibile al sito: https://blog.osservatori.net/it_it/natural-language-processing-nlp-come-funziona-lelaborazione-del-linguaggio-naturale

[90] Financial Stability Board, *The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions - Market developments and financial stability implications*, 2020, Allegato 1 – Caso studio 24.

[91] La competenza sulla vigilanza delle banche meno significative, salvo eccezioni, spetta alle autorità nazionali competenti che operano sotto la supervisione della BCE. Si rimanda al par. 2.1 per una trattazione approfondita.

[92] Financial Stability Board, *The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions - Market developments and financial stability implications*, 2020, Allegato 1 – Caso studio 18.

in quanto regolata da un quadro normativo che può esser facilmente codificato[93]. L'Autorità monetaria di Singapore supervisiona le istituzioni regolamentate, per la gestione del rischio di riciclaggio e di finanziamento al terrorismo, attraverso uno strumento di analisi di rete di segnalazione delle operazioni sospette per identificare i gruppi di soggetti con comportamenti sospetti, nonché, gli istituti regolamentati coinvolti[94]. L'approccio innovativo ha favorito il migliore perseguimento degli obiettivi di vigilanza e di perseguimento del fenomeno del crimine finanziario attraverso una rappresentazione visiva e intuitiva delle operazioni sospette e dei loro artefici.
Per concludere, numerose autorità hanno adottato strumenti di IA per permettere al personale di concentrare l'attenzione su quelle fasi del ciclo di vita dei dati caratterizzate, storicamente, da un'intensa attività manuale.

3.5. I limiti all'utilizzo dei dati personali da parte dei sistemi di intelligenza artificiale

Il trattamento dei dati personali, nonché, il loro utilizzo attraverso qualunque modalità, durante l'attività di vigilanza bancaria, rientra nell'ambito di applicazione del GDPR.
Il Regolamento Generale sulla Protezione dei Dati (GDPR) è una legge europea che regola la protezione dei dati personali dei cittadini dell'Unione Europea. È stato adottato il 27 aprile 2016 ed è entrato in vigore il 25 maggio 2018, sostituendo la precedente Direttiva sulla protezione dei dati del 1995. La sua adozione ha rivoluzionato la gestione dei dati personali, imponendo regole più stringenti e promuovendo una maggiore trasparenza e responsabilità nell'uso dei dati. Una delle caratteristiche fondamentali del GDPR è la sua ampia portata; si applica a tutte le organizzazioni che trattano dati personali di individui nell'Unione Europea, indipendentemente dalla loro ubicazione geografica. Questo significa che aziende, enti governativi, organizzazioni *no profit* e qualsiasi altra entità che gestisca dati personali di cittadini europei deve conformarsi al regolamento, come ad esempio la BCE. La tutela degli individui, riguardo ai loro dati personali, assume importanza centrale nel Regolamento attribuendogli il diritto di: essere informati su come i loro dati vengono utilizzati, accedere ai propri dati, correggerli, cancellarli, limitare il loro trattamento e trasferirli ad altre organizzazioni.

[93] Ivi par. 7.
[94] Ivi Allegato 1 – Caso studio 12.

Questi diritti danno agli individui un maggiore controllo sui propri dati e impongono agli enti che li trattano di essere più trasparenti e responsabili. Il Regolamento richiede anche che le organizzazioni ottengano un consenso esplicito e informato prima di trattare i dati personali degli individui. Inoltre, il GDPR impone alle organizzazioni di adottare misure adeguate a proteggere i dati personali e di notificare le violazioni dei dati alle autorità competenti e agli individui interessati entro tempi definiti.

Sono numerose le categorie di dati personali coinvolte nell'attività di supervisione delle banche quali, ad esempio, i dettagli riguardanti la sfera personale o professionale, dati finanziari o amministrativi, casellari giudiziari, nonché, dettagli sulle interazioni commerciali di un individuo. I dati personali possono essere utilizzati per scopi di sorveglianza, come, ad esempio, nell'ambito di valutazioni di idoneità e correttezza, autorizzazioni o revoca di licenze bancarie, o ispezioni in loco[95]. In alcuni casi, l'attività di vigilanza della BCE non può prescindere dal trattamento di dati sensibili. Ad esempio, dal 4 novembre 2014, la Banca Centrale Europea (BCE) è responsabile della verifica dell'idoneità di tutti i membri degli organi di amministrazione delle istituzioni finanziarie, ritenute significative e soggette alla sua vigilanza diretta. Nel caso della valutazione circa la sussistenza del requisito dell'onorabilità, la Guida alla verifica dei requisiti di idoneità[96] stabilisce che si tiene conto dei casellari giudiziari e dei registri amministrativi pertinenti, considerando il tipo di condanna o incriminazione, il ruolo del soggetto coinvolto, la pena inflitta, il grado di giudizio raggiunto, il valore probatorio dei rilievi e di qualsivoglia informazione che abbia il sortito effetto[97].

La BCE, quale titolare del trattamento, deve garantire che il trattamento dei dati avvenga in modo chiaro, equo e trasparente[98], esplicitando il fine per cui vengono specificamente raccolti[99]. Inoltre, è chiamata a rispettare il principio di minimizzazione dei dati[100], nonché, a garantirne l'esattezza[101].

---

[95] RINGE W.G. *et al*., *Navigating the Legal Landscape of AI-Enhanced Banking Supervision: Protecting EU Fundamental Rights and Ensuring Good Administration,* European Banking Institute Working Paper Series 2023 - no. 140, 2023, Cap. IV, par. B.1.

[96] BCE, *Guida alla verifica dei requisiti di idoneità*, dicembre 2021. [Online]. Disponibile su: https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.fit_and_proper_guide_update202112~d66f230eca.it.pdf

[97] Ivi p. 16.

[98] Art. 5, comma 1, lett. a) del GDPR.

[99] Art. 5, comma 1, lett. b) del GDPR.

[100] Art. 5, comma 1, lett. c) del GDPR. Per principio di minimizzazione assicura che i dati siano: «*adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati*»

[101] Art. 5, comma 1, lett. d) del GDPR.

All'art. 14 del GDPR sono riconosciuti i diritti che spettano all'interessato. In particolare, su tutti, il diritto: di accesso[102], di informazione[103], di rettifica[104] e cancellazione[105], di limitazioni di trattamento[106], portabilità dei dati[107], opposizione[108], di non essere sottoposto a una decisione basata unicamente su un trattamento automatizzato[109]. La portata di tali diritti non è assoluta, infatti, l'art. 23 al comma 1 lett. e), prevede che il diritto dell'Unione o dello Stato membro, cui è soggetto il titolare del trattamento o il responsabile del trattamento, può limitare, in misura proporzionale e necessaria, la portata degli obblighi e dei diritti di cui agli art. 12 a 22 e 34, per la salvaguardia di obiettivi di interesse pubblico generale dell'Unione o di uno Stato membro, come un rilevante interesse economico o finanziario dell'Unione o di uno Stato membro, anche in materia monetaria, di bilancio e tributaria, di sanità pubblica e sicurezza sociale. Tra gli obiettivi rientra, certamente, la garanzia della stabilità del sistema bancario di cui è responsabile la BCE che, al fine di esercitare adeguatamente le funzioni di vigilanza, potrà beneficiare di talune esenzioni agli obblighi previsti in capo al titolare e al responsabile del trattamento. Alla luce di quanto detto precedentemente, sono facilmente percepibili i possibili motivi di attrito fra l'impiego dell'IA nell'attività di supervisione e il GDPR, in quanto, l'incremento della qualità dell'*output* di qualunque sistema di ML passa per la raccolta e il consequenziale *training* su un gran numero di dati. L'esistenza di una disciplina a protezione dei dati personali limita lo sviluppo e il miglioramento dei sistemi di IA. In particolare, l'esercizio del diritto alla minimizzazione e all'oblio, cioè, che i trattamenti siano «*adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati*»[110] e alla «*cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo*»[111] può porre dei limiti alla raccolta e all'utilizzo dei dati personali. Alla luce di ciò, supponendo che l'addestramento dell'IA sia una motivazione

[102] Art. 15 del GDPR.
[103] Art. 34 del GDPR.
[104] Art. 16 del GDPR.
[105] Art. 17 del GDPR.
[106] Art. 18 del GDPR.
[107] Art. 20 del GDPR.
[108] Art. 21 del GDPR.
[109] Art. 22 del GDPR.
[110] Art. 5, comma 1, lett. a) del GDPR.
[111] Art. 17, comma 1 del GDPR.

valida e legittima, fino a che punto la restrizione dei diritti alla protezione dei dati può essere consentita per l'esercizio delle funzioni di vigilanza[112]?

Il secondo conflitto di interessi può sussistere tra il diritto, di cui all'art. 22, che sancisce il diritto dell'interessato «*di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona*»[113] e l'automazione delle procedure di vigilanza. In altre parole, da un lato, vi è il destinatario del provvedimento che ha diritto alla presenza della componente umana nel corso del procedimento per permettergli di esprimere la sua opinione ed eventualmente contestare la decisione, dall'altro, l'interesse della BCE a velocizzare e rendere più efficienti le procedure, anche escludendo l'apporto dell'attività umana in quelle più semplici. Inoltre, sono previste ulteriori tutele che impongono di informare l'individuo sull'esistenza di un trattamento automatizzato e di fornire una spiegazione sulla logica della tecnologia e delle possibili conseguenze, che equivale ad una sorta di spiegabilità dell'IA, essenziale anche per il rispetto della buona amministrazione[114]. Per concludere, anche se per aspetti diversi, la salvaguardia della trasparenza e della controllabilità dell'IA assume importanza, indipendentemente dal principio di buona amministrazione, essendo in gioco interessi diversi, altrettanto meritevoli di tutela.

4. *AI-Driven banking supervision* e il diritto ad una buona amministrazione

La salvaguardia della stabilità del sistema bancario costituisce una priorità dell'Unione europea che ha, con il Regolamento (UE) n. 1024/2013, stabilito un quadro regolamentare per la disciplina della vigilanza delle banche attraverso l'attribuzione di un ruolo centrale alla BCE e concorrente alle autorità nazionali. Ma, in un mondo in continua evoluzione, dove le minacce alla stabilità del sistema sono molteplici e spesso in grado di pregiudicare in pochissimo tempo la salute di una banca[115], l'innovazione, in virtù della sua capacità

---

[112] RINGE W.G. *et al*., *Navigating the Legal Landscape of AI-Enhanced Banking Supervision: Protecting EU Fundamental Rights and Ensuring Good Administration,* European Banking Institute Working Paper Series 2023 - no. 140, 2023, Cap. IV, par. B.1.

[113] Art. 22, comma 1 del GDPR.

[114] RINGE W.G. *et al*., *Navigating the Legal Landscape of AI-Enhanced Banking Supervision: Protecting EU Fundamental Rights and Ensuring Good Administration,* European Banking Institute Working Paper Series 2023 - no. 140, 2023, Cap. IV, par. B.1.

[115] Si pensi al caso della *Silicon Valley Bank* ove in meno di 10 ore, con il *digitale banking*, i clienti tramite un passaparola via *social* hanno ritirato in totale circa 42 miliardi di euro. Si veda: GRAZIANI A., *Silicon Valley Bank, il primo default nell'era del mobile banking e dei social,* Il Sole 24 ORE, 2023. [Online].

di elaborazione e velocità di calcolo, diventa cruciale per riuscire ad anticipare future crisi.

Premesso ciò, ci si interroga sull'ammissibilità in futuro, accanto alla vigilanza "migliorata" dall'IA[116], di una vigilanza "guidata" dall'IA[117].

Sono vari i rischi associati allo sviluppo e all'integrazione dell'IA nel procedimento decisionale, alcuni comuni a tutte le applicazioni di IA come quello della mancanza di trasparenza della logica algoritmica, cosiddetto "*black box problem*" e del garantire la qualità e la riservatezza dei dati, altri tipici dell'*AI-Driven* come la garanzia della "buona amministrazione".

L'attività di vigilanza è un'attività amministrativa che deve essere esercitata necessariamente nel rispetto dei diritti del destinatario del procedimento, tra cui il diritto al contraddittorio, all'esser ascoltati, di accesso al fascicolo, ad una decisione motivata che non possono esser sempre garantiti in caso di utilizzo di tecnologie innovative. Con i sottoparagrafi successivi, si procederà, dopo una breve illustrazione[118] del funzionamento e della *governance* del MVU, ad analizzare il diritto ad una buona amministrazione *ex* art. 41 della Carta dei diritti fondamentali dell'Unione europea e i possibili vantaggi, limitazioni ed interrogativi che possono derivare dall'automazione del procedimento di supervisione bancaria.

4.1. Compiti, poteri e procedimento decisionale della BCE

Il Meccanismo di vigilanza unico, istituito con Regolamento (UE) n. 1024/2013, è un sistema di vigilanza costituito per monitorare, in via unitaria, le banche nell'eurozona[119]. Sebbene in dottrina sono state avanzate differenti interpretazioni circa l'architettura del

Disponibile su: https://www.ilsole24ore.com/art/silicon-valley-bank-primo-default-nell-era-mobile-banking-e-social-AE5bwj3C

[116] *AI-Enhanced banking supervision*.

[117] *AI-Driven banking supervision.*

[118] L'illustrazione del paragrafo successivo (par. 2.1) non mira ad essere esaustiva, ma si concentrerà esclusivamente sulla descrizione degli aspetti fondamentali del MVU al fine di fornire al lettore una visione generale del contesto in cui opera la *SupTech*.

[119] Anche gli altri Stati Membri, che non hanno adottato l'euro, possono aderirvi tramite un accordo di cooperazione rafforzata.

meccanismo[120], la Corte di Giustizia nelle prime sentenze[121], riguardanti provvedimenti adottati dalla BCE nell'ambito dell'attività di vigilanza microprudenziale, ha affermato che il Regolamento ha attribuito alla stessa competenza esclusiva «*nei confronti di tutti gli enti creditizi stabiliti negli Stati membri partecipanti senza distinzione tra gli enti significativi e gli enti meno significativi*»[122]. Le autorità nazionali collaborano con la BCE mediante un'attuazione decentralizzata di alcune mansioni in relazione agli enti meno significativi, fatto salvo il potere della BCE di avocare a sé la vigilanza sugli stessi, in quanto, responsabile del buon funzionamento dell'intero sistema.

I compiti della BCE, nell'ambito della vigilanza microprudenziale, sono elencati all'art. 4 del sopracitato regolamento sono: il rilascio o la revoca dell'autorizzazione all'esercizio dell'attività bancaria[123], la valutazione delle notifiche di acquisto e cessione di partecipazioni al capitale delle banche[124], il monitoraggio continuo sul rispetto dei requisiti prudenziali in materia di fondi propri, cartolarizzazione, limiti ai grandi rischi, liquidità, leva finanziaria, segnalazione e informativa al pubblico delle informazioni su tali aspetti[125]. La BCE ha il compito di assicurare il rispetto delle regole di governo societario, compresi i requisiti di professionalità e onorabilità per le persone responsabili dell'amministrazione degli enti creditizi, di processi di gestione del rischio, di meccanismi di controllo interno, di politiche e prassi di remunerazione e di processi efficaci di valutazione dell'adeguatezza del capitale interno, compresi i modelli basati sui rating interni[126]. Inoltre, effettua le valutazioni prudenziali, comprese le prove di stress per accertare se i dispositivi, le strategie, i processi e meccanismi instaurati dagli enti creditizi e i fondi propri da essi detenuti permettano una gestione solida e la copertura dei rischi imponendo, alla luce della valutazione, ulteriori obblighi specifici in materia di fondi propri aggiuntivi, specifici requisiti di informativa e di liquidità[127]. Con riferimento

[120] Una parte a sostegno del completo trasferimento, dalle autorità nazionali alla BCE, di tutte le competenze in materia di vigilanza e un'altra parte a sostegno dell'interpretazione secondo la quale alla BCE fossero stati trasferiti i compiti principali nei confronti delle banche "più significative" e lasciati alle autorità nazionali, quelli verso le banche "meno significative". Si veda: BRESCIAMORRA C., *Il diritto delle banche*, Il Mulino, Bologna, 2020, par. 8.4.1.

[121] Tribunale UE, 16 maggio 2017, Caso T-122/15, *Landeskreditbank- Württemberg- Förderbank* c. Banca centrale europea confermata in appello con sentenza della Corte di Giustizia, 8 maggio 2019, Caso C-450/17 P.

[122] Corte di Giustizia, 8 maggio 2019, Caso C-450/17 P.

[123] Art. 4, par. 1, lett. a), del Regolamento 1024/2013.

[124] Art. 4, par. 1, lett. c), del Regolamento 1024/2013.

[125] Art. 4, par. 1, lett. d)., del Regolamento 1024/2013.

[126] Art. 4, par. 1, lett. e), del Regolamento 1024/2013.

[127] Art. 4, par. 1, lett. f), del Regolamento 1024/2013.

ai gruppi, la BCE esercita la vigilanza, su base consolidata, delle imprese madri degli enti creditizi stabilite in uno degli Stati membri partecipanti e partecipa ai collegi delle autorità di vigilanza sulle imprese madri non stabilite in uno degli Stati membri partecipanti[128]. In ultimo, la BCE assolve i compiti di vigilanza collegati ai piani di risanamento e alle misure di intervento precoce qualora un ente creditizio non soddisfi, o rischi di non soddisfare, i requisiti prudenziali applicabili[129].

A livello macroprudenziale la competenza ad adottare misure volte ad affrontare i rischi sistemici spetta, in via principale, alle autorità nazionali che devono operare in stretto coordinamento con la BCE e in via sussidiaria, alla stessa BCE cui è attribuita la potestà di assumere, in luogo delle autorità nazionali, misure più rigorose per scongiurare i rischi sistemici.

L'esecuzione dei compiti previsti dal regolamento è funzionale alla realizzazione degli obiettivi della vigilanza bancaria: la verifica formale del soddisfacimento dei requisiti prudenziali e la garanzia della sana e prudente gestione[130] [131]. Affinché si possa individuare la fase dell'attività di supervisione ove possono esser maggiormente impiegati i sistemi di ML, può essere utile adottare una distinzione fatta in dottrina tra "poteri di vigilanza" e "strumenti di vigilanza": i primi attengono alle tipologie di decisione di cui possono essere destinatarie le banche; i secondi alle tecniche utilizzate per monitorare il soddisfacimento dei requisiti prudenziali[132]. Tra i "poteri di vigilanza" anche noti come poteri di vigilanza specifici, rinveniamo quelli in cui la BCE è chiamata a prendere una decisione, non a monitorare un'attività, come: sulla valutazione della dirigenza, sull'autorizzazione o revoca all'esercizio dell'attività bancaria, sull'acquisto di partecipazioni rilevanti, sulle sanzioni amministrative per le violazioni della normativa e su questioni macroprudenziali, di risoluzione o risanamento.

Un ruolo altrettanto essenziale all'interno del MVU è svolto dagli "strumenti di vigilanza" quali: la richiesta d'informazioni, le indagini generali e le ispezioni in loco nei confronti

[128] Art. 4, par. 1, lett. g), del Regolamento 1024/2013.
[129] Art. 4, par. 1, lett. i), del Regolamento 1024/2013.
[130] L'obiettivo di garantire la sana e prudente gestione sarebbe perseguito attraverso la previsione di requisiti patrimoniali, valutazioni di idoneità della dirigenza e regole in materia di *governance*.
[131] WYMEERSCH E., *The Single Supervisory Mechanism or SSM, Part One of the Banking Union*, in "ECGI Working Paper Series in Law", n. 240, 2014, par. 6.9. [Online]. Disponibile: https://www.ecgi.global/sites/default/files/working_papers/documents/SSRN-id2397800.pdf
[132] Ibidem.

delle banche, le istruzioni impartite a singoli soggetti sull'attività di vigilanza, nonché, raccomandazioni e gli orientamenti dettati e la redazione di regolamenti[133] [134].

Il primo potere d'indagine, disciplinato dall'art. 10 del regolamento consiste nella richiesta di informazioni con la quale la BCE può esigere, dalle persone fisiche o giuridiche di cui al par. 1 lett. a) – lett. f), la comunicazione di tutte le informazioni di cui necessita per assolvere i compiti di cui al regolamento, comprese le informazioni da fornire con frequenza periodica e in formati specifici sia a scopo di vigilanza e che relative fini statistici. La comunicazione e la valutazione di queste informazioni può esser agevolata, migliorata ed ottimizzata con l'uso del ML.

Ai sensi dell'art. 11 la BCE può svolgere tutte le indagini necessarie tra cui chiedere la presentazione di documenti (lett. a), esaminare i libri, i registri contabili, fare copie o estratti dei suddetti libri e documenti (lett. b), ottenere spiegazioni scritte o orali (lett. c), organizzare audizioni per ascoltare altre persone che acconsentano ad essere interpellate allo scopo di raccogliere informazioni pertinenti all'oggetto dell'indagine (lett. d). Talvolta, a norma dell'art. 13[135] e previa notifica all'autorità nazionale competente interessata, essa procede alle ispezioni necessarie presso i locali commerciali delle persone giuridiche di cui all'art. 10, par. 1, e di qualsiasi altra impresa inclusa nella vigilanza su base consolidata esercitata dalla BCE a norma dell'art. 4, par 1, lett. g).

4.2. Il diritto ad una buona amministrazione nella vigilanza bancaria automatizzata

Tra i vari obiettivi dell'Unione europea vi rientra quello di garantire la fornitura efficace ed efficiente dei servizi pubblici svolti dalle istituzioni europee e di riconoscere, allo stesso tempo, una protezione giuridica ai destinatari in caso di violazioni perpetrate nei loro confronti.

Per questo motivo, si è fatto largo il concetto di "buona amministrazione" come criterio "guida" dell'azione amministrativa e come diritto fondamentale della Carta dei diritti fondamentali dell'Unione europea. L'art. 41 sancisce un diritto essenziale per il funzionamento delle istituzioni dell'Unione Europea, in quanto, garantisce ai cittadini

[133] Art, 4, par. 3 del Regolamento 1024/2013.

[134] La BCE può, inoltre, adottare regolamenti solo nella misura in cui ciò sia necessario per organizzare o precisare le modalità di assolvimento dei compiti attribuitile dal presente regolamento. Pertanto, tale competenza non interferirà con i compiti di potestà regolamentare dell'ABE.

[135] L'art. 13 impone alla BCE di richiedere l'autorizzazione giudiziaria ogniqualvolta sia richiesta dalle regole nazionali.

l'agire in modo imparziale, equo e tempestivo dell'amministrazione. L'attività di vigilanza bancaria, svolta dalla BCE[136], è un'attività amministrativa ed in quanto tale conosce i suoi limiti anche nella protezione offerta dall'art. 41 ai destinatari dei procedimenti, ossia, gli istituti di credito nell'ambito del MVU.

La previsione del diritto ad una buona amministrazione non costituisce una novità nell'ordinamento comunitario in quanto l'obiettivo dei redattori della Carta era quello di riaffermare dei diritti già esistenti del diritto dell'Unione europea per garantire un innalzamento dello *standard* di tutela[137].

La giurisprudenza comunitaria, sin dalle prime decisioni in materia amministrativa, aveva introdotto i concetti di "buona"[138], "sana"[139] e "corretta"[140] amministrazione fino a giungere all'affermazione del principio in un'ottica di protezione dell'individuo dall'agire delle istituzioni. I primi corollari di tale principio, affermati in fase di elaborazione dello stesso, sono stati: la tutela del contraddittorio[141] tra privato e procedente e il diritto ad ottenere l'accesso ai documenti amministrativi[142] per vagliare l'ammissibilità e la fondatezza del procedimento e quindi, garantire l'esercizio del diritto alla difesa[143]. Dai primi, ne sono derivati altri come naturale conseguenza, quale, ad esempio, l'obbligo di motivazione[144], essenziale per garantire il diritto alla difesa ma anche il controllo sull'operato delle istituzioni da parte dei cittadini. Tuttavia, trattandosi di un principio e non di una regola specifica, nella giurisprudenza dei primi decenni[145] si sosteneva che non avesse forza autonoma né giustiziabile dai destinatari[146] ma, natura

---

[136] La BCE è un'istituzione europea ai sensi dell'art. 13, comma 1 TUE.

[137] PROVENZANO P, *Procedimento amministrativo e diritto ad una buona amministrazione,* in D.U. Galetta (a cura di), *Diritto amministrativo nell'unione europea: argomenti e materiali*, Giappichelli, Torino, 2014, p. 332. [Online]. Disponibile su: https://air.unimi.it/handle/2434/261152

[138] Corte di Giustizia, 4 luglio del 1963, causa 32/62.

[139] Corte di Giustizia, 31 marzo del 1992, causa C-255/90 P *Burban,* Racc. I-2253, par. 7 e 12.

[140] Corte di Giustizia, 12 luglio del 1957, cause riunite 7/56, da 3/57 a 7/57 *Algera*.

[141] Corte di Giustizia, 4 luglio 1963, causa 32/63*, Alvis* e Corte di Giustizia, 23 ottobre 1974, causa 17/74, *Transocean Marine Paint Association*.

[142] Corte di Giustizia, 15 marzo 1984, causa 64/82, *Tradax Graanhandel BV*.

[143] PERFETTI L., *Il diritto ad una buona amministrazione, determinazione dell'interesse pubblico ed equità*, Riv. Ital. Dir. Pubbl. Comunitario-2010, 2010, par. 3. [Online]. Disponibile su: https://scholar.google.com/scholar?hl=it&as_sdt=0%2C5&q=il+diritto+ad+una+buona+amministrazione&oq=

[144] Corte di Giustizia, 13 luglio 1966, cause riunite 56 e 58/64, *Consten & Grundig* c. Commissione.

[145] Corte di Giustizia 13 luglio 1966, cause riunite 56 e 58/64, *Consten & Grundig* c. Commissione a Corte di Giustizia dalla sentenza 15 marzo 1984, causa 64/82, *Tradax Graanhandel* BV.

[146] PERFETTI L., *Il diritto ad una buona amministrazione, determinazione dell'interesse pubblico ed equità*, Riv. Ital. Dir. Pubbl. Comunitario-2010, 2010, par. 3. [Online]. Disponibile su: https://scholar.google.com/scholar?hl=it&as_sdt=0%2C5&q=il+diritto+ad+una+buona+amministrazione&oq=

residuale e quindi, finalizzato a colmare una lacuna normativa o ad integrare una normativa carente o ancora ad imporre un obbligo di comportamento alle istituzioni. Dall'inizio degli anni '90, si è registrata un'evoluzione nella giurisprudenza della Corte di Giustizia[147], che sancisce la possibilità, da parte del singolo, di invocare direttamente il principio di buona amministrazione nei confronti dell'ente procedente: se da un lato, in capo all'amministrazione sussistono degli obblighi, dall'altro, in capo ai destinatari, esistono dei diritti immediatamente azionabili[148]. Il principio, quindi, diviene regola e da subito, si collega con i principi di legalità e certezza del diritto[149].

Con l'entrata in vigore della Carta dei diritti fondamentali dell'Unione europea[150], il filone giurisprudenziale viene recepito all'interno dell'art. 41 che con il Trattato di Lisbona diviene giuridicamente vincolante. Il diritto enucleato all'interno della Carta si caratterizza per elasticità ed ampiezza adattandosi per riassumere le interpretazioni fornite dalla dottrina e dalla giurisprudenza riguardo alle diverse rivendicazioni dei soggetti privati nei confronti dell'amministrazione pubblica[151]. Inoltre, i suoi contenuti sono stati esplicati e integrati dal Codice europeo di buona condotta amministrativa, approvato nel 2001 dal Parlamento, nonché dai Principi del servizio pubblico[152], pubblicati nel 2012 dal Mediatore europeo che, pur non essendo vincolanti, fungono da guida nella lettura della norma. Prima di procedere all'analisi della fattispecie, è necessario soffermarsi sull'ambito soggettivo e materiale di applicazione della disposizione in commento. Per quanto riguarda la sua portata soggettiva - passiva, sebbene essa possa apparire a prima

---

[147] Tribunale UE del 17 dicembre 1991, causa T-7/89, *SA Hercules Chemicals NV* contro Commissione delle Comunità europee.

[148] PERFETTI L., *Il diritto ad una buona amministrazione, determinazione dell'interesse pubblico ed equità*, Riv. Ital. Dir. Pubbl. Comunitario-2010, par. 3, nota 42. [Online]. Disponibile su: https://scholar.google.com/scholar?hl=it&as_sdt=0%2C5&q=il+diritto+ad+una+buona+amministrazione&oq=

[149] Tribunale UE, 25 marzo 1999, causa T-37/97, *Forges de Clabecq*, Corte di Giustizia, 16 gennaio 2003, causa C-205/01, Paesi Bassi.

[150] La Carta dei diritti fondamentali dell'Unione europea è stata proclamata, la prima volta, dal Parlamento europeo, dal Consiglio e dalla Commissione, a Nizza, il 7 dicembre 2000. Successivamente, dopo alcune modifiche, è stata proclamata, una seconda volta, a Strasburgo, il 12 dicembre 2007.

[151] CELONE C., "*Il nuovo rapporto tra cittadino e pubblica amministrazione alla luce dell'art. 41 della Carta dei diritti fondamentali dell'unione europea*", in Editoriale Scientifica Napoli a cura di Astone F. *et al*, 2017, p. 440. [Online]. Disponibile su: https://iris.unipa.it/retrieve/e3ad891b-7085-da0e-e053-3705fe0a2b96/Art%2041%20Carta%20dei%20diritti%20fondamentali%20dell%27Unione%20europea.pdf

[152] I Principi sono stati pubblicati al fine «*aiutare i funzionari a comprendere e ad applicare le norme in maniera corretta nonché orientarli verso la decisione giusta laddove siano chiamati a operare in base al proprio giudizio*». Essi sono: impegno verso l'Unione europea e i suoi cittadini, integrità, obiettività, rispetto per gli altri, trasparenza. Cfr. Mediatore europeo, *Principi del servizio pubblico per i funzionari dell'Unione*, 2012.

vista chiara[153], ha innescato un acceso dibattito giurisprudenziale sul se fosse applicabile anche ai casi in cui, ad avviare un procedimento amministrativo, fosse stata l'amministrazione di uno Stato membro. In relazione a questa fattispecie bisogna distinguere il caso di questione interna da quello di amministrazione comunitaria indiretta[154]. Nel primo caso, affrontato con la sentenza Cicala, la Corte ha escluso, in principio, l'applicazione, mentre nel secondo, con la sentenza *M.*[155], riguardante un caso di una domanda di protezione sussidiaria da parte di un richiedente asilo[156], la Corte, dopo aver ricordato che «*Il paragrafo 2 del citato articolo 41 prevede che tale diritto a una buona amministrazione comporta, in particolare, il diritto di ogni individuo di essere ascoltato prima che nei suoi confronti venga adottato un provvedimento individuale lesivo, il diritto di ogni individuo di accedere al fascicolo che lo riguarda, nel rispetto dei legittimi interessi della riservatezza e del segreto professionale, nonché l'obbligo per l'amministrazione di motivare le proprie decisioni*», ha affermato che «*come emerge dalla sua stessa formulazione, tale disposizione è di applicazione generale*». Tuttavia, dal 2014 in poi, con il caso *Y.S.* [157] e *Mukarubega*[158], ha affermato espressamente che dall'interpretazione dell'art. 41 comma 1 emerge l'intenzione del legislatore di rivolgersi unicamente alle istituzioni, agli organi e agli organismi dell'Unione, e non agli Stati membri. Nella sentenza *WebMindLicenses*[159] del 2015, però, ritorna in parte sui suoi passi affermando che: «*il rispetto dei diritti della difesa costituisce un principio generale del diritto dell'Unione (...)(che) incombe sulle amministrazioni degli Stati membri ogniqualvolta esse adottano decisioni che rientrano nella sfera d'applicazione del diritto dell'Unione, quand'anche la normativa dell'Unione applicabile non preveda espressamente siffatta formalità*». Quindi, conclude affermando l'applicazione ai casi di amministrazione comunitaria indirettta.

Discorso diverso, invece, con riferimento all'ambito materiale di applicazione, ove la tutela assume una portata diversa a seconda se "la buona amministrazione" sia intesa come diritto fondamentale (di cui all'art. 41 della Carta) o come principio generale

[153] L'art. 41, comma 1 della CDUE fa riferimenti solo alle istituzioni, organi e organismi dell'Unione.
[154] L'amministrazione nazionale esercita un'attività per il perseguimento di finalità per le quali è stato effettuato a livello sovranazionale il conferimento di un potere.
[155] Corte di Giustizia, 22 novembre 2012, causa C-277/11 – *M.*
[156] Una tipica ipotesi di amministrazione comunitaria indiretta.
[157] Corte di Giustizia, 17 luglio 2014, in cause riun. C-141/12 e C-372/12, *Y.S.*
[158] Corte di Giustizia, 5 novembre 2014, in causa C-166/13, *Mukarubega*.
[159] Corte di Giustizia, 17 dicembre 2015, in causa C-419/14, *WebMindLicenses*.

dell'ordinamento dell'Unione europea (come inteso dai Tribunali Ue)[160]. La giurisprudenza più recente sul punto è rappresentata dai casi *N*[161] e *Ispas*[162] le cui decisioni attengono indirettamente anche alla questione dell'ambito soggettivo di applicazione. Nel caso *N.* la Corte ha statuito che: «*il diritto a una buona amministrazione, sancito all'articolo 41 della Carta (...) riflette un principio generale di diritto dell'Unione*»; «*sicché (...) poiché nella causa di cui al procedimento principale uno Stato membro applica il diritto dell'Unione*». Quindi, se si considera la buona amministrazione, non come diritto ma come principio generale dell'unione, nei casi di amministrazione indiretta, essa sarà ugualmente tutelata, ma con notevoli ricadute pratiche in termini di grado di protezione del destinatario[163]. Secondo l'avvocato generale *Bobek*, nelle conclusioni durante la causa *Ispas*[164], il rischio di una differenziazione nel trattamento, a seconda se alla fattispecie si applichi l'art. 41 o meno, è alto, atteso che secondo il legale il contenuto del principio generale «*con riferimento all'applicazione del diritto dell'Unione da parte degli Stati membri può differire dalle garanzie (specifiche e autonome) previste all'articolo 41 della Carta, applicabili all'amministrazione diretta dell'Unione*». Infatti, avendo il diritto portata costituzionale ed essendo previsto in una Carta giuridicamente vincolante, le sue garanzie potranno esser modificate solo attraverso una procedura di revisione, mentre, la portata del principio generale, come considerato dalla giurisprudenza, sarà sempre più incerta e indefinita offrendo un grado di protezione minore[165].

---

[160] HOFMANN CH., MIHAESCU B., "*The Relation between the Charter's Fundamental Rights and the Unwritten General Principles of EU Law: Good Administration as the Test Case*", in 9 EU Constitutional Law Review 73, 2013, p. 88-96. [Online]. Disponibile su: https://www.researchgate.net/publication/259432820_The_Relation_between_the_Charter's_Fundamental_Rights_and_the_Unwritten_General_Principles_of_EU_Law_Good_Administration_as_the_Test_Case

[161] Corte di Giustizia, 8 maggio 2014, in causa C-604/12, *H.N.*

[162] Corte di Giustizia, 9 settembre 2017, in causa C-298/16, *Ispas*.

[163] Tuttavia, in tale caso, secondo la Corte vi sarebbe una coincidenza totale in termini di ampiezza della tutela tra il diritto alla buona amministrazione *ex* art. 41 CDUE e il principio generale della buona amministrazione. A tal riguardo si veda l'interpretazione sul punto di: GALETTA D.U., "*Il diritto ad una buona amministrazione nei procedimenti amministrativi oggi (anche alla luce delle discussioni sull'ambito di applicazione dell'art. 41 della Carta dei diritti UE)*", in M.C. Pierro (a cura di), *Il diritto a una buona amministrazione nei procedimenti tributari*, Giuffré Francis Lefebvre, Milano, 2019, p. 24.

[164] Nel caso *Ispas* la Corte sulla scia di quanto detto ha affermato che il principio della buona amministrazione quale rispettoso dei diritti alla difesa non ha una valenza assoluta ma può esser limitata in caso di obiettivi di interesse generale sempre che non costituiscano una limitazione sproporzionata e inaccettabile. Si veda il punto 35 della sentenza.

[165] GALETTA D.U., "*Il diritto ad una buona amministrazione nei procedimenti amministrativi oggi (anche alla luce delle discussioni sull'ambito di applicazione dell'art. 41 della Carta dei diritti UE)*", M.C. Pierro (a cura di), *Il diritto a una buona amministrazione nei procedimenti tributari*, Giuffré Francis Lefebvre,

L'analisi ricognitiva dell'ambito soggettivo e materiale di applicazione risulta funzionale al fine di comprendere se i destinatari dei procedimenti amministrativi, automatizzati dall'IA, avviati dalle autorità di vigilanza nazionale siano titolari dei diritti di cui all'art. 41.

Alla luce di quanto sancito dalla giurisprudenza precedentemente citata, l'interpretazione letterale individua come soggetti passivi le istituzioni europee, non ricomprendono le autorità di vigilanza, come la Banca d'Italia che sono autorità degli Stati membri. Tuttavia, essendo il MVU un sistema unitario caratterizzato da un decentramento amministrativo[166], più che un modello di coamministrazione[167] o di amministrazione comunitaria indiretta, la questione sembra esser irrisolta. La giurisprudenza comunitaria, infatti, si è espressa sui casi di amministrazione indiretta[168] dove è netta la separazione fra istituzioni europee e amministrazioni nazionali, invece, nell'ambio della vigilanza bancaria la linea di demarcazione non è altrettanto definita. La BCE può, infatti, avocare a sé la competenza anche nei casi in cui è delle autorità nazionali, mente in altri casi, come quello relativo all'autorizzazione all'esercizio dell'attività bancaria, la procedura prevede il coinvolgimento di entrambe le autorità. Per fare un esempio, appare evidente che se si sostenesse la non applicabilità alla Banca d'Italia dell'art. 41 CDUE ma del principio generale (in quanto, comunque, applica il diritto dell'Unione e persegue finalità unionali) si potrebbe arrivare al paradosso di permettere l'applicazione di determinate tecnologie IA all'autorità nazionale nella formulazione della proposta di autorizzazione all'attività bancaria e precludere l'utilizzo delle stesse in fase di rilascio da parte della BCE, in quanto, incompatibili con la più ampia e definita tutela offerta dalla norma.

Per l'Italia, il *vulnus* sarebbe, comunque, coperto dall'art. 97 Cost. in quanto stabilendo che «*i pubblici uffici sono organizzati secondo disposizioni di legge, in modo che siano assicurati il buon andamento e l'imparzialità dell'amministrazione*» sancisce il principio

---

Milano, 2019, p. 24. [Online]. Disponibile su: https://air.unimi.it/retrieve/dfa8b9a1-d298-748b-e053-3a05fe0a3a96/Saggio2019VolTributaristiOpenAccess.pdf

[166] Si veda il par. 2.1.

[167] «*La coamministrazione, intesa come modalità di esercizio di una funzione, si caratterizza, dunque, per la circostanza che una funzione unitaria viene attribuita a soggetti distinti che operano in stretta connessione tra di loro e sulla base di un rapporto di necessarietà, poiché l'attività dell'uno è essenziale per l'attività dell'altro*». Si veda FRATICCELLI C., "*L'integrazione amministrativa europea nel settore delle telecomunicazioni"*, Università degli Studi Roma Tre facoltà di giurisprudenza, 2008, p. 21. [Online]. Disponibile: https://opac.bncf.firenze.sbn.it/Record/TD10016328

[168] L'amministrazione indiretta garantisce comunque l'indipendenza delle amministrazioni nazionali da quelle comunitarie. Si veda FRATICCELLI C., "*L'integrazione amministrativa europea nel settore delle telecomunicazioni*", Università degli Studi Roma Tre facoltà di giurisprudenza, 2008, p. 14.

di legalità, da cui discendono la tipicità, l'obbligo di motivazione, il principio di imparzialità e di buon andamento e dalla legge n. 241/1990[169] per quanto riguarda il diritto di accesso ai documenti amministrativi[170] e al contraddittorio attraverso la possibilità di presentare memorie scritte[171].

Analizzato il contesto giuridico in cui è stato introdotto e poi reso vincolante l'art. 41, nonché, l'ambito di applicazione della fattispecie e le annesse conseguenze derivanti da una sua applicazione, si procederà ad un'illustrazione del contenuto dei vari diritti specifici. Sarà importante verificare se la BCE impiegherà l'IA nel rispetto della normativa consentendo ai soggetti regolamentati e ad altri interessati di esercitare i loro diritti a una gestione adeguata, compresa la possibilità di ottenere il riesame delle decisioni della BCE e l'assunzione di responsabilità da parte di quest'ultima[172].

4.2.1. Il diritto all'imparzialità, equità e ragionevole durata delle questioni trattate

L'assenza di una vera e propria disciplina sul procedimento amministrativo rende essenziale sia la previsione dell'art. 41 all'interno dell'ordinamento europeo sia necessario indagare specificamente su ciascuno dei diritti procedimentali ivi enucleati[173]. In questo senso il Codice della buona amministrazione, sebbene non sia uno strumento giuridicamente vincolate, ha tra le finalità quella di specificare il contenuto dei vari diritti previsti. Tuttavia, la giurisprudenza comunitaria rimane la fonte principale per indagare sul significato delle varie garanzie.

Il primo comma dell'art. 41 CDUE recita: «*Ogni persona ha diritto a che le questioni che la riguardano siano trattate in modo imparziale ed equo ed entro un termine ragionevole dalle istituzioni, organi e organismi dell'Unione*».

---

[169] Nello svolgimento della propria attività amministrativa la Banca d'Italia applica la disciplina sul procedimento amministrativo e sull'accesso ai documenti amministrativi di cui alla legge n. 241 del 7 agosto 1990 e s.m.i..

[170] Art. 10, comma 1, lett. a) della l. n. 241/1990.

[171] Art. 10, comma 1, lett. b) della l. n. 241/1990.

[172] RINGE W.G. *et al.*, *Navigating the Legal Landscape of AI-Enhanced Banking Supervision: Protecting EU Fundamental Rights and Ensuring Good Administration,* European Banking Institute Working Paper Series 2023 - no. 140, 2023, pp. 33-34.

[173] PROVENZANO P, *Procedimento amministrativo e diritto ad una buona amministrazione*, in D.U. Galetta (a cura di), *Diritto amministrativo nell'unione europea: argomenti e materiali*, Giappichelli, Torino, 2014, par. 3. [Online]. Disponibile su: https://air.unimi.it/handle/2434/261152

Appare evidente la previsione di un obbligo generale, nel caso specifico, in capo alla BCE, di diligenza volto a regolare l'esercizio dell'attività di vigilanza in modo imparziale, equo ed in tempi ragionevoli.

In ordine all'obbligo d'imparzialità, la giurisprudenza comunitaria consolidata ha affermato che una decisione imparziale e rispettosa del principio di buona amministrazione prende in considerazione «*tutti gli elementi di fatto e di diritto disponibili al momento dell'adozione dell'atto*», poiché sussiste l'obbligo di assumere la decisione «*con tutta la diligenza richiesta e di adottarla prendendo a fondamento tutti i dati idonei ad incidere sul risultato*»[174] [175]. All'interno del Codice europeo di buona condotta amministrativa, all'art. 8, l'imparzialità viene declinata come regola di comportamento del funzionario responsabile del procedimento che deve astenersi «*da qualsiasi azione arbitraria che abbia effetti negativi su membri del pubblico, nonché da qualsiasi trattamento preferenziale quali che ne siano i motivi*»[176]. Il comma 2 sancisce, poi, il principio di indipendenza strettamente correlato a quello dell'imparzialità, vietando che il funzionario agisca al fine di perseguire interessi personali, familiari o nazionali o che dipenda da pressioni politiche.

Parimenti sancito dal comma 1 dell'art. 41, il diritto a che le questioni vengano «*trattate in modo equo*». La dottrina si è soffermata sulla portata di tale diritto giungendo, dalle stesse premesse, a conclusioni diverse. Nel diritto amministrativo italiano l'equità può esser intesa in due accezioni diverse: sostanziale e procedurale. Secondo una parte della dottrina[177] l'art. 41, comma 1, si riferirebbe all'equità procedurale poiché essa implica, per potersi realizzare, che l'amministrazione procedente riconosca al destinatario tutte le garanzie di cui al comma 2 come il contradditorio, l'accesso al fascicolo, la motivazione delle decisioni etc. In particolare, questo orientamento troverebbe conferma in una sentenza della Corte di Giustizia che ha affermato che, qualora la Commissione,

---

[174] Tribunale UE, 19 marzo 1997, in causa T-73/95, *Oliveira* c. Commissione, punto 32; Tribunale UE, 9 luglio 1999, in causa T-231/97, *New Europe Consulting* e a. c. Commissione, punto 41.

[175] GALETTA D.U., *Il diritto ad una buona amministrazione nei procedimenti amministrativi oggi (anche alla luce delle discussioni sull'ambito di applicazione dell'art. 41 della Carta dei diritti UE)*, M.C. Pierro (a cura di), *Il diritto a una buona amministrazione nei procedimenti tributari*, Giuffré Francis Lefebvre, Milano, 2019, p. 3.

[176] Art. 8, comma 1 del Codice europeo di buona condotta amministrativa.

[177] GALETTA D.U., *Il diritto ad una buona amministrazione nei procedimenti amministrativi oggi (anche alla luce delle discussioni sull'ambito di applicazione dell'art. 41 della Carta dei diritti UE)*, M.C. Pierro (a cura di), *Il diritto a una buona amministrazione nei procedimenti tributari*, Giuffré Francis Lefebvre, Milano, 2019, p. 4.

nell'ambito della procedura di autorizzazione alla concentrazione, si avvalga di modelli econometrici dovrà mettere le parti in condizione di far conoscere le proprie osservazioni a riguardo, in quanto la divulgazione di questi modelli e le modalità con cui sono stati elaborati contribuiscono a conferire al procedimento carattere equo[178].

Secondo un'altra parte della dottrina[179], farebbe riferimento all' «*equità proporzionale nel senso che la decisione può dirsi equa quando è, per così dire, "misurata" ossia appare idonea, necessaria ed adeguata rispetto alle esigenze di cura dell'interesse pubblico assicurando nel contempo il minor sacrificio possibile dell'interesse privato*». Il concetto di equità proporzionale o sostanziale è connesso ai concetti di giustizia e proporzionalità dell'azione amministrativa, inteso come «*come regola che impone all'azione amministrativa di scendere sul terreno della parità, del dialogo con il privato, del consenso e dell'accordo di natura privatistica con il medesimo, tutte le volte che ciò sia possibile relegando l'esercizio del potere in una zona residuale*»[180]

Tutelato, altresì il diritto alla ragionevole durata del procedimento intesa come obbligo, in capo dell'amministrazione procedente, nell'ambito di procedimenti che possono condurre all'adozione di una misura che incida negativamente su uno o più interessi del destinatario, di assumere una decisione definitiva da emanare entro un termine ragionevole che decorre dalla ricezione delle osservazioni del denunciante[181].

Prima della Carta, la giurisprudenza comunitaria lo aveva già riconosciuto come principio generale del diritto comunitario[182], in quanto strettamente collegato al principio della certezza del diritto e forse, più di altri, la massima espressione del diritto ad una buona amministrazione[183]. Non a caso, anche la giurisprudenza nelle sue prime pronunce ha avuto modo di affermare che: «*un'amministrazione lenta è una cattiva amministrazione*» e che è necessario evitare ritardi ingiustificati garantendo che ciascuna fase del procedimento venga conclusa in un termine ragionevole[184]. La principale caratteristica di

---

[178] Corte di Giustizia, 16 gennaio 2019, in causa C-265/17 P, *United Parcel Service*, punto 33 s.
[179] ZITO A., *Il «diritto ad una buona amministrazione» nella Carta dei diritti fondamentali dell'Unione europea e nell'ordinamento interno*, in Riv. Ital. Dir. Pubbl. Comunitario – 2002, 435.
[180] Ibidem.
[181] Corte di Giustizia, 28 marzo 1997, in causa C-282/95P, *Guerin*, punto 37.
[182] Corte di Giustizia, 28 marzo 1997, in causa C-282/95P, *Guerin*, punto 37; Tribunale UE, 22 ottobre 1997, in cause riun. T-213/95 e T-18/96, *SCK* e *FNK*, punto 55 ss.; Tribunale UE, 7 ottobre 1999, in causa T-228/97, *Irish Sugar*, punto 276.
[183] PERFETTI L., *Diritto ad una buona amministrazione, determinazione dell'interesse pubblico ed equità*, in, Riv. Ital. Dir. Pubbl. Comunitario-2010, 2010, p. 796 ss.
[184] Così l'Avv. gen. *Jacobs*, nelle sue conclusioni del 22 marzo 2001, in causa C-270/99, Z, punto 40.

questo principio è la sua indeterminatezza su quali siano le modalità per determinare quale sia l'entità di un termine ragionevole per un determinato procedimento o per una fase dello stesso. Per questo motivo. la priorità della giurisprudenza comunitaria è stata di riempire il contenuto di questo principio affermando che risulta doveroso prevedere termini precisi di conclusione dei procedimenti nei casi in cui sia in gioco anche la certezza del diritto e non solo la "buona amministrazione"[185]. Ha sottolineato, infatti, che «(...) *la durata ragionevole del procedimento amministrativo si valuta sulla scorta delle circostanze specifiche di ciascuna pratica e, in particolare, del contesto della stessa, delle varie fasi procedurali espletate dalla Commissione, della condotta delle parti nel corso del procedimento, della complessità della pratica, nonché degli interessi delle parti nella contesa*»[186] [187]. A ben vedere l'obiettivo è di tutelare gli operatori da «*un'incertezza giuridica protratta*»[188] che può comportare numerose conseguenze negative, soprattutto, in un sistema sensibile come quello bancario. La violazione del diritto ad una ragionevole durata del procedimento non determina, però, il diritto ad ottenere l'annullamento del provvedimento. Infatti, secondo il Tribunale Ue: «(...) *qualora la violazione del termine ragionevole non incida sull'esito del procedimento, una simile violazione può condurre il Tribunale, nell'esercizio della sua competenza estesa al merito, a correggere adeguatamente la violazione che risulta dal superamento del termine ragionevole del procedimento amministrativo mediante l'eventuale riduzione dell'importo dell'ammenda inflitta*»[189].

L'annullamento del provvedimento si avrà, invece, nel caso in cui i termini del procedimento abbiano carattere perentorio ma ciò, attiene a profili differenti rispetto alla generale previsione della ragionevole durata del procedimento.

---

[185] Sentenza in tema di controllo preventivo in materia di aiuti di Stato, Corte di Giustizia, 11 dicembre 1973, in causa 120-73, *Lorenz*, punto 4 ss.

[186] Tribunale UE, 22 ottobre 1997, in cause riun. T-213/95 e T-18/96, cit., punto 57. V. anche Tribunale UE, 19 marzo 1997, in causa T-73/95, cit.; Tribunale UE, 14 luglio 1997, in causa T-81/95, *Interhotel*.

[187] GALETTA D.U., *Il diritto ad una buona amministrazione nei procedimenti amministrativi oggi (anche alla luce delle discussioni sull'ambito di applicazione dell'art. 41 della Carta dei diritti UE)*, in M.C. Pierro (a cura di), *Il diritto a una buona amministrazione nei procedimenti tributari*, Giuffré Francis Lefebvre, Milano, 2019, p. 6.

[188] Avv. Gen. *Mischo*, nelle sue conclusioni del 25 ottobre 2001, in causa C-244/99P, DSM, punto 83 ss.

[189] Tribunale UE, 15 luglio 2015, in cause riun. T-413/10 e T-414/10, *Socitrel*, punto 155.

4.2.2. Il diritto di esser ascoltati

L'art. 41, al comma 2, nell'elencare i diritti "particolari" che discendono dal generale diritto ad una buona amministrazione, sancisce, in *primis*, il diritto di ogni persona di essere ascoltata prima che nei suoi confronti venga adottato un provvedimento individuale che le rechi pregiudizio. Esso costituisce, oltre che un corollario del diritto ad una buona amministrazione, il principale corollario del diritto alla difesa in quanto permette al destinatario di un eventuale provvedimento di fornire una propria rappresentazione dei fatti che concorrerà, assieme ad altri elementi raccolti dall'amministrazione, alla formazione della volontà decisionale. L'affermazione, prima ancora che come diritto, quale principio generale applicabile anche laddove non specificamente previsto[190], è stata compiuta dalla giurisprudenza comunitaria[191] già prima dell'entrata in vigore della Carta, in quanto oggetto di numerose disposizioni UE contenute in vari regolamenti[192].

Attualmente, con il Trattato di Lisbona, il diritto ha trovato due fondamenti normativi nel diritto primario: l'art. 41 della CDUE e implicitamente l'art. 15 TFUE. Laddove è previsto che «*al fine di promuove il buon governo e garantire la partecipazione della società civile, le istituzioni, gli organi e gli organismi dell'Unione operano nel modo più trasparente possibile*». La trasparenza dell'azione amministrativa sarà data, anche e soprattutto, dal grado di partecipazione dei destinatari dei suoi effetti[193]. Continuando

---

[190] Secondo la giurisprudenza comunitaria: «*il rispetto del diritto alla difesa in qualsiasi procedimento promosso nei confronti di una persona e che possa sfociare in un atto per essa lesivo costituisce un principio fondamentale del diritto comunitario e dev'essere garantito anche in mancanza di qualsiasi norma riguardante il procedimento di cui trattasi*». Corte di Giustizia., 29 giugno 1994, in causa C-135/92, *Fiskano* c. Commissione, punto 39.

[191] *Ex multis*: Corte di Giustizia, 18 dicembre 2008, in causa C-349/07*, Sopropé*, punto 36 ss.; Corte di Giustizia, 22 novembre 2012, in causa C-277/11, M., punto 81 ss.; Corte di Giustizia, 3 luglio 2014, in causa C-129/13, *Kamino International Logistics*, punto 28 ss.; Corte di Giustizia, 5 novembre 2014, in causa C-166/13, *Mukarubega*, punto 42 ss.

[192] Si vedano, ad es., l'art. 19 del Regolamento n. 17, in GUCE, n. L 13 del 21 febbraio 1962, p. 204 ss. (210), nonché il Regolamento 2842/98/CE del 22 dicembre 1998, che statuisce il diritto di essere ascoltati nel contesto di specifici procedimenti ex artt. 85 e 86 CE, in GUCE, n. L 354 del 30 dicembre 1998, p. 18. L'art. 18 del Regolamento 4064/89/ CEE, relativo ai procedimenti di controllo sulle fusioni, in collegamento con il Regolamento 447/98/CE del 1° marzo 1998, in GUCE, n. L 61 del 2 marzo 1998, p. 1 ss.; l'art. 11 del Regolamento 2026/97/CE, in GUCE, n. L 288 del 21 ottobre 1997, p. 1 ss. (12), relativo all'audizione nel contesto dei procedimenti antidumping. Esempi tratti dalla nota n. 32 in GALETTA D.U., *Il diritto ad una buona amministrazione nei procedimenti amministrativi oggi (anche alla luce delle discussioni sull'ambito di applicazione dell'art. 41 della Carta dei diritti UE)*, in M.C. Pierro (a cura di), *Il diritto a una buona amministrazione nei procedimenti tributari*, Giuffré Francis Lefebvre, Milano, 2019.

[193] PROVENZANO P, *Procedimento amministrativo e diritto ad una buona amministrazione*, in D.U. Galetta (a cura di), *Diritto amministrativo nell'unione europea: argomenti e materiali*, Giappichelli, Torino, 2014, par. 3.2.

l'analisi dell'art. 41, un'interpretazione letterale della disposizione sembrerebbe tutelare solo ed esclusivamente la posizione del destinatario del procedimento qualora il provvedimento finale sia volto ad incidere negativamente sulla situazione giuridica soggettiva[194], cioè, ove esso abbia un interesse oppositivo, escludendo i casi di provvedimenti ampliativi. La sopracitata interpretazione non ha, però, convinto i più[195], in quanto anche i provvedimenti avviati su istanza di parte potrebbero concludersi in senso negativo, causando un pregiudizio all'interessato; si pensi, ad esempio, al caso del rigetto della richiesta di autorizzazione all'esercizio dell'attività bancaria.

Tuttavia, sempre attorno all'ambito di estensione della tutela, la giurisprudenza comunitaria ha affermato che il diritto ad esser ascoltati può esser limitato, o in alcuni casi escluso, in ragione della natura del provvedimento, del tipo di potere esercitato o di particolari esigenze alla base. In passato, la Corte in relazione alla natura del provvedimento non ha riconosciuto il diritto alla difesa, inteso come diritto ad esser ascoltati, in quanto la decisione impugnata non pregiudicava le prerogative dell'interessato[196]. Nei casi relativi al tipo di potere esercitato, la giurisprudenza ha attribuito maggiore peso e spazio alle garanzie procedimentali all'aumentare della discrezionalità del potere[197]. Per quanto riguarda le esigenze alla base del provvedimento, è possibile che la restrizione del diritto possa dipendere da esigenze cautelari, ovvero, quando la partecipazione dell'interessato potrebbe far venir meno l'esigenza che ha spinto l'amministrazione ad avviare un procedimento, laddove sia necessario mantenere la segretezza per scongiurare l'occultamento o la distruzione delle prove[198]. In questi casi, non si tratta di un'"abrogazione" del diritto ma di una posticipazione del suo esercizio.

È da dire, inoltre, che il diritto ad esser ascoltati non può prescindere dall'esercizio di altri due diritti che possono considerarsi "propedeutici", in quanto fondanti i presupposti per esercitare il diritto in questione: il diritto ad esser informati dell'avvio di un procedimento e il diritto di accedere al fascicolo. Al primo, corrisponde un dovere, in capo all'amministrazione procedente, di informare il destinatario degli addebiti mossi nella

---

[194] Come, ad esempio, i provvedimenti sanzionatori.

[195] Su tutti: PROVENZANO P, *Procedimento amministrativo e diritto ad una buona amministrazione*, in D.U. Galetta (a cura di), *Diritto amministrativo nell'unione europea: argomenti e materiali*, Giappichelli, Torino, 2014, par. 3.2.

[196] Corte di Giustizia, 28 maggio 1980, C-33/79 e 75/79, *Ku¨hner* c. Commissione, punto 25.

[197] Corte di Giustizia, 21 novembre 1991, in causa C-269/90, cit., punto 14.

[198] Si vedano, su questo punto, le conclusioni dell'Avv. gen. *Warner* del 30 aprile 1980, in causa 136/79, *National Panasonic*.

comunicazione. A questo proposito, in un'occasione, in cui all'impresa non erano stati comunicati tutti i documenti alla base degli addebiti, il Tribunale Ue[199] ha legittimato il comportamento di un'impresa che «(...) *ha potuto giustamente ritenere ch'essi fossero irrilevanti ai fini del procedimento*», sicchè «*non informando un'impresa del fatto che taluni documenti sarebbero stati usati per la decisione, la Commissione ha impedito a quest'ultima di manifestare tempestivamente il proprio punto di vista circa il valore probante di tali documenti*» e ne è conseguito che i documenti stessi non potessero essere considerati validi mezzi di prova per la parte che la riguardava. Il secondo è funzionale al fine di esaminare gli elementi in possesso dell'autorità e garantire che il diritto di difesa si svolga su un piano paritario[200].

4.2.3. Il diritto di accesso al fascicolo

Un altro diritto procedurale, corollario del diritto di esser ascoltati, consiste nel «*diritto di ogni persona di accedere al fascicolo che la riguarda, nel rispetto dei legittimi interessi della riservatezza e del segreto professionale e commerciale*» e anch'esso, semplicemente, recepito dalla Carta in quanto già elaborato quale principio generale dalla giurisprudenza comunitaria[201]. Come affermato nel paragrafo precedente, il diritto di accesso al fascicolo è un diritto "propedeutico", in quanto, permette al destinatario del procedimento di valutare se le accuse mosse dall'amministrazione procedente sono fondate, valutando i documenti e più in generale, le prove raccolte. Infatti, qualunque sia l'istituzione a capo del procedimento, essa non potrà basare il provvedimento su mezzi di prova la cui parte non abbia avuto previamente accesso, così come affermato dalla sentenza *Solvay* del Tribunale UE nel 1995. In quella occasione, è stato statuito che il procedimento amministrativo deve svolgersi sul piano della parità delle armi in quanto: «*il Tribunale non può ammettere che la Commissione, pronunciandosi sull' infrazione, sia stata l'unica ad avere a disposizione i documenti (...) e abbia dunque potuto decidere da sola se utilizzarli o meno contro la ricorrente, mentre quest'ultima non aveva accesso a tali documenti e non ha dunque potuto decidere parallelamente se utilizzarli o meno*

[199] Tribunale UE, 10 marzo 1992, T-9/89, *Hu¨els AG* c. Commissione, ove al punto 38.
[200] Il diritto di accesso al fascicolo verrà trattato nello specifico nel par. 2.2.3.
[201] Tribunale UE, 18 dicembre 1992, in cause riun. 10, 11, 12 e 15/92, *Cimenteries CBR SA* c. Commissione, punto 38.

per la propria difesa»[202]. Il principio della parità delle armi, quindi, si traduce nel principio della parità delle informazioni tra le parti[203].

Dalla lettura dell'art., emerge che l'esercizio del diritto deve avvenire nel rispetto degli interessi della riservatezza, del segreto professionale e commerciale, concordemente a quanto sancito all'art. 339 TFUE: «*i membri delle istituzioni dell'Unione, i membri dei comitati e parimenti i funzionari e agenti dell'Unione sono tenuti (...) a non divulgare le informazioni che per loro natura siano protette dal segreto professionale e in particolare quelle relative alle imprese e riguardanti i loro rapporti commerciali ovvero gli elementi dei loro costi*». La limitazione, come affermato dalla giurisprudenza consolidata[204], non potrà esser assoluta, cioè, fino a precludere l'esercizio del diritto di accesso. Come ribadito dalla Corte di Giustizia: «(...) *spetta alle autorità o agli organi giurisdizionali competenti ricercare, alla luce delle circostanze di ciascun caso di specie, un equilibrio tra tali interessi contrapposti*»[205]. Un'ulteriore ipotesi in cui l'accesso potrà esser limitato o escluso riguarda il caso in cui questo rappresenti un rischio per le indagini in corso[206].

Il diritto di accesso al fascicolo non va confuso con il «*diritto di accedere ai documenti delle istituzioni, organi o organismi dell'Unione*», statuito dall'art. 42 CDUE. Il diritto di accesso ai documenti, a differenza del diritto endoprocedimentale di accesso al fascicolo, è un diritto esoprocedimentale, in quanto riconosciuto in via generale e indipendentemente da un procedimento riguardante l'interessato. Quest'ultimo, è, quindi, un corollario del principio di trasparenza nell'operato delle istituzioni[207], mentre il diritto di accesso al fascicolo è un corollario del diritto all'esser ascoltati[208].

---

[202] Tribunale UE, 29 giugno 1995, in causa T-30/91, *Solvay SA* c. Commissione, punto 83.

[203] GALETTA D.U., *Il diritto ad una buona amministrazione nei procedimenti amministrativi oggi (anche alla luce delle discussioni sull'ambito di applicazione dell'art. 41 della Carta dei diritti UE)*, in M.C. Pierro (a cura di), *Il diritto a una buona amministrazione nei procedimenti tributari*, Giuffré Francis Lefebvre, Milano, 2019, p. 13.

[204] Corte di Giustizia, 20 marzo 1985, in causa 264/82, *Timex Corporation* c. Consiglio, punto 29.

[205] Corte di Giustizia, 13 settembre 2018, in causa C-358/16, punto 70.

[206] GALETTA D.U., *Il diritto ad una buona amministrazione nei procedimenti amministrativi oggi (anche alla luce delle discussioni sull'ambito di applicazione dell'art. 41 della Carta dei diritti UE)*, in M.C. Pierro (a cura di), *Il diritto a una buona amministrazione nei procedimenti tributari*, Giuffré Francis Lefebvre, Milano, 2019, p. 14.

[207] Art. 15 TFUE.

[208] PROVENZANO P, *Procedimento amministrativo e diritto ad una buona amministrazione*, in D.U. Galetta (a cura di), *Diritto amministrativo nell'unione europea: argomenti e materiali*, Giappichelli, Torino, 2014, par. 3.3.

4.2.4. Il diritto ad una decisione motivata

Il diritto a una decisione motivata è enucleato all'interno dell'art. 41 quale «*obbligo per l'amministrazione di motivare le proprie decisioni*» e all'interno dell'art. 296, comma 2 del TFUE che statuisce, più generalmente, che «*gli atti giuridici sono motivati*». La previsione di un obbligo di motivazione, in capo alle istituzioni dell'Unione europea, è considerata, in primo luogo, un «*elemento essenziale*»[209] per garantire l'esercizio del diritto di difesa, in sede giudiziale, ma anche per il rispetto dell'art. 15 TFUE, nella misura in cui la motivazione assurge, anche, a strumento di controllo delle istituzioni da parte dei cittadini dell'Unione[210]. Nonostante tale obbligo sia stato previsto in più norme del diritto primario, il legislatore non ha dettato i criteri da seguire per redigere una motivazione esaustiva.

La Corte di Giustizia è intervenuta per colmare la lacuna normativa, anche prima delle previsioni sopracitate, affermando che nella motivazione debbano risultare: «*gli accertamenti di fatto nonché le valutazioni giuridiche su cui le decisioni poggiano. Essa deve indicare le considerazioni su cui la decisione si fonda in modo da consentire che su di esse si eserciti il controllo giurisdizionale. Non è tuttavia prescritto che nella motivazione siano enunciate tutte le obiezioni che contro la decisione sarebbe possibile fare*»[211]. Come osservato in dottrina[212], sarà considerata sufficiente una motivazione, anche non molto lunga, in grado di far comprendere al destinatario le ragioni che hanno portato a prendere una data decisione, senza che sia «*necessario che la motivazione specifichi tutti i vari aspetti di fatto o di diritto pertinenti*»[213]. D'altro canto, una motivazione molto lunga ma apparente, cioè, carente sul piano qualitativo determinerà l'illegittimità della decisione[214].

---

[209] Corte di Giustizia, 10 dicembre 1957, 1/57 e 14/57, *Société des usines à tubes de la Sarre* c. l'Alta Autorità della Comunità europea del Carbone e dell'Acciaio. Corte di Giustizia, 17 novembre 1987, in cause riun. 142 e 156/84, *British American Tobacco Co. Ltd* c. Commissione, punto 72.

[210] PROVENZANO P, *Procedimento amministrativo e diritto ad una buona amministrazione*, in D.U. Galetta (a cura di), *Diritto amministrativo nell'unione europea argomenti e materiali*, Giappichelli, Torino, 2014, par. 3.4.

[211] Corte di Giustizia, 20 marzo 1957, in causa 2/56, *Die in der "Geitling" Ruhrkohlen-Verkaufsgesellschaft mbH zusammengeschlossenen Bergwerksgesellschaften* c. Alta Autorità, p. 35 ss.

[212] PERFETTI L., *Diritto ad una buona amministrazione, determinazione dell'interesse pubblico ed equità*, in, Riv. Ital. Dir. Pubbl. Comunitario - 2010, 2010, p. 801.

[213] Corte di Giustizia, 26 giugno 1986, in causa 203/85, *Nicolet Instrument* c. *Hauptzollamt Frankfurt*, punto 10.

[214] Corte di Giustizia, 20 marzo 1959, in causa 18/57, I. *Nolde* c. Alta Autorità, p. 115: «(...) la motivazione (...) non indica in modo soddisfacente ed adeguato — nemmeno per richiamo alle decisioni del 1956 — le considerazioni di fatto e di diritto sulle quali dette decisioni, ora impugnate, si fondano; essa non consente

Per quanto riguarda l'ampiezza e l'analiticità della motivazione questa dipenderà dalle circostanze del caso[215], dalla natura dell'atto[216], dal complesso di norme giuridiche che disciplinano la materia[217] e dal contesto in cui è stata adottata[218] [219]. In relazione alla natura dell'atto, la motivazione dovrà esser più analitica nei casi in cui il potere esercitato alla base è discrezionale. Un esempio, è quello della BCE che, data la rarità dei casi in cui il potere è interamente vincolato[220], ha ampia discrezionalità nell'esercizio delle funzioni di vigilanza e quindi, dovrà dimostrare nella motivazione, che ha preso in considerazione, in modo imparziale, tutti i fattori rilevanti, rispettando tutte le regole procedurali previste. La motivazione diviene ancor più essenziale, non tanto per poter contestare le valutazioni discrezionali, ma per garantire adeguati livelli di trasparenza nel procedimento decisionale[221].

4.2.5. Le limitazioni al diritto ad una buona amministrazione derivanti dall'ipotetico impiego dell'*AI-Driven*

In questo paragrafo, si illustreranno le questioni giuridiche che solleva l'automazione del procedimento amministrativo derivanti, a loro volta, dalle limitazioni tecniche dei sistemi di IA. Infatti, nella maggior parte dei casi, i motivi di attrito derivano da aspetti legati al funzionamento dell'algoritmo che, talvolta, ostacolano l'esercizio dei diritti fondamentali.

Come ampiamente spiegato nel par. 2.1., i sistemi di ML apprendono o migliorano la loro azione attraverso il *training* su un *set* di dati riguardanti situazioni analoghe o simili a quelle in cui vengono impiegati. Per questo motivo, quest'ultimi, si basano sulla correlazione piuttosto che sulla causalità su cui, invece, si basa una qualunque attività di

perciò il controllo giurisdizionale della Corte». Nota tratta da GALETTA D.U., *Il diritto ad una buona amministrazione nei procedimenti amministrativi oggi (anche alla luce delle discussioni sull'ambito di applicazione dell'art. 41 della Carta dei diritti UE)*, in M.C. Pierro (a cura di), *Il diritto a una buona amministrazione nei procedimenti tributari*, Giuffré Francis Lefebvre, Milano, 2019, n.75.

[215] Tribunale UE, 12 settembre 2006, T-155/04, *Selex Sistemi integrati* c. Commissione.

[216] Tribunale UE, 7 novembre 2002, T-141/99, T-142/99, T-150/99 e T-151/99, *Vela s.r.l.* c. Commissione.

[217] Corte di Giustizia, 10 luglio 2019, C-39/18 P, Commissione c. *NEX International Limited* e altri.

[218] Tribunale UE, 9 luglio 2008, T-301/01, *Alitalia* e altri c. Commissione.

[219] PROVENZANO P, *Procedimento amministrativo e diritto ad una buona amministrazione*, in D.U. Galetta (a cura di), *Diritto amministrativo nell'unione europea: argomenti e materiali*, Giappichelli, Torino, 2014, par. 3.4.

[220] In quanto i parametri normativi che circoscrivono l'operato dell'autorità non sono stringenti.

[221] RINGE W.G. *et al*., *Navigating the Legal Landscape of AI-Enhanced Banking Supervision: Protecting EU Fundamental Rights and Ensuring Good Administration,* European Banking Institute Working Paper Series 2023 - no. 140, 2023, par. B.3.

vigilanza. La correlazione si riferisce ad una relazione tra due variabili che tendono a verificarsi insieme, mentre, la causalità implica una sequenza temporale in cui un evento precede l'altro. Poiché, le previsioni o le raccomandazioni di sistemi ML si basano su regolarità statistiche, quindi, su proprietà generalizzate piuttosto che sul singolo caso, possono portare a decisioni non fondate sui fatti[222] ma, soprattutto, a decisioni basate sulla correlazione e non sulla causalità. L'approccio utilizzato, che prescinde dal caso concreto, può omettere di prendere in considerazione dei particolari determinanti ai fini della decisione, oltre a ridurre il grado di spiegabilità dell'azione amministrativa. In relazione a quest'ultimo aspetto, data l'assenza di una spiegazione causale, la BCE non sarebbe in grado nemmeno di motivare la decisione rendendo l'attività di vigilanza inaccessibile e non trasparente[223].

Un secondo aspetto tecnico, forse il limite più importante anche quando l'IA svolge funzione "servente" (*Enhanced*), è legato alla natura dei nuovi algoritmi alla base dei sistemi di IA, cioè, di ML ma, soprattutto, di *deep learning*.

Questi algoritmi hanno la straordinaria capacità di apprendere da vasti insiemi di dati e, una volta assimilati, di prendere decisioni in modo esperienziale o intuitivo, simile al modo in cui agiscono gli esseri umani. Questo significa che essi non si limitano più a eseguire rigide istruzioni predefinite come quelli "deterministici"[224], ma sono in grado di adattarsi dinamicamente ai problemi, facendo affidamento su modelli di dati complessi che potrebbero superare la comprensione umana[225]. Il prezzo da pagare, per l'utilizzo di questi tipi di algoritmi, è il "*black box*" sul funzionamento interno, anche per i loro stessi creatori.

Per "*black box*" si intende il massimo livello di opacità che caratterizza alcuni sistemi di IA, in grado di rendere imperscrutabile l'*iter* logico seguito dall'algoritmo per giungere ad un dato risultato, comportante, sul piano giuridico, una violazione del principio di

---

[222] RINGE W.G. *et al*., *Navigating the Legal Landscape of AI-Enhanced Banking Supervision: Protecting EU Fundamental Rights and Ensuring Good Administration,* European Banking Institute Working Paper Series 2023 - no. 140, 2023, Cap. IV, par. A.2.

[223] Ibidem.

[224] Si veda par. 1.1. su cosa sia un algoritmo deterministico.

[225] BATHAEE Y., "*The Artificial Intelligence Black Box and the Failure of Intent and Causation*", 31 Harvard Journal of Law & Technology, 2018, p. 891. [Online]. Disponibile su: https://jolt.law.harvard.edu/volumes/volume-31

trasparenza dell'azione amministrativa[226]. L'opacità è un fenomeno a "geometria variabile"[227], in quanto i sistemi di *deep learning* si caratterizzano per un'opacità assoluta, mentre, altri,[228] presentano un grado di opacità nettamente inferiore, ad esempio, perché fondati sulla causalità piuttosto che sulla correlazione.

L'opacità di un sistema è figlia di diversi fattori. In primo luogo, può dipendere dalla scelta delle aziende produttrici, in quanto prima di esser algoritmi sono entità economiche, la cui creazione ha comportato un costo, da proteggere dalla concorrenza. Per le autorità di vigilanza bancaria, l'opacità può servire a impedire ai soggetti vigilati di eludere il sistema di IA attraverso il *reverse engineering*[229]. Inoltre, l'opacità è inevitabile ogni volta che si impiegano metodi di ML complessi e auto-evolutivi, come quelli basati sul *deep learning*. In ultimo, sono trascritti per poter esser elaborati da "codici sorgente" in uno tra le migliaia di linguaggi di programmazione e non in linguaggio naturale con cui si esprimono le norme e le argomentazioni giuridiche[230]. Da tale aspetto tecnico, discende l'elevato rischio d'inadempimento dell'obbligo di motivazione, in capo alla BCE, che impone di illustrare gli accertamenti di fatto e le valutazioni giuridiche su cui le decisioni poggiano[231], quindi, a fornire una descrizione dell'*iter* logico. Allo stato attuale, ciò potrebbe accadere nei casi in cui i supervisori umani si affidino a tali sistemi, in quanto, i primi potrebbero non esser in grado di comprendere i fattori presi in considerazione dagli algoritmi per arrivare ad una determinata decisione. Tornando alla motivazione, essa costituisce elemento essenziale del provvedimento la cui assenza o insufficienza inficerebbe sulla validità dello stesso. Ciò, vale in particolare per la BCE che, essendo titolare di un potere che presenta sempre una componente discrezionale, dovrà offrire una motivazione specifica, individuale e concreta. La questione giuridica, su come un sistema di *deep learning*, operante con metodo

---

[226] LO SAPIO G., *La black box: l'esplicabilità delle scelte algoritmiche quale garanzia di buona amministrazione*, in Federalismi.it, n. 16/2021, 2021, p. 117. [Online]. Disponibile su: https://www.federalismi.it/nv14/articolo-documento.cfm?artid=45610

[227] Ivi, p. 121.

[228] Ad esempio, gli algoritmi deterministici o condizionali.

[229] RINGE W.G. *et al*., *Navigating the Legal Landscape of AI-Enhanced Banking Supervision: Protecting EU Fundamental Rights and Ensuring Good Administration,* European Banking Institute Working Paper Series 2023 - no. 140, 2023, Cap. IV, par. A.2

[230] LO SAPIO G., *La black box: l'esplicabilità delle scelte algoritmiche quale garanzia di buona amministrazione*, in Federalismi.it, n. 16/2021, p. 121.

[231] Per una portata generale del contenuto dell'obbligo si veda il par. 2.2.4.

correlazionale, possa offrire una motivazione logica[232], sorge spontanea. Come può l'algoritmo fornire la prova del nesso causale tra le circostanze di fatto e la decisione se non utilizza un metodo causale?

Ulteriori problemi, sorgono in relazione ai requisiti della specificità e individualità della motivazione che non può prescindere dal caso concreto e che verrebbero violati, in quanto, le decisioni degli algoritmi sono prese su regole statistiche, quindi, generalizzate[233]. In ultimo, l'omissione o insufficienza della motivazione pregiudicherebbe "in astratto"[234] il diritto alla difesa, perché non permetterebbe alla parte di contestare il merito del provvedimento.

L'integrazione dell'IA, nell'attività di vigilanza bancaria, contribuisce ad un'automazione di alcune fasi della stessa. Se da un lato, l'automazione permette di perseguire alcuni dei vantaggi illustrati precedentemente, dall'altro, complica notevolmente la partecipazione del destinatario nel procedimento, limitando uno dei diritti "procedurali" di buona amministrazione: il diritto di esser ascoltati[235].

Per quanto riguarda il diritto ad esser ascoltati, appaiono evidenti i dubbi su come e quanto l'algoritmo possa prendere in considerazione la versione offerta dal destinatario del procedimento. In particolare, risulta difficile pensare che un algoritmo, allenato in precedenza su una miriade di dati, possa dare rilevanza ad un singolo *set* di dati offerti da una parte ed eventualmente, spiegare le ragioni del dissenso in motivazione.

5. La responsabilità della BCE e dei suoi funzionari nell'*AI-driven banking supervision*

La BCE, nella veste di autorità di vigilanza bancaria, è responsabile per «*i danni cagionati da essa stessa o dai suoi agenti nell'esercizio delle loro funzioni*»[236], in quanto, il Regolamento n. 1024/2013 sul Meccanismo di vigilanza unico, l'assoggetta alla stessa

[232] Una motivazione è illogica quando non consente il riscontro degli sviluppi che hanno portato a una decisione.

[233] RINGE W.G. *et al*., *Navigating the Legal Landscape of AI-Enhanced Banking Supervision: Protecting EU Fundamental Rights and Ensuring Good Administration,* European Banking Institute Working Paper Series 2023 - no. 140, 2023, Cap. IV, par. A.2.

[234] In astratto, in quanto, in concreto il diritto alla difesa non verrebbe pregiudicato avendo l'interessato il diritto a chiedere l'annullamento del provvedimento sprovvisto di motivazione.

[235] RINGE W.G. *et al*., *Navigating the Legal Landscape of AI-Enhanced Banking Supervision: Protecting EU Fundamental Rights and Ensuring Good Administration,* European Banking Institute Working Paper Series 2023 - no. 140, 2023, Cap. IV, par. A.2.

[236] Art. 340, comma 2 del TFUE.

responsabilità a cui vanno incontro le altre istituzioni UE. Pertanto, il rispetto del principio di buona amministrazione, non funge esclusivamente da parametro per valutare la legittimità dei provvedimenti, ma anche come criterio di attribuzione della responsabilità[237].

Tale approccio non è, però in linea, né con il principio n. 2 di Basilea[238] del 2012, ove emerge la tendenza verso la limitazione della responsabilità delle autorità di vigilanza all'interno degli Stati membri dell'UE, né con le regole nazionali sul regime di responsabilità delle autorità di vigilanza degli Stati membri, che godono di forme di limitazione della responsabilità, in ragione del fatto che l'attività di vigilanza bancaria è prevalentemente discrezionale.

Per questo motivo, al fine di evitare che il margine di manovra della BCE fosse eccessivamente ristretto, tenuto conto anche di interessi diversi rispetto a quelli del danneggiato, come la stabilità del sistema bancario, la Corte di Giustizia ha adottato una soluzione di compromesso che ricercasse un corretto bilanciamento tra gli interessi in gioco e rimuovesse le disparità normative tra autorità di vigilanza nazionali e BCE.

La soluzione è stata adottata dal caso *Bergaderm*[239] in poi, in cui la Corte ha ritenuto che per valutare se la condotta sia sufficientemente grave[240], si dovrebbe far riferimento, non già al carattere amministrativo o legislativo della misura, bensì, al grado di discrezionalità di cui dispone l'istituzione in questione. Nel caso di *specie*, godendo la BCE di un potere prevalentemente discrezionale, la condotta sarà considerata sufficientemente grave qualora l'istituzione comunitaria interessata abbia violato manifestamente e gravemente i limiti del suo potere discrezionale[241]. Viceversa, qualora l'istituzione eserciti un potere privo di margini di discrezionalità, anche la semplice violazione del diritto comunitario sarà sufficiente per integrare il requisito della condotta sufficientemente grave.

---

[237] RINGE W.G. *et al*., *Navigating the Legal Landscape of AI-Enhanced Banking Supervision: Protecting EU Fundamental Rights and Ensuring Good Administration,* European Banking Institute Working Paper Series 2023 - no. 140, 2023, Cap. III, par. D.

[238] D'AMBROSIO R., *The ECB and NCA liability within the Single Supervisory Mechanism*, in Quaderni di Ricerca Giuridica della Banca d'Italia, 2015, n. 78, p. 17. [Online]. Disponibile su: https://www.bancaditalia.it/pubblicazioni/quaderni-giuridici/2015-0078/index.html

[239] Corte di Giustizia, 4 luglio 2000, C-352/98, *Laboratoires Pharmaceutiques Bergaderm*.

[240] La responsabilità dello Stato o di un'istituzione per i danni cagionati ai singoli sussisterà qualora siano soddisfatte tre condizioni: la norma giuridica violata deve essere destinata a conferire diritti agli individui; la violazione deve essere sufficientemente grave; deve sussistere il nesso causale tra la violazione dell'obbligo a carico dello Stato membro o dell'istituzione dell'Ue e il danno subito dai danneggiati. Si veda: Corte di Giustizia, 5 marzo 1996, *Brasserie du Pêcheur SA* contro *Bundesrepublik Deutschland* e *The Queen* contro *Secretary of State for Transport, ex parte: Factortame Ltd* e altri, punto 51.

[241] Ivi, punto 55.

La responsabilità derivante dall'attività di vigilanza non ha solo una dimensione esterna, tra BCE e parti danneggiate, ma anche interna, tra BCE e funzionari. I membri del personale saranno responsabili per eventuali danni causati alla BCE o a terzi, nello svolgimento delle loro rispettive funzioni, nel caso in cui siano stati realizzati da una condotta gravemente negligente o dolosa[242].

La distinzione fra le due tipologie di responsabilità risulta essenziale, ai fini dell'inquadramento delle problematiche che possono derivare, qualora l'errore nel procedimento sia stato realizzato da un'intelligenza artificiale o determinato dalla collaborazione con la stessa. Per quanto riguarda la responsabilità esterna, l'impiego di tali tecnologie durante l'attività non pone, di per sé, preoccupazioni circa la responsabilità della BCE, in caso di errori commessi dall'IA[243], di risarcire i danni subiti dai soggetti. Anche nel caso in cui il servizio di IA sia offerto da terzi sarà sempre la BCE a risponderne verso il danneggiato, fatto salvo il diritto di rivalsa sul fornitore[244].

I dubbi sorgono, in tema di responsabilità interna, sul criterio di ripartizione della responsabilità, nel caso in cui la condotta dannosa fosse stata realizzata dall'IA o con il suo ausilio. Sarà possibile ritenere responsabili i funzionari, nei casi in cui non abbiano competenze informatiche, per non aver vigilato correttamente sui risultati di un algoritmo di cui non hanno conoscenza e le cui logiche di funzionamento sono, spesso, oscure[245]? Inoltre, con riferimento a quest'ultimo aspetto, l'applicazione sicura dei concetti giuridici tradizionali di responsabilità, come il dolo e la colpa, è messa a dura prova[246] data le difficoltà nel ricostruire il processo che ha portato ad un dato *output*.

---

[242] BCE, *Condizioni di impiego per il personale della Banca centrale europea*, Parte 1 Disposizioni generali, par. 6. [Online]. Disponibile su: https://www.ecb.europa.eu/careers/pdf/conditions_of_employment.pdf

[243] RINGE W.G. *et al*., *Navigating the Legal Landscape of AI-Enhanced Banking Supervision: Protecting EU Fundamental Rights and Ensuring Good Administration,* European Banking Institute Working Paper Series 2023 - no. 140, 2023, Cap. IV, par. A.2.

[244] Ibidem.

[245] Si veda il par. 2.2.6. per maggiori spiegazioni sul "*black box problem*".

[246] RINGE W.G. *et al*., *Navigating the Legal Landscape of AI-Enhanced Banking Supervision: Protecting EU Fundamental Rights and Ensuring Good Administration,* European Banking Institute Working Paper Series 2023 - no. 140, 2023, Cap. IV, par. A.2.

CAPITOLO II – IL QUADRO NORMATIVO EUROPEO SULL'INTELLIGENZA ARTIFICIALE

1. I primi passi verso un quadro normativo europeo: le comunicazioni della Commissione, il "Libro bianco sull'intelligenza artificiale, le risoluzioni del Parlamento

Negli ultimi anni il campo dell'IA è stato protagonista di uno sviluppo esponenziale che ha interessato svariati ambiti della vita sociale comportando grandi cambiamenti. Agli innumerevoli vantaggi si sono contrapposti svariati rischi, spesso, figli della logica imperscrutabile che accomuna i sistemi più avanzati (*machine learning*, *deep learning*, *neural networks*)[247]. Per tali ragioni, il fenomeno ha catturato l'interesse delle istituzioni europee che hanno cominciato a muovere i "primi passi" verso un quadro normativo europeo elaborando principi, struttura e contenuti di tale legislazione[248].

Il 25 aprile 2018 la Commissione ha adottato la Comunicazione[249] "*L'intelligenza artificiale per l'Europa"* annunciando la strategia europea per l'IA.

In questa comunicazione ha definito, ufficialmente e per la prima volta, l'IA come «*sistemi che mostrano un comportamento intelligente analizzando il proprio ambiente e compiendo azioni, con un certo grado di autonomia, per raggiungere specifici obiettivi*» e ha preso atto dell'importanza di tali sistemi nel migliorare la qualità della vita ma, soprattutto, nell'affrontare le sfide più importanti della società moderna[250].

Con tale atto sono state indicate le principali iniziative da intraprendere quali: incentivare l'adozione e lo sviluppo dei sistemi di IA investendo in ricerca e innovazione; prepararsi ai cambiamenti in ambito formativo, occupazionale ed economico apportati dall'avvento

---

[247] CASONATO C., MARCHETTI B., *Prime osservazioni sulla proposta di regolamento della Commissione Ue in materia di intelligenza artificiale*, in "BioLaw Journal - Rivista di BioDiritto", 2021, n. 3, pp. 415-437, si veda par. 2. [Online]. Disponibile su: https://www.biodiritto.org/Online-First-BLJ/Online-First-BLJ-3-21-Prime-osservazioni-sulla-proposta-di-Regolamento-dell-Unione-europea-in-materia-di-Intelligenza-Artificiale

[248] Ibidem.

[249] Commissione europea, Comunicazione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, *L'intelligenza artificiale per l'Europa*, 25 aprile 2018. [Online] Disponibile su: https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52018DC0237

[250] Tra le tante: «*dal trattamento delle malattie croniche o dalla riduzione dei tassi di incidenti stradali mortali alla lotta contro il cambiamento climatico o alla prevenzione delle minacce alla sicurezza informatica*».

di tali sistemi e «*assicurare un quadro giuridico ed etico adeguato*»[251] in linea con la Carta dei diritti fondamentali.

Il 7 dicembre 2018, in un'ottica proiettata a favorire la cooperazione e il coordinamento tra Stati Membri e di incentivo agli investimenti congiunti e progetti di ricerca su tali sistemi, ha adottato un piano coordinato che «*fornisce un quadro strategico per le strategie nazionali per l'IA*»[252].

L'8 aprile 2019 la Commissione ha approvato la Comunicazione[253] "*Creare fiducia nell'intelligenza artificiale antropocentrica"* con l'intento di sviluppare un'IA che ponga al centro l'essere umano e permetterle di ottenere la fiducia del pubblico. A tal fine, la Commissione ha incaricato un gruppo di esperti indipendenti che ha individuato sette requisiti[254] che garantirebbero un'applicazione affidabile dell'IA.

Il 19 febbraio 2020 la Commissione ha pubblicato "*Il Libro bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia*"[255] con l'intento di presentare «*opzioni strategiche che consentano uno sviluppo sicuro e affidabile dell'IA in Europa, nel pieno rispetto dei valori e dei diritti dei cittadini dell'UE».* In particolare, da un lato, incentivando lo sviluppo di un «*ecosistema di eccellenza*» attraverso investimenti pubblici e privati lungo tutta la filiera dell'IA (*in primis* in ricerca e innovazione) e dall'altro, creando un «*ecosistema di fiducia*» per evitare la frammentazione del mercato interno che comprometterebbe gli obiettivi di fiducia e certezza del diritto[256].

---

[251] L'obiettivo di assicurare un quadro giuridico ed etico adeguato passa attraverso: l'elaborazione di orientamenti etici per l'IA, la riflessione sulle norme di sicurezza vigente e le questioni relative alla responsabilità, il garantire un utilizzo sicuro su larga scala.

[252] Commissione europea, Comunicazione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, *Piano coordinato sull'intelligenza artificiale,* 7 dicembre 2018. [Online] Disponibile su: https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52018DC0795

[253] Commissione europea, Comunicazione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, *Creare fiducia nell'intelligenza artificiale antropocentrica,* 8 aprile 2019. [Online] Disponibile su: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52019DC0168

[254] I sette requisiti fondamentali sono: intervento e sorveglianza umana; robustezza tecnica e sicurezza; riservatezza e governance dei dati; trasparenza; diversità, non discriminazione, equità; benessere sociale e ambiente; accountability.

[255] Commissione europea, *Libro bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia*, 19 febbraio 2020. [Online] Disponibile su: https://op.europa.eu/it/publication-detail/-/publication/ac957f13-53c6-11ea-aece-01aa75ed71a1

[256] TADDEI ELMI, G., MARCHIAFAVA, S., *Sviluppi recenti in tema di Intelligenza Artificiale e diritto: una rassegna di legislazione, giurisprudenza e dottrina*. Rivista italiana di informatica e diritto. 4, 2022, 123-139. [Online]. Disponibile su: https://doi.org/10.32091/RIID0084

Successivamente a questi atti, che costituiscono i "primi passi" più importanti compiuti dalla Commissione verso una proposta di regolamentazione del fenomeno, sono altrettanto significative le due Risoluzioni, adottate dal Parlamento europeo, concernenti rispettivamente un quadro relativo agli aspetti etici dell'intelligenza artificiale[257] e un regime di responsabilità civile[258].

In particolare, nella prima si sottolinea l'esistenza di un'asimmetria tra chi impiega l'IA e coloro che ad essa sono assoggettati, richiamando la necessità di rispettare quei sette requisiti fondamentali, già affermati dalla Commissione in una sua Comunicazione, e confermando il criterio del rischio come più adatto per operare le distinzioni normative necessarie tra i vari sistemi di intelligenza artificiale presenti e futuri[259].

Nella seconda si propone l'adozione di un regime di responsabilità oggettiva per i sistemi di IA "ad alto rischio", mentre, un regime per colpa, per quelli che operano a basso rischio[260].

2. Il quadro normativo: il "pacchetto europeo" sull'IA e gli obiettivi del Regolamento

Il pacchetto europeo sull'intelligenza artificiale lanciato dalla Commissione nell'aprile del 2021 include: una Comunicazione sulla promozione di un approccio europeo all'IA[261], una revisione del piano coordinato sull'IA[262], e la proposta di Regolamento sull'IA[263].

---

[257] Parlamento europeo, *Raccomandazione alla commissione concernenti il quadro relativo agli aspetti etici dell'intelligenza artificiale della robotica e delle tecnologie correlate,* 20 ottobre 2020. [Online] Disponibile su: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_IT.html

[258] Parlamento europeo, *Raccomandazione alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale*, 20 ottobre 2020. [Online] Disponibile su: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_IT.html

[259] TADDEI ELMI, G., MARCHIAFAVA, S. *Sviluppi recenti in tema di Intelligenza Artificiale e diritto: una rassegna di legislazione, giurisprudenza e dottrina*. Rivista italiana di informatica e diritto. 4, 2022, 123-139.

[260] Ibidem.

[261] Commissione europea, Comunicazione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, *Promuovere un approccio europeo all'intelligenza artificiale*, 21 aprile 2021. [Online] Disponibile su: https://www.senato.it/web/docuorc2004.nsf/4d9255edaa0d94f8c12576ab0041cf0a/fd08ed88aeca1edac12586fc006a3991/$FILE/COM2021_0205_IT.pdf

[262] Nel Piano Coordinato 2021, l'obiettivo principale è tradurre la strategia in azioni. La Commissione e gli Stati membri sono chiamati ad accelerare gli investimenti in tecnologie di IA per una ripresa economica e sociale resilienti, attuare le strategie di IA in modo completo e tempestivo e allineare le politiche per affrontare sfide globali e rimuovere la frammentazione.

[263] Commissione europea, *Proposta di Regolamento europeo del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'unione,* 21 aprile 2021. [Online] Disponibile su: https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX%3A12012E294

A partire dalla pubblicazione della strategia sull'intelligenza artificiale per l'Europa nell'aprile 2018, l'obiettivo della duplice politica della Commissione è stato rendere l'UE un polo di classe mondiale per l'IA, assicurando allo stesso tempo che l'IA sia antropocentrica e affidabile. Il pacchetto rappresenta una pietra miliare per entrambe le dimensioni di tale politica. Al fine di promuovere lo sviluppo dell'IA e allo stesso tempo, affrontare i potenziali rischi elevati che essa pone per la sicurezza e i diritti fondamentali, la Commissione presenta un piano coordinato riveduto sull'IA e una proposta di un quadro normativo[264].

Quest'ultima si pone in un contesto europeo di totale assenza di disciplina di portata generale[265] e con l'intento di colmare il *gap* normativo ed economico,[266] con Stati Uniti e Cina. Negli Stati Uniti, il 30 ottobre 2023, il presidente Biden ha firmato un ordine esecutivo al fine di dettare delle linee guida per uno sviluppo "responsabile", nonostante la preoccupazione che ciò possa far perdere terreno rispetto alla Cina che sta promuovendo, invece, uno sviluppo dell'IA anche a discapito dei diritti fondamentali[267].

Nella relazione si afferma che il Regolamento si prefigge quale obiettivo generale quello di assicurare il buon funzionamento del mercato interno per i sistemi di IA proponendo un quadro giuridico per un'IA affidabile.

La proposta permetterebbe di perseguire tale obiettivo attraverso un'azione unitaria e orientata su quattro linee direttrici: «*assicurare che i sistemi di IA immessi sul mercato dell'Unione e utilizzati siano sicuri e rispettino la normativa vigente in materia di diritti fondamentali e i valori dell'Unione; assicurare la certezza del diritto per facilitare gli investimenti e l'innovazione nell'intelligenza artificiale; migliorare la governance e l'applicazione effettiva della normativa esistente in materia di diritti fondamentali e*

---

[264] In ciò consiste l'approccio europeo evidenziato nella Comunicazione e che la Commissione mira a promuovere con la presentazione del pacchetto sull'IA. Cfr. Commissione europea, Comunicazione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, *Promuovere un approccio europeo all'intelligenza artificiale,* p. 1.

[265] CASONATO C., MARCHETTI B., *Prime osservazioni sulla proposta di regolamento della Commissione Ue in materia di intelligenza artificiale*, in "BioLaw Journal - Rivista di BioDiritto", 2021, n. 3, pp. 415-437, par. 1.

[266] GALLI G., LOREGGIA A., MAROCCIA I., VALPEDA I., *Intelligenza artificiale: cos'è e dov'è*, in Osservatorio sui Conti Pubblici Italiani, 2023, p. 3. [Online]. Disponibile su: https://osse rvatoriocpi.unicatt.it/ocpi-Intelligenza%20Artificiale%20cosa%20e%20dove.pdf. In cui si afferma che in termini di apporto di capitale di rischio alle imprese che sviluppano IA, la leadership rimane di gran lunga quella degli Stati Uniti (273 miliardi di dollari), seguita a distanza dalla Cina (76 miliardi).

[267] CASONATO C., MARCHETTI B, *Prime osservazioni sulla proposta di regolamento della Commissione Ue in materia di intelligenza artificiale*, in "BioLaw Journal - Rivista di BioDiritto", 2021, n. 3, pp. 415-437, par 1.

requisiti di sicurezza applicabili ai sistemi di IA; facilitare lo sviluppo di un mercato unico per applicazioni di IA lecite, sicure e affidabili nonché prevenire la frammentazione del mercato»[268].

In particolare, proponendo un approccio *top-down* volto a individuare *ex ante* le pratiche proibite e quelle potenzialmente in grado di ledere i diritti fondamentali classificandole in base al rischio (risk-*based approach*) e facendone derivare, per ciascuna tipologia di rischio, le regole applicabili[269]. Questo approccio non è andato esente da critiche in dottrina. Una parte della stessa, sottolineando che il metodo *top-down* avrebbe come difetto quello di andare a creare delle categorie astratte che potrebbero non cogliere tutti i rischi delle tecnologie impiegate, ha evidenziato la maggiore adeguatezza dell'approccio *bottom-up*[270]. Quest'ultimo è basato sull'individuazione della tecnologia, delle sue caratteristiche e dei processi in cui viene utilizzata. Un'altra parte della dottrina, ha criticato: l'eccesiva rigidità del modello del legislatore europeo perché non in grado di stare al passo con gli sviluppi tecnologici; la scarsa distinzione fra i sistemi di IA; il rischio di isolarsi, a livello normativo, dal resto del mondo[271].

All'esigenza di delineare un quadro giuridico certo e uniforme, si contrappone la necessità di renderlo flessibile. In questo senso, sono stati previsti dei meccanismi per evitare che la rapida evoluzione tecnologica e l'impossibilità di prevedere *ex ante* rischi non calcolabili, possano rendere rapidamente obsoleta la disciplina[272]. La Commissione, infatti, è titolare di un potere di delega a tempo indeterminato attribuito da alcuni articoli del Regolamento. Per esempio, al fine di aggiornare l'elenco di cui all'allegato III aggiungendo nuovi sistemi di IA "ad alto rischio" in presenza delle condizioni di cui all'art. 7[273]. È, inoltre, previsto un obbligo in capo alla stessa di trasmettere, al Parlamento

---

[268] Commissione europea, *Relazione alla Proposta di Regolamento sull'intelligenza artificiale*, 21 aprile 2021, Cap. 1, par. 1.1. [Online]. Disponibile su: https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52021PC0206

[269] CONTISSA G., GALLI F., GODANO F., SARTOR G., *Il Regolamento europeo sull'intelligenza artificiale. Analisi informatico – giuridica*, in i-lex. Rivista di Scienza Giuridiche, Scienze Cognitive ed Intelligenza Artificiale, 2021, p. 32 [Online]. Disponibile su: http://www.i-lex.it/articles/Volume14/Fascicolo2RegulationOfAI/Contissa_et_al_Proposta_regolamento.pdf

[270] Ibidem.

[271] FINOCCHIARO G., *La proposta di Regolamento sull'intelligenza artificiale. Il modello europeo basato sulla gestione del rischio*, in "Il diritto dell'informazione o dell'informatica, n. 2, 2022, p. 322. [Online]. Disponibile su: https://www.digitalmedialaws.com/wp-content/uploads/2022/11/Giusella-Finocchiaro.pdf

[272] CASONATO C., MARCHETTI B., *Prime osservazioni sulla proposta di regolamento della Commissione Ue in materia di intelligenza artificiale*, in "BioLaw Journal - Rivista di BioDiritto", 2021, n. 3, pp 418-419.

[273] Le condizioni sono le seguenti*: «a) i sistemi di IA sono destinati a essere usati in uno dei settori elencati ai punti da 1 a 8 dell'allegato III; b) i sistemi di IA presentano un rischio di danno per la salute e la*

europeo e al Consiglio, una relazione di valutazione e sul riesame del presente Regolamento sullo stato delle risorse finanziare e umane, a disposizione delle autorità nazionali, per l'esercizio delle competenze loro assegnate e sullo stato delle sanzioni[274]. In ultimo, anche un potere esercitabile dalla Commissione, di presentare proposte di modifica alla luce degli sviluppi tecnologici[275]. L'elenco delle rimanenti valutazioni che la Commissione deve redigere periodicamente è analiticamente descritto all'art. 112 del Regolamento.

Il Regolamento costituisce, per certi versi, un punto di arrivo in quanto sulla scorta delle svariate Comunicazioni, del Libro bianco della Commissione e delle Risoluzioni del Parlamento[276], si è giunti ad una disciplina unitaria del fenomeno, ma per altri versi, un punto di partenza, in quanto appena approvato e destinato ad entrare in vigore a scaglioni[277].

2.1. La base giuridica del Regolamento e il rispetto dei principi sussidiarietà e proporzionalità

Prima di procedere ad un esame della sua struttura, occorre interrogarsi su quali basi giuridiche il legislatore europeo ha giustificato il suo intervento e quale atto giuridico ha adottato per disciplinare la materia. Per rispondere al primo interrogativo, occorre rintracciare il principale obiettivo del Regolamento, ossia, assicurare attraverso l'armonizzazione il buon funzionamento del mercato interno. La principale base giuridica della, quindi, è l'art. 114 TFUE che si riferisce a misure che abbiano "per oggetto" l'instaurazione ed il funzionamento del mercato interno dati i rischi di: frammentazione del mercato concernenti i requisiti dei servizi e dei prodotti IA; riduzione della certezza del diritto per fornitori e utenti circa le regole da applicare a tali sistemi[278]. Inoltre, essendo previste delle regole specifiche per la protezione dei dati personali delle persone

sicurezza, o un rischio di impatto negativo sui diritti fondamentali, che è, in relazione alla sua gravità e alla probabilità che si verifichi, e tale rischio è equivalente o superiore al rischio di danno o di impatto negativo presentato dai sistemi di IA ad alto rischio di cui all'allegato III».

[274] Art. 112, par. 2 del Regolamento.

[275] Art. 112, par. 10 del Regolamento.

[276] Vedi sopra, par. 1.

[277] A seguito del via libera all'unanimità del Consiglio del 21 maggio 2024, sarà pubblicato quest'estate sulla Gazzetta Ufficiale.

[278] Commissione Europea, *Relazione alla Proposta di Regolamento sull'intelligenza artificiale*, 21 aprile 2021, Cap. 2, par. 2.1. [Online]. Disponibile su: https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52021PC0206

fisiche che limita fortemente l'utilizzo di taluni sistemi di IA[279], l'iniziativa si basa anche sull'art. 16 TFUE[280]. La Commissione, in relazione al tipo di atto giuridico, poteva adottare una proposta di regolamento o una di direttiva. È noto che, mentre quest'ultima quando ha portata generale e vincola gli Stati membri «*per quanto riguarda il risultato da raggiungere*»[281] lasciando, una più o meno ampia, discrezionalità circa forme e mezzi per perseguire quell'obiettivo[282], il regolamento è obbligatorio in tutti i suoi elementi ed è direttamente applicabile[283]. Alla luce di ciò, dato il dichiarato obiettivo di voler prevedere un quadro normativo unitario e onde evitare divergenze nelle modalità di attuazione, si è optato per lo strumento del regolamento[284].

Nei settori che non sono di competenza esclusiva dell'UE, ai sensi dell'art. 5, par. 3 del TFUE, l'esercizio delle competenze avviene nel rispetto dei principi di sussidiarietà e proporzionalità. Nel caso di specie, la natura dell'IA, spesso, basata su vasti e diversificati *set* di dati integrabili in una varietà di prodotti o servizi liberamente circolanti nel mercato interno, suggerisce che gli obiettivi proposti non possono essere raggiunti in modo efficace da singoli Stati membri.

L'adozione di regole nazionali divergenti rischierebbe di ostacolare la circolazione fluida di prodotti e servizi legati all'IA nell'Unione Europea, compromettendo la sicurezza e la tutela dei diritti fondamentali, nonché, l'adozione dell'IA da parte del mercato[285]. Il rispetto del principio di proporzionalità passa attraverso un approccio basato sul rischio che impone oneri normativi sempre più considerevoli all'aumentare del rischio di pregiudizio dei diritti fondamentali. Le regole previste a tutela di tali diritti «*non devono*

[279] Si rivolge a quei sistemi di IA che permettono l'identificazione biometrica remota ed in tempo reale in spazi accessibili al pubblico. Quest'ultimi potranno esser utilizzati, eccezionalmente, a fini di contrasto di talune attività criminali.

[280] Commissione Europea, *Relazione alla Proposta di Regolamento sull'intelligenza artificiale*, Cap. 2, par. 2.1.

[281] Art. 288.3 TFUE.

[282] La direttiva può aver portata generale o essere rivolta solo a taluni Stati membri, non è mai direttamente applicabile ma in taluni casi le disposizioni possono avere efficacia diretta (possono esser direttamente applicate in caso di mancato recepimento a livello nazionale).

[283] Art. 288.2 TFUE.

[284] CASONATO C., MARCHETTI B., *Prime osservazioni sulla proposta di regolamento della Commissione Ue in materia di intelligenza artificiale*, , in "BioLaw Journal - Rivista di BioDiritto", 2021, n. 3, pp. 415-437, par. 2.

[285] Commissione Europea, *Relazione alla Proposta di Regolamento sull'intelligenza artificiale*, Cap. 2, par. 2.2.

però arrecare un ostacolo sproporzionato rispetto ai margini di sviluppo tecnologico economico e sociale che l'IA può rappresentare»[286].

2.2. La struttura del Regolamento

In questa sede, si procederà ad un'illustrazione generale della struttura del testo del Regolamento che sarà, poi, approfondita nei prossimi paragrafi. Innanzitutto, il Regolamento europeo sull'intelligenza artificiale è accompagnato da una relazione che illustra: i motivi e gli obiettivi della proposta, la base giuridica, il rispetto dei principi di proporzionalità e sussidiarietà, i risultati delle consultazioni pubbliche e delle valutazioni di impatto, l'incidenza sul bilancio.

Il documento è costituito da 13 Capi, composti da 113 articoli e preceduti da 180 considerando. È corredato da 13 allegati tecnici.

Il Capo I detta delle disposizioni generali sull'oggetto e sull'ambito di applicazione del Regolamento. L'insieme di disposizioni del presente regolamento, indicate in linea generale all'art. 1, si applicano: ai fornitori[287] che immettono sul mercato o mettono in servizio sistemi di IA nell'Unione; agli utenti dei sistemi di IA situati nell'Unione; ai fornitori e agli utenti di sistemi a situati in un paese terzo, laddove l'*output* prodotto dal sistema sia utilizzato nell'Unione. L'art. 3 detta le definizioni dei termini presenti nel Regolamento.

I Capi II - IV individuano le categorie di IA esistenti, classificandole in base al rischio derivante dal loro utilizzo. Il Regolamento individua quattro livelli di rischio: inaccettabile, alto, medio, minimo[288].

Il Capo II sancisce il divieto nell'utilizzo dei sistemi che comportano un rischio inaccettabile, in particolare, l'art. 5 individua varie categorie di sistemi vietati: le pratiche di manipolazione che utilizzano tecniche subliminali o sfruttano la vulnerabilità di categorie specifiche di persone per distorcerne il comportamento; le pratiche che classificano e valutano l'affidabilità delle persone sulla base del loro comportamento e delle loro caratteristiche (*social scoring*); le pratiche finalizzate alla determinazione della

---

[286] CASONATO C., MARCHETTI B., *Prime osservazioni sulla proposta di regolamento della Commissione Ue in materia di intelligenza artificiale,* in "BioLaw Journal - Rivista di BioDiritto", 2021, n. 3, pp. 415-437, par.1.

[287] Indipendentemente dal fatto che siano stabiliti nell'Unione o in un Paese terzo.

[288] Art. 95 del Regolamento.

probabilità che una persona commetta reati; le pratiche che creano o ampliano banche di dati di riconoscimento facciale; le pratiche per inferire le emozioni di una persona fisica, nell'ambito del luogo di lavoro e degli istituti di istruzione; le pratiche di identificazione biometrica a distanza e in tempo reale,

Il Capo III è dedicato ai sistemi di IA "ad alto rischio". Alla Sezione 1, sono indicati i casi in cui un sistema di IA è considerato "ad alto rischio", ossia, quando: è destinato a essere utilizzato come componente di sicurezza di un prodotto o è esso stesso un prodotto disciplinato e soggetto a una valutazione di conformità ai fini dell'immissione sul mercato o della messa in servizio, ai sensi della normativa di armonizzazione dell'Unione elencata nell'allegato I[289]; è indicato all'allegato III[290].

Alla Sezione 2, sono indicati i requisiti che tali sistemi devono rispettare. È richiesto che: adottino un sistema di gestione e mitigazione dei rischi[291] e tecniche in grado di assicurare la protezione[292] e la qualità dei dati su cui si addestrano[293], garantiscano la tracciabilità dei risultati[294] e che il loro funzionamento sia sufficientemente trasparente[295], forniscano informazioni concise, complete, corrette, chiare e pertinenti all'utente[296].

Alla Sezione 3, sono indicati gli obblighi dei fornitori[297], degli importatori[298], dei distributori[299], degli utenti[300] di sistemi di IA "ad alto rischio" e dei fabbricanti dei prodotti collegati a tali sistemi.

Le Sezioni 4 e 5 disciplinano la procedura di valutazione *ex ante* della conformità di tali sistemi al presente Regolamento, nonché, gli organismi coinvolti.

Il Capo IV sancisce degli obblighi di trasparenza ulteriori per tutti quei sistemi di IA destinati a interagire con le persone fisiche. In particolare, i fornitori garantiscono che tali sistemi «*siano progettati e sviluppati in modo tale che le persone fisiche siano informate del fatto di stare interagendo con un sistema di IA, a meno che ciò non risulti evidente*

[289] Art. 6, par. 1, lett. a), b) del Regolamento.
[290] Art. 6, par. 2 del Regolamento.
[291] Art. 9 del Regolamento.
[292] Art. 15 del Regolamento.
[293] Art. 10 del Regolamento.
[294] Art. 12 del Regolamento.
[295] Art. 13, par.1 del Regolamento.
[296] Art. 13, par. 2 e 3 del Regolamento. Le informazioni da fornire sono indicate al par. 3 del presente articolo e saranno trattate specificamente nel par. 2.6.
[297] Artt. 16-22 del Regolamento.
[298] Art. 23 del Regolamento.
[299] Art. 24 del Regolamento.
[300] Art. 26 del Regolamento.

dalle circostanze e dal contesto di utilizzo»[301]. Sono esentati dall'obbligo quelli «*autorizzati dalla legge per accertare, prevenire, indagare e perseguire reati, a meno che tali sistemi non siano a disposizione del pubblico per segnalare un reato*»[302].

Al Capo V, individua una categoria particolare di modelli IA per finalità generali: quelli a rischio sistemico. Poi, provvede ed elencare gli obblighi ulteriori per i fornitori di sistemi per finalità generali e per quelli a rischio sistemico.

Il Regolamento al Capo VI, con l'obiettivo di incentivare le misure a sostegno dell'innovazione, sostiene la possibilità di costituire delle *sandboxes* normative[303], rimandando ad atti di esecuzione le modalità e le condizioni di funzionamento degli spazi.

Al Capo VII è delineato il sistema di *governance* dell'IA. A livello sovranazionale, nella Sezione 1, è istituito il "comitato europeo per l'intelligenza artificiale"[304] che fornisce assistenza e consulenza alla Commissione al fine di contribuire ad una efficace cooperazione con le autorità nazionali e garantire una applicazione uniforme del Regolamento. A livello nazionale, la Sezione 2, prevede che ogni Stato membro dovrà istituire o investire un'autorità nazionale che si occupi di garantire il rispetto e l'attuazione del Regolamento[305].

Il Capo successivo prevede l'istituzione di una "Banca dati dell'UE per i sistemi di IA indipendenti "ad alto rischio" al fine di garantire una facile individuazione e conoscenza dei sistemi "ad alto rischio".

Al controllo di conformità *ex ante*, previsto alla Sezione 5 del Capo III, si aggiunge una forma di controllo *ex post*: il "monitoraggio successivo all'immissione sul mercato" prevista al Capo IX.

Il Capo X incoraggia l'elaborazione di codici di condotta volti a promuovere l'applicazione volontaria, a tali sistemi, dei requisiti previsti per i sistemi "ad alto rischio".

I restanti Capi dettano norme di carattere generale che garantiranno una migliore attuazione del Regolamento. In particolare, con la previsione al Capo X, viene prevista la facoltà di adottare Codici di condotta per l'applicazione volontaria di requisiti specifici nei casi sistemi di IA a "rischio minimo o nullo". Al Capo XI, invece, si attribuisce il

[301] Art. 50, par. 1 del Regolamento.
[302] Ibidem.
[303] Sono spazi di sperimentazione dei sistemi di IA. Saranno trattati specificamente nel 2.11.
[304] Art. 65 del Regolamento.
[305] Art. 70 del Regolamento.

potere di adottare atti delegati alla Commissione ed al Capo XII, un sistema di *enforcement* per garantire il rispetto del Regolamento.

2.3. La definizione di intelligenza artificiale

Tracciare le linee di confine, entro le quali il fenomeno dell'IA si manifesta, costituisce una delle principali criticità che trascina con sé la regolamentazione della materia. Non è un caso che uno dei motivi di frizione tra Consiglio e Parlamento europeo, al fine di raggiungere un "compromesso politico" sul contenuto del Regolamento, ha riguardato la definizione di cosa sia un'intelligenza artificiale.

Inizialmente, la Proposta all'art. 3, n.1 definiva l'intelligenza artificiale come: «*un software sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I, che può, per una determinata serie di obiettivi definiti dall'uomo, generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono*». La definizione era costituita da due parti tendenti verso due direzioni diverse. Una parte, collocata nel secondo periodo, con una valenza generale, si caratterizzava per un approccio neutrale rispetto alla tecnologia di base, in quanto, volta a ricomprendere qualunque tipologia di *software* in grado di perseguire obiettivi attraverso la generazione di *output* che influenzano l'ambiente esterno. L'altra parte, collocata nel primo periodo, tendeva a restringere la definizione stessa con il riferimento a tre tecnologie specifiche: l'apprendimento automatico (apprendimento supervisionato e non, apprendimento per rinforzo), gli approcci basati su logica e modelli espliciti della conoscenza (sistemi esperti), e gli approcci statistici (stima *bayesiana*). Questa parte aveva come obiettivo quello di offrire maggiori certezze, a produttori e utilizzatori, sulla disciplina applicabile.

A seguito della proposta, sono state parecchie le obiezioni e le perplessità mosse alla definizione della Commissione, in quanto, contraddittoria ed eccessivamente ampia. La definizione, al primo periodo, era contraddittoria in quanto non era in linea con l'approccio basato sul rischio, perché contraria al principio di neutralità tecnologica. Inoltre, era eccessivamente ampia, in quanto, non restringeva l'ambito di applicazione ma includeva tecnologie non considerate IA[306] e soprattutto, generava incertezze tra gli

[306] Ad esempio, i modelli logici e statistici.

operatori del mercato durante la fase di verifica della categoria di appartenenza tra quelle elencate nell'allegato 1[307].

Per questo motivo, il 6 dicembre 2022, il Consiglio con la proposta di compromesso, ha sottolineato la necessarietà di procedere ad una restrizione della definizione. In particolare, al fine di garantire che la definizione di sistema di IA fornisca criteri sufficientemente chiari per distinguere l'IA dai sistemi *software* più classici, il testo di compromesso limita la stessa, ai sistemi sviluppati mediante approcci di apprendimento automatico e approcci basati sulla logica e sulla conoscenza[308].

Si è, inoltre, proceduto alla soppressione dell'allegato I e il corrispondente potere conferito alla Commissione di aggiornarlo mediante atti delegati e sono stati aggiunti i nuovi considerando 6 *bis* e 6 *ter* per chiarire cosa si debba intendere per approcci di apprendimento automatico e approcci basati sulla logica e sulla conoscenza[309].

In ultimo, al fine di permettere un continuo e veloce adeguamento della normativa a esigenze future, è stata prevista la possibilità di adottare atti di esecuzione per specificare ulteriormente e aggiornare le tecniche nell'ambito degli approcci di apprendimento automatico e degli approcci basati sulla logica e sulla conoscenza[310].

La modifica suggerita, però, non ha convinto ed infatti, la definizione presente nel testo finale[311] è totalmente diversa dalla precedente nelle caratteristiche che deve avere un sistema di IA, ma identica negli obiettivi. L'art. 3 recita che un sistema di IA: «*un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali*». Dalla disposizione vengono definitivamente eliminate le indicazioni alle tipologie di tecnologie sancendo, in modo pieno, il principio di neutralità tecnologica. La definizione si allinea con quella

[307] CONTISSA G, GALLI F., GODANO F., SARTOR G., *Il Regolamento europeo sull'intelligenza artificiale. Analisi informatico – giuridica*, in "i-lex. Rivista di Scienza Giuridiche, Scienze Cognitive ed Intelligenza Artificiale", 2021, pp. 8-9.

[308] Consiglio dell'Unione europea, *Regolamento sull'intelligenza artificiale, orientamento generale del Consiglio*, 6 dicembre 2022, p. 4. [Online]. Disponibile su: https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/it/pdf

[309] Ibidem.

[310] Ibidem.

[311] Il 6 marzo il Parlamento ha approvato il testo definitivo dell'*AI Act*.

adottata precedentemente dall'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE)[312].

Pertanto, affinché un dato sistema rientri nella definizione offerta dal Regolamento, è necessario che ricorrano vari presupposti. Deve, innanzitutto, essere basato su una macchina (sistema computazionale che per certi obiettivi è in grado di produrre un *output*) in grado di operare, almeno in parte, senza l'intervento umano. In secondo luogo, deve presentare una capacità di adattamento che gli permette di migliorarsi ed evolversi a seguito della sua attivazione. Deve essere in grado di raggiungere alcuni obiettivi come, ad esempio, la valutazione dei questionari "*fit and proper*". Ed in ultimo, deve esser in grado di influenzare gli ambienti esterni e di contribuire ad un data decisione.

2.4. L'ambito di applicazione e i destinatari della regolamentazione

La definizione di intelligenza artificiale specifica l'applicazione oggettiva della regolamentazione, cioè, individua i sistemi considerabili "intelligenti" a cui dovranno esser applicate le disposizioni dell'*AI Act*.

All'art. 2, invece, il Regolamento individua l'ambito di applicazione soggettiva, i destinatari della regolamentazione.

Il regolamento non mira a raggiungere i soli produttori, programmatori, distributori, fabbricanti, rappresentanti, importatori, il cui luogo di stabilimento è nell'Unione europea ma anche quelli ubicati in un Paese terzo, il cui prodotto produce un *output* utilizzato nell'Unione[313]. L'attenzione alla collocazione del prodotto, piuttosto che alla localizzazione dei destinatari della regolamentazione, evita comportamenti elusivi e assicura piena ed efficace tutela.

L'efficacia del Regolamento viene limitata ai soli settori che rientrano nell'ambito di applicazione del diritto dell'Unione e in ogni caso, «*non pregiudica le competenze degli Stati membri in materia di sicurezza nazionale, indipendentemente dal tipo di entità incaricata dagli Stati membri di svolgere compiti in relazione a tali competenze*»[314].

---

[312] «*An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment*». Si veda la modifica del 8/11/2023 alla Raccomandazione del Consiglio sull'Intelligenza Artificiale adottata il 22/05/2019.

[313] Art. 2, par. 1, lett. a) – lett. g) del Regolamento.

[314] Art. 2, par. 3, comma 1, del Regolamento.

Inoltre, è prevista un'eccezione in tutti i casi in cui i sistemi di IA, non immessi sul mercato o messi in servizio nell'Unione, sono impiegati per scopi militari, di difesa o di sicurezza nazionale, indipendentemente dal tipo di entità che svolge tali attività. Se tali sistemi sono immessi nel mercato, il Regolamento non si applicherà se e nella misura in cui vengono impiegati per gli scopi sopraelencati[315].

Il Regolamento, parificando soggetti pubblici e privati, impone per le due categorie di soggetti le stesse garanzie, senza dare rilevanza al diverso regime giuridico che differenzia l'operato dei soggetti pubblici rispetto ai privati. L'unica eccezione, oltre a quelle di cui sopra, riguarda il caso in cui le «*autorità pubbliche di un paese terzo o organizzazioni internazionali utilizzino i sistemi di IA nel quadro della cooperazione o di accordi internazionali per la cooperazione delle autorità di contrasto e giudiziarie con l'Unione o con uno o più Stati membri*[316]». La condizione essenziale per rientrare nell'eccezione è che le autorità o le organizzazioni che ne faranno uso dovranno garantire il rispetto dei diritti e delle libertà fondamentali delle persone.

Sempre all'art. 2, è prevista la non applicazione dell'*AI Act* nei casi in cui i sistemi siano esclusivamente destinati ad attività di ricerca e sviluppo[317] o nei casi in cui tali attività si riferiscano a sistemi non immessi sul mercato o in servizio[318].

2.5. Le pratiche di intelligenza artificiale «vietate»

Il regolamento individua tre categorie diverse di sistemi di IA assoggettando ciascuna di esse a un regime giuridico, più o meno severo, a seconda del rischio. Innanzitutto, considera l'applicazione dell'IA vietate, cioè, tutti quei sistemi che costituiscono una minaccia alle persone[319].

È vietata, in termini assoluti, ai sensi del Regolamento la messa in servizio o uso di sistemi di IA che: utilizzano tecniche subliminali o manipolative, al fine di influenzare il comportamento di una persona in modo significativo, compromettendo la sua capacità di

[315] Art. 2, par. 3, comma 2-3, del Regolamento.
[316] Art. 2, par. 4 del Regolamento.
[317] Art. 2, par. 6 del Regolamento.
[318] Art. 2, par. 8, comma 2-3, del Regolamento.
[319] La definizione è rinvenibile sul sito del Parlamento europeo: https://www.europarl.europa.eu/topics/it/article/20230601STO93804/normativa-sull-ia-la-prima-regolamentazione-sull-intelligenza-artificiale#:~:text=I%20sistemi%20di%20intelligenza%20artificiale%20sono%20considerati%20a%20rischio%20inaccettabile,una%20minaccia%20per%20le%20persone.

prendere decisioni informate in modo che provochi o possa provocare un danno significativo a tale persona o ad altre[320]; sfruttano le vulnerabilità di un individuo o di un gruppo specifico, come quelle legate all'età, alla disabilità o alla situazione sociale ed economica, con l'obiettivo o l'effetto di alterare significativamente il comportamento di queste persone in modo che provochi o possa provocare un danno significativo a tale persona o ad altre[321]; valutano o classificano persone fisiche sulla base del loro comportamento sociali o caratteristiche personali inferite, presunte o note, in cui il punteggio sociale comporti un trattamento pregiudizievole di persone fisiche in contesti sociali non collegati a quelli in cui dati sono stati raccolti o un trattamento ingiustificato o sproporzionato rispetto al loro comportamento sociale o a alla sua gravità[322]; valutano o prevedano la probabilità che una persona fisica commetta un reato unicamente attraverso un'analisi dei tratti e delle caratteristiche della personalità, salvo il caso in cui tale valutazione non funga da supporto ad un'attività di valutazione umana che si basa già su fatti oggettivi e verificabili direttamente connessi a un'attività criminosa[323]; creano o ampliano le banche dati di riconoscimento facciale mediante *scraping* non mirato di immagini facciali da *internet* o da filmati di telecamere a circuito chiuso[324]; giungono a delle conclusioni sfruttando le emozioni di una persona fisica nell'ambito del luogo di lavoro e degli istituti di istruzione, salvo l'utilizzo per motivi medici o di sicurezza; usano sistemi di categorizzazione biometrica che classificano individualmente le persone fisiche sulla base dei loro dati biometrici per trarre deduzioni o inferenze in merito a razza, opinioni politiche, appartenenza sindacale, convinzioni religiose o filosofiche, vita sessuale o orientamento sessuale[325].

All'interno dell'art. 5 non sono previsti solo sistemi vietati in termini assoluti ma anche in termini relativi, cioè, sistemi il cui utilizzo è subordinato ad una serie di condizioni e finalità specifiche.

In particolare, l'uso di sistemi di identificazione biometrica[326] in spazi accessibili al pubblico a fini di attività di contrasto è vietato, salvo il caso in cui siano strettamente

[320] Art. 5, par.1, lett. a) del Regolamento.
[321] Art. 5, par.1, lett. b) del Regolamento.
[322] Art. 5, par.1, lett. c) del Regolamento.
[323] Art. 5, par.1, lett. d) del Regolamento.
[324] Art. 5, par.1, lett. e) del Regolamento.
[325] Art. 5, par.1, lett. g) del Regolamento.
[326] Una definizione è offerta all'art. 3.18 del Regolamento n. 1725/2018 che recita: «*i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di*

necessari per: la ricerca vittime di rapimento; tratta di esseri umani o sfruttamento sessuale di esseri umani, nonché, ricerca di persone scomparse; sventare minacce terroristiche; la localizzazione o l'identificazione di una persona sospettata di aver commesso un reato con una pena detentiva di durata massima di minimo 4 anni[327].

Oltre alla specifica finalità a cui devono necessariamente tendere, l'art. 5 subordina l'utilizzo a due condizioni. La prima è che deve esser finalizzato a confermare l'identità della persona specificamente interessata tenendo conto, da un lato, della gravità della situazione che dà luogo all'uso, della probabilità e dell'entità del danno che sarebbe derivato dal caso del mancato uso del sistema[328] e dall'altro, delle conseguenze derivanti dall'utilizzo di tali sistemi sui diritti e le libertà delle persone coinvolte[329]. La seconda consiste nell'obbligo di effettuare una richiesta motivata di autorizzazione preventiva ad un'autorità giudiziaria o amministrativa indipendente, la cui decisione è vincolante, dello Stato membro in cui deve avvenire l'uso[330]. Tuttavia, in una situazione d'urgenza debitamente giustificata, sarà possibile utilizzarli anche senza l'autorizzazione, a patto che venga richiesta entro 24 ore. Nei casi in cui l'autorizzazione venga respinta, l'uso è interrotto con effetto immediato e tutti i dati, nonché, i risultati e gli *output* di tale uso sono immediatamente eliminati e cancellati.

In dottrina, è stata criticata la scelta del legislatore europeo di utilizzare il concetto di "urgenza debitamente giustificata" in quanto la giustificazione alla situazione di urgenza è rinvenibile solo successivamente, non essendo ravvisabile una situazione d'urgenza giustificata *tout court*[331].

L'autorità competente rilascia l'autorizzazione solo se ha accertato, sulla base di prove oggettive o indicazioni chiare, che risulta necessario e proporzionato ad una delle finalità indicate dal par. 1, lett. h) e in particolare limitato a quanto necessario in termini di periodo di tempo e ambito geografico.

---

una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici».

[327] Art 5, par. 1, lett. h) del Regolamento.

[328] Art 5, par. 2, comma 1, lett. a) del Regolamento.

[329] Art 5, par. 2, comma 1, lett. b) del Regolamento.

[330] Art 5, par. 3, comma 1, lett. b) del Regolamento.

[331] MARCHIANÒ G., *Proposta di regolamento della Commissione europea del 21 aprile 2021 sull'intelligenza artificiale con particolare riferimento alle IA ad alto rischio*, Riv. Giur. AmbienteDiritto.it, Fascicolo 2/2021, p. 11. [Online]. Disponibile su: https://www.ambientediritto.it/wp-content/uploads/2021/06/PROPOSTA-DI-REGOLAMENTO-DELLA-COMMISSIONE-EUROPEA-DEL-21-APRILE-2021-SULLINTELLIGENZA-ARTIFICIALE-CON-PARTICOLARE-RIFERIMENTO-ALLE-IA-AD-ALTO-RISCHIO_Marchiano.pdf

2.6. I sistemi ad "alto rischio" e i relativi requisiti

La seconda categoria riguarda i sistemi di IA "ad alto rischio". L'art. 6 stabilisce che un sistema IA è considerato "ad alto rischio" se è destinato a essere utilizzato come componente di sicurezza di un prodotto, o è esso stesso un prodotto[332] e se è soggetto a una valutazione della conformità da parte di terzi ai fini dell'immissione sul mercato o della messa in servizio di tale prodotto ai sensi della normativa di armonizzazione dell'Unione elencata nell'Allegato I[333]. Tuttavia, il sistema di IA è considerato "ad alto rischio", indipendentemente dalle condizioni appena citate, se rientra nei casi di cui all'Allegato III, cioè, quei casi in cui i sistemi sono destinati ad esser utilizzati: per l'identificazione biometrica remota; per la categorizzazione biometrica in base ad attributi o caratteristiche sensibili protetti, basati sulla deduzione di tali attributi o caratteristiche[334]; per il riconoscimento delle emozioni della persona[335]; come componenti di sicurezza nella gestione e nel funzionamento delle infrastrutture digitali critiche, del traffico stradale o nella fornitura di acqua, gas, riscaldamento o elettricità; per fini d'istruzione e formazione professionale; alla gestione dei lavoratori e accesso al lavoro autonomo; a valutare l'accesso e la fruizione a servizi privati e pubblici essenziali; per valutare dei rischi e determinare dei prezzi in relazione a persone fisiche nel caso di assicurazioni sulla vita e assicurazioni sanitarie; per valutare e classificare le chiamate di emergenza effettuate da persone fisiche o per inviare servizi di emergenza di primo soccorso o per stabilire priorità in merito all'invio di tali servizi; nelle attività di contrasto ai reati per determinare il rischio di una persona di una persona di divenirne vittima, per le attività di indagine e per vagliare l'affidabilità degli strumenti probatori; per la gestione delle migrazioni, degli asili e del controllo delle frontiere; per l'amministrazione della giustizia nella ricerca e nell'interpretazione dei fatti, nell'applicazione delle norme ed in ultimo nei processi democratici.

Da tale elenco, si desume che numerosi sistemi ad "alto rischio" possono esser impiegati in procedimenti amministrativi aventi ad oggetto la selezione e la valutazione del personale o l'accertamento di una violazione di legge.

---

[332] Art. 6, par. 1, lett. a) del Regolamento.
[333] Art. 6, par. 1, lett. a) del Regolamento.
[334] Non vi rientrano quei sistemi la cui verifica biometrica è finalizzata ad accertare che una determinata persona è quello che dice di essere.
[335] Fatti salvi i casi in cui tali sistemi rientrano nei casi di applicazioni di IA vietate.

Tuttavia, il sistema, anche nel caso in cui rientri all'interno di quelli indicati nell'Allegato III, non è considerato "ad alto rischio" «*se non presenta un rischio significativo di danno per la salute, la sicurezza o i diritti fondamentali delle persone fisiche, anche nel senso di non influenzare materialmente il risultato del processo decisionale*»[336]. Tale situazione si realizza nel caso in cui svolga una delle seguenti attività: eseguire un compito procedurale limitato[337], migliorare il risultato di un'attività umana precedentemente completata[338], rilevare schemi decisionali o deviazioni da schemi decisionali precedenti e non è inteso a sostituire o influenzare la valutazione umana[339], eseguire un compito preparatorio per una valutazione pertinente ai fini dei casi d'uso elencati nell'allegato III[340]. L'esenzione non si applica ai sistemi di che svolgono attività di profilazione di persone fisiche, in quanto considerati sempre ad "alto rischio".

Ai sensi del par. 6 dello stesso articolo, è attribuito alla Commissione il potere di aggiungere nuove condizioni a quelle stabilite nel par. 3 per escludere, dall'ambito di applicazione della disciplina dei sistemi "ad alto rischio", le tecnologie previste all'Allegato III che non presentano un rischio significativo di danno alle persone fisiche, sulla base di prove concrete e affidabili. In via speculare, è attribuito alla stessa, nella situazione opposta, il potere di sopprimerle.

Il legislatore europeo, stante l'obiettivo fondamentale di garantire la certezza del diritto, ha preso atto della velocità e dell'estrema mutevolezza del fenomeno dell'IA e per questo motivo ha attribuito all'art. 7 un ulteriore potere alla Commissione. Quest'ultima, ha la facoltà di adottare atti delegati per modificare l'Allegato III, al fine di aggiungere o rimuovere categorie di sistemi di IA, valutato il rischio di danno alla salute, sicurezza e d'impatto sui diritti fondamentali delle persone coinvolte. La valutazione sarà svolta tenuto conto dei seguenti criteri[341]: le finalità del sistema, la misura in cui il sistema sarà usato, la misura di eventuali danni già arrecati dal sistema, la portata potenziale del danno, la reversibilità del risultato prodotto dal sistema, la presenza di misure di ricorso efficaci in relazione ai rischi (anche prevenzione).

[336] Art. 6, par. 3 del Regolamento.
[337] Art. 6, par. 3, lett. a) del Regolamento.
[338] Art. 6, par. 3, lett. b) del Regolamento.
[339] Art. 6, par. 3, lett. c) del Regolamento.
[340] Art. 6, par. 3, lett. d) del Regolamento.
[341] Art. 7, par. 2, lett. a) – h) del Regolamento.

Nelle Sezioni 2 e 3 del Capo I vengono rispettivamente dettati i requisiti che un'IA ad "alto rischio" deve rispettare per esser utilizzata o messa in servizio e gli obblighi dei suoi fornitori e utilizzatori. In via preliminare, occorre segnalare al lettore che in questa sede, non verranno analizzati in modo esaustivo tutti gli aspetti del sistema di *governance* dell'IA "ad alto rischio" e gli obblighi che riguardano le parti coinvolte.

Innanzitutto, è richiesta l'istituzione e il mantenimento di un sistema di gestione dei rischi inteso come un processo iterativo continuo, programmato e aggiornato, nonché, finalizzato: all'identificazione, analisi e stima dei rischi noti o prevedibili che il sistema di IA può comportare per la salute; a valutare se il sistema IA sia utilizzato conformemente alla sua finalità prevista o in condizioni di uso improprio ragionevolmente prevedibili[342]; a valutare eventuali rischi ottenuti mediante l'analisi dei dati raccolti da sistema di gestione dopo l'utilizzo dell'IA[343]; all'adozione di misure rivolte ad affrontare ed eliminare o limitare i rischi i previsti[344].

Per quei sistemi che utilizzano tecniche, il *Machine Learning* su tutte, che si addestrano su *set* di dati, devono soddisfare i criteri di qualità, indicati negli articoli precedenti, nonché, un *set* d'informazioni, come la convalida e le pratiche di gestione[345].

Tali pratiche riguardano: le scelte di progettazione, le attività legate alla raccolta dati[346], le operazioni di trattamento finalizzate alla preparazione dei dati[347], la formulazione di ipotesi su ciò che i dati rappresentano, la valutazione della disponibilità e dell'adeguatezza dei *set* di dati necessari, l'esame delle possibili distorsioni e adozione di misure adeguate a evitarle, individuazioni di eventuali lacune o carenze nei dati[348]. Nel caso in cui i fornitori addestrino i sistemi su dati personali, oltre alle disposizioni di cui al Regolamento (UE) 2016/679, alla Direttiva (UE) 2016/680 e al Regolamento (UE) 2018/1725, affinché tale trattamento avvenga si applicano le condizioni indicate dalla lett. a) a f) del punto 5.

---

[342] Art. 9, par. 2, lett. a), b) del Regolamento.
[343] Art. 9, par. 2, lett. c) del Regolamento.
[344] Art. 9, par. 2, lett. d) del Regolamento.
[345] MARCHIANÒ G., *Proposta di regolamento della Commissione europea del 21 aprile 2021 sull'intelligenza artificiale con particolare riferimento alle IA ad alto rischio*, Riv. Giur. AmbienteDiritto.it, Fascicolo 2/2021, p. 19.
[346] Le attività riguardano i processi e l'origine dei dati e per quanto riguarda i dati personali anche la finalità originaria.
[347] Le operazioni di trattamento sono: annotazione, etichettatura, pulizia, aggiornamento, arricchimento e aggregazione.
[348] Art. 10, par. 2, lett. a) – h), del Regolamento.

Un ulteriore requisito, prima dell'immissione sul mercato, è rappresentato dall'obbligo di redigere, in modo chiaro e comprensibile, la documentazione tecnica in modo da fornire, alle autorità nazionali competenti e agli organismi notificati, le informazioni necessarie per valutare la conformità del sistema di IA ai requisiti[349].

In particolare, essa deve contenere una descrizione generale del sistema comprendente: la finalità prevista; il nome del fornitore e la versione del sistema che indichi il suo rapporto con le versioni precedenti; il modo in cui il sistema di IA interagisce o può essere utilizzato per interagire con *hardware* o *software*, compresi altri sistemi di IA; le versioni di *software* e *firmware* e i requisiti relativi all'aggiornamento della versione; le forme in cui il sistema IA è disponibile sul mercato; una descrizione dell'uso e dell'interfaccia utente fornita all'utilizzatore; una descrizione degli elementi dello stesso e un'altra serie di elementi previsti assieme a questi nell'Allegato IV. Le istruzioni per l'uso contengono almeno l'identità e i dati di contatto del fornitore, le caratteristiche, le limitazioni e le capacità di un sistema di IA.

Altro aspetto, è che ai sensi dell'art. 12, tali sistemi devono consentire la registrazione automatica degli eventi durante il loro ciclo di vita per garantire la loro tracciabilità e supervisionare il funzionamento degli stessi. Le capacità di registrazione devono esser in grado di garantire la registrazione di eventi come l'individuazione di situazioni che presentano dei rischi.

All'art. 13 viene declinato il principio di trasparenza che impone ai fornitori di progettare e sviluppare sistemi di IA in modo tale da garantire che gli utilizzatori siano in grado di comprendere l'*output* e utilizzarlo adeguatamente.

Al fine di prevenire o ridurre al minimo i rischi per la salute, la sicurezza o i diritti fondamentali, i sistemi di IA sono sviluppati con interfacce uomo-macchina in moda tale da poter esser supervisionati da persone fisiche durante il periodo in cui sono in uso.[350]

In ultimo, ai sensi dell'art. 15, l'IA "ad alto rischio" deve garantire accuratezza, robustezza, cibersicurezza.

L'accuratezza è garantita attraverso l'obbligo di dichiarazione degli stessi nelle istruzioni per l'uso che accompagnano il sistema e la sua verifica attraverso il confronto con i parametri di adeguatezza stabiliti dalla Commissione e in cooperazione con i portatori di

[349] Art. 11, par. 1, commi 1 e 2 del Regolamento.
[350] Art. 14 del Regolamento.

interessi e le organizzazioni pertinenti, quali le autorità di metrologia e di analisi comparativa[351]. La robustezza può esser raggiunta attraverso soluzioni tecniche di ridondanza che possono includere piani di *backup* o *fail-safe*[352]. La cibersicurezza con l'adozione di misure tecniche volte a prevenire, accertare, rispondere, risolvere e controllare gli attacchi che cercano di manipolare: il *set* di dati di addestramento o i componenti preaddestrati utilizzati nell'addestramento, gli *input* progettati in modo da far sì che il modello di IA commetta un errore, gli attacchi alla riservatezza o i difetti del modello[353].

2.7. La valutazione della conformità e l'organismo notificato

L'immissione sul mercato dei sistemi di IA "ad alto rischio" è condizionata ad una valutazione di conformità degli stessi ai requisiti previsti dal Regolamento. In particolare, ai sensi dell'art. 43, par. 1, il fornitore potrà optare tra due procedure di valutazione: il controllo interno di cui all'Allegato VI o la valutazione del sistema di gestione della qualità e della documentazione tecnica a cura di un organismo notificato[354].

La procedura generale è la prima, basata sul controllo interno, prevista per tutti i sistemi di IA indicati all'Allegato III, ad eccezione del par. 1[355]. I controlli sono "interni" in quanto a carico dello stesso fornitore che dovrà valutare: la conformità del sistema di gestone della qualità; il rispetto dei requisiti essenziali, di cui al Capo III, Sezione 2, delle informazioni contenute nella documentazione tecnica; la conformità alla documentazione tecnica del processo di progettazione e sviluppo del sistema di IA e del monitoraggio successivo alla sua immissione[356].

Per altri sistemi di IA, in particolare. per quelli biometrici di cui all'Allegato III par. 1 e quelli che rientrano all'interno dell'art. 43, par. 1, comma 2, è prevista la procedura di conformità condotta da organismi terzi denominati "organismi notificati". Questa previsione costituisce un temperamento alla regola generale di autovalutazione della conformità ed è conseguenza, sempre, del *risk-based approach*.

[351] Art. 15, par. 2 del Regolamento.
[352] Art. 15, par. 4, comma 2 del Regolamento.
[353] Art. 15, par. 5, comma 3 del Regolamento.
[354] Prevista all'Allegato VII.
[355] Art. 43, par. 2 del Regolamento.
[356] Allegato VI, par. 1 – 4 del Regolamento.

Gli organismi notificati, operanti a seguito di apposita autorizzazione ricevuta da parte dell'autorità di notifica attraverso la procedura *ex* art. 29 ss., verificano la conformità dei sistemi di IA "ad alto rischio" secondo le procedure di valutazione della conformità di cui all'art. 43[357].

2.8. I sistemi a "rischio limitato": gli obblighi di trasparenza

Oltre alla categoria dei sistemi di IA "vietati" e quella dei sistemi "ad alto rischio", il Regolamento all'art. 50 prevede una disciplina per «*determinati sistemi di IA*» che non rientrano nei campi d'applicazione delle categorie sopracitate e che, i primi commentatori, hanno definito a "rischio limitato"[358]. La categoria, nonostante abbia natura residuale e ricavabile per sottrazione, costituisce la parte più consistente di sistemi di IA presenti nel mercato comune[359].

Trattandosi di una normativa basata sul *risk-based approach*, al diminuire dei rischi alla salute, alla sicurezza e ai diritti fondamentali, corrisponderà una disciplina più flessibile, con meno limitazioni e obblighi.

Tali sistemi, benché siano caratterizzati da un "rischio limitato", presentano profili problematici e potenzialmente dannosi che il legislatore mira a superare attraverso l'imposizione di obblighi di trasparenza alle persone fisiche che interagiscono con il sistema: fornitori e utilizzatori.

In via preliminare, si sottolinea che la trasparenza richiesta dall'art. 50 non coincide con quella prevista all'art. 13 per i sistemi "ad alto rischio". In quanto, per questa categoria la trasparenza si traduce in un obbligo di render noto a chi la utilizza che sta interagendo con un sistema di IA o che il contenuto è stato creato artificialmente, mentre, per i sistemi "ad alto rischio", il rispetto dell'obbligo viene garantito consentendo agli utilizzatori di poter interpretare l'*output* e utilizzarlo adeguatamente. Inoltre, la normativa non impone anche per tali sistemi di esser accompagnati da istruzioni per l'uso. Nulla vieta che ulteriori obblighi di trasparenza possano derivare dall'adozione di codici di condotta. In

[357] Art. 34, par. 1 del Regolamento.

[358] CONTISSA G., GALLI F., GODANO F., SARTOR G., *Il Regolamento europeo sull'intelligenza artificiale. Analisi informatico – giuridica*, in "i-lex. Rivista di Scienza Giuridiche, Scienze Cognitive ed Intelligenza Artificiale", 2021, pp. 27-29.

[359] CASONATO C., MARCHETTI B., *Prime osservazioni sulla proposta di regolamento della Commissione Ue in materia di intelligenza artificiale*, in "BioLaw Journal - Rivista di BioDiritto", 2021, n. 3, pp. 415-437, par. 5.

questo senso, l'Ufficio per l'IA incoraggia e agevola l'elaborazione di codici di buone pratiche a livello dell'Unione, approvati successivamente dalla Commissione secondo l'art. 56, par. 6, 7 e 8, per facilitare l'efficace attuazione degli obblighi relativi alla rilevazione e all'etichettatura dei contenuti generati o manipolati artificialmente[360].

L'art. 50 individua quattro categorie di sistemi a "medio rischio": «*i sistemi destinati ad interagire direttamente con le persone fisiche*»; i sistemi che generano contenuti audio, immagine, video o testuali sintetici; i sistemi di riconoscimento delle emozioni e di categorizzazione biometrica; sistemi che si avvalgono della tecnica "*deep fake*".

La prima categoria è stata prevista per affrontare il problema dei *chatbot* e dell'IA personificati, cioè, sistemi di IA che simulando una conversazione con un essere umano, interagiscono con gli utenti attraverso interfacce basate sul dialogo. Il rischio di tali sistemi è che gli utenti possano cadere in errore, credendo di star interagendo con una persona fisica, anziché, con l'IA. Per questo motivo, essi devono esser progettati e sviluppati in modo tale da far comprendere alle persone fisiche che si stanno relazionando con un sistema di IA, salvo il caso in cui, dalle circostanze e dal contesto di utilizzo, tale situazione, sia evidente agli occhi di una persona ragionevolmente avveduta e informata[361]. Un'ulteriore eccezione riguarda i casi in cui i sistemi di IA siano autorizzati dalla legge per accertare, prevenire, indagare o perseguire reati, nel rispetto della tutela dei diritti e delle libertà di terzi[362].

Il secondo gruppo ha ad oggetto i sistemi di IA che generano contenuti audio, immagine, video o testuali sintetici. L'obbligo di trasparenza, in capo ai fornitori, impone di garantire che su ogni *output* del sistema sia presente, in un formato leggibile, l'informazione che è stata generata o manipolata artificialmente. I fornitori sono obbligati a garantire la qualità delle loro soluzioni tecniche nella misura in cui ciò sia possibile, tenuto conto delle specificità dei vari contenuti, dei costi di attuazione e dello stato dell'arte attuale, come eventualmente indicato all'interno di norme tecniche[363].

L'obbligo di trasparenza, circa la natura dell'*output*, non si applica ai sistemi di IA che svolgono attività di assistenza per l'*editing standard* o non modificano, sostanzialmente,

[360] Art. 50, par. 7 del Regolamento.
[361] Art. 50, par. 1 del Regolamento.
[362] Ibidem.
[363] Art. 50, par. 2 del Regolamento.

i dati di *input* forniti dall'utilizzatore, o se autorizzati dalla legge ad accertare, prevenire, indagare o perseguire reati[364].

La terza categoria ricomprende i sistemi di riconoscimento dell'emozioni e di categorizzazione biometrica. Essi interpretano i dati biometrici e fanno valutazione sugli individui, ma differiscono da quelli "vietati" di cui all'art. 5 lett. f) e lett. g) e da quelli "ad alto rischio" di cui all'allegato III n. 1, per la finalità. I sistemi "vietati" sono finalizzati a inferire le emozioni di una persona nell'ambito del luogo di lavoro o degli istituti di istruzioni o per trarre deduzioni o inferenze in merito a razza, opinioni politiche, appartenenza sindacale, convinzioni religiose o filosofiche, vita sessuale o orientamento sessuale attraverso la categorizzazione biometrica. Mentre, quelli "ad alto rischio" sono finalizzati all'identificazione della persona.

Nella categoria, quindi, rientrano tutti quei sistemi che non hanno tali finalità. Per fare un esempio, ai sistemi di categorizzazione biometrica possono esser ricollegati *wearable* come *Apple SmartWatch* che utilizza dati biometrici per effettuare un'analisi sullo stato di salute di chi lo indossa[365].

L'ultimo gruppo ricomprende i sistemi di IA che generano o manipolano immagini o contenuti audio o video che costituiscono un "*deep fake*"[366]. Con questo termine, si fa riferimento a: «*foto, video e audio creati grazie a software di intelligenza artificiale che, partendo da contenuti reali (immagini e audio), riescono a modificare o ricreare, in modo estremamente realistico, le caratteristiche e i movimenti di un volto o di un corpo e a imitare fedelmente una determinata voce*»[367]. L'utilizzatore deve render noto che il contenuto è stato generato o manipolato artificialmente, salvo sempre il caso, in cui i sistemi siano utilizzati per lo svolgimento di indagini e accertamento dei reati[368].

---

[364] Ibidem.

[365] CONTISSA G., GALLI F., GODANO F., SARTOR G., *Il Regolamento europeo sull'intelligenza artificiale. Analisi informatico – giuridica*, in "i-lex. Rivista di Scienza Giuridiche, Scienze Cognitive ed Intelligenza Artificiale", 2021, pp. 27-29.

[366] Art. 50, par. 4, comma 1 del Regolamento.

[367] Definizione del Garante per la protezione dei dati personali rinvenibile al sito: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9512278

[368] Art. 50, par. 4, comma 2 del Regolamento.

2.9. I modelli di IA per finalità generali con rischio sistemico

Un sistema di IA per finalità generali è considerato a rischio sistemico se, a seguito di una valutazione condotta tramite l'utilizzo di strumenti tecnici e metodologie adeguate, nonché, parametri di riferimento, presenta capacità d'impatto elevate[369].

In alternativa, sarà considerato tale sulla base di una decisione[370] della Commissione, se il sistema presenta una capacità o un impatto equivalente a quelli di cui alla lettera a), tenuto conto dei criteri di cui all'allegato XIII[371].

Il concetto di "rischio sistemico a livello dell'Unione" «*si riferisce alla possibilità che l'uso dell'IA possa avere un impatto significativo sul mercato interno a causa della sua portata e con effetti negativi reali o ragionevolmente prevedibili su salute pubblica, sicurezza, diritti fondamentali o sulla società nel suo insieme, che possono essere propagati su larga scala lungo tutta la catena del valore*»[372].

In particolare, quest'ultimo impone alla Commissione di tenere conto dei seguenti criteri: il numero di parametri del modello, la qualità o la dimensione del *set* di dati, le modalità di addestramento, modalità di *input* e *output* del modello, i parametri di riferimento e le valutazioni delle capacità del modello, alto impatto del modello sul mercato, il numero di utenti finali registrati[373].

Nel caso in cui il modello soddisfi la condizione di cui sopra, il fornitore presenta, senza indugio ed entro due settimane dal soddisfacimento del requisito, un'informativa che dimostra ciò[374]. È fatta salva, la possibilità in capo al fornitore, nel caso in cui il sistema integri formalmente la condizione di cui all'art. 51, par. 1, lett. a), di presentare argomentazioni atte a dimostrare che in concreto non presenta rischi sistemici e che pertanto, non dovrebbe essere pertanto classificato come modello di IA per finalità generali con rischio sistemico[375].

---

[369] Art. 51, par. 1, lett. a).
[370] La procedura decisionale può esser avviata *ex officio* o a seguito di una segnalazione qualificata del gruppo di esperti scientifici, si veda l'art. 51 par. 1 lett. a).
[371] Art. 51, par. 1, lett. b).
[372] Camera dei deputati, *Il regolamento UE in materia di intelligenza artificiale n. 26*, Documentazione per le Commissioni attività dell'Unione Europea, 5 febbraio 2024, p. 7. [Online]. Disponibile su: https://documenti.camera.it/Leg19/Dossier/Pdf/AT026.Pdf
[373] Allegato XIII al Regolamento.
[374] Art. 52, par. 1 del Regolamento.
[375] Art. 52, par. 2 del Regolamento.

2.10. I casi di "rischio minimo o nullo": codici di condotta

Per i sistemi di IA che presentano rischi minimi o nulli non sono previsti particolari obblighi.

Il Regolamento, per questi, incoraggia l'elaborazione e l'adozione di Codici di condotta che estendono l'applicazione di alcuni dei requisiti di cui al Capo III, Sezione 2, previsti per i sistemi "ad alto rischio"[376].

L'ufficio per l'IA e gli Stati membri hanno il compito di agevolare l'elaborazione dei codici, anche per gli utilizzatori, sulla base di obiettivi chiari e indicatori di prestazione volti a misurare il conseguimento degli stessi[377]. A titolo esemplificativo, vengono indicati taluni obiettivi quali: gli elementi applicabili previsti negli orientamenti etici[378], la riduzione dell'impatto sulla sostenibilità ambientale[379], la promozione di una cultura sull'IA[380], la facilitazione di una progettazione inclusiva e diversificata dei sistemi di IA, la valutazione e la prevenzione dell'impatto negativo dei sistemi di IA sulle persone vulnerabili o sui gruppi di persone vulnerabili[381].

2.11. *Regulatory sandbox*

L'avvento dell'IA ha reso necessaria una sua regolamentazione, accompagnata dalla consapevolezza di adottare un approccio normativo innovativo. Uno strumento giuridico, figlio di quest'approccio, sono le "*Regulatory sandbox*" o "*sandbox normativa*". Questo spazio di sperimentazione garantisce «*un ambiente controllato che promuove l'innovazione e facilita lo sviluppo, l'addestramento, la sperimentazione e la convalida di sistemi di IA innovativi per un periodo di tempo limitato prima della loro immissione sul mercato o della loro messa in servizio conformemente a un piano specifico dello spazio di sperimentazione concordato tra i potenziali fornitori e l'autorità competente*»[382]. L'istituzione degli spazi deve essere affidata all'autorità competente di ciascuno Stato membro, al fine di istituirne almeno uno a livello nazionale o uno congiunto con una o più autorità competenti di altri Stati membri[383]. Dalle seguenti

[376] Art. 95, par. 1 del Regolamento.
[377] Art. 95, par. 2 del Regolamento.
[378] Art. 95, par. 2, lett. a) del Regolamento.
[379] Art. 95, par. 2, lett. b) del Regolamento.
[380] Art. 95, par. 2, lett. c) del Regolamento.
[381] Art. 95, par. 2, lett. e) del Regolamento.
[382] Art. 57, par. 5 del Regolamento.
[383] Art. 57, par. 1 del Regolamento.

informazioni, è possibile dedurre, innanzitutto, che la *sandbox* normativa può essere multi-giurisdizionale, cioè, in comune con più Stati Membri e che opera per un periodo di tempo limitato, secondo determinati parametri di prova contenuti in un piano specifico. I vari fornitori, intenzionati a testare i loro sistemi in questi spazi, dovranno presentare apposita domanda contente l'illustrazione del rispetto dei criteri di ammissibilità alla *sandbox* determinati dalla Commissione[384]. Una volta ammessi, i fornitori si atterrano agli orientamenti delle autorità competenti sulle aspettative normative e sulle modalità per soddisfare i requisiti e gli obblighi di cui al presente regolamento[385]. Le attività svolte con successo all'interno dello spazio possono esser certificate dall'autorità competente, a mezzo di prova scritta, su richiesta del fornitore di sistema IA[386]. Al termine del periodo di partecipazione allo spazio di sperimentazione l'autorità fornirà, inoltre, una relazione di uscita che illustrerà nel dettaglio le attività svolte, i relativi risultati e le conclusioni dell'apprendimento[387]. Le documentazioni ottenute saranno utilizzabili dai fornitori per dimostrare la conformità al Regolamento.

L'istituzione delle *regulatory sandbox* è finalizzata al perseguimento degli obiettivi di: miglioramento della certezza del diritto, al fine di conseguire la conformità normativa al presente regolamento; condivisione delle migliori pratiche attraverso la cooperazione delle autorità coinvolte; promozione dell'innovazione, della competitività e dello sviluppo di un ecosistema di IA; contribuzione all'apprendimento normativo basato su dati concreti; accelerazione al processo di accesso al mercato dei sistemi di IA, in particolare se il fornitore è una PMI[388].

2.12. La *governance*

Il Regolamento prevede, al Capo VII, un sistema di *governace* articolato su due livelli: europeo e nazionale. Il modello di amministrazione prescelto per la *governance* è quello dell'amministrazione indiretta, in quanto, benché il Regolamento abbia previsto la

[384] Art. 58, par. 1 del Regolamento.
[385] Art. 57, par. 7 del Regolamento.
[386] Art. 57, par. 7 del Regolamento.
[387] Ibidem.
[388] Art. 57, par. 9, lett. a) – lett. e).

creazione di un Comitato europeo, sono stati attribuiti alle autorità statali i poteri di controllo circa l'attuazione e applicazione del Regolamento[389].

Al livello UE, il Regolamento istituisce il Comitato europeo per l'Intelligenza artificiale composto da un rappresentante per ciascuno Stato membro avente diritto di voto e dal Garante europeo della protezione dei dati e l'Ufficio per l'IA come osservatori senza partecipare alle votazioni[390]. La designazione del rappresentante, a cura del rispettivo Stato membro, per un periodo di tre anni, avviene tenuto conto delle competenze richieste per lo svolgimento dell'incarico[391] e al fine di fungere da punto di contatto unico nei confronti del Comitato[392] e di agevolare la coerenza e il coordinamento tra le autorità nazionali competenti nel rispettivo Stato membro[393].

Il Comitato svolge funzioni di consulenza e assistenza alla Commissione e agli Stati membri al fine di facilitare l'applicazione coerente ed efficace del Regolamento attraverso: lo svolgimento di un ruolo di coordinamento tra autorità nazionali competenti e le autorità di vigilanza del mercato interessate; la raccolta e condivisione tra gli Stati membri conoscenze e migliori pratiche tecniche e normative; la consulenza sull'attuazione del regolamento in particolare sui modelli IA per finalità generali; il contributo all'armonizzazione delle pratiche amministrative negli Stati membri; la formulazione di raccomandazioni e pareri scritti su qualsiasi questione pertinente attuazione applicazione del regolamento[394]. Il Comitato, dunque, non si trova in una posizione di supremazia rispetto alle autorità nazionali ed è sprovvisto del potere di porre in esser atti giuridicamente vincolanti, sebbene, le raccomandazioni e i pareri svolgano un ruolo cruciale per la tenuta unitaria del sistema[395]. Sono stati previsti anche: un Ufficio europeo sull'IA, istituto all'interno della Commissione come centro di competenza in materia di IA, nonché, base per un unico sistema europeo di *governance* dell'IA[396]; un

[389] CASONATO C., MARCHETTI B., *Prime osservazioni sulla proposta di regolamento della Commissione Ue in materia di intelligenza artificiale*, in "BioLaw Journal - Rivista di BioDiritto", 2021, n. 3, pp. 415-437, p. 23.
[390] Art. 65, par. 2 del Regolamento.
[391] Art. 65, par. 2-3 del Regolamento.
[392] Art. 65, par. 4, lett. b) del Regolamento.
[393] Art. 65, par. 4, lett. c) del Regolamento.
[394] Art. 66 del Regolamento.
[395] CASONATO C., MARCHETTI B., *Prime osservazioni sulla proposta di regolamento della Commissione Ue in materia di intelligenza artificiale*, in "BioLaw Journal - Rivista di BioDiritto", 2021, n. 3, pp. 415-437, pp. 24- 25.
[396] Art. 64 del Regolamento.

Gruppo di esperti scientifici indipendenti finalizzato a sostenere le attività di esecuzione a norma del presente regolamento[397].

A livello nazionale ciascuno Stato, ai sensi del Regolamento, istituisce almeno un'autorità di notifica e un'autorità di vigilanza del mercato. Le autorità hanno l'obbligo di esercitare i loro poteri in modo indipendente, imparziale e senza pregiudizi, in modo da salvaguardare i principi di obiettività delle loro attività e dei loro compiti[398]. L'autorità di notifica, prevista all'art. 28, è «*responsabile della predisposizione e dell'esecuzione delle procedure necessarie per la valutazione, la designazione e la notifica degli organismi di valutazione della conformità e per il loro monitoraggio*»[399]. In particolare, avrà il compito di valutare se gli organismi, da cui ha ricevuto domanda di notifica, siano idonei a effettuare una valutazione di conformità sui tipi di sistemi di IA per i quali dichiarano di essere competenti[400]. L'idoneità di un organismo è data dal soddisfacimento di requisiti organizzativi, di gestione della qualità e relativi alle risorse e ai processi necessari all'assolvimento dei loro compiti, nonché, dei requisiti di cibersicurezza[401].

Per quanto riguarda l'Autorità di vigilanza del mercato, è incaricata di svolgere attività di monitoraggio successiva all'immissione sul mercato mediante *audit* e offrendo ai fornitori la possibilità di segnalare incidenti o violazioni gravi degli obblighi in materia di diritti fondamentali di cui sono venuti a conoscenza.

Attualmente, sebbene il regolamento sia stato approvato definitivamente[402], l'Italia non ha provveduto ancora a designare, una o più, autorità competenti a svolgere funzioni di vigilanza. Con comunicato stampa del 25 marzo 2024, il Garante della *privacy* si è candidata ad assumere il ruolo di autorità nazionale competente affermando che «*la designazione dell'autorità per la protezione dati come autorità nazionale di controllo assicurerebbe (...) un approccio normativo più armonizzato e contribuirebbe all'adozione di un'interpretazione coerente delle disposizioni in materia di trattamento*

[397] Art. 68, par. 1 del Regolamento.
[398] Art. 70, par. 1 del Regolamento.
[399] Art. 28, par. 1 del Regolamento.
[400] Art. 29, par. 2 del Regolamento.
[401] Art. 31, par. 2 del Regolamento.
[402] Si veda nota 277.

dei dati nonché a evitare contraddizioni nella loro applicazione nei diversi Stati membri»[403].

2.13. La banca dati sull'IA

Tra i vari obblighi del fornitore, antecedenti all'immissione nel mercato del sistema di IA "ad alto rischio", figura l'obbligo di registrazione nella banca dati. Quest'ultima, è istituita e gestita dalla Commissione in collaborazione con gli Stati membri, dovrà contenere tutte le informazioni di cui ai par. 2 e 3 relative ai sistemi di IA "ad alto rischio" di cui all'art. 6, par. 2[404]. Le informazioni contenute nella banca dati dell'UE, registrate a norma dell'art. 49, sono accessibili e disponibili al pubblico in modo facilmente fruibile. La funzione dell'archivio è consentire la pubblicità e la sorveglianza dei sistemi circolanti nell'Unione per facilitare l'attività delle istituzioni competenti e per informare il pubblico, in virtù, del principio di accessibilità delle informazioni in esso contenute[405] [406]. La Commissione, quale gestore della banca dati, sarà anche titolare del trattamento dei dati personali contenuti nel sistema: nomi e dati di contatto delle persone fisiche responsabili della registrazione[407]. In merito a questo aspetto, in dottrina sono stati sollevati dei dubbi sul se la registrazione determini la conoscibilità di tutte le informazioni date dal fornitore oppure solamente della dichiarazione di conformità e il numero identificativo dell'organismo certificatore quando previsto[408].

2.14. Gli strumenti di *enforcement*

Il Regolamento, all'art. 99, demanda agli Stati membri la determinazione delle regole, relative alle sanzioni e ad altre misure di esecuzione, tra cui avvertimenti e misure non

[403] Garante per la protezione dei dati personali, *Segnalazione al Parlamento e al Governo sull'Autorità per l'IA*, 25 marzo 2024. [Online]. Disponibile su: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9996493
[404] Art. 71, par. 1 del Regolamento.
[405] CASONATO C., MARCHETTI B., *Prime osservazioni sulla proposta di regolamento della Commissione Ue in materia di intelligenza artificiale*, in "BioLaw Journal - Rivista di BioDiritto", 2021, n. 3, pp. 415-437, par. 7.
[406] Art. 71, par. 4 del Regolamento.
[407] Art. 71, par. 6 del Regolamento.
[408] CASONATO C., MARCHETTI B., *Prime osservazioni sulla proposta di regolamento della Commissione Ue in materia di intelligenza artificiale*, in "BioLaw Journal - Rivista di BioDiritto", 2021, n. 3, pp. 415-437, par. 7.

pecuniare[409], nel rispetto delle condizioni e dei termini fissati dal Regolamento. L'autorità di sorveglianza, occupandosi del monitoraggio successivo all'immissione, ogni qualvolta rilevi una difformità dei sistemi di IA con i requisiti imposti dal Regolamento, potrà adottare misure idonee a garantire il rispetto della normativa nei confronti del soggetto interessato.

I criteri per la determinazione delle sanzioni variano a seconda della tipologia di violazione e devono esser improntati sulla base dei principi di effettività, proporzionalità e dissuasività.

La violazione al divieto delle pratiche di IA vietate di cui all'art. 5 è soggetta a sanzioni amministrative pecuniarie fino a 35 000 000 di euro o, se l'autore del reato è un'impresa, fino al 7 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore[410].

La non conformità di un sistema IA a qualsiasi delle disposizioni connesse a operatori o organismi notificati, diverse da quelle di cui all'art. 5 o la violazione degli obblighi dei fornitori[411], rappresentanti[412], importatori[413], distributori[414], utilizzatori[415], organismi notificati[416], di trasparenza dei fornitori[417], è soggetta, invece, a una sanzione amministrativa che può arrivare fino a 15 000 000 di euro o, se l'autore del reato è un'impresa, fino al 3 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore[418].

Nei casi in cui la violazione si traduca nella «*fornitura di informazioni inesatte, incomplete o fuorvianti agli organismi notificati o alle autorità nazionali competenti per dare seguito a una richiesta è soggetta a sanzioni amministrative pecuniarie fino a 500000 euro o, se l'autore del reato è un'impresa, fino all'1 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore*»[419].

Definiti i limiti all'entità della sanzione, nel determinare l'importo del singolo caso, si dovrà tener conto delle circostanze specifiche quali: la natura; la gravità e la durata della

[409] Ad esempio: ordinare il ritiro del sistema di IA dal mercato o richiamarlo per un periodo di tempo in ragione della gravità della violazione.
[410] Art. 99, par. 3 del Regolamento.
[411] Art. 16 del Regolamento.
[412] Art. 22 del Regolamento.
[413] Art. 23 del Regolamento.
[414] Art. 24 del Regolamento.
[415] Art. 26 del Regolamento.
[416] Art. 31 del Regolamento.
[417] Art. 50 del Regolamento.
[418] Art. 99, par. 4 del Regolamento.
[419] Art. 99, par. 5 del Regolamento.

violazione e delle sue conseguenze; il numero di persone interessate e il livello del danno da esse subito; se sono state irrogate da autorità di vigilanza di altri Stati membri sanzioni allo stesso operatore per la stessa violazione o per violazioni di altre normative dell'Unione o nazionali, qualora tali violazioni derivino dalla stessa attività o omissione che costituisce una violazione pertinente del presente regolamento; le dimensioni; il fatturato annuo e la quota di mercato dell'operatore che ha commesso la violazione; eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione; il grado di cooperazione con le autorità nazionali competenti per rimediare alla violazione e attenuarne i possibili effetti negativi; il grado di responsabilità dell'operatore, tenuto conto delle misure tecniche e organizzative attuate; il modo in cui le autorità nazionali competenti sono venute a conoscenza della violazione, in particolare se e in che misura è stata notificata dall'operatore; il carattere doloso o colposo della violazione; l'eventuale azione intrapresa dall'operatore per attenuare il danno subito dalle persone interessate a seguito della condotta dannosa[420].

Accanto agli strumenti di *enforcement* previsti in caso di violazioni dei privati, all'art. 100, è stato attribuito il potere al Garante europeo della protezione dei dati di infliggere sanzioni amministrative pecuniarie alle istituzioni, agli organi e agli organismi dell'Unione che rientrano nell'ambito di applicazione del presente regolamento, secondo le modalità previste per l'irrogazione contro privati, ma con massimali molto meno elevati[421].

Ultimo aspetto di rilievo, oltre alla previsione di una disciplina sanzionatoria *ad hoc* per l'lA con finalità generali[422], la previsione del diritto alla difesa e quindi, dei suoi corollari durante il procedimento amministrativo. Sebbene venga menzionato esplicitamente il solo diritto al fascicolo, si ritiene che il destinatario del procedimento sia titolare di tutti diritti[423] che discendono dal più generale principio di buona amministrazione, anche alla luce della disamina fatta sul punto nel Cap. I.

[420] Art. 99, par. 7, lett. a) – j) del Regolamento.
[421] Art. 99, par. 2 – 4 del Regolamento.
[422] Art. 101 del Regolamento.
[423] Art. 99, par. 5 del Regolamento.

3. La proposta di direttiva sulla responsabilità dell'intelligenza artificiale: obiettivi e opzioni giuridiche prescelte

La Commissione europea, alla luce della Risoluzione del Parlamento europeo del 20 ottobre 2020, ha approvato una proposta di direttiva sulla responsabilità extracontrattuale per i danni causati dai sistemi di IA[424]. La proposta va ad integrare il quadro normativo, già composto dal Regolamento sull'intelligenza artificiale, posizionandosi nella fase patologica del funzionamento di un sistema IA, cioè, dopo il verificarsi di un eventuale danno. D'altro canto, il Regolamento, collocato nella fase fisiologica, è finalizzato a prevenire le conseguenze dannose che potrebbero discendere dall'uso dell'IA, quindi, a garantire che il suo impiego avvenga in completa sicurezza.

La proposta nasce data l'incapacità delle attuali norme nazionali sulla responsabilità, basate sulla colpa, di far fronte a richieste di risarcimento, per danni causati da prodotti e servizi basati sull'intelligenza artificiale[425]. Le caratteristiche tipiche dell'IA, quali l'estrema complessità, l'autonomia, l'opacità (*black box problem*) renderebbero costoso e complesso, per la vittima, identificare il responsabile, l'azione o l'omissione illecita ed il nesso di causalità. Per questo motivo, il danneggiato potrebbe desistere dal chiedere un risarcimento in ragione di costi iniziali molto elevati e procedimenti legali molto lunghi, rispetto ai casi che non coinvolgono l'IA[426].

L'ambito di applicazione della proposta riguarda i solo giudizi civili promossi dinanzi a giudici nazionali per ottenere il risarcimento del danno causato da un sistema di IA[427] e detta regole comuni sui mezzi di prova riguardanti i sistemi di IA "ad alto rischio"[428], nonché, sull'onere della prova[429].

Date le difficoltà nel soddisfare l'onere della prova, la Proposta prevede il diritto, in capo al danneggiato, di chiedere al giudice un ordine di esibizione, al fornitore[430] o all'utente, di informazioni e documenti sul sistema di IA, "ad alto rischio", potenzialmente

---

[424] Commissione europea, *Proposta di Direttiva del Parlamento europeo e del Consiglio sull'adeguamento delle norme sulla responsabilità civile extracontrattuale all'intelligenza artificiale (direttiva sulla responsabilità civile IA)*, 28 settembre 2022. [Online]. Disponibile su: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A0496%3AFIN

[425] Commissione europea, *Proposta di Direttiva del Parlamento europeo e del Consiglio sull'adeguamento delle norme sulla responsabilità civile extracontrattuale all'intelligenza artificiale (direttiva sulla responsabilità civile IA)*, 28 settembre 2022, par. 1 della relazione esplicativa.

[426] Ibidem.

[427] Art. 1, par. 1, lett. b) della Proposta di direttiva sulla responsabilità dell'IA.

[428] Art. 1, par. 1, lett. a) della Proposta di direttiva sulla responsabilità dell'IA.

[429] Art. 1, par. 1, lett. b) della Proposta di direttiva sulla responsabilità dell'IA.

[430] O anche ad una persona soggetta agli obblighi del fornitore secondo il Regolamento.

responsabile[431]. All'interno della richiesta di esibizione, il futuro attore dovrà dimostrare di aver compiuto ogni sforzo proporzionato per ottenere tali elementi di prova dal convenuto[432], oltre a dimostrare il fondato sospetto del danno subito. Nel caso di mancata esecuzione dell'ordinanza di esibizione, viene prevista una presunzione circa la non conformità ad un obbligo del fornitore in relazione a cosa gli elementi di prova richiesti erano tesi a dimostrare[433].

La divulgazione degli elementi di prova è limitata, dal giudice, a quanto necessario e proporzionato per sostenere una domanda di risarcimento tenuto conto dei legittimi interessi di tutte le parti, specialmente in relazione alla protezione dei segreti commerciali[434].

Il secondo rimedio processuale, previsto a favore dell'attore, è la presunzione relativa al nesso di causalità tra la colpa del convenuto e l'*output* prodotto da un sistema IA o la mancata produzione di un *output* da parte di tale sistema se sono soddisfatte le seguenti condizioni: l'attore ha dimostrato o il giudice ha presunto la colpa del convenuto, consistente nella non conformità a un obbligo di diligenza previsto per evitare il danno verificatesi; sia ragionevolmente probabile l'influenza del comportamento colposo sull'*output* o sul mancato *output*, l'attore ha dimostrato che il danno è stato causato dall'*output* o dalla mancata produzione dello stesso[435].

Per quanto riguarda i sistemi "ad alto rischio", se la domanda di risarcimento è presentata contro il fornitore del sistema di IA, la violazione rilevante sarà quella derivante dal mancato rispetto dei requisiti[436] imposti per tali sistemi o la violazione degli obblighi del fornitore.

---

[431] Art. 3, par. 1 della Proposta di direttiva sulla responsabilità dell'IA.
[432] Art. 3, par. 3 della Proposta di direttiva sulla responsabilità dell'IA.
[433] Art. 3, par. 5 della Proposta di direttiva sulla responsabilità dell'IA.
[434] Art. 3, par. 4 della Proposta di direttiva sulla responsabilità dell'IA.
[435] Art. 4, par. 1 della Proposta di direttiva sulla responsabilità dell'IA.
[436] I requisiti sono indicati all'art. 4, par. 2 della Proposta: «*(...)(a) il sistema di IA è un sistema che utilizza tecniche che prevedono l'uso di dati per l'addestramento di modelli e che non è stato sviluppato sulla base di set di dati di addestramento, convalida e prova che soddisfano i criteri di qualità di cui; b) il sistema di IA non è stato progettato e sviluppato in modo da soddisfare gli obblighi di trasparenza; (c) il sistema di IA non è stato progettato e sviluppato in modo da consentire una supervisione efficace da parte di persone fisiche durante il periodo in cui il sistema di IA è in uso; (d) il sistema di IA non è stato progettato e sviluppato in modo da conseguire, alla luce della sua finalità prevista, un adeguato livello di accuratezza, robustezza e cibersicurezza; oppure(e) non sono state immediatamente adottate le azioni correttive necessarie per rendere il sistema di IA conforme ai requisiti o per ritirarlo o richiamarlo, a seconda dei casi*».

Nel caso in cui la domanda sia presentata contro un utente di un sistema di IA "ad alto rischio", la non conformità a un obbligo di diligenza consisterà: in utilizzo improprio, rispetto alle istruzioni per l'uso, di un sistema di IA o un cattivo monitoraggio; in un'esposizione del sistema a dati di *input* sotto il suo controllo che non sono pertinenti alla luce della finalità prevista dal sistema[437].

A differenza dell'*AI Act*, la disciplina, essendo contenuta all'interno di una direttiva, richiederà un intervento normativo di recepimento degli Stati membri. Quest'ultimi, saranno tenuti a modificare l'impianto normativo vigente in conformità con le previsioni dettate dalla Proposta, fatta salva la possibilità di adottare o mantenere in vigore norme nazionali più favorevoli all'attore[438].

Attualmente, la direttiva non è ancora stata approvata, essendo in corso la prima lettura al Consiglio dell'Unione.

4. L'*AI Pact*: uno strumento per adeguarsi all'entrata in vigore del Regolamento

Come è noto, con l'adozione del Regolamento non consegue la sua applicabilità, in quanto una parte delle disposizioni saranno applicabili da sei mesi dall'entrata in vigore, (alcuni requisiti dei sistemi di IA "ad alto rischio") altre solo dopo un anno, mentre, altre ancora dopo due.

Per agevolare l'adeguamento dei sistemi già esistenti alla normativa, la Commissione ha deciso di permettere al settore di anticipare il processo di conformità alle regole comunitarie incentivandone l'adeguamento volontario.

Il processo di adesione volontaria inizierà a breve data la recente approvazione del Regolamento[439].

Il Patto avrà come obiettivo quello di incoraggiare a comunicare volontariamente i processi e le pratiche che verranno messe in atto per garantire la progettazione, lo sviluppo e l'utilizzo di un'IA affidabile[440]. In particolare, si vuole creare una *community* interessata ad aprire un dialogo diretto con la Commissione per orientare le decisioni commerciali in

[437] Art. 4, par. 3 della Proposta di direttiva sulla responsabilità dell'IA.
[438] Art. 1, par. 4 della Proposta di direttiva sulla responsabilità dell'IA.
[439] *Come funziona l'AI Pact, il patto per anticipare le regole europee sull'intelligenza artificiale*, in Wired, il 19 aprile 2024. [Online]. Disponibile su: https://www.wired.it/article/ai-pact-ai-act-europa-regole-aziende/
[440] Si consulti la sezione delle politiche dell'unione sull'*AI Pact* rinvenibile al sito: https://digital-strategy.ec.europa.eu/it/policies/ai-pact

attesa dell'entrata in vigore della normativa. I pareri richiesti e ottenuti dalla Commissione, sebbene non vincolanti, costituiranno un'interpretazione anticipata del Regolamento con un valore nettamente superiore rispetto a quella che potrà dare un professionista del settore.

L'adesione è condizionata a delle dichiarazioni di impegno a lavorare per adeguarsi alle disposizioni, con una descrizione delle misure che si intendono adottare, anche attraverso un approccio graduale[441]. Per incentivare le imprese ad aderire all'*AI Pact*, le dichiarazioni di impegno saranno pubblicate al fine di accrescere la fiducia nelle tecnologie delle imprese che partecipano al Patto.

I vantaggi del Patto per i partecipanti saranno molteplici: incentivare lo sviluppo di una consapevolezza comune sugli obiettivi dell'*AI Pact*; adottare misure effettive per prepararsi al cambiamento derivante dalla futura attuazione del Regolamento; render note le garanzie messe in atto per aumentare la credibilità e creare un clima di fiducia verso l'IA; agevolare le imprese tecnologiche nelle scelte di impresa attraverso pareri forniti dalla Commissione[442].

5. Quale tipo di "rischio" presentano i sistemi di intelligenza artificiale applicati alla vigilanza bancaria?

L'analisi del Regolamento sull'intelligenza artificiale, effettuata in questo capitolo, si è resa necessaria, in quanto l'elaborato ha come oggetto l'indagine sui possibili risvolti giuridici derivanti dallo svolgimento dell'attività di supervisione bancaria coadiuvata dall'IA. L'impiego delle nuove tecnologie da parte della BCE, durante la sua attività amministrativa, deve avvenire nel rispetto del diritto ad una buona amministrazione sancito all'art. 41 della Carta di Nizza, ma anche nel rispetto del Regolamento sull'intelligenza artificiale. Infatti, l'ambito di applicazione di quest'ultimo, investe sia soggetti privati che pubblici come la BCE. Alla luce di ciò, occorrerà valutare in quale fascia di rischio rientrano i vari sistemi di IA che assistono l'autorità di vigilanza e assoggettare ciascuno al regime normativo adatto. L'elaborato costituisce uno dei primi

[441] Ibidem.
[442] Ibidem.

lavori accademici[443] aventi l'ambizione di tentare di classificare, sulla base del *risk-based approach*, i sistemi di IA, sebbene il Regolamento entrerà in vigore fra due anni.

L'individuazione della tipologia di rischio presuppone, in via preliminare, una riflessione sulla finalità generale che intende perseguire l'utilizzatore di tali sistemi, nel caso di specie: la vigilanza degli istituti bancari rientranti nel MVU. La vigilanza ha come obiettivi quelli di salvaguardare la sicurezza e la solidità del sistema bancario europeo, accrescere l'integrazione e la stabilità finanziaria ed assicurare una vigilanza coerente[444]. In dottrina[445], ci si è chiesti, innanzitutto, se l'utilizzo dell'IA nella vigilanza bancaria potesse configurarsi quale eccezione ai sensi dell'art. 2, par. 3. Ai sensi di quest'ultimo, il Regolamento non si applica: «*se e nella misura in cui sono immessi sul mercato, messi in servizio o utilizzati con o senza modifiche esclusivamente per scopi militari, di difesa o di sicurezza nazionale, indipendentemente dal tipo di entità che svolge tali attività*». Preso atto di ciò, ci si è domandati se fosse ragionevole ritenere che i sistemi di IA in questione concorrano al mantenimento della sicurezza nazionale nella misura in cui assicurano la salvaguardia della vita sociale ed economica delle persone. La riflessione si è conclusa nel senso di ritenere "azzardata" l'equiparazione dell'interesse pubblico perseguito dalla BCE durante l'attività di vigilanza, a quello della sicurezza nazionale di tipo militare. In realtà, l'attività di vigilanza della BCE non ricadrebbe all'interno dell'ambito di applicazione dell'eccezione, in quanto la "sicurezza nazionale" è una materia di esclusiva competenza degli Stati membri ai sensi dell'art. 4, par. 2, TUE, quindi, non può riguardare un'istituzione dell'Unione come la BCE. Al massimo, l'eccezione potrebbe esser applicata ai sistemi utilizzati dalle autorità nazionali di vigilanza, anche se è noto, che gli spazi di manovra di quest'ultime sono frutto di un mero "decentramento amministrativo", essendo la BCE titolare della competenza esclusiva in materia di vigilanza[446]. Per quanto riguarda l'impiego nell'ambito della vigilanza macroprudenziale, l'obiettivo di scongiurare un rischio sistemico potrebbe configurarsi

---

[443] Il primo tentativo è stato effettuato da: RINGE W.G. *et al*., *Navigating the Legal Landscape of AI-Enhanced Banking Supervision: Protecting EU Fundamental Rights and Ensuring Good Administration,* European Banking Institute Working Paper Series 2023 - no. 140, 2023, Cap. IV, sez. B, par. 2, lett. i).

[444] Le finalità sono indicate sul sito della BCE rinvenibile all'indirizzo: https://www.bankingsupervision.europa.eu/about/thessm/html/index.it.html#:~:text=Le%20principali%20finalit%C3%A0%20della%20vigilanza,assicurare%20una%20vigilanza%20coerente

[445] RINGE W.G. *et al*., *Navigating the Legal Landscape of AI-Enhanced Banking Supervision: Protecting EU Fundamental Rights and Ensuring Good Administration,* European Banking Institute Working Paper Series 2023 - no. 140, 2023, Cap. IV, sez. B, par. 2, lett. i).

[446] Per maggiori approfondimenti sul punto si veda il Cap. I, par. 2.1.

come una questione di sicurezza nazionale e quindi, rientrare nell'ambito di applicazione dell'eccezione. Inoltre, spettando la competenza in via principale alle autorità nazionali, non si porrebbero i problemi sollevati per la vigilanza microprudenziale. In ogni caso, sono necessari dei chiarimenti su cosa il legislatore europeo abbia voluto intendere con il termine "sicurezza nazionale".

Esclusa l'applicabilità dell'eccezione[447], occorre valutare che tipo di rischio presentano i sistemi impiegati dalla BCE alla luce dei compiti di vigilanza microprudenziale, di cui all'art. 4 del Regolamento 1024/2013. La valutazione deve esser condotta caso per caso. Ad esempio, *Heimdall* è un sistema che valuta i requisiti di professionalità e onorabilità degli organi direttivi delle istituzioni significative in uso da giugno 2022. Tale IA potrebbe rientrare all'interno del par. 4, lett. a) dell'Allegato III che afferma che sono sistemi "ad alto rischio" quelli destinati a essere utilizzati per la selezione di persone fisiche, in particolare per analizzare o filtrare le candidature e valutare i candidati. Il sistema di *sentiment analysis* che consente alle autorità di vigilanza di valutare come l'istituto sottoposto a vigilanza è percepito dal pubblico potrebbe rientrare all'interno del par. 1, lett. c) dell'Allegato III, in quanto sistema utilizzato per il riconoscimento delle emozioni. È ragionevole ritenere che tra i sistemi "ad alto rischio" rientri anche il sistema di "allerta precoce" per gli istituti meno significativi in quanto volto a valutare i casi di "sofferenza finanziaria", quindi, analogo a quelli, previsti al par. 5, lett. a) dell'Allegato III, volti a valutare l'affidabilità creditizia delle persone fisiche o per stabilire il loro merito di credito.

I rischi per i diritti fondamentali sono più accentuati quando l'IA viene utilizzata, ai sensi del par. 8, lett. a) dell'Allegato III, per la ricerca e l'interpretazione dei fatti e del diritto e nell'applicazione della legge. Sebbene l'ipotesi si riferisca ai procedimenti giudiziari, è ragionevole ritenere che faccia riferimento anche ai procedimenti amministrativi. Un esempio, è *Truffle Search Analytics* per documenti di testo strutturati in quanto finalizzato alla ricerca di informazioni (fatti) tra le diverse decisioni SREP e a semplificare l'identificazione di tendenze emergenti e gruppi di rischi.

Il Regolamento, secondo quanto affermato nella relazione, si prefigge quale obiettivo generale quello di assicurare il buon funzionamento del mercato interno per i sistemi di IA, proponendo un quadro giuridico per un'IA affidabile. Uno dei sette requisiti che deve

[447] È esclusa certamente per i sistemi di IA impiegati nella vigilanza microprudenziale.

avere un IA affidabile, secondo la Comunicazione della Commissione del 8 aprile 2019[448], è la trasparenza che impone ai fornitori di progettare e sviluppare sistemi di IA in modo tale da garantire che gli utilizzatori siano in grado di comprendere l'*output* e utilizzarlo adeguatamente[449].

La trasparenza è assicurata, principalmente, dal documento sulle istruzioni per l'uso contenente informazioni concise, complete, corrette e chiare, pertinenti, accessibili e comprensibili agli utilizzatori. Sebbene all'interno del documento, le divulgazioni forniscano informazioni privilegiate sul se il sistema di intelligenza artificiale possa esser adatto per l'obiettivo che intende perseguire l'utilizzatore, tali informazioni saranno solo raramente comprensibili e fruibili per gli utenti, non aventi una formazione minima nello sviluppo o nella pratica del *machine learning*[450]. La trasparenza, in questione, potrebbe essere descritta come trasparenza "da parte di esperti per esperti"[451]. Inoltre, non vengono fornite indicazioni specifiche sul funzionamento interno del sistema, ma si limitano semplicemente alla descrizione del tipo specifico o alla descrizione di caratteristiche tecniche o metriche. Per concludere, il Regolamento mira a garantire una trasparenza tecnica e non una funzionale all'esercizio dei diritti di difesa. L'obiettivo dei requisiti di trasparenza è finalizzato a far comprendere al potenziale utilizzatore le modalità d'impiego del sistema, oltre che ad agevolare il controllo dell'autorità competente.

Appurato che la vigilanza bancaria coadiuvata dall'IA rientra nell'ambito di applicazione dell'*AI Act*, è necessario prendere atto che la BCE può rivestire contemporaneamente il ruolo di utilizzatore e di fornitore con il conseguente assoggettamento a tutti gli obblighi che ne discendono. È questo il caso in cui la BCE decida di sviluppare sistemi di IA internamente e metterli sul mercato o in servizio con il proprio nome o marchio. L'adempimento della BCE agli obblighi previsti per i fornitori potrebbe incidere sulla sua indipendenza intesa come un agire «*senza chiedere né ricevere istruzioni da parte di istituzioni od organismi dell'Unione, dai governi degli Stati membri o da altri soggetti pubblici o privati*»[452]. Nel caso di specie, l'indipendenza potrebbe esser minata dal

[448] Si veda la nota 265.
[449] Art. 13, par. 1 del Regolamento.
[450] HACKER P., PASSOTH J.-H., *Varieties of AI Explanations Under the Law. From the GDPR to the AIA, and Beyond*, in Andreas Holzinger and others (eds), xxAI - Beyond Explainable AI, 2022, p. 359-362. [Online]. Disponibile su: https://link.springer.com/chapter/10.1007/978-3-031-04083-2_17
[451] Ibidem.
[452] Art. 19, par. 1 del Regolamento (UE) n. 1024/2013.

Garante europeo della protezione dei dati che agisce in qualità di autorità di vigilanza del mercato, nei casi in cui le istituzioni, gli organi e gli organismi dell'Unione rientrano nell'ambito di applicazione del presente regolamento[453]. In particolare, il rischio risiederebbe sul modo in cui la BCE svolge i propri compiti di vigilanza, nella misura in cui la supervisione del Garante non sarebbe strettamente limitata a un adeguato controllo della *governance* dell'IA[454]. La problematica è stata sollevata anche dalla stessa BCE, con il Parere sulla proposta di Regolamento sull'IA, affermando che: «*qualsiasi eventuale vigilanza della BCE da parte del GEPD e delle BCN da parte delle autorità nazionali competenti sarebbe limitata a controlli adeguati su un sistema di IA e sulla governance del sistema stesso e non sarebbe in alcun modo intesa a pregiudicare la capacità della BCE e delle BCN di svolgere in modo indipendente i compiti loro attribuiti dal trattato*»[455].

Viceversa, nel caso in cui la BCE delegasse lo sviluppo di modelli IA a fornitori privati, i rischi risiederebbero nell'affidamento, a soggetti diversi dalle istituzioni previste all'interno dei Trattati, della definizione delle metodologie e del *modus operandi* dell'attività di vigilanza, data l'impossibilità di contestare o rimodulare l'*output* generato dall'IA[456]. L'affidamento a terzi potrebbe comportare, quindi, da un lato, un rischio per la sua indipendenza[457] in quanto si demanderebbe a tali organizzazioni la definizione delle metodologie di azione della prassi di vigilanza, con l'annessa difficoltà di valutare i

[453] Art. 74, par. 9 del Regolamento sull'IA.

[454] RINGE W.G. *et al.*, *Navigating the Legal Landscape of AI-Enhanced Banking Supervision: Protecting EU Fundamental Rights and Ensuring Good Administration*, European Banking Institute Working Paper Series 2023 - no. 140, 2023, Cap. IV, sez. B, par. 2, lett. i).

[455] BCE, *Parere della Banca centrale europea del 29 dicembre 2021 su una proposta di regolamento che stabilisce norme armonizzate in materia di intelligenza artificiale*, 29 dicembre 2021, par. 2.4. [Online]. Disponibile su: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=OJ:C:2022:115:FULL&from=MT

[456] RINGE W.G. *et al.*, *Navigating the Legal Landscape of AI-Enhanced Banking Supervision: Protecting EU Fundamental Rights and Ensuring Good Administration*, European Banking Institute Working Paper Series 2023 - no. 140, 2023, Cap. IV, sez. B, par. 2, lett. i).

[457] Il principio è sancito all'art. 130 TFUE che recita: «Nell'esercizio *dei poteri e nell'assolvimento dei compiti e dei doveri loro attribuiti dai trattati e dallo statuto del SEBC e della BCE, né la Banca centrale europea né una banca centrale nazionale né un membro dei rispettivi organi decisionali possono sollecitare o accettare istruzioni dalle istituzioni, dagli organi o dagli organismi dell'Unione, dai governi degli Stati membri né da qualsiasi altro organismo. Le istituzioni, gli organi e gli organismi dell'Unione nonché i governi degli Stati membri si impegnano a rispettare questo principio e a non cercare di influenzare i membri degli organi decisionali della Banca centrale europea o delle banche centrali nazionali nell'assolvimento dei loro compiti*».

risultati dell'IA da parte dei supervisori e dall'altro, una delega dei poteri di vigilanza in violazione della dottrina Meroni[458].

Quest'ultima sancisce un divieto di «*delega di poteri discrezionali ad organi diversi da quelli che il Trattato ha istituito per esplicarli o controllarne l'esercizio nell'ambito delle loro rispettive attribuzioni*»[459]. Il divieto della delega copre «*il potere discrezionale che comporti una ampia libertà di valutazione ed atto ad esprimere*»[460] e non «*poteri d'esecuzione nettamente circoscritti ed il cui esercizio può per ciò stesso venir rigorosamente controllato in base a criteri obbiettivi stabiliti dall'autorità delegante*»[461]. Nel caso di *specie*, come già ampiamento ribadito[462], trattandosi di un'attività discrezionale, lo svolgimento di fasi dell'attività demandato a soggetti esterni potrebbe porsi in contrasto con la dottrina Meroni. Diversamente, nel caso in cui la BCE, ricoprisse anche il ruolo di fornitore, non sussisterebbe alcun contrasto con la sopracitata dottrina.

Un ulteriore motivo di preoccupazione, legato all'affidamento dello sviluppo a fornitori esterni, è il rischio di dipendenza dalle grandi aziende tecnologiche. Da tale fenomeno discenderebbero almeno due conseguenze: possibili pregiudizi economici, derivanti dalla concentrazione del mercato, all'innovazione e al dinamismo economico; rischi per la stabilità finanziaria, operativi e reputazionali, nei casi di guasti di sistema o attacchi informatici ai fornitori.

Per concludere l'applicazione del Regolamento, è condizionata ai rischi che gli strumenti *SupTech* presentano e mira garantire la comprensione e la corretta utilizzazione dell'*output*, cioè, la cosiddetta trasparenza tecnica. Questa tipologia di trasparenza non è, però, in grado di garantire appieno il diritto ad una buona amministrazione ed è per questo che sarà necessaria l'adozione di ulteriori misure. Al massimo, il rispetto degli obblighi di trasparenza imposti dal Regolamento potrà concorrere, in via indiretta, alla promozione della buona amministrazione.

---

458 RINGE W.G. *et al*., *Navigating the Legal Landscape of AI-Enhanced Banking Supervision: Protecting EU Fundamental Rights and Ensuring Good Administration,* European Banking Institute Working Paper Series 2023 - no. 140, 2023, Cap. IV, par. A.2.

459 Corte di Giustizia, 13 giugno 1958, C-10/56, *impresa Meroni et co*., *industrie metallurgiche, società in accomandita semplice*, c. l'Alta Autorità.

460 Ibidem.

461 Ibidem.

462 Si veda il par. 2.1.

CAPITOLO III – UNA CHIAVE DI LETTURA PER SUPERARE LA RELAZIONE POTENZIALMENTE CONFLITTUALE TRA LA VIGILANZA BANCARIA E L'INTELLIGENZA ARTIFICIALE

1. *AI-Enhanced banking supervision*: possibili soluzioni per garantirne un uso legittimo

L'impiego dell'IA, nell'attività di vigilanza bancaria, costituisce, come affermato nel par. 3.4. del Cap. I, un "approdo obbligatorio", in quanto, permetterà alle autorità di stare al passo con i tempi e adattarsi alle sfide sempre più complesse dell'attività. Non è, quindi, possibile pensare di risolvere le questioni giuridiche sorte dalla relazione tra supervisione bancaria e IA astenendosi dall'utilizzo della stessa. Per questo motivo, l'obiettivo dell'elaborato è quello di ricercare un compromesso tra l'esigenza di efficienza, velocità ed economicità nella previsione ed eventualmente, nell'individuazione e risoluzione dei rischi e il rispetto del quadro legale ed istituzionale.

Come ampiamente affermato in precedenza, l'*AI-Enhanced banking supervision* è finalizzata a migliorare l'attività di vigilanza in talune fasi quali: le segnalazioni di vigilanza, la gestione dei dati, l'analisi microprudenziale e più specificamente, sul rispetto delle norme antiriciclaggio e contro il finanziamento del terrorismo. Sono molteplici le applicazioni di IA con funzione "servente" e sono elencate al par. 4 e ss. di questo Capitolo. I principali rischi derivanti da un suo utilizzo sono legati alla difficoltà di valutare l'*output* a causa della scarsa trasparenza sul funzionamento interno e alla compatibilità con il GDPR essendo il loro funzionamento dipendente dal *training* anche su dati personali

1.1. L'*eXplAInable AI*: una tecnica per superare "*the black box problem*" e garantire la trasparenza nell'operato della BCE

Il principale ostacolo all'impiego dei sistemi di apprendimento automatico nell'attività di supervisione svolta dalla BCE è rappresentato dall'opacità che caratterizza il loro funzionamento interno. Distinguiamo tre livelli di opacità: *black*, *grey* e *white*.

Per "*black*" si intende il massimo livello di opacità che caratterizza alcuni sistemi di IA tale da rendere imperscrutabile l'*iter* logico seguito dall'algoritmo per giungere ad un risultato che sul piano giuridico determina una violazione del principio di trasparenza

dell'azione amministrativa[463]. Per "*grey*" si fa riferimento al livello intermedio di opacità tale da richiedere, ai fini della comprensione del funzionamento, una conoscenza specifica del dominio[464]. Il "*white*" è il livello più basso e caratterizza un sistema IA che opera in modo trasparente e in cui è facile individuare i fattori che hanno influenzato una determinata decisione[465]. In questo paragrafo non ci soffermeremo sul "*black box problem*", in quanto già analizzato nel Cap. I, par. 4.2.5., ma su come potrebbe essere risolto.

Il "*black box problem*" non riguarda i sistemi computazionali basati su semplici modelli statistici, essendo in grado di esser compresi dai loro utilizzatori, ma i sistemi di *machine learning* e *deep learning*, in quanto, più complessi e meno comprensibili[466]. Per questo motivo, essendo i sistemi di ML e DL quelli più adatti ad esser impiegati nell'attività di vigilanza bancaria, è fortemente avvertita la necessità di sperimentare delle tecniche in grado di rendere "spiegabile" il processo decisionale di questi algoritmi. La "spiegabilità" permetterebbe agli utilizzatori di verificare la fondatezza di una decisione e di non farla propria, nel caso in cui fosse errata o discriminatoria, oltre che garantire la buona amministrazione attraverso il rispetto dell'obbligo di motivazione.

Il campo di ricerca principale è l'*eXplAInable AI* (XAI) che si concentra sulla ricerca di soluzioni tecniche per affrontare i problemi di opacità nel ML e che ci aspetti trovi applicazione nel contesto *SupTech* per soddisfare l'obbligo di trasparenza, richiesto alla BCE, nello svolgimento dell'attività di vigilanza bancaria[467].

Un sistema XAI può esser essere definito come un sistema intelligente autoesplicativo che descrive il ragionamento alla base delle decisioni e previsioni di un sistema di ML o DL[468].

Le tecniche XAI sono classificate in due categorie: metodi trasparenti e metodi *post-hoc*. I metodi trasparenti sono metodi in cui il funzionamento interno e il processo decisionale

---

[463] Si veda nota 226.

[464] RINGE W.G. *et al*., *Navigating the Legal Landscape of AI-Enhanced Banking Supervision: Protecting EU Fundamental Rights and Ensuring Good Administration*, European Banking Institute Working Paper Series 2023 - no. 140, 2023, Cap. V, lett. A.

[465] Si veda nota 485.

[466] HOFFMAN R. *et al*., *Metrics for Explainable AI: Challenges and Prospects*, arXiv, 2018, p. 1. [Online]. Disponibile su: https://arxiv.org/abs/1812.04608

[467] RINGE W.G. *et al*., *Navigating the Legal Landscape of AI-Enhanced Banking Supervision: Protecting EU Fundamental Rights and Ensuring Good Administration*, European Banking Institute Working Paper Series 2023 - no. 140, 2023, Cap. V, lett. B, intro.

[468] HOFFMAN R. *et al*., *Metrics for Explainable AI: Challenges and Prospects*, arXiv, 2018, abstract.

del modello sono semplici da interpretare e rappresentare[469]. La complessità di funzionamento dei modelli di ML potrebbe esser ridotta convertendoli in modelli che si avvalgono di metodi trasparenti, quindi, più lineari[470]. La maggiore interpretabilità di un modello, tuttavia, determina una minore accuratezza dello stesso nella produzione dell'*output* aumentando il rischio di un risultato non soddisfacente per il perseguimento delle finalità di vigilanza bancaria. I modelli che rientrano in questa categoria sono il modello *bayesiano*, gli alberi decisionali, la regressione lineare e i sistemi di inferenza *fuzzy*[471].

Data la scarsa accuratezza dei metodi trasparenti, i ricercatori hanno cercato di progettare delle tecniche che consentissero di interpretare qualunque algoritmo di ML preservandone la sua complessità e accuratezza: i metodi esplicativi *post-hoc*.

Un metodo XAI *post-hoc* riceve come *input* un modello di IA addestrato e/o testato, quindi, genera utili approssimazioni sul funzionamento interno del modello e della logica decisionale producendo rappresentazioni comprensibili sotto forma di punteggi di importanza delle funzionalità, *set* di regole, mappe termiche o linguaggio naturale[472]. Il metodo *post-hoc*, per il compimento dell'attività esplicativa, si avvale di algoritmi indipendenti, denominati *explainer ad-hoc*[473]. Quest'ultimi, mirano ad offrire delle spiegazioni sulla logica che ha portato ad una determinata decisione o previsione dell'algoritmo. Distinguiamo varie tipologie di spiegazioni.

Le spiegazioni "*Why – Not*" aiutano l'utente a comprendere il perché un *output* specifico non era nell'*output* del sistema, cioè, le ragioni delle differenze tra la previsione di un modello e il risultato atteso dall'utente[474]. Le spiegazioni "*What-If*" implicano la dimostrazione di come i diversi cambiamenti algoritmici e di dati influiscano sull'*output* del modello in base a nuovi *input*, sulla manipolazione degli *input* o sulla modifica dei

---

[469] GOHEL P, SINGH P., MOHANTY M., *Explainable AI: current status and future directions*, Centre for Forensic Science, University of Technology Sydney, Australia, 2016, Cap. IV. [Online]. Disponibile su: https://arxiv.org/abs/2107.07045

[470] RUDIN C., *Stop Explaining black box machine learning models for high stakes decisions and use interpretable models instead*, 1 Nature Machine Intelligence, 2019, 206-215. [Online]. Disponibile su: https://arxiv.org/abs/1811.10154

[471] Ibidem.

[472] GOHEL P, SINGH P., MOHANTY M., *Explainable AI: current status and future directions*, Centre for Forensic Science, University of Technology Sydney, Australia, 2016, Cap. IV, par. B.

[473] MOHSENI S., ZAREI N., RAGAN E. D., *Multidisciplinary Survey and Framework for Design and Evaluation of Explainable AI Systems*. ACM Trans. Interagire. Intel. Sist. 11, 3–4, Article 24, 2021, par. 4.2. [Online]. Disponibile su: https://dl.acm.org/doi/abs/10.1145/3387166

[474] Ivi, par. 4.3.

parametri del modello[475]. In altre parole, offrono una spiegazione/previsione di cosa sarebbe successo se fosse stato inserito un *input* diverso da quello attuale. Questo approccio, basato sul metodo controfattuale, potrebbe esser utilizzato dalla BCE per offrire una motivazione indicando al destinatario i fattori che hanno inciso nella decisione di un sistema di ML. Si pensi al caso di un membro del consiglio di amministrazione di una banca la cui nomina viene rifiutata a seguito di una valutazione di idoneità e correttezza compiuta da un sistema di apprendimento automatico[476]. Le spiegazioni controfattuali riguardano i requisiti che il candidato avrebbe dovuto avere affinché la sua nomina venisse accettata[477].

Le spiegazioni "*What-Else*" presentano agli utenti istanze di *input* simili che generano *output* uguali o simili dal modello, note anche come "spiegazioni per esempio" [478].

Le spiegazioni, poi, possono esser classificate in relazione alla loro scala di interpretazione e dei loro destinatari.

Con riferimento alla scala di interpretazione, ogni spiegazione potrebbe sia esser finalizzata alla descrizione dell'intero modello di *machine learning* (spiegazione generale) sia a spiegare la relazione tra specifiche coppie *input* - *output* o il ragionamento alla base dei risultati per una singola *user query* (spiegazione locale)[479].

Le scelte di progettazione dell'applicazione XAI, ad esempio, il tipo di spiegazione, l'ambito e il livello di dettaglio, saranno influenzate dal tipo di utente a cui la spiegazione sarà rivolta[480]. Per questo motivo, distinguiamo tre gruppi generali di utenti: esperti di intelligenza artificiale, esperti di dati e principianti dell'intelligenza artificiale.

Ad esempio, mentre gli esperti di *machine learning* preferiscono visualizzazioni altamente dettagliate di modelli profondi per aiutarli a ottimizzare e diagnosticare gli algoritmi, gli utenti finali dei prodotti di intelligenza artificiale non si aspettano spiegazioni completamente dettagliate per ogni *query* da un agente personalizzato[481].

---

[475] Ibidem.
[476] RINGE W.G. *et al*., *Navigating the Legal Landscape of AI-Enhanced Banking Supervision: Protecting EU Fundamental Rights and Ensuring Good Administration*, European Banking Institute Working Paper Series 2023 - no. 140, 2023, Cap. V, lett. A.
[477] Ibidem.
[478] Ibidem.
[479] Ivi par. 4.1.
[480] MOHSENI S., ZAREI N., RAGAN E. D., *Multidisciplinary Survey and Framework for Design and Evaluation of Explainable AI Systems*, ACM Trans. Interagire. Intel. Sist. 11, 3–4, Article 24, 2021, par. 6.
[481] Ibidem.

Il ruolo delle applicazioni XAI nella vigilanza bancaria sarà finalizzato a far comprendere una decisione basata sull'IA risolvendo il "*black box problem*", quindi, uno dei motivi di attrito con la buona amministrazione ma, più in generale, a fornire delle informazioni a tutti i soggetti coinvolti nell'attività automatizzata. Per i progettisti e gli sviluppatori, la "spiegabilità" aiuterà a migliorare la sicurezza e le prestazioni dei sistemi di IA, minimizzando il rischio di risultati distorti e di difformità alla normativa[482]. Questi professionisti avranno bisogno di spiegazioni tecniche dettagliate per affinare e perfezionare i loro sistemi[483].

Le autorità di vigilanza bancaria, che si affidano ai risultati dell'IA per avvisi e raccomandazioni, richiederanno un tipo di "spiegabilità" che permetta loro di monitorare e regolare il comportamento dei sistemi di IA[484] e se necessario, confutare o rifiutare il risultato delle decisioni e prendere il controllo diretto delle operazioni[485].

Gli esperti legali, d'altra parte, necessiteranno di spiegazioni per vagliarne la conformità alle norme e ai principi giuridici ed eventualmente, dettare delle misure per adeguarsi[486].

I soggetti regolati e le parti interessate, come gli istituti vigilati, richiederanno una trasparenza che consenta loro di riprodurre il processo decisionale, per esercitare i propri diritti, come quelli di buona amministrazione e di difesa[487].

Infine, per permettere ai giudici di poter sindacare la legittimità e la ragionevolezza della decisione amministrativa robotizzata, si richiederà di assicurare che il processo informatico che ha portato ad una data decisione avvenga in maniera trasparente attraverso la conoscibilità dei dati ammessi e della "regola" che governa l'algoritmo[488].

1.2. Una risposta alle implicazioni derivanti dall'impiego dell'IA nella vigilanza bancaria ed il GDPR

Come già affermato nel par. 3.5 del Cap. I, l'impiego dell'intelligenza artificiale dovrà uniformarsi, non solo all'*AI Act* e agli obblighi previsti per il rispetto dei diritti

---

[482] RINGE W.G. *et al*., *Navigating the Legal Landscape of AI-Enhanced Banking Supervision: Protecting EU Fundamental Rights and Ensuring Good Administration*, European Banking Institute Working Paper Series 2023 - no. 140, 2023, Cap. V, lett. B, par. 2.
[483] Ibidem.
[484] Ibidem.
[485] Ibidem.
[486] Ibidem.
[487] Ibidem.
[488] Cons. Stato, 13 dicembre 2019, n. 8472, massima redazionale, *Wolters Kluver*, 2019.

fondamentali, ma anche al Regolamento sulla protezione dei dati personali (GDPR), nel caso in cui tratti dati personali.

In linea generale, alla necessità di garantire una vigilanza celere ed efficace per scongiurare crisi alla stabilità del sistema bancario, si contrappone l'esigenza di tutelare i diritti dell'interessato al trattamento dei dati personali, viste le modalità di funzionamento dei sistemi di apprendimento automatico, basate sulla raccolta, analisi ed elaborazione dei dati.

Con i successivi due sottoparagrafi si cercherà di trovare una soluzione di compromesso tra le due esigenze contrapposte, andando a suggerire delle soluzioni ai problemi sollevati nel par. 3.5. del Cap. I.

In questo contesto, la riflessione verterà sulle modalità con cui gli interessati potranno chiedere la cancellazione dei dati o la limitazione del trattamento dei dati che li riguardano, nonché, le modalità attraverso cui il diritto all'intervento umano possa esser garantito nei casi di cui al par. 2 dell'art. 22 del GDPR.

Quando si decide di automatizzare una qualunque attività, le criticità aumentano perché si prende atto che il trattamento dei dati personali, a cura di un sistema IA, interferisce con il suo funzionamento. Infatti, i dati personali possono costituire un *set* di dati funzionale al *training* algoritmico, quindi, costituire una risorsa in grado di accrescere la qualità dell'*output*.

1.2.1. L'art. 22: un limite al trattamento automatizzato dei dati

L'art. 22 sancisce il diritto dell'interessato «*di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona*»[489]. La norma è incentrata sulla piena tutela del diritto ad avere il controllo sui propri dati, assicurando un confronto con una persona fisica. Al divieto, come generalmente avviene nel GDPR, sono previste eccezioni nei casi in cui la decisione: sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e il titolare del trattamento[490]; sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento che precisa, altresì, misure adeguate a tutela dei diritti,

[489] Art. 22, par. 1 del GDPR.
[490] Art. 22, par. 2, lett. a) del GDPR.

delle libertà e dei legittimi interessi dell'interessato[491]; si basi sul consenso esplicito dell'interessato[492]. In questi casi, il titolare del trattamento sarà tenuto ad adottare misure in grado di garantire, quantomeno, il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione[493]. Alla luce del terzo comma del Considerando 71 collegato all'art. 22, le misure idonee impongono al titolare del trattamento di avvalersi di procedure matematiche o statistiche appropriate per la profilazione, mettendo in atto misure tecniche e organizzative adeguate, al fine di garantire un trattamento corretto e trasparente nel rispetto dell'interessato. In particolare, per ridurre le imprecisioni dei dati e minimizzare il rischio di errori, è essenziale correggere, immediatamente, i fattori responsabili; per garantire la sicurezza dei dati personali, è necessario adottare misure che considerino i rischi potenziali per i diritti e gli interessi della persona coinvolta, evitando conseguenze discriminatorie. Per i sistemi di apprendimento automatico, tali operazioni consisteranno nel dimostrare che i dati di *input*[494] non sono "imprecisi o irrilevanti, o estrapolati dal contesto" e che non violino "le ragionevoli aspettative degli interessati", in relazione allo scopo per il quale i dati sono stati raccolti[495].

La regola generale, ad eccezione delle ipotesi di cui alla lett. a) e lett. b), è che l'ammissibilità del trattamento automatizzato dipenderà dal consenso dell'interessato che mantiene il pieno controllo dei propri dati, secondo una visione quasi proprietaria[496].

In relazione ad uno dei temi della ricerca, cioè se l'art. 22 possa costituire un ostacolo all'utilizzo dei sistemi di apprendimento automatico nella supervisione bancaria qualora trattino dati personali, dovrà distinguersi il caso in cui l'IA sia utilizzata per "attività interne" e non aventi riflessi diretti sulle decisioni di vigilanza, dal caso in cui l'utilizzo è finalizzato ad assurgere a fattore decisivo ai fini della decisione o vada a costituire la decisione stessa.

---

[491] Art. 22, par. 2, lett. b) del GDPR.
[492] Art. 22, par. 2, lett. c) del GDPR.
[493] Art. 22, par. 3 del GDPR.
[494] Per dati di *input* si intende non solo i dati personali dell'interessato ma tutto il *set* di dati di addestramento.
[495] SARTOR G., LAGIOA F., *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*, 2020, par. 3.6.3. [Online]. Disponibile su: https://cris.unibo.it/handle/11585/763225#
[496] PIZZETTI F., *Intelligenza artificiale, protezione dei dati personali e regolazione*, collana diretta *da* Franco Pizzetti: I diritti nella "rete" della rete, Torino, 2018, p. 35.

Trattandosi di un divieto riferito ai soli trattamenti interamente automatizzati, questo costituirà un ostacolo solo nel secondo caso, cioè, ogni qualvolta si sia in presenza di un'attività di vigilanza completamente automatizzata caratterizzata dall'assenza della supervisione umana o quando l'IA produca un *output* determinante per una decisione umana, ma non permetta all'interessato di contestare quel risultato[497] [498].
Anche per questo motivo non è immaginabile, per alcuni compiti, un'attività di vigilanza completamente automatizzata senza la supervisione umana.

1.2.2. I diritti alla cancellazione e alla limitazione dei dati personali e l'attività di addestramento dell'algoritmo

I diritti alla cancellazione e alla limitazione dei dati personali rispettivamente disciplinati agli artt. 17 e 18 del GDPR costituiscono un ulteriore motivo di attrito, in quanto il funzionamento degli algoritmi di ML dipende dal *training* su set di dati, tra cui rientrano, certamente, i dati personali.
Un minor numero di dati a disposizione e per giunta, per un tempo limitato, riduce la qualità dell'*output* di un sistema di ML, aumentando la percentuale di errore e di inaffidabilità e di conseguenza, la percentuale di rischi ai diritti fondamentali.
Da questo motivo di attrito discendono due ordini di problemi: l'individuazione del limite fino al quale la restrizione dei diritti alla protezione dei dati personali può essere consentita per l'esercizio delle funzioni di vigilanza; come garantire, in concreto, l'esercizio di tali diritti.
L'art. 17 sancisce l'obbligo giuridico, in capo al titolare, del trattamento di procedere senza ingiustificato ritardo alla cancellazione dei dati che riguardano l'interessato nei casi in cui sussista uno dei motivi di cui al par. 1[499]. L'obbligo non è assoluto, infatti, il titolare

[497] Per via del "*Black box problem*".
[498] In tal caso essendo la decisione presa da un esser umano sarebbe, in ogni caso, garantito il diritto ad ottenere l'intervento del titolare del trattamento.
[499] «(...) *a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;*
b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;
c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;
d) i dati personali sono stati trattati illecitamente;

del trattamento sarà esentato nel caso in cui il trattamento sia previsto per l'esecuzione di un compito svolto nel pubblico interesse, oppure, nell'esercizio di pubblici poteri a lui attribuiti[500], oltre che per altre specifiche situazioni elencate nel par. 3, lett. a) – e). Il perseguimento della stabilità bancaria è, certamente, un compito che la BCE svolge nell'interesse pubblico ed esercitando pubblici poteri. Tuttavia, i dati personali in questione non sarebbero utilizzati per perseguire direttamente un interesse pubblico, ma verrebbero impiegati nel *training* di un sistema di apprendimento automatico finalizzato a fornire un supporto, per ora non essenziale, all'attività di supervisione bancaria e quindi, solo indirettamente contribuirebbero all'esecuzione di un compito pubblicistico.

Discorso analogo per il diritto alla limitazione del trattamento data la previsione di cui al par. 2 dell'art. 18.

Una soluzione per eliminare il problema in radice, senza chiedersi se si applichi o meno l'eccezione all'obbligo di cancellazione e di limitazione del trattamento dei dati personali, potrebbe esser quella di anonimizzare i dati per continuare a utilizzarli liberamente e nel modo in cui la BCE riterrà opportuno[501].

La garanzia, in concreto, dell'esercizio di tali diritti, qualora sussistessero i presupposti per esercitarli, implica un'attività di "*unlearning*" o "*de-training*" dell'algoritmo di IA utilizzato. L'attività di "*unlearning*" consiste nel processo di rimozione di dati usati per l'apprendimento, finalizzato alla modifica del comportamento e dell'*output* dell'IA, per salvaguardare la *privacy* degli utenti e garantire l'imparzialità dei sistemi autonomi[502]. Il *de-training* richiede la conoscenza esatta del modo in cui i singoli punti di *training* hanno contribuito agli aggiornamenti dei parametri del modello e ciò è possibile quando l'algoritmo di apprendimento interroga i dati in un ordine deciso prima dell'inizio dell'apprendimento[503]. La procedura inizia con una richiesta di rimozione dei dati, il

---

e) i dati personali devono essere cancellati per adempiere un obbligo giuridico previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento ([1])

f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1».

[500] Art. 17, par. 3, lett. b) del GDPR.

[501] RINGE W.G. *et al*., *Navigating the Legal Landscape of AI-Enhanced Banking Supervision: Protecting EU Fundamental Rights and Ensuring Good Administration*, European Banking Institute Working Paper Series 2023 - no. 140, 2023, Cap. IV, par. B.1., lett. i).

[502] Definizione rinvenibile su: https://www.ai4business.it/intelligenza-artificiale/connessioni-sintetiche/machine-unlearning-cose-e-come-corregge-errori-e-bias-dellai/

[503] BOURTOULE L. *et al*., *Machine Unlearning*, 2021 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2021, introduction. [Online]. Disponibile su: https://ieeexplore.ieee.org/abstract/document/9519428

modello corrente verrà elaborato da un algoritmo di disapprendimento per dimenticare le informazioni corrispondenti ai dati da cancellare all'interno del modello[504]. Al termine, i metodi di verifica dell'"*unlearning*" valuteranno il risultato dell'attività.

2. Alla ricerca di un compromesso tra il diritto ad una buona amministrazione e l'*AI-Driven banking supervision*

Fino ad ora, la giurisprudenza e la dottrina europea, hanno trattato il diritto ad una buona amministrazione solo con riferimento ai casi di "cattiva amministrazione" tradizionale, cioè, solo con riguardo ai casi in cui il pregiudizio alle prerogative del destinatario derivava da un errore umano.

In questa sede si cercherà, sulla base della normativa e della giurisprudenza della Corte di Giustizia[505], di suggerire come le banche, destinatarie dei procedimenti di vigilanza automatizzati, potranno esercitare i propri diritti, stante, le limitazioni tecniche dell'IA, nell'ipotetico caso in cui venga impiegata per "guidare" la vigilanza bancaria.

Le limitazioni tecniche variano a seconda della tipologia di sistema di IA. Ad esempio, nel caso di IA che si avvalgono di algoritmi condizionali, non sussisteranno rischi legati alla qualità dei dati, in quanto, il loro funzionamento non dipenderà dal *training* su dati. Viceversa, in caso di sistemi di IA basati sul *machine learning*, impiegati in una procedura amministrativa, le minacce e i danni potenziali al diritto alla buona amministrazione saranno nettamente superiori, considerata la loro natura[506].

In particolare, essendo l'*output* basato sulla correlazione e non sulla causalità, è alto il rischio di inadempimento all'obbligo di motivazione, in quanto, la BCE non riuscirebbe a dare una spiegazione causale della sua decisione[507]. La violazione di tale obbligo potrebbe discendere, inoltre, anche dalla mancanza di specificità e individualità che deve caratterizzare la motivazione, essendo le decisioni prese su base statistica. Tuttavia, ancor più problematica, al di là del metodo utilizzato, è la natura imperscrutabile del procedimento che porta ad una data decisione: il "*black box problem*". Quest'ultimi, sono

---

[504] NGUYEN T. T. *et al*, *A Survey of Machine Unlearning*, arXiv, 2022, par. 2.1. [Online]. Disponibile su: https://arxiv.org/abs/2209.02299

[505] Le pronunce della giurisprudenza, prese in considerazioni dall'elaborato, sono state trattate al par. 2.2. (comprensivo dei suoi sottoparagrafi) del Cap. I.

[506] WRÓBEL I, *Artificial Intelligence Systems and the Right to Good Administration*, 49(2) Review of European and Comparative Law 203, 2022, p. 216. [Online]. Disponibile su: https://repozytorium.kul.pl/server/api/core/bitstreams/3683b92d-7296-47cd-9df2-cb6a0443bfe1/content

[507] Si veda nota 222.

solo alcuni dei, principali e già trattati[508], aspetti problematici a cui si tenterà di dare una soluzione.

L'uso dell'IA nella vigilanza bancaria, in sintesi, può impedire alla BCE di rispettare il diritto ad una buona amministrazione. Per evitare ciò in dottrina sono stati proposti due approcci: riadattare le norme e i principi del diritto amministrativo come risposta alla tendenza sovversiva dell'IA; utilizzare il principio di buona amministrazione come base per lo sviluppo e l'uso sicuro e responsabile dell'IA nella vigilanza bancaria[509].

Alcuni studiosi hanno espresso preoccupazioni per il fatto che il processo decisionale automatizzato («ADM») sia in contrasto contro le norme di diritto amministrativo, in quanto, concepite partendo dal presupposto che le decisioni siano prese da esseri umani e non da algoritmi[510]. Per questo motivo, hanno suggerito un riadattamento delle norme e dei principi al nuovo fenomeno. Secondo altri, l'uso delle nuove tecnologie può adattarsi facilmente ai parametri legali convenzionali in ragione delle finalità per cui vengono generalmente impiegati[511]. Questo perché, nella maggior parte dei casi, la finalità è quella di informare i funzionari nei loro giudizi, svolgendo una funzione analoga a qualsiasi altro supporto alla ricerca o *input* informativo nel processo decisionale[512]. Maggiori problemi di adattamento si configurerebbero negli scenari in cui l'IA concorresse nella determinazione della decisione o generasse la stessa. In questo caso, il funzionario non avrà né possibilità d'intervento, né di scelta, sul se utilizzare l'*output* del sistema IA.

Sotto un'altra prospettiva, la "buona amministrazione" può fungere anche da causa di giustificazione dell'impiego dell'IA nella vigilanza bancaria, cioè, come presupposto imprescindibile per tutelare al meglio le stesse garanzie che, per altri motivi, sono messe in pericolo dall'impiego della tecnologia.

---

[508] Sono trattati nei par. 2.2.6. e 2.2.7. del Cap. I.

[509] RINGE W.G. *et al.*, *Navigating the Legal Landscape of AI-Enhanced Banking Supervision: Protecting EU Fundamental Rights and Ensuring Good Administration*, European Banking Institute Working Paper Series 2023 - no. 140, 2023, pp. 42 – 43.

[510] HUGGINS A., *Addressing Disconnection: Automated Decision-Making, Administrative Law and Regulatory*, 44(3) University of New South Wales Law Journal 1048, 2021, p. 1049. [Online]. Disponibile su: https://www.researchgate.net/publication/356974750_Addressing_Disconnection_Automated_Decision-Making_Administrative_Law_and_Regulatory_Reform

[511] COGLIANESE C., LEHR D., *Regulating by Robot: Administrative Decision Making in the Machine-Learning Era*, 105(5) Georgetown Law Journal 1147, pp. 1169 - 1170. [Online]. Disponibile su: https://scholarship.law.upenn.edu/faculty_scholarship/1734/

[512] Ibidem.

Con riferimento alla durata ragionevole del procedimento, è chiaro che l'ausilio di tali sistemi può comportare una diminuzione dei tempi del procedimento data l'estrema velocità nell'elaborazione e visualizzazione di informazioni. Non trattandosi di persone fisiche, i sistemi di IA agiranno liberi da influenze, pressioni esterne e senza interessi personali. Tuttavia, il rischio di pregiudizio all'obbligo di imparzialità è alto, in quanto, spesso i risultati riflettono le preferenze e i pregiudizi degli esseri umani che hanno concorso al loro sviluppo e dei dati su cui si sono allenati. L'utilizzo dell'IA, poi, potrebbe ridurre i casi di responsabilità da supervisione rendendo più razionale e prevedibile l'uso dei poteri discrezionali[513]. Questi sistemi garantirebbero che l'adozione delle decisioni avvenga dopo aver considerato e individuato, grazie alle loro capacità di selezione, tutti i fattori rilevanti e pertinenti al caso concreto.

In coerenza con il principio di proporzionalità dell'azione amministrativa, la BCE dovrebbe adottare tutti gli strumenti necessari per perseguire gli obiettivi imposti dal mandato istituzionale ed i sistemi di IA, attualmente, rientrano in quelli a sua disposizione.

2.1. Riadattare le norme e i principi del diritto amministrativo alla luce della rivoluzione tecnologica

L'avvento della tecnologia nella pubblica amministrazione, per le comunicazioni intergovernative e con i cittadini, risale agli anni 90'. L'effetto di queste innovazioni è stato relativamente limitato, poiché, non ha portato modifiche profonde nelle procedure amministrative, ma un cambiamento epocale nell'organizzazione dell'amministrazione con: l'utilizzo dei computer negli uffici, l'archiviazione dei dati e la fornitura di servizi *online*. La tecnologia era vista come uno strumento per migliorare la qualità dei servizi e accrescere la trasparenza attraverso un facile accesso alle informazioni e un maggiore coinvolgimento dei cittadini. Tuttavia, negli ultimi anni, con l'avvento dei sistemi di apprendimento automatico, all'interno delle procedure amministrative, si son fatte largo nuove sfide in relazione ai principi del diritto amministrativo. Il cambiamento dell'oggetto della regolamentazione, ossia, il passaggio dall'attività umana pura a quella

[513] RINGE W.G. *et al*., *Navigating the Legal Landscape of AI-Enhanced Banking Supervision: Protecting EU Fundamental Rights and Ensuring Good Administration*, European Banking Institute Working Paper Series 2023 - no. 140, 2023, Cap. IV, lett. A, par. 1.

integrata dall'IA ha reso necessaria una riflessione sulla capacità dell'attuale legislazione di far fronte al nuovo fenomeno.

Per questo motivo in dottrina, si è fatta largo la tesi secondo cui sarebbe necessario un riadattamento delle norme e dei principi che regolano l'attività amministrativa sulla base dell'incapacità delle regole tradizionali di tutelare adeguatamente i soggetti coinvolti in un eventuale procedimento automatizzato. I diritti di quest'ultimi, discendenti dai principi fondamentali del procedimento amministrativo, sono stati previsti per esser esercitati nei confronti di un'amministrazione le cui decisioni sono frutto della decisione umana. Per fare un esempio, come potrà esser esercitato il diritto alla difesa se un sistema di apprendimento automatico non è in grado di "spiegare" come mai ha prodotto un determinato risultato?

Secondo alcuni autori[514], i problemi evidenziati, sebbene sotto un'ottica diversa, sono stati già affrontati nel corso della storia, in particolare con le amministrazioni basate su prerogative reali o dittatoriali. In particolare, in entrambi i casi, si è al cospetto di un'amministrazione opaca, le cui azioni non sono né spiegate né giustificate. Infatti, come in passato le scelte erano figlie del libero arbitrio del sovrano, oggi, le stesse possono dipendere dalla decisione di un algoritmo di cui è impossibile comprenderne il funzionamento, in ragione del "*black box problem*"[515]. Per fare un esempio, si pensi al caso in cui un sistema, che valuta i requisiti di professionalità e onorabilità degli organi direttivi delle istituzioni significative, commetta un errore e reputi inidoneo un amministratore di una banca che ha, invece, tutti i requisiti previsti dalla legge e non fornisca alcuna giustificazione. È evidente che la situazione non differisce più di tanto da una decisione arbitraria di un sovrano. Questa situazione mette in luce la necessità di un aggiornamento urgente dei principi chiave dell'amministrazione pubblica, come il diritto a un giusto procedimento e la responsabilità del funzionario, per includere le sfide poste dalle nuove tecnologie[516]. Dall'altro lato, ci confrontiamo con problemi di responsabilità

[514] DUARTE F. A. e LANCEIRO R. T., *Vulnerability and the Algorithmic Public Administration: Administrative Principles for a Public Administration of the Future* ,62(1) Revista da Faculdade de Direito da Universidade de Lisboa 1, 2021, Sez. 2. [Online]. Disponibile su: https://www.fd.ulisboa.pt/wp-content/uploads/2021/10/Francisco-de-Abreu-Duarte-Rui-Tavares-Lanceiro.pdf

[515] Ibidem.

[516] Ibdiem.

simili a quelli di un'amministrazione "immune", tipici dei regimi del diciannovesimo secolo piuttosto che di un sistema basato sul costituzionalismo liberale moderno[517].

Tuttavia, gli autori di questa tesi evidenziano che, mentre, nel passato la violazione dei diritti fondamentali proveniva direttamente dall'amministrazione, oggi l'amministrazione scarica la responsabilità della scarsa trasparenza sui privati fornitori che invocano, a loro volta, i diritti di proprietà intellettuale o il segreto commerciale.

Con l'affermazione dello Stato di diritto, ai cittadini è stato concesso di porre tre domande all'amministrazione: il cosa, il perché ed il chi dell'azione amministrativa che rimangono al centro della trasparenza algoritmica[518].

Nello specifico, gli autori suggeriscono di collegare tali domande a quattro principi interdipendenti per la *governance* pubblica algoritmica del futuro: trasparenza, giusto processo, responsabilità e non discriminazione. In particolare, "il cosa" dell'azione è riconducibile alla trasparenza nell'azione algoritmica. L'amministrazione deve garantire il diritto d'accesso alla documentazione e al fascicolo, quindi, deve operare in modo trasparente. La domanda sul "perché" è riconducibile al principio del giusto processo, o più precisamente, del giusto procedimento[519]. L'amministrazione deve illustrare al destinatario di una decisione le ragioni alla base della stessa attraverso una motivazione che ripercorra l'*iter* logico del procedimento decisionale. L'amministrazione algoritmica del futuro dovrà esser giustificata e spiegabile. Il "chi" dell'azione amministrativa risponde all'esigenza di individuare un responsabile nei confronti dei cittadini e permettere agli stessi di ottenere un adeguato risarcimento, nei casi di violazioni commesse dall'amministrazione[520]. Nel caso in cui quest'ultima utilizzi sistemi di IA, risponderà anche se tali tecnologie sono state progettate da privati, in quanto, la decisione finale è pur sempre presa dall'amministrazione.

Per quanto riguarda il principio della "non discriminazione", l'amministrazione deve garantire, in primo luogo, la possibilità di usufruire di un dato servizio offerto da un sistema di IA a tutti i cittadini, tenendo in considerazione le incapacità di alcuni gruppi di usare strumenti digitali o di accedere alla rete per via dei costi di connessione. In secondo luogo, di far operare il sistema in modo imparziale[521]. Per concludere, gli autori

[517] Ibidem.
[518] Ibidem.
[519] Ibidem.
[520] Ibidem.
[521] Ibidem.

terminano la loro riflessione affermando che i principi di trasparenza, giusto processo, responsabilità e non discriminazione saranno i primi capisaldi del diritto amministrativo algoritmico del futuro e che dovranno avere natura procedurale, data la loro dimensione tecnica estremamente complessa, per permettere ai cittadini di controllare il loro operato e ottenere adeguate motivazioni nei provvedimenti che li coinvolgono.

Un altro autore[522], ha analizzato le tre caratteristiche di un sistema di IA difficilmente compatibili con il diritto amministrativo australiano. La disamina, sebbene riguardi un confronto con il diritto australiano, è utile anche per indagare sul rapporto con i principi del diritto amministrativo europeo. L'autore si è chiesto, innanzitutto, se il codice informatico e gli algoritmi utilizzati nei sistemi automatizzati siano congruenti con i linguaggi e la logica della legge. In relazione a questo aspetto, si pongono numerose questioni su come un sistema di apprendimento automatico possa prendere in considerazione il testo di una legge.

Le questioni sono varie, ma le più rilevanti sono le seguenti: il rischio che in fase di progettazione il vocabolario, relativamente limitato del codice informatico, non rifletta adeguatamente le sfumature delle disposizioni di legge; il rischio che l'interpretazione della disposizione si distacchi dal testo di legge, in virtù della ponderazione di più variabili legate al caso concreto; il rischio derivante dall'errore nella traduzione della legislazione nel codice informatico, data l'assenza di competenze giuridiche dei programmatori informatici[523]. Per queste problematiche l'autore suggerisce, l'introduzione di una normativa che imponga un riesame dei vari sistemi sia al momento della loro attuazione, sia all'esito dei ricorsi giudiziari aventi ad oggetto una loro decisione[524].

In secondo luogo, l'autore si è interrogato sulla capacità di un sistema di operare, potenzialmente, in modo autonomo. Egli sottolinea come nell'ordinamento australiano manchino delle garanzie che impongano ai supervisori umani di controllare i sistemi automatizzati autonomi e suggerisce l'introduzione di una normativa che indichi, per ogni

---

[522] HUGGINS A., *Addressing Disconnection: Automated Decision-Making, Administrative Law and Regulatory Reform*, 44(3) University of New South Wales Law Journal 1048, 2021, pp. 1052 - 1053, 1073 – 1076 [Online]. Disponibile su: https://www.unswlawjournal.unsw.edu.au/wp-content/uploads/2021/09/Issue-443_final_Huggins_v2.pdf

[523] Ibidem.

[524] In questo senso l'*AI Act* ha previsto un monitoraggio successivo e costante sull'operato di tali sistemi. Per maggiori approfondimenti si veda il par. 2.12. del Cap. II.

operazione, se sia necessario ed in che misura l'intervento umano. In relazione a questo aspetto, lo stesso problema pare non sussistere a livello europeo, dato che l'art. 22 del GDPR sancisce un divieto, salvo eccezioni, di assoggettare l'interessato ad un processo decisionale esclusivamente automatizzato qualora incida sugli interessi e i diritti individuali[525].

La terza problematica è legata all'opacità che i sistemi di ML presentano, in contrasto con il principio di trasparenza che dovrebbe guidare un'amministrazione pubblica. Per questa problematica, l'autore suggerisce di obbligare i fornitori a render pubbliche informazioni significative sulla logica del processo decisionale e non solo il codice sorgente.

Poi, conclude affermando che in Europa la risposta, all'assenza di trasparenza, sarebbe duplice: l'art. 13 dell'*AI Act*; l'art. 13, par. 2, lett. f), l'art. 14, par. 2, lett. g), e l'art. 15, par. 1, lett. h), del GDPR. In particolare, la norma dell'*AI Act* permetterà all'utilizzatore di comprendere l'*output* e utilizzarlo adeguatamente, mentre, le disposizioni del GDPR obbligheranno l'utilizzatore a fornire informazioni significative sulla logica utilizzata, nonché, sull'importanza e sulle conseguenze previste da tale trattamento per l'interessato[526].

In conclusione, sebbene le tesi offerte dai sostenitori su un riadattamento delle norme e dei principi del diritto amministrativo siano in parte condivisibili, l'*AI Act*, il GDPR ed il diritto ad una buona amministrazione potrebbero costituire strumenti in grado di fungere da base, almeno in parte, per un impiego sicuro e rispettoso dei diritti fondamentali dei sistemi di ML nella vigilanza bancaria.

2.2. Il diritto ad una buona amministrazione come base per una rivoluzione tecnologica responsabile

A conclusione del precedente paragrafo, si è affermato che il Regolamento sull'intelligenza artificiale, quello sulla protezione dei dati personali e il diritto ad una buona amministrazione costituiscono un ottimo punto di partenza per instaurare una riflessione normativa sull'IA. Metaforicamente parlando, gli strumenti normativi, appena elencati, non sono altro che tessere di un mosaico e come tali, presentano caratteristiche

[525] HUGGINS A., *Addressing Disconnection: Automated Decision-Making, Administrative Law and Regulatory Reform*, 44(3) University of New South Wales Law Journal 1048, 2021, pp. 1052 - 1053, 1073 – 1076

[526] Ibidem.

diverse ma soprattutto, si collocano in posizione diverse. Ciascuno di essi ha una finalità essenziale, ma da sola non sufficiente a perseguire il più generale obiettivo di un'IA affidabile. Il problema di fondo delle tesi illustrate nel paragrafo precedente è di non aver preso in considerazione il mosaico normativo attualmente esistente[527].

In linea generale, il rapporto fra l'utilizzo dell'intelligenza artificiale nel procedimento amministrativo e il diritto ad avere una buona amministrazione è stato trattato da diversi autori nel panorama accademico europeo e statunitense.

Secondo un'autrice[528], bisognerebbe, prima di ricercare delle soluzioni tecniche al problema, distinguere le procedure amministrative tradizionali e quelle che utilizzano la stima *bayesiana* o gli algoritmi condizionali dalle procedure che utilizzano il *machine learning* e il *deep learning*. Questo perché, le insidie e i rischi dietro l'esercizio del diritto ad una buona amministrazione assumono portata diversa, a seconda del tipo di tecnologia impiegata. Dopo aver riassunto i vari motivi di attrito tra sistemi di IA e il diritto sancito all'art. 41 della Carta, l'autrice ha suggerito delle soluzioni di compromesso per ogni relazione conflittuale con ciascun diritto previsto. Ha, innanzitutto, escluso motivi di attrito con il diritto alla ragionevole durata del procedimento, in quanto, i sistemi di IA per loro natura tendono, in realtà, ad accelerare il corso di qualunque procedimento amministrativo. In relazione, all'obbligo di rimanere imparziali e di equità, invece, il problema sussisterà solo qualora l'amministrazione decida di avvalersi di un sistema di *machine learning* che necessita di allenarsi su dati[529]. In quel caso, sarà importante garantire la quantità e la qualità dei dati inseriti, al fine di evitare che gli stessi possano riflettere i pregiudizi del programmatore o che possano esser basati su fatti non veritieri o verosimili.

Il diritto di accedere ai fascicoli, nonché di chiederne modifiche a proprio favore, sarà condizionato dalle conoscenze e dalle competenze della parte destinataria del procedimento[530]. Come fatto notare dall'autrice, uno degli ostacoli maggiori legati all'automatizzazione dell'attività amministrativa è l'incapacità del cittadino medio di completare alcune procedure *online* e di conseguenza, anche la capacità di consultare il

[527] Ad eccezione di HUGGINS A. (n. 525).
[528] WRÓBEL I., *Artificial Intelligence Systems and the Right to Good Administration*, 49(2) Review of European and Comparative Law 203, 218, 2022, par. 5. [Online]. Disponibile su: https://czasopisma.kul.pl/index.php/recl/article/view/13616
[529] Ibidem.
[530] Ibidem.

fascicolo digitale. Perciò, l'unica soluzione è incentivare e finanziare programmi di formazione digitale dei cittadini al fine di permettere loro di esercitare tale diritto.

Il rispetto dell'obbligo di motivazione, invece, dipenderà dalla qualità del sistema di IA e dal grado di coinvolgimento del funzionario nel procedimento, supponendo che non tutte le fasi del procedimento siano svolte da un sistema di apprendimento automatico[531].

L'autrice conclude il suo articolo richiamando la Dichiarazione europea sui diritti e i principi digitali per il decennio digitale, proclamata solennemente dal Parlamento europeo, dal Consiglio e dalla Commissione europea il 26 gennaio 2022. Con questa dichiarazione, le istituzioni dell'Unione europea si sono impegnate a raggiungere tra i vari obiettivi: la trasparenza sull'uso dell'intelligenza artificiale e la responsabilizzazione e l'informazione delle persone quando interagiscono con loro; l'adeguatezza dei *set* di dati su cui si basano i sistemi algoritmici, per evitare discriminazioni e consentire la supervisione umana dei risultati che riguardano gli individui; la sicurezza che i sistemi di IA siano utilizzati nel pieno rispetto dei diritti fondamentali[532]. Questi sono solo alcuni degli impegni presenti nella Dichiarazione, ma sono quelli che secondo l'autrice assumono rilevanza nel procedimento amministrativo automatizzato. Il loro rispetto costituirà condizione necessaria e sufficiente per garantire l'esercizio effettivo del diritto ad una buona amministrazione.

In accordo sulla non necessarietà di adattare le norme esistenti alle nuove tecnologie, sebbene con riferimento a principi costituzionali e di diritto amministrativo dell'ordinamento statunitense, anche una parte della dottrina americana[533]. In questo articolo, gli autori si interrogano sul se l'impiego delle nuove tecnologie possa entrare in conflitto con le dottrine fondamentali del diritto amministrativo americano, alcune delle quali, affini ai principi del diritto europeo come: l'equità procedurale, la ragionevolezza e soprattutto, la trasparenza. Dopo aver preso atto delle possibili minacce giuridiche ed etiche dietro l'impiego dell'apprendimento automatico, affermano che quest'ultime difficilmente potranno realizzarsi. Gli algoritmi di apprendimento automatico hanno

[531] L'autrice non offre una soluzione soddisfacente rispetto all'obbligo di motivazione ad una decisione di un sistema di ML. Infatti, non si comprende come il funzionario possa interpretare un dato *output* se il sistema non dovesse fornire alcuna motivazione.

[532] WRÓBEL I., *Artificial Intelligence Systems and the Right to Good Administration*, 49(2) Review of European and Comparative Law 203, 218, 2022, par. 5.

[533] COGLIANESE C e LEHR D., *Regulating by Robot*, 105 Georgetown Law Journal 1147, 1184, 2017. [Online]. Disponibile su: https://scholarship.law.upenn.edu/faculty_scholarship/1734/

bisogno degli esseri umani per specificare le loro funzioni obiettivo e costruire i processi matematici che le massimizzeranno[534]. Anche se l'apprendimento automatico potrebbe sostituire o integrare molte attività amministrative di *routine*, la supervisione e la direzione dell'amministrazione sarà sempre presente[535]. A causa dell'esistenza di limiti tecnici nella programmazione di un algoritmo, non potrà mai prendere decisioni cruciali[536]. Quest'ultime, spesso, comportano giudizi di valore che difficilmente saranno compatibili con il grado di specificazione richiesto ai fini dell'incorporazione in funzioni matematiche[537]. Alla luce di ciò, il ruolo di un sistema IA sarà sempre quello di informare le scelte, senza mai determinarle[538].

Gli autori, in ultimo, affrontano il principale problema dei sistemi di ML: il "*black box*". La principale esitazione nell'uso di tali strumenti da parte delle istituzioni deriverebbe dalla percezione degli algoritmi di apprendimento come diversi, rispetto ai processi decisionali dell'essere umano e quindi, incompatibili con l'agire trasparente dell'amministrazione[539]. In realtà, vi sarebbero delle somiglianze fra le modalità di ragionamento umano e quelle degli algoritmi, quali la complessità e la scarsa intuitività che le renderebbero meno comprensibili rispetto ad altre tecniche[540]. Per concludere, l'era dell'apprendimento automatico non sostituirà il giudizio umano, ma verrà incorporata nel processo decisionale umano e lo renderà più accurato e veloce.

Approfondito in linea generale la relazione esistente fra l'impiego dell'intelligenza artificiale in qualunque attività amministrativa e la garanzia di una buona amministrazione, è necessario focalizzare l'attenzione sulla prima domanda di ricerca a cui questo elaborato tenta di dare una risposta: l'impiego dell'intelligenza artificiale nella vigilanza bancaria della BCE è conforme al diritto ad avere una buona amministrazione? Il tema è stato oggetto solo di un altro lavoro accademico[541], oltre a codesto elaborato.

Gli autori dell'articolo, dopo aver esaminato il quadro normativo sull'IA, prendono atto che le normative esistenti non forniscono una disciplina che garantisca un utilizzo dell'IA

---

[534] Ibidem.
[535] Si veda l'introduzione al Cap III dell'articolo in questione.
[536] COGLIANESE C e LEHR D., *Regulating by Robot*, 105 Georgetown Law Journal 1147, 1184, 2017.
[537] Ibidem.
[538] Ibidem.
[539] Ibidem.
[540] Ibidem.
[541] RINGE W.G. *et al*., *Navigating the Legal Landscape of AI-Enhanced Banking Supervision: Protecting EU Fundamental Rights and Ensuring Good Administration*, European Banking Institute Working Paper Series 2023 - no. 140, 2023.

rispettoso della "buona amministrazione". Il Regolamento sull'intelligenza artificiale assicurerà, una volta entrato in vigore, una trasparenza "da parte di esperti per esperti"[542], la cui finalità principale sarà, come affermato dall'art. 13, garantire all'utilizzatore e non al destinatario, di interpretare e utilizzare l'*output*. Data la generalità dell'obbligo, soprattutto, in relazione alla sua portata, è essenziale richiedere, per l'attività di vigilanza automatizzata della BCE, uno *standard* di trasparenza più alto, al fine di adempiere all'obbligo di garantire una buona amministrazione[543].

In via preliminare, l'articolo muove dalla considerazione che le applicazioni di IA presentano rischi diversi per i diritti fondamentali, di conseguenza, non è opportuno adottare un approccio normativo univoco.

Gli autori, in linea con la tecnica del *risk-based approach* utilizzata dal legislatore europeo, propongono una classificazione dei sistemi di IA sulla base di quattro parametri diversi: lo specifico compito di vigilanza assegnato a un determinato sistema di IA e la possibilità che esso produca effetti giuridici (ossia "Ambito di applicazione"); la natura e le caratteristiche degli insiemi di dati rilevanti trattati per tale compito (ossia "Tipi di dati"); la capacità di tale sistema di svolgere autonomamente il proprio compito (ossia "Livello di autonomia"); la facilità per gli utenti umani di comprendere e controllare il funzionamento del sistema (ossia "Grado di opacità").

Sulla base di questi parametri sono state individuate tre categorie di sistemi di rischio diverse.

La prima categoria è rappresentata dai sistemi a basso rischio o nullo che non presentano rischi particolari per la buona amministrazione. Sono sistemi che non svolgono compiti di vigilanza la cui esecuzione è in grado di produrre effetti giuridici, ma solo attività di raccolta, elaborazione e visualizzazione dei dati relativi all'attività di vigilanza[544]. Il grado di opacità è pressoché nullo, non a caso sono stati battezzati dalla comunità scientifica come "*white box*" *AI system*. Il funzionamento interno è trasparente e un *data scientist* sarà perfettamente in grado di comprendere i fattori che influenzano il processo

[542] Si veda nota 450.
[543] RINGE W.G. *et al*., *Navigating the Legal Landscape of AI-Enhanced Banking Supervision: Protecting EU Fundamental Rights and Ensuring Good Administration*, European Banking Institute Working Paper Series 2023 - no. 140, 2023, Cap. V, lett. A.
[544] Ibidem.

decisionale[545]. L'unica precauzione che l'autore impone, alla BCE in relazione a questa tipologia di sistemi, riguarda i casi in cui trattino dati personali[546]. In tal caso, saranno tenuti a rispettare il GDPR adottando le misure prescritte dallo stesso.

La seconda categoria ha ad oggetto i sistemi che presentano un rischio elevato per la buona amministrazione, in base ai parametri sopra elencati. La BCE, prima di impiegarli, dovrebbe effettuare una valutazione del rischio e dell'impatto sui diritti fondamentali, in particolare sul diritto alla buona amministrazione e sui requisiti imposti dall'*AI Act*[547]. Questi sistemi si caratterizzano per un maggiore grado di autonomia rispetto a quelli a basso rischio e possono trovare applicazione in una serie di casi d'uso come supporto diretto al processo decisionale umano attraverso analisi, previsioni e raccomandazioni[548]. Il grado di opacità è maggiore, ma non è tale da rendere l'algoritmo imperscrutabile, in proposito si usa parlare di "*grey box AI system*". La comprensione del loro funzionamento richiede comunque una conoscenza specifica del dominio. Nel caso in cui trattino dati personali, dovranno soddisfare requisiti più elevati in materia di trasparenza, responsabilità e verificabilità.

L'ultima categoria è rappresentata dalle applicazioni vietate di sistemi di IA nella supervisione bancaria. Il divieto riguarda tutti quei sistemi che per loro natura sono inconciliabili con l'obiettivo di garantire la buona amministrazione. Nello specifico, ogni sistema di apprendimento automatico che ha come finalità quello di supportare o sostituire il decisore umano in decisioni che esplicheranno effetti nella sfera giuridica del destinatario del provvedimento. Per ricadere in questa categoria è, tuttavia, necessario che si caratterizzino per un grado di opacità massimo, ossia, "*black box AI system*". L'assenza di chiarezza su come l'algoritmo sia arrivato ad un dato *output*, impedisce tali sistemi di prender parte o sostituirsi a decisioni umane, data l'impossibilità di descrivere l'*iter* logico che li ha portati a una determinata conclusione[549]. Un'ulteriore categoria di sistemi vietati, non per la violazione del diritto ad una buona amministrazione, riguarda i casi in cui i dati personali di un individuo vengano sottoposti ad un trattamento interamente

[545] Definizione rinvenibile sul sito: https://bigcloud.global/the-difference-between-white-box-and-black-box-ai/
[546] Ringe W.G. *et al*., *Navigating the Legal Landscape of AI-Enhanced Banking Supervision: Protecting EU Fundamental Rights and Ensuring Good Administration*, European Banking Institute Working Paper Series 2023 - no. 140, 2023, Cap. V, lett. A.
[547] Ibidem.
[548] Ibidem.
[549] Ibidem.

automatizzato, in virtù, del divieto di cui all'art. 22 del GDPR e quando, i *grey box AI system* comportino un uso improprio dei dati personali[550].

2.3. La responsabilità del funzionario nel caso in cui il procedimento sia "guidato" dall'IA

Nel par. 5 del Cap. I, sono illustrate le due problematiche relative al criterio di ripartizione della responsabilità interna qualora la condotta dannosa sia stata realizzata dall'IA o con il suo ausilio.

La prima problematica ha ad oggetto il se un funzionario della BCE, responsabile di una determinata fase del procedimento, possa rispondere o meno nei confronti della BCE per non aver vigilato correttamente sull'operato di un sistema di apprendimento automatico che ha causato dei danni.

La seconda, correlata alla prima, riguarda la presunta crisi dei concetti giuridici tradizionali, come il dolo e la colpa, non essendo più l'attività condotta unicamente dall'uomo.

In via preliminare, si ritiene che la diligenza richiesta al funzionario nello svolgimento delle sue mansioni non vari a seconda del grado di coinvolgimento del sistema IA nel procedimento.

Il funzionario dovrà sincerarsi che il sistema IA rispetti i requisiti imposti dall'*AI Act*, a seconda del tipo di rischio che presenta ed eventualmente, comunicare al suo supervisore eventuali violazioni.

In secondo luogo, in coerenza con quanto prescritto dalla Proposta di Direttiva sulla responsabilità dell'intelligenza artificiale, il soggetto responsabile dell'utilizzo, dovrà verificare che il sistema IA sia impiegato conformemente alle istruzioni per l'uso che accompagnano il sistema[551] e verificare la pertinenza dei dati di *input* a cui il sistema è stato esposto[552].

Con riferimento all'apporto del sistema nella procedura, il funzionario non potrà esimersi dalla valutazione dell'*output* prima di assumerlo come fattore per basare in parte o *in toto* una sua decisione.

---

[550] Ibidem.
[551] Art. 4, par. 3, lett. a) della Proposta di Direttiva.
[552] Art. 4, par. 3, lett. b) della Proposta di Direttiva.

Pertanto, sarà necessario garantire al funzionario la possibilità di comprendere il funzionamento interno dell'algoritmo attraverso tecniche XAI.

L'applicazione di queste tecniche potrebbe garantire il superamento della problematica legata alla presunta crisi dei concetti di dolo e colpa, infatti, il funzionario potrà valutare, autonomamente, quali fattori ha considerato l'algoritmo, il peso dato a ciascuno di essi ed il perché si è giunti ad un dato *output*. A tal fine sarà necessario collocare nei ruoli di supervisione dei sistemi di IA un personale qualificato e più in generale, avviare programmi di formazione sulla *Suptech*.

L'auspicio è che, per garantire la certezza del diritto, vengano redatte delle linee guida e *best practice* su come i funzionari debbano procedere alla valutazione dell'*output*, quindi, lo *standard* di diligenza e perizia richiesto a seconda dell'utilizzo che verrà fatto del sistema di apprendimento automatico.

Per concludere, non sarà necessario modificare la portata e il contenuto dei concetti giuridici tradizionali di dolo e colpa, in quanto, l'autonomia dei sistemi di IA troverà un limite invalicabile nella necessità, in ogni caso, di un atto di recepimento di un essere umano affinché la decisione esplichi effetti giuridici. L'opacità potrà esser attenuata o superata con le tecniche XAI che permetteranno di supervisionare l'algoritmo lungo tutto il processo di elaborazione dell'*output*.

3. Considerazioni sull'opportunità dell'impiego dell'IA nella vigilanza bancaria

Esaminato nei paragrafi precedenti se sia possibile, da un punto di vista giuridico, l'impiego dell'IA nella vigilanza bancaria e le caratteristiche che dovrà necessariamente avere, occorre chiedersi se sia anche opportuno o, meglio ancora, desiderabile. Il coinvolgimento dell'IA potrebbe render molto più complicato, per via della scarsa trasparenza che caratterizza i sistemi di apprendimento automatico, il controllo dell'operato della BCE da parte delle altre istituzioni europee e dell'opinione pubblica in generale. Le complicazioni deriverebbero esclusivamente da quei sistemi che nel processo decisionale andrebbero a ricoprire funzioni di supporto essenziale o addirittura, funzioni decisorie e non quelli impiegati per "attività interne" di raccolta di notizie, traduzione, riassunti ed estrapolazione di informazioni essenziali da documenti. Questo in ragione del fatto che l'esigenza di controllo attiene alla conformità procedurale e sostanziale della decisione di vigilanza e non ad ogni singola modalità di organizzazione

dell'attività. La questione è stata già prospettata in dottrina[553], con riferimento alla politica monetaria, ove ci si è chiesti se un impegno più pronunciato della BCE nelle questioni sociali potesse condurre ad un ampliamento di fatto del mandato secondario[554]. Infatti, l'impegno in tali ambiti avrebbe come conseguenza quella di rendere più complessa la verifica sull'operato della Banca e condurre a possibili istanze di revisione del regime di indipendenza[555]. Ci si chiede se tale riflessione possa, *mutatis mutandis*, esser fatta con riferimento all'impiego dell'IA nell'attività di supervisione bancaria.

Anche nell'ambito del MVU, l'indipendenza[556] della BCE, deve essere sempre accompagnata da una forte *accountability*[557]. Quest'ultima, assume rilevanza quando vengono attribuite funzioni ad organismi indipendenti, sganciati dal circuito politico e non aventi legittimazione democratica diretta, per evitare l'esercizio di un potere senza alcun tipo di controllo.

L'*accountability*, nell'ambito del MVU, è bidirezionale, cioè, si rivolge verso le istituzioni e verso i privati.

La prima, giustificata dall'esigenza di bilanciare l'indipendenza dell'istituzione, impone una serie di obblighi in capo alla BCE, affinché renda conto alle altre istituzioni dell'attuazione del presente regolamento[558]. Nello specifico, la BCE «*trasmette annualmente al Parlamento europeo, al Consiglio, alla Commissione e all'Eurogruppo una relazione sull'esecuzione dei compiti attribuitile*»[559] nonché è tenuta a «*rispondere oralmente o per iscritto alle interrogazioni o ai quesiti ad essa rivolti dal Parlamento*

---

[553] FELICETTI R., *A Study on Central Banks and Social Responsibility: the Case of the ESCB*, Journal of Financial Regulation Volume 10, Issue 1, 2024, par. 5.1. [Online]. Disponibile su: https://blogs.law.ox.ac.uk/oblb/blog-post/2024/04/study-central-banks-and-social-responsibility-case-escb

[554] Ai sensi dell'art. 127 TFUE: «*Fatto salvo l'obiettivo della stabilità dei prezzi, il SEBC sostiene le politiche economiche generali nell'Unione al fine di contribuire alla realizzazione degli obiettivi dell'Unione definiti nell'articolo 3 del trattato sull'Unione europea*».

[555] Si veda nota 553.

[556] L'indipendenza della BCE, anche nel MVU, assume quattro dimensioni diverse: istituzionale, personale, operativa e finanziaria. Cfr. MAGLIARI A., *Il Single Supervisory Mechanism. Funzioni e modelli di integrazione amministrativa* (tesi di dottorato), Trento: Università degli Studi di Trento, 2016, p. 105 ss. [Online]. Disponibile su: http://eprints-phd.biblio.unitn.it/1830/1/Magliari_TESI_DOTTORATO_Il_single_supervisory_mechanism._Funzioni_e_modelli_di_integrazione_amministrativa.pdf

[557] «*La BCE è un'istituzione indipendente che utilizza a totale discrezione i propri strumenti, ove necessario, per assolvere le sue funzioni e il suo mandato. Un complemento indispensabile di questa indipendenza è l'obbligo di rendere conto del proprio operato (accountability). La BCE è tenuta a rispondere del proprio operato al Parlamento europeo, in quanto istituzione che riunisce i rappresentanti eletti dei cittadini dell'UE*». Informazioni rinvenibili sul sito della BCE all'indirizzo: https://www.ecb.europa.eu/ecb/our-values/accountability/html/index.it.html

[558] Art. 20, par. 1 del Regolamento 1024/2013.

[559] Art. 20, par. 2 del Regolamento 1024/2013.

europeo, o dall'Eurogruppo conformemente alle proprie procedure»[560]. La stessa relazione dovrà esser presentata anche ai parlamenti nazionali degli Stati membri partecipanti, oltre alla possibilità anche per quest'ultimi di instaurare un dialogo istituzionale[561]. L'*accountability* verso i privati è rappresentata dalla previsione di garanzie sul piano procedimentale e giurisdizionale. La BCE, a livello procedimentale, concede alle persone il diritto ad esser sentite, di accedere al fascicolo e di ottenere una motivazione che illustri le ragioni a fondamento di una decisione[562].

Sul piano giurisdizionale è esperibile sia l'azione di annullamento prevista dall'art. 263 TFUE che l'azione di responsabilità per violazione del diritto dell'unione di cui all'art. 340 TFUE.

A livello interno, è, invece, istituita la Commissione amministrativa del riesame a cui qualsiasi persona fisica o giuridica può chiedere il riesame di una decisione della BCE presa nei suoi confronti o che la riguardi direttamente ed individualmente[563]. Il riesame interno della decisione ha ad oggetto la sua conformità procedurale e sostanziale con il regolamento[564].

Quanto detto, rispetto alla necessarietà di una marcata *accountability* per bilanciare l'indipendenza della BCE in materia di politica monetaria, vale anche quando essa riveste il ruolo di autorità di vigilanza degli enti creditizi.

In questo contesto, occorre chiedersi se il controllo sull'operato della BCE, quale autorità di vigilanza, possa divenire più complicato, sia per le istituzioni sia per la Commissione del riesame e la Corte di Giustizia, nel caso in cui l'IA concorra alla formazione della volontà decisionale.

A livello istituzionale, non è chiaro come la BCE possa rispondere a interrogazioni o a quesiti vertenti sulle procedure impiegate, data la natura oscura della maggior parte dei sistemi di apprendimento automatico. In generale, anche la redazione della stessa relazione potrebbe diventare difficile, avendo delegato l'esecuzione di talune fasi di tutti procedimenti di vigilanza, a sistemi di IA.

A livello interno, la Commissione del riesame potrebbe riscontrare difficoltà a valutare la conformità procedurale e sostanziale di una decisione con riferimento alla fase

[560] Art. 20, par. 6 del Regolamento 1024/2013.
[561] Art. 21 del Regolamento 1024/2013
[562] Art. 22 del Regolamento 1024/2013.
[563] Art. 25, par. 5 del Regolamento 1024/2013.
[564] Art. 25, par. 1 del Regolamento 1024/2013.

dell'attività svolta da sistemi di ML. Per fare un esempio, si pensi alla valutazione automatizzata sulla professionalità e onorabilità degli esponenti bancari. Il sistema, così come strutturato, è in grado di fornire un riassunto delle informazioni ed evidenziare eventuale "*red flag*" sui requisiti del candidato. Il rischio è che potrebbe non esser in grado di spiegare sulla base di quali criteri ha condotto la sintesi ed ha segnalato alcuni aspetti come critici, impedendo al funzionario di motivare appieno la decisione nel caso in cui decida di far affidamento sul lavoro svolto da tale sistema. Sulla base di ciò, come potrà la Commissione del riesame valutare la conformità di una procedura, che non è stata resa nota per via dei limiti tecnici dell'algoritmo?

Un'ulteriore questione riguarda la libertà della BCE nella scelta di come eseguire i compiti a lei assegnati; cioè, l'indipendenza di tale istituzione può spingersi sino a fare affidamento su sistemi, in generale progettati da società private, per il perseguimento di interessi pubblici, così importanti, rischiando di pregiudicare l'*accountability*.

4. I primi risvolti applicativi dell'IA da parte della BCE

Sino ad ora si è fatto riferimento, per comodità espositiva, ai sistemi di apprendimento automatico in generale, citando solo alcune delle varie applicazioni IA nella vigilanza bancaria della BCE.

Attualmente, le applicazioni di IA consentono alla BCE di interrogare i dati di vigilanza e di utilizzare funzionalità di *chatbot* per normative e metodologie di vigilanza[565]. Lo sviluppo di tali applicazioni è stato reso possibile grazie al *SupTech Hub*. Questo centro, come è stato detto nel Cap. 1, par. 3.3, promuove la collaborazione interdisciplinare per l'elaborazione di tecnologie di supervisione innovative attraverso l'utilizzo di risorse umane con elevate competenze in materia di intelligenza artificiale, di vigilanza bancaria e di protezione dei dati personali. In quest'ultimo caso, essendo inevitabile il trattamento dei dati personali per ciascun sistema, le applicazioni dovranno rispettare gli adempimenti imposti dal GDPR.

Con riferimento all'*AI Act*, la disciplina applicabile dipenderà dal tipo di funzione che sono destinati a svolgere e quindi, non si potrà prescindere dall'analisi caso per caso.

[565] MCCAUL E., *The impact of suptech on European banking supervision*, at the Supervision Innovators Conference, 2022.

Nei prossimi paragrafi verranno descritte, singolarmente, le principali innovazioni sperimentate dalla BCE e verranno fatti alcuni cenni su applicazioni di singole autorità nazionali.

4.1. La lettura automatica del questionario "*fit and proper*": *Heimdall*

Ai sensi dell'art. 4, par. 1, lett. e) del Regolamento SSM, la BCE è tenuta ad assicurare il rispetto dei requisiti di professionalità e onorabilità per le persone responsabili dell'amministrazione degli enti creditizi.

La BCE conduce ogni anno circa 2500 valutazioni di idoneità, su questionari lunghi fino a 40 pagine, presentati in diversi formati e lingue a seconda dello Stato partecipante di provenienza[566].

Per questo motivo, si è deciso di sviluppare uno strumento che, utilizzando tecniche di ML, da un lato, analizzi e trasformi tutte le informazioni contenute nei questionari facilitando il lavoro del funzionario e dall'altro, identifichi immediatamente eventuali dubbi sulle credenziali che richiederebbero un ulteriore esame[567]. Lo strumento è stato denominato *Heimdall* ed è in uso dal giugno del 2022.

L'utilizzo di questo sistema IA è in grado di far risparmiare tempo alle risorse umane addette alla valutazione del questionario "*fit and proper*" ed agevola la registrazione delle informazioni archiviandole digitalmente[568]. D'altro canto, è presente il rischio della commissione di errori nella scansione dei dati e nella loro elaborazione oltre il rischio effettuare segnalazioni errate a causa di *bias* cognitivi.

Allo stato attuale, lo strumento non sembra destare particolare preoccupazione per il diritto ad una buona amministrazione, in quanto l'attività di valutazione dei risultati dello stesso è mediata da un'attività umana. *Heimdall* indica solo le situazioni in cui è richiesto un esame più approfondito del funzionario che a seguito dello stesso avvierà la procedura di audizione con l'esponente e prenderà una decisione motivata.

Tuttavia, se in futuro lo strumento dovesse esser usato per eseguire una valutazione completa sull'idoneità di uno dei soggetti di cui all'art. 4 par. 1, lett. e) vanificando il

[566] Financial Stability Board, *The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions - Market developments and financial stability implications*, 2020, Allegato 1 – Caso studio 8.
[567] Ibidem.
[568] Ibidem.

ruolo del funzionario allora, senza dei dovuti accorgimenti tecnici, contrasterà con il diritto ad avere una buona amministrazione.

4.2. Un sistema di allerta precoce per le istituzioni meno significative

La BCE esercita, in linea generale, la vigilanza diretta sulle banche significative[569], mentre le autorità nazionali competenti su quelle meno significative[570]. Nonostante ciò, la BCE rimane responsabile del funzionamento del MVU.

Per questo motivo, al fine di supportare il lavoro delle autorità nazionali competenti, è stato sviluppato uno strumento che identifica gli istituti che necessitano di esser monitorati più da vicino, onde scongiurare difficoltà finanziare[571]. Il modello si avvale di una tecnica di ML finalizzata ad ottenere, per ogni istituto vigilato, un elenco di variabili e di indicatori di rischio chiave, tali da permettere di prevedere con sufficiente anticipo i casi di una futura sofferenza finanziaria[572].

La capacità di comprendere correttamente quale tra i migliaia di istituti sia a rischio, dipenderà da un addestramento condotto su grandi quantità di dati di elevato livello qualitativo.

Anche in questo caso, come nel paragrafo precedente, lo strumento esplica le sue funzioni nell'attività di indagine e non ha particolari effetti verso l'esterno, in quanto, le misure opportune saranno adottate solo al seguito di un'attività umana di valutazione dei risultati che tenga conto anche di altri fattori.

Tuttavia, nel caso in cui si decidesse di far dipendere dalla sola segnalazione del sistema di allerta precoce delle misure in grado di incidere nella sfera giuridica degli interessati, sussisteranno motivi di attrito con la buona amministrazione.

4.3. *NAVI - Network Analytics and Visualisation*

È uno strumento *SupTech* che utilizza la tecnica dell'analisi di rete per ottenere una visualizzazione grafica delle strutture proprietarie delle banche vigilate e più in generale,

---

[569] In linea generale, la BCE esercita vigilanza diretta sulle banche significative ed in casi eccezionali, anche su quelle non significative.
[570] Art. 6 del Regolamento 1024/2013.
[571] Financial Stability Board, *The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions - Market developments and financial stability implications*, 2020, Allegato 1 – Caso studio 15.
[572] Ibidem.

attraverso la combinazione di dati provenienti da numerose fonti, ottenere una panoramica completa dei proprietari delle banche e delle loro interdipendenze[573].

In particolare, va a rappresentare l'entità delle partecipazioni di questi e di altri gruppi di azionisti, negli enti creditizi dei paesi partecipanti al MVU, nonché, la misura in cui gli azionisti di enti significativi sono interconnessi[574].

L'idea di sviluppare NAVI è figlia di due ordini di ragioni: la BCE deve avere un quadro chiaro degli assetti proprietari delle banche e delle partecipazioni incrociate che detengono i vari gruppi di investitori data la complessità del loro assetto strutturale; sviluppare una capacità di filtraggio per permettere ai funzionari di concentrarsi sulle interconnessioni più importanti[575].

Sebbene anche per questa applicazione valgano le considerazioni fatte nei paragrafi precedenti con riferimento al diritto ad avere una buona amministrazione, il rischio maggiore è che il funzionario possa far eccessivo affidamento sullo strumento concentrandosi solo su quelle interconnessioni che NAVI ha reputato rilevanti, trascurando le altre.

4.4. *Athena*

Athena è una piattaforma finalizzata ad assistere la BCE nella ricerca, estrazione ed analisi di informazioni contenute in articoli, *report* di vigilanza e documenti finanziari[576].

Questo sistema integra un motore di ricerca avanzato e utilizza tecnologie di elaborazione del linguaggio naturale, riconoscimento ottico dei caratteri automatizzato e funzionalità multilingue per minimizzare il lavoro manuale nelle attività di supervisione[577].

Anche questo sistema svolge un'attività di ottimizzazione delle ore di lavoro disponibili che non esplica effetti giuridici verso i destinatari della decisione.

---

[573] Informazioni rinvenibili sul sito della BCE nell'articolo: *From data to decisions: AI and supervision*: https://www.bankingsupervision.europa.eu/press/interviews/date/2024/html/ssm.in240226~c6f7fc9251.en.html

[574] Financial Stability Board, *The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions - Market developments and financial stability implications*, 2020, Allegato 1 – Caso studio 21.

[575] Ibidem.

[576] Informazioni rinvenibili sul sito della BCE nell'articolo: *Suptech: thriving in the digital age*: https://www.bankingsupervision.europa.eu/press/publications/newsletter/2023/html/ssm.nl231115_2.en.html

[577] Ibidem.

4.5. SREP - *Truffle Search Analytics* per documenti di testo strutturati

Le autorità di vigilanza effettuano un'analisi periodica dei rischi di ciascuna banca, un passaggio cruciale noto come "processo di revisione e valutazione prudenziale" (*supervisory review and evaluation process*, SREP).

Questo processo implica la raccolta e la sintesi dei dati analitici annuali, al fine di valutare la solidità patrimoniale dell'istituto e la qualità della sua gestione del rischio, sulla base dei quali vengono stabilite le azioni correttive che la banca deve adottare[578]. Al termine di questo processo, l'autorità di vigilanza formula delle direttive chiare, inviate alla banca, che delineano le misure essenziali per affrontare le problematiche identificate, e la banca sarà tenuta a implementare le soluzioni correttive entro i termini stabiliti[579].

Per questo motivo, è stato previsto uno strumento di ML, denominato *Truffle Analytics*, in grado di identificare, tra le diverse decisioni SREP, le tendenze emergenti e i gruppi di rischio[580].

Oltre alla ricerca di parole chiave, consente di produrre grafici e metriche rilevanti, che possono essere personalizzate dall'autorità di vigilanza con una serie di funzioni di filtraggio[581]. Valgono le stesse considerazioni con riferimento all'impatto sui diritti fondamentali fatte nei paragrafi precedenti.

4.6. *Agora*

Un altro strumento sviluppato dalla BCE è *Agora* che garantisce un unico *data lake*[582] per tutti i dati riguardanti la vigilanza bancaria come dati statistici o commerciali che altrimenti sarebbero dispersi in vari sistemi[583].

---

[578] Informazioni rinvenibili sul sito della BCE nell'articolo: Cos'è lo SREP?: https://www.bankingsupervision.europa.eu/about/ssmexplained/html/srep.it.html

[579] Ibidem.

[580] Financial Stability Board, *The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions - Market developments and financial stability implications*, 2020, Allegato 1 – Caso studio 16.

[581] Ibidem.

[582] «*Un data lake è un repository centralizzato che permette di archiviare tutti i dati strutturati e non su qualsiasi scala. È possibile archiviare i dati così come sono, senza doverli prima strutturare, ed eseguire diversi tipi di analisi dei dati - da pannelli di controllo e visualizzazioni all'elaborazione di Big Data, analisi dei dati in tempo reale e machine learning per prendere decisioni migliori*». La definizione è tratta dal sito: https://aws.amazon.com/it/what-is/data-lake/

[583] Informazioni rinvenibili sul sito della BCE nell'articolo: *Scaling up suptech*: https://www.bankingsupervision.europa.eu/press/publications/newsletter/2022/html/ssm.nl221117_4.en.html

Il vantaggio è di facilitare i supervisori nell'analisi dei dati in modo più rapido ed efficiente.

Attualmente il sistema richiede, al fine di accedere al *database*, una certa conoscenza del linguaggio di programmazione dell'utente, ma attraverso l'uso dell'intelligenza artificiale generativa i supervisori, senza esperienza di programmazione, potrebbero chiedere ad *Agora* dove trovare punti dati molto specifici[584]. Lo strumento, avendo come obiettivo quello di facilitare e velocizzare la ricerca di informazioni, non presenta particolari motivi di attrito con il diritto ad una buona amministrazione.

4.7. La *Sentiment Analysis*

La *Sentiment Analysis* è un'analisi finalizzata a consentire alle autorità di vigilanza di valutare come l'istituto di vigilanza è percepito dal pubblico al fine di integrare la valutazione SREP con informazioni pertinenti[585].

La BCE, nel 2020, si è domandata come ottimizzare l'analisi del *sentiment* attraverso l'utilizzo di tecniche di elaborazione del linguaggio naturale e di ML e ha progettato uno strumento che dovrebbe fornire, in *dashboard format*, una panoramica del *sentiment* di mercato durante un periodo di tempo e raggruppare gli argomenti identificati in categorie di rischio[586]. Lo strumento, avendo come obiettivo quello di facilitare l'analisi, non presenta particolari motivi di attrito con il diritto alla buona amministrazione.

4.8. Il *credit risk forecasting*

Uno degli obiettivi della BCE è quello di migliorare la previsione del rischio di credito. Il rischio di credito consiste nel rischio di perdita della banca in caso d'inadempimento dei debitori. L'autorità di vigilanza accerta che gli istituti bancari abbiano delineato un sistema di controllo e gestione del rischio di credito verificando che tali politiche e processi costituiscano contesto adeguato al monitoraggio di tale rischio[587].

---

[584] Informazioni rinvenibili sul sito della BCE nell'articolo: *From data to decisions: AI and supervision*: https://www.bankingsupervision.europa.eu/press/interviews/date/2024/html/ssm.in240226~c6f7fc9251.en.html

[585] Financial Stability Board, *The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions - Market developments and financial stability implications*, 2020, Allegato 1 – Caso studio 20.

[586] Ibidem.

[587] Si veda par. 1.2 del Cap. I.

Alla luce di ciò, la BCE ha sviluppato uno strumento di analisi avanzata dei dati, basato sul ML, per prevedere meglio il rischio di credito, attraverso la combinazione dei dati di settore a livello di prestiti bancari, le previsioni macroeconomiche e le informazioni prudenziali[588].

Lo strumento, avendo come obiettivo quello di facilitare l'analisi, non presenta particolari motivi di attrito con il diritto alla buona amministrazione.

4.9. Cenni sulle applicazioni da parte della Banca d'Italia e delle altre autorità di vigilanza nazionali

Il fenomeno *SupTech* non ha coinvolto solo la BCE ma anche le autorità di vigilanza di Stati partecipanti e non al MVU. Sono numerosi i sistemi di IA utilizzati da ciascuna autorità, per questo motivo, la trattazione sarà limitata a dei brevi cenni sugli strumenti utilizzati dalle autorità più all'avanguardia sotto questo punto di vista.

La Banca d'Italia, nella relazione sulla gestione relativa all'anno 2023, ha dichiarato di aver utilizzato uno strumento volto a verificare l'idoneità degli esponenti aziendali degli intermediari vigilati sulla base dei requisiti e dei criteri fissati dal decreto ministeriale del n°169 del 23 novembre del 2020[589]. Inoltre, ha impiegato tecniche di IA in grado di leggere e schematizzare automaticamente i verbali degli organi degli intermediari a supporto delle verifiche sugli assetti proprietari e delle attività di redazione e revisione dei rilievi ispettivi[590].

La *Monetary Authority of Singapore* (MAS) che svolge anche funzione di vigilanza degli istituti di credito, utilizza l'intelligenza artificiale in modi strategici per migliorare l'efficacia e l'efficienza della supervisione nel settore bancario.

Nell'ambito della vigilanza in materia di gestione del rischio di riciclaggio e finanziamento del terrorismo, il MAS ha sviluppato uno strumento di *Network Analysis*

[588] Financial Stability Board, *The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions - Market developments and financial stability implications*, 2020, Allegato 1 – Caso studio 21.

[589] Banca d'Italia, Relazione sulla gestione e sulle attività, 31 maggio 2014, p. 76. [Online]. Disponibile: https://www.bancaditalia.it/pubblicazioni/relazione-gestione/2024/rel_gest_BI-2023.pdf

[590] Ibidem.

di segnalazione di transazioni sospette su flussi di denaro potenzialmente illeciti, in grado di agevolare la vigilanza riducendo la complessità delle transazioni[591].

Un ulteriore settore di applicazione dei sistemi di IA riguarda la valutazione dei segnali d'allarme. Questa attività, tradizionalmente affidata al giudizio umano, è oggi supportata da algoritmi automatizzati che permettono ai supervisori di analizzare interi *set* di dati, invece, di affidarsi al solo campionamento[592].

Fra gli Stati partecipanti al MVU, la Francia con l'*Autorité de contrôle prudentiel et de résolution* è sicuramente quella che ha avviato il numero maggiore di progetti ("*J-Veille*", "*Isitext*", "*Dixit*", "*Kartodoc*") all'interno di un progetto più generale volto ad incrementare il livello di efficienza della supervisione automatizzando i controlli che richiedono un tempo maggiore[593].

Tra i vari progetti, c'è "*J-Veille*" che si serve di un algoritmo basato su NLP per facilitare l'estrapolazione di informazioni rilevanti nelle decisioni giudiziarie, al fine di identificare le pratiche bancarie scorrette[594].

Poi, vi è "*Isitext*" il cui obiettivo è quello di verificare la coerenza ed identificare le questioni chiave di tutti i "*narrative reports*" (ogni relazione è lunga dalle 50 alle 100 pagine) inviati dalle autorità[595].

Con "*Dixit*", invece, si facilita la ricerca della normativa bancaria, sempre più ampia e complessa e dispersa in numerose fonti, per permettere ai supervisori di vagliare la conformità alla normativa degli istituti di credito[596].

In ultimo "*Kartodoc*", che mira a facilitare il lavoro dei supervisori, attraverso un motore di ricerca unificato in grado di ordinare tutti i tipi di *file* (dai pdf ai fogli di calcolo *Excel*), inviati dagli istituti vigilati, per poter permettere agli stessi di focalizzarsi sull'analisi delle informazioni presenti al loro interno.

---

[591] Financial Stability Board, *The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions - Market developments and financial stability implications*, 2020, Allegato 1 – Caso studio 12.
[592] Ivi – Caso studio 19.
[593] Ivi – Caso studio 22.
[594] Ibidem.
[595] Ibidem.
[596] Ibidem.

5. Riflessioni conclusive

Nel corso di questo elaborato è stato illustrato al lettore il fenomeno *SupTech*, in particolare hanno costituito oggetto di approfondimento le implicazioni derivanti dall'uso di tecnologie basate sull'intelligenza artificiale nella vigilanza bancaria. Sono state esplorate le potenzialità delle nuove tecnologie nel migliorare l'attività di supervisione della BCE, ma allo stesso tempo, si è fatto luce sui motivi di attrito esistenti con il quadro normativo (attuale e futuro) e istituzionale.

In questo paragrafo conclusivo, l'obiettivo è quello di offrire un manuale di azione per delineare specifiche raccomandazioni su cosa la BCE dovrebbe fare e cosa dovrebbe evitare per garantire che l'uso dell'IA nella vigilanza bancaria rispetti la "buona amministrazione", la disciplina a tutela dei dati personali, e l'*accountability* verso le istituzioni, i privati destinatari dei procedimenti di vigilanza e più in generale, dell'opinione pubblica.

Nella sua funzione di vigilanza è utile distinguere, come descritto nel par. 4.1. del Cap. 1, tra "poteri di vigilanza" e "strumenti di vigilanza" al fine di comprendere le differenze tra le varie sfaccettature dell'attività ma soprattutto, per valutare l'impatto che eventuali applicazioni IA potranno avere a seconda del grado di partecipazione al procedimento decisionale. I "poteri di vigilanza" sono quelli in cui la BCE è chiamata a prendere una decisione. Gli "strumenti di vigilanza" si riferiscono alle tecniche utilizzate per monitorare il soddisfacimento dei requisiti prudenziali e quindi, individuare eventuali violazioni o rischi che potrebbero pregiudicare lo stato di salute di una banca.

Non tutti i sistemi di IA presentano gli stessi rischi, molto dipende dalla tecnica su cui si basano e dal ruolo che essi svolgono all'interno dell'attività di supervisione.

In relazione al primo aspetto, al par. 2.1. del Cap. I, si sono distinti gli algoritmi condizionali da quelli basati sul *machine learning*. I primi, operando con metodo causale ed in modo trasparente e facilmente interpretabile, non dovrebbero costituire un pericolo né per la buona amministrazione né per la tutela dei dati personali (non avendo bisogno di *set* di dati per allenarsi) né per l'*accountability* (essendo il loro operato trasparente). Con riferimento alla buona amministrazione, gli algoritmi condizionali opererebbero in modo imparziale, eseguendo, a seconda dei casi, un blocco di codice, nel caso in cui le condizioni si siano realizzate ed un altro, nel caso in cui ciò non sia avvenuto. Inoltre, sarebbero perfettamente in grado di motivare una decisione, in quanto trasparenti e

operanti sulla base di un metodo causale, quindi, in grado di dimostrare perché da determinate premesse si è arrivati ad una data conclusione. Alla luce di queste caratteristiche, tali algoritmi potrebbero, in astratto, esser utilizzati sia come "strumenti di vigilanza" per svolgere un'attività non avente riflessi diretti nella sfera giuridica dei soggetti vigilati, sia per concorrere o addirittura, determinare la decisione e quindi, esercitare un "potere di vigilanza".
Tuttavia, a causa della loro natura deduttiva e non esperienziale, come affermato al par. 2.1 del Cap. I, mal si conciliano, in generale, con l'attività della BCE, i cui i parametri normativi che circoscrivono l'operato non sono stringenti e lasciano ampia discrezionalità nell'esercizio delle funzioni di vigilanza.

I secondi, gli algoritmi di ML alla base di un sistema di IA, svolgono operazioni, senza istruzioni esplicite, attraverso l'utilizzo di una logica induttiva, quindi, legata ad un modello esperienziale. Tali sistemi, da un lato, garantiscono la possibilità di comprendere come l'autorità ha agito in casi analoghi o simili e dall'altro, di prendere in considerazione molte più variabili contemporaneamente.
Non a caso la BCE, seguita da numerose autorità di vigilanza nazionali, ha incominciato già dal 2020 ad impiegare, in costanza della propria attività, sistemi basati prevalentemente su tecniche di ML e DL, in quanto, più adatti per caratteristiche tecniche.
Allo stato attuale, come è desumibile dai paragrafi precedenti, gli strumenti di apprendimento automatico vengono impiegati dalla BCE per attività di raccolta di notizie, traduzione, riassunti, estrapolazione di informazioni essenziali da documenti, nonché, per svolgere attività come la previsione del rischio di credito, di allerta precoce e di individuazione di eventuali ostacoli, in capo a persone fisiche, a rivestire incarichi di amministrazione e direzione.
In questi casi, i rischi, sia per la buona amministrazione che per l'*accountability* sono pressoché assenti, in quanto non vi sarebbero differenze sostanziali dall'impiego, in tali attività, di assistenti umani o stagisti. Infatti, il risultato delle attività sopraelencate non è di per sé in grado di esplicare effetti verso il destinatario del procedimento né di impedire alla BCE di render conto del proprio operato alle altre istituzioni. In più, la presenza del sistema non verrebbe nemmeno avvertita dal destinatario del procedimento, che sarà in grado di esercitare i diritti connessi alla buona amministrazione, interfacciandosi in ogni momento con un funzionario persona fisica.

L'impiego dell'*output* di un sistema di apprendimento automatico sarà vagliato dal funzionario che ne valuterà la qualità e la fondatezza (nel caso in cui si tratti di una segnalazione di una violazione di un requisito prudenziale o di assenza di un requisito per la carica di amministratore). La valutazione, però, può divenire estremamente complessa, data le numerose difficoltà che si possano incontrare nella comprensione del funzionamento interno per via della scarsa trasparenza. Per questo motivo, l'impiego dovrebbe limitarsi ai sistemi "*grey box*"[597] o al massimo, ai "*black box*" il cui funzionamento è desumibile, in via indiretta, attraverso l'utilizzo di tecniche XAI affidabili e verificate[598].

Diverso è il caso in cui, tali strumenti, siano impiegati per assumere una decisione, che viene fatta propria dall'organo competente automaticamente. Si pensi ad un sistema di valutazione "*fit and proper*" che non si limiti alla sola lettura e valutazione del questionario, come avviene attualmente, ma ad un esame completo sull'idoneità di un determinato soggetto. Questa situazione non permetterebbe, allo stato attuale della tecnica, al destinatario del procedimento di esercitare i diritti connessi alla buona amministrazione. Infatti, per quanto riguarda il diritto ad esser ascoltati, rimarrebbe irrisolta la questione sul peso che verrà dato alla versione offerta dall'amministratore per difendere la propria posizione, nel caso in cui sussistano dubbi sulla sua idoneità a rivestire quel ruolo. In secondo luogo, ad oggi, le tecniche XAI non sono in grado, con elevato livello di certezza e in tempi brevi, di dare una spiegazione del perché si è giunti ad un dato *output* e quindi, non sarebbe esercitabile il diritto ad ottenere una decisione motivata e di conseguenza, anche a contestare la decisione. Tuttavia, in relazione, a quest'ultimo aspetto, tale diritto sarebbe pregiudicato solo in astratto[599], in quanto, in concreto il provvedimento sarebbe, comunque, invalido per difetto di motivazione.

Un ulteriore ostacolo, come illustrato analiticamente nel par. 1.2.1. di questo Capitolo, è l'art. 22 del GDPR che vieta i trattamenti dei dati personali interamente automatizzati. Tuttavia, è probabile che in futuro, ai sensi del par. 2 dell'articolo in questione, la possibilità che il diritto dell'Unione escluda dal divieto i procedimenti di vigilanza della BCE.

[597] Si veda il par. 1.1. di questo Capitolo.
[598] Ibidem.
[599] Il destinatario, in assenza di motivazione, è in grado di comprendere le ragioni alla base della decisione.

In conclusione, l'auspicio è che l'elaborato, sebbene offra una chiave di lettura per cercare di superare la relazione conflittuale tra intelligenza artificiale e vigilanza bancaria, possa inaugurare un'intensa stagione di studi accademici. Allo stesso tempo, si spera che le istituzioni europee prendano in considerazione l'elaborazione di linee guida, se non addirittura di normative specifiche, che indichino alla BCE in che modo e in quale fase del procedimento impiegare i sistemi di IA, onde evitare, da un lato, la lesione del diritto ad avere una buona amministrazione e alla protezione dei dati personali e dall'altro, possibili ed eventuali istanze di revisione del regime di indipendenza della BCE.

BIBLIOGRAFIA

BATHAEE Y., "*The Artificial Intelligence Black Box and the Failure of Intent and Causation*", 31 Harvard Journal of Law & Technology, 2018. [Online]. Disponibile su: https://jolt.law.harvard.edu/volumes/volume-31

BOURTOULE L. *et al*., *Machine Unlearning*, 2021 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2021, introduction. [Online]. Disponibile su: https://ieeexplore.ieee.org/abstract/document/9519428

BRENNER M., *The Role of AI in Cloud Computing*, in The Forecast by Nutanix, 2023. [Online]. Disponibile su: https://www.nutanix.com/theforecastbynutanix/technology/ai-in-the-cloud

BRESCIAMORRA C., *Il diritto delle banche*, Il Mulino, Bologna, 2020.

BUSUIOC V. M., *Accountability, Control and Independence: The Case of European Agencies*, 15 Europe LJ 599, 2009. [Online]. Disponibile su: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1838265

CAPELLI M., *Codice sorgente*, Enciclopedia della Scienza e della Tecnica, 2008. [Online]. Disponibile su: https://www.treccani.it/enciclopedia/codice-sorgente_(Enciclopedia-della-Scienza-e-della-Tecnica)/

CARULLO G., *Decisione amministrativa e intelligenza artificiale*, in: Diritto dell'informazione e dell'informatica, fasc. 3, 2021. [Online]. Disponibile su: https://air.unimi.it/handle/2434/891372

CASONATO C., MARCHETTI B., *Prime osservazioni sulla proposta di regolamento della Commissione Ue in materia di intelligenza artificiale*, in "BioLaw Journal - Rivista di BioDiritto", n. 3, pp. 415-437, 2021. [Online]. Disponibile su: https://www.biodiritto.org/Online-First-BLJ/Online-First-BLJ-3-21-Prime-osservazioni-sulla-proposta-di-Regolamento-dell-Unione-europea-in-materia-di-Intelligenza-Artificiale

CELONE C., "*Il nuovo rapporto tra cittadino e pubblica amministrazione alla luce dell'art. 41 della Carta dei diritti fondamentali dell'unione europea*", in Editoriale

Scientifica Napoli a cura di Astone F. *et al*, 2017. [Online]. Disponibile su: https://iris.unipa.it/retrieve/e3ad891b-7085-da0e-e053-3705fe0a2b96/Art%2041%20Carta%20dei%20diritti%20fondamentali%20dell%27Unione%20europea.pdf

CHOLLET F., *Deep learning with Python*, II Ed., Manning, Shelther Island, New York, 2021. [Online]. Disponibile su: https://sourestdeeds.github.io/pdf/Deep%20Learning%20with%20Python.pdf

COELHO R., DE SIMONI M., PRENIO J., *N. 14 - Applicazioni suptech per l'antiriciclaggio*, in Quaderni dell'antiriciclaggio, 2019. [Online]. Disponibile su: https://uif.bancaditalia.it/pubblicazioni/quaderni/2019/quaderno-14-2019/index.html

COGLIANESE C., LEHR D., *Regulating by Robot: Administrative Decision Making in the Machine-Learning Era*, 105(5) Georgetown Law Journal 1147. [Online]. Disponibile su: https://scholarship.law.upenn.edu/faculty_scholarship/1734/

CONTISSA G., GALLI F., GODANO F., SARTOR G., *Il Regolamento europeo sull'intelligenza artificiale. Analisi informatico – giuridica*, in i-lex. Rivista di Scienza Giuridiche, Scienze Cognitive ed Intelligenza Artificiale, 2021. [Online]. Disponibile su: http://www.i-lex.it/articles/Volume14/Fascicolo2RegulationOfAI/Contissa_et_al_Proposta_regolamento.pdf

D'AMBROSIO R., *The ECB and NCA liability within the Single Supervisory Mechanism*, in Quaderni di Ricerca Giuridica della Banca d'Italia, 2015, n. 78. [Online]. Disponibile su: https://www.bancaditalia.it/pubblicazioni/quaderni-giuridici/2015-0078/index.html

DI CASTRI S. *et al*., "*The suptech generations*", FSI Insights on policy implementation No Bank for International Settlements, 2019 [Online]. Disponibile su: The suptech generations (bis.org)

DUARTE F. A. e LANCEIRO R. T., *Vulnerability and the Algorithmic Public Administration: Administrative Principles for a Public Administration of the Future* ,62(1) Revista da Faculdade de Direito da Universidade de Lisboa 1, 2021. [Online]. Disponibile su:

https://www.fd.ulisboa.pt/wp-content/uploads/2021/10/Francisco-de-Abreu-Duarte-Rui-Tavares-Lanceiro.pdf

FELICETTI R., *A Study on Central Banks and Social Responsibility: the Case of the ESCB*, Journal of Financial Regulation Volume 10, Issue 1, 2024. [Online]. Disponibile su: https://blogs.law.ox.ac.uk/oblb/blog-post/2024/04/study-central-banks-and-social-responsibility-case-escb

FERILLI S. *et al*., *L'intelligenza artificiale per lo sviluppo sostenibile*, Consiglio Nazionale delle Ricerche, 2021. [Online]. Disponibile: https://www.cnr.it/sites/default/files/public/media/attivita/editoria/VOLUME%20FULL%2014%20digital%20LIGHT.pdf

FINOCCHIARO G., *La proposta di Regolamento sull'intelligenza artificiale. Il modello europeo basato sulla gestione del rischio*, in "Il diritto dell'informazione o dell'informatica, n. 2, 2022. [Online]. Disponibile su: https://www.digitalmedialaws.com/wp-content/uploads/2022/11/Giusella-Finocchiaro.pdf

FLORIDI L., *Etica dell'intelligenza artificiale. Sviluppi, opportunità e sfide*, s.l., Raffaello Cortina Editore, 2022. [Online]. Disponibile su: https://books.google.it/books?id=kABlEAAAQBAJ&printsec=copyright&hl=it#v=onepage&q&f=false

FRATICCELLI C., "*L'integrazione amministrativa europea nel settore delle telecomunicazioni"*, Università degli Studi Roma Tre facoltà di giurisprudenza, 2008. [Online]. Disponibile: https://opac.bncf.firenze.sbn.it/Record/TD10016328

GALETTA D.U., "*Il diritto ad una buona amministrazione nei procedimenti amministrativi oggi (anche alla luce delle discussioni sull'ambito di applicazione dell'art. 41 della Carta dei diritti UE)*", in M.C. Pierro (a cura di), *Il diritto a una buona amministrazione nei procedimenti tributari*, Giuffré Francis Lefebvre, Milano, 2019. [Online]. Disponibile su: https://air.unimi.it/retrieve/dfa8b9a1-d298-748b-e0533a05fe0a3a96/Saggio2019VolTributaristiOpenAccess.pdf

GALLI G., LOREGGIA A., MAROCCIA I., VALPEDA I., *Intelligenza artificiale: cos'è e dov'è*, in Osservatorio sui Conti Pubblici Italiani, 2023. [Online]. Disponibile su: https://osservatoriocpi.unicatt.it/ocpiIntelligenza%20Artificiale%20cosa%20e%20dove.pdf.

GOHEL P, SINGH P., MOHANTY M., *Explainable AI: current status and future directions*, Centre for Forensic Science, University of Technology Sydney, Australia, 2016. [Online]. Disponibile su: https://arxiv.org/abs/2107.07045

GRAZIANI A., *Silicon Valley Bank, il primo default nell'era del mobile banking e dei social,* Il Sole 24 ORE, 2023. [Online]. Disponibile su: https://www.ilsole24ore.com/art/silicon-valley-bank-primo-default-nell-era-mobile-banking-e-social-AE5bwj3C

HACKER P., PASSOTH J.-H., *Varieties of AI Explanations Under the Law. From the GDPR to the AIA, and Beyond*, in Andreas Holzinger and others (eds), xxAI - Beyond Explainable AI, 2022. [Online]. Disponibile su: https://link.springer.com/chapter/10.1007/978-3-031-04083-2_17

HOFFMAN R. *et al*., *Metrics for Explainable AI: Challenges and Prospects*, arXiv, 2018. [Online]. Disponibile su: https://arxiv.org/abs/1812.04608

HOFMANN CH., MIHAESCU B., *The Relation between the Charter's Fundamental Rights and the Unwritten General Principles of EU Law: Good Administration as the Test Case*, in 9 EU Constitutional Law Review 73, 2013. [Online]. Disponibile su: https://www.researchgate.net/publication/259432820_The_Relation_between_the_Charter's_Fundamental_Rights_and_the_Unwritten_General_Principles_of_EU_Law_Good_Administration_as_the_Test_Case

HUGGINS A., *Addressing Disconnection: Automated Decision-Making, Administrative Law and Regulatory*, 44(3) University of New South Wales Law Journal 1048, 2021. [Online]. Disponibile su: https://www.researchgate.net/publication/356974750_Addressing_Disconnection_Automated_Decision-Making_Administrative_Law_and_Regulatory_Reform

JOHNSON M. J., *A Concise Introduction to Programming in Python*, CRC Press, 2018. [Online]. Disponibile su: https://dokumen.pub/a-concise-introduction-to-programming-in-python-second-edition-2nbsped-9781138082588-1138082589.html

JORION P., *Value at Risk: The New Benchmark for Managing Financial Risk*, New York: McGraw-Hill, 2007. [Online]. Disponibile su: https://www.researchgate.net/publication/243767965_Value_at_Risk_The_New_Benchmark_for_Managing_Financial_Risk

LAVECCHIA V., *Differenza tra Apprendimento supervisionato, non supervisionato e con rinforzo*, Informatica e Ingegneria online. [Online]. Disponibile su: https://vitolavecchia.altervista.org/differenza-tra-apprendimento-supervisionato-non-supervisionato-e-con-rinforzo/

LEGG S., HUTTER M, *Universal Intelligence: A Definition of Machine Intelligence*, *Minds and Machines*. 17, pp. 391-444, 2024. [Online]. Disponibile su: https://philpapers.org/rec/LEGUIA

LEO M. *et al*., "Machine *Learning in Banking Risk Management: A Literature Review*" in Risks, 2019. [Online]. Disponibile su: https://www.mdpi.com/2227-9091/7/1/29

LETTIERI N., DONÀ S., *Critical data studies e tecno-regolazione. Paradigmi emergenti di ricerca e tutela nell'era del lavoro data-driven*, su Dirittifondamentali.it - Fascicolo 2/2020, 2020. [Online]. Disponibile se: https://dirittifondamentali.it/wp-content/uploads/2020/06/Lettieri-Don%C3%A0-Critical-data-studies-e-tecno-regolazione.-Paradigmi-emergenti-di-ricerca-e-tutela-nell%E2%80%99era-del-lavoro-data-driven.pdf

LO SAPIO G., *La black box: l'esplicabilità delle scelte algoritmiche quale garanzia di buona amministrazione*, in Federalismi.it, n. 16/2021, 2021. [Online]. Disponibile su: https://www.federalismi.it/nv14/articolo-documento.cfm?artid=45610

MAGLIARI A., *Il Single Supervisory Mechanism. Funzioni e modelli di integrazione amministrativa* (tesi di dottorato), Trento: Università degli Studi di Trento, 2016. [Online]. Disponibile su: http://eprints-

phd.biblio.unitn.it/1830/1/Magliari_TESI_DOTTORATO_Il_single_supervisory_mechanism._Funzioni_e_modelli_di_integrazione_amministrativa.pdf

MCCAUL E., *The impact of suptech on European banking supervision*, at the Supervision Innovators Conference, 2022. [Online]. Disponibile su: https://www.bankingsupervision.europa.eu/press/interviews/date/2024/html/ssm.in240226~c6f7fc9251.en.html

MISURACA G., VAN NOORDT C., *AI Watch - Artificial Intelligence in public services: Overview of the use and impact of AI in public services in the EU*, EUR 30255 EN, (Ufficio delle pubblicazioni dell'Unione europea, 2020). [Online]. Disponibile su: AI watch, artificial intelligence in public services - Publications Office of the EU (europa.eu)

MOHSENI S., ZAREI N., RAGAN E. D., *Multidisciplinary Survey and Framework for Design and Evaluation of Explainable AI Systems*. ACM Trans. Interagire. Intel. Sist. 11, 3–4, Article 24, 2021. [Online]. Disponibile su: https://dl.acm.org/doi/abs/10.1145/3387166

NGUYEN T. T. *et al*, *A Survey of Machine Unlearning*, arXiv, 2022. [Online]. Disponibile su: https://arxiv.org/abs/2209.02299

PERFETTI L., *Il diritto ad una buona amministrazione, determinazione dell'interesse pubblico ed equità*, Riv. Ital. Dir. Pubbl. Comunitario-2010, 2010. [Online]. Disponibile su: https://scholar.google.com/scholar?hl=it&as_sdt=0%2C5&q=il+diritto+ad+una+buona+amministrazione&oq=

PIZZETTI F., *Intelligenza artificiale, protezione dei dati personali e regolazione*, collana diretta *da* Franco Pizzetti: I diritti nella "rete" della rete, Torino, 2018.

PROVENZANO P, *Procedimento amministrativo e diritto ad una buona amministrazione,* in D.U. Galetta (a cura di), *Diritto amministrativo nell'unione europea: argomenti e materiali*, Giappichelli, Torino, 2014 [Online]. Disponibile su: https://air.unimi.it/handle/2434/261152

RINGE W.G. *et al*., *Navigating the Legal Landscape of AI-Enhanced Banking Supervision: Protecting EU Fundamental Rights and Ensuring Good Administration,* European Banking Institute Working Paper Series 2023 - no. 140, 2023. [Online]. Disponibile su: https://ssrn.com/abstract=4430642

RUDIN C., *Stop Explaining black box machine learning models for high stakes decisions and use interpretable models instead*, 1 Nature Machine Intelligence, 2019, 206-215. [Online]. Disponibile su: https://arxiv.org/abs/1811.10154

SARTOR G., LAGIOA F., *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*, 2020. [Online]. Disponibile su: https://cris.unibo.it/handle/11585/763225#

TADDEI ELMI, G., MARCHIAFAVA, S. 2022, *Sviluppi recenti in tema di Intelligenza Artificiale e diritto: una rassegna di legislazione, giurisprudenza e dottrina*. Rivista italiana di informatica e diritto. 4, 2022. [Online]. Disponibile su: https://doi.org/10.32091/RIID0084

TESTOLIN A., ZORZI M., *L'approccio moderno all'intelligenza artificiale e la rivoluzione del deep learning*, in "Giornale italiano di psicologia, Rivista trimestrale" 2/2021, pp. 313-334, 2021. [Online]. Disponibile su: http://ccnl.psy.unipd.it/publications/l2019approccio-moderno-all2019intelligenza-artificiale-e-la-rivoluzione-del-deep-learning/view

TRÖGER T. H., *The Single Supervisory Mechanism – Panacea or Quack Banking Regulation?*, SAFE Working Paper Series, n. 27, 2014. [Online]. Disponibile su: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2311353

WRÓBEL I, *Artificial Intelligence Systems and the Right to Good Administration*, 49(2) Review of European and Comparative Law 203, 2022. [Online]. Disponibile su: https://repozytorium.kul.pl/server/api/core/bitstreams/3683b92d-7296-47cd-9df2-cb6a0443bfe1/content

WYMEERSCH E., *The Single Supervisory Mechanism or SSM, Part One of the Banking Union*, in "ECGI Working Paper Series in Law", n. 240, 2014. [Online]. Disponibile:

https://www.ecgi.global/sites/default/files/working_papers/documents/SSRN-id2397800.pdf

ZITO A., *Il «diritto ad una buona amministrazione» nella Carta dei diritti fondamentali dell'Unione europea e nell'ordinamento interno*, in Riv. Ital. Dir. Pubbl. Comunitario – 2002.

SITOGRAFIA

Come funziona l'AI Pact, il patto per anticipare le regole europee sull'intelligenza artificiale, in Wired, il 19 aprile 2024. [Online]. Disponibile su: https://www.wired.it/article/ai-pact-ai-act-europa-regole-aziende/

Cos'è il *Natural Language Processing* (NLP) e come funziona: https://blog.osservatori.net/it_it/natural-language-processing-nlp-come-funziona-lelaborazione-del-linguaggio-naturale

Cos'è un modello di Machine Learning o Apprendimento Automatico? [Online]. Disponibile su: https://www.intelligenzaartificialeitalia.net/post/cos-%C3%A8-un-modello-di-machine-learning-o-apprendimento-automatico

Definizione del Garante per la protezione dei dati personali rinvenibile al sito: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9512278

Definizione è rinvenibile sul sito del Parlamento europeo: https://www.europarl.europa.eu/topics/it/article/20230601STO93804/normativa-sull-ia-la-prima-regolamentazione-sull-intelligenza-artificiale#:~:text=I%20sistemi%20di%20intelligenza%20artificiale%20sono%20considerati%20a%20rischio%20inaccettabile,una%20minaccia%20per%20le%20persone.

Definizione rinvenibile su: https://www.ai4business.it/intelligenza-artificiale/connessioni-sintetiche/machine-unlearning-cose-e-come-corregge-errori-e-bias-dellai/

Definizione rinvenibile sul sito: https://bigcloud.global/the-difference-between-white-box-and-black-box-ai/

Definizione tratta dal sito *Microsft Azure*: https://azure.microsoft.com/it-it/resources/cloud-computing-dictionary/what-is-the-cloud/

Definizione tratta dal sito: https://aws.amazon.com/it/what-is/data-lake/

Definizione tratta dal vocabolario Treccani rinvenibile al sito: https://www.treccani.it/vocabolario/vantaggio/

Definizione tratta dall'articolo rinvenibile al sito: https://aws.amazon.com/it/what-is-cloud-computing/

Definizione tratta dall'articolo rinvenibile al sito: https://www.it-impresa.it/blog/dati-strutturati-e-non-strutturati/

Definizione tratta dall'articolo rinvenibile al sito: https://www.capterra.it/glossary/884/application-programming-interface#:~:text=Un'interfaccia%20di%20programmazione%20delle,programmi%20software%20comunicano%20tra%20loro.

Definizione tratta dall'articolo rinvenibile al sito: https://www.forumpa.it/pa-digitale/open-data-cosa-sono-come-sfruttarli-e-stato-dellarte-in-italia/

Definizione tratta dall'articolo rinvenibile al sito: https://www.tableau.com/it-it/learn/articles/data-visualization#:~:text=La%20visualizzazione%20dei%20dati%20%C3%A8,e%20ricorrenze%20presenti%20nei%20dati.

Definizione tratta dall'articolo: *What is AI-driven?* [Online]. Disponibile su: https://evolv.ai/glossary/ai-driven

Finalità indicate sul sito della BCE rinvenibile all'indirizzo: https://www.bankingsupervision.europa.eu/about/thessm/html/index.it.html#:~:text=Le%20principali%20finalit%C3%A0%20della%20vigilanza,assicurare%20una%20vigilanza%20coerente
Informazioni rinvenibili sul sito della BCE all'indirizzo: https://www.ecb.europa.eu/ecb/our-values/accountability/html/index.it.html

Informazioni rinvenibili sul sito della BCE nell'articolo: Cos'è lo SREP?: https://www.bankingsupervision.europa.eu/about/ssmexplained/html/srep.it.html

Informazioni rinvenibili sul sito della BCE nell'articolo: *From data to decisions: AI and supervision*: https://www.bankingsupervision.europa.eu/press/interviews/date/2024/html/ssm.in240226~c6f7fc9251.en.html

Informazioni rinvenibili sul sito della BCE nell'articolo: *Scaling up suptech*: https://www.bankingsupervision.europa.eu/press/publications/newsletter/2022/html/ssm.nl221117_4.en.html

Informazioni rinvenibili sul sito della BCE nell'articolo: *Suptech: thriving in the digital age*: https://www.bankingsupervision.europa.eu/press/publications/newsletter/2023/html/ssm.nl231115_2.en.html

Intelligenza Artificiale, significato e applicazioni dell'AI: https://blog.osservatori.net/it_it/intelligenza-artificiale-funzionamento-applicazioni

Qual è la differenza tra machine learning e deep learning? Rinvenibile al sito: https://aws.amazon.com/it/compare/the-difference-between-machine-learning-and-deep-learning/#:~:text=Il%20deep%20learning%20%C3%A8%20ideale,senso%20ai%20dati%20non%20strutturati.&text=Il%20machine%20learning%20risolve%20problemi,un'architettura%20di%20rete%20neural

Segnalazioni *whistleblowing*: https://whistleblowing.bankingsupervision.europa.eu/

Sezione delle politiche dell'unione sull'*AI Pact* rinvenibile al sito: https://digital-strategy.ec.europa.eu/it/policies/ai-pact

Una descrizione del portale IMAS è offerta dal sito della BCE: https://www.bankingsupervision.europa.eu/banking/portal/imas/html/index.it.html

NORMATIVA, GIURISPRUDENZA E ALTRO

Banca d'Italia, Relazione sulla gestione e sulle attività, 31 maggio 2014. [Online]. Disponibile: https://www.bancaditalia.it/pubblicazioni/relazione-gestione/2024/rel_gest_BI-2023.pdf

BCE, *Condizioni di impiego per il personale della Banca centrale europea*, Parte 1 Disposizioni generali. [Online]. Disponibile su: https://www.ecb.europa.eu/careers/pdf/conditions_of_employment.pdf

BCE, *Guida alla verifica dei requisiti di idoneità*, dicembre 2021. [Online]. Disponibile su: https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.fit_and_proper_guide_update202112~d66f230eca.it.pdf

BCE, *Parere della Banca centrale europea del 29 dicembre 2021 su una proposta di regolamento su una proposta di regolamento che stabilisce norme armonizzate in materia di intelligenza artificiale*, 29 dicembre 2021. [Online]. Disponibile su: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=OJ:C:2022:115:FULL&from=MT

Camera dei deputati, *Il regolamento UE in materia di intelligenza artificiale n. 26*, Documentazione per le Commissioni attività dell'Unione Europea, 5 febbraio 2024. [Online]. Disponibile su: https://documenti.camera.it/Leg19/Dossier/Pdf/AT026.Pdf

Codice europeo di buona condotta amministrativa, 6 settembre 2001.

Commissione europea, Comunicazione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, *Piano coordinato sull'intelligenza artificiale,* 7 dicembre 2018. [Online] Disponibile su: https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52018DC0795

Commissione europea, Comunicazione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, *Creare fiducia nell'intelligenza artificiale antropocentrica,* 8 aprile 2019. [Online] Disponibile su: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52019DC0168

Commissione europea, Comunicazione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, *L'intelligenza artificiale per l'Europa*, 25 aprile 2018. [Online] Disponibile su: https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52018DC0237

Commissione europea, Comunicazione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, *Promuovere un approccio europeo all'intelligenza artificiale*, 21 aprile 2021. [Online] Disponibile su: https://www.senato.it/web/docuorc2004.nsf/4d9255edaa0d94f8c12576ab0041cf0a/fd08ed88aeca1edac12586fc006a3991/$FILE/COM2021_0205_IT.pdf

Commissione europea, Comunicazione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, *Promuovere un approccio europeo all'intelligenza artificiale*.

Commissione europea, *Libro bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia*, 19 febbraio 2020. [Online] Disponibile su: https://op.europa.eu/it/publication-detail/-/publication/ac957f13-53c6-11ea-aece-01aa75ed71a1

Commissione europea, *Proposta di Direttiva del Parlamento europeo e del Consiglio sull'adeguamento delle norme sulla responsabilità civile extracontrattuale all'intelligenza artificiale (direttiva sulla responsabilità civile IA)*, 28 settembre 2022. [Online]. Disponibile su: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A0496%3AFIN

Commissione europea, *Proposta di Regolamento europeo del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'unione,* 21 aprile 2021. [Online] Disponibile su: https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX%3A12012E294

Commissione Europea, *Relazione alla Proposta di Regolamento sull'intelligenza artificiale*, 21 aprile 2021. [Online]. Disponibile su: https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52021PC0206

Conclusioni dell'Avv. gen. *Jacobs*, nelle sue conclusioni del 22 marzo 2001, in causa C-270/99, *Z.*

Conclusioni dell'Avv. gen. *Warner* del 30 aprile 1980, in causa 136/79, *National Panasonic*.

Cons. Stato, 13 dicembre 2019, n. 8472, massima redazionale, *Wolters Kluver*, 2019.

Consiglio dell'Unione europea, *Regolamento sull'intelligenza artificiale, orientamento generale del Consiglio*, 6 dicembre 2022. [Online]. Disponibile su: https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/it/pdf

Corte di giustizia 13 luglio 1966, cause riunite 56 e 58/64, *Consten & Grundig* contro Commissione.

Corte di Giustizia, 10 dicembre 1957, 1/57 e 14/57, *Société des usines à tubes de la Sarre* c. l'Alta Autorità della Comunità europea del Carbone e dell'Acciaio.

Corte di Giustizia, 10 luglio 2019, C-39/18 P, Commissione c. *NEX International Limited* e altri.

Corte di Giustizia, 11 dicembre 1973, in causa 120-73, *Lorenz*.

Corte di Giustizia, 12 luglio del 1957, cause riunite 7/56, da 3/57 a 7/57 *Algera*.

Corte di Giustizia, 13 giugno 1958, C-10/56, *impresa Meroni et co*., *industrie metallurgiche, società in accomandita semplice*, c. l'Alta Autorità.

Corte di Giustizia, 13 luglio 1966, cause riunite 56 e 58/64, *Consten & Grundig* c. Commissione.

Corte di giustizia, 15 marzo 1984, causa 64/82, *Tradax Graanhandel* BV.

Corte di Giustizia, 15 marzo 1984, causa 64/82, *Tradax Graanhandel BV*.

Corte di giustizia, 16 gennaio 2003, causa C-205/01, Paesi Bassi.

Corte di Giustizia, 16 gennaio 2019, in causa C-265/17 P, *United Parcel Service*.

Corte di Giustizia, 17 dicembre 2015, in causa C-419/14, *WebMindLicenses*.

Corte di Giustizia, 17 luglio 2014, in cause riun. C-141/12 e C-372/12, *Y.S.*

Corte di Giustizia, 17 novembre 1987, in cause riun. 142 e 156/84, *British American Tobacco Co. Ltd* c. Commissione.

Corte di Giustizia, 18 dicembre 2008, in causa C-349/07, *Sopropé*.

Corte di Giustizia, 20 marzo 1957, in causa 2/56, *Die in der " Geitling" Ruhrkohlen-Verkaufsgesellschaft mbH zusammengeschlossenen Bergwerksgesellschaften* c. Alta Autorità.

Corte di Giustizia, 20 marzo 1985, in causa 264/82, *Timex Corporation* c. Consiglio.

Corte di Giustizia, 22 novembre 2012, causa C-277/11 – *M*.

Corte di Giustizia, 23 ottobre 1974, causa 17/74, *Transocean Marine Paint Association*.

Corte di Giustizia, 26 giugno 1986, in causa 203/85, *Nicolet Instrument* c. *Hauptzollamt Frankfurt*.

Corte di Giustizia, 28 maggio 1980, C-33/79 e 75/79, *Ku¨hner c. Commissione*, punto 25.

Corte di Giustizia, 28 marzo 1997, in causa C-282/95P, *Guerin*, punto 37.

Corte di Giustizia, 3 luglio 2014, in causa C-129/13, *Kamino International Logistics*.

Corte di Giustizia, 31 marzo del 1992, causa C-255/90 P *Burban,* Racc. I-2253.

Corte di Giustizia, 4 luglio 1963, causa 32/63*, Alvis* e Corte di giustizia.

Corte di Giustizia, 4 luglio 2000, C-352/98, *Laboratoires Pharmaceutiques Bergaderm*.

Corte di Giustizia, 4 luglio del 1963, causa 32/62.

Corte di Giustizia, 5 marzo 1996, *Brasserie du Pêcheur SA* c. *Bundesrepublik Deutschland* e *The Queen* contro *Secretary of State for Transport, ex parte: Factortame Ltd* e altri.

Corte di Giustizia, 5 novembre 2014, in causa C-166/13, *Mukarubega*.

Corte di Giustizia, 8 maggio 2014, in causa C-604/12, *H.N.*

Corte di Giustizia, 8 maggio 2019, Caso C-450/17 P.

Corte di Giustizia, 9 settembre 2017, in causa C-298/16, *Ispas*.

Corte di giustizia, sentenza 13 settembre 2018, in causa C-358/16.

Corte di giustizia, sentenza 20 marzo 1959, in causa 18/57, I. *Nolde* c. Alta Autorità.

Corte di giustizia, sentenza 21 novembre 1991, in causa C-269/90.

Corte di Giustizia., 29 giugno 1994, in causa C-135/92, *Fiskano* c. Commissione.

Financial Stability Board, "*The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions - Market developments and financial stability implications*", 2020. [Online]. Disponibile su: The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions: Market developments and financial stability implications (fsb.org)

Future of Life Institute*, I Principi di Asilomar per l'IA*, gennaio 2017.

Garante per la protezione dei dati personali, *Segnalazione al Parlamento e al Governo sull'Autorità per l'IA*, 25 marzo 2024. [Online]. Disponibile su: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9996493

Legge n. 241 del 7 agosto del 1990, Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi.

Mediatore europeo, *Principi del servizio pubblico per i funzionari dell'Unione*, 2012.

Parlamento europeo, *Raccomandazione alla commissione concernenti il quadro relativo agli aspetti etici dell'intelligenza artificiale della robotica e delle tecnologie correlate,* 20 ottobre 2020. [Online] Disponibile su: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_IT.html

Parlamento europeo, *Raccomandazione alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale*, 20 ottobre 2020. [Online] Disponibile su: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_IT.html

Parlamento europeo, *Risoluzione del Parlamento europeo recante raccomandazioni alla Commissione concernenti il quadro relativo agli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate*, 20 ottobre 2020.

Regolamento (CE) n. 2026/97 del Consiglio del 6 ottobre 1997 relativo alla difesa contro le importazioni oggetto di sovvenzioni provenienti da paesi non membri della Comunità europea.

Regolamento (CEE) n. 4064/89 del Consiglio, del 21 dicembre 1989, relativo al controllo delle operazioni di concentrazione tra imprese.

Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati.

Regolamento (UE) n. 1024/2013 del Consiglio, del 15 ottobre 2013, che attribuisce alla Banca centrale europea compiti specifici in merito alle politiche in materia di vigilanza prudenziale degli enti creditizi

Regolamento n. 17, del 21 febbraio 1962, Primo regolamento d'applicazione degli articoli 85 e 86 del Trattato.

Tribunale UE, 10 marzo 1992, T-9/89, *Hu¨els AG* c. Commissione.

Tribunale UE, 15 luglio 2015, in cause riun. T-413/10 e T-414/10, *Socitrel*.

Tribunale UE, 16 maggio 2017, Caso T-122/15, *Landeskreditbank- Württemberg-Förderbank* c. Banca centrale europea confermata in appello con sentenza della Corte di Giustizia, 8 maggio 2019, Caso C-450/17 P.

Tribunale UE, 17 dicembre 1991, causa T-7/89, *SA Hercules Chemicals NV* c. Commissione delle Comunità europee.

Tribunale UE, 18 dicembre 1992, in cause riun. 10, 11, 12 e 15/92, *Cimenteries CBR SA* c. Commissione.

Tribunale UE, 19 marzo 1997, in causa T-73/95.

Tribunale UE, 22 ottobre 1997, in cause riun. T-213/95 e T-18/96, *SCK* e *FNK*.

Tribunale UE, 22 ottobre 1997, in cause riun. T-213/95 e T-18/96, *V*.

Tribunale UE, 25 marzo 1999, causa T-37/97, *Forges de Clabecq*.

Tribunale UE, 29 giugno 1995, in causa T-30/91, *Solvay SA* c. Commissione.

Tribunale UE, 7 ottobre 1999, in causa T-228/97, *Irish Sugar*.

Tribunale UE, 9 luglio 1999, in causa T-231/97, *New Europe Consulting e a.* c. Commissione.

Tribunale UE, sentenza 12 settembre 2006, T-155/04, *Selex Sistemi integrati* c. Commissione.

Tribunale UE, sentenza 14 luglio 1997, in causa T-81/95, *Interhotel*.

Tribunale UE, sentenza 19 marzo 1997, in causa T-73/95, *Oliveira* c. Commissione.

Tribunale UE, sentenza 7 novembre 2002, T-141/99, T-142/99, T-150/99 e T-151/99, *Vela s.r.l.* c. Commissione.

Tribunale UE, sentenza 9 luglio 2008, T-301/01, *Alitalia* e altri c. Commissione.

Università di *Montréal*, *La dichiarazione di Montréal per l'IA responsabile*, novembre 2017.