LavoroDirittiEuropa
Rivista nuova di Diritto del Lavoro

Numero 4 / 2024

Licia GAROTTI

Giulia DI BIASE

Intelligenza artificiale, trasparenza e tutela dei dati aziendali

Intelligenza artificiale, trasparenza e tutela dei dati aziendali

Licia GAROTTI

Avvocato, Partner responsabile Dipartimento di Proprietà Intellettuale e Diritto delle Tecnologie dello Studio PedersoliGattai, Milano

Giulia DI BIASE

Associate, Dipartimento di Proprietà Intellettuale e Diritto delle Tecnologie dello Studio PedersoliGattai, Milano

1. L'utilizzo dei sistemi di intelligenza artificiale nell'ecosistema aziendale contemporaneo

L'impiego di sistemi di intelligenza artificiale nei processi produttivi o decisionali trova una diffusione sempre maggiore e, con essa, la necessità di tutela di tali tecnologie sotto il profilo della proprietà intellettuale. Se lo strumento di tutela preferita (o, per meglio dire, preferibile) sembra restare quella del segreto commerciale, occorre valutare il rapporto di questa forma di tutela con gli obblighi di trasparenza posti a presidio dei fondamentali diritti della persona e della collettività. Il presente contributo intende fornire un'analisi del rapporto tra diritto alla segretezza sulle tecnologie di intelligenza artificiale utilizzate nell'ambito dell'attività di impresa e le esigenze di trasparenza e intelligibilità delle stesse.

È ormai pacifico che i sistemi di intelligenza artificiale, nelle diverse e possibili declinazioni e peculiarità, costituiscono una componente spesso essenziale dell'ecosistema aziendale contemporaneo. L'impiego di queste tecnologie in ambito imprenditoriale e industriale viene considerato fondamentale per accelerare o mantenere un buon vantaggio competitivo, con un particolare riguardo alla concorrenza, ma anche più semplicemente per aumentare l'efficienza operativa di un'impresa. L'utilizzo dei sistemi di intelligenza artificiale è, infatti, trasversale: dall'implementazione di sistemi automatizzati per migliorare e velocizzare le interazioni con i clienti, anche nei servizi di assistenza, all'elaborazione di dati di diverso tipo per facilitare le attività di analisi, all'utilizzo in campo diagnostico, di ricerca, all'automatizzazione di processi nell'ambito delle attività della pubblica amministrazione, alla robotica integrata con componenti di intelligenza artificiale nei settori manifatturieri. Le istituzioni finanziarie non sono rimaste indietro. Vi è chi ha integrato il proprio *business* con sistemi di intelligenza artificiale per numerose finalità: monitoraggio e analisi dei rischi, rilevamento delle frodi e, ancora, elaborazione e analisi di dati che consentano di prendere decisioni in maniera più rapida[1].

2. La tutela dei sistemi di intelligenza artificiale come segreti commerciali

Lo sviluppo di nuove tecnologie necessita di strumenti di tutela sotto il profilo, tra l'altro, della proprietà intellettuale. E ciò vale, a maggior ragione, in ambito societario: indipendentemente dal

[1] Sul punto si veda la recente decisione della CGUE, C-634/21, EU:C:2023:957, 7 dicembre 2023. In particolare, la decisione ha preso posizione sul concetto di "*processo decisionale automatizzato*", con espresso riferimento al calcolo automatizzato delle capacità probabilistiche di una persona fisica di onorare futuri impegni di pagamento, con tutte le implicazioni che ne conseguono sotto il diverso profilo del trattamento dei dati ai sensi del GDPR.

settore di riferimento, l'insieme di *asset* immateriali di un'impresa, spesso costituiti in prevalenza dal *know-how*, rappresenta un elemento di estrema importanza a fini di efficienza e competitività.

L'implementazione di tecnologie che includono sistemi di intelligenza artificiale può essere parte del *know-how* riservato dell'impresa e costituire – autonomamente o nel complesso del patrimonio informativo aziendale – un *asset* tutelabile come segreto commerciale. Le strategie, le metodologie utilizzate nella produzione o, in generale, nel *business* aziendale sono frutto di investimenti più o meno consistenti, che possono includere attività di ricerca e sviluppo di algoritmi o sistemi di intelligenza artificiale o, in alternativa, il loro acquisto presso terzi fornitori di tecnologia. La certezza di una tutela legale delle informazioni, delle strategie e di ciò che può costituire *know-how* qualificato di un'impresa cui si giunge all'esito di un'attività di ricerca e sviluppo incentiva chi compie tali attività a sostenere gli investimenti necessari per giungervi[2].

Invero, la scelta dello strumento di tutela più adeguato assume caratteristiche di soggettività e tiene normalmente conto di diversi fattori. La tutela delle tecnologie può senz'altro passare attraverso il diritto d'autore o, in determinati casi, attraverso la tutela brevettuale. Quali sono le ragioni per preferire una soluzione all'altra? Se ne possono rilevare alcune: *in primis*, le caratteristiche del bene oggetto di tutela. Le tecnologie di intelligenza artificiale sono in continua evoluzione e sono sottoposte a processi di aggiornamento e perfezionamento pressoché continui. Una privativa di durata ventennale, qual è quella del brevetto, potrebbe non rivelarsi perfettamente idonea allo scopo di tutela richiesto. Il tema dei costi non è irrilevante: la tutela del segreto commerciale trova il suo investimento economico maggiore nel mantenimento di misure di sicurezza adeguate a proteggere la confidenzialità delle informazioni, non richiedendo tuttavia alcuna particolare spesa iniziale per la costituzione del diritto. In definitiva, le scelte in ordine agli strumenti di tutela dipendono strettamente dalla tipologia dell'*asset* che si intende proteggere e prescindono da valutazioni di carattere assoluto, fermo restando che non tutte le tecnologie sono brevettabili di per sé (tanto il Codice di Proprietà Industriale quanto la Convenzione sul brevetto europeo escludono la brevettabilità del software "*in quanto tale*")[3].

Parimenti, la tutela del segreto commerciale non può estendersi a qualsiasi tipo di informazione. Al contrario, la legge subordina l'accesso alla tutela al soddisfacimento di specifici requisiti. La Direttiva (UE) 2016/943 sulla *Protezione del know-how riservato e delle informazioni commerciali riservate (segreti commerciali) contro l'acquisizione, l'utilizzo e la divulgazione illeciti* ("Direttiva Trade Secrets") prevede, all'art. 2 par. 1, che le informazioni suscettibili di tutela siano segrete (non generalmente note o facilmente accessibili), abbiano valore economico in quanto segrete e, da ultimo, siano

[2] Sui vantaggi del ricorso alla tutela del segreto commerciale, si vedano, tra gli altri, MAGNANI, *La tutela concorrenziale del segreto nella ricerca di un equilibrio tra interessi privati e collettivi: fondamenti giuridici ed economici della protezione alla luce della direttiva 2016/943*, in AA.VV., Studi per Luigi Carlo Ubertazzi, Giuffrè, Milano, 2019, 463 – 482; LEMLEY, *The Surprising Virtues of treating Trade Secrets as IP Rights*, in Stanford Law Review, Vol. 61, N. 2, 2008, pp. 311 – 353.

[3] Ai sensi dell'art. 45, comma 2, lett. b del Codice di proprietà industriale, i "*programmi per elaboratore*" non sono considerati di per sé "*invenzioni*" ai fini della brevettabilità. Il comma 3 della medesima disposizione specifica che "*le disposizioni del comma 2 escludono la brevettabilità di ciò che in esse è nominato solo nella misura in cui la domanda di brevetto o il brevetto concerne scoperte, teorie, piani, principi, metodi, programmi e presentazioni di informazioni considerati in quanto tali*." La non brevettabilità del software "*in quanto tale*" è stabilita anche dalla European Patent Convention (EPC) all'art. 52, par. 2, lett. c e par. 3. Per una illustrazione esaustiva della brevettabilità delle cc.dd. *Computer Implemented Inventions*, si veda EPO, *Guidelines for examination in the European Patent Office*, Marzo 2024, disponibile all'indirizzo *https://www.epo.org/en/legal/guidelines-epc/2024/index.html.*

sottoposte a misure ragionevolmente idonee a mantenerle segrete. Tali requisiti sono poi stati trasposti nel Codice di proprietà industriale ("c.p.i.") all'art. 98[4].

Per connettere il dato normativo all'esperienza, ponendosi dalla prospettiva di un'impresa che utilizza nella propria attività sistemi di intelligenza artificiale integrati in una rete più ampia di tecniche e metodologie di produzione o di gestione, è semplice comprendere il motivo per cui la tutela del segreto commerciale, pur integrata con altre tipologie di tutela, possa spesso essere preferibile. Si tratta di beni (sostanzialmente dati e metodologie) naturalmente idonee a evolvere rapidamente, per i quali vengono sostenuti investimenti consistenti e che richiedono una tutela piuttosto immediata rispetto al loro sviluppo. A tale fine, la segretezza è in grado di garantire una protezione illimitata nel tempo (finché si è in grado di predisporre misure di sicurezza idonee) anche rispetto ad eventuali modifiche o aggiornamenti e, soprattutto, immediata rispetto all'integrazione di tali tecnologie nell'attività d'impresa, senza oneri di costituzione del diritto e senza costi iniziali (al netto di quelli relativi alla predisposizione delle misure di protezione). Ai sensi dell'art. 3 della Direttiva Trade Secrets e dell'art. 99 del c.p.i., il divieto di sottrazione di segreti commerciali soffre tuttavia alcune eccezioni, come la scoperta indipendente o, in taluni casi, il *reverse engineering*. Ciò non pare problematico rispetto alla protezione di sistemi di intelligenza artificiale, la cui estrema complessità (in termini di programmazione, selezione dei dati per l'addestramento e per la validazione, anche considerando l'unicità dell'apporto umano allo sviluppo del sistema) rende abbastanza improbabile tanto l'ipotesi di scoperta indipendente quanto quella del *reverse engineering*[5].

I sistemi di intelligenza artificiale sembrano soddisfare i requisiti di tutela imposti dalle norme nazionali e comunitarie, le quali consentono la protezione in regime di segreto di algoritmi non banali e codici sorgente. Ciò, naturalmente, sotto una prospettiva generale, senza tener conto delle specificità e delle modalità di utilizzo dei singoli sistemi soprattutto rispetto alle misure di segretezza, la cui analisi risulta in questa sede particolarmente complessa.

3. Tutela della riservatezza delle informazioni commerciali e obblighi di trasparenza dei sistemi di intelligenza artificiale: esigenza di bilanciamento

La tutela degli *asset* tecnologici, inclusi sistemi di intelligenza artificiale, passa spesso attraverso la riservatezza e come visto, per poter accedere a questo tipo di tutela, va garantita l'effettiva segretezza dell'informazione.

Occorre però dare atto di un aspetto fondamentale: quando il bene tutelato include sistemi di intelligenza artificiale, è necessario garantire la riservatezza di processi e decisioni che sottostanno ad un *output* artificialmente generato. Questo dato è fonte di non poche perplessità, rispetto alle quali spesso non rappresenta adeguata rassicurazione l'esistenza di un controllo umano sulle decisioni della macchina. A ben vedere, infatti, l'apporto umano in tali processi non ne esclude l'essenza "artificiale". Anche l'Artificial Intelligence Act di recente emanazione ("AI Act" o

[4] Il recepimento della Direttiva Trade Secrets nell'ordinamento italiano è avvenuto mediante l'emanazione del d.lgs 11 maggio 2018, n. 63. Per una illustrazione delle novità che la Direttiva Trade Secrets ha introdotto nel sistema di tutela dei segreti commerciali già previsto dal Codice di Proprietà Industriale, si veda, tra gli altri, OTTOLIA, *Il d.lgs. n. 63/18 di attuazione della Dir. 2016/943/UE sulla Protezione dei Segreti Commerciali fra tutela e bilanciamenti*, in *Le Nuove Leggi Civili Commentate*, n. 5, 1 settembre 2019, pp. 1091 – 1133.

[5] In questo senso, VOGT, *Show Me Your Secrets: How the Use of Trade Secrets Relates to the Demand for Transparent Artificial Intelligence* – Part II, in *Robotics, Artificial Intelligence & Law*, Settembre – Ottobre 2022, Vol. 5, N. 5, pp. 305–337.

"Regolamento", approvato il 21 maggio 2024 dal Consiglio dell'UE, ma – al momento in cui si scrive – non ancora pubblicato in Gazzetta Ufficiale), infatti, prevede specifiche regole sulla necessità di supervisione umana nel funzionamento dei sistemi di intelligenza artificiale, la quale viene comunque inquadrata nel complesso dell'attività del sistema e per questo non toglie autonomia decisionale allo stesso.

Se, da un lato, per accedere alla tutela del segreto commerciale è richiesto un livello adeguato di segretezza e di non facile accessibilità dell'insieme di dati che si intende proteggere, dall'altro lato si fa spazio un'esigenza di intelligibilità dell'*output*, dei processi decisionali che conducono al risultato, nonché del punto di origine dell'intero processo (i dati di addestramento).

L'esigenza di trasparenza rispetto alle decisioni algoritmiche deriva, ancor prima che da un dichiarato intento normativo di cui si dirà fra poco, da un sentimento fortemente umano di timore e diffidenza rispetto a tutto ciò che appare incontrollabile. Una prospettiva assolutamente comprensibile, soprattutto se si pensa che decisioni di tale specie possono influire su un elenco pressoché illimitato di interessi e diritti: da una prospettiva imprenditoriale, sulle decisioni e sull'andamento dell'impresa, quindi sulla concorrenza; da una prospettiva più ampia, invece, sugli interessi dei consumatori, dei cittadini, dell'ambiente e, di conseguenza, sui diritti fondamentali. Proprio con riferimento a interessi di tale rilevanza, l'intelligibilità di un sistema di intelligenza artificiale e del processo che conduce a un determinato *output* rimane preziosa anche al fine di individuarne possibili *bias*, che potrebbero condurre a risultati discriminatori o contrari al rispetto dei predetti diritti fondamentali.

Questa esigenza di chiarezza e di intelligibilità delle decisioni "artificiali" è stata fatta propria dal legislatore europeo e riflessa nell'intera architettura normativa dell'AI Act attraverso il concetto di affidabilità dell'intelligenza artificiale, la c.d. *Trustworthy AI*[6].

Invero, già prima dell'approvazione del Regolamento, la Trustworthy AI ha trovato la sua estrinsecazione in un insieme di principi che vengono in esso espressamente richiamati. Ci si riferisce, in particolare, agli *Orientamenti etici per un'intelligenza artificiale affidabile* («*Ethics Guidelines for Trustworthy AI*»), redatti dal Gruppo Indipendente di esperti ad Alto Livello sull'intelligenza artificiale («*High-Level Expert Group on AI (HLEG)*»), istituito dalla Commissione Europea nel giugno del 2018[7]. Tale documento prevede un'architettura di principi tra cui il rispetto dell'autonomia umana (intervento e sorveglianza), prevenzione dei danni (robustezza tecnica e sicurezza dei sistemi, non discriminazione), trasparenza e spiegabilità. Gli ultimi due principi, tra loro strettamente connessi, hanno la finalità di creare e mantenere un alto livello di fiducia nei sistemi di intelligenza artificiale da parte degli utenti, muovendo dall'assunto per cui la comunicazione dei processi e delle finalità dei sistemi è fondamentale per poter contestare eventuali decisioni o *output*.

[6] Per un'illustrazione del concetto di Trustworthy AI in relazione alle esigenze di tutela dei segreti commerciali, si veda VOGT, *Show Me Your Secrets: How the Use of Trade Secrets Relates to the Demand for Transparent Artificial Intelligence* – Part I, in *Robotics, Artificial Intelligence & Law,* Luglio – Agosto 2022, Vol. 5, N. 4, pp. 223–241.

[7] *Ethics guidelines for trustworthy AI,* High-Level Expert Group on AI, 8 aprile 2019, disponibili all'indirizzo *https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.*

Allo stesso modo, tra i Principi OCSE «*Recommendation of the Council on Artificial Intelligence*» adottati nel maggio 2019 e oggetto di revisione nel maggio 2024[8], assumono un ruolo preminente i principi di trasparenza e accuratezza dei sistemi di intelligenza artificiale, volti a garantire la comunicazione in modo semplice e comprensibile delle fonti di dati e dei processi che conducono a un determinato risultato. Tuttavia, occorre precisare (e tale aspetto viene preso in considerazione anche negli Orientamenti etici) che la spiegabilità non è sempre perseguibile ove vi siano risultati o decisioni particolarmente complesse (è il caso dei sistemi c.d. "*black-box*", per i quali sono richiesti livelli di trasparenza specifici a seconda della gravità di possibili conseguenze dannose).

Il concetto di Trustworthy AI trova ampio riscontro anche nelle norme dell'AI Act, tra cui l'art. 1 sulle finalità del Regolamento, l'art. 13 sulla trasparenza e la fornitura di informazioni ai *deployer*, ma soprattutto l'art. 50, che introduce il Capo IV rubricato "*Obblighi di trasparenza per i fornitori e i deployer di determinati sistemi di IA*".

Trasparenza e spiegabilità del funzionamento dei sistemi di intelligenza artificiale sono alla base di una IA affidabile. Al tempo stesso, tutelare gli *asset* immateriali delle imprese, incluso il *know-how* qualificato e riservato relativo alle tecniche e metodologie di IA utilizzate nell'ambito del proprio *business* assume il ruolo vitale di incentivo alla concorrenza e all'innovazione.

Sulla base di queste premesse, è evidente che l'apparente contrasto tra il diritto alla segretezza delle informazioni e il rispetto degli obblighi di trasparenza nello sviluppo e nell'utilizzo di sistemi di intelligenza artificiale riguarda interessi entrambi meritevoli di eguale tutela e non può vedere una soccombenza assoluta dell'uno rispetto all'altro, ma necessita piuttosto di un adeguato bilanciamento.

Proviamo a fornire alcuni spunti interpretativi delle norme e alcune considerazioni di carattere pratico per ipotizzare un punto di incontro tra i diversi interessi che l'ordinamento intende tutelare.

Una prima considerazione riguarda l'essenza del contrasto tra diritto alla segretezza e obblighi di trasparenza. Invero, il contrasto non riguarda tanto gli interessi fondamentali sottostanti, quanto le modalità di perseguimento degli stessi. La finalità ultima della tutela del segreto commerciale non è, infatti, quella di creare un monopolio sull'informazione fine a sé stesso, ma, al contrario, quella di consentire il recupero degli investimenti effettuati per giungere (nel caso in esame) allo sviluppo di una determinata tecnologia, creando un vantaggio competitivo a favore di colui che ha sostenuto tali investimenti. La disponibilità dell'informazione unicamente in capo al singolo rappresenta la modalità di perseguimento di questo obiettivo. Allo stesso modo, la finalità ultima dell'obbligo di trasparenza in materia di sviluppo delle tecnologie di IA consiste nel prevenire ed escludere nel modo più accurato e tempestivo possibile, potenziali errori di valutazione che potrebbero condurre a risultati iniqui e/o discriminatori. Ciò non sembra porsi in contrasto con la tutela della concorrenza e dell'innovazione. Dunque, la soluzione andrebbe individuata in misure che consentano di tutelare entrambi gli interessi fondamentali sottostanti.

[8] OECD, *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449, 2024, disponibile all'indirizzo: *https://legalinstruments.oecd.org/fr/instruments/oecd-legal-0449*.

Quest'ultimo punto offre una chiave di lettura ulteriore rispetto al contrasto tra segretezza e trasparenza delle informazioni: non è sempre logico creare una barriera assoluta alla comunicazione di informazioni sul funzionamento dei sistemi di intelligenza artificiale, ma non è altrettanto realistico immaginare una spiegabilità totale e immediatamente possibile con riferimento a tecnologie per loro stessa natura estremamente complesse[9].

L'AI Act sembra in realtà tenere conto della necessità di trovare un bilanciamento tra il diritto alla segretezza e l'esigenza di spiegabilità dei sistemi di intelligenza artificiale. Ciò si riflette già nei Considerando, ove si legge che "*Al fine di aumentare la trasparenza sui dati utilizzati nelle fasi di pre-addestramento e addestramento dei modelli di IA per finalità generali, compresi testo e dati protetti dalla normativa sul diritto d'autore, è opportuno che i fornitori di tali modelli elaborino e mettano a disposizione del pubblico una sintesi sufficientemente dettagliata dei contenuti utilizzati per l'addestramento del modello per finalità generali. Pur tenendo debitamente conto della necessità di proteggere i segreti commerciali e le informazioni commerciali riservate, la presente sintesi dovrebbe essere di respiro ampio e generale, anziché dettagliata sotto il profilo tecnico…*"

Non solo: il legislatore comunitario, nell'imporre obblighi di trasparenza, ad esempio con riferimento ai modelli di intelligenza artificiale per finalità generali (c.d. *general purpose AI*), introduce una clausola di salvaguardia dei diritti di proprietà intellettuale e delle informazioni commerciali riservate, in conformità con il diritto dell'Unione e degli Stati membri. In particolare, l'art. 78 ("*Riservatezza*") impone alla Commissione, alle autorità e a tutti coloro che siano tenuti all'osservanza del Regolamento il rispetto dei diritti di proprietà intellettuale e delle informazioni commerciali riservate o dei i segreti commerciali di una persona fisica o giuridica, inclusi i codici sorgente (con l'eccezione di quanto previsto all'art. 5 della Direttiva Trade Secrets, che disciplina alcune eccezioni alla tutela del segreto commerciale quando la sua divulgazione sia richiesta da esigenze di tutela di legittimi interessi riconosciuti dal diritto comunitario o nazionale).

Se il dato normativo sembra chiaro rispetto alla necessità di contemperare gli obblighi di trasparenza con la tutela delle informazioni commerciali riservate, non è semplice immaginare come ciò possa essere garantito sotto il profilo applicativo. Ciò soprattutto quando non sia possibile ricondurre l'esigenza di *disclosure* ad un "legittimo interesse" connotato da un carattere pubblicistico.

Per maggiore completezza, è bene ricordare che l'esigenza di tutela dei diritti fondamentali trova riscontro anche in previsioni che non riguardano obblighi divulgativi. Si pensi, ad esempio, al divieto di utilizzo di sistemi che vengono definiti "a rischio inaccettabile" o, anche, alla previsione di norme specifiche per i sistemi ad alto rischio in tema di valutazione dell'impatto sui diritti fondamentali o in tema di corretto utilizzo dei dati per l'individuazione e correzione di eventuali *bias*. Si tratta di norme che, anche senza prevedere obblighi di divulgazione di informazioni, rappresentano presidi per la prevenzione di errori e malfunzionamenti che potrebbero incidere in modo dannoso sui destinatari e sui loro diritti (in particolare, ci si riferisce agli artt. 10, 14 e 27 del Regolamento).

4. Conclusioni

[9] Sulla difficoltà in termini concreti di ottenere un sufficiente livello di trasparenza anche con riferimento alla tutela dei dati, si veda PELLECCHIA, *Profilazione e Decisioni Automatizzate al tempo della Black Box Society: Qualità dei dati e leggibilità dell'algoritmo nella cornice della responsible Research and Innovation*, in *Le Nuove Leggi Civili Commentate*, n. 5, 1 settembre 2018, pp. 1209 – 1935.

Alla luce degli spunti interpretativi finora illustrati, sembra opportuno propendere per un approccio flessibile sulla base delle specificità del caso, individuando volta per volta, a seconda delle circostanze concrete, gli interessi cui attribuire necessariamente maggior peso. Tale valutazione dovrà tener conto dei diritti su cui un sistema produce effetti, nonché sull'entità degli effetti medesimi. Occorrerà far prevalere le esigenze di trasparenza qualora la "decisione" del sistema di IA possa dirsi discriminatoria e/o lesiva dei diritti del destinatario della stessa, prevedendo un obbligo di *disclosure* che sia anche solo limitato alle autorità competenti. Al contrario, un maggior peso potrà essere dato alle esigenze di riservatezza qualora l'impatto della decisione "artificiale" sui diritti dei destinatari non sia diretto né gravoso e, in generale, non leda un particolare interesse pubblico[10]. Tale valutazione dipende fortemente da una serie di elementi, incluso il settore di riferimento, la tipologia e il livello di rischio, le modalità di impiego del sistema di intelligenza artificiale e la "prossimità" della decisione ai diritti dei destinatari.

[10] Una simile valutazione viene effettuata anche nell'ambito del diritto amministrativo rispetto al contrasto tra istanze di accesso e tutela della riservatezza di informazioni protette come segreti commerciali. A questo proposito, si veda la recente ordinanza del Consiglio di Stato, Sez. V, 29 gennaio 2024, in *Sprint*, che richiama Consiglio di Stato, Sez. V, 18 settembre 2023, n. 8382, secondo cui "*in occasione della disamina delle ragioni che giustificano una domanda di accesso, quelle legate alle esigenze di difesa del richiedente non prevalgono sempre e comunque su qualunque altro interesse, specie se contrapposto, giacché invocato da chi, al contrario, deduce che, consentendosi l'accesso, si permetterebbe il disvelamento di dati tecnici contenuti nella documentazione richiesta che rappresentano 'Know how' dell'impresa controinteressata*."