

PROVVEDIMENTO AMMINISTRATIVO: Consiglio di Stato, Sezione Quarta, Sentenza 4 giugno 2025, n. 4857.

1. Atto amministrativo – Utilizzo dell’algoritmo – Decisione amministrativa algoritmica – Algoritmo di mero supporto – Distinzione.

2. Atto amministrativo – Utilizzo dell’algoritmo –Disciplina ex art. 30, comma 2, lett. a), del d.lgs. 31 marzo 2023, n. 36 -Applicabilità alla sola decisione amministrativa algoritmica – Inapplicabilità all’algoritmo di mero supporto.

3. Atto amministrativo – Accesso ai documenti – Contratti pubblici e obbligazioni della pubblica amministrazione – Codice dei contratti pubblici – Novella ex art. 35, del d.lgs. 31 marzo 2023, n. 36 – Accesso difensivo –Indispensabilità e strumentalità alla difesa in giudizio - Necessità.

4. Atto amministrativo – Utilizzo dell’algoritmo – Decisione amministrativa algoritmica — Motivazione – Indicazione codice sorgente – Necessità.

5. Atto amministrativo – Utilizzo dell’algoritmo – Decisione amministrativa algoritmica – Codice Sorgente – Accesso - Ammissibilità.

1. Occorre distinguere tra decisione amministrativa algoritmica e algoritmo di mero supporto alle decisioni che restano rigorosamente affidate al fattore umano e che, dunque, si inscrivono nella più tradizionale impostazione, che vede nell’informatica un mero ausilio rispetto allo svolgimento dell’attività amministrativa nelle sue classiche modalità operative.

2. Le decisioni che si avvalgono di un algoritmo di mero supporto – che restano rigorosamente ancorate al fattore umano – non sono disciplinate dall’art. 30, comma 2, lett. a), del d.lgs. 31 marzo 2023, n. 36 il quale, di contro regola solamente i principi che devono governare l’adozione dei “provvedimenti per algoritmi” (principio di trasparenza, principio di non esclusività della decisione algoritmica, principio di non discriminazione).

3. L’art. 35, del d.lgs. 31 marzo 2023, n. 36 ha ulteriormente circoscritto l’oggetto della situazione legittimante l’accesso difensivo rispetto all’accesso “ordinario”, esigendo che la stessa, oltre a corrispondere al contenuto dell’astratto paradigma legale, sia anche collegata al documento al quale è chiesto l’accesso (art. 24, comma 7, della l. n. 241 del 1990), in modo tale da evidenziare in maniera diretta ed inequivoca il nesso di strumentalità che avvinca la situazione soggettiva finale al documento di cui viene richiesta l’ostensione, e per l’ottenimento del quale l’accesso difensivo, in quanto situazione strumentale, fa da tramite. (3).

In motivazione, la sezione ha evidenziato come dal tenore letterale dell’art. 35, del d.lgs. 31 marzo 2023, n. 36, emerga che il diritto di accesso al codice sorgente di una piattaforma di *e-procurement* adoperata per la conduzione delle operazioni di gara debba prevalere sul diritto alla riservatezza aziendale solo quando sia indispensabile e strettamente strumentale alla difesa in giudizio del richiedente, nell’ambito della procedura di affidamento del contratto. La nozione di “indispensabilità” deve essere declinata nel senso di insussistenza di altri mezzi di prova idonei a dimostrare i fatti oggetto di contesa tra le parti. Ciò anche alla luce del principio, di valenza anche eurounitaria, di proporzionalità, che impone di adottare la soluzione che comporta il sacrificio minore per il diritto fondamentale che si intende comprimere, senza che quest’ultimo risulti vanificato del tutto.

4. L’art. 30 del d.lgs. 31 marzo 2023, n. 36 esprime una chiara preferenza per gli algoritmi open source rispetto a quelli proprietari e, in ogni caso, assicura la disponibilità del codice sorgente, prevedendo inoltre che, nei casi di decisione algoritmica, la motivazione del provvedimento finale deve richiamare il codice sorgente e il modello matematico impiegati. (4).

5. *L'art. 30 del d.lgs. 31 marzo 2023, n. 36 mostra un evidente favor per l'esercizio dell'accesso difensivo rispetto alla tutela della proprietà intellettuale, ancorché coperta da brevetto, e, di conseguenza, consente, per la decisione algoritmica, di accedere al data set, ritenendo che la mancata conoscenza del codice sorgente impedisce la tracciabilità dell'algoritmo, violando il dovere esplicativo minimo previsto dalle raccomandazioni europee. (5).*

Visti il ricorso in appello e i relativi allegati;

Visti gli atti di costituzione in giudizio di Srtspa e di Digitalpa s.r.l.;

Visti tutti gli atti della causa;

Relatore nell'udienza pubblica del giorno 10 aprile 2025 il Cons. Luigi Furno e uditi per le parti gli avvocati presenti come da verbale;

FATTO

La Srt s.p.a. (società pubblica per il recupero e il trattamento dei rifiuti) ha indetto una procedura aperta in modalità telematica per l'affidamento dell'appalto del servizio di lavorazione rifiuti presso le piattaforme di valorizzazione.

In particolare, l'art. 13.1. del disciplinare di gara ha previsto che *“I documenti dell'offerta economica e tecnica dovranno essere marcati mediante generazione dell'impronta digitale entro e non oltre il termine indicato al punto 19 del bando di gara, pena la non ammissione alla procedura, ed inoltrati alla S.A., a pena di esclusione, entro la finestra temporale che verrà comunicata contestualmente alla comunicazione della conferma di partecipazione (in ogni caso successivamente alla data di cui al punto 19 del bando di gara). I documenti di offerta economica devono essere firmati digitalmente. La S.A. verificherà, a pena di esclusione, la corrispondenza dell'impronta digitale dei documenti di offerta trasmessi con quella assegnata dal sistema in fase di conferma di partecipazione. Dopo aver allegato la documentazione richiesta, sarà necessario confermare la propria partecipazione tramite l'apposito tasto, inderogabilmente prima del termine di scadenza, a questo punto il sistema invierà una ricevuta di partecipazione via PEC, contenente l'elenco dei documenti caricati e le informazioni relative. La PEC inviata costituisce notifica del corretto recepimento dell'offerta stessa”*.

L'art. 19 del bando di gara ha previsto, quale termine di presentazione delle offerte, *“...il giorno 12/07/2024 alle ore 12,00”*.

Alla procedura di gara ha partecipato anche Teknoservice s.r.l., la quale, in data 12 luglio 2024 (ore 14:54), ha effettuato una segnalazione al gestore della piattaforma con la seguente comunicazione: *“Buongiorno, durante la fase di caricamento dei file marcati temporalmente per la generazione dell'impronta, uno dei file è stato sostituito e ri-caricato in piattaforma. Nel momento del caricamento dei file dopo l'apertura della finestra di caricamento, lo stesso file sostituito precedentemente riporta*

a sistema la dicitura "Verifica impronta: Impronta del file non corrispondente" -quando il file è lo stesso-...".

In riscontro a tale comunicazione e ad una successiva richiesta di approfondimento, il gestore della piattaforma ha riferito alla Teknoservice s.r.l. che il file in questione non risultava corrispondere all'impronta calcolata nella prima fase in quanto avente un codice *hash* diverso da quello indicato nella conferma di partecipazione della predetta fase e che tale diversità sarebbe stata determinata da una modifica del file.

Con verbale n. 2, del 23 luglio 2024 il seggio di gara ha escluso la Teknoservice s.r.l. con la seguente motivazione: *"Mancato rispetto delle Regole per la presentazione dell'offerta ovvero mancata corrispondenza dell'impronta digitale dei documenti di offerta trasmessi con quella assegnata dal sistema in fase di conferma di partecipazione. Nella fase di valutazione dei documenti facenti parte dell'offerta tecnica la piattaforma telematica ha evidenziato che l'elaborato denominato "relazione tecnica parco automezzi" facente parte dell'Offerta tecnica non risulta corrispondere con lo stesso documento marcato mediante generazione dell'impronta digitale entro la data di scadenza fissata per la presentazione dell'offerta". Infatti, come chiaramente indicato al punto 13 del Disciplinare di gara, tale difformità determina la non ammissibilità e conseguentemente l'esclusione dell'OE dalla procedura di gara. A tal fine si segnala che la SA, in risposta alla segnalazione pervenuta tramite PEC dall'OE partecipante, ha preventivamente acquisito l'attestazione del gestore della piattaforma che conferma l'assenza di malfunzionamenti della piattaforma. Tale documentazione risulta posta agli atti della procedura".*

Con verbale n. 3, del 24 luglio 2024, la Commissione giudicatrice ha disposto l'aggiudicazione in favore di Gea Service s.r.l., successivamente approvata con verbale n. 11, del 26 luglio 2024 dal Consiglio di Amministrazione di Srt s.p.a.

Con istanza datata 21 agosto 2024 la Teknoservice s.r.l. ha richiesto l'accesso ai seguenti atti: "a) copia del file «relazione tecnica parco mezzi» caricato entro le ore 12:00 del 12.7.2024. in sede di presentazione di domanda di partecipazione; b) copia del file «relazione tecnica parco mezzi» caricato successivamente, quando si è aperta la «finestra temporale» per il nuovo upload del file; c) copia delle impronte digitali apposte automaticamente dal sistema, sia in occasione del primo caricamento (quello effettuato prima delle ore 12:00 del 12 luglio 2024) sia in occasione del secondo caricamento (quello effettuato in occasione della apertura della finestra temporale per il nuovo upload); d) copia di tutti i file di log dai quali si evincano le operazioni effettuate dal sistema; e) copia del codice sorgente della piattaforma di e-procurement «Acquisti Telematici» adoperata per la conduzione delle operazioni di gara. f) copia della attestazione del gestore della piattaforma alla quale si fa riferimento nel provvedimento di esclusione".

Con nota del 30 agosto 2024, in riscontro a tale richiesta, la stazione appaltante ha trasmesso la documentazione sopra citata (con le precisazioni di cui all'allegata relazione di Digitalpa), ad esclusione della copia del codice sorgente della piattaforma utilizzata nella procedura di gara.

Le argomentazioni poste a sostegno del diniego parziale dell'accesso possono essere così riassunte:

a) il codice sorgente è protetto da copyright; b) il programma è stato certificato da Agid, Anac e Acn; c) la consultazione del codice sorgente sarebbe inutile per la Teknoservice; d) il codice sorgente non sarebbe un documento informatico.

Avverso tale provvedimento, la Teknoservice s.r.l. ha proposto dinanzi al T.a.r Piemonte – unitamente al ricorso avverso il provvedimento di esclusione e gli atti di gara – istanza ai sensi dell'art. 116, secondo comma, c.p.a., chiedendo di “accertare e dichiarare il diritto d'accesso della ricorrente agli atti e documenti domandati in ostensione, condannando le parti intimare a concedere copia di quanto richiesto in sede di accesso, ed annullando gli atti mediante i quali si è opposto il parziale diniego alla richiesta ostensiva formulata da Teknoservice”.

Con l'istanza incidentale di accesso presentata nell'ambito del giudizio di primo grado, la Teknoservice ha, in particolare:

- 1) contestato la ricostruzione dei fatti operata dal gestore della piattaforma, poiché la Teknoservice avrebbe provveduto a caricare per tempo l'impronta digitale del file «relazione tecnica parco mezzi;
- 2) eccepito l'inattendibilità delle argomentazioni poste da DigitalPa a fondamento della ricostruzione fattuale che ha giustificato la sua esclusione, richiamando l'orientamento giurisprudenziale secondo cui è la stazione appaltante a dover fornire prova dei fatti «su cui grava quindi l'onere della prova circa “l'assenza di anomalie o malfunzionamenti della piattaforma prescelta per la gara” (Cons. St., Sez. III, 24.11.2020 n. 7352; Cons. St., Sez. III, 7.1.2020 n. 86)» (Cons. Giust. Amm. Sic., 28.4.2022, n. 522; in termini Cons. St., Sez. IV, 15.12.2022, n. 10983);
- 3) dedotto la violazione del principio di pubblicità delle sedute di gara, visto che l'integrità del file (*rectius*: la corretta modalità di caricamento dello stesso) è stata appurata senza le dovute garanzie della seduta pubblica;
- 4) lamentato la violazione dell'art. 30 del d.lgs. n. 36/2023 nella parte in cui afferma la regola della «b) non esclusività della decisione algoritmica, per cui comunque esiste nel processo decisionale un contributo umano capace di controllare, validare ovvero smentire la decisione automatizzata», visto che nessun essere umano (né all'interno della stazione appaltante, né all'interno di Digitalpa) è in grado di operare una ricostruzione dei fatti che chiarisca se al momento di caricamento dell'offerta la Teknoservice abbia commesso un errore nel caricare la impronta digitale, ovvero l'errore sia stato commesso dalla piattaforma e, dunque, Teknoservice sia incolpevole;

5) lamentato l'inversione procedimentale predisposta dalla piattaforma telematica, che ha scisso in due fasi il procedimento di caricamento dell'offerta, con una regola che non trova alcuna ragione di interesse pubblico ed è contrastante con la scansione prevista dall'art. 71 c.p.a.

Il T.ar. ha respinto l'istanza di accesso con l'ordinanza 4 dicembre 2024, n. 1269.

La società Teknoservice s.r.l. ha proposto appello per i motivi riportati nella parte in diritto.

Si sono costituite nel giudizio di secondo grado Srt s.p.a. e Digitalpa s.r.l., chiedendo di dichiarare l'appello infondato.

All'udienza del 10 aprile 2025 la causa è stata trattenuta in decisione.

DIRITTO

Con un unico, articolato, mezzo di gravame Teknoservice s.r.l. deduce *“violazione e falsa applicazione dell'art. 97 cost., degli artt. 22 ss. della l. n. 241/1990 e dell'art. 30 del d.lgs. n. 36/2023. i.a. le argomentazioni sottese alla richiesta formulata in prime cure”*.

Premette la parte appellante che, nel giudizio di primo grado, aveva lamentato il fatto che la propria istanza di accesso non fosse stata esitata dalla stazione appaltante, ma da Digitalpa, alle cui determinazioni la Srt si sarebbe supinamente adagiata.

In particolare, ad avviso della Teknoservice, Digitalpa avrebbe rifiutato di concedere l'accesso al codice adducendo ragioni strumentali, che Srt in maniera illegittima non si sarebbe peritata di autonomamente valutare.

In ogni caso, nel ricorso di primo grado si era evidenziato che le argomentazioni addotte dal gestore privato a sostegno del diniego di accesso al software avrebbero dovuto considerarsi illegittime.

In particolare, Digitalpa non avrebbe potuto negare la ostensibilità del codice sorgente adducendo la ipotetica natura di opera dell'ingegno del codice stesso, come tale coperta da *copyright*, posto che nel caso di specie dovrebbero, in ogni caso, prevalere le esigenze sottese al principio di trasparenza. Ciò in ragione del fatto che i dati adoperati dalla commissione nello svolgimento della procedura, e sulla base dei quali quest'ultima ha deciso di estromettere Teknoservice s.r.l. dalla gara ad evidenza pubblica in esame, sono gestiti da un software di una società privata.

Tale conclusione trarrebbe argomento, nella prospettiva in esame, dalla previsione di cui all'art. 30 del Codice dei contratti pubblici, secondo cui le amministrazioni debbono assicurare la disponibilità del codice sorgente dei prodotti software adoperati ai fini dello svolgimento dell'attività amministrativa e devono adottare soluzioni che garantiscano informazioni significative sulla logica utilizzata.

Né in senso contrario potrebbe addursi la circostanza che tale software sia stato certificato da Agid o Anac. Tale certificazione, secondo la società appellante, non priverebbe la Teknoservice del diritto di controllare direttamente le modalità di funzionamento del software e non abilita certamente il

gestore della piattaforma telematica a violare quanto afferma l'art. 30 dello stesso articolato normativo.

In favore di tale conclusione deporrebbe un consolidato orientamento giurisprudenziale sviluppatosi con riguardo alle procedure relative a concorsi pubblici per l'accesso al pubblico impiego.

Su tali basi, la parte appellante lamenta, in primo luogo, l'erroneità della decisione impugnata nella parte in cui si ha ritenuto di discostarsi dagli orientamenti giurisprudenziali richiamati a sostegno dell'istanza incidentale di accesso formulata in primo grado.

In senso contrario, la parte appellante rileva che, analogamente a quanto verificatosi nella fattispecie esaminate dalla giurisprudenza richiamata, anche nella odierna procedura concorsuale sarebbe stato il programma a svolgere funzioni di «recettore intermediario», acquisendo la prima impronta digitale, e comparandola con la seconda.

Di qui la necessità di accesso al codice sorgente al fine di verificare come si sono svolte le operazioni di acquisizione delle impronte digitali e se il programma contenga dei «bug» o delle debolezze di sistema.

Inoltre, l'accesso al software appare, nella prospettiva in esame, necessario anche per la delicatezza delle funzioni svolte dalla piattaforma al momento in cui ha acquisito le impronte digitali e, quindi, le offerte.

Ciò in quanto nel caso in esame il processo di acquisizione è stato svolto autonomamente da un software, senza alcun intervento umano e senza che nessuno (né all'interno della stazione appaltante, né all'interno di Digitalpa) sia in grado di operare una ricostruzione «a ritroso» dei fatti in violazione del principio di pubblicità delle sedute di gara.

Ricorda, al riguardo, la parte appellante che, nelle procedure concorsuali condotte tradizionalmente, la gestione del plico chiuso contenente l'offerta recapitata alla stazione appaltante sarebbe stata effettuata da un ufficio protocollo e l'apertura del plico, al fine della verifica della completezza della documentazione, sarebbe avvenuta in seduta pubblica, alla presenza dei rappresentanti delle imprese. Nel caso in esame, invece, la valutazione della integrità dell'offerta «uploadata» da Teknoservice è stata fatta in automatico da un algoritmo, senza che delle operazioni compiute dal programma si abbia traccia in un registro che possa avere rilievo fidefacente. La disponibilità del codice sorgente e la conoscibilità delle logiche di funzionamento costituirebbero, dunque, ad avviso dell'appellante, indispensabili succedanei della seduta pubblica e delle tecniche di verbalizzazione idonee a conferire fede privilegiata a determinati momenti.

Ciò anche alla luce del fatto che le imprese private che gestiscono i software hanno interesse a negare che vi siano stati dei problemi imputabili ad errori di programmazione posto che ove *“si diffondesse la voce che una piattaforma è mal programmata e commette errori, le amministrazioni tenderebbero*

a rivolgersi ad altre piattaforme, con evidente danno economico per l'impresa che ha progettato la piattaforma sospettata di inaffidabilità".

Di qui la conclusione per cui tali imprese verserebbero in una posizione di conflitto di interessi, e non potrebbero, per tale ragione, essere ritenute aprioristicamente affidabili quando chiamate a riferire su come si sono svolte talune vicende concretatesi per mezzo delle piattaforme da essi realizzate.

Del resto, rileva l'appellante, la Teknoservice opera in un settore diverso rispetto a quello di Digitalpa, la quale offre servizi informatici alle amministrazioni, laddove Teknoservice effettua servizi di igiene urbana.

Il che dimostrerebbe che l'acquisizione del software non potrebbe mai portare ad un indebito vantaggio commerciale a favore della odierna appellante anche alla luce del fatto che quest'ultima, peraltro, sarebbe obbligata a trattare il codice sorgente acquisito in ostensione con le dovute cautele, senza alcuna possibilità di divulgarlo.

La necessità della ostensione del codice sorgente sarebbe ulteriormente corroborata dalla considerazione per cui che i *files di log* risentirebbero degli eventuali errori di programmazione.

Più in generale, assume l'appellante che i *files di log* sono documenti informatici di natura eterogenea e la cui affidabilità va valutata in ragione di quanto previsto dall'art. 20, comma 1 bis, del Codice dell'amministrazione digitale, secondo il quale il valore probatorio di ciascun documento informatico va valutato in base alle caratteristiche di sicurezza, integrità e immodificabilità.

Tanto premesso, rileva l'appellante che i log prodotti da Digitalpa sarebbero facilmente modificabili, come dimostrerebbe il fatto che la stessa Teknoservice ne ha volutamente prodotto in giudizio di prime cure una copia modificata.

Sotto un ulteriore profilo, la parte appellante lamenta l'erroneità della decisione impugnata nella parte in cui, sulla base dell'art. 35, del codice dei contratti pubblici, ha ritenuto non indispensabile l'accesso al software.

Tale conclusione, ad avviso della società appellante, sarebbe erronea posto che, alla stregua del citato art. 35, la stretta indispensabilità andrebbe valutata in termini di strumentalità tra l'acquisizione del codice sorgente e le censure formulate o a formularsi, non in termini di «unicità» del mezzo di prova. Infine, la parte appellante, con la memoria di replica depositata in data 28 marzo 2025, ha formulato istanza di rinvio ex art. 267 TFUE.

Ricorda, al riguardo, la parte appellante che la materia oggetto dell'odierno giudizio è profondamente conformata dal diritto dell'UE sia con riferimento al settore dei contratti pubblici, sia con riferimento a quello delle firme elettroniche, e della prestazione di servizi telematici. Quest'ultimo settore, osserva l'appellante, è disciplinato anzitutto dal Regolamento Eidas, n. 910/2014.

Nel considerando n. 7 del predetto Regolamento, si ricorda che «il Parlamento europeo ha sottolineato l'importanza della sicurezza dei servizi elettronici». Nel considerando n. 28, poi, si afferma che «al fine di migliorare in particolare la fiducia delle piccole e medie imprese (PMI) e dei consumatori nel mercato interno e di promuovere l'impiego dei servizi e prodotti fiduciari, è opportuno introdurre le nozioni di servizi fiduciari qualificati e di prestatori di servizi fiduciari qualificati, per precisare i requisiti e gli obblighi che garantiscano un elevato livello di sicurezza di tutti i servizi e prodotti fiduciari qualificati impiegati o prestati». All'art. 3, comma 1, n. 52, si afferma che «52) “registro elettronico”, una sequenza di registrazioni di dati elettronici che garantisce l'integrità di tali registrazioni e l'accuratezza dell'ordine cronologico di tali registrazioni».

Identiche prescrizioni sono, poi, recate dall'art. 19 e da molte altre norme del regolamento eIDAS.

Alla luce del richiamato contesto normativo, ritiene l'appellante che non sia conforme alle predette fonti di regolazione eurounitarie il fatto che la Teknoservice sia stata esclusa da una gara di appalto per effetto di una decisione assunta sulla base di evidenze informatiche (i log prodotti da Digitalpa) prive di un elevato livello di sicurezza.

Sotto altro profilo, la negazione dell'accesso al codice sorgente violerebbe il diritto ad un ricorso effettivo, che in materia di appalti è garantito in maniera vigorosa dalla direttiva europea 1989/665, viene ad essere compromesso laddove la Teknoservice non è posta in condizioni di contestare le argomentazioni svolte da Digitalpa in ordine ai presunti errori di caricamento dell'offerta in cui sarebbe incorsa la odierna appellante.

Il motivo, complessivamente articolato, non è fondato.

In via preliminare il Collegio ricorda che, come chiarito dall'Adunanza Plenaria 18 marzo 2021, n. 4, la necessità (o la stretta indispensabilità) della conoscenza del documento determina il nesso di strumentalità tra il diritto all'accesso e la situazione giuridica 'finale', nel senso che l'ostensione del documento amministrativo deve essere valutata, sulla base di un giudizio prognostico ex ante, come il tramite – in questo senso strumentale – per acquisire gli elementi di prova in ordine ai fatti (principali e secondari) integranti la fattispecie costitutiva della situazione giuridica 'finale' controversa e delle correlative pretese astrattamente azionabili in giudizio.

In tale ordine di idee, è stato chiarito che la pubblica amministrazione detentrica del documento e il giudice amministrativo adito nel giudizio di accesso ai sensi dell'art. 116 c.p.a. non devono svolgere alcuna ultronea valutazione sulla influenza o sulla decisività del documento richiesto nell'eventuale giudizio instaurato, poiché un simile apprezzamento compete, se del caso, solo all'autorità giudiziaria investita della questione e non certo alla pubblica amministrazione o allo stesso giudice amministrativo nel giudizio sull'accesso.

Un diverso ragionamento, ad avviso della Plenaria, reintrodurrebbe nella disciplina dell'accesso difensivo e, soprattutto, nella sua pratica applicazione limiti e preclusioni che, invece, non sono contemplati dalla legge, la quale ha già previsto, come si è detto, adeguati criteri per valutare la situazione legittimante all'accesso difensivo e per effettuare il bilanciamento tra gli interessi contrapposti all'ostensione del documento o alla riservatezza.

Alla stregua di tali preliminari considerazioni, la Plenaria ha, pertanto, affermato i seguenti principi di diritto:

- a) in materia di accesso difensivo ai sensi dell'art. 24, comma 7, della l. n. 241 del 1990 si deve escludere che sia sufficiente nell'istanza di accesso un generico riferimento a non meglio precisate esigenze probatorie e difensive, siano esse riferite a un processo già pendente oppure ancora instaurando, poiché l'ostensione del documento richiesto passa attraverso un rigoroso, motivato, vaglio sul nesso di strumentalità necessaria tra la documentazione richiesta e la situazione finale che l'istante intende curare o tutelare;
- b) la pubblica amministrazione detentrica del documento e il giudice amministrativo adito nel giudizio di accesso ai sensi dell'art. 116 c.p.a. non devono invece svolgere ex ante alcuna ultronea valutazione sull'ammissibilità, sull'influenza o sulla decisività del documento richiesto nell'eventuale giudizio instaurato, poiché un simile apprezzamento compete, se del caso, solo all'autorità giudiziaria investita della questione e non certo alla pubblica amministrazione detentrica del documento o al giudice amministrativo nel giudizio sull'accesso, salvo il caso di una evidente, assoluta, mancanza di collegamento tra il documento e le esigenze difensive e, quindi, in ipotesi di esercizio pretestuoso o temerario dell'accesso difensivo stesso per la radicale assenza dei presupposti legittimanti previsti dalla l. n. 241 del 1990.

È nel perimetro di tali principi che deve trovare soluzione la questione all'odierno esame, senza, dunque, alcuna possibilità per l'odierna decisione di interferire nella definizione della diversa questione relativa alla legittimità o meno della esclusione della parte appellante dalla gara ad evidenza pubblica di che trattasi.

Tanto premesso, destituito di fondamento è, in primo luogo, il sub-motivo con il quale la parte appellante invoca l'applicazione al caso in esame dell'art. 30, del d.lgs. 32 marzo 2023, n. 36.

Come riferito, la società appellante giunge a tale conclusione muovendo dalla premessa secondo cui l'algoritmo utilizzato dalla Digitalpa s.r.l. costituisca un sistema informatico sostitutivo di un'ordinaria sequenza procedimentale e come tale, strettamente funzionale al contenuto dispositivo dell'atto con cui l'appellante stessa è stata esclusa dalla gara.

L'argomentazione dell'appellante non può essere condivisa.

Ritiene, infatti, il Collegio che nel caso in esame non venga in rilievo una decisione amministrativa algoritmica, ma, più limitatamente, un algoritmo di mero supporto alle decisioni che restano rigorosamente affidate al fattore umano e che, dunque, si inscrivono nella più tradizionale impostazione, che vede nell'informatica un mero ausilio rispetto allo svolgimento dell'attività amministrativa nelle sue classiche modalità operative.

A sostegno di questa conclusione, occorre osservare che il software in esame si limita a comparare alcuni parametri caratterizzanti le offerte e, segnatamente, le impronte digitali calcolate nella “fase 1” con quelle riferibili ai file effettivamente caricati nella “fase 2”, durante l'apertura della finestra temporale denominata: “arco temporale di caricamento dei file offerta tecnica ed economica”.

Una volta rilevata la corrispondenza ovvero la difformità, esso fornisce alla Stazione appaltante - e dunque alla Commissione giudicatrice -, il dato relativo a tale corrispondenza o difformità.

Più in particolare:

- nella “fase 1” del procedimento, il software si limita a memorizzare le impronte digitali dei file calcolati dai partecipanti;
- nella “fase 2” del procedimento, il software raffronta tali impronte con quelle dei file effettivamente caricati sulla piattaforma, restituendo unicamente un dato di conformità o difformità delle impronte medesime.

Sulla base di tali considerazioni è possibile confutare la tesi dell'appellante secondo cui nel caso in esame il software avrebbe compiuto decisioni automatizzate in luogo della commissione di gara e che lo stesso software ha provveduto all'automatica esclusione dell'operatore economico.

La decisione di escludere Teknoservice s.r.l., in conformità al doc. 3, punto 13.1, del Disciplinare di gara, recante le Regole per la presentazione dell'offerta, secondo cui : *“La S.A. verificherà, a pena d'esclusione, la corrispondenza dell'impronta digitale dei documenti di offerta trasmessi con quella assegnata dal sistema in fase di conferma di partecipazione”*, è stata adottata dalla Commissione di gara, nella seduta pubblica telematica del 23 luglio 2024, in piena autonomia, sulla base dei dati registrati dalla Piattaforma.

Da quanto rilevato discende la non applicabilità alla fattispecie in esame dell'art. 30, comma 2, lett. a), disposizione quest'ultima che, invece, disciplina, codificando sul punto gli approdi della più recente giurisprudenza del Consiglio di Stato, i principi che devono governare l'adozione dei “provvedimenti per algoritmi”(principio di trasparenza; principio di non esclusività della decisione algoritmica principio di non discriminazione: *cfr. ex multis*, Consiglio di Stato, 8 aprile 2019, n. 2270).

Proprio l'appartenenza del software in esame al *genus* degli algoritmi di mero supporto segna una netta discontinuità con le fattispecie analizzate dalle decisioni giurisprudenziali invocate

dall'appellante a sostegno delle proprie argomentazioni, nelle quali, ad esempio, si è rinvenuta la necessità di ampliare il campo del diritto di accesso, fino a ricomprendervi il diritto di accedere al codice sorgente del programma che si occupa dell'assegnazione delle sedi per la mobilità dei docenti, spostando i trasferimenti in una provincia piuttosto che in un'altra, in un posto di sostegno piuttosto che in un posto comune, senza tener conto delle preferenze indicate nelle rispettive domande di trasferimento, senza alcuna motivazione e in difetto della benché minima trasparenza, rispetto alle quali si è, in maniera condivisibile, affermato che l'utilizzo di procedure "robotizzate" non può, tuttavia, essere motivo di elusione dei principi che conformano il nostro ordinamento e che regolano lo svolgersi dell'attività amministrativa. (Cons. Stato, sez. VI, 2 gennaio 2020 n. 30).

La pronunce giurisprudenziali richiamate dalla parte appellante muovono, infatti, dal presupposto che il codice sorgente sia da considerare «atto amministrativo» o « documento amministrativo » nei cui confronti è dunque necessario accordare il diritto di accesso ai sensi della l. n. 241 del 1990, senza che sia di ostacolo l'eventuale permanenza di diritti di proprietà intellettuale sul software in capo al privato appaltatore.

Il recente Codice dei contratti pubblici, con il citato art. 30, conferma questa impostazione, esprimendo una chiara preferenza per gli algoritmi *open source* rispetto a quelli proprietari e, in ogni caso, assicurando la disponibilità del codice sorgente, prevedendo inoltre che, nei casi di decisione algoritmica, la motivazione del provvedimento finale deve richiamare il codice sorgente e il modello matematico impiegati, salva la possibilità per l'interessato di esercitare il diritto d'accesso documentale a tali "documenti" ed anche al data set.

In questi casi, l'art. 30 mostra un deciso *favor* per l'esercizio dell'accesso difensivo rispetto alla tutela della proprietà intellettuale, ancorché coperta da brevetto, evidentemente ritenendo che la mancata conoscenza del codice sorgente impedirebbe infatti la tracciabilità dell'algoritmo, violando il dovere esplicativo minimo previsto dalle raccomandazioni europee.

I principi affermati nelle predette decisioni, così come codificati dal citato art. 30, non possono, tuttavia trovare applicazione nel caso in esame in cui non ricorre la fattispecie del procedimento amministrativo basato su decisioni algoritmiche, ma una decisione affidata al fattore umano rispetto alla quale la procedura automatizzata si è limitata ad accertare uno specifico fatto, ovvero l'effettuazione o meno da parte dell'operatore economico del calcolo dell'impronta digitale.

Parimenti da disattendere è la censura che, al fine di ulteriormente argomentare la necessità dell'accesso al codice sorgente, contesta la mancata trasparenza della procedura relativa alla verifica della completezza della documentazione e, per tale via, la violazione del principio di pubblicità delle sedute di gara.

Ricorda il Collegio che l'adozione delle tecnologie dell'informazione, sia pure con funzione di mero supporto alla decisione affidata al fattore umano, si riflette sugli istituti del procedimento amministrativo, contribuendo alla costruzione di una amministrazione che si adatti ai mutamenti tecnologici al fine di gestire in maniera più efficiente e trasparente il procedimento.

La digitalizzazione ha inciso sulle modalità di esercizio del potere, ampliando le possibilità di azione amministrativa con l'obiettivo di fornire nuovi servizi.

L'uso della telematica nell'azione amministrativa è oramai riconosciuto come principio generale di un nuovo diritto amministrativo; in questa direzione può essere letto l'art. 3 bis della L. n. 241 del 1990 ("Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi"), inserito a seguito della novella del 2005, il quale prevede che per conseguire maggiore efficienza nella loro attività le amministrazioni incentivano l'uso della telematica, anche nei rapporti con i privati.

Prima del riconoscimento espresso di tale principio, la rilevanza dell'attività amministrativa in forma elettronica era stata sancita in maniera indiretta nel Testo unico sulla documentazione amministrativa (d.P.R. n. 445/2000) e nel Codice dell'Amministrazione Digitale (D.Lgs. n. 82/2005).

Le procedure ad evidenza pubblica non sfuggono alla propensione del procedimento amministrativo verso gli strumenti telematici (artt. 20, 27 e 28, del d.lgs. 31 marzo 2023, n. 36).

Il principio della trasformazione digitale è stato fortemente valorizzato dal nuovo Codice dei contratti pubblici.

In particolare, le disposizioni della Parte II del Libro I del Codice, in linea con il PNRR e con le indicazioni rivenienti dalla legge delega, mirano, infatti, all'obiettivo di fondo di digitalizzare l'intera procedura dei contratti pubblici (c.d. digitalizzazione dell'intero ciclo di vita del contratto), fondandola sulla acquisizione di dati e sulla creazione di documenti nativi digitali, da realizzarsi tramite piattaforme digitali in modo da rendere possibile la interazione con le banche dati esistenti e consentendo, contemporaneamente, un arricchimento delle stesse con i nuovi dati prodotti dalle singole procedure.

Ciò che, oggi, caratterizza le gare telematiche rispetto ad una tradizionale gara d'appalto è l'utilizzo di una piattaforma *on-line* di *e-procurement* e di strumenti di comunicazione digitali (firma digitale e PEC), che, di fatto, rendono l'iter più efficiente, veloce e sicuro e trasparente rispetto a quello tradizionale, basato sull'invio cartaceo della documentazione e delle offerte. Non si tratta solo di sostituire il documento cartaceo, scritto e sottoscritto, col documento informatico bensì di gestire per intero, tramite piattaforme, il ciclo di vita del contratto che va dalla programmazione all'esecuzione.

Le fasi di gara seguono una successione temporale che offre la garanzia di corretta partecipazione, inviolabilità e segretezza delle offerte: la firma digitale garantisce infatti la certezza del firmatario dell'offerta e la marcatura temporale ne garantisce la data certa di firma e l'univocità della stessa.

Attraverso l'apposizione della firma e marcatura temporale, da effettuare inderogabilmente prima del termine perentorio fissato per la partecipazione, e la trasmissione delle offerte esclusivamente durante la successiva finestra temporale, si garantisce la corretta partecipazione e inviolabilità delle offerte.

I sistemi provvedono, invero, alla verifica della validità dei certificati e della data e ora di marcatura. L'affidabilità degli algoritmi di firma digitale e marca temporale garantiscono la provenienza del documento (firma digitale) e la data di perfezionamento (marca temporale) contribuendo alla sicurezza della fase di invio/ricezione delle offerte in busta chiusa.

Nella gara telematica la sottoscrizione e la marcatura temporale dell'offerta, a cura del concorrente, garantiscono che l'offerta stessa non venga, nelle more, modificata; in qualche modo, come è stato attentamente osservato, firma e marcatura corrispondono anche alla tradizionale "chiusura della busta".

Il *timing* di gara indica poi all'impresa, oltre che il termine ultimo perentorio di "chiusura della busta", anche il periodo, e relativo termine ultimo, di upload, ossia di trasferimento dei dati sul server della stazione appaltante.

Inoltre, nessuno degli addetti alla gestione della gara potrà accedere ai documenti dei partecipanti, fino alla data e all'ora di seduta della gara, specificata in fase di creazione della procedura.

Alla luce di quanto fin qui detto - in ordine, in particolare, alla garanzia non solo della tracciabilità di tutte le fasi delle gare telematiche, ma anche dell'inviolabilità delle buste elettroniche contenenti le offerte e dell'incorruttabilità di ciascun documento presentato –il principio della pubblicità delle sedute risulta, nell'ambito della gara telematica, maggiormente garantito rispetto al procedimento tradizionale.

L'analisi dei precedenti giurisprudenziali conferma le conclusioni qui esposte.

Il Consiglio di Stato ha infatti, avuto modo di chiarire che il principio di pubblicità delle sedute deve essere rapportato non ai canoni storici che hanno guidato l'applicazione dello stesso, quanto piuttosto alle peculiarità e specificità che l'evoluzione tecnologica ha consentito di mettere a disposizione delle procedure di gara telematiche, in ragione del fatto che la piattaforma elettronica che ha supportato le varie fasi di gara assicura l'intangibilità del contenuto delle offerte (indipendentemente dalla presenza o meno del pubblico) posto che ogni operazione compiuta risulta essere ritualmente tracciata dal sistema elettronico senza possibilità di alterazioni. In altri termini è garantita non solo la tracciabilità di tutte le fasi ma proprio l'inviolabilità delle buste elettroniche contenenti le offerte e l'incorruttabilità di ciascun documento presentato (Consiglio di Stato sez. V, 21 novembre 2017, n. 5388).

Parimenti da respingere è l'ulteriore argomento, invocato dalla parte appellante a sostegno del proprio diritto di accessi difensivo, facente leva sull'asserito conflitto di interessi di Digitalspa.

Sul punto occorre premettere che la scelta della stazione appaltante di avvalersi del software di Digitalpa è coerente al quadro normativo di riferimento.

Gli artt. 68 e 69 del Codice dell'Amministrazione Digitale (CAD) prevedono una certa discrezionalità nell'acquisizione della soluzione più adeguata tra quelle disponibili sul mercato, sia essa open source o di tipo proprietario. In particolare, per le esigenze di riuso del software da parte di altre pubbliche amministrazioni (ma diremmo qui anche per le esigenze di trasparenza), si prevede che la p.a. committente acquisisca, quando possibile, la titolarità dei programmi informatici sviluppati per essa, a meno che ciò risulti eccessivamente oneroso per comprovate ragioni di carattere tecnico-economico (art. 69, comma 2, CAD). In alternativa, la p.a. può decidere di avvalersi, per ragioni tecniche ed economiche, di soluzioni di tipo proprietario, lasciando in capo al privato appaltatore i diritti di proprietà intellettuale sul software, acquisendo solamente la facoltà d'uso, secondo il *business model* individuato nella procedura di acquisizione, nell'ambito della quale, attraverso il bando e il contratto, vengono chiariti i diritti e gli obblighi dell'appaltatore e del committente.

In tale ultimo caso il privato conserva i diritti esclusivi anche sul codice sorgente e, dunque, le facoltà di negare l'accesso a terzi per la tutela dei segreti industriali.

La scelta delle modalità di acquisizione del software è rimessa alla p.a., secondo i criteri di valutazione indicati negli artt. 68 e 69 CAD.

Tanto premesso, l'art. 16 comma 1, del d.lgs. 31 marzo 2023 n. 36, stabilisce che “ *Si ha conflitto di interessi quando un soggetto che, a qualsiasi titolo, interviene con compiti funzionali nella procedura di aggiudicazione o nella fase di esecuzione degli appalti o delle concessioni e ne può influenzare, in qualsiasi modo, il risultato, gli esiti e la gestione, ha direttamente o indirettamente un interesse finanziario, economico o altro interesse personale che può essere percepito come una minaccia concreta ed effettiva alla sua imparzialità e indipendenza nel contesto della procedura di aggiudicazione o nella fase di esecuzione*”.

Il successivo comma 2, con l'obiettivo di perimetrare e rendere tassativa la nozione di conflitto di interessi, recependo gli insegnamenti della giurisprudenza nazionale in materia, stabilisce che “ *In coerenza con il principio della fiducia e per preservare la funzionalità dell'azione amministrativa, la percepita minaccia all'imparzialità e indipendenza deve essere provata da chi invoca il conflitto sulla base di presupposti specifici e documentati e deve riferirsi a interessi effettivi, la cui soddisfazione sia conseguibile solo subordinando un interesse all'altro*”.

In conformità con il fondamentale principio della fiducia, codificato dall'art. 2, del d.lgs. 31 marzo 2023 n. 36, il legislatore richiede, dunque, che la prova del conflitto di interessi sia fornita dalla parte che lo invoca sulla base di presupposti specifici e documentati.

Nel caso di che trattasi, al di là delle mere congetture formulate dalla parte appellante, manca financo un principio di prova in ordine alla posizione di conflitto di interessi di Digitalpa.

Ne discende che il dedotto vizio è, pertanto, rimasto indimostrato e solo apoditticamente affermato. Destituite di fondamento appaiono anche le censure formulate dalla Teknoservice s.r.l. in ordine alla mancata attendibilità, sotto il profilo del relativo valore probatorio, dei *files di log* trasmessi da Digitalpa alla stazione appaltante.

Le argomentazioni sviluppate sul punto dalla parte appellante, per un verso, appaiono non corrette e per altro verso provano troppo.

In particolare, non corretto è l'assunto, peraltro supportato da apodittiche affermazioni in ordine ad un asserito malfunzionamento della piattaforma telematica, in ordine alla intrinseca inattendibilità dei *files di log*.

I *files di log* della piattaforma telematica (c.d. giornale di bordo) sono dei registri informatici contenenti il dettaglio degli accessi (c.d. chiamate) e degli eventi occorsi. I *files di log*, in particolare, sono costituiti dalla registrazione sequenziale e cronologica da parte del sistema informatico delle operazioni effettuate da un utente o da un amministratore ovvero anche dalla registrazione delle operazioni compiute in automatico da un sistema e costituisce una sorta di "registro degli eventi".

Essi consentono, dunque, per quanto concerne le gare ad evidenza pubblica, di avere conoscenza delle attività eseguite dagli operatori economici e dalla stazione appaltante che hanno interagito con il sistema.

In ordine alla attendibilità, sotto il profilo probatorio, dei *files log* si esprime un costante orientamento del Consiglio di Stato, secondo cui *"se invece l'amministrazione deposita i file log, ossia report tecnici ricostruenti le interazioni tra utente e sistema informatico nel periodo di interesse, da cui risulta l'assenza di anomalie o malfunzionamenti della piattaforma prescelta per la gara, è da ritenersi dimostrato il corretto funzionamento della piattaforma durante le operazioni di caricamento della domanda e il ritardo, anche se esiguo, è pertanto da imputare al concorrente, che correttamente viene quindi escluso dalla gara"*. (ex pluribus, Cons. Stato, Sez. III, 24 novembre 2020, n. 7352; cfr. Consiglio di Stato, sez. V, sent. n. 6605 del 4 ottobre 2021).

In senso analogo è stato chiarito che *«Sul piano probatorio infine il principio di vicinanza della prova impone un onere di allegazione all'Amministrazione, che essa ha soddisfatto nei termini esposti (ndr. file log e relazione sul funzionamento della piattaforma, forniti dal gestore della piattaforma stessa). Non risulta quindi un malfunzionamento della piattaforma ovvero una incertezza in ordine alle cause*

del mancato invio della documentazione di offerta, a fronte delle relazioni tecniche depositate in atti e del dato di fatto che, entro il termine di scadenza del 04/04/2024, sono pervenute regolarmente alla Stazione appaltante n. 12 offerte per i 3 lotti, di cui 8 giunte proprio nella mattinata del giorno di scadenza 4 aprile 2024».

Per altro verso, prova troppo l'affermazione di parte appellante secondo cui i log prodotti da Digitalpa sarebbero facilmente modificabili, come dimostrerebbe il fatto che la stessa Teknoservice ne ha volutamente prodotto in giudizio di prime cure una copia modificata.

In senso contrario occorre, infatti, osservare che tutte le prove documentali sono, in linea di principio, suscettibili di essere alterate, ma ciò non influisce di certo sulla loro intrinseca attendibilità quando, come accaduto nel caso in esame, non si riesce a provare in giudizio la loro effettiva alterazione. Volendo fare un paragone col passato, la possibilità di alterare un documento analogico, ad esempio una scrittura privata, non costituisce prova del fatto che la specifica scrittura prodotta da controparte in giudizio sia stata alterata; è invece necessario, in capo a chi lo deduce, dare prova dell'effettiva alterazione del documento e non della astratta possibilità di alterazione.

A sostegno di questa conclusione depone, del resto, il principio della fiducia, previsto dall'art. 2, del codice dei contratti pubblici, inteso come reciproca fiducia nell'azione legittima, trasparente e corretta dell'amministrazione, dei suoi funzionari e degli operatori economici.

Non coglie nel segno neanche il sub-motivo che censura la violazione dell'art. 35, del d.lgs. 31 marzo 2023 n. 36.

In linea generale, occorre ricordare che il legislatore ha ulteriormente circoscritto l'oggetto della situazione legittimante l'accesso difensivo rispetto all'accesso "ordinario", esigendo che la stessa, oltre a corrispondere al contenuto dell'astratto paradigma legale, sia anche collegata al documento al quale è chiesto l'accesso (art. 24, comma 7, della l. n. 241 del 1990), in modo tale da evidenziare in maniera diretta ed inequivoca il nesso di strumentalità che avvince la situazione soggettiva finale al documento di cui viene richiesta l'ostensione, e per l'ottenimento del quale l'accesso difensivo, in quanto situazione strumentale, fa da tramite.

Come chiarito dall'Adunanza plenaria 18 marzo 2021 n. 4, questa esigenza è soddisfatta, sul piano procedimentale, dal successivo art. 25, comma 2, della l. n. 241 del 1990, ai sensi del quale *«la richiesta di accesso ai documenti deve essere motivata»*.

La volontà del legislatore è di esigere che le finalità dell'accesso siano dedotte e rappresentate dalla parte in modo puntuale e specifico nell'istanza di ostensione, e suffragate con idonea documentazione (ad es. scambi di corrispondenza; diffide stragiudiziali; in caso di causa già pendente, indicazione sintetica del relativo oggetto e dei fatti oggetto di prova; ecc.), così da permettere all'amministrazione

detentrica del documento il vaglio del nesso di strumentalità necessaria tra la documentazione richiesta *sub specie* di astratta pertinenza con la situazione “finale” controversa.

In questa prospettiva, l'Adunanza plenaria ha escluso che possa ritenersi sufficiente un generico riferimento a non meglio precisate esigenze probatorie e difensive, siano esse riferite a un processo già pendente oppure ancora instaurando, poiché l'ostensione del documento passa attraverso un rigoroso vaglio circa l'appena descritto nesso di strumentalità necessaria tra la documentazione richiesta e la situazione finale controversa.

A tal fine, l'art. 24 della l. n. 241 del 1990 prevede, al comma 7, un'esclusione basata su un giudizio valutativo di tipo comparativo di composizione degli interessi confliggenti facenti capo al richiedente e, rispettivamente, al controinteressato, modulato in ragione del grado di intensità dei contrapposti interessi ed improntato ai tre criteri della necessità, dell'indispensabilità e della parità di rango.

In particolare, l'art. 24, comma 7 declina il rapporto tra accesso e difensivo e riservatezza entro alcune regole di valutazione, prevedendosi che (a) con riferimento a dati sensibili e giudiziari, l'accesso è consentito nei limiti in cui sia strettamente indispensabile (rapporto di stretta indispensabilità), e (b) in caso di dati idonei a rilevare lo stato di salute e la vita sessuale, se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi sia di rango almeno pari ai diritti dell'interessato, ovvero consista in un diritto della personalità o in un altro diritto o libertà fondamentale (rapporto di stretta indispensabilità con valori di pari rango).

Da quanto osservato discende che, già sul piano della normativa generale relativa all'accesso difensivo, la valutazione di “stretta indispensabilità” costituisce il criterio che regola il rapporto tra accesso difensivo e tutela della segretezza industriale e commerciale, richiedendo un “motivato vaglio sul nesso di strumentalità necessaria tra la documentazione richiesta e la situazione finale che l'istante intende curare o tutelare”.

L'articolo 35, commi 4 e 5, d.lgs. 36/2023 (rubricato: “Accesso agli atti e riservatezza”), a sua volta, prevede che: “Fatta salva la disciplina prevista per i contratti secretati o la cui esecuzione richiede speciali misure di sicurezza e salvo quanto disposto dal comma 5, il diritto di accesso e ogni forma di divulgazione: [...] b) sono esclusi in relazione [...] 3) alle piattaforme digitali e alle informazioni informatiche utilizzate dalla stazione appaltante o dall'ente concedente, ove coperte da diritti di privativa intellettuale [...] 5. In relazione all'ipotesi di cui al comma 4, lett. a) e b), numero 3), è consentito l'accesso al concorrente, se indispensabile ai fini della difesa in giudizio dei propri interessi giuridici rappresentati in relazione alla procedura di gara”. IV-2.2).

Dal tenore letterale della norma emerge, quindi, che il diritto di accesso debba prevalere sul diritto alla riservatezza aziendale solo quando sia indispensabile e strettamente strumentale alla difesa in giudizio del richiedente, nell'ambito della procedura di affidamento del contratto.

In altri termini, con l'art. 35, commi 4 e 5, d.lgs 36/2023, il legislatore ha previsto, a tutela dei diritti di privativa intellettuale relativi alle piattaforme digitali utilizzate nelle procedure di gara (qual è quella, nel caso di specie, utilizzata da Digitalpa), un divieto di accesso e di ogni forma di divulgazione della stessa, incluso, quindi il suo codice sorgente; tale divieto può essere superato, nel bilanciamento dei contrapposti interessi, solamente se il concorrente che chiede l'accesso ne dimostri l'indispensabilità ai fini della difesa in giudizio.

La nozione di "indispensabilità", cui il codice appalti subordina l'accesso nell'ipotesi sopra descritta, deve essere declinata nel senso di insussistenza di altri mezzi di prova idonei a dimostrare i fatti oggetto di contesa tra le parti.

La semplice volontà di verificare e sondare (come è nel caso di specie) non legittima un accesso "meramente esplorativo" alle informazioni riservate, in quanto difetterebbe la comprova della specifica e concreta indispensabilità ai fini difensivi.

Va, al riguardo, ulteriormente evidenziato che l'accesso al codice sorgente da parte dell'interessato espone il titolare dei diritti di proprietà intellettuale al grave rischio di vanificare definitivamente la libertà di iniziativa economica connessa alla commercializzazione di tale software (nell'ipotesi in cui sia fornito alla p.a. committente senza trasferire i codici sorgenti, né i diritti di privativa sul software medesimo), senza tuttavia che l'interessato riesca a soddisfare gli scopi — "difensivi" e non "esplorativi" — per i quali l'accesso viene richiesto.

Ciò pure alla luce del principio, di valenza anche eurounitaria, di proporzionalità, che impone di adottare la soluzione che comporta il sacrificio minore per il diritto fondamentale che si intende comprimere, senza che quest'ultimo risulti vanificato del tutto.

Alla stregua del principio di proporzionalità, occorre in altri termini, che il diritto da sacrificare non venga svilito o frustrato nella sua essenza, ma che sia comunque salvaguardato, e che, nel bilanciamento con un altro diritto fondamentale, venga limitato solamente nella misura strettamente necessaria a consentire la soddisfazione del contrapposto interesse: il che impone di verificare che, tra le varie misure tutte egualmente idonee a perseguire il fine dichiarato (in questo caso la trasparenza della decisione algoritmica per esigenze difensive correlate all'istanza di accesso) venga adottata quella che impone il sacrificio minore per il diritto che si intende limitare.

Pertanto, per l'esercizio del diritto di accesso alle informazioni contenenti possibili segreti tecnici o commerciali, è fondamentale dimostrare non semplicemente un generico interesse alla tutela dei propri interessi giuridicamente rilevanti, quanto piuttosto la concreta necessità di utilizzare la documentazione in giudizio.

Nel caso in esame, tale rigorosa dimostrazione non risulta essere stata fornita dalla Teknoservice S.r.l..

Al riguardo, come in precedenza esposto, la parte appellante si è limitata ad affermare che i *files di log* trasmessi dalla stazione appaltante in sede di richiesta di accesso sarebbero stati forniti in una versione modificabile e, quindi, privi di valore probatorio.

Essa non ha, tuttavia, comprovato le ragioni tecniche in base alle quali non sarebbe idonea, ai fini dell'accertamento tecnico in questione, un'eventuale disamina da parte di un proprio consulente dei predetti *files* in estensione originale, conservati sui server della stazione appaltante e di Digitalpa.

La società appellante non ha fornito neppure un principio di prova in ordine ad un malfunzionamento della piattaforma, non avendo, peraltro, nemmeno contestato specificamente, al di là delle generiche e già ritenute non condivisibili affermazioni in ordine alla loro modificabilità, il report tecnico fornito dalla stazione appaltante.

Reputa il Collegio che anche la richiesta rinvio pregiudiziale alla Corte di Giustizia UE formulata dalla Tecknoservice non sia accoglibile alla luce delle pregresse considerazioni, in punto di mancata lesione del principio di trasparenza, e di quelle che seguono.

La Corte di giustizia ha di recente chiarito che, al fine di attivare l'obbligo per il giudice di ultima istanza di sollevare una questione di pregiudizialità comunitaria, non basta una qualsivoglia possibile interpretazione alternativa della disposizione *sub iudice*, ma essa deve essere plausibile alla luce del contesto e delle finalità della disposizione e del sistema normativo in cui è inserita, a meno che l'interpretazione alternativa non sia riscontrata dal fatto che è stata seguita da altri giudici nazionali o di un altro Stato .

In particolare, la Corte di giustizia ha avuto modo di affermare che “*la mera possibilità di effettuare una o diverse altre letture di una disposizione del diritto dell'Unione, nei limiti in cui nessuna di queste altre letture appaia sufficientemente plausibile al Giudice nazionale interessato, segnatamente alla luce del contesto e della finalità di detta disposizione, nonché del sistema normativo in cui essa si inserisce, non può essere sufficiente per considerare che sussista un dubbio ragionevole quanto all'interpretazione corretta di tale disposizione*”. (Grande Sezione, 6 ottobre 2021 ,in causa C-561/19, Consorzio Italian Management - Catania Multiservizi SpA/Rete Ferroviaria Italiana).

Nella medesima decisione si è ulteriormente evidenziato che andrebbe esclusa l'assenza di ogni ragionevole dubbio legittimante la facoltà di non operare il rinvio pregiudiziale, quando sussistano “orientamenti giurisprudenziali divergenti – in seno agli organi giurisdizionali di un medesimo Stato membro o tra organi giurisdizionali di Stati membri diversi – relativi all'interpretazione di una disposizione del diritto dell'Unione applicabile alla controversia di cui al procedimento principale”.

Dal che, come è stato attentamente rilevato in dottrina, discende, *a contrario*, che il pacifico diritto vivente, anche riconducibile “agli organi giurisdizionali di un medesimo Stato membro”, è condizione sufficiente per rendere flessibile l'obbligo, e per evitare dunque l'abuso del rimedio.

Tanto premesso, la Corte di giustizia, si è, in più occasioni, occupata del rapporto tra le previsioni delle direttive europee sui contratti pubblici e il diritto ad un ricorso efficace verso un giudice imparziale contro le decisioni in materia di contratti pubblici, stabilito dall'art. 1, Dir. 89/665/CE, in linea con l'art. 47, commi 1 e 2, della Carta di Nizza esprimendo a più riprese un *favor* europeo per la tutela dei segreti tecnici e industriali.

La nozione di segreti tecnici o commerciali si desume dall'art. 98 d.lgs. 10 febbraio 2005, n. 30, che, in attuazione dell'art. 2 n. 1 direttiva n. 2016/943/UE del Parlamento europeo e del Consiglio dell'8 giugno 2016, sulla protezione del know-how riservato e delle informazioni commerciali riservate (segreti commerciali) contro l'acquisizione, l'utilizzo e la divulgazione illeciti, contiene la "definizione omogenea di segreto commerciale" e comprende "il know-how, le informazioni commerciali e le informazioni tecnologiche quando esiste un legittimo interesse a mantenere la riservatezza nonché una legittima aspettativa circa la tutela di tale riservatezza", aventi "un valore commerciale, sia esso effettivo o potenziale" (considerando 14).

Il considerando 4 della direttiva 2016/943 stabilisce che: «Le imprese innovative sono sempre più esposte a pratiche fraudolente intese ad appropriarsi illecitamente di segreti commerciali, quali furto, copia non autorizzata, spionaggio economico o violazione degli obblighi di riservatezza, aventi origine sia all'interno che all'esterno dell'Unione. Gli sviluppi recenti, quali la globalizzazione, il maggiore ricorso all'esternalizzazione (outsourcing), le catene di approvvigionamento più lunghe e un uso più diffuso delle tecnologie dell'informazione e della comunicazione, contribuiscono ad aumentare il rischio di diffusione di tali pratiche. L'acquisizione, l'utilizzo o la divulgazione illeciti di un segreto commerciale compromettono la capacità dei legittimi detentori del segreto commerciale di ottenere i vantaggi derivanti dal loro ruolo di precursori grazie ai risultati dei propri sforzi in materia di innovazione. Senza strumenti giuridici di tutela del segreto commerciale efficaci e comparabili in tutta l'Unione, gli incentivi a intraprendere attività transfrontaliere innovative sul mercato interno risultano indeboliti e i segreti commerciali non sono in grado di mettere a frutto le loro potenzialità di motori della crescita economica e dell'occupazione. Pertanto, l'innovazione e la creatività sono scoraggiate e gli investimenti diminuiscono, incidendo in tal modo sul corretto funzionamento del mercato interno e mettendone a repentaglio le potenzialità di sostegno alla crescita. »

Il successivo considerando 18 stabilisce: «Inoltre dovrebbero ritenersi leciti ai fini della presente direttiva l'acquisizione, l'utilizzo o la divulgazione dei segreti commerciali quando imposti o consentiti dalla legge. Ciò riguarda, in particolare, l'acquisizione e la divulgazione dei segreti commerciali nel contesto dell'esercizio dei diritti all'informazione, alla consultazione e alla partecipazione da parte di rappresentanti dei lavoratori, in conformità del diritto e delle prassi

dell'Unione e nazionali, come pure la difesa collettiva degli interessi dei lavoratori e dei datori di lavoro, compresa la codeterminazione, e l'acquisizione o la divulgazione di un segreto commerciale nel contesto delle revisioni legali effettuate conformemente al diritto dell'Unione o al diritto nazionale. Tuttavia, tale fatto di considerare lecita l'acquisizione di un segreto commerciale non dovrebbe pregiudicare eventuali obblighi di riservatezza per quanto concerne il segreto commerciale o eventuali limitazioni al suo utilizzo, che il diritto dell'Unione o nazionale impongono al destinatario delle informazioni o al soggetto che le acquisisce. In particolare, la presente direttiva non dovrebbe esonerare le autorità pubbliche dagli obblighi di riservatezza cui sono soggette in relazione alle informazioni trasmesse dai detentori di segreti commerciali, a prescindere dal fatto che tali obblighi siano sanciti dal diritto dell'Unione o da quello nazionale. Tali obblighi di riservatezza includono, tra l'altro, gli obblighi connessi alle informazioni trasmesse alle amministrazioni aggiudicatrici nel contesto delle procedure di aggiudicazione, quali previsti, ad esempio, (...) dalla direttiva [2014/24]».

Ai sensi dell'articolo 1 della Direttiva 2016/943, intitolato «Oggetto e ambito di applicazione»:

«1. La presente direttiva stabilisce le norme relative alla tutela contro l'acquisizione, l'utilizzo e la divulgazione illeciti dei segreti commerciali.(...)»

2. La presente direttiva non pregiudica:(...) b)l'applicazione delle norme dell'Unione o nazionali che impongono al detentore del segreto commerciale di rivelare, per motivi di interesse pubblico, informazioni, compresi segreti commerciali, alle autorità pubbliche o amministrative o giudiziarie nell'espletamento delle loro funzioni; c)l'applicazione delle norme dell'Unione o nazionali che impongono o consentono alle istituzioni e agli organi dell'Unione o alle autorità pubbliche nazionali di divulgare informazioni fornite da imprese di cui tali istituzioni, organi o autorità dispongono in conformità e nel rispetto degli obblighi e delle prerogative stabiliti nel diritto dell'Unione o nel diritto nazionale(...)».

L'articolo 3 della suddetta direttiva, intitolato «Acquisizione, utilizzo e divulgazione leciti dei segreti commerciali», al suo paragrafo 2 così dispone:

«L'acquisizione, l'utilizzo o la divulgazione di un segreto commerciale sono da considerarsi leciti nella misura in cui siano richiesti o autorizzati dal diritto dell'Unione o dal diritto nazionale».

L'articolo 4 della medesima direttiva, rubricato «Acquisizione, utilizzo e divulgazione illeciti dei segreti commerciali», al paragrafo 2, lettera a), prevede:

«L'acquisizione di un segreto commerciale senza il consenso del detentore è da considerarsi illecita qualora compiuta in uno dei seguenti modi:

a)con l'accesso non autorizzato, appropriazione o la copia non autorizzate di documenti, oggetti, materiali, sostanze o file elettronici sottoposti al lecito controllo del detentore del segreto

commerciale, che contengono il segreto commerciale o dai quali il segreto commerciale può essere desunto».

L'articolo 9 della direttiva 2016/943, rubricato «Tutela della riservatezza dei segreti commerciali nel corso di procedimenti giudiziari», al suo paragrafo 2 così dispone:

«Gli Stati membri garantiscono inoltre che le competenti autorità giudiziarie possano, su richiesta debitamente motivata di una delle parti, adottare le misure specifiche necessarie a tutelare la riservatezza di qualunque segreto commerciale o presunto segreto commerciale utilizzato o menzionato nel corso dei procedimenti giudiziari concernenti l'acquisizione, l'utilizzo o la divulgazione illeciti di un segreto commerciale. Gli Stati membri possono inoltre consentire alle competenti autorità giudiziarie di adottare tali misure di propria iniziativa.

Le misure di cui al primo comma prevedono almeno la possibilità di:

- a) limitare l'accesso, totale o parziale, a qualsiasi documento contenente segreti commerciali o presunti segreti commerciali prodotto dalle parti o da terzi, ad un numero ristretto di persone;*
- b) limitare l'accesso alle udienze e alle relative registrazioni o trascrizioni, quando sussiste la possibilità di divulgazione di segreti commerciali o presunti segreti commerciali, ad un numero ristretto di persone;*
- c) rendere disponibili a qualsiasi persona diversa da quelle incluse nel numero ristretto di persone di cui alle lettere a) e b), le decisioni giudiziarie in una versione non riservata, nella quale i punti contenenti segreti commerciali siano stati eliminati o oscurati.*

Il numero di persone di cui al secondo comma, lettere a) e b), non è superiore a quanto necessario al fine di assicurare il rispetto del diritto delle parti del procedimento giudiziario a una tutela effettiva e a un processo equo e comprende almeno una persona fisica di ciascuna parte in causa, nonché i rispettivi avvocati o altri rappresentanti di tali parti del procedimento giudiziario.».

Tra le norme della direttiva in materia di appalti pubblici poste a sostegno di tale posizione di favore nei confronti della tutela dei segreti industriali e commerciali, la Corte di giustizia ha richiamato gli artt. 50, par. 4, e 55, par. 3, Dir. 2014/24/UE, ai sensi dei quali si prevede che le amministrazioni, che pur devono informare i concorrenti e pubblicare informazioni sull'esito delle procedure di selezione, possono non pubblicare informazioni la cui divulgazione ostacoli l'applicazione della legge, sia contraria all'interesse pubblico, pregiudichi i legittimi interessi commerciali di un particolare operatore economico, pubblico o privato oppure possa recare pregiudizio alla concorrenza leale tra operatori economici.

Sulla base di tale quadro normativo, la Corte di giustizia ha tratto la conclusione per cui il diritto di difesa non implica che le parti abbiano diritto di accesso illimitato e assoluto sicché esso può essere bilanciato con altri diritti e interessi, come appunto quello relativo al segreto commerciale, collegato

al diritto al rispetto della vita privata e delle comunicazioni di cui all'art. 7 della Carta di Nizza, e per questo qualificabile anch'esso di diritto fondamentale e di principio generale del diritto europeo. (Corte di giustizia UE, grande sezione, 7 settembre 2021, C-927/19).

Tale soluzione appare, del resto, rispettosa : (i) della libertà di iniziativa economica consentendo al privato di non sacrificare il proprio investimento quando ciò non appare indispensabile per consentire l'accesso difensivo ; (ii) del diritto di proprietà intellettuale, che ha una espressa protezione all'art. 17, par. 2, della Carta dei diritti fondamentali dell'UE; (iii) del il principio di proporzionalità e di necessità posti a base del necessario bilanciamento di interessi fondamentali contrapposti.

In conclusione, per le ragioni esposte, l'appello deve essere respinto, con conseguente conferma della ordinanza appellata. Va precisato che questa decisione riguarda unicamente la controversia relativa all'accesso, oggetto dell'ordinanza appellata, e che nessuna incidenza ha rispetto al giudizio relativo alla legittimità o meno dell'esclusione impugnata sulla quale questo Collegio non può, né deve, pronunciarsi.

La parziale novità delle questioni esaminate giustifica l'integrale compensazione delle spese di giudizio.

P.Q.M.

Il Consiglio di Stato in sede giurisdizionale, Sezione Quarta, definitivamente pronunciando sull'appello, come in epigrafe proposto, lo respinge nei sensi di cui in motivazione.

Compensa tra le parti integralmente le spese di questo grado di giudizio.

Ordina che la presente sentenza sia eseguita dall'autorità amministrativa.

Così deciso in Roma nella camera di consiglio del giorno 10 aprile 2025 con l'intervento dei magistrati:

Vincenzo Neri, Presidente

Michele Conforti, Consigliere

Luca Monteferrante, Consigliere

Luigi Furno, Consigliere, Estensore

Paolo Marotta, Consigliere