Raccolta della giurisprudenza

SENTENZA DEL TRIBUNALE (Sesta Sezione)

16 ottobre 2024*

«Politica estera e di sicurezza comune – Misure restrittive adottate in considerazione della situazione in Iran – Congelamento dei capitali – Elenco delle persone, delle entità e degli organismi cui si applica il congelamento dei capitali e delle risorse economiche – Inserimento del nome del ricorrente nell'elenco – Obbligo di motivazione – Diritti della difesa – Diritto a una tutela giurisdizionale effettiva – Proporzionalità – Sviamento di potere»

Nella causa T-201/23,

Communications Regulatory Authority (CRA), con sede in Teheran (Iran), rappresentata da T. Clay, T. Zahedi Vafa e K. Mehtiyeva, avvocati,

ricorrente,

contro

Consiglio dell'Unione europea, rappresentato da D. Laurent, P. Mahnič e S. Lejeune, in qualità di agenti,

convenuto,

IL TRIBUNALE (Sesta Sezione),

composto da M.J. Costeira, presidente, M. Kancheva (relatrice) e U. Öberg, giudici,

cancelliere: V. Di Bucci

vista la fase scritta del procedimento,

vista la mancata presentazione, ad opera delle parti, nel termine di tre settimane a decorrere dalla notifica della chiusura della fase scritta del procedimento, di una domanda di fissazione di un'udienza, e avendo deciso, in applicazione dell'articolo 106, paragrafo 3, del regolamento di procedura del Tribunale, di statuire senza fase orale,

ha pronunciato la seguente

* Lingua processuale: il francese.

Sentenza

1 Con il suo ricorso fondato sull'articolo 263 TFUE, la Communications Regulatory Authority (Autorità di regolamentazione delle comunicazioni, CRA), ricorrente, chiede l'annullamento del regolamento di esecuzione (UE) 2023/152 del Consiglio, del 23 gennaio 2023, che attua il regolamento (UE) n. 359/2011 concernente misure restrittive nei confronti di determinate persone, entità e organismi in considerazione della situazione in Iran (GU 2023, L 20 I, pag. 1; in prosieguo: il «regolamento impugnato»), nella parte in cui tale atto la riguarda.

Fatti

2 La ricorrente è un'istituzione governativa affiliata al Ministero iraniano delle Comunicazioni e delle Tecnologie dell'informazione (in prosieguo: il «Ministero delle Comunicazioni»), disciplinata ed organizzata dalla legge sulle funzioni e sui poteri di detto ministero, nonché dal proprio statuto. Secondo quest'ultimo, la ricorrente realizza in particolare gli obiettivi fissati dal Ministero delle Comunicazioni nel settore delle radiocomunicazioni ed esercita funzioni e poteri governativi, esecutivi e di supervisione di detto ministero. La principale attività della ricorrente è la regolamentazione, la gestione e il controllo dello spettro delle frequenze in Iran. La ricorrente è più specificamente incaricata di rilasciare le licenze di gestione di servizi di telecomunicazione e di monitorare le prestazioni dei loro titolari. La ricorrente svolge altresì un ruolo normativo proponendo alle autorità competenti norme nazionali relative alle comunicazioni nonché istruzioni e normative sulla interconnessione delle reti di telecomunicazione e delle reti informatiche relative alla sicurezza delle connessioni. La ricorrente svolge anche funzioni di tutela dei diritti degli utenti dei servizi di telecomunicazione e di rappresentanza della Repubblica islamica dell'Iran nelle associazioni regionali e internazionali del settore delle comunicazioni.

3 Il 21 marzo 2011, il Consiglio dell'Unione europea ha adottato conclusioni che indicavano che l'Unione europea era profondamente preoccupata per la situazione dei diritti umani che continuava a deteriorarsi in Iran. Il Consiglio ha attirato l'attenzione sulla sistematica repressione attuata nei confronti dei cittadini iraniani, che erano vittime di vessazioni e arresti poiché esercitavano i loro legittimi diritti alla libertà di espressione e di riunione pacifica. Inoltre, il Consiglio ha ivi affermato l'intenzione dell'Unione di affrontare gli abusi concernenti i diritti umani in Iran, anche attraverso la rapida introduzione di misure restrittive nei confronti dei responsabili di gravi violazioni in materia.

4 Il 12 aprile 2011 il Consiglio ha adottato la decisione 2011/235/PESC, concernente misure restrittive nei confronti di determinate persone ed entità in considerazione della situazione in Iran (GU 2011, L 100, pag. 51), che stabilisce una serie di misure restrittive dirette a persone che, in qualità di complici o responsabili, hanno ordinato o attuato gravi violazioni dei diritti umani.

5 La decisione 2011/235 è stata attuata con regolamento (UE) n. 359/2011 del Consiglio, del 12 aprile 2011, concernente misure restrittive nei confronti di determinate persone, entità e organismi in considerazione della situazione in Iran (GU 2011, L 100, pag. 1), adottato sulla base dell'articolo 215, paragrafo 2, TFUE.

6 L'articolo 2, paragrafi 1 e 2, del regolamento n. 359/2011 così dispone:

«1. Sono congelati tutti i fondi e le risorse economiche appartenenti, posseduti, detenuti o controllati dalle persone fisiche o giuridiche, le entità e gli organismi figuranti nell'allegato I.

2. Nessun fondo o risorsa economica è messo a disposizione, direttamente o indirettamente, delle persone fisiche o giuridiche, delle entità o degli organismi elencati nell'allegato I o utilizzato a loro beneficio».

7 Conformemente all'articolo 3, paragrafi 1 e 2, del regolamento n. 359/2011, le persone che il Consiglio ha identificato come responsabili di gravi violazioni dei diritti umani in Iran o le persone, le entità o gli organismi ad essi associati sono state inserite nell'elenco contenuto nell'allegato I. Tale elenco indica i motivi dell'inserimento.

8 L'articolo 12, paragrafi da 1 a 3, del regolamento n. 359/2011 così dispone:

«1. Qualora il Consiglio decida di applicare a una persona fisica o giuridica, a un'entità o a un organismo le misure di cui all'articolo 2, paragrafo 1, esso modifica di conseguenza l'allegato I.

2. Il Consiglio trasmette la sua decisione e i motivi dell'inserimento nell'elenco alla persona fisica o giuridica, all'entità o all'organismo (…) fornendo a tale persona, entità o organismo la possibilità di presentare osservazioni.

3. Qualora siano avanzate osservazioni o siano presentate nuove prove sostanziali, il Consiglio riesamina la decisione e ne informa opportunamente la persona fisica o giuridica, l'entità o l'organismo».

9 Il 16 settembre 2022, la sig.ra Mahsa Amini, una cittadina iraniana ventiduenne, è deceduta all'ospedale durante la sua detenzione da parte della polizia morale iraniana. Manifestazioni di ampia portata hanno seguito il suo decesso e sono state represse dalle autorità iraniane.

10 Il 25 settembre 2022, l'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza ha rilasciato una dichiarazione, a nome dell'Unione, nella quale deplorava il diffuso e sproporzionato ricorso alla forza da parte delle forze di sicurezza iraniane nei confronti di manifestanti non violenti. Nella dichiarazione ha inoltre dichiarato che i responsabili dell'uccisione di Mahsa Amini dovevano essere chiamati a risponderne e ha invitato le autorità iraniane a garantire indagini trasparenti e credibili per chiarire il numero di persone decedute e gli arresti, rilasciare tutti i manifestanti non violenti e garantire un giusto processo a tutte le persone detenute. Inoltre, esso ha sottolineato che la decisione dell'Iran di limitare drasticamente l'accesso a Internet e di bloccare le piattaforme di messaggistica istantanea violava palesemente la libertà di espressione. Infine, ha indicato che l'Unione avrebbe valutato tutte le opzioni disponibili per affrontare l'uccisione di Mahsa Amini e il modo in cui le forze di sicurezza iraniane avevano risposto alle successive manifestazioni.

11 Il 23 gennaio 2023, il Consiglio ha adottato la decisione di esecuzione (PESC) 2023/153, che attua la decisione 2011/235 (GU 2023, L 20 I, pag. 23). Il considerando 2 della decisione di esecuzione 2023/153 faceva riferimento alla dichiarazione dell'alto rappresentante dell'Unione per gli affari esteri nei termini ripresi al precedente punto 10. Il considerando 3 della medesima decisione precisava che, «[i]n tale contesto, e in linea con l'impegno dell'Unione [ad] affrontare con l'Iran tutte le questioni che desta[va]no preoccupazione, compresa la situazione dei diritti umani, 18

persone e 19 entità [avrebbero dovuto] essere inserite nell'elenco delle persone ed entità oggetto delle misure restrittive di cui all'allegato della decisione 2011/235». L'articolo 1 della decisione di esecuzione 2023/153 prevedeva che l'allegato della decisione 2011/235 fosse modificato conformemente al suo allegato.

12 Al numero 15 dell'elenco delle entità contenuto nell'allegato della decisione di esecuzione 2023/153 erano inseriti, in particolare, il cognome della ricorrente nonché i motivi del suo inserimento nei seguenti termini:

«L'Autorità di regolamentazione delle comunicazioni (CRA) opera sotto l'autorità del ministero iraniano delle tecnologie dell'informazione e della comunicazione. La CRA esegue l'obbligo imposto dal governo iraniano di filtrare i contenuti Internet mediante uno spyware denominato SIAM.

Durante le proteste del 2022 la CRA ha utilizzato il proprio controllo dell'accesso a Internet e dei telefoni cellulari per localizzare i manifestanti e creare un quadro dettagliato delle attività dei dissidenti e dei manifestanti affinché le autorità se ne avvalessero a loro discrezione. La CRA è pertanto responsabile di aver sostenuto la repressione di dimostranti pacifici, giornalisti, difensori dei diritti umani, studenti e altre persone che rivendicano i propri diritti legittimi.

La CRA è pertanto responsabile di gravi violazioni dei diritti umani in Iran».

13 Lo stesso giorno, il Consiglio ha adottato il regolamento impugnato sulla base dell'articolo 12, paragrafo 1, del regolamento n. 359/2011. I termini dei considerando 2 e 3 del regolamento impugnato sono identici a quelli dei considerando 2 e 3 della decisione di esecuzione 2023/153, ad eccezione della menzione dell'allegato I del regolamento n. 359/2011 in luogo dell'allegato della decisione 2011/235. L'articolo 1 del regolamento impugnato prevedeva che l'allegato I del regolamento n. 359/2011 fosse modificato conformemente al suo allegato.

14 Al numero 15 dell'elenco delle entità contenuto nell'allegato del regolamento impugnato erano inseriti, in particolare, il nome della ricorrente nonché i motivi di tale inserimento in termini identici a quelli menzionati al punto 12 *supra*.

15 Il 24 gennaio 2023 il Consiglio ha pubblicato nella *Gazzetta ufficiale dell'Unione europea* un avviso all'attenzione delle persone, entità e organismi cui si applicano le misure di cui alla decisione 2011/235, attuata dalla decisione di esecuzione 2023/153, e dal regolamento n. 359/2011, attuato dal regolamento impugnato (GU 2023, C 25, pag. 8).

16 Detto avviso precisava, in particolare, che il Consiglio aveva deciso che tali persone ed entità avrebbero dovuto essere incluse nell'elenco delle persone ed entità oggetto delle misure restrittive di cui alla decisione 2011/235 e al regolamento n. 359/2011 e che dette persone ed entità potevano presentargli, unitamente ai documenti giustificativi, una richiesta volta a ottenere il riesame della decisione che le includeva nell'elenco summenzionato. Ogni richiesta in tal senso doveva essere inviata entro il 15 febbraio 2023 agli estremi indicati nel medesimo avviso.

Conclusioni delle parti

17 La ricorrente chiede che il Tribunale voglia annullare il regolamento impugnato, nella parte in cui inserisce il suo nome nell'allegato I del regolamento n. 359/2011.

18 Il Consiglio chiede che il Tribunale voglia:

– respingere il ricorso;

– condannare la ricorrente alle spese del procedimento.

In diritto

19 A sostegno del suo ricorso, la ricorrente solleva quattro motivi. Il primo verte, in sostanza, su uno sviamento di potere; il secondo su una violazione dell'obbligo di motivazione e del diritto ad una tutela giurisdizionale effettiva; il terzo, in sostanza, sull'inesattezza materiale dei fatti ed il quarto su una violazione del principio di proporzionalità.

20 L'analisi di tali motivi di ricorso evidenzia che occorre esaminare, in un primo momento, il secondo motivo, relativo alla violazione dell'obbligo di motivazione e ad una violazione del diritto ad una tutela giurisdizionale effettiva; in un secondo momento, il terzo motivo, relativo ad un errore manifesto di valutazione dei fatti; in un terzo momento, il quarto motivo, relativo alla violazione del principio di proporzionalità; poi, in un quarto momento, il primo motivo, relativo a uno sviamento di potere.

Sul secondo motivo di ricorso, vertente su una violazione dell'obbligo di motivazione e su una violazione del diritto ad una tutela giurisdizionale effettiva

21 In primo luogo, la ricorrente sostiene che, poiché il Consiglio non ha comunicato, contemporaneamente all'adozione del regolamento impugnato o immediatamente dopo tale adozione, le informazioni o gli elementi di prova alla base dell'inserimento del suo nome nell'elenco di cui all'allegato I del regolamento n. 359/2011, esso non avrebbe adempiuto il suo obbligo di dimostrare la fondatezza di detti motivi e, di conseguenza, avrebbe violato il suo obbligo di motivazione.

22 In secondo luogo, la ricorrente sostiene che la motivazione del regolamento impugnato, nella parte in cui la concerne, consiste in una motivazione stereotipata composta da tre paragrafi succinti di quindici righe, in cui il Consiglio riassume le sue supposizioni fondate sulla natura pubblica della ricorrente. Una tale motivazione non sarebbe conforme alla giurisprudenza secondo cui la motivazione di un atto deve consentire, da un lato, alla persona interessata dall'atto controverso di contestarne la validità dinanzi al giudice con piena cognizione di causa in merito al fatto che le viene addebitato e, dall'altro, al giudice di esercitare il suo controllo giurisdizionale sull'atto contestato. Secondo la ricorrente, l'obbligo di motivazione non può essere attenuato sulla base del contesto politico nel quale una misura è adottata, tanto più che la contestualizzazione non consente alla ricorrente di comprendere la portata delle misure restrittive adottate nei suoi confronti e, correlativamente, al giudice di operare il controllo sulla misura in questione. Il Consiglio non potrebbe dunque violare il suo obbligo di motivazione «rifugiandosi» dietro considerazioni attinenti agli interessi di sicurezza e di politica estera.

23 In terzo luogo, nella replica, la ricorrente contesta, sulla base degli articoli 47 e 48 della Carta dei diritti fondamentali dell'Unione europea (in prosieguo: la «Carta»), la ricevibilità del documento prodotto dal Consiglio dinanzi al Tribunale quale elemento di prova a sostegno dei motivi

invocati per giustificare l'inserimento del suo nome nell'allegato I del regolamento n. 359/2011. Essa contesta altresì la pertinenza e l'efficacia probatoria delle informazioni contenute in detto documento.

24 Il Consiglio contesta gli argomenti della ricorrente.

25 Occorre ricordare che, secondo costante giurisprudenza, l'obbligo di motivare un atto pregiudizievole, che costituisce un corollario del principio del rispetto dei diritti della difesa, ha lo scopo, da un lato, di fornire all'interessato indicazioni sufficienti per giudicare se l'atto sia fondato oppure se sia eventualmente inficiato da un vizio che consente di contestarne la validità dinanzi al giudice dell'Unione e, dall'altro, di consentire a quest'ultimo di esercitare il suo controllo di legittimità dell'atto stesso (v. sentenza del 15 novembre 2012, Consiglio/Bamba (C-417/11 P, EU:C:2012:718, punto 49 e giurisprudenza citata).

26 Occorre altresì ricordare che la motivazione richiesta dall'articolo 296 TFUE e dall'articolo 41, paragrafo 2, lettera c), della Carta dev'essere adeguata alla natura dell'atto di cui trattasi e al contesto nel quale è stato adottato. L'obbligo di motivazione deve essere valutato in funzione delle circostanze del caso, in particolare del contenuto dell'atto, della natura dei motivi esposti e dell'interesse che i destinatari dell'atto o altre persone da questo colpite direttamente e individualmente possano avere a ricevere spiegazioni. La motivazione non deve necessariamente specificare tutti gli elementi di fatto e di diritto pertinenti, in quanto l'adeguatezza della motivazione dev'essere valutata alla luce non solo del suo tenore, ma anche del suo contesto e del complesso delle norme giuridiche che disciplinano la materia di cui trattasi (v. sentenza del 17 settembre 2020, Rosneft e a./Consiglio, C-732/18 P, non pubblicata, EU:C:2020:727, punto 77 e giurisprudenza ivi citata; sentenza del 27 luglio 2022, RT France/Consiglio, T-125/22, EU:T:2022:483, punto 103).

27 Infatti, da una parte, un atto pregiudizievole è sufficientemente motivato quando è stato emanato in un contesto noto all'interessato, che gli consente di comprendere la portata del provvedimento adottato nei suoi confronti. (v. sentenza del 17 settembre 2020, Rosneft e a./Consiglio (C-732/18 P, non pubblicata, EU:C:2020:727, punto 78 e la giurisprudenza ivi citata). Dall'altra, il grado di precisione della motivazione di un atto dev'essere proporzionato alle possibilità materiali e alle condizioni tecniche o al tempo disponibile per la sua adozione (v. sentenza del 27 luglio 2022, RT France/Consiglio, T-125/22, EU:T:2022:483, punto 104 e giurisprudenza ivi citata).

28 Inoltre, la giurisprudenza ha precisato che la motivazione di un atto del Consiglio che impone una misura restrittiva deve identificare non soltanto la base giuridica di tale misura, ma anche i motivi specifici e concreti per i quali il Consiglio ritiene, nell'esercizio del suo potere discrezionale, che l'interessato debba essere assoggettato a una misura di questo tipo (v. sentenza del 27 luglio 2022, RT France/Consiglio, T-125/22, EU:T:2022:483, punto 105 e giurisprudenza ivi citata).

29 Infine, si deve rammentare che l'obbligo di motivare un atto costituisce una forma sostanziale che dev'essere distinta dalla questione della fondatezza dei motivi, questione che ricade nella legalità sostanziale dell'atto controverso. Infatti, la motivazione di un atto consiste nell'esprimere formalmente le ragioni su cui si fonda tale atto. Qualora tali ragioni siano viziate da errori, questi ultimi inficiano la legalità sostanziale della decisione, ma non la sua motivazione, che può essere sufficiente pur illustrando ragioni errate. (v., in tal senso, sentenza del 13 settembre 2013, Makhlouf/Consiglio, T-383/11, EU:T:2013:431, punti 73 e 74 e giurisprudenza ivi citata).

30 Nel caso di specie, per quanto riguarda il contesto in cui il nome della ricorrente è stato inserito nell'allegato I del regolamento n. 359/2011, occorre rilevare che, come giustamente sottolineato dal Consiglio, il considerando 2 del regolamento impugnato faceva riferimento alla dichiarazione resa il 25 settembre 2022 a nome dell'Unione da parte dell'alto rappresentante dell'Unione, i cui termini sono richiamati al precedente 10 *supra*.

31 Inoltre, come indicato al punto 11 *supra*, il considerando 3 del regolamento impugnato precisa che sono il contesto ricordato al punto 10 *supra* e l'impegno dell'Unione ad affrontare con l'Iran tutte le questioni che destavano preoccupazione, compresa la situazione dei diritti umani, ad aver giustificato in particolare l'inserimento di diciannove entità, tra cui la ricorrente, nell'elenco delle persone fisiche e giuridiche, delle entità e degli organismi oggetto di misure restrittive contenuto nell'allegato I del regolamento n. 359/2011.

32 In particolare, le ragioni per le quali il nome della ricorrente è stato inserito nell'allegato I del regolamento n. 359/2011 erano enunciate nell'allegato del regolamento impugnato nei termini ricordati al punto 12 *supra*.

33 È giocoforza constatare che tali motivi, letti alla luce degli elementi contestuali ricordati ai considerando 2 e 3 del regolamento impugnato, esponevano in modo sufficientemente specifico e concreto le ragioni per le quali il Consiglio riteneva, nell'esercizio del suo potere discrezionale di valutazione, che la ricorrente dovesse essere oggetto di una misura restrittiva.

34 Risulta infatti dalla motivazione del regolamento impugnato che la ricorrente era considerata responsabile di gravi violazioni dei diritti umani in Iran per aver eseguito l'obbligo imposto dal governo iraniano di filtrare i contenuti Internet mediante uno spyware denominato SIAM e per avere, in particolare, utilizzato, in occasione delle manifestazioni del 2022 successive alla morte di Mahsa Amini, il proprio controllo dell'accesso a Internet e dei telefoni cellulari per localizzare i manifestanti e creare un quadro dettagliato delle attività dei dissidenti e dei manifestanti, di cui le autorità si sono avvalse a loro discrezione, sostenendo in tal modo la repressione esercitata da parte di dette autorità su manifestanti che rivendicavano i propri diritti legittimi.

35 Inoltre, occorre respingere l'argomento della ricorrente secondo cui il Consiglio è venuto meno al suo obbligo di motivazione in quanto non le ha trasmesso contemporaneamente all'adozione del regolamento impugnato o immediatamente dopo tale adozione gli elementi di prova sui quali si fondano i motivi invocati per giustificare il suo inserimento nell'allegato I del regolamento n. 359/2011 e, pertanto, non ha dimostrato la fondatezza di detti motivi.

36 Infatti, da un lato, nei limiti in cui, con tale argomento, la ricorrente intende sostenere che il Consiglio non ha fornito la prova della fondatezza dei motivi invocati nel regolamento impugnato per giustificare la sua iscrizione nell'allegato I del regolamento n. 359/2011, occorre rilevare che, conformemente alla giurisprudenza richiamata al punto 29 *supra*, tale questione deve essere distinta da quella della motivazione del regolamento impugnato, che riguarda la legalità esterna di detto regolamento.

37 Dall'altro lato, nei limiti in cui, con il medesimo argomento, la ricorrente intende sostenere che il Consiglio ha violato i suoi diritti della difesa in quanto era tenuto a fornirle d'ufficio l'accesso agli elementi del suo fascicolo, occorre rilevare che il regolamento impugnato è stato notificato alla ricorrente mediante un avviso pubblicato nella Gazzetta ufficiale il 24 gennaio 2023, che invitava

le persone e le entità interessate a presentare una richiesta di riesame al Consiglio entro il 15 febbraio 2023 e che la ricorrente non ha formulato una tale richiesta, né ha chiesto al Consiglio l'accesso al suo fascicolo al di fuori del presente procedimento.

38 Orbene, occorre ricordare che, nel caso di un inserimento iniziale in un elenco di persone ed entità sottoposte a misure restrittive, quando informazioni sufficientemente precise, che permettano all'entità interessata di far conoscere utilmente il suo punto di vista sugli elementi ritenuti a suo carico da parte del Consiglio, sono state comunicate, il principio del rispetto dei diritti della difesa non implica per quest'ultimo l'obbligo di concedere spontaneamente l'accesso ai documenti contenuti nel suo fascicolo. Soltanto su richiesta della parte interessata il Consiglio è tenuto a consentire l'accesso a tutti i documenti amministrativi non riservati relativi alla misura di cui trattasi. La comunicazione spontanea degli elementi del fascicolo costituirebbe infatti una condizione eccessiva, dato che, al momento dell'adozione di una misura di congelamento dei capitali, non è certo che l'entità interessata voglia verificare, tramite l'accesso al fascicolo, gli elementi di fatto sottesi alle affermazioni formulate a suo carico dal Consiglio (sentenze del 14 ottobre 2009, Bank Melli Iran/Consiglio, T-390/08, EU:T:2009:401, punto 97, e del 16 settembre 2013, Bank Kargoshaei e a./Consiglio, T-8/11, non pubblicata, EU:T:2013:470, punto 68).

39 Nel caso di specie, da quanto precede risulta che, con la motivazione del regolamento impugnato, la ricorrente disponeva di informazioni sufficientemente precise per consentirle di far conoscere il suo punto di vista sugli elementi posti a suo carico dal Consiglio. Pertanto, quest'ultimo non era tenuto a comunicare d'ufficio alla ricorrente gli elementi contenuti nel suo fascicolo.

40 Occorre altresì sottolineare che gli argomenti della ricorrente relativi alla ricevibilità del documento prodotto nell'allegato B.11 e al carattere probatorio delle informazioni in esso contenute riguardano la fondatezza dei motivi invocati per giustificare l'inserimento del suo nome nell'allegato I del regolamento n. 359/2011 e sono quindi irrilevanti per quanto riguarda il motivo di ricorso vertente sulla asserita violazione dell'obbligo di motivazione. Tali argomenti saranno quindi esaminati congiuntamente agli argomenti analoghi presentati dalla ricorrente nell'ambito del terzo motivo di ricorso, vertente su un errore manifesto di valutazione.

41 Di conseguenza, occorre respingere il secondo motivo di ricorso in quanto infondato.

Sul terzo motivo di ricorso, vertente sull'inesattezza materiale dei fatti

42 La ricorrente sostiene che il regolamento impugnato è viziato, nella parte in cui la riguarda, da un «errore manifesto di valutazione dei fatti» in quanto, da un lato, essa non ha la capacità giuridica di compiere i fatti che le sono addebitati dal Consiglio e, dall'altro, non ha neppure le capacità tecniche di seguire le tracce o di creare un «quadro dettagliato» delle attività dei manifestanti.

43 Infatti, in primo luogo, la ricorrente sostiene che il suo statuto non l'autorizza ad effettuare una sorveglianza di massa della popolazione e ancor meno a «tracciare» i manifestanti. Conformemente al suo statuto, la ricorrente svolgerebbe un ruolo di regolatore, di moderatore o ancora di rappresentante dell'Iran. Inoltre, la ricorrente sottolinea che, quandanche essa intendesse predisporre un filtraggio, essa non potrebbe farlo, poiché una tale prassi è giuridicamente vincolata. Infatti, contrariamente a quanto sostenuto dal Consiglio, in Iran la raccolta di dati sarebbe disciplinata da numerosi testi giuridici, in particolare dall'articolo 25 della Costituzione, dall'articolo 582 del codice penale iraniano, integrato dalla «legge sui cyber reati» del 26 maggio 2009, e dagli articoli 104 e 150 del codice di procedura penale iraniano. Tale

inquadramento normativo sarebbe conforme alla risoluzione del Consiglio del 17 gennaio 1995 sull'intercettazione legale delle telecomunicazioni (GU 1996, C 329, pag. 1). Inoltre, da due relazioni realizzate da una società di telecomunicazioni risulterebbe che, contrariamente a quanto affermato dal Consiglio, le domande della ricorrente non vanno al di là dei requisiti tradizionali in materia di intercettazione legale.

44 Peraltro, la ricorrente sostiene che occorre distinguere la sorveglianza di massa dalla sorveglianza individuale delle persone. Secondo la ricorrente, la sorveglianza di massa può essere necessaria in qualsiasi società al fine di mantenere la pace e l'ordine pubblico, in particolare sorvegliando il flusso delle persone e l'assembramento delle masse. Ciò consentirebbe di prevenire, in occasione di manifestazioni pubbliche, qualsiasi disordine derivante dall'affollamento. Ogni Stato sovrano disporrebbe di tale potere di sorveglianza e dall'esercizio di tale potere non si potrebbe desumere che siano commesse violazioni di diritti umani individuali. Tale potere di sorveglianza costituirebbe una prerogativa dei pubblici poteri riconosciuta in particolare dalla Corte europea dei diritti dell'uomo.

45 In secondo luogo, secondo la ricorrente, il software da essa utilizzato, denominato «SIAM» o «Samaneh yekparche Estehlamate Mokhaberati» in persiano, non dispone di funzioni che consentano di sorvegliare collettivamente o individualmente i manifestanti sul territorio iraniano.

46 La ricorrente sostiene che il software SIAM costituisce un'interfaccia di programmazione di applicazioni (API), ossia un dispositivo che funge da ponte e che permette ad un cliente esterno ad un'entità di utilizzare delle API interne ed i loro servizi. In Iran, la Mezzaluna Rossa, le ambulanze, i vigili del fuoco e le organizzazioni operanti nel settore delle strade e della gestione delle crisi utilizzerebbero tale software. Pertanto, secondo la ricorrente, il software SIAM sarebbe utilizzato dai call center, in particolare quando interpellati dai servizi di emergenza. I call center utilizzerebbero tale software per contattare gli operatori di telefonia mobile che fornirebbero poi una localizzazione solamente approssimativa della persona che si trova in una situazione di pericolo.

47 Peraltro, la ricorrente sottolinea che essa non può comunicare direttamente alle autorità di polizia e alle autorità giudiziarie informazioni relative agli utenti di servizi di comunicazione, poiché tali informazioni sarebbero conservate dagli operatori titolari di una licenza di gestione della rete.

48 La ricorrente contesta, infine, gli argomenti dedotti dal Consiglio nel suo controricorso riguardanti i presunti «componenti funzionali» del sistema di intercettazione dell'Iran.

49 Infatti, la ricorrente sostiene che il Consiglio travisa le funzionalità del software SIAM, «Force2GNumber», «LocationCustomerList», «GetCDR», «GetIPDR» e «ApplySusplp», alle quali fa riferimento nel controricorso. La ricorrente spiega che la descrizione di tali funzioni da parte del Consiglio, che si basa unicamente sull'articolo del giornale d'indagine online *The Intercept*, non corrisponde alla realtà. Secondo la ricorrente, si tratta dei comandi classici e ordinari a disposizione di un organo statale di regolamentazione delle telecomunicazioni e tutti gli Stati membri dell'Unione dispongono di strumenti analoghi. Lo stesso varrebbe per quanto riguarda i sistemi «Legal Intercept» (LI), «Control Illegal Devices» (CID), «SHAHKAR» e «SHAMSA».

50 Inoltre, nella replica, la ricorrente contesta la ricevibilità dell'articolo intitolato «Hacked documents: How Iran track and control protesters phones», pubblicato il 28 ottobre 2022 da *The Intercept*, prodotto dal Consiglio nell'allegato B.11 (in prosieguo: «l'articolo di *The Intercept*»).

Secondo la ricorrente, i fatti addotti in tale articolo si basano su una serie di documenti interni di un operatore mobile iraniano che non sono stati acquisiti al procedimento dinanzi al Tribunale e il Consiglio si limita ad affermare che gli autori di tale articolo avrebbero avuto accesso a documenti che sarebbero stati loro comunicati «da una persona che ha [asseritamente] piratato un operatore mobile iraniano». Tale articolo, che costituirebbe il documento chiave del fascicolo del Consiglio, non sarebbe quindi altro che una prova per sentito dire. Orbene, conformemente alla giurisprudenza della Corte relativa agli articoli 47 e 48 della Carta, nonché alla giurisprudenza della Corte europea dei diritti dell'uomo relativa all'articolo 6 della Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, firmata a Roma il 4 novembre 1950, le deposizioni di testimoni poi assenti all'udienza, che non possono essere esaminate dalla parte avversa, sono in linea di principio vietate, salvo quando l'accusa giustifica sufficientemente la necessità di utilizzare le loro testimonianze e all'imputato sono concesse altre garanzie procedurali, nonché quando esistono altre prove a suo carico. La Corte avrebbe altresì dichiarato, nella sentenza dell'8 dicembre 2022, HYA e a. (Impossibilità di interrogare i testimoni a carico) (C-348/21, EU:C:2022:965), che, in caso di impossibilità di esaminare i testimoni a carico, l'efficacia probatoria delle loro testimonianze deve essere relativizzata anche se tali testimonianze sono ricevibili.

51 Ne conseguirebbe che, fondando il regolamento impugnato sulle presunte affermazioni di una persona sconosciuta, il Consiglio avrebbe agito in violazione degli articoli 47 e 48 della Carta, il che imporrebbe di respingere tale offerta di prova in quanto irricevibile.

52 La ricorrente sostiene altresì nella replica che, in forza del principio del contraddittorio, il giudice può prendere in considerazione solo gli atti processuali e i documenti di cui le parti hanno potuto prendere conoscenza e sui quali hanno potuto pronunciarsi. Orbene, lo stesso Consiglio avrebbe riconosciuto che l'operatore mobile iraniano citato nell'articolo di *The Intercept* non ha risposto all'invito dei giornalisti a formulare osservazioni.

53 Il Consiglio contesta l'argomento della ricorrente.

54 Occorre rilevare che, nell'ambito del terzo motivo di ricorso, la ricorrente contesta la fondatezza dei motivi invocati per giustificare il suo inserimento nell'allegato I del regolamento n. 359/2011. Essa sostiene infatti di non avere né la capacità giuridica né la capacità tecnica di svolgere le attività addebitatele.

55 Tuttavia, occorre inoltre osservare che, come risulta dal punto 23 *supra*, nell'ambito del secondo motivo di ricorso, la ricorrente contesta al Consiglio di aver violato gli articoli 47 e 48 della Carta e di aver invertito l'onere della prova, fondando la sua valutazione sull'articolo di *The Intercept*, dal momento che, siccome i documenti menzionati in tale pubblicazione non sono stati acclusi al fascicolo del presente procedimento, i fatti e le dichiarazioni riportati in tale articolo costituiscono mere allegazioni rispetto alle quali la ricorrente si trova privata della possibilità di esercitare i suoi diritti della difesa. La ricorrente sostiene inoltre nella replica che il mancato inserimento di elementi di prova nel fascicolo nell'ambito del presente procedimento viola il principio del contraddittorio di cui all'articolo 85, paragrafo 1, del regolamento di procedura del Tribunale. La ricorrente sottolinea, inoltre, l'assenza di valore probatorio di una tale pubblicazione.

56 Occorre esaminare gli argomenti della ricorrente vertenti sulla violazione degli articoli 47 e 48 della Carta nonché sulla violazione del principio del contraddittorio prima di esaminare quelli riguardanti il valore probatorio dell'articolo di *The Intercept*, e successivamente gli argomenti relativi ad un «errore manifesto di valutazione dei fatti».

Sulla violazione degli articoli 47 e 48 della Carta e del principio del contraddittorio

57 Anzitutto, occorre respingere l'argomento della ricorrente secondo cui l'articolo di *The Intercept* prodotto dal Consiglio nell'allegato B.11 del controricorso dovrebbe essere respinto in quanto irricevibile per il motivo che, in sostanza, non le sarebbe possibile difendersi contro semplici allegazioni, il che lederebbe i suoi diritti della difesa dinanzi al Tribunale.

58 Occorre rilevare che la questione della ricevibilità dei mezzi di prova dinanzi al Tribunale, disciplinata dall'articolo 85 del regolamento di procedura, deve essere distinta dalla questione della valutazione delle prove da parte del giudice dell'Unione.

59 A tal riguardo, occorre ricordare che, secondo la giurisprudenza della Corte, in sede di controllo delle misure restrittive, i giudici dell'Unione devono garantire un controllo, in linea di principio completo, della legittimità di tutti gli atti dell'Unione con riferimento ai diritti fondamentali che costituiscono parte integrante dell'ordinamento giuridico dell'Unione (v., in tal senso, sentenze del 18 luglio 2013, Commissione e a./Kadi, C-584/10 P, C-593/10 P e C-595/10 P, EU:C:2013:518, punto 97; del 28 novembre 2013, Consiglio/Fulmen e Mahmoudian, C-280/12 P, EU:C:2013:775, punto 58, e del 28 marzo 2017, Rosneft, C-72/15, EU:C:2017:236, punto 106).

60 Nel novero di tali diritti fondamentali figurano, in particolare, il rispetto dei diritti della difesa e il diritto ad una tutela giurisdizionale effettiva (v. sentenza del 28 novembre 2013, Consiglio/Fulmen e Mahmoudian, C-280/12 P, EU:C:2013:775, punto 59 e giurisprudenza ivi citata; sentenza del 28 novembre 2013, Consiglio/Manufacturing Support & Procurement Kala Naft, C-348/12 P, EU:C:2013:776, punto 66).

61 L'effettività del controllo giurisdizionale garantito dall'articolo 47 della Carta postula che, nello svolgere il controllo della legittimità della motivazione su cui si basa la decisione di inserire o di mantenere il nominativo di una persona o di un'entità nell'elenco delle persone sottoposte a misure restrittive, il giudice dell'Unione si assicuri che tale decisione, la quale riveste una portata individuale per detta persona o entità, si fondi su una base di fatto sufficientemente solida. Ciò comporta una verifica dei fatti addotti nell'esposizione dei motivi sottesa a tale decisione, cosicché il controllo giurisdizionale non si limiti alla valutazione dell'astratta verosimiglianza dei motivi dedotti, ma consista invece nell'accertare se questi motivi, o per lo meno uno di essi considerato di per sé sufficiente a suffragare detti atti, siano fondati (v., in tal senso, sentenze del 18 luglio 2013, Commissione e a./Kadi, C-584/10 P, C-593/10 P e C-595/10 P, EU:C:2013:518, punto 119; del 18 giugno 2015, Ipatau/Consiglio, C-535/14 P, EU:C:2015:407, punto 42, e del 18 febbraio 2016, Consiglio/Bank Mellat, C-176/13 P, EU:C:2016:96, punto 109).

62 In tale contesto, è infatti all'autorità competente dell'Unione che incombe, in caso di contestazione, il compito di dimostrare la fondatezza dei motivi posti a carico della persona o dell'entità interessata, e non già a queste ultime di produrre la prova negativa dell'infondatezza di tali motivi (v., in tal senso, sentenza del 18 luglio 2013, Commissione e a./Kadi, C-584/10 P, C-593/10 P e C-595/10 P, EU:C:2013:518, punto 121).

63 Tuttavia, contrariamente a quanto sostiene la ricorrente, non ne consegue che l'asserita incapacità del Consiglio di fornire la prova che i motivi invocati per giustificare l'inserimento del nome della ricorrente nell'allegato I del regolamento n. 359/2011, anche supponendola dimostrata, lederebbe i diritti della difesa della ricorrente.

64 Infatti, come risulta dalla giurisprudenza richiamata al punto 61 *supra*, è al contrario perché la salvaguardia dell'effettività dell'articolo 47 della Carta lo esige che il giudice dell'Unione è tenuto a verificare, nell'ambito del controllo di legittimità delle misure restrittive, la fondatezza dei motivi sottesi a tali misure e, pertanto, il valore probatorio dei documenti prodotti, nel caso di specie, dal Consiglio.

65 Occorre poi respingere in quanto non pertinenti nel caso di specie le considerazioni, invocate dalla ricorrente, esposte nella sentenza dell'8 dicembre 2022, HYA e a. (Impossibilità di interrogare i testimoni a carico) (C-348/21, EU:C:2022:965), nella quale la Corte era stata interrogata in merito all'interpretazione dell'articolo 6, paragrafo 1, e dell'articolo 8, paragrafo 1, della direttiva (UE) 2016/343 del Parlamento europeo e del Consiglio, del 9 marzo 2016, sul rafforzamento di alcuni aspetti della presunzione di innocenza e del diritto di presenziare al processo nei procedimenti penali (GU 2016, L 65, pag. 1), nonché dell'articolo 47, secondo comma, della Carta.

66 Si deve ricordare che il principio della presunzione di innocenza, enunciato all'articolo 6, paragrafo 2, della Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e all'articolo 48, paragrafo 1, della Carta, costituisce un diritto fondamentale che conferisce ai singoli o alle entità dirette da singoli diritti di cui il giudice dell'Unione garantisce il rispetto (v. sentenza del 18 maggio 2017, Makhlouf/Consiglio, T-410/16, non pubblicata, EU:T:2017:349, punto 122 e giurisprudenza ivi citata).

67 Il principio della presunzione di innocenza, il quale esige che ogni persona accusata di un reato sia presunta innocente fino a quando la sua colpevolezza non sia stata legalmente accertata, non osta all'adozione di misure cautelari di congelamento di capitali, dal momento che queste ultime non hanno ad oggetto l'avvio di un procedimento penale a carico della persona o dell'entità interessata. Tuttavia, tenuto conto della loro gravità, tali misure devono essere previste dalla legge, essere adottate da un'autorità competente e presentare un carattere limitato nel tempo. Dal punto 13 *supra* risulta che i primi due criteri sono soddisfatti. Inoltre, per quanto riguarda il carattere limitato nel tempo, occorre constatare che, conformemente all'articolo 12, paragrafi 3 e 4, del regolamento n. 359/2011, l'allegato I del medesimo regolamento è riesaminato periodicamente e almeno ogni dodici mesi, potendo l'inserimento di una persona o di un'entità in detto allegato essere eventualmente prorogato o modificato. Le misure imposte alla ricorrente hanno dunque effettivamente un carattere limitato nel tempo. (v., in tal senso, sentenza del 18 maggio 2017, Makhlouf/Consiglio, T-410/16, non pubblicata, EU:T:2017:349, punto 123 e giurisprudenza ivi citata).

68 Inoltre, occorre rilevare che le misure restrittive di cui trattasi non comportano una confisca dei beni della ricorrente in quanto proventi di reato, bensì un congelamento a titolo cautelare. Tali misure non costituiscono quindi una sanzione e non implicano peraltro alcuna accusa di tale natura (v. sentenza del 18 maggio 2017, Makhlouf/Consiglio, T-410/16, non pubblicata, EU:T:2017:349, punto 124 e giurisprudenza ivi citata).

69 Infatti, il regolamento impugnato, nella parte in cui riguarda la ricorrente, non contiene la constatazione del fatto che un reato sia stato effettivamente commesso, essendo stato adottato, piuttosto, nel contesto e ai fini di una procedura di natura amministrativa che persegue una funzione cautelare e mira unicamente a consentire al Consiglio di garantire la tutela delle popolazioni civili (v., in tal senso, sentenza del 18 maggio 2017, Makhlouf/Consiglio, T-410/16, non pubblicata, EU:T:2017:349, punto 125 e giurisprudenza ivi citata).

70 Infine, occorre ugualmente respingere l'argomento della ricorrente secondo cui, poiché i documenti menzionati nell'articolo di *The Intercept* non sono stati inseriti nel fascicolo della presente causa, tale articolo dovrebbe essere escluso in quanto irricevibile per il motivo che, in forza del principio del contraddittorio, il giudice può prendere in considerazione solo gli atti processuali e gli atti di cui le parti hanno potuto prendere conoscenza e sui quali esse hanno potuto pronunciarsi. Infatti, è sufficiente rilevare al riguardo che la ricorrente ha avuto occasione di prendere posizione nella sua replica sugli elementi di prova prodotti dal Consiglio nell'allegato B.11, in particolare su tale articolo, di cui essa del resto contesta il valore probatorio.

71 Peraltro, occorre rilevare che i due manuali d'uso del software SIAM redatti, il primo, in persiano e, il secondo, in inglese erano consultabili direttamente a partire dall'articolo di *The Intercept* tramite un collegamento ipertestuale contenuto a pagina 3 del fascicolo WK 307/2023 INIT prodotto dal Consiglio nell'allegato B.11 del controricorso.

72 Occorre quindi respingere le censure della ricorrente vertenti sulla violazione degli articoli 47 e 48 della Carta e del principio del contraddittorio.

Sul valore probatorio dell'articolo di The Intercept

73 La ricorrente contesta all'articolo di *The Intercept* di essere una semplice pubblicazione giornalistica contenente unicamente allegazioni non verificabili e di essere, pertanto, privo di qualsiasi efficacia probatoria.

74 A tale riguardo, occorre ricordare che, conformemente a una giurisprudenza costante, per l'attività della Corte e del Tribunale vale il principio della libera valutazione delle prove e soltanto l'attendibilità delle prove prodotte è decisiva per la valutazione delle stesse. Inoltre, per valutare l'efficacia probatoria di un documento si deve verificare la verosimiglianza dell'informazione in esso contenuta e considerare, in particolare, la provenienza del documento, le circostanze in cui esso è stato elaborato, il suo destinatario e chiedersi se, in base al suo contenuto, esso appaia ragionevole e affidabile (v. sentenza del 31 maggio 2018, Kaddour/Consiglio, T-461/16, EU:T:2018:316, punto 107 e giurisprudenza ivi citata).

75 In assenza di poteri di indagine in paesi terzi, la valutazione delle autorità dell'Unione deve, di fatto, basarsi su fonti di informazione accessibili al pubblico, come rapporti, articoli di stampa, relazioni dei servizi segreti o altre fonti di informazione simili (sentenze del 14 marzo 2018, Kim e a./Consiglio e Commissione, T-533/15 e T-264/16, EU:T:2018:138, punto 107, e del 1º giugno 2022, Prigozhin/Consiglio, T-723/20, non pubblicata, EU:T:2022:317, punto 59).

76 Infatti, sarebbe eccessivo e sproporzionato richiedere al Consiglio di condurre esso stesso indagini sul campo riguardanti la veridicità dei fatti che sono riportati da numerosi media (sentenza del 25 gennaio 2017, Almaz-Antey Air and Space Defence/Consiglio, T-255/15, non pubblicata, EU:T:2017:25, punto 148).

77 Articoli di stampa possono quindi essere utilizzati per corroborare l'esistenza di taluni fatti quando provengono da più fonti diverse e sono sufficientemente concreti, precisi e concordanti quanto ai fatti ivi descritti (v. sentenza dell'11 settembre 2019, Topor-Gilka e WO Technopromexport/Consiglio, T-721/17 e T-722/17, non pubblicata, EU:T:2019:579, punto 137 e giurisprudenza ivi citata).

78 Nel caso di specie, il Consiglio ha fondato l'inserimento del nome della ricorrente nell'allegato I del regolamento n. 359/2011 su quattro documenti del fascicolo WK 307/2023 INIT che figurano nell'allegato B.11 del controricorso.

79 Si tratta, in primo luogo, dell'articolo di *The Intercept*; in secondo luogo, dell'articolo intitolato «Hacker Leaks Manuals Showing How Iran Uses Mobile Networks to Track Protesters», pubblicato il 31 ottobre 2022 dal sito Internet specializzato Commrisk; in terzo luogo, dell'articolo intitolato «Iran: New tactics for digital repression as protests continue», pubblicato il 17 novembre 2022 sul sito Internet dell'associazione ARTICLE 19; e, in quarto luogo, dell'articolo intitolato «Iran is using spyware to track citizens attending protests», pubblicato dal giornale di inchiesta online *The Tech Monitor* il 3 novembre 2022.

80 La ricorrente sostiene che il Consiglio ha fondato il regolamento impugnato, nella parte che la concerne, sulle sole allegazioni contenute nell'articolo di *The Intercept*, a loro volta fondate sulle affermazioni di una persona anonima.

81 Occorre rilevare che l'articolo di *The Intercept* rivela che, sulla base di documenti interni di un operatore di telefonia mobile iraniano, in particolare scambi di corrispondenza che coinvolgevano i dirigenti della ricorrente e due manuali, uno in inglese e l'altro in persiano, di utilizzo di un software denominato SIAM, gli autori di tale articolo hanno scoperto come le autorità iraniane, tramite la ricorrente, avevano istituito un sistema funzionante sullo sfondo delle reti mobili iraniane che consentiva al governo iraniano di aggirare il sistema di cifratura delle chiamate, seguire gli spostamenti di un utente telefonico, identificare tutti i telefoni situati in una determinata località, analizzare tutti i contatti di un utente telefonico e interrompere o rallentare la connessione Internet dell'utente, e che era stato utilizzato per reprimere e controllare la popolazione iraniana a seguito della morte di Mahsa Amini nel 2022. Tale articolo spiega altresì che il manuale d'uso del software SIAM redatto in inglese precisa che, «[s]econdo le norme e i regolamenti della [ricorrente], tutti gli operatori di telecomunicazioni devono fornire a [quest'ultima] un accesso diretto al loro sistema per interrogare (sic) le informazioni dei clienti e modificare i loro servizi attraverso il servizio web» e contiene, inoltre, informazioni tecniche sui comandi più potenti utilizzati dal software SIAM per raccogliere dati sugli utenti direttamente dagli operatori mobili iraniani.

82 Occorre altresì osservare che gli autori dell'articolo di *The Intercept* hanno avuto cura di interrogare due persone presentate come esperti.

83 A tal riguardo, occorre sottolineare che, contrariamente a quanto sostiene la ricorrente, la prima persona presentata come esperto non è «qualcuno che nessuno conosce e che non sembra disporre di alcuna legittimazione particolare». Risulta infatti dal fascicolo che tale prima persona è ricercatore presso il CitizenLab Canada, laboratorio interdisciplinare con sede all'Università di Toronto (Canada) specializzato in «ricerca, sviluppo, politica strategica di alto livello e impegno giuridico all'intersezione delle tecnologie dell'informazione e della comunicazione, dei diritti dell'uomo e della sicurezza mondiale», e che essa è già stata presentata in tal modo in un articolo pubblicato il 1º febbraio 2022 dal rinomato giornale *The Guardian*.

84 Allo stesso modo, dal fascicolo risulta che la seconda persona indicata come esperto nell'articolo di *The Intercept* si presenta ed è stata presentata più volte dall'agenzia di stampa internazionale Reuters come direttore dei diritti digitali e della sicurezza in seno al MIAAN group, un'organizzazione con sede in Texas (Stati Uniti) che «difende i diritti umani in Iran». Contrariamente a quanto sostiene la ricorrente, la semplice circostanza che sia «notorio che [si tratta di] un personaggio pubblico impegnato apertamente e senza riserve contro il governo iraniano» non può necessariamente privare le sue dichiarazioni di pertinenza, per il motivo che non è neutrale e imparziale.

85 A tal riguardo, occorre rilevare che l'esperienza di una tale persona, specializzata nella difesa dei diritti umani, in particolare dei diritti digitali, e che è qualificata come oppositore al regime iraniano dalla ricorrente stessa, è pertinente per fornire un parere utile sul modo in cui le autorità iraniane potrebbero utilizzare un sistema come quello descritto nell'articolo di *The Intercept* per violare detti diritti.

86 Peraltro, occorre sottolineare che l'articolo pubblicato sul sito di *The Intercept* non si limitava alla formulazione di semplici allegazioni, e neppure alla riproduzione dell'opinione degli esperti, ma suffragava le proprie allegazioni ed opinioni mediante la messa a disposizione del manuale d'uso del software SIAM redatto in inglese, che esso consentiva di consultare direttamente in una finestra di visualizzazione, e del secondo manuale redatto in persiano sul quale compariva il logo della ricorrente.

87 Inoltre, per quanto riguarda gli altri articoli contenuti nel fascicolo WK 307/2023 INIT, occorre rilevare che il sito Internet Commrisk, che si descrive come «un sito web che descrive i rischi cui sono esposti i fornitori di comunicazioni elettroniche e i loro clienti», e *The Tech Monitor*, che si definisce come volto a fornire «informazioni basate su dati e analisi autorevoli agli imprenditori, ai responsabili digitali e ai responsabili politici in un mondo perturbato ed ispirato dalla tecnologia», sono media specializzati nel settore delle telecomunicazioni e che l'associazione ARTICLE 19, con sede a Londra (Regno Unito), si descrive come «un'organizzazione internazionale di riflessione che sostiene il movimento a favore della libertà di espressione a livello locale e mondiale al fine di garantire che tutti gli individui prendano atto del potere della loro voce», cosicché devono essere considerati come fonti di informazione pertinenti nell'utilizzo delle tecnologie dell'informazione e della comunicazione in relazione all'esercizio dei diritti fondamentali e, in particolare, del diritto alla libertà di espressione.

88 Mentre gli articoli di Commrisk, ARTICLE 19 e *The Tech Monitor* fanno tutti e tre riferimento all'articolo di *The Intercept*, l'articolo di Commrisk attesta anche l'esperienza del suo autore, che avrebbe incontrato il rappresentante di una società tecnologica che tentava di vendere all'Iran un software dotato di funzioni «stranamente simili» a quelle del software SIAM e che gli aveva volontariamente fornito informazioni in merito a tale vendita.

89 Inoltre, dall'articolo dell'associazione ARTICLE 19 risulta che quest'ultima ha monitorato la portata dei controlli effettuati su Internet in Iran da diversi anni e che ha rivelato, in una relazione intitolata «Iran Tightening the Net 2020», il funzionamento dell'infrastruttura di Internet in tale paese e la sua governance da parte delle autorità. In particolare, esisterebbe un sistema centralizzato che consente di interrompere l'accesso a Internet in occasione delle manifestazioni nel corso delle quali la governance di Internet sarebbe considerata una questione di sicurezza nazionale. L'associazione ARTICLE 19 avrebbe scoperto che la ricorrente, sotto il controllo del Ministero delle Comunicazioni, che sarebbe in realtà controllato dai servizi di intelligence iraniani, utilizzerebbe strumenti di sorveglianza e di censura a livello dei fornitori di

accesso a Internet e ordinerebbe interruzioni e altre perturbazioni dell'accesso a Internet per conto del Consiglio supremo di sicurezza nazionale. L'articolo dell'associazione ARTICLE 19 menziona altresì l'uso da parte delle autorità iraniane di tecnologie che bloccano l'utilizzo di strumenti che consentono di eludere la censura di Internet, come le reti private virtuali (VPN), nonché di interruzioni o perturbazioni gravi delle connessioni mobili come tattiche di repressione digitale. Ad esempio, le interruzioni dell'accesso all'Internet mobile sarebbero sempre più utilizzate dal novembre 2019. Tali interruzioni sarebbero state particolarmente utilizzate durante le manifestazioni regionali dal 2021 ad oggi. Viene così indicato che le connessioni all'Internet mobile sono state disattivate in molti luoghi nella maggior parte dei giorni successivi alle manifestazioni che hanno fatto seguito alla morte di Mahsa Amini. Tali interruzioni avrebbero colpito i maggiori fornitori di accesso all'Internet mobile in tutto il paese, il che, in un paese in cui l'Internet mobile costituisce la principale fonte di accesso a Internet per la popolazione, avrebbe avuto un impatto negativo sull'accesso a Internet.

90 Da quanto precede risulta quindi che le allegazioni contenute nell'articolo di *The Intercept* sono corroborate dagli altri elementi di prova che compongono il fascicolo WK 307/2023 INIT e che, di conseguenza, contrariamente a quanto sostiene la ricorrente, il Consiglio non si è basato unicamente sulle allegazioni enunciate in tale articolo. Pertanto, tenuto conto della concordanza dei diversi elementi di prova e delle circostanze summenzionate della loro elaborazione, dette allegazioni potevano essere validamente prese in considerazione.

Sulla fondatezza dell'inserimento del nome della ricorrente

91 In via preliminare, occorre rilevare che, sebbene la ricorrente sostenga che il Consiglio ha commesso nel caso di specie un «errore manifesto di valutazione dei fatti», gli argomenti da essa dedotti al riguardo devono essere considerati come consistenti in una contestazione dell'esattezza materiale dei fatti che le sono addebitati. Infatti, dalla sua argomentazione sviluppata a sostegno del presente motivo, ricordata al punto 42 *supra*, risulta che la ricorrente non contesta che i fatti che le sono addebitati possano rientrare nei criteri di inserimento previsti all'articolo 3, paragrafi 1 e 2, del regolamento n. 359/2011, bensì la realtà di detti fatti.

92 A tal riguardo, dalla giurisprudenza richiamata al punto 62 *supra* risulta che il controllo del giudice dell'Unione comporta una verifica dei fatti addotti nell'esposizione dei motivi sottesa alla decisione che adotta misure restrittive nei confronti di un'entità e che tale verifica non si limita alla valutazione dell'astratta verosimiglianza dei motivi dedotti, ma consiste invece nell'accertare se questi motivi, o per lo meno uno di essi considerato di per sé sufficiente a suffragare la medesima decisione, siano fondati.

93 La valutazione della fondatezza di questi motivi deve essere effettuata esaminando gli elementi di prova e di informazione non in maniera isolata, bensì nel contesto nel quale essi si inseriscono. Infatti, il Consiglio adempie l'onere della prova che gli incombe qualora evochi dinanzi al giudice dell'Unione un complesso di indizi sufficientemente concreti, precisi e concordanti che consentano di dimostrare l'esistenza di un collegamento sufficiente tra la persona sottoposta ad una misura restrittiva e il regime o, in generale, le situazioni combattute (v., in tal senso, sentenza del 20 luglio 2017, Badica e Kardiam/Consiglio, T-619/15, EU:T:2017:532, punto 99 e giurisprudenza ivi citata).

94 È alla luce di tali considerazioni che occorre verificare se il Consiglio abbia potuto legittimamente ritenere, in sede di adozione dell'atto impugnato, che la ricorrente potesse essere soggetta a misure restrittive.

95 A tal riguardo, in primo luogo, per quanto riguarda le disposizioni di diritto iraniano invocate dalla ricorrente per dimostrare che essa si troverebbe nell'impossibilità giuridica di monitorare e controllare le comunicazioni degli utenti delle reti mobili iraniane, occorre rilevare che, ai sensi dell'articolo 25 della Costituzione della Repubblica islamica dell'Iran, «[l]'ispezione e la mancata consegna delle lettere, la registrazione e la divulgazione delle conversazioni telefoniche, la divulgazione delle comunicazioni telegrafiche e telex, la censura, […] le intercettazioni e qualsiasi forma di sorveglianza sono vietate, salvo quanto previsto dalla legge».

96 L'articolo 582 del codice penale iraniano stabilisce quanto segue:

«Il fatto che un ufficiale dello Stato o un funzionario, in casi diversi da quelli autorizzati dalla legge, acceda a, sequestri, distrugga, ispezioni, registri o intercetti lettere o comunicazioni telegrafiche o telefoniche delle persone, o che ne divulghi il contenuto senza l'autorizzazione del proprietario, è punito con una pena detentiva da uno a tre anni o con una pena pecuniaria da sei a diciotto milioni di [r]ial».

97 L'articolo 104 del codice di procedura penale iraniano dispone quanto segue:

«Il controllo [l'intercettazione] delle telecomunicazioni degli individui è vietato, salvo nei casi in cui sia connesso alla sicurezza interna o esterna del paese o sia ritenuto necessario per l'indagine sui reati elencati all'articolo 302, lettere a), b), c) e d) del presente codice. In tal caso, l'intercettazione è effettuata con l'approvazione del presidente della Corte suprema provinciale e la determinazione della durata e della frequenza dell'intercettazione. L'intercettazione delle conversazioni telefoniche delle persone e dei funzionari elencati all'articolo 307 del presente codice è soggetta all'approvazione del presidente della Corte suprema e tale autorità non può essere delegata ad altri soggetti».

98 Da tali disposizioni risulta che, sebbene l'intercettazione delle comunicazioni sia in linea di principio vietata, essa rimane tuttavia legalmente possibile, in particolare nei casi in cui è connessa «alla sicurezza interna o esterna del paese o sia ritenuta necessaria per [taluni reati]» o quando «il caso è connesso alla sicurezza del paese». A tal riguardo, occorre peraltro osservare che le ipotesi in cui l'intercettazione delle telecomunicazioni è legalmente possibile sono definite in modo molto ampio.

99 Inoltre, occorre rilevare che la tesi della ricorrente è contraddetta anche dal manuale d'uso del software SIAM redatto in inglese, di cui essa peraltro non contesta l'autenticità, nel quale si afferma che, «[s]econdo le norme e i regolamenti della [ricorrente], tutti gli operatori di telecomunicazioni devono fornire a [quest'ultima] un accesso diretto al loro sistema per interrogare (sic) le informazioni dei clienti e modificare i loro servizi attraverso il servizio web».

100 In secondo luogo, per quanto riguarda l'asserita incapacità tecnica della ricorrente di condurre operazioni di sorveglianza e di controllo nei confronti degli utenti delle reti mobili iraniane, è giocoforza constatare che così non è.

101 Occorre infatti sottolineare che la ricorrente non contesta l'esistenza del software SIAM, né dei comandi «Force2GNumber», «LocationCustomerList», «GetCDR», «GetIPDR» e «ApplySusplp» o dei sistemi «Legal Intercept» (LI), «Control Illegal Devices» (CID), «SHAHKAR» e «SHAMSA». La ricorrente non contesta neppure il fatto di utilizzare il software SIAM nonché i detti sistemi. Né tantomeno essa contesta l'autenticità degli scambi di corrispondenza tra i suoi dirigenti e l'operatore mobile iraniano citato nell'articolo di *The Intercept*, né quella dei manuali d'uso del software SIAM, il primo redatto in inglese e il secondo in persiano.

102 Difatti, la ricorrente si limita a sostenere, da un lato, che l'utilizzo di tali comandi o non produce l'effetto descritto dal Consiglio oppure risponde ad un obiettivo legittimo e, dall'altro, che i sistemi «Legal Intercept» (LI), «Control Illegal Devices» (CID), «SHAHKAR» e «SHAMSA» sono comuni nella maggior parte degli Stati.

103 A tal riguardo, occorre ricordare che nel manuale d'uso del software SIAM redatto in inglese si afferma che, «[s]econdo le norme e i regolamenti della [ricorrente], tutti gli operatori di telecomunicazioni devono fornire a [quest'ultima] un accesso diretto al loro sistema per interrogare (sic) le informazioni dei clienti e modificare i loro servizi attraverso il servizio web».

104 Occorre inoltre rilevare che, secondo la traduzione francese fornita dal Consiglio, nell'introduzione del manuale d'uso del software SIAM redatto in persiano è indicato che l'obiettivo di tale software è di «creare un sistema centralizzato, unico e riunificato per effettuare richieste presso i diversi server» e di «consentire la gestione e il controllo sulle comunicazioni e sull'azione degli utenti».

105 Inoltre, nella sezione «Principi di comunicazione» del medesimo manuale viene indicato che «i parametri di input sono nelle informazioni inviate dal software SIAM per ciascun metodo (funzione) di richiesta all'operatore e [che] i parametri di output sono i dati di risposta alla richiesta (e l'ordine della loro classificazione) [e che g]li operatori devono rinviare al SIAM la risposta di ciascuna funzione richiesta precisamente secondo l'ordine e la composizione descritti nella parte dedicata ai parametri di output di detta funzione».

106 Inoltre, viene precisato, sempre in tale manuale, che gli operatori sono tenuti «a rispondere giorno e notte (24x7) alle richieste del software SIAM» e ad assicurarsi che «siano presenti tutti gli strumenti necessari in materia di computer, software, comunicazione di rete e sicurezza, quali la [r]idondanza dei dati (Redundancy), la ripartizione del carico (Road Balancing), i firewall e tutte le altre esigenze».

107 Da tali constatazioni risulta che i comandi del software SIAM sono rivolti a tutti gli operatori mobili iraniani e che questi ultimi sono tenuti a rispondervi nel modo prescritto in qualsiasi momento.

108 È alla luce di tali constatazioni che occorre valutare gli argomenti della ricorrente relativi ai comandi del software SIAM e ai sistemi «Legal Intercept» (LI), «Control Illegal Devices» (CID), «SHAHKAR» e «SHAMSA».

109 Così, per quanto riguarda il comando «LocationCustomerList», la ricorrente sostiene che esso non consente di seguire con precisione un particolare utente di rete mobile, in quanto consentirebbe unicamente di identificare gli utenti di una rete mobile in una zona che va da 200 metri a 2 chilometri intorno ad un'antenna rete GSM. Tuttavia, è giocoforza constatare che la ricorrente ammette che tale comando consente di identificare tutti gli utenti di una rete mobile che si trovano in una certa zona geografica, anche se quest'ultima è approssimativa. È del resto quanto emerge chiaramente dalla descrizione di tale comando nel manuale d'uso del software SIAM redatto in inglese, nel quale viene indicato che «tale funzione, che riceve un parametro di ubicazione, dovrebbe fornire un elenco dei numeri che si trovano in tale luogo». Inoltre, occorre rilevare che dal manuale redatto in persiano risulta che il comando «IdentitySearch» impone agli operatori di inviare i risultati sotto forma di una «tabella» in cui sono indicati, per quanto riguarda le persone fisiche, il numero di telefono, il nome, il cognome, il nome del padre, il numero dell'atto di nascita, la data di nascita, il codice postale, la cittadinanza, il numero di passaporto, l'indirizzo o

gli indirizzi postali, il tipo di pagamento (pagamento anticipato/pagamento successivo), il tipo di linea (carta SIM o altro), la data di concessione, l'indirizzo IP nonché la longitudine e la latitudine geografica dell'indirizzo.

110 Per quanto riguarda il comando «Force2GNumber», la ricorrente afferma che, contrariamente a quanto sostenuto dal Consiglio, esso non aumenterebbe i rischi di pirateria delle comunicazioni. Tuttavia, come giustamente osservato dal Consiglio, la circostanza, quand'anche accertata, che tale ordine non aumenti il rischio di pirateria non mette in discussione la constatazione che un siffatto comando, volto a costringere un telefono cellulare ad utilizzare la rete 2G al posto delle reti 3G e 4G più recenti, ha l'effetto di rendere impossibili la visione e la condivisione di video a partire da tale telefono.

111 Per quanto riguarda i comandi «GetCDR» e «GetIPDR», la ricorrente sostiene che essi servono rispettivamente a consultare la cronologia di un telefono e ad ottenere l'indirizzo IP degli apparecchi nei quali è stata attivata una determinata carta SIM. Secondo la ricorrente, tali funzioni servono esclusivamente a rispondere a richieste nel corso di istruttorie giudiziarie e sono strumenti essenziali messi a disposizione degli organi giurisdizionali, come testimoniano le ordinanze giudiziarie e le lettere della polizia allegate alla replica. Tuttavia, da un lato, occorre rilevare che la ricorrente non fornisce alcun elemento di prova idoneo a dimostrare che tale comando potrebbe essere utilizzato solo in risposta alle legittime richieste degli organi giurisdizionali iraniani e delle autorità di polizia. Dall'altro lato, come già rilevato *supra* al punto 98, le ipotesi in cui l'intercettazione delle telecomunicazioni è legalmente possibile sono definite in modo molto ampio.

112 Per quanto riguarda i comandi «ApplySusp» e «ApplySuspIP», la ricorrente sostiene che essi consentono di disattivare le carte SIM dichiarate dagli utenti come perdute o rubate o appartenenti a persone dichiarate decedute. La ricorrente sottolinea che tale capacità è del tutto classica e paragonabile a quella degli organi di regolamentazione di altri Stati come la Germania. A tal riguardo, occorre rilevare che dalla relazione intitolata «Iran: informazioni sulla capacità di sorveglianza del governo e sul controllo da esso esercitato, compresa la censura dei media e la sorveglianza dell'uso di Internet», pubblicata il 16 gennaio 2015 dalla Commissione per l'immigrazione e lo status di rifugiato del Canada (allegato B.8), dalla relazione pubblicata da Amnesty International il 16 novembre 2020 sulle manifestazioni del novembre 2019 in Iran e sulle interruzioni di Internet (allegato B.10), dalla relazione pubblicata dall'agenzia di stampa Human Rights Activists News Agency (HRANA) l'8 dicembre 2022, contenente un esame statistico, un'analisi e una sintesi dei primi 82 giorni delle manifestazioni e indicante il numero stimato di morti e di arresti (allegato B.3), e dalla relazione del 2022 in materia di libertà su Internet in Iran, pubblicata da Freedom House (allegato B.6), risulta che il contesto in Iran è caratterizzato da regolari contestazioni del regime da parte della popolazione civile, sistematicamente represse dalle autorità di tale paese con l'ausilio, in particolare, di mezzi di sorveglianza di Internet. In tali circostanze, non si può escludere, come osserva il Consiglio, che comandi ideati originariamente a fini «legali», come «ApplySusp» e «ApplySuspIP», siano utilizzati impropriamente dalle autorità iraniane a fini repressivi.

113 Per quanto riguarda i componenti funzionali del sistema di intercettazione delle comunicazioni dell'Iran, la ricorrente precisa che il sistema «SHAHKAR» è semplicemente una rete di verifica dell'identità dell'utente di comunicazioni al momento dell'assegnazione della sua carta SIM, il cui scopo è di evitare le frodi. Secondo la ricorrente, tale sistema raccoglie le informazioni sull'individuo cui appartiene ciascuna carta SIM o linea fissa e crea una banca dati utilizzata per combattere la frode, le molestie e altre attività delittuose analoghe. Tuttavia, occorre rilevare che

la ricorrente spiega altresì che tale sistema consente, in particolare, agli operatori mobili iraniani di verificare l'identità degli utenti dei servizi di comunicazione. Orbene, come constatato al punto 107 *supra*, i comandi del software SIAM sono indirizzati a tutti gli operatori di reti mobili iraniani e questi ultimi sono tenuti a rispondervi in qualsiasi momento nel modo prescritto e ad offrire al software SIAM un accesso permanente ai dati che essi possiedono sugli utenti. Ne consegue che la spiegazione fornita dalla ricorrente non è idonea a confutare l'affermazione del Consiglio quanto al fatto che il sistema «SHAHKAR» costituisce un componente funzionale del sistema di intercettazione delle comunicazioni delle autorità iraniane.

114 Per quanto riguarda il sistema «SHAMSA», la ricorrente nega che esso sia una «interfaccia per la raccolta in blocco di dati vocali e SMS (CDR) e di dati IP (IPDR)», come sostenuto dal Consiglio. Secondo la ricorrente, si tratta semplicemente di «una rete o canale di comunicazione tra [essa] e gli operatori [di reti mobili], attraverso la quale questi ultimi interagiscono inserendovi codici e comandi». Orbene, ancora una volta, tenuto conto, da un lato, della constatazione effettuata al punto 107 *supra*, secondo cui i comandi del software SIAM sono rivolti a tutti gli operatori di reti mobili iraniani e secondo cui questi ultimi sono tenuti a rispondervi in qualsiasi momento nel modo prescritto e, dall'altro, della menzione nell'indice del manuale d'uso del software SIAM redatto in persiano, secondo la traduzione francese fornita dal Consiglio, di un comando diretto a trasferire gli SMS ad un numero, la spiegazione fornita dalla ricorrente è poco convincente.

115 Per quanto riguarda il sistema «CID», la ricorrente sostiene che esso consente di far corrispondere il numero di apparecchio, il numero di cellulare e il numero di carta SIM. La funzione di tale sistema sarebbe unicamente quella di identificare e controllare la legalità dell'importazione in Iran dei telefoni cellulari e dei dispositivi elettronici che possono ospitare una carta SIM al fine di comunicare successivamente tali informazioni agli operatori di telecomunicazioni. Ancora una volta, al di là del legittimo scopo dichiarato di tale sistema, occorre ricordare che è stato constatato che gli operatori di reti mobili iraniani sono tenuti a concedere alla ricorrente, tramite il software SIAM, un accesso permanente alle informazioni in loro possesso sui loro utenti, cosicché la ricorrente può così accedere ai dati raccolti dal sistema «CID».

116 Infine, per quanto riguarda il sistema «LI», la ricorrente ammette che si tratta di un sistema di sicurezza che consente di chiedere ad un operatore di rete di raccogliere e fornire alle forze dell'ordine comunicazioni intercettate di privati o di organizzazioni. La ricorrente sottolinea che tale sistema è rigorosamente disciplinato dalle disposizioni di diritto iraniano applicabili. Tuttavia, come constatato al punto 98 *supra*, dalle disposizioni del diritto iraniano invocate dalla ricorrente stessa risulta che le ipotesi in cui le intercettazioni di telecomunicazioni sono legalmente possibili sono definite in modo molto ampio.

117 Alla luce delle considerazioni esposte ai punti da 95 a 115 *supra*, si deve ritenere che il Consiglio abbia dedotto dinanzi al Tribunale un insieme di indizi sufficientemente concreti, precisi e concordanti che consentono di dimostrare l'esistenza di un collegamento sufficiente tra la ricorrente e la situazione combattuta nel caso di specie, vale a dire la repressione esercitata dalle autorità iraniane nei confronti di manifestanti pacifici, giornalisti, difensori dei diritti umani, studenti e altre persone che rivendicano i propri diritti legittimi.

118 Pertanto, le censure della ricorrente relative all'inesattezza materiale dei fatti devono essere respinte.

119 Ne consegue che il terzo motivo di ricorso deve essere respinto in quanto integralmente infondato.

Sul quarto motivo di ricorso, vertente su una violazione del principio di proporzionalità

120 La ricorrente sostiene che le misure restrittive alle quali è soggetta a causa del suo inserimento nell'allegato I del regolamento n. 359/2011 sono contrarie al principio di proporzionalità.

121 In tal senso, in primo luogo, la ricorrente sostiene che le «sanzioni internazionali» imposte all'Iran in passato avevano comportato il blocco di strumenti per essa particolarmente utili, uno dei quali viene utilizzato per impedire la sovrapposizione delle frequenze iraniane con quelle degli Stati confinanti e l'altro, il *Location Based System*, per la localizzazione precisa dei dispositivi collegati. Inoltre, le sanzioni inflitte oggi all'Iran impedirebbero alla ricorrente di svolgere il suo ruolo di regolatore delle frequenze e di garantire un buon funzionamento della rete di telecomunicazioni nazionali.

122 In secondo luogo, la ricorrente sostiene che le «sanzioni» le impediscono di far parte della Global System for Mobile Communications Association (GSMA) e che essa non può quindi utilizzare il registro della GSMA per impedire la riparazione degli apparecchi contraffatti e illegali. Ne deriverebbero diverse conseguenze negative, tra cui, in particolare, l'impossibilità per l'Iran di lottare efficacemente contro la frode, la creazione di un mercato parallelo di telefoni rubati o ancora l'incapacità di restituire i telefoni rubati ai loro proprietari.

123 Il Consiglio contesta l'argomento della ricorrente.

124 Occorre ricordare che, in forza del principio di proporzionalità, che fa parte dei principi generali del diritto dell'Unione, la legittimità del divieto di un'attività economica è subordinata alla condizione che le misure di divieto siano adeguate e necessarie al conseguimento degli scopi legittimamente perseguiti dalla normativa di cui trattasi, fermo restando che, qualora sia possibile una scelta fra più misure appropriate, occorre ricorrere alla meno restrittiva e che gli inconvenienti causati non devono essere sproporzionati rispetto agli scopi perseguiti (v. sentenza del 6 settembre 2013, Bank Melli Iran/Consiglio, T-35/10 e T-7/11, EU:T:2013:397, punto 179 e giurisprudenza ivi citata).

125 Inoltre, sebbene il rispetto dei diritti fondamentali costituisca una condizione di legittimità degli atti dell'Unione, da una giurisprudenza costante risulta che tali diritti fondamentali non godono, nel diritto dell'Unione, di una tutela assoluta, ma vanno considerati in relazione alla loro funzione nella società. Di conseguenza, possono essere apportate restrizioni dell'esercizio di tali diritti, a condizione che tali restrizioni rispondano effettivamente ad obiettivi di interesse generale perseguiti dall'Unione e non costituiscano, rispetto allo scopo perseguito, un intervento sproporzionato e inaccettabile, tale da ledere la sostanza stessa dei diritti così garantiti (v. sentenza del 13 settembre 2013, Makhlouf/Consiglio, T-383/11, EU:T:2013:431, punto 97 e giurisprudenza ivi citata; sentenza del 16 gennaio 2019, Haswani/Consiglio, T-477/17, non pubblicata, EU:T:2019:7, punto 74).

126 Nel caso di specie, occorre sottolineare che la ricorrente non deduce alcun argomento idoneo a dimostrare che le misure restrittive previste dal regolamento n. 359/2011 e alle quali essa è soggetta a causa dell'adozione del regolamento impugnato non perseguano un obiettivo legittimo o non siano necessarie né appropriate per conseguire tale obiettivo. Essa si limita infatti a sostenere, in sostanza, che le sanzioni internazionali alle quali l'Iran è stato soggetto in passato hanno avuto ripercussioni sfavorevoli sulla sua capacità di adempiere i suoi compiti, senza stabilire un nesso necessario con le misure previste dal regolamento n. 359/2011.

127 In ogni caso, occorre rilevare che uno degli obiettivi perseguiti dal regolamento n. 359/2011, come risulta, in sostanza, dai suoi considerando 1 e 2, consiste nell'esercitare pressioni, congelando i loro fondi e le loro risorse economiche, nei confronti di determinate persone ed entità responsabili di aver ordinato o attuato gravi violazioni dei diritti umani in Iran reprimendo manifestanti pacifici, giornalisti, difensori dei diritti umani, studenti o altre persone che rivendicano i propri diritti legittimi, tra cui la libertà di espressione.

128 È giocoforza constatare che un tale obiettivo corrisponde a un obiettivo legittimo della politica estera e di sicurezza comune (PESC), ossia consolidare e sostenere la democrazia, lo Stato di diritto, i diritti dell'uomo e i principi del diritto internazionale, di cui all'articolo 21, paragrafo 2, lettera b), TUE.

129 Inoltre, le misure restrittive previste dal regolamento n. 359/2011 non possono essere considerate inadeguate alla luce del ruolo chiave svolto dalla ricorrente nell'attuazione delle prescrizioni del governo iraniano relative al filtraggio dei contenuti Internet mediante lo spyware SIAM, come risulta dall'esame del terzo motivo di ricorso.

130 Tali misure devono poi essere considerate necessarie, dal momento che, come giustamente rilevato dal Consiglio, non è stato dimostrato che misure alternative e meno restrittive, quali un sistema di autorizzazione preventiva o un obbligo di giustificazione *a posteriori* dell'uso dei fondi versati, consentirebbero di raggiungere altrettanto efficacemente l'obiettivo perseguito.

131 Pertanto, occorre respingere il quarto motivo di ricorso in quanto infondato.

Sul primo motivo di ricorso, vertente, in sostanza, su uno sviamento di potere

132 La ricorrente sostiene che, sebbene la competenza del Consiglio ad adottare il regolamento impugnato non sia contestata, detto regolamento è viziato da un eccesso di potere da parte del Consiglio nella parte in cui la riguarda. A suo avviso, tale eccesso di potere deriverebbe dal fatto che la vera ragione che ha indotto il Consiglio a inserire il suo nome nell'allegato I del regolamento n. 359/2011 sarebbe quella di colpire lo Stato iraniano.

133 Così, il Consiglio non avrebbe sanzionato la ricorrente a causa della sua attività, come sarebbe stato falsamente indicato nel regolamento impugnato, ma unicamente a causa della sua natura governativa risultante dalla sua affiliazione al Ministero delle Comunicazioni, come avviene in qualsiasi altro paese. Sottoponendo la ricorrente alle misure restrittive previste dal regolamento n. 359/2011, il Consiglio cercherebbe di sanzionare la sua affiliazione e quindi di paralizzare il potere iraniano.

134 Secondo la ricorrente, conformemente alla giurisprudenza, anche se lo status giuridico di una persona oggetto delle misure restrittive o il suo rapporto giuridico o economico con il governo di un paese può costituire un indizio idoneo a far sorgere nel Consiglio un sospetto, esso non può, di per sé, giustificare l'adozione di tali misure.

135 L'identità delle altre persone inserite nell'allegato I del regolamento n. 359/2011 dimostrerebbe parimenti il carattere eccessivo dell'inserimento del nome della ricorrente in detto allegato.

136 La ricorrente sottolinea, inoltre, il mimetismo tra le misure restrittive adottate dal Consiglio e le sanzioni adottate dall'Office of Foreign Assets Control, che dimostrerebbe un risentimento politico nei confronti della Repubblica islamica dell'Iran.

137 Il Consiglio contesta l'argomento della ricorrente.

138 Occorre ricordare che, secondo la giurisprudenza consolidata della Corte, un atto è viziato da sviamento di potere solo se risulta, sulla base di indizi oggettivi, pertinenti e concordanti, che è stato adottato allo scopo esclusivo, o quantomeno determinante, di raggiungere fini diversi da quelli dichiarati o di eludere una procedura appositamente prevista dal Trattato per far fronte alle circostanze del caso in questione (v. sentenza del 31 gennaio 2019, Islamic Republic of Iran Shipping Lines e a./Consiglio, C-225/17 P, EU:C:2019:82, punto 115 e giurisprudenza ivi citata).

139 Nel caso di specie, la ricorrente sostiene che il Consiglio ha inserito il suo nome nell'allegato I del regolamento n. 359/2011 unicamente in ragione della sua natura governativa risultante dalla sua affiliazione al Ministero delle Comunicazioni e non della sua attività.

140 Tuttavia, dall'esame del secondo motivo di ricorso (v. punti da 25 a 34 *supra*) risulta che l'inserimento del suo nome nell'allegato I del regolamento n. 359/2011 da parte del regolamento impugnato non è stato motivato unicamente dalla sua affiliazione al Ministero delle Comunicazioni, bensì, essenzialmente, dalla sua attuazione delle prescrizioni del governo iraniano relative al filtraggio dei contenuti Internet mediante lo spyware SIAM e, in particolare, dall'aver sfruttato il proprio controllo dell'accesso a Internet e dei telefoni cellulari per localizzare i manifestanti e creare un quadro dettagliato delle attività dei dissidenti e dei manifestanti, di cui le autorità si sono avvalse a loro discrezione durante le manifestazioni del 2022 in seguito alla morte di Mahsa sig.ra Amini.

141 Inoltre, dall'esame del terzo motivo di ricorso risulta che i motivi invocati dal Consiglio per giustificare l'inserimento del nome della ricorrente nell'allegato I del regolamento n. 359/2011 da parte del regolamento impugnato si fondavano su una base fattuale sufficientemente solida.

142 Peraltro, la ricorrente non dimostra in che modo la circostanza che il nome di altre persone nell'allegato I del regolamento n. 359/2011, rispetto alle quali essa stessa precisa di non voler fare commenti, o il fatto che le autorità degli Stati Uniti d'America abbiano anch'esse deciso di adottare misure restrittive nei suoi confronti, sarebbero rilevanti per dimostrare che il Consiglio, nel caso di specie, avrebbe commesso uno sviamento di potere, ai sensi della giurisprudenza richiamata al punto 138 *supra*.

143 Occorre pertanto respingere il primo motivo di ricorso in quanto infondato e, pertanto, il ricorso nel suo insieme.

Sulle spese

144 Ai sensi dell'articolo 134, paragrafo 1, del regolamento di procedura, la parte soccombente è condannata alle spese se ne è stata fatta domanda. Nel caso di specie, poiché la ricorrente è rimasta soccombente, occorre condannarla a farsi carico delle proprie spese nonché di quelle del Consiglio, conformemente alla domanda di quest'ultimo.

Per questi motivi,

IL TRIBUNALE (Sesta Sezione)

dichiara e statuisce:

1) Il ricorso è respinto.

2) La Communications Regulatory Authority (CRA) è condannata alle spese.

Costeira Kancheva Öberg

Così deciso e pronunciato a Lussemburgo il 16 ottobre 2024.

Firme