Reports of Cases

JUDGMENT OF THE GENERAL COURT (Sixth Chamber)

16 October 2024*

(Common foreign and security policy – Restrictive measures taken in view of the situation in Iran – Freezing of funds – List of persons, entities and bodies subject to the freezing of funds and economic resources – Inclusion of the applicant's name on the list – Obligation to state reasons – Rights of the defence – Right to effective judicial protection – Proportionality – Misuse of powers)

In Case T-201/23,

Communications Regulatory Authority (CRA), established in Tehran (Iran), represented by T. Clay, T. Zahedi Vafa and K. Mehtiyeva, lawyers,

applicant,

v

Council of the European Union, represented by D. Laurent, P. Mahnič and S. Lejeune, acting as Agents,

defendant,

THE GENERAL COURT (Sixth Chamber),

composed of M.J. Costeira, President, M. Kancheva (Rapporteur) and U. Öberg, Judges,

Registrar: V. Di Bucci,

having regard to the written part of the procedure,

having regard to the fact that no request for a hearing was submitted by the parties within three weeks after service of notification of the close of the written part of the procedure, and having decided to rule on the action without an oral part of the procedure, pursuant to Article 106(3) of the Rules of Procedure of the General Court,

gives the following

* Language of the case: French.

Judgment

1 By its action under Article 263 TFEU, the applicant, the Communications Regulatory Authority (CRA), seeks the annulment of Council Implementing Regulation (EU) 2023/152 of 23 January 2023 implementing Regulation (EU) No 359/2011 concerning restrictive measures directed against certain persons, entities and bodies in view of the situation in Iran (OJ 2023 L 20 I, p. 1) ('the contested regulation'), in so far as that act concerns it.

Background to the dispute

2 The applicant is a government institution affiliated with the Iranian Ministry of Communications and Information Technology ('the Ministry of Communications'). It is governed and organised by the law on the functions and powers of that ministry and by its own statutes. Under those statutes, the applicant achieves inter alia the objectives set by the Ministry of Communications in the radio-communications sector and exercises governmental, executive and supervisory functions and powers of that ministry. The applicant's main activity is the regulation, management and control of the frequency space in Iran. More specifically, the applicant is responsible for issuing operating licences for telecommunications services and for monitoring the performance of licence holders. The applicant also performs a normative role by proposing to the competent authorities national standards for communications as well as instructions and regulations on the mutual connection of telecommunications and computer networks from the perspective of the security of connections. In addition, the applicant carries out functions to protect the rights of users of telecommunications services and to represent the Islamic Republic of Iran in regional and international associations within the communications sector.

3 On 21 March 2011, the Council of the European Union adopted conclusions stating that the European Union was deeply concerned by the continuing deterioration of the human rights situation in Iran. The Council drew attention to the systematic repression to which Iranian citizens were subject, who faced harassment and arrest for exercising their legitimate right to freedom of expression and peaceful assembly. Furthermore, in those conclusions, the Council affirmed the European Union's intention to address human rights abuses committed in Iran, in particular by swiftly introducing restrictive measures targeted against those responsible for grave human rights violations.

4 On 12 April 2011, the Council adopted Decision 2011/235/CFSP concerning restrictive measures directed against certain persons and entities in view of the situation in Iran (OJ 2011 L 100, p. 51), which establishes a series of restrictive measures targeting persons complicit in or responsible for directing or implementing grave human rights violations in Iran.

5 Decision 2011/235 was implemented by Council Regulation (EU) No 359/2011 of 12 April 2011 concerning restrictive measures directed against certain persons, entities and bodies in view of the situation in Iran (OJ 2011 L 100, p. 1), adopted on the basis of Article 215(2) TFEU.

6 Article 2(1) and (2) of Regulation No 359/2011 provides:

'1. All funds and economic resources belonging to, owned, held or controlled by the natural or legal persons, entities and bodies listed in Annex I shall be frozen.

2. No funds or economic resources shall be made available, directly or indirectly, to or for the benefit of the natural or legal persons, entities or bodies listed in Annex I.'

7 Under Article 3(1) and (2) of Regulation No 359/2011, persons who have been identified by the Council as being persons responsible for serious human rights violations in Iran, and persons, entities or bodies associated with them, are to be included in the list contained in Annex I. That list includes the grounds for the listing.

8 Article 12(1) to (3) of Regulation No 359/2011 provides:

'1. Where the Council decides to subject a natural or legal person, entity or body to the measures referred to in Article 2(1), it shall amend Annex I accordingly.

2 The Council shall communicate its decision, including the grounds for the listing, to the natural or legal person, entity or body …, providing such person, entity or body with an opportunity to present observations.

3. Where observations are submitted, or where substantial new evidence is presented, the Council shall review its decision and shall inform the person, entity or body accordingly.'

9 On 16 September 2022, Ms Mahsa Amini, a 22-year-old Iranian, died in hospital whilst being detained by the Iranian morality police. Large-scale protests followed her death and were suppressed by the Iranian authorities.

10 On 25 September 2022, the High Representative of the Union for Foreign Affairs and Security Policy issued a declaration on behalf of the Union deploring the widespread and disproportionate use of force by the Iranian security forces against non-violent protesters. That declaration also spelled out that those responsible for the death of Ms Amini had to be held accountable and called on the Iranian authorities to ensure transparent and credible investigations to clarify the number of deaths and arrests, to release all non-violent protesters and to provide due process to all detainees. Furthermore, the declaration stressed that Iran's decision to severely restrict internet access and to block instant messaging platforms blatantly violated freedom of expression. Finally, the declaration stated that the European Union would consider all the options at its disposal to address the killing of Ms Amini and the way Iranian security forces had responded to the ensuing demonstrations.

11 On 23 January 2023, the Council adopted Implementing Decision (CFSP) 2023/153 implementing Decision 2011/235 (OJ 2023 L 20 I, p. 23). Recital 2 of Implementing Decision 2023/153 referred to the declaration by the High Representative of the Union for Foreign Affairs in the terms reproduced in paragraph 10 above. Recital 3 of that decision stated that, 'in this context, and in line with the Union's commitment to address all issues of concern with Iran, including the human rights situation, 18 persons and 19 entities [were to] be included in the list of persons and entities subject to restrictive measures set out in the Annex to Decision [2011/235]'. Article 1 of Implementing Decision 2023/153 provided that the annex to Decision 2011/235 was amended in accordance with its own annex.

12 Entry 15 on the list of entities in the annex to Implementing Decision 2023/153 stated, inter alia, the applicant's name and the reasons for its listing in the following terms:

'The Communications Regulatory Authority (CRA) is under the authority of the Iranian Ministry for Information and Communications Technology (ICT). The CRA enforces the Iranian government's requirements to filter internet content through a spyware called SIAM.

During the 2022 protests, the CRA used its control of internet access and mobile phones to track protestors and create a detailed picture of dissidents' and protesters' activities for the authorities to use at their will. The CRA is therefore responsible for supporting the repression of peaceful demonstrators, journalists, human rights defenders, students or other persons who speak up in defence of their legitimate rights.

The CRA is therefore responsible for serious human rights violations in Iran.'

13 On the same day, the Council adopted the contested regulation on the basis of Article 12(1) of Regulation No 359/2011. The wording of recitals 2 and 3 of the contested regulation is identical to that of recitals 2 and 3 of Implementing Decision 2023/153, with the exception of the reference to Annex I to Regulation No 359/2011 rather than to the annex to Decision 2011/235. Article 1 of the contested regulation provided that Annex I to Regulation No 359/2011 was amended in accordance with its own annex.

14 Entry 15 on the list of entities in the annex to the contested regulation stated, inter alia, the applicant's name and the reasons for that listing in identical terms to those set out in paragraph 12 above.

15 On 24 January 2023, the Council published in the *Official Journal of the European Union* a notice for the attention of the persons, entities and bodies to whom measures provided for in Decision 2011/235, as implemented by Implementing Decision 2023/153 and in Regulation No 359/2011, as implemented by the contested regulation, apply (OJ 2023 C 25, p. 8).

16 That notice stated, inter alia, that the Council had decided that those persons and entities should be included on the list of persons and entities subject to the restrictive measures provided for in Decision 2011/235 and Regulation No 359/2011, and that those persons and entities could make a request to it, together with supporting documentation, that the decision to include them on the abovementioned lists should be reconsidered. Any request to that end was to be sent before 15 February 2023 to the address stated in that notice.

Forms of order sought

17 The applicant claims that the Court should annul the contested regulation in so far as that regulation includes the applicant's name in Annex I to Regulation No 359/2011.

18 The Council contends that the Court should:

– dismiss the action;

– order the applicant to pay the costs.

Law

19 In support of its action, the applicant raises four pleas in law. The first alleges, in essence, misuse of powers; the second alleges, breach of the obligation to state reasons and of the right to effective judicial protection; the third alleges, in essence, the material inaccuracy of the facts; and the fourth alleges breach of the principle of proportionality.

20 It is clear from analysing those pleas that it is appropriate to examine, in the first place, the second plea relating to breach of the obligation to state reasons and breach of the right to effective judicial protection; in the second place, the third plea relating to a manifest error of assessment of the facts; in the third place, the fourth plea relating to breach of the principle of proportionality; and, in the fourth place, the first plea relating to misuse of powers.

The second plea, alleging breach of the obligation to state reasons and breach of the right to effective judicial protection

21 In the first place, the applicant claims that, by having failed to communicate, concomitantly with the adoption of the contested regulation, or immediately after, the information or evidence forming the basis of the reasons for including its name on the list in Annex I to Regulation No 359/2011, the Council did not discharge its duty to establish that those reasons were well founded and, consequently, breached its obligation to state reasons.

22 In the second place, the applicant submits that the statement of reasons for the contested regulation, in so far as it concerns it, is a stereotypical statement of reasons consisting of three brief paragraphs of 15 lines summarising the assumptions made by the Council on account of its public nature. Such a statement of reasons is incompatible with the case-law according to which the statement of reasons for a measure must enable, first, the person concerned by the measure at issue to contest its validity before the courts in full knowledge of the case against him or her and, second, the court to carry out its judicial review of the contested measure. According to the applicant, the requirement to state reasons cannot be tempered by the political context in which a measure is adopted, particularly since contextualisation cannot assist the applicant in understanding the scope of the restrictive measures adopted against it and, as a corollary, enable the court to review the measure at issue. The Council cannot therefore breach its obligation to state reasons by 'hiding' behind considerations related to security and foreign policy interests.

23 In the third place, in the reply, the applicant contests, on the basis of Articles 47 and 48 of the Charter of Fundamental Rights of the European Union ('the Charter'), the admissibility of the document produced by the Council before the Court as evidence in support of the reasons relied on to justify the inclusion of its name in Annex I to Regulation No 359/2011. The applicant also contests the relevance and the evidential value of the information contained in that document.

24 The Council disputes the applicant's arguments.

25 It should be recalled that, according to settled case-law, the purpose of the obligation to state the reasons on which an act adversely affecting an individual is based, which is a corollary of the principle of respect for the rights of the defence is, first, to provide the person concerned with sufficient information to make it possible to ascertain whether the act is well founded or whether it is vitiated by a defect which may permit its legality to be contested before the European Union

judicature and, second, to enable that judicature to review the legality of that act (see judgment of 15 November 2012, *Council* v *Bamba*, C-417/11 P, EU:C:2012:718, paragraph 49 and the case-law cited).

26 It should also be borne in mind that the statement of reasons required by Article 296 TFEU and by Article 41(2)(c) of the Charter must be appropriate to the act at issue and the context in which it was adopted. The requirements to be satisfied by the statement of reasons depend on the circumstances of each case, in particular the content of the measure in question, the nature of the reasons given and the interest which the addressees of the measure, or other parties to whom it is of direct and individual concern, may have in obtaining explanations. It is not necessary for the reasoning to go into all the relevant facts and points of law, since the question whether the statement of reasons is sufficient must be assessed with regard not only to its wording but also to its context and to all the legal rules governing the matter in question (see judgment of 17 September 2020, *Rosneft and Others* v *Council*, C-732/18 P, not published, EU:C:2020:727, paragraph 77 and the case-law cited; judgment of 27 July 2022, *RT France* v *Council*, T-125/22, EU:T:2022:483, paragraph 103).

27 Thus, first, the reasons given for a measure adversely affecting a person are sufficient if that measure was adopted in circumstances known to the party concerned which enable him or her to understand the scope of the measure concerning him or her (see judgment of 17 September 2020, *Rosneft and Others* v *Council*, C-732/18 P, not published, EU:C:2020:727, paragraph 78 and the case-law cited). Second, the degree of precision of the statement of reasons for a measure must be weighed against practical realities and the time and technical facilities available for taking the measure (see judgment of 27 July 2022, *RT France* v *Council*, T-125/22, EU:T:2022:483, paragraph 104 and the case-law cited).

28 In addition, it has been made clear in case-law that the statement of reasons for an act of the Council which imposed a restrictive measure had not only to identify the legal basis for that measure but also the actual and specific reasons why the Council considered, in the exercise of its discretion, that such a measure had to be adopted in respect of the person concerned (see judgment of 27 July 2022, *RT France* v *Council*, T-125/22, EU:T:2022:483, paragraph 105 and the case-law cited).

29 Finally, it should be recalled that the obligation to state the reasons on which an act is based is an essential procedural requirement which must be distinguished from the question of the merits of the reasons, which goes to the substantive legality of the act in question. The reasoning for an act is the formal expression of the reasons upon which that act is based. If those reasons are vitiated by errors, those errors vitiate the substantive legality of the act but not the statement of reasons for it, which can be sufficient whilst setting out erroneous reasons (see, to that effect, judgment of 13 September 2013, *Makhlouf* v *Council*, T-383/11, EU:T:2013:431, paragraphs 73 and 74 and the case-law cited).

30 In the present case, with regard to the context in which the applicant's name was included in Annex I to Regulation No 359/2011, it must be observed that, as the Council rightly notes, recital 2 of the contested regulation referred to the declaration issued on 25 September 2022 on behalf of the European Union by the High Representative of the Union, the wording of which is reproduced in paragraph 10 above.

31 In addition, as stated in paragraph 11 above, recital 3 of the contested regulation explains that it was the context set out in paragraph 10 above and the European Union's commitment to address all issues of concern with Iran, including the human rights situation, which prevailed inter alia when 19 entities, including the applicant, were included on the list of natural and legal persons, entities and bodies subject to restrictive measures contained in Annex I to Regulation No 359/2011.

32 Specifically, the reasons why the applicant's name was included in Annex I to Regulation No 359/2011 were set out in the annex to the contested regulation in the terms reproduced in paragraph 12 above.

33 It must be observed that such reasons, read in the light of the contextual information reproduced in recitals 2 and 3 of the contested regulation, set out in a sufficiently specific and precise manner the reasons why the Council considered, in the exercise of its discretion, that a restrictive measure had to be adopted in respect of the applicant.

34 It is apparent from the statement of reasons for the contested regulation that the applicant was considered responsible for serious human rights violations in Iran because it had enforced the Iranian government's requirements to filter internet content through a spyware called SIAM and, in particular, during the 2022 protests following the death of Ms Amini, used its control of internet access and mobile phones to track protesters and create a detailed picture of dissidents' and protesters' activities for the authorities to use at their will, thus supporting those authorities' repression of protesters who spoke up in defence of their legitimate rights.

35 Furthermore, the applicant's argument that the Council failed to fulfil its obligation to state reasons because the Council did not communicate to it, concomitantly with the adoption of the contested regulation, or immediately after, the evidence forming the basis of the reasons relied on to justify its inclusion in Annex I to Regulation No 359/2011 and, therefore, failed to establish that those reasons are well founded must be rejected.

36 First, in so far as, by that line of argument, the applicant seeks to claim that the Council failed to produce evidence that the reasons relied on in the contested regulation to justify its inclusion in Annex I to Regulation No 359/2011 were well founded, it must be borne in mind that, in accordance with the case-law recalled in paragraph 29 above, that question must be distinguished from that of the statement of reasons for the contested regulation, which concerns the external legality of the regulation.

37 Second, in so far as, by that line of argument, the applicant seeks to claim that the Council breached its rights of defence because it was obliged to grant to the applicant, of its own motion, access to the information in its file, it must be observed that the contested regulation was notified to the applicant by a notice published in the Official Journal on 24 January 2023 which invited the persons and entities concerned to submit a request for reconsideration to the Council before 15 February 2023, and that the applicant did not make such a request or even ask the Council for access to its file outside the present proceedings.

38 In addition, it must be recalled that, in the case of an initial inclusion on a list of persons and entities subject to restrictive measures, when sufficiently precise information has been communicated, enabling the entity concerned effectively to state its point of view on the evidence adduced against it by the Council, the principle of respect for the rights of the defence does not mean that the Council is obliged spontaneously to grant access to the documents in its

file. It is only on the request of the party concerned that the Council is required to provide access to all non-confidential official documents concerning the measure at issue. It would in fact be excessive to require spontaneous communication of the matters in the file, given that when a fund-freezing measure is adopted it is not certain that the entity concerned intends to check, by means of access to the file, the matters of fact supporting the allegations made against it by the Council (judgments of 14 October 2009, *Bank Melli Iran* v *Council*, T-390/08, EU:T:2009:401, paragraph 97, and of 16 September 2013, *Bank Kargoshaei and Others* v *Council*, T-8/11, not published, EU:T:2013:470, paragraph 68).

39 In the present case, it follows from the foregoing that, by the statement of reasons for the contested regulation, the applicant had sufficiently precise information to enable it to state its point of view on the evidence adduced against it by the Council. Accordingly, the Council was not required to communicate to the applicant, of its own motion, the information contained in its file.

40 It must also be observed that the applicant's arguments concerning the admissibility of the document produced in Annex B.11 and the evidential value of the information contained therein concern the merits of the reasons relied on to justify the inclusion of its name in Annex I to Regulation No 359/2011 and are therefore irrelevant when raised in support of a plea alleging breach of the obligation to state reasons. Those arguments will thus be examined together with the similar arguments put forward by the applicant in the context of the third plea, alleging a manifest error of assessment.

41 The second plea must therefore be dismissed as unfounded.

The third plea, alleging the material inaccuracy of the facts

42 The applicant claims that the contested regulation is, in so far as it concerns it, vitiated by a 'manifest error of assessment of the facts' since, first, it does not have the legal capacity to perform the acts of which it is accused by the Council and, second, nor does it have the technical capacities to track or create a 'detailed picture' of protesters' activities.

43 Thus, first, the applicant argues that its statutes do not authorise it to conduct mass surveillance of the population, let alone 'track' protesters. In accordance with its statutes, the applicant performs a role of regulator, moderator or even representative of Iran. In addition, the applicant also states that, even if it wished to establish a filtering system, it could not do so because such a practice is governed by a legal framework. Thus, contrary to what the Council contends, data is collected in Iran within a framework governed by a number of legal instruments, including Article 25 of the Constitution, Article 582 of the Iranian Criminal Code, as supplemented by the 'Law on cyber offences' of 26 May 2009, and Articles 104 and 150 of the Iranian Code of Criminal Procedure. That normative framework is consistent with Council Resolution of 17 January 1995 on the lawful interception of telecommunications (OJ 1996 C 329, p. 1). Moreover, it is apparent from two reports produced by a telecommunications company that, contrary to the Council's contentions, the applicant's requests do not go beyond the traditional requirements in terms of lawful interception.

44 Furthermore, the applicant submits that a distinction should be drawn between mass surveillance and the individual surveillance of persons. According to the applicant, mass surveillance may prove necessary in any society in order to maintain peace and public order, inter alia by monitoring the movement of persons and mass gatherings. This makes it possible to prevent any

disorderly behaviour from the crowd when public protests take place. Every sovereign State has that power of surveillance and its exercise cannot be deemed to result in individual human rights violations. That power of surveillance is a public authority power which has been recognised inter alia by the European Court of Human Rights.

45 Second, according to the applicant, the software which it uses, called 'SIAM' or 'Samaneh yekparche Estehlamate Mokhaberati' in Farsi, does not offer functions which allow for the mass or individual surveillance of protesters on Iranian soil.

46 The applicant submits that the SIAM software is an application programming interface (API) gateway, that is, a device which performs a bridging role and allows a client external to an entity to use internal APIs and their services. That software is used by the Red Crescent, ambulances, firefighters and road traffic and crisis management organisations in Iran. Thus, according to the applicant, the SIAM software is used by call centres, in particular when they receive request from the emergency services. The call centres use that software to reach the mobile phone operators, which then provide a merely approximate location of the person in a dangerous situation.

47 Furthermore, the applicant states that it cannot communicate information about the users of communications services directly to the police and judicial authorities because that information is held by the operators with a network operating licence.

48 Last, the applicant disputes the arguments put forward by the Council in its defence regarding the alleged 'functional components' of the intercept system in Iran.

49 Thus, the applicant claims that the Council is mistaken about the functionalities of the SIAM software – 'Force2GNumber', 'LocationCustomerList', 'GetCDR', 'GetIPDR' and 'ApplySusplp' – to which it refers in the defence. The applicant explains that the Council's description of those functions, which is based solely on an article from the online investigative newspaper *The Intercept*, is inaccurate. According to the applicant, they are well-established and ordinary commands available to a State telecommunications regulator and that all Member States of the European Union have similar tools. The same is true in relation to the 'Legal Intercept' (LI), 'Control Illegal Devices' (CID), 'SHAHKAR' and 'SHAMSA' systems.

50 In addition, in the reply, the applicant contests the admissibility of the article entitled 'Hacked documents: How Iran can track and control protesters' phones', published on 28 October 2022 by *The Intercept*, produced by the Council in Annex B.11 ('*The Intercept* article'). According to the applicant, the facts alleged in that article are based on a series of internal documents of an Iranian mobile operator which were not added to the file in the proceedings before the Court, and the Council simply asserts that the authors of that article had access to documents which were sent to them 'by a person [claiming] to have hacked an Iranian mobile operator'. That article, which is the centrepiece of the Council's file, is therefore merely hearsay evidence. In accordance with the case-law of the Court of Justice on Articles 47 and 48 of the Charter and with the case-law of the European Court of Human Rights on Article 6 of the Convention for the Protection of Human Rights and Fundamental Freedoms, signed in Rome on 4 November 1950, the testimonies of witnesses who are then absent from the hearing and which cannot be examined by the opposing party are prohibited in principle, save where the prosecution provides sufficient justification for the need to use their testimonies and where other procedural safeguards are afforded to the accused person, and there is other evidence against him or her. The Court of Justice also held in

the judgment of 8 December 2022, *HYA and Others (Impossibility of questioning prosecution witnesses)* (C-348/21, EU:C:2022:965), that, if it is impossible to question prosecution witnesses, the evidential value of their testimonies must be qualified, even if such testimonies are admissible.

51 It follows that, by basing the contested regulation on alleged claims by an unknown person, the Council acted in breach of Articles 47 and 48 of the Charter, and therefore that offer of evidence must be rejected as inadmissible.

52 The applicant also claims in the reply that, pursuant to the adversarial principle, a court can take into consideration only the procedural documents and evidence which the parties have seen and on which they have been able to comment. The Council has itself acknowledged that the Iranian mobile operator referred to in *The Intercept* article did not respond to the journalists' request for comment.

53 The Council disputes the applicant's line of argument.

54 It must be observed that, in the context of the third plea, the applicant contests the merits of the reasons relied on to justify its inclusion in Annex I to Regulation No 359/2011. Indeed, it argues that it has neither the legal nor technical capacity to engage in the activities of which it is accused.

55 However, it must also be noted that, as is apparent from paragraph 23 above, in the context of the second plea, the applicant complains that the Council infringed Articles 47 and 48 of the Charter and reversed the burden of proof by basing its assessment on *The Intercept* article given that, as the documents mentioned in that publication were not added to the file in these proceedings, the facts and comments set out in that article are merely allegations in respect of which the applicant is denied the opportunity to exercise its rights of defence. The applicant also argues in the reply that the failure to add evidence to the file in these proceedings undermines respect for the adversarial principle as provided for in Article 85(1) of the Rules of Procedure of the General Court. Moreover, the applicant argues that such a publication has no evidential value.

56 The applicant's arguments alleging infringement of Articles 47 and 48 of the Charter and breach of the adversarial principle must be examined before considering those relating to the evidential value of *The Intercept* article, and next the arguments relating to a 'manifest error of assessment of the facts'.

Infringement of Articles 47 and 48 of the Charter and breach of the adversarial principle

57 First of all, the applicant's argument that *The Intercept* article produced by the Council in Annex B.11 to the defence should be rejected as inadmissible because, in essence, it is not possible for it to defend itself against mere allegations, which undermines its rights of defence before the Court, must be rejected.

58 It must be observed that the issue of the admissibility of evidence offered before the Court, which is governed by Article 85 of the Rules of Procedure, must be distinguished from the question of the assessment of the evidence by the Courts of the European Union.

59 In that regard, it must be recalled that, according to settled case-law of the Court of Justice, when reviewing restrictive measures, the Courts of the European Union must ensure the review, in principle the full review, of the lawfulness of all Union acts in the light of the fundamental rights forming an integral part of the European Union legal order (see, to that effect, judgments of

18 July 2013, *Commission and Others* v *Kadi*, C-584/10 P, C-593/10 P and C-595/10 P, EU:C:2013:518, paragraph 97; of 28 November 2013, *Council* v *Fulmen and Mahmoudian*, C-280/12 P, EU:C:2013:775, paragraph 58; and of 28 March 2017, *Rosneft*, C-72/15, EU:C:2017:236, paragraph 106).

60 Those fundamental rights include, inter alia, respect for the rights of the defence and the right to effective judicial protection (see judgment of 28 November 2013, *Council* v *Fulmen and Mahmoudian*, C-280/12 P, EU:C:2013:775, paragraph 59 and the case-law cited; judgment of 28 November 2013, *Council* v *Manufacturing Support & Procurement Kala Naft*, C-348/12 P, EU:C:2013:776, paragraph 66).

61 The effectiveness of the judicial review guaranteed by Article 47 of the Charter requires that, as part of the review of the lawfulness of the grounds which are the basis of the decision to include or to maintain the name of a person or an entity on the list of persons and entities subject to restrictive measures, the Courts of the European Union are to ensure that that decision, which affects that person or that entity individually, is taken on a sufficiently solid factual basis. That entails a verification of the factual allegations in the summary of reasons underpinning that decision, with the consequence that judicial review cannot be restricted to an assessment of the cogency in the abstract of the reasons relied on, but must concern whether those reasons, or, at the very least, one of those reasons, deemed sufficient in itself to support that decision, are substantiated (see, to that effect, judgments of 18 July 2013, *Commission and Others* v *Kadi*, C-584/10 P, C-593/10 P and C-595/10 P, EU:C:2013:518, paragraph 119; of 18 June 2015, *Ipatau* v *Council*, C-535/14 P, EU:C:2015:407, paragraph 42; and of 18 February 2016, *Council* v *Bank Mellat*, C-176/13 P, EU:C:2016:96, paragraph 109).

62 In that context, it is the task of the competent European Union authority, in the event of challenge, to establish that the reasons relied on against the person or entity concerned are well founded, and not the task of that person or entity to adduce evidence of the negative, that those reasons are not well founded (see, to that effect, judgment of 18 July 2013, *Commission and Others* v *Kadi*, C-584/10 P, C-593/10 P and C-595/10 P, EU:C:2013:518, paragraph 121).

63 However, contrary to what the applicant claims, it does not follow that the alleged lack of capacity of the Council to adduce the evidence that the reasons relied on to justify the applicant's listing in Annex I to Regulation No 359/2011, if it were established, would undermine the applicant's rights of defence.

64 As is apparent from the case-law recalled in paragraph 61 above, it is on the contrary because, in order to preserve the effectiveness of Article 47 of the Charter, the Courts of the European Union are obliged to verify, in the context of reviewing the legality of the restrictive measures, the merits of the reasons underlying those measures and, therefore, the evidential value of the documents produced, in the present case, by the Council.

65 Next, it is necessary to dismiss as irrelevant in the present case the considerations, relied on by the applicant, which are set out in the judgment of 8 December 2022, *HYA and Others (Impossibility of questioning prosecution witnesses)* (C-348/21, EU:C:2022:965), in which the Court of Justice was asked about the interpretation of Article 6(1) and Article 8(1) of Directive (EU) 2016/343 of the European Parliament and of the Council of 9 March 2016 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings (OJ 2016 L 65, p. 1) and the second paragraph of Article 47 of the Charter.

66 It must be recalled that the principle of the presumption of innocence, set out in Article 6(2) of the Convention for the Protection of Human Rights and Fundamental Freedoms and in Article 48(1) of the Charter, is a fundamental right which confers rights on individuals or entities managed by individuals which are enforced by the Courts of the European Union (see judgment of 18 May 2017, *Makhlouf* v *Council*, T-410/16, not published, EU:T:2017:349, paragraph 122 and the case-law cited).

67 The principle of the presumption of innocence, which requires that any person charged with a criminal offence is presumed innocent until proved guilty according to law, does not preclude the adoption of precautionary measures for the freezing of funds, provided that they are not intended to commence criminal proceedings against the person or entity concerned. Such measures must however, in the light of their seriousness, be laid down by law, be adopted by a competent authority and be limited in time. It follows from paragraph 13 above that those first two criteria are satisfied. In addition, with regard to the time limitation, it must be observed that, in accordance with Article 12(3) and (4) of Regulation No 359/2011, Annex I to that regulation is to be reviewed at regular intervals and at least every 12 months, with the result that the listing of a person or an entity in that annex may be extended or amended where appropriate. The measures imposed on the applicant are indeed therefore limited in time (see, to that effect, judgment of 18 May 2017, *Makhlouf* v *Council*, T-410/16, not published, EU:T:2017:349, paragraph 123 and the case-law cited).

68 In addition, it must be observed that the restrictive measures at issue do not entail the applicant's assets being confiscated as the proceeds of crime but rather frozen as a precautionary measure. Those measures do not therefore constitute a criminal sanction and do not, moreover, imply any accusation of a criminal nature (see judgment of 18 May 2017, *Makhlouf* v *Council*, T-410/16, not published, EU:T:2017:349, paragraph 124 and the case-law cited).

69 The contested regulation, in so far as it concerns the applicant, does not constitute a finding of fact that an offence has actually been committed, rather it was adopted in the context and for the purpose of an administrative procedure with a precautionary function which is solely intended to allow the Council to guarantee the protection of civilian populations (see, to that effect, judgment of 18 May 2017, *Makhlouf* v *Council*, T-410/16, not published, EU:T:2017:349, paragraph 125 and the case-law cited).

70 Finally, it is also necessary to reject the applicant's argument that, since the documents referred to in *The Intercept* article were not added to the file in the present case, that article should be rejected as inadmissible because, pursuant to the adversarial principle, a court can take into consideration only the procedural documents and evidence which have been made available to the parties and on which they have been able to comment. It is sufficient to observe in that regard that the applicant had the opportunity in its reply to set out its views on the evidence produced by the Council in Annex B.11, including that article, the evidential value of which it moreover contests.

71 Furthermore, it must be noted that the two user manuals for the SIAM software, the first written in Farsi and the second in English, could be consulted directly by following a hyperlink in *The Intercept* article at page 3 of file WK 307/2023 INIT produced by the Council in Annex B.11 to the defence.

72 The applicant's arguments alleging infringement of Articles 47 and 48 of the Charter and breach of the adversarial principle must therefore be rejected.

The evidential value of The Intercept *article*

73 The applicant alleges that *The Intercept* article is merely a news publication containing solely unverifiable allegations and, therefore, it has no evidential value

74 In that regard, it must be recalled that, in accordance with settled case-law, the activity of the Court of Justice and of the General Court is governed by the principle of unfettered assessment of the evidence, and it is only the reliability of the evidence before the EU Courts which is decisive when it comes to the assessment of its value. In addition, in order to assess the evidential value of a document, regard should be had to the credibility of the account it contains and, in particular, to the person from whom the document originates, the circumstances in which it came into being, the person to whom it was addressed and whether, on its face, the document appears to be sound and reliable (see judgment of 31 May 2018, *Kaddour* v *Council*, T-461/16, EU:T:2018:316, paragraph 107 and the case-law cited).

75 In the absence of investigative powers in third countries, the assessment of the EU authorities must rely on publicly available sources of information, reports, articles in the press, intelligence reports or other similar sources of information (judgments of 14 March 2018, *Kim and Others* v *Council and Commission*, T-533/15 and T-264/16, EU:T:2018:138, paragraph 107, and of 1 June 2022, *Prigozhin* v *Council*, T-723/20, not published, EU:T:2022:317, paragraph 59).

76 It would be excessive and disproportionate to require the Council itself to investigate on the ground the accuracy of the facts which are relayed by numerous media (judgment of 25 January 2017, *Almaz-Antey Air and Space Defence* v *Council*, T-255/15, not published, EU:T:2017:25, paragraph 148).

77 Press articles may therefore be used in order to corroborate the existence of certain facts where they come from several different sources and they are sufficiently specific, precise and consistent as regards the facts there described (see judgment of 11 September 2019, *Topor-Gilka and WO Technopromexport* v *Council*, T-721/17 and T-722/17, not published, EU:T:2019:579, paragraph 137 and the case-law cited).

78 In the present case, the Council based the applicant's listing in Annex I to Regulation No 359/2011 on four documents in file WK 307/2023 INIT, which are contained in Annex B.11 to the defence.

79 The first document is *The Intercept* article; the second, the article entitled 'Hacker Leaks Manuals Showing How Iran Uses Mobile Networks to Track Protesters', published on 31 October 2022 by the specialist website Commsrisk; the third, the article entitled 'Iran: New tactics for digital repression as protests continue', published on 17 November 2022 on the website of the association ARTICLE 19; and the fourth, the article entitled 'Iran is using spyware to track citizens attending protests', published by the online investigative newspaper *The Tech Monitor* on 3 November 2022.

80 The applicant claims that the Council bases the contested regulation, in so far as it concerns it, on the mere allegations contained in the article from *The Intercept*, which are themselves based on statements made by an anonymous individual.

81 It must be observed that *The Intercept* article reveals that, on the basis of internal documents of an Iranian mobile operator, in particular email exchanges involving the applicant's management and two user manuals, one in English and the other in Farsi, for a software called SIAM, the authors of that article discovered how the Iranian authorities, through the applicant, had established a

system working behind the scenes of Iranian mobile networks which allowed the Iranian Government to bypass the encryption of telephone calls, track the movements of a telephone user, identify all the telephones in a particular location, analyse all of a telephone user's contacts and interrupt or slow down the user's internet connection, and which had been used to repress and control the Iranian people following the death of Ms Amini in 2022. That article also explains that the English-language SIAM software user manual states that 'based on [the applicant's] rules and regulations all telecom operators must provide [the applicant] direct access to their system for query customer information and change their services via web service' and contains, in addition, technical information about the most powerful commands used by the SIAM software to collect user data directly from Iranian mobile operators.

82 It must also be noted that the authors of *The Intercept* article ensured that they interviewed two individuals presented as experts.

83 In that regard, it must be pointed out that, contrary to what the applicant claims, the first person presented as an expert is not 'someone who nobody knows and who seems to lack any particular legitimacy'. It is in fact apparent from the file that that first person is a researcher at Citizen Lab Canada, an interdisciplinary laboratory based at the University of Toronto (Canada) specialising in 'research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security', and that he has previously been presented as such in an article published on 1 February 2022 by the prominent newspaper *The Guardian*.

84 Similarly, it is apparent from the file that the second person presented as an expert in *The Intercept* article describes himself and has been presented on a number of occasions by the international press agency Reuters as the Director of Digital Rights and Security at the MIAAN group, an organisation based in Texas (United States) which 'defends human rights in Iran'. Contrary to what the applicant claims, the mere fact that it is 'well known that [he] is a public figure who is openly and unreservedly engaged against the Iranian Government' cannot necessarily render statements made by him irrelevant on the ground that he is not neutral and impartial.

85 In that regard, it must be observed that the experience of such an individual, a specialist in the defence of human rights, in particular digital rights, and who is described as an opponent of the Iranian regime by the applicant itself, is relevant to providing a valuable opinion as to how the Iranian authorities could use a system such as that described in *The Intercept* article to undermine those rights.

86 Furthermore, it must be observed that the article published on the website of *The Intercept* did not simply make allegations or even reproduce the opinion of experts, but rather substantiated its claims and views by providing access to the English-language SIAM software user manual, which could be consulted directly via a window embedded in the article, and to the second manual written in Farsi which bore the applicant's logo.

87 In addition, with regard to the other articles contained in file WK 307/2023 INIT, it must be observed that the Commsrisk website, which describes itself as 'a website that reports on the risks faced by electronic communications providers and their customers', and *The Tech Monitor*, which explains that it seeks to provide 'data-driven insight and authoritative analysis for business, digital, and policy leaders in a world disrupted and inspired by technology', are specialist media in the field of telecommunications, and that the ARTICLE 19 association, based in London (United

Kingdom), describes itself as 'an international think-do organisation that propels the freedom of expression movement locally and globally to ensure all people realise the power of their voices'. They must therefore be regarded as relevant sources of information in connection with the use of information and communications technology in conjunction with the exercise of fundamental rights and, in particular, the right to freedom of expression.

88 While the Commsrisk, ARTICLE 19 and *The Tech Monitor* articles do all refer to *The Intercept* article, the Commsrisk article also reports on its author's experience of meeting the representative of a technology company who was trying to sell Iran software with 'disturbingly similar' functions to those of the SIAM software and who had volunteered information about that sale.

89 In addition, it is apparent from the article by the ARTICLE 19 organisation that that organisation has monitored the extent of internet controls in Iran for several years, and that it outlined in a report entitled 'Iran: Tightening the Net 2020' how the internet infrastructure operated in that country and its governance by the authorities. In particular, it stated that there is a centralised system for shutting down internet access during protests in the course of which internet governance is treated as a national security matter. The ARTICLE 19 organisation claims to have discovered that the applicant, operating under the control of the Ministry of Communications, which is in actual fact controlled by Iran's intelligence services, enforced the use of surveillance and censorship equipment at internet service provider (ISP) level and ordered shutdowns and other disruptions of internet access acting on behalf of the Supreme National Security Council. The article by the ARTICLE 19 organisation also reports on the Iranian authorities' use of technology to block the use of tools which allow internet censorship to be circumvented, such as virtual private networks (VPNs), and of shutdowns or major disruptions of mobile internet connections as digital repression tactics. For instance, it states that shutdowns of mobile internet access have been a tactic increasingly in use since November 2019. Such shutdowns have been reportedly used particularly during regional protests from 2021 to the present day. The article states that mobile internet connections were disabled in a number of locations on most days following the protests in the wake of Ms Amini's death. Those shutdowns affected the largest providers of mobile internet access across the country, which – in a country in which mobile internet service is people's main source of internet access – had a detrimental impact on access to the internet.

90 It thus follows from the foregoing that the allegations set out in *The Intercept* article are corroborated by the other evidence contained in file WK 307/2023 INIT and that, therefore, contrary to what the applicant maintains, the Council did not rely solely on the allegations set out in that article. Accordingly, given the consistency of the various items of evidence and the circumstances described above in which they came into being, those allegations could legitimately be taken into account.

The merits of including the applicant's name

91 As a preliminary point, it must be observed that, while the applicant claims that the Council committed a 'manifest error of assessment of the facts' in the present case, the arguments put forward by it in that regard must be regarded as seeking to challenge the material accuracy of the facts of which it is accused. It is apparent from its line of argument developed in support of the present plea, as reproduced in paragraph 42 above, that the applicant does not contest that the facts of which it is accused may be covered by the listing criteria provided for in Article 3(1) and (2) of Regulation No 359/2011, but the reality of those facts.

92 In that regard, it follows from the case-law recalled in paragraph 62 above that the review by the Courts of the European Union entails a verification of the factual allegations in the summary of reasons underpinning the decision by which restrictive measures against an entity are adopted, and that such verification cannot be restricted to an assessment of the cogency in the abstract of the reasons relied on, but must concern whether those reasons, or, at the very least, one of those reasons, deemed sufficient in itself to support that decision, is substantiated.

93 The assessment of the merits of those reasons must be carried out by examining the evidence and information not in isolation but in their context. The Council discharges the burden of proof borne by it if it presents to the EU Courts a body of sufficiently specific, precise and consistent evidence to establish that there is a sufficient link between the person subject to a restrictive measure and the regime or, in general, the situations, being combated (see, to that effect, judgment of 20 July 2017, *Badica and Kardiam* v *Council*, T-619/15, EU:T:2017:532, paragraph 99 and the case-law cited).

94 It is in the light of those considerations that it is necessary to determine whether the Council was right to take the view, in adopting the contested act, that restrictive measures could be imposed on the applicant.

95 In that regard, first, with regard to the provisions of Iranian law upon which the applicant relies to justify its claim that it is prevented by law from monitoring and controlling the communications of the users of Iranian mobile networks, it must be observed that, under Article 25 of the Constitution of the Islamic Republic of Iran, 'the inspection of letters and the failure to deliver them, the recording and disclosure of telephone conversations, the disclosure of telegraphic and telex communications, censorship, … eavesdropping, and all forms of covert investigation are forbidden, except as provided by law'.

96 Article 582 of the Iranian Criminal Code provides:

'A State official or civil servant who, in cases other than those permitted by law, opens, seizes, destroys, inspects, records or intercepts letters, telegraph or telephone communications of persons, or discloses their contents without their owners' permission, shall be liable to a term of imprisonment of one to three years or a fine of 6 to 18 million rials'.

97 Article 104 of the Iranian Code of Criminal Procedure provides:

'Control [interception] of individuals' telecommunications shall be prohibited, save in cases in which it is connected with the internal or external security of the country or is deemed necessary for the investigation of the crimes listed in Article 302(a), (b), (c) and (d) of this Code. In such cases, the interception shall be first approved by the President of the Supreme Court of the province and the duration and frequency of the interception shall be specified. The interception of the telephone communications of the persons and civil servants listed in Article 307 of this Code shall be subject to the approval of the President of the Supreme Court, and that authority may not be delegated to others.'

98 It is clear from those provisions that, while the interception of communications is prohibited in principle, it does however remain possible as a matter of law, in particular 'in cases in which it is connected with the internal or external security of the country or is deemed necessary for [certain crimes]' or where 'the matter is related to national security'. In that regard, it must further be observed that the situations in which the interception of telecommunications is permitted by law are defined very broadly.

99 In addition, it must be noted that the applicant's argument is also contradicted by the English-language SIAM software user manual, the authenticity of which the applicant does not contest, in which it is stated that 'based on [the applicant's] rules and regulations all telecom operators must provide [the applicant] direct access to their system for query customer information and change their services via web service'.

100 Second, as regards the applicant's alleged technical inability to monitor or control the users of Iranian mobile networks, it must be stated that that is not the case.

101 It should thus be observed that the applicant does not dispute that the SIAM software exists, nor the existence of the 'Force2GNumber', 'LocationCustomerList', 'GetCDR', 'GetIPDR' and 'ApplySusplp' commands or the 'Legal Intercept' (LI), 'Control Illegal Devices' (CID), 'SHAHKAR' and 'SHAMSA' systems. The applicant also does not deny that it uses the SIAM software and those systems. Furthermore, nor does the applicant contest the authenticity of the email exchanges between its management and the Iranian mobile operator referred to in *The Intercept* article or that of the SIAM software user manuals, the first written in English and the second in Farsi.

102 The applicant in fact simply claims that, first, the use of those commands either does not produce the effect described by the Council or serves a legitimate purpose and, second, the 'Legal Intercept' (LI), 'Control Illegal Devices' (CID), 'SHAHKAR' and 'SHAMSA' systems are in widespread use in most States.

103 In that regard, it must be recalled that the English-language SIAM software user manual states that 'based on [the applicant's] rules and regulations all telecom operators must provide [the applicant] direct access to their system for query customer information and change their services via web service'.

104 It must also be observed that, according to the French translation provided by the Council, the introduction to the SIAM software user manual in Farsi states that the purpose of that software is to 'create a single, centralised and reunified system for submitting queries to different servers' and to 'allow users' communications and actions to be managed and controlled'.

105 In addition, in the 'Principles of Communications' section of that manual, it is stated that 'the input parameters are in the information sent by the SIAM software for each query method (function) to the operator and [that] the output parameters are the response data to the query (and the order of their classification), [and that the] operators must deliver to SIAM the response of each function specifically requested according to the order and composition described in the section concerned with the output parameters of that function'.

106 Moreover, that manual goes on to state that operators are required 'to respond day and night (24x7) to queries from the SIAM software' and to ensure that 'all the necessary equipment in terms of hardware, software, network communications and security, such as data redundancy (Redundancy), load sharing (Road Balancing), firewalls (Firewall), is provided and that all other requirements are met'.

107 It follows from those findings that the SIAM software commands are addressed to all Iranian mobile operators and that those operators are required to respond to them in the manner prescribed at any time.

108 The applicant's arguments related to the SIAM software commands and to the 'Legal Intercept' (LI), 'Control Illegal Devices' (CID), 'SHAHKAR' and 'SHAMSA' systems must be assessed in the light of those findings.

109 Thus, with regard to the 'LocationCustomerList' command, the applicant claims that that command does not enable a particular mobile network user to be tracked with any precision because it only allows users of a mobile network to be identified within a range of between 200 metres and 2 kilometres from a GSM relay antenna. However, it must be observed that the applicant does concede that that command allows all users of a mobile network in a particular geographic area – albeit an approximate one – to be identified. This is, moreover, made clear in the description of that command in the English-language SIAM software user manual, which states that 'this function, which receives a location parameter, should provide a list of numbers which are in that location'. In addition, it must be observed that it is apparent from the manual written in Farsi that the 'IdentitySearch' command requires operators to send results in the form of a 'table' which, in the case of natural persons, states the person's telephone number, first name, surname, father's first name, birth certificate number, date of birth, postcode, nationality, passport number, postal address(es), payment type (prepaid/postpaid), line type (SIM card or other), registration date, IP address and the geographical longitude and latitude of the address.

110 As regards the 'Force2GNumber' command, the applicant submits that, contrary to what the Council argues, that command does not increase the risks of communications being hacked. However, as the Council rightly observes, the fact, assuming it were to be established, that that command does not increase the risk of hacking does not call into question the finding that such a command, the purpose of which is to force a mobile telephone to use the 2G network instead of the newer 3G and 4G networks, has the effect of making it impossible to view or share videos using that telephone.

111 As for the 'GetCDR' and 'GetIPDR' commands, the applicant submits that they are used, in the case of the former, to consult a telephone's call history and, in the case of the latter, to obtain the IP address of the devices in which a particular SIM card has been activated. According to the applicant, those functions are used exclusively to comply with requests made in judicial investigations and are essential tools at the disposal of courts, as is shown by the judicial orders and police correspondence attached as annexes to the reply. However, first, it must be observed that the applicant does not produce any evidence to show that that command can be used only to respond to legitimate requests made by Iranian courts and police authorities. Second, as has already been pointed out in paragraph 98 above, the situations in which the interception of telecommunications is permitted by law are defined very broadly.

112 In the case of the 'ApplySusp' and 'ApplySuspIP' commands, the applicant submits that they allow SIM cards reported lost or stolen by users or belonging to persons who have been declared dead to be disabled. The applicant notes that that is an entirely standard capacity and is comparable to that relied on by the regulatory bodies of other States such as Germany. In that regard, it must be observed that it is apparent from the report entitled 'Iran: Government surveillance capacity and control, including media censorship and surveillance of individual Internet activity', published on 16 January 2015 by the Immigration and Refugee Board of Canada (Annex B.8), the report published by Amnesty International on 16 November 2020 on the November 2019 protests in Iran and the internet shutdowns (Annex B.10), the report published by the Human Rights Activists News Agency (HRANA) on 8 December 2022, which contains a statistical review, an analysis and a summary of the first 82 days of protests and states the estimated number of deaths and arrests (Annex B.3), and the 2022 report on freedom on the internet in Iran published by

Freedom House (Annex B.6) that the situation in Iran is marked by regular challenges to the regime by the civilian population, challenges which are systematically repressed by the Iranian authorities using, inter alia, internet surveillance methods. In those circumstances, it cannot be ruled out, as the Council observes, that commands originally designed for 'legal' purposes, such as 'ApplySusp' and 'ApplySuspIP', may be misused and used by the Iranian authorities for law enforcement purposes.

113 With respect to the functional components of Iran's system of intercepting communications, the applicant states that the 'SHAHKAR' system is simply a network used to verify the identity of the communications user when a SIM card is assigned to him or her in order to prevent fraud. According to the applicant, that system compiles information about the individual to whom each SIM card or fixed line belongs and creates a database which is used to combat fraud, harassment and other similar criminal activities. However, it must be observed that the applicant also explains that that system allows, inter alia, Iranian mobile operators to verify the identity of users of communication services. As found in paragraph 107 above, the SIAM software commands are addressed to all Iranian mobile operators and those operators are required to respond to those commands in the prescribed manner at any time and to provide the SIAM software with permanent access to the information they hold about users. It follows that the explanation provided by the applicant is not such as to reject the Council's assertion that the 'SHAHKAR' system is a functional component of the system used by the Iranian authorities to intercept communications.

114 As for the 'SHAMSA' system, the applicant disputes that that system is an 'interface for the collection of voice data and SMS in bulk (CDR) and IP data (IPDR)', as the Council contends. According to the applicant, it is merely a 'communication network or channel between [it] and the [mobile] operators, via which operators interact by entering codes and commands'. However, once again, in the light, first, of the finding made in paragraph 107 above that the SIAM software commands are addressed to all Iranian mobile operators and that those operators are required to respond to those commands in the prescribed manner at any time and, second, of the reference in the table of contents of the Farsi version of the SIAM software user manual – according to the French translation provided by the Council – to a command that SMS be transferred to a number, the explanation provided by the applicant is unconvincing.

115 With regard to the 'CID' system, the applicant claims that that system allows the device number, the mobile number and the SIM card number to be matched to one another. According to the applicant, the sole function of that system is to identify and monitor the legality of the importation into Iran of mobile telephones and electronic devices into which a SIM card can be inserted, in order subsequently to pass on that information to telecommunications operators. Once more, alongside the declared legitimate purpose of that system, it must be recalled that it has been found that Iranian mobile operators are required to grant the applicant, via the SIAM software, permanent access to the information which they hold on their users, so that the applicant can thus access the data compiled by the 'CID' system.

116 Last, so far as concerns the 'LI' system, the applicant acknowledges that it is a security system which allows a network operator to be asked to collect and provide to law enforcement authorities intercepted communications of individuals or organisations. The applicant states that that system is subject to strict limitations imposed by the applicable provisions of Iranian law. However, as held in paragraph 98 above, it is apparent from the provisions of Iranian law upon which the applicant itself relies that the situations in which interceptions of telecommunications are permitted by law are defined very broadly.

117 In the light of the considerations set out in paragraphs 95 to 115 above, it must be found that the Council has produced before the Court a body of sufficiently specific, precise and consistent evidence to establish that there is a sufficient link between the applicant and the situation being combated in the present case, namely the repression by the Iranian authorities of peaceful demonstrators, journalists, human rights defenders, students and others speaking up in defence of their legitimate rights.

118 The applicant's complaints based on the material inaccuracy of the facts must therefore be rejected.

119 It follows that the third plea must be dismissed as unfounded in its entirety.

The fourth plea, alleging breach of the principle of proportionality

120 The applicant claims that the restrictive measures to which it is subject because of its listing in Annex I to Regulation No 359/2011 are contrary to the principle of proportionality.

121 In that regard, first, it argues that the 'international sanctions' adopted in the past against Iran had given rise to tools being withheld which are of particular use to it, one of which is used to prevent Iranian frequencies from overlapping with those of neighbouring states and the other, the Location Based System, for the accurate location of connected devices. Moreover, the sanctions currently imposed on Iran prevent the applicant from performing its role as the regulator of frequencies and from ensuring that the national telecommunications network operates effectively.

122 Second, the applicant argues that the 'sanctions' prevent it from joining the Global System for Mobile Communications Association (GSMA) and that it cannot therefore use the GSMA register to prevent counterfeit or illegal devices from being repaired. This has a number of harmful consequences, including, in particular, Iran's inability to combat fraud effectively, the creation of a parallel market in stolen telephones and the impossibility of returning stolen telephones to their owners.

123 The Council disputes the applicant's line of argument.

124 It must be recalled that, by virtue of the principle of proportionality, which is one of the general principles of European Union law, the lawfulness of the prohibition of an economic activity is subject to the condition that the prohibitory measures should be appropriate and necessary in order to achieve the objectives legitimately pursued by the legislation in question; when there is a choice between several appropriate measures, recourse must be had to the least onerous, and the disadvantages caused must not be disproportionate to the aims pursued (see judgment of 6 September 2013, *Bank Melli Iran* v *Council*, T-35/10 and T-7/11, EU:T:2013:397, paragraph 179 and the case-law cited).

125 In addition, whilst respect for fundamental rights is a condition for the legality of acts of the Union, it is settled case-law that those fundamental rights do not enjoy, under European Union law, absolute protection, but must be viewed in relation to their function in society. Consequently, the exercise of those rights may be restricted, provided that those restrictions correspond to objectives of public interest pursued by the European Union and do not constitute, in relation to the aim pursued, a disproportionate and intolerable interference,

impairing the very substance of the rights thus guaranteed (see judgment of 13 September 2013, *Makhlouf* v *Council*, T-383/11, EU:T:2013:431, paragraph 97 and the case-law cited; judgment of 16 January 2019, *Haswani* v *Council*, T-477/17, not published, EU:T:2019:7, paragraph 74).

126 In the present case, it must be observed that the applicant does not raise any argument to demonstrate that the restrictive measures provided for in Regulation No 359/2011 and to which it is subject as a result of the adoption of the contested regulation do not pursue a legitimate objective or are not necessary or appropriate to achieve that objective. It simply claims, in essence, that the international sanctions to which Iran has been subject in the past have had a negative impact on its ability to perform its role, without establishing the necessary link to the measures provided for in Regulation No 359/2011.

127 In any event, it must be observed that one of the objectives pursued by Regulation No 359/2011, as is made clear, in essence, in recitals 1 and 2 thereof, consists in exerting pressure, by freezing their funds and economic resources, on certain persons and entities responsible for directing or implementing grave human rights violations in Iran in the repression of peaceful demonstrators, journalists, human rights defenders, students or other persons who speak up in defence of their legitimate rights, including freedom of expression.

128 It must be observed that such an objective is a legitimate objective of common foreign and security policy (CFSP), namely to consolidate and support democracy, the rule of law, human rights and the principles of international law, as set out in Article 21(2)(b) TEU.

129 Furthermore, the restrictive measures provided for in Regulation No 359/2011 cannot be regarded as inappropriate in view of the key role played by the applicant in the enforcement of the Iranian Government's requirements to filter internet content through the SIAM spyware, as is apparent from the examination of the third plea.

130 Moreover, those measures must be regarded as necessary since, as the Council rightly observes, it has not been shown that alternative and less onerous measures such as a pre-authorisation system or an obligation to provide justification a posteriori for the use of the funds disbursed would enable the objective pursued to be achieved as effectively.

131 The fourth plea must therefore be dismissed as unfounded.

The first plea, alleging, in essence, misuse of powers

132 The applicant claims that, although the competence of the Council to adopt the contested regulation is not contested, that regulation is vitiated by a misuse of powers by the Council in so far as the applicant is concerned. In the applicant's view, that misuse of powers stems from the fact that the real reason which led the Council to include its name in Annex I to Regulation No 359/2011 was to target the Iranian State.

133 Thus, in its opinion, the Council did not sanction the applicant because of its activity, as is falsely stated in the contested regulation, but solely because of its governmental status, which is the result of its affiliation with the Ministry of Communications, as in any other country. By making the applicant subject to the restrictive measures provided for in Regulation No 359/2011, the Council seeks to penalise that affiliation and, in so doing, to paralyse the Iranian authorities.

134 The applicant is of the view that, in accordance with case-law, while the legal status of a person covered by restrictive measures or its legal or economic ties to the government of a country may be an indication that might raise suspicions in the eyes of the Council, it cannot, on its own, justify the adoption of such measures.

135 The identity of the other persons listed in Annex I to Regulation No 359/2011 also demonstrates that the applicant's listing in that annex is excessive.

136 Moreover, the applicant notes that the restrictive measures adopted by the Council mirror the sanctions adopted by the Office of Foreign Assets Control, which is evidence of the political hostility towards the Islamic Republic of Iran.

137 The Council disputes the applicant's line of argument.

138 It must be recalled that, according to the case-law of the Court of Justice, a measure is only vitiated by misuse of powers if it appears, on the basis of objective, relevant and consistent evidence, to have been taken with the exclusive or main purpose of achieving an end other than that stated or of evading a procedure specifically prescribed by the Treaty for dealing with the circumstances of the case (see judgment of 31 January 2019, *Islamic Republic of Iran Shipping Lines and Others* v *Council*, C-225/17 P, EU:C:2019:82, paragraph 115 and the case-law cited).

139 In the present case, the applicant claims that the Council included its name in Annex I to Regulation No 359/2011 solely because of its governmental status stemming from its affiliation with the Ministry of Communications and not because of its own activities.

140 However, it is apparent from the examination of the second plea (see paragraphs 25 to 34 above) that the inclusion of the applicant's name in Annex I to Regulation No 359/2011 by the contested regulation was not solely based on its affiliation with the Ministry of Communications, but essentially on its enforcement of the Iranian Government's requirements to filter internet content through the SIAM spyware and, in particular, the use of its control of internet access and mobile phones to track protesters and create a detailed picture of dissidents' and protesters' activities for the authorities to use at their will during the 2022 protests which followed the death of Ms Amini.

141 In addition, it is apparent from the examination of the third plea that the reasons relied on by the Council to justify the inclusion of the applicant's name in Annex I to Regulation No 359/2011 by the contested regulation had a sufficiently solid factual basis.

142 Furthermore, the applicant fails to substantiate how the fact that the names of other persons in Annex I to Regulation No 359/2011, upon which it itself explains that it does not wish to comment, or the fact the authorities of the United States of America also decided to adopt restrictive measures in its regard is relevant to demonstrating that, in the present case, the Council misused its powers within the meaning of the case-law recalled in paragraph 138 above.

143 The first plea must therefore be rejected as unfounded and, consequently, the action must be dismissed in its entirety.

Costs

144 Under Article 134(1) of the Rules of Procedure, the unsuccessful party is to be ordered to pay the costs if they have been applied for in the successful party's pleadings. In the present case, as the applicant has been unsuccessful, it must be ordered to bear its own costs and to pay those incurred by the Council, in accordance with the form of order sought by the latter.

On those grounds,

THE GENERAL COURT (Sixth Chamber)

hereby:

1. Dismisses the action;

2. Orders the Communications Regulatory Authority (CRA) to pay the costs.

Costeira Kancheva Öberg

Delivered in open court in Luxembourg on 16 October 2024.

[Signatures]