Recueil de la jurisprudence

ARRÊT DU TRIBUNAL (sixième chambre)

16 octobre 2024*

« Politique étrangère et de sécurité commune – Mesures restrictives prises au regard de la situation en Iran – Gel des fonds – Liste des personnes, des entités et des organismes auxquels s'applique le gel des fonds et des ressources économiques – Inscription du nom du requérant sur la liste – Obligation de motivation – Droits de la défense – Droit à une protection juridictionnelle effective – Proportionnalité – Détournement de pouvoir »

Dans l'affaire T-201/23,

Communications Regulatory Authority (CRA), établie à Téhéran (Iran), représentée par M[es] T. Clay, T. Zahedi Vafa et K. Mehtiyeva, avocats,

partie requérante,

contre

Conseil de l'Union européenne, représenté par M[mes] D. Laurent, P. Mahnič et S. Lejeune, en qualité d'agents,

partie défenderesse,

LE TRIBUNAL (sixième chambre),

composé de M[mes] M. J. Costeira, présidente, M. Kancheva (rapporteure) et M. U. Öberg, juges,

greffier : M. V. Di Bucci,

vu la phase écrite de la procédure,

vu l'absence de demande de fixation d'une audience présentée par les parties dans le délai de trois semaines à compter de la signification de la clôture de la phase écrite de la procédure et ayant décidé, en application de l'article 106, paragraphe 3, du règlement de procédure du Tribunal, de statuer sans phase orale de la procédure,

rend le présent

* Langue de procédure : le français.

Arrêt

1 Par son recours fondé sur l'article 263 TFUE, la requérante, Communications Regulatory Authority (CRA), demande l'annulation du règlement d'exécution (UE) 2023/152 du Conseil, du 23 janvier 2023, mettant en œuvre le règlement (UE) nº 359/2011 concernant des mesures restrictives à l'encontre de certaines personnes, entités et organismes au regard de la situation en Iran (JO 2023, L 20 I, p. 1, ci-après le « règlement attaqué »), en tant que cet acte la concerne.

Antécédents du litige

2 La requérante est une institution gouvernementale affiliée au ministère iranien des Communications et des Technologies de l'information (ci-après le « ministère des Communications »), régie et organisée par la loi sur les fonctions et pouvoirs dudit ministère ainsi que par ses propres statuts. Selon ces derniers, la requérante réalise notamment les objectifs fixés par le ministère des Communications dans le secteur des radiocommunications et exerce des fonctions et pouvoirs gouvernementaux, exécutifs et de supervision dudit ministère. La principale activité de la requérante est la réglementation, la gestion et le contrôle de l'espace de fréquences en Iran. La requérante est plus spécifiquement chargée de délivrer les licences d'exploitation de services de télécommunication et de surveiller les performances de leurs titulaires. La requérante exerce également un rôle normatif en proposant aux autorités compétentes des normes nationales relatives aux communications ainsi que des instructions et des réglementations sur la connexion mutuelle des réseaux de télécommunications et informatiques relatives à la sûreté des connexions. La requérante exerce aussi des fonctions de protection des droits des usagers des services de télécommunications et de représentation de la République islamique d'Iran dans les associations régionales et internationales du secteur des communications.

3 Le 21 mars 2011, le Conseil de l'Union européenne a adopté des conclusions indiquant que l'Union européenne était vivement préoccupée par la situation des droits de l'homme qui continuait de se détériorer en Iran. Le Conseil attirait l'attention sur la répression systématique dont faisaient l'objet les citoyens iraniens, qui étaient persécutés et arrêtés parce qu'ils exerçaient leur droit légitime de liberté d'expression et d'assemblée pacifique. Par ailleurs, le Conseil y a affirmé l'intention de l'Union de lutter contre les violations des droits de l'homme commises en Iran, notamment en adoptant rapidement des mesures restrictives contre les personnes enfreignant gravement ces droits.

4 Le 12 avril 2011, le Conseil a adopté la décision 2011/235/PESC, concernant des mesures restrictives à l'encontre de certaines personnes et entités au regard de la situation en Iran (JO 2011, L 100, p. 51), qui établit une série de mesures restrictives visant les personnes responsables d'avoir ordonné ou mis en œuvre de graves violations des droits de l'homme en Iran, et celles qui s'en sont rendues complices.

5 La décision 2011/235 a été mise en œuvre par le règlement (UE) nº 359/2011 du Conseil, du 12 avril 2011, concernant des mesures restrictives à l'encontre de certaines personnes, entités et organismes au regard de la situation en Iran (JO 2011, L 100, p. 1), adopté sur le fondement de l'article 215, paragraphe 2, TFUE.

6 L'article 2, paragraphes 1 et 2, du règlement nº 359/2011 dispose :

« 1. Sont gelés tous les fonds et ressources économiques qui appartiennent aux personnes physiques ou morales, entités ou organismes énumérés à l'annexe I, de même que tous les fonds et ressources économiques qu'ils possèdent, détiennent ou contrôlent.

2. Aucun fonds ni aucune ressource économique n'est mis, directement ou indirectement, à la disposition des personnes physiques ou morales, entités ou organismes énumérés à l'annexe I, ni utilisé à leur profit. »

7 Conformément à l'article 3, paragraphes 1 et 2, du règlement nº 359/2011, les personnes qui ont été reconnues par le Conseil comme étant responsables de graves violations des droits de l'homme en Iran ainsi que les personnes, entités et organismes qui leur sont associés sont inscrits sur la liste comprise dans l'annexe I. Cette liste indique les motifs de l'inscription.

8 L'article 12, paragraphes 1 à 3, du règlement nº 359/2011 dispose :

« 1. Lorsque le Conseil décide d'appliquer à une personne physique ou morale, à une entité ou à un organisme les mesures visées à l'article 2, paragraphe 1, il modifie l'annexe I en conséquence.

2. Le Conseil communique sa décision à la personne physique ou morale, à l'entité ou à l'organisme, y compris les motifs de l'inscription sur la liste […] en lui donnant la possibilité de présenter des observations.

3. Si des observations sont formulées, ou si de nouveaux éléments de preuve substantiels sont présentés, le Conseil revoit sa décision et en informe la personne, l'entité ou l'organisme concerné en conséquence. »

9 Le 16 septembre 2022, Mme Mahsa Amini, une Iranienne de 22 ans, est décédée à l'hôpital pendant sa détention par la police des mœurs iranienne. Des manifestations de grande ampleur ont suivi son décès et ont été réprimées par les autorités iraniennes.

10 Le 25 septembre 2022, le haut représentant de l'Union pour les affaires étrangères et la politique de sécurité a fait une déclaration, au nom de l'Union, dans laquelle il déplorait l'usage généralisé et disproportionné de la force contre des manifestants non violents par les forces de sécurité iraniennes. Il y déclarait également que les responsables de la mort de Mme Amini devaient répondre de leurs actes et a appelé les autorités iraniennes à mener des enquêtes transparentes et crédibles afin de clarifier le nombre de décès et d'arrestations, à libérer tous les manifestants non violents et à garantir des procès équitables pour tous les détenus. En outre, il y soulignait que la décision de l'Iran de restreindre sévèrement l'accès à Internet et de bloquer les plateformes de messagerie instantanée constituait une violation flagrante de la liberté d'expression. Enfin, il y a indiqué que l'Union examinerait toutes les options à sa disposition pour réagir à l'homicide de Mme Amini et à la manière dont les forces de sécurité iraniennes avaient répondu aux manifestations qui ont suivi.

11 Le 23 janvier 2023, le Conseil a adopté la décision d'exécution (PESC) 2023/153, mettant en œuvre la décision 2011/235 (JO 2023, L 20 I, p. 23). Le considérant 2 de la décision d'exécution 2023/153 se référait à la déclaration du haut représentant de l'Union pour les affaires étrangères dans les termes repris au point 10 ci-dessus. Le considérant 3 de cette même décision précisait que, « [d]ans ce contexte, et conformément à l'engagement pris par l'Union de traiter tous les sujets

de préoccupation liés à l'Iran, y compris la situation en matière de droits de l'homme, il y a[vait] lieu d'inscrire dix-huit personnes et dix-neuf entités sur la liste des personnes et entités faisant l'objet de mesures restrictives qui figur[ait] à l'annexe de la décision 2011/235 ». L'article 1er de la décision d'exécution 2023/153 prévoyait que l'annexe de la décision 2011/235 était modifiée conformément à sa propre annexe.

12 Au numéro 15 de la liste des entités figurant à l'annexe de la décision d'exécution 2023/153 étaient inscrits, notamment, le nom de la requérante ainsi que les motifs de son inscription dans les termes suivants :

« L'Autorité de régulation des communications est placée sous l'autorité du ministère iranien des technologies de l'information et des communications. Elle met en œuvre les exigences du gouvernement iranien concernant le filtrage des contenus internet grâce à un logiciel espion appelé SIAM.

Au cours des manifestations de 2022, l'Autorité de régulation des communications a mis à profit le contrôle qu'elle exerce sur l'accès à internet et sur les téléphones portables pour suivre les manifestants à la trace et créer un tableau détaillé des activités des dissidents et des manifestants, que les autorités ont utilisé comme elles l'entendaient. L'Autorité de régulation des communications est donc responsable d'avoir soutenu la répression exercée contre des manifestants pacifiques, des journalistes, des défenseurs des droits de l'homme, des étudiants et d'autres personnes qui s'expriment pour défendre leurs droits légitimes.

L'Autorité de régulation des communications est donc responsable de graves violations des droits de l'homme en Iran. »

13 Le même jour, le Conseil a adopté le règlement attaqué sur le fondement de l'article 12, paragraphe 1, du règlement nº 359/2011. Les termes des considérants 2 et 3 du règlement attaqué sont identiques à ceux des considérants 2 et 3 de la décision d'exécution 2023/153, à l'exception de la mention de l'annexe I du règlement nº 359/2011 en lieu et place de l'annexe de la décision 2011/235. L'article 1er du règlement attaqué prévoyait que l'annexe I du règlement nº 359/2011 était modifiée conformément à sa propre annexe.

14 Au numéro 15 de la liste des entités figurant à l'annexe du règlement attaqué étaient inscrits, notamment, le nom de la requérante ainsi que les motifs de cette inscription dans des termes identiques à ceux mentionnés au point 12 ci-dessus.

15 Le 24 janvier 2023, le Conseil a publié au *Journal officiel de l'Union européenne* un avis à l'attention des personnes, entités et organismes auxquels s'appliquent les mesures prévues par la décision 2011/235, mise en œuvre par la décision d'exécution 2023/153, et par le règlement nº 359/2011, mis en œuvre par le règlement attaqué (JO 2023, C 25, p. 8).

16 Cet avis précisait, notamment, que le Conseil avait décidé que les personnes et les entités en question devraient être inscrites sur la liste des personnes et entités faisant l'objet des mesures restrictives prévues par la décision 2011/235 et par le règlement nºº359/2011 et que lesdites personnes et entités pouvaient lui adresser une demande de réexamen de la décision par laquelle elles avaient été inscrites sur les listes susmentionnées, en y joignant des pièces justificatives. Toute demande en ce sens devait être envoyée avant le 15 février 2023 aux coordonnées indiquées dans ce même avis.

Conclusions des parties

17 La requérante conclut à ce qu'il plaise au Tribunal d'annuler le règlement attaqué, en ce qu'il inscrit son nom dans l'annexe I du règlement n°°359/2011.

18 Le Conseil conclut à ce qu'il plaise au Tribunal :

– rejeter le recours ;

– condamner la requérante aux dépens.

En droit

19 À l'appui de son recours, la requérante soulève quatre moyens. Le premier est tiré, en substance, d'un détournement de pouvoir, le deuxième d'une violation de l'obligation de motivation et du droit à une protection juridictionnelle effective, le troisième, en substance, de l'inexactitude matérielle des faits et le quatrième d'une violation du principe de proportionnalité.

20 L'analyse de ces moyens met en évidence qu'il convient d'examiner, dans un premier temps, le deuxième moyen, relatif à la violation de l'obligation de motivation et à une violation du droit à une protection juridictionnelle effective, dans un deuxième temps, le troisième moyen, relatif à une erreur manifeste d'appréciation des faits, dans un troisième temps, le quatrième moyen, relatif à la violation du principe de proportionnalité, puis, dans un quatrième temps, le premier moyen, relatif à un détournement de pouvoir.

Sur le deuxième moyen, tiré d'une violation de l'obligation de motivation et d'une violation du droit à une protection juridictionnelle effective

21 En premier lieu, la requérante fait valoir que, le Conseil n'ayant pas communiqué, concomitamment à l'adoption du règlement attaqué ou immédiatement après cette adoption, les informations ou les éléments de preuve fondant les motifs d'inscription de son nom sur la liste figurant dans l'annexe I du règlement n° 359/2011, il ne se serait pas acquitté de son obligation d'établir le bien-fondé desdits motifs et aurait, par conséquent, violé son obligation de motivation.

22 En deuxième lieu, la requérante soutient que la motivation du règlement attaqué, en ce qui la concerne, consiste en une motivation stéréotypée composée de trois paragraphes succincts de quinze lignes consistant à résumer les suppositions faites par le Conseil en raison de son caractère public. Une telle motivation ne serait pas conforme à la jurisprudence selon laquelle la motivation d'un acte doit permettre, d'une part, à la personne concernée par l'acte litigieux de contester sa validité devant le juge en pleine connaissance de cause de ce qu'on lui reproche et, d'autre part, au juge d'exercer son contrôle juridictionnel de l'acte contesté. Selon la requérante, l'exigence de motivation ne saurait être tempérée par le contexte politique dans lequel une mesure est adoptée, et ce d'autant plus que la contextualisation ne saurait permettre à la requérante de comprendre la portée des mesures restrictives adoptées à son égard et, de manière corrélative, au juge d'opérer le contrôle de la mesure en cause. Le Conseil ne pourrait donc pas violer son obligation de motivation en « s'abritant » derrière des considérations tenant aux intérêts de sécurité et de politique extérieure.

23 En troisième lieu, dans la réplique, la requérante conteste, sur le fondement des articles 47 et 48 de la charte des droits fondamentaux de l'Union européenne (ci-après la « Charte »), la recevabilité du document produit par le Conseil devant le Tribunal en tant qu'élément de preuve à l'appui des motifs invoqués pour justifier l'inscription de son nom à l'annexe I du règlement nº 359/2011. Elle conteste également la pertinence et la force probante des informations contenues dans ledit document.

24 Le Conseil conteste les arguments de la requérante.

25 Il y a lieu de rappeler que, selon une jurisprudence constante, l'obligation de motiver un acte faisant grief, qui constitue le corollaire du principe du respect des droits de la défense, a pour but, d'une part, de fournir à l'intéressé une indication suffisante pour savoir si l'acte est bien-fondé ou s'il est éventuellement entaché d'un vice permettant d'en contester la validité devant le juge de l'Union et, d'autre part, de permettre à ce dernier d'exercer son contrôle sur la légalité de cet acte (voir arrêt du 15 novembre 2012, Conseil/Bamba, C-417/11 P, EU:C:2012:718, point 49 et jurisprudence citée).

26 Il convient également de rappeler que la motivation exigée par l'article 296 TFUE et par l'article 41, paragraphe 2, sous c), de la Charte doit être adaptée à la nature de l'acte en cause et au contexte dans lequel il a été adopté. L'exigence de motivation doit être appréciée en fonction des circonstances de l'espèce, notamment du contenu de l'acte, de la nature des motifs invoqués et de l'intérêt que les destinataires ou d'autres personnes concernées directement et individuellement par l'acte peuvent avoir à recevoir des explications. Il n'est pas exigé que la motivation spécifie tous les éléments de fait et de droit pertinents, dans la mesure où le caractère suffisant d'une motivation doit être apprécié au regard non seulement de son libellé, mais aussi de son contexte ainsi que de l'ensemble des règles juridiques régissant la matière concernée (voir arrêt du 17 septembre 2020, Rosneft e.a./Conseil, C-732/18 P, non publié, EU:C:2020:727, point 77 et jurisprudence citée ; arrêt du 27 juillet 2022, RT France/Conseil, T-125/22, EU:T:2022:483, point 103).

27 Ainsi, d'une part, un acte faisant grief est suffisamment motivé dès lors qu'il est intervenu dans un contexte connu de l'intéressé, qui lui permet de comprendre la portée de la mesure prise à son égard (voir arrêt du 17 septembre 2020, Rosneft e.a./Conseil, C-732/18 P, non publié, EU:C:2020:727, point 78 et jurisprudence citée). D'autre part, le degré de précision de la motivation d'un acte doit être proportionné aux possibilités matérielles et aux conditions techniques ou de délai dans lesquelles celui-ci doit intervenir (voir arrêt du 27 juillet 2022, RT France/Conseil, T-125/22, EU:T:2022:483, point 104 et jurisprudence citée).

28 En outre, la jurisprudence a précisé que la motivation d'un acte du Conseil imposant une mesure restrictive ne devait pas seulement identifier la base juridique de cette mesure, mais également les raisons spécifiques et concrètes pour lesquelles le Conseil considérait, dans l'exercice de son pouvoir discrétionnaire d'appréciation, que l'intéressé devait faire l'objet d'une telle mesure (voir arrêt du 27 juillet 2022, RT France/Conseil, T-125/22, EU:T:2022:483, point 105 et jurisprudence citée).

29 Enfin, il y a lieu de rappeler que l'obligation de motiver un acte constitue une forme substantielle qui doit être distinguée de la question du bien-fondé des motifs, celui-ci relevant de la légalité au fond de l'acte litigieux. En effet, la motivation d'un acte consiste à exprimer formellement les motifs sur lesquels repose cet acte. Si ces motifs sont entachés d'erreurs, celles-ci entachent la

légalité au fond dudit acte, mais non la motivation de celui-ci, qui peut être suffisante tout en exprimant des motifs erronés (voir, en ce sens, arrêt du 13 septembre 2013, Makhlouf/Conseil, T-383/11, EU:T:2013:431, points 73 et 74 et jurisprudence citée).

30 En l'espèce, s'agissant du contexte dans lequel le nom de la requérante a été inscrit à l'annexe I du règlement nº 359/2011, il convient de relever que, ainsi que le souligne à juste titre le Conseil, le considérant 2 du règlement attaqué se référait à la déclaration faite le 25 septembre 2022 au nom de l'Union par le haut représentant de l'Union dont les termes sont rappelés au point 10 ci-dessus.

31 En outre, comme cela est indiqué au point 11 ci-dessus, le considérant 3 du règlement attaqué précise que c'est le contexte rappelé au point 10 ci-dessus et l'engagement de l'Union à traiter tous les sujets de préoccupation liés à l'Iran, y compris la situation en matière de droits de l'homme, qui ont présidé notamment à l'inscription de dix-neuf entités, dont la requérante, sur la liste des personnes physiques et morales, des entités et des organismes faisant l'objet de mesures restrictives qui figure à l'annexe I du règlement nº 359/2011.

32 En particulier, les raisons pour lesquelles le nom de la requérante a été inscrit à l'annexe I du règlement nº 359/2011 étaient énoncées à l'annexe du règlement attaqué dans les termes rappelés au point 12 ci-dessus.

33 Force est de constater que de tels motifs, lus à la lumière des éléments de contexte rappelés aux considérants 2 et 3 du règlement attaqué, exposaient de façon suffisamment spécifique et concrète les raisons pour lesquelles le Conseil estimait, dans l'exercice de son pouvoir discrétionnaire d'appréciation, que la requérante devait faire l'objet d'une mesure restrictive.

34 Il ressort en effet de la motivation du règlement attaqué que la requérante était considérée comme responsable de graves violations des droits de l'homme en Iran pour avoir mis en œuvre les exigences du gouvernement iranien concernant le filtrage des contenus Internet grâce à un logiciel espion appelé SIAM et, en particulier, mis à profit, lors des manifestations de 2022 suivant la mort de Mme Amini, le contrôle qu'elle exerce sur l'accès à Internet et sur les téléphones portables pour suivre les manifestants à la trace et créer un tableau détaillé des activités des dissidents et des manifestants, que les autorités ont utilisé comme elles l'entendaient, soutenant ainsi la répression exercée par lesdites autorités à l'encontre des manifestants qui s'exprimaient pour défendre leurs droits légitimes.

35 Par ailleurs, il y a lieu d'écarter l'argument de la requérante selon lequel le Conseil a manqué à son obligation de motivation dès lors qu'il ne lui a pas transmis concomitamment à l'adoption du règlement attaqué ou immédiatement après cette adoption les éléments de preuve sur lesquels reposent les motifs invoqués pour justifier son inscription à l'annexe I du règlement nº 359/2011 et, partant, n'a pas établi le bien-fondé desdits motifs.

36 En effet, d'une part, pour autant que, par cette argumentation, la requérante entend faire valoir que le Conseil n'a pas rapporté la preuve du bien-fondé des motifs invoqués dans le règlement attaqué pour justifier son inscription à l'annexe I du règlement nº 359/2011, il convient de relever que, conformément à la jurisprudence rappelée au point 29 ci-dessus, cette question doit être distinguée de celle de la motivation du règlement attaqué, qui concerne la légalité externe dudit règlement.

37 D'autre part, pour autant que, par cette même argumentation, la requérante entend faire valoir que le Conseil a violé ses droits de la défense en ce qu'il était tenu de lui fournir d'office un accès aux éléments de son dossier, il importe de relever que le règlement attaqué a été notifié à la requérante par un avis publié au Journal officiel le 24 janvier 2023 qui invitait les personnes et entités concernées à adresser une demande de réexamen au Conseil avant le 15 février 2023 et que la requérante n'a pas formulé une telle demande, ni même demandé au Conseil l'accès à son dossier en dehors de la présente procédure.

38 Or, il convient de rappeler que, s'agissant d'une inscription initiale sur une liste de personnes et d'entités faisant l'objet de mesures restrictives, lorsque des informations suffisamment précises permettant à l'entité intéressée de faire connaître utilement son point de vue sur les éléments retenus à sa charge par le Conseil, ont été communiquées, le principe du respect des droits de la défense n'implique pas l'obligation pour ce dernier de donner spontanément accès aux documents contenus dans son dossier. Ce n'est que sur demande de la partie intéressée que le Conseil est tenu de donner accès à tous les documents administratifs non confidentiels concernant la mesure en cause. La communication spontanée des éléments de dossier constituerait effectivement une exigence excessive, étant donné qu'il n'est pas certain au moment de l'adoption d'une mesure de gel des fonds que l'entité visée entende vérifier, par le biais de l'accès au dossier, les éléments de fait sous-tendant les allégations retenues à sa charge par le Conseil (arrêts du 14 octobre 2009, Bank Melli Iran/Conseil, T-390/08, EU:T:2009:401, point 97, et du 16 septembre 2013, Bank Kargoshaei e.a./Conseil, T-8/11, non publié, EU:T:2013:470, point 68).

39 En l'espèce, il résulte de ce qui précède que, par la motivation du règlement attaqué, la requérante disposait d'informations suffisamment précises pour lui permettre de faire connaître son point de vue sur les éléments retenus à sa charge par le Conseil. Dès lors, ce dernier n'était pas tenu de communiquer d'office à la requérante les éléments contenus dans son dossier.

40 Il importe également de souligner que les arguments de la requérante relatifs à la recevabilité du document produit à l'annexe B.11 et au caractère probant des informations qu'il contient ont trait au bien-fondé des motifs invoqués pour justifier l'inscription de son nom à l'annexe I du règlement n° 359/2011 et sont donc dénués de pertinence au soutien d'un moyen tiré de la violation de l'obligation de motivation. Ces arguments seront ainsi examinés conjointement avec les arguments similaires présentés par la requérante dans le cadre du troisième moyen, tiré d'une erreur manifeste d'appréciation.

41 Par conséquent, il y a lieu de rejeter le deuxième moyen comme non fondé.

Sur le troisième moyen, tiré de l'inexactitude matérielle des faits

42 La requérante soutient que le règlement attaqué est, en ce qui la concerne, entaché d'une « erreur manifeste d'appréciation des faits » dès lors que, d'une part, elle n'a pas la capacité juridique d'accomplir les faits qui lui sont reprochés par le Conseil et, d'autre part, elle n'a pas non plus les capacités techniques de traquer ou de créer un « tableau détaillé » des activités des manifestants.

43 Ainsi, premièrement, la requérante fait valoir que ses statuts ne l'autorisent pas à effectuer une surveillance de masse de la population et encore moins à « tracer » les manifestants. Conformément à ses statuts, la requérante occuperait un rôle de régulateur, de modérateur ou encore de représentant de l'Iran. En outre, la requérante souligne que même si elle souhaitait mettre en place un filtrage, elle ne le pourrait pas puisqu'une telle pratique est juridiquement

encadrée. Ainsi, contrairement à ce que fait valoir le Conseil, en Iran, la collecte de données serait encadrée par de nombreux textes juridiques, notamment l'article 25 de la Constitution, l'article 582 du code pénal iranien, complété par la « loi sur les infractions cyber » du 26 mai 2009, et les articles 104 et 150 du code de procédure pénale iranien. Cet encadrement normatif serait conforme à la résolution du Conseil du 17 janvier 1995 relative à l'interception légale des télécommunications (JO 1996, C 329, p. 1). En outre, il ressortirait de deux rapports réalisés par une société de télécommunications que, contrairement à ce qui a été allégué par le Conseil, les demandes de la requérante ne vont pas au-delà des exigences traditionnelles en matière d'interception légale.

44 Par ailleurs, la requérante soutient qu'il convient de distinguer la surveillance de masse de la surveillance individuelle des personnes. Selon la requérante, la surveillance de masse peut être nécessaire dans toute société afin de maintenir la paix et l'ordre public, notamment en surveillant le flux des personnes et les masses qui se rassemblent. Cela permettrait de prévenir, lors des manifestations publiques, tout débordement lié aux foules. Tout État souverain disposerait de ce pouvoir de surveillance et il ne pourrait être tiré comme conséquence de l'exercice de ce pouvoir des violations de droits humains individuels. Ce pouvoir de surveillance constituerait une prérogative de puissance publique reconnue notamment par la Cour européenne des droits de l'homme.

45 Deuxièmement, selon la requérante, le logiciel qu'elle utilise, dénommé « SIAM » ou « Samaneh yekparche Estehlamate Mokhaberati » en farsi, ne dispose pas de fonctions permettant de surveiller massivement ou individuellement les manifestants sur le territoire iranien.

46 La requérante soutient que le logiciel SIAM est une passerelle d'interface de programmation d'application (API), à savoir un dispositif qui joue un rôle de pont et qui permet à un client externe à une entité d'utiliser des API internes et les services de celles-ci. En Iran, le Croissant-Rouge, les ambulances, les pompiers et les organisations relatives aux routes et à la gestion de crises feraient appel à ce logiciel. Ainsi, selon la requérante, le logiciel SIAM serait utilisé par les centres d'appel, notamment lorsqu'ils sont sollicités par les services d'urgence. Les centres d'appel utiliseraient ce logiciel pour parvenir aux opérateurs de téléphonie mobile qui fourniraient ensuite une localisation seulement approximative de la personne se trouvant dans une situation à risque.

47 Par ailleurs, la requérante souligne qu'elle ne peut pas communiquer directement aux autorités de police et aux autorités judiciaires des informations relatives aux utilisateurs de services de communication car ces informations seraient détenues par les opérateurs titulaires d'une licence d'exploitation du réseau.

48 La requérante conteste, enfin, les arguments avancés par le Conseil dans son mémoire en défense concernant les prétendus « composants fonctionnels » du système d'interception de l'Iran.

49 Ainsi, la requérante fait valoir que le Conseil se méprend sur les fonctionnalités du logiciel SIAM, « Force2GNumber », « LocationCustomerList », « GetCDR », « GetIPDR » et « ApplySusplp », auxquelles il se réfère dans le mémoire en défense. La requérante explique que la description de ces fonctions par le Conseil, qui repose uniquement sur l'article du journal d'investigation en ligne *The Intercept*, ne correspond pas à la réalité. Selon la requérante, il s'agit des commandes classiques et ordinaires à disposition d'un organe de régulation des télécommunications d'un État

et l'intégralité des États membres de l'Union dispose d'outils similaires. Il en irait de même en ce qui concerne les systèmes « Legal Intercept » (LI), « Control Illegal Devices » (CID), « SHAHKAR » et « SHAMSA ».

50 En outre, dans la réplique, la requérante conteste la recevabilité de l'article intitulé « Hacked documents : How Iran track and control protesters phones », publié le 28 octobre 2022 par *The Intercept*, produit par le Conseil à l'annexe B.11 (ci-après l'« article de *The Intercept* »). Selon la requérante, les faits allégués dans cet article reposent sur une série de documents internes d'un opérateur mobile iranien qui n'ont pas été versés à la procédure devant le Tribunal et le Conseil se contente d'affirmer que les auteurs de cet article auraient eu accès à des documents qui leur auraient été communiqués « par une personne [affirmant] avoir piraté un opérateur mobile iranien ». Cet article, qui constituerait la pièce maîtresse du dossier du Conseil, ne serait donc qu'une preuve par ouï-dire. Or, conformément à la jurisprudence de la Cour relative aux articles 47 et 48 de la Charte ainsi qu'à la jurisprudence de la Cour européenne des droits de l'homme relative à l'article 6 de la convention de sauvegarde des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950, les dépositions de témoins ensuite absents à l'audience qui sont insusceptibles d'être examinées par la partie adverse sont en principe interdites, sauf si l'accusation justifie suffisamment le besoin d'utiliser leurs témoignages et si d'autres garanties procédurales sont accordées à l'accusé, ainsi que l'existence d'autres preuves à charge contre lui. La Cour aurait également jugé dans l'arrêt du 8 décembre 2022, HYA e.a. (Impossibilité d'interroger les témoins à charge) (C-348/21, EU:C:2022:965), que, en cas d'impossibilité d'interroger les témoins à charge, la force probante de leurs témoignages doit être relativisée même si de tels témoignages sont recevables.

51 Il s'ensuivrait que, en fondant le règlement attaqué sur les prétendues affirmations d'une personne inconnue, le Conseil aurait agi en violation des articles 47 et 48 de la Charte, ce qui imposerait de rejeter cette offre de preuve comme irrecevable.

52 La requérante fait également valoir dans la réplique que, en vertu du principe du contradictoire, le juge ne peut prendre en considération que les actes de procédure et les pièces dont les parties ont pu prendre connaissance et sur lesquels elles ont pu se prononcer. Or, le Conseil aurait lui-même reconnu que l'opérateur mobile iranien cité dans l'article de *The Intercept* n'a pas répondu à la demande de commentaire des journalistes.

53 Le Conseil conteste l'argumentation de la requérante.

54 Il convient de relever que, dans le cadre du troisième moyen, la requérante conteste le bien-fondé des motifs invoqués pour justifier son inscription à l'annexe I du règlement n° 359/2011. Elle soutient en effet qu'elle n'a ni la capacité juridique, ni la capacité technique de se livrer aux activités qui lui sont reprochées.

55 Toutefois, il convient également de relever que, ainsi qu'il ressort du point 23 ci-dessus, dans le cadre du deuxième moyen, la requérante fait grief au Conseil de violer les articles 47 et 48 de la Charte, et de renverser la charge de la preuve, en fondant son appréciation sur l'article de *The Intercept* dès lors que, en l'absence de versement des documents mentionnés dans cette publication au dossier de la présente procédure, les faits et propos relatés dans cet article ne constituent que des allégations à l'égard desquelles la requérante se trouve privée de la possibilité d'exercer ses droits de la défense. La requérante fait également valoir dans le mémoire en réplique que l'absence d'éléments de preuve versés au dossier dans le cadre de la présente procédure porte

atteinte au respect du principe du contradictoire visé à l'article 85, paragraphe 1, du règlement de procédure du Tribunal. La requérante souligne, en outre, l'absence de valeur probante d'une telle publication.

56 Il convient d'examiner les arguments de la requérante tirés de la violation des articles 47 et 48 de la Charte ainsi que de la violation du principe du contradictoire avant d'examiner ceux concernant la valeur probante de l'article de *The Intercept*, puis les arguments relatifs à une « erreur manifeste d'appréciation des faits ».

Sur la violation des articles 47 et 48 de la Charte et du principe du contradictoire

57 Tout d'abord, il convient d'écarter l'argument de la requérante selon lequel l'article de *The Intercept* produit par le Conseil à l'annexe B.11 du mémoire en défense devrait être rejeté comme irrecevable au motif, en substance, qu'il ne lui serait pas possible de se défendre contre de simples allégations, ce qui porterait atteinte à ses droits de la défense devant le Tribunal.

58 Il importe de relever que la question de la recevabilité des offres de preuve devant le Tribunal, qui est régie par l'article 85 du règlement de procédure, doit être distinguée de la question de l'appréciation des preuves par le juge de l'Union.

59 À cet égard, il convient de rappeler que, selon la jurisprudence de la Cour, lors du contrôle de mesures restrictives, les juridictions de l'Union doivent assurer un contrôle en principe complet de la légalité de l'ensemble des actes de l'Union au regard des droits fondamentaux faisant partie intégrante de l'ordre juridique de l'Union (voir, en ce sens, arrêts du 18 juillet 2013, Commission e.a./Kadi, C-584/10 P, C-593/10 P et C-595/10 P, EU:C:2013:518, point 97 ; du 28 novembre 2013, Conseil/Fulmen et Mahmoudian, C-280/12 P, EU:C:2013:775, point 58, et du 28 mars 2017, Rosneft, C-72/15, EU:C:2017:236, point 106).

60 Au rang de ces droits fondamentaux figurent, notamment, le respect des droits de la défense et le droit à une protection juridictionnelle effective (voir arrêt du 28 novembre 2013, Conseil/Fulmen et Mahmoudian, C-280/12 P, EU:C:2013:775, point 59 et jurisprudence citée ; arrêt du 28 novembre 2013, Conseil/Manufacturing Support & Procurement Kala Naft, C-348/12 P, EU:C:2013:776, point 66).

61 L'effectivité du contrôle juridictionnel garanti par l'article 47 de la Charte exige que, au titre du contrôle de la légalité des motifs sur lesquels est fondée la décision d'inscrire ou de maintenir le nom d'une personne ou d'une entité sur la liste des personnes et des entités faisant l'objet de mesures restrictives, le juge de l'Union s'assure que cette décision, qui revêt une portée individuelle pour cette personne ou pour cette entité, repose sur une base factuelle suffisamment solide. Cela implique une vérification des faits allégués dans l'exposé des motifs qui sous-tend ladite décision, de sorte que le contrôle juridictionnel ne soit pas limité à l'appréciation de la vraisemblance abstraite des motifs invoqués, mais porte sur la question de savoir si ces motifs, ou à tout le moins l'un d'eux considéré comme suffisant en soi pour soutenir lesdits actes, sont étayés (voir, en ce sens, arrêts du 18 juillet 2013, Commission e.a./Kadi, C-584/10 P, C-593/10 P et C-595/10 P, EU:C:2013:518, point 119 ; du 18 juin 2015, Ipatau/Conseil, C-535/14 P, EU:C:2015:407, point 42, et du 18 février 2016, Conseil/Bank Mellat, C-176/13 P, EU:C:2016:96, point 109).

62 Dans ce cadre, c'est en effet à l'autorité compétente de l'Union qu'il appartient, en cas de contestation, d'établir le bien-fondé des motifs retenus à l'encontre de la personne ou de l'entité concernée, et non à ces dernières d'apporter la preuve négative de l'absence de bien-fondé desdits motifs (voir, en ce sens, arrêt du 18 juillet 2013, Commission e.a./Kadi, C-584/10 P, C-593/10 P et C-595/10 P, EU:C:2013:518, point 121).

63 Toutefois, contrairement à ce que soutient la requérante, il ne s'ensuit pas que la prétendue incapacité du Conseil à rapporter la preuve que les motifs invoqués pour justifier l'inscription de la requérante à l'annexe I du règlement nº 359/2011, à la supposer avérée, porterait atteinte aux droits de la défense de la requérante.

64 En effet, ainsi que cela ressort de la jurisprudence rappelée au point 61 ci-dessus, c'est au contraire parce que la préservation de l'effectivité de l'article 47 de la Charte l'exige que le juge de l'Union est tenu de vérifier, dans le cadre du contrôle de légalité des mesures restrictives, le bien-fondé des motifs qui sous-tendent ces mesures et, partant, la valeur probante des documents produits, en l'espèce, par le Conseil.

65 Ensuite, il convient d'écarter comme dénuées de pertinence en l'espèce les considérations, invoquées par la requérante, exposées dans l'arrêt du 8 décembre 2022, HYA e.a. (Impossibilité d'interroger les témoins à charge) (C-348/21, EU:C:2022:965), dans lequel la Cour était interrogée sur l'interprétation de l'article 6, paragraphe 1, et de l'article 8, paragraphe 1, de la directive (UE) 2016/343 du Parlement européen et du Conseil, du 9 mars 2016, portant renforcement de certains aspects de la présomption d'innocence et du droit d'assister à son procès dans le cadre des procédures pénales (JO 2016, L 65, p. 1), ainsi que de l'article 47, deuxième alinéa, de la Charte.

66 Il doit être rappelé que le principe de la présomption d'innocence, énoncé à l'article 6, paragraphe 2, de la convention de sauvegarde des droits de l'homme et des libertés fondamentales et à l'article 48, paragraphe 1, de la Charte, constitue un droit fondamental qui confère aux particuliers ou aux entités dirigées par des particuliers des droits dont le juge de l'Union garantit le respect (voir arrêt du 18 mai 2017, Makhlouf/Conseil, T-410/16, non publié, EU:T:2017:349, point 122 et jurisprudence citée).

67 Le principe de la présomption d'innocence, qui exige que toute personne accusée d'une infraction soit présumée innocente jusqu'à ce que sa culpabilité ait été légalement établie, ne s'oppose pas à l'adoption de mesures conservatoires de gel de fonds, dès lors que celles-ci n'ont pas pour objet d'engager une procédure pénale à l'encontre de la personne ou de l'entité visée. De telles mesures doivent cependant, compte tenu de leur gravité, être prévues par la loi, être adoptées par une autorité compétente et présenter un caractère limité dans le temps. Il résulte du point 13 ci-dessus que ces deux premiers critères sont remplis. En outre, s'agissant du caractère limité dans le temps, il convient de constater que, conformément à l'article 12, paragraphes 3 et 4, du règlement nº 359/2011, l'annexe I de ce même règlement est examinée à intervalles réguliers et au moins tous les douze mois, l'inscription d'une personne ou d'une entité à ladite annexe pouvant être prorogée ou modifiée le cas échéant. Les mesures imposées à la requérante ont donc bien un caractère limité dans le temps (voir, en ce sens, arrêt du 18 mai 2017, Makhlouf/Conseil, T-410/16, non publié, EU:T:2017:349, point 123 et jurisprudence citée).

68 De plus, il y a lieu de relever que les mesures restrictives en cause n'entraînent pas une confiscation des avoirs de la requérante en tant que produit du crime, mais un gel à titre conservatoire. Ces mesures ne constituent donc pas une sanction et n'impliquent par ailleurs aucune accusation de cette nature (voir arrêt du 18 mai 2017, Makhlouf/Conseil, T-410/16, non publié, EU:T:2017:349, point 124 et jurisprudence citée).

69 En effet, le règlement attaqué, en ce qu'il concerne la requérante, ne constitue pas une constatation du fait qu'une infraction a été effectivement commise, mais a été adopté dans le cadre et aux fins d'une procédure de nature administrative ayant une fonction conservatoire et ayant pour unique but de permettre au Conseil de garantir la protection des populations civiles (voir, en ce sens, arrêt du 18 mai 2017, Makhlouf/Conseil, T-410/16, non publié, EU:T:2017:349, point 125 et jurisprudence citée).

70 Enfin, il convient de rejeter également l'argument de la requérante selon lequel, en l'absence de versement au dossier de la présente affaire des documents dont il est fait mention dans l'article de *The Intercept*, cet article devrait être rejeté comme irrecevable au motif que, en vertu du principe du contradictoire, le juge ne peut prendre en considération que les actes de procédure et les pièces dont les parties ont pu prendre connaissance et sur lesquels elles ont pu se prononcer. En effet, il suffit de relever à cet égard que la requérante a eu l'occasion de prendre position dans son mémoire en réplique sur les éléments de preuve produits par le Conseil à l'annexe B.11, notamment cet article, dont elle conteste d'ailleurs la valeur probante.

71 Par ailleurs, il importe de relever que les deux manuels d'utilisation du logiciel SIAM rédigés, le premier, en farsi et, le second, en anglais étaient consultables directement depuis l'article de *The Intercept* via un hyperlien figurant en page 3 du dossier WK 307/2023 INIT produit par le Conseil à l'annexe B.11 du mémoire en défense.

72 Il convient donc de rejeter les griefs de la requérante tirés de la violation des articles 47 et 48 de la Charte et du principe du contradictoire.

Sur la valeur probante de l'article de The Intercept

73 La requérante fait grief à l'article de *The Intercept* d'être une simple publication journalistique contenant uniquement des allégations invérifiables et d'être, partant, dépourvu de toute force probante.

74 À cet égard, il convient de rappeler que, conformément à une jurisprudence constante, l'activité de la Cour et du Tribunal est régie par le principe de libre appréciation des preuves et que le seul critère pour apprécier la valeur des preuves produites réside dans leur crédibilité. En outre, pour apprécier la valeur probante d'un document, il convient de vérifier la vraisemblance de l'information qui y est contenue et de tenir compte, notamment, de l'origine du document, des circonstances de son élaboration, de son destinataire et de se demander si, d'après son contenu, il semble sensé et fiable (voir arrêt du 31 mai 2018, Kaddour/Conseil, T-461/16, EU:T:2018:316, point 107 et jurisprudence citée).

75 En l'absence de pouvoirs d'enquête dans des pays tiers, l'appréciation des autorités de l'Union doit, de fait, se fonder sur des sources d'information accessibles au public, des rapports, des articles de presse, des rapports des services secrets ou d'autres sources d'information similaires (arrêts du 14 mars 2018, Kim e.a./Conseil et Commission, T-533/15 et T-264/16, EU:T:2018:138, point 107, et du 1er juin 2022, Prigozhin/Conseil, T-723/20, non publié, EU:T:2022:317, point 59).

76 En effet, il serait excessif et disproportionné d'exiger du Conseil qu'il mène lui-même des investigations sur le terrain concernant la véracité des faits qui sont relayés par de nombreux médias (arrêt du 25 janvier 2017, Almaz-Antey Air and Space Defence/Conseil, T-255/15, non publié, EU:T:2017:25, point 148).

77 Des articles de presse peuvent donc être utilisés aux fins de corroborer l'existence de certains faits lorsqu'ils émanent de plusieurs sources différentes et qu'ils sont suffisamment concrets, précis et concordants quant aux faits qui y sont décrits (voir arrêt du 11 septembre 2019, Topor-Gilka et WO Technopromexport/Conseil, T-721/17 et T-722/17, non publié, EU:T:2019:579, point 137 et jurisprudence citée).

78 En l'espèce, le Conseil a fondé l'inscription de la requérante à l'annexe I du règlement nº 359/2011 sur quatre documents du dossier WK 307/2023 INIT qui figurent à l'annexe B.11 du mémoire en défense.

79 Il s'agit, premièrement, de l'article de *The Intercept* ; deuxièmement, de l'article intitulé « Hacker Leaks Manuals Showing How Iran Uses Mobile Networks to Track Protesters », publié le 31 octobre 2022 par le site Internet spécialisé Commrisk ; troisièmement, de l'article intitulé « Iran : New tactics for digital repression as protests continue », publié le 17 novembre 2022 sur le site Internet de l'association ARTICLE 19 ; et, quatrièmement, de l'article intitulé « Iran is using spyware to track citizens attending protests », publié par le journal d'investigation en ligne *The Tech Monitor* le 3 novembre 2022.

80 La requérante fait valoir que le Conseil fonde le règlement attaqué en ce qui la concerne sur les seules allégations contenues dans l'article de *The Intercept*, elles-mêmes fondées sur les dires d'une personne anonyme.

81 Il y a lieu d'observer que l'article de *The Intercept* révèle que, sur la base de documents internes à un opérateur mobile iranien, notamment des échanges de courriels impliquant les dirigeants de la requérante et deux manuels, l'un en anglais, l'autre en farsi, d'utilisation d'un logiciel dénommé SIAM, les auteurs de cet article ont découvert comment les autorités iraniennes, au travers de la requérante, avaient mis en place un système fonctionnant en arrière-plan des réseaux mobiles iraniens qui permettait au gouvernement iranien de contourner le système de cryptage des appels, de suivre les déplacements d'un utilisateur de téléphone, d'identifier tous les téléphones se trouvant à un endroit donné, d'analyser tous les contacts d'un utilisateur de téléphone et d'interrompre ou de ralentir la connexion Internet de l'utilisateur et qui avait été utilisé pour réprimer et contrôler la population iranienne à la suite de la mort de M^me^ Amini en 2022. Cet article explique également que le manuel d'utilisation du logiciel SIAM rédigé en anglais précise que, « [s]elon les règles et réglementations de la [requérante], tous les opérateurs de télécommunications doivent fournir à [celle-ci] un accès direct à leur système pour interroger (sic) les informations des clients et modifier leurs services via le service web » et contient, en outre, des informations techniques sur les commandes les plus puissantes utilisées par le logiciel SIAM pour collecter des données sur les utilisateurs directement chez les opérateurs mobiles iraniens.

82 Il convient également d'observer que les auteurs de l'article de *The Intercept* ont pris soin d'interroger deux personnes présentées comme des experts.

83 À cet égard, il importe de souligner que, contrairement à ce que soutient la requérante, la première personne présentée comme un expert n'est pas « quelqu'un que personne ne connaît et qui ne semble disposer d'aucune légitimité particulière ». Il ressort en effet du dossier que cette première personne est chercheur au CitizenLab Canada, laboratoire interdisciplinaire basé à l'université de Toronto (Canada) spécialisé dans « la recherche, le développement, la politique stratégique de haut niveau et l'engagement juridique à l'intersection des technologies de l'information et de la communication, des droits de l'homme et de la sécurité mondiale », et qu'elle a déjà été présentée en tant que tel dans un article publié le 1er février 2022 par le journal renommé *The Guardian.*

84 De la même manière, il ressort du dossier que la seconde personne présentée comme un expert dans l'article de *The Intercept* se présente et a été présentée à de nombreuses reprises par l'agence de presse internationale Reuters comme le directeur des droits numériques et de la sécurité au sein du MIAAN group, une organisation basée au Texas (États-Unis) qui « défend les droits de l'homme en Iran ». Contrairement à ce que soutient la requérante, la simple circonstance qu'il est « notoire qu'[il s'agit d']un personnage public engagé ouvertement et sans réserve contre le gouvernement iranien » ne saurait nécessairement priver ses déclarations de pertinence, au motif qu'il n'est pas neutre et impartial.

85 À cet égard, il convient de relever que l'expérience d'une telle personne, spécialisée dans la défense des droits de l'homme, en particulier des droits numériques, et qui est qualifiée d'opposant au régime iranien par la requérante elle-même, est pertinente pour donner un avis utile sur la façon dont les autorités iraniennes pourraient utiliser un système tel que celui décrit dans l'article de *The Intercept* pour porter atteinte auxdits droits.

86 Par ailleurs, il importe de souligner que l'article publié sur le site de *The Intercept* ne se limitait pas à la formulation de simples allégations, ni même à la reproduction de l'opinion d'experts, mais étayait ses allégations et opinions par la mise à disposition du manuel d'utilisation du logiciel SIAM rédigé en anglais, qu'il permettait de consulter directement dans une fenêtre de visualisation, et du second manuel rédigé en farsi sur lequel apparaissait le logo de la requérante.

87 En outre, s'agissant des autres articles contenus dans le dossier WK 307/2023 INIT, il convient de relever que le site Internet Commrisk, qui se décrit comme « un site web qui rend compte des risques auxquels sont confrontés les fournisseurs de communications électroniques et leurs clients », et *The Tech Monitor*, qui se définit comme visant à fournir « des informations fondées sur des données et des analyses faisant autorité aux chefs d'entreprise, aux responsables numériques et aux responsables politiques dans un monde perturbé et inspiré par la technologie », sont des médias spécialisés dans le domaine des télécommunications et que l'association ARTICLE 19, basée à Londres (Royaume-Uni), se décrit comme « une organisation internationale de réflexion qui soutient le mouvement en faveur de la liberté d'expression au niveau local et mondial afin de garantir que tous les individus réalisent le pouvoir de leur voix », de sorte qu'ils doivent être regardés comme des sources d'informations pertinentes dans l'usage des technologies de l'information et de la communication avec l'exercice des droits fondamentaux et, en particulier, du droit à la liberté d'expression.

88 Si les articles de Commrisk, ARTICLE 19 et *The Tech Monitor* se réfèrent tous les trois à l'article de *The Intercept*, l'article de Commrisk fait également état de l'expérience de son auteur qui aurait rencontré le représentant d'une société technologique qui essayait de vendre à l'Iran un logiciel possédant des fonctions « étrangement similaires » à celles du logiciel SIAM et qui lui avait volontairement fourni des informations au sujet de cette vente.

89 De plus, il ressort de l'article de l'association ARTICLE 19 que cette dernière a surveillé la portée des contrôles exercés sur Internet en Iran depuis plusieurs années et qu'elle a révélé dans un rapport intitulé « Iran Tightening the Net 2020 » le fonctionnement de l'infrastructure d'Internet dans ce pays et sa gouvernance par les autorités. En particulier, il existerait un système centralisé permettant de couper l'accès à Internet lors des manifestations au cours desquelles la gouvernance d'Internet serait considérée comme une question de sécurité nationale. L'association ARTICLE 19 aurait découvert que la requérante, sous le contrôle du ministère des Communications, qui serait en réalité contrôlé par les services de renseignements iraniens, mettrait en œuvre des équipements de surveillance et de censure au niveau des fournisseurs d'accès à Internet et ordonnerait des coupures et d'autres perturbations de l'accès à Internet pour le compte du Conseil suprême national de sécurité. L'article de l'association ARTICLE 19 fait également état de l'usage par les autorités iraniennes de technologies bloquant l'utilisation des outils permettant de contourner la censure d'Internet, tels les réseaux privés virtuels (VPN), ainsi que de coupures ou de sévères perturbations des connexions à l'internet mobile comme tactiques de répression digitale. Ainsi, les coupures d'accès à l'internet mobile seraient de plus en plus utilisées depuis novembre 2019. De telles coupures auraient été particulièrement utilisées pendant les manifestations régionales depuis 2021 jusqu'à présent. Il est ainsi indiqué que les connexions à l'internet mobile ont été désactivées dans de nombreux endroits la plupart des jours qui ont suivi les manifestations faisant suite à la mort de M^me^ Amini. Ces coupures auraient affecté les plus grands fournisseurs d'accès à l'internet mobile à travers le pays, ce qui, dans un pays où l'internet mobile constitue la principale source d'accès à Internet pour la population, aurait eu un impact négatif sur l'accès à Internet.

90 Il résulte ainsi de ce qui précède que les allégations énoncées dans l'article de *The Intercept* sont corroborées par les autres éléments de preuve composant le dossier WK 307/2023 INIT et que, par conséquent, contrairement à ce que soutient la requérante, le Conseil ne s'est pas fondé uniquement sur les allégations énoncées dans cet article. Partant, eu égard à la concordance des différents éléments de preuve et aux circonstances susmentionnées de leur élaboration, lesdites allégations pouvaient valablement être prises en compte.

Sur le bien-fondé de l'inscription du nom de la requérante

91 À titre liminaire, il importe de relever que si la requérante fait valoir que le Conseil a commis en l'espèce une « erreur manifeste d'appréciation des faits », les arguments qu'elle avance à cet égard doivent être regardés comme consistant en une contestation de l'exactitude matérielle des faits qui lui sont reprochés. En effet, il résulte de son argumentation développée au soutien du présent moyen, rappelée au point 42 ci-dessus, que la requérante ne conteste pas que les faits qui lui sont reprochés puissent être couverts par les critères d'inscription prévus à l'article 3, paragraphes 1 et 2, du règlement n° 359/2011, mais la réalité desdits faits.

92 À cet égard, il résulte de la jurisprudence rappelée au point 62 ci-dessus que le contrôle du juge de l'Union implique une vérification des faits allégués dans l'exposé des motifs qui sous-tend la décision adoptant des mesures restrictives concernant une entité et que cette vérification ne se limite pas à l'appréciation de la vraisemblance abstraite des motifs invoqués, mais porte sur la question de savoir si ces motifs, ou à tout le moins l'un d'eux considéré comme suffisant en soi pour soutenir cette même décision, sont étayés.

93 L'appréciation du bien-fondé de ces motifs doit être effectuée en examinant les éléments de preuve et d'information non de manière isolée, mais dans le contexte dans lequel ils s'insèrent. En effet, le Conseil satisfait à la charge de la preuve qui lui incombe s'il fait état devant le juge de

l'Union d'un faisceau d'indices suffisamment concrets, précis et concordants permettant d'établir l'existence d'un lien suffisant entre la personne sujette à une mesure restrictive et le régime ou, en général, les situations combattues (voir, en ce sens, arrêt du 20 juillet 2017, Badica et Kardiam/Conseil, T-619/15, EU:T:2017:532, point 99 et jurisprudence citée).

94 C'est à la lumière de ces considérations qu'il convient de vérifier si le Conseil a pu considérer à bon droit, lors de l'adoption de l'acte attaqué, que la requérante pouvait être visée par des mesures restrictives.

95 À cet égard, premièrement, s'agissant des dispositions de droit iranien invoquées par la requérante pour justifier qu'elle se trouverait juridiquement empêchée de surveiller et de contrôler les communications des utilisateurs des réseaux mobiles iraniens, il convient de relever que, aux termes de l'article 25 de la Constitution de la République islamique d'Iran, « [l]'inspection et la non-livraison des lettres, l'enregistrement et la divulgation des conversations téléphoniques, la divulgation des communications télégraphiques et télex, la censure, […] les écoutes clandestines et toute forme de surveillance sont interdits, sauf conformément à la loi ».

96 L'article 582 du code pénal iranien dispose :

« Le fait pour un officier d'État ou un fonctionnaire, dans des cas autres que ceux autorisés par la loi, d'accéder à, de saisir, de détruire, d'inspecter, d'enregistrer ou d'intercepter des lettres ou des communications télégraphiques ou téléphoniques des personnes, ou de divulguer leur contenu sans l'autorisation de leur propriétaire, est puni d'une peine d'emprisonnement d'un an à trois ans ou d'une amende de six à dix-huit millions de [r]ials. »

97 L'article 104 du code de procédure pénale iranien dispose :

« Le contrôle [l'interception] des télécommunications des individus est interdit, sauf dans les cas où il est lié à la sécurité intérieure ou extérieure du pays ou est jugé nécessaire pour l'enquête sur les crimes énumérés à l'article 302(a), (b), (c) et (d) du présent code. Dans ce cas, l'interception est effectuée avec l'approbation du président de la Cour suprême de la province et la détermination de la durée et de la fréquence de l'interception. L'interception des conversations téléphoniques des personnes et des fonctionnaires énumérés à l'article 307 du présent code est soumise à l'approbation du président de la Cour suprême, et cette autorité ne peut être déléguée à d'autres personnes. »

98 Il ressort de ces dispositions que si l'interception des communications est en principe interdite, elle reste toutefois légalement possible, notamment « dans des cas où elle est liée à la sécurité intérieure ou extérieure du pays ou est jugée nécessaire pour [certains crimes] » ou lorsque « l'affaire est liée à la sécurité du pays ». À cet égard, il convient d'ailleurs d'observer que les hypothèses dans lesquelles l'interception des télécommunications est légalement possible sont définies de façon très large.

99 En outre, il convient de relever que la thèse de la requérante est également contredite par le manuel d'utilisation du logiciel SIAM rédigé en anglais, dont elle ne conteste d'ailleurs pas l'authenticité, dans lequel il est indiqué que, « selon les règles et réglementations de la [requérante], tous les opérateurs de télécommunications doivent fournir à [celle-ci] un accès direct à leur système pour interroger (sic) les informations des clients et modifier leurs services via le service web ».

100 Deuxièmement, s'agissant de la prétendue incapacité technique de la requérante à conduire des opérations de surveillance et de contrôle sur les utilisateurs des réseaux mobiles iraniens, force est de constater que ce n'est pas le cas.

101 Il importe ainsi de souligner que la requérante ne conteste pas l'existence du logiciel SIAM, ni des commandes « Force2GNumber », « LocationCustomerList », « GetCDR », « GetIPDR » et « ApplySusplp » ou des systèmes « Legal Intercept » (LI), « Control Illegal Devices » (CID), « SHAHKAR » et « SHAMSA ». La requérante ne conteste pas non plus le fait qu'elle utilise le logiciel SIAM ainsi que lesdits systèmes. La requérante ne conteste pas davantage l'authenticité des échanges de courriels entre ses dirigeants et l'opérateur mobile iranien cité dans l'article de *The Intercept*, ni celle des manuels d'utilisation du logiciel SIAM, le premier rédigé en anglais et le second en farsi.

102 En effet, la requérante se borne à faire valoir que, d'une part, l'utilisation de ces commandes soit ne produit pas l'effet décrit par le Conseil soit répond à un objectif légitime et, d'autre part, les systèmes « Legal Intercept » (LI), « Control Illegal Devices » (CID), « SHAHKAR » et « SHAMSA » sont communs dans la plupart des États.

103 À cet égard, il convient de rappeler qu'il est indiqué dans le manuel d'utilisation du logiciel SIAM rédigé en anglais que, « [s]elon les règles et réglementations de la [requérante], tous les opérateurs de télécommunications doivent fournir à [celle-ci] un accès direct à leur système pour interroger (sic) les informations des clients et modifier leurs services via le service web ».

104 Il convient en outre de relever que, selon la traduction française fournie par le Conseil, il est indiqué dans l'introduction du manuel d'utilisation du logiciel SIAM rédigé en farsi que l'objectif de ce logiciel est de « créer un système centralisé, unique et réunifié pour effectuer des requêtes auprès des différents serveurs » et de « permettre la gestion et le contrôle sur les communications et sur l'action des utilisateurs ».

105 De plus, il est indiqué dans la partie « Principes de communications » de ce même manuel que « les paramètres d'entrée sont dans les informations envoyées par le logiciel SIAM concernant chaque méthode (fonction) de requête à l'opérateur et [que] les paramètres de sortie sont les données de réponse à la requête (et l'ordre de leur classification) [et que l]es opérateurs doivent renvoyer au SIAM la réponse de chaque fonction demandée précisément selon l'ordre et la composition décrites dans la partie consacrée aux paramètres de sortie de ladite fonction ».

106 En outre, il est précisé, toujours dans ce manuel, que les opérateurs sont tenus « de répondre jour et nuit (7X24) aux requêtes du logiciel SIAM » et de s'assurer que « tous les équipements nécessaires en matière d'ordinateur, de logiciel, de communication de réseau et de sécurité tel[s] que la [r]edondance des données (Redundancy), la répartition de charge (Road Balancing), les pare-feu (Firewall) et toutes les autres nécessités sont réunis ».

107 Il découle de ces constatations que les commandes du logiciel SIAM sont adressées à tous les opérateurs mobiles iraniens et que ceux-ci sont tenus d'y répondre de la façon prescrite à tout moment.

108 C'est à la lumière de ces constatations qu'il convient d'apprécier les arguments de la requérante relatifs aux commandes du logiciel SIAM et aux systèmes « Legal Intercept » (LI), « Control Illegal Devices » (CID), « SHAHKAR » et « SHAMSA ».

109 Ainsi, s'agissant de la commande « LocationCustomerList », la requérante soutient que celle-ci ne permet pas de suivre avec précision un utilisateur de réseau mobile particulier puisqu'elle permettrait uniquement d'identifier les utilisateurs d'un réseau mobile dans une zone allant de 200 mètres à 2 kilomètres autour d'une antenne relais GSM. Toutefois, force est de constater que la requérante admet que cette commande permet d'identifier tous les utilisateurs d'un réseau mobile se trouvant dans une certaine zone géographique, même si celle-ci est approximative. C'est d'ailleurs ce qui ressort clairement de la description de cette commande dans le manuel d'utilisation du logiciel SIAM rédigé en anglais, dans lequel il est indiqué que « cette fonction, qui reçoit un paramètre de lieu, devrait fournir une liste des numéros qui se trouvent dans ce lieu ». En outre, il y a lieu de relever qu'il ressort du manuel rédigé en farsi que la commande « IdentitySearch » impose aux opérateurs d'envoyer les résultats sous forme d'un « tableau » dans lequel sont indiqués, pour ce qui concerne les personnes physiques, le numéro de téléphone, le prénom, le nom, le prénom du père, le numéro d'acte de naissance, la date de naissance, le code postal, la nationalité, le numéro de passeport, l'adresse ou les adresses postales, le type de paiement (prépayé/paiement postérieur), le type de ligne (carte SIM ou autre), la date d'octroi, l'adresse IP ainsi que la longitude géographique et la latitude géographique de l'adresse.

110 S'agissant de la commande « Force2GNumber », la requérante soutient que, contrairement à ce que fait valoir le Conseil, celle-ci n'augmenterait pas les risques de piratage des communications. Toutefois, ainsi que le fait justement observer le Conseil, la circonstance, à la supposer avérée, que cette commande n'augmente pas le risque de piratage ne remet pas en cause le constat qu'une telle commande, qui vise à forcer un téléphone mobile à utiliser le réseau 2G en lieu et place des 3G et 4G plus récents, a pour effet de rendre impossibles le visionnage et le partage de vidéos à partir de ce téléphone.

111 S'agissant des commandes « GetCDR » et « GetIPDR », la requérante soutient que celles-ci servent, pour la première, à consulter l'historique d'un téléphone et, pour la seconde, à obtenir l'adresse IP des appareils dans lesquels une certaine carte SIM a été activée. Selon la requérante, ces fonctions servent exclusivement à répondre à des demandes d'instructions judiciaires et sont des outils essentiels mis à la disposition des juridictions, ce dont témoignent les ordonnances judiciaires et les courriers de la police joints en annexe à la réplique. Toutefois, d'une part, il y a lieu de relever que la requérante ne fournit aucun élément de preuve de nature à démontrer que cette commande ne pourrait être utilisée que pour les réponses aux demandes légitimes des juridictions iraniennes et des autorités de police. D'autre part, ainsi qu'il a déjà été relevé au point 98 ci-dessus, les hypothèses dans lesquelles l'interception des télécommunications est légalement possible sont définies de façon très large.

112 S'agissant des commandes « ApplySusp » et « ApplySuspIP », la requérante soutient que celles-ci permettent de mettre hors service les cartes SIM qui sont déclarées comme perdues ou volées par les usagers ou appartenant à des personnes qui sont déclarées comme décédées. La requérante souligne que cette capacité est tout à fait classique et comparable à celle des organes de régulation d'autres États comme l'Allemagne. À cet égard, il convient de relever qu'il ressort du rapport intitulé « Iran : information sur la capacité de surveillance du gouvernement et le contrôle qu'il exerce, y compris sur la censure des médias et la surveillance de l'utilisation d'Internet », publié le 16 janvier 2015 par la Commission de l'immigration et du statut de réfugié du Canada (annexe B.8), du rapport publié par Amnesty International le 16 novembre 2020 concernant les manifestations de novembre 2019 en Iran et les coupures d'Internet (annexe B.10) ainsi que du rapport publié par l'agence de presse Human Rights Activists News Agency (HRANA) le 8 décembre 2022, contenant un examen statistique, une analyse et une synthèse des 82 premiers jours des manifestations et indiquant le nombre estimé de morts et d'arrestations

(annexe B.3), et du rapport de 2022 consacré à la liberté sur Internet en Iran publié par Freedom House (annexe B.6) que le contexte en Iran est marqué par des contestations régulières du régime par la population civile, systématiquement réprimées par les autorités de ce pays à l'aide, notamment, de moyens de surveillance de l'internet. Dans ces conditions, il ne saurait être exclu, ainsi que le fait observer le Conseil, que des commandes conçues originellement à des fins « légales », telles que « ApplySusp » et « ApplySuspIP », soient détournées et utilisées par les autorités iraniennes à des fins répressives.

113 S'agissant des composants fonctionnels du système d'interception des communications de l'Iran, la requérante précise que le système « SHAHKAR » est simplement un réseau de vérification de l'identité de l'utilisateur de communications au moment de l'allocation de sa carte SIM dont le but est d'éviter les fraudes. Selon la requérante, ce système compile les informations sur l'individu auquel appartient chaque carte SIM ou ligne fixe et crée une base de données utilisées pour lutter contre la fraude, le harcèlement et d'autres activités délictuelles analogues. Toutefois, il convient de relever que la requérante explique également que ce système permet, notamment, aux opérateurs mobiles iraniens de vérifier l'identité des usagers des services de communication. Or, ainsi qu'il a été constaté au point 107 ci-dessus, les commandes du logiciel SIAM sont adressées à tous les opérateurs mobiles iraniens et ceux-ci sont tenus d'y répondre de la façon prescrite à tout moment et d'offrir au logiciel SIAM un accès permanent aux données qu'ils possèdent sur les utilisateurs. Il s'ensuit que l'explication fournie par la requérante n'est pas de nature à écarter l'affirmation du Conseil quant au fait que le système « SHAHKAR » constitue un composant fonctionnel du système d'interception des communications des autorités iraniennes.

114 S'agissant du système « SHAMSA », la requérante conteste que celui-ci soit une « interface de collecte de données vocales et SMS en vrac (CDR) et de données IP (IPDR) » comme le fait valoir le Conseil. Selon la requérante, il s'agit simplement d'« un réseau ou canal de communication entre [elle] et les opérateurs [mobiles], à travers lequel ces derniers interagissent en y entrant des codes et commandes ». Or, à nouveau, eu égard, d'une part, au constat opéré au point 107 ci-dessus selon lequel les commandes du logiciel SIAM sont adressées à tous les opérateurs mobiles iraniens et selon lequel ceux-ci sont tenus d'y répondre de la façon prescrite à tout moment et, d'autre part, à la mention dans la table des matières du manuel d'utilisation du logiciel SIAM rédigé en farsi, selon la traduction française fournie par le Conseil, d'une commande visant à transférer les SMS vers un numéro, l'explication fournie par la requérante est peu convaincante.

115 S'agissant du système « CID », la requérante fait valoir que celui-ci permet de faire correspondre le numéro d'appareil, le numéro de mobile et le numéro de carte SIM. La fonction de ce système serait uniquement d'identifier et de contrôler la légalité de l'importation en Iran des téléphones mobiles et des appareils électroniques pouvant accueillir une carte SIM afin de communiquer ensuite ces informations aux opérateurs de télécommunications. Encore une fois, au-delà du but légitime affiché de ce système, il convient de rappeler qu'il a été constaté que les opérateurs mobiles iraniens sont tenus d'accorder à la requérante, via le logiciel SIAM, un accès permanent aux informations qu'ils possèdent sur leurs utilisateurs, de sorte que la requérante peut ainsi accéder aux données compilées par le système « CID ».

116 Enfin, s'agissant du système « LI », la requérante admet qu'il s'agit d'un système de sécurité qui permet de solliciter d'un opérateur de réseau qu'il collecte et fournisse aux forces de l'ordre des communications interceptées de particuliers ou d'organisations. La requérante souligne que ce système est strictement encadré par les dispositions du doit iranien applicables. Toutefois, ainsi

qu'il a été constaté au point 98 ci-dessus, il ressort des dispositions du droit iranien invoquées par la requérante elle-même que les hypothèses dans lesquelles les interceptions de télécommunications sont légalement possibles sont définies de façon très large.

117 Eu égard aux considérations exposées aux points 95 à 115 ci-dessus, il y a lieu de considérer que le Conseil a fait état devant le Tribunal d'un faisceau d'indices suffisamment concrets, précis et concordants permettant d'établir l'existence d'un lien suffisant entre la requérante et la situation combattue en l'espèce, à savoir la répression exercée par les autorités iraniennes contre des manifestants pacifiques, des journalistes, des défenseurs des droits de l'homme, des étudiants et d'autres personnes qui s'expriment pour défendre leurs droits légitimes.

118 Dès lors, les griefs de la requérante tirés de l'inexactitude matérielle des faits doivent être rejetés.

119 Il s'ensuit que le troisième moyen doit être rejeté comme non fondé dans son ensemble.

Sur le quatrième moyen, tiré d'une violation du principe de proportionnalité

120 La requérante fait valoir que les mesures restrictives auxquelles elle est soumise en raison de son inscription à l'annexe I du règlement nº 359/2011 sont contraires au principe de proportionnalité.

121 En ce sens, premièrement, la requérante fait valoir que les « sanctions internationales » prises par le passé à l'encontre de l'Iran avaient engendré des rétentions d'outils particulièrement utiles pour elle dont l'un est utilisé pour éviter le chevauchement des fréquences iraniennes avec celles des États voisins et l'autre, le *Location Based System*, pour la localisation précise d'appareils connectés. En outre, les sanctions imposées aujourd'hui à l'Iran empêcheraient la requérante de remplir son rôle de régulateur des fréquences et d'assurer un bon fonctionnement du réseau de télécommunications nationales.

122 Deuxièmement, la requérante soutient que les « sanctions » l'empêchent de faire partie de la Global System for Mobile Communications Association (GSMA) et qu'elle ne peut donc pas utiliser le registre de la GSMA pour empêcher les appareils contrefaits et illégaux d'être réparés. Il en découlerait plusieurs conséquences néfastes dont, notamment, l'impossibilité pour l'Iran de lutter efficacement contre la fraude, la création d'un marché parallèle de téléphones volés ou encore l'incapacité de restituer les téléphones volés à leurs propriétaires.

123 Le Conseil conteste l'argumentation de la requérante.

124 Il convient de rappeler que, en vertu du principe de proportionnalité, qui fait partie des principes généraux du droit de l'Union, la légalité de l'interdiction d'une activité économique est subordonnée à la condition que les mesures d'interdiction soient appropriées et nécessaires à la réalisation des objectifs légitimement poursuivis par la réglementation en cause, étant entendu que, lorsqu'un choix s'offre entre plusieurs mesures appropriées, il convient de recourir à la moins contraignante et que les inconvénients causés ne doivent pas être démesurés par rapport aux buts visés (voir arrêt du 6 septembre 2013, Bank Melli Iran/Conseil, T-35/10 et T-7/11, EU:T:2 013:397, point 179 et jurisprudence citée).

125 De plus, si le respect des droits fondamentaux constitue une condition de la légalité des actes de l'Union, il résulte d'une jurisprudence constante que ces droits fondamentaux ne jouissent pas, en droit de l'Union, d'une protection absolue, mais doivent être pris en considération par rapport à leur fonction dans la société. Par conséquent, des restrictions peuvent être apportées à l'usage de

ces droits, à condition qu'elles répondent effectivement à des objectifs d'intérêt général poursuivis par l'Union et ne constituent pas, au regard du but poursuivi, une intervention démesurée et intolérable qui porterait atteinte à la substance même des droits ainsi garantis (voir arrêt du 13 septembre 2013, Makhlouf/Conseil, T-383/11, EU:T:2013:431, point 97 et jurisprudence citée ; arrêt du 16 janvier 2019, Haswani/Conseil, T-477/17, non publié, EU:T:2019:7, point 74).

126 En l'espèce, il importe de souligner que la requérante n'avance aucun argument de nature à démontrer que les mesures restrictives prévues par le règlement nº 359/2011 et auxquelles elle est soumise du fait de l'adoption du règlement attaqué ne poursuivraient pas un objectif légitime ou ne seraient pas nécessaires ni appropriées pour atteindre cet objectif. Elle se borne en effet à faire valoir, en substance, que les sanctions internationales auxquelles l'Iran a été soumis par le passé ont eu des répercussions défavorables sur sa capacité à remplir ses missions, sans établir de lien nécessaire avec les mesures prévues par le règlement nº 359/2011.

127 En tout état de cause, il convient de relever que l'un des objectifs poursuivis par le règlement nº 359/2011, ainsi qu'il ressort, en substance, de ses considérants 1 et 2, consiste à exercer une pression, en gelant leurs fonds et leurs ressources économiques, à l'encontre de certaines personnes et entités responsables d'avoir ordonné ou mis en œuvre de graves violations des droits de l'homme en Iran par des actes de répression contre des manifestants pacifiques, des journalistes, des défenseurs des droits de l'homme, des étudiants ou d'autres personnes qui prennent la parole pour défendre leurs droits légitimes, y compris le droit à la liberté d'expression.

128 Force est de constater qu'un tel objectif correspond à un objectif légitime de la politique étrangère et de sécurité commune (PESC), à savoir consolider et soutenir la démocratie, l'État de droit, les droits de l'homme et les principes du droit international, visé à l'article 21, paragraphe 2, sous b), TUE.

129 En outre, les mesures restrictives prévues par le règlement nº 359/2011 ne sauraient être considérées comme inappropriées au regard du rôle clé joué par la requérante dans la mise en œuvre des exigences du gouvernement iranien concernant le filtrage des contenus Internet au moyen du logiciel espion SIAM, tel qu'il ressort de l'examen du troisième moyen.

130 De plus, ces mesures doivent être considérées comme nécessaires dès lors que, ainsi que le relève justement le Conseil, il n'a pas été démontré que des mesures alternatives et moins contraignantes telles qu'un système d'autorisation préalable ou une obligation de justification a posteriori de l'usage des fonds versés permettraient d'atteindre aussi efficacement l'objectif poursuivi.

131 Dès lors, il convient de rejeter le quatrième moyen comme non fondé.

Sur le premier moyen, tiré, en substance, d'un détournement de pouvoir

132 La requérante fait valoir que, bien que la compétence du Conseil pour adopter le règlement attaqué ne soit pas contestée, ledit règlement est vicié par un excès de pouvoir du Conseil en ce qu'il la concerne. Selon elle, cet excès de pouvoir découlerait du fait que la véritable raison qui a conduit le Conseil à inscrire son nom à l'annexe I du règlement nº 359/2011 serait d'atteindre l'État iranien.

133 Ainsi, le Conseil n'aurait pas sanctionné la requérante en raison de son activité, comme cela serait faussement indiqué dans le règlement attaqué, mais uniquement en raison de sa nature gouvernementale qui résulte de son affiliation au ministère des Communications, comme dans

tout autre pays. En soumettant la requérante aux mesures restrictives prévues par le règlement nº 359/2011, le Conseil chercherait à sanctionner son affiliation et ainsi à paralyser le pouvoir iranien.

134 Selon la requérante, conformément à la jurisprudence, si le statut juridique d'une personne visée par les mesures restrictives ou son lien juridique ou économique avec le gouvernement d'un pays peut constituer un indice susceptible de créer un soupçon aux yeux du Conseil, il ne saurait, à lui seul, justifier l'adoption de telles mesures.

135 L'identité des autres personnes inscrites à l'annexe I du règlement nº 359/2011 témoignerait également du caractère excessif de l'inscription de la requérante à ladite annexe.

136 La requérante souligne, en outre, le mimétisme entre les mesures restrictives adoptées par le Conseil et les sanctions adoptées par l'Office of Foreign Assets Control, qui témoignerait d'un ressentiment politique à l'égard de la République islamique d'Iran.

137 Le Conseil conteste l'argumentation de la requérante.

138 Il convient de rappeler que, selon la jurisprudence de la Cour, un acte n'est entaché de détournement de pouvoir que s'il apparaît, sur la base d'indices objectifs, pertinents et concordants, avoir été pris dans le but exclusif, ou à tout le moins déterminant, d'atteindre des fins autres que celles excipées ou d'éluder une procédure spécialement prévue par le traité pour parer aux circonstances de l'espèce (voir arrêt du 31 janvier 2019, Islamic Republic of Iran Shipping Lines e.a./Conseil, C-225/17 P, EU:C:2019:82, point 115 et jurisprudence citée).

139 En l'espèce, la requérante fait valoir que le Conseil a inscrit son nom à l'annexe I du règlement nº 359/2011 uniquement en raison de sa nature gouvernementale résultant de son affiliation au ministère des Communications et non de sa propre activité.

140 Toutefois, il ressort de l'examen du deuxième moyen (voir points 25 à 34 ci-dessus) que l'inscription de son nom à l'annexe I du règlement nº 359/2011 par le règlement attaqué n'était pas uniquement motivée par son affiliation au ministère des Communications, mais essentiellement par sa mise en œuvre des exigences du gouvernement iranien concernant le filtrage des contenus Internet grâce au logiciel espion SIAM et, en particulier, par la mise à profit du contrôle qu'elle exerce sur l'accès à Internet et sur les téléphones portables pour suivre les manifestants à la trace et créer un tableau détaillé des activités des dissidents et des manifestants, que les autorités ont utilisé comme elles l'entendaient lors des manifestations de 2022 à la suite de la mort de Mme Amini.

141 En outre, il ressort de l'examen du troisième moyen que les motifs invoqués par le Conseil pour justifier l'inscription du nom de la requérante à l'annexe I du règlement nº 359/2011 par le règlement attaqué reposaient sur une base factuelle suffisamment solide.

142 Par ailleurs, la requérante n'étaye pas en quoi la circonstance que le nom d'autres personnes à l'annexe I du règlement nº 359/2011 à l'égard desquelles elle précise elle-même ne pas vouloir faire de commentaires ou le fait que les autorités des États-Unis d'Amérique auraient également décidé d'adopter des mesures restrictives à son égard seraient pertinents pour démontrer que le Conseil aurait, en l'espèce, commis un détournement de pouvoir, au sens de la jurisprudence rappelée au point 138 ci-dessus.

143 Il convient dès lors de rejeter le premier moyen comme non fondé et, partant, le recours dans son ensemble.

Sur les dépens

144 Aux termes de l'article 134, paragraphe 1, du règlement de procédure, toute partie qui succombe est condamnée aux dépens, s'il est conclu en ce sens. En l'espèce, la requérante ayant succombé, il y a lieu de la condamner à supporter ses propres dépens ainsi que ceux du Conseil, conformément aux conclusions de celui-ci.

Par ces motifs,

LE TRIBUNAL (sixième chambre)

déclare et arrête :

1) Le recours est rejeté.

2) Communications Regulatory Authority (CRA) est condamnée aux dépens.

Costeira Kancheva Öberg

Ainsi prononcé en audience publique à Luxembourg, le 16 octobre 2024.

Le greffier
V. Di Bucci

Le président
S. Papasavvas