Sammlung der Rechtsprechung

URTEIL DES GERICHTS (Sechste Kammer)

16. Oktober 2024*

„Gemeinsame Außen- und Sicherheitspolitik – Restriktive Maßnahmen angesichts der Lage in Iran – Einfrieren von Geldern – Liste der Personen, Organisationen und Einrichtungen, deren Gelder und wirtschaftliche Ressourcen eingefroren werden – Aufnahme des Namens des Klägers in die Liste – Begründungspflicht – Verteidigungsrechte – Recht auf effektiven gerichtlichen Rechtsschutz – Verhältnismäßigkeit – Befugnismissbrauch“

In der Rechtssache T-201/23,

Communications Regulatory Authority (CRA) mit Sitz in Teheran (Iran), vertreten durch Rechtsanwälte T. Clay und T. Zahedi Vafa sowie Rechtsanwältin K. Mehtiyeva,

Klägerin,

gegen

Rat der Europäischen Union, vertreten durch D. Laurent, P. Mahnič und S. Lejeune als Bevollmächtigte,

Beklagter,

erlässt

DAS GERICHT (Sechste Kammer)

unter Mitwirkung der Präsidentin M. J. Costeira, der Richterin M. Kancheva (Berichterstatterin) und des Richters U. Öberg,

Kanzler: V. Di Bucci,

aufgrund des schriftlichen Verfahrens,

aufgrund des Umstands, dass keine der Parteien innerhalb von drei Wochen nach Bekanntgabe des Abschlusses des schriftlichen Verfahrens die Anberaumung einer mündlichen Verhandlung beantragt hat, und der Entscheidung gemäß Art. 106 Abs. 3 der Verfahrensordnung des Gerichts, ohne mündliches Verfahren zu entscheiden,

folgendes

* Verfahrenssprache: Französisch.

Urteil

1 Mit ihrer Klage nach Art. 263 AEUV begehrt die Klägerin, die Communications Regulatory Authority (CRA), die Nichtigerklärung der Durchführungsverordnung (EU) 2023/152 des Rates vom 23. Januar 2023 zur Durchführung der Verordnung (EU) Nr. 359/2011 über restriktive Maßnahmen gegen bestimmte Personen, Organisationen oder Einrichtungen angesichts der Lage in Iran (ABl. 2023, L 20 I, S. 1, im Folgenden: angefochtene Verordnung), soweit dieser Rechtsakt sie betrifft.

Vorgeschichte des Rechtsstreits

2 Die Klägerin ist eine Regierungsinstitution, die dem iranischen Ministerium für Kommunikations- und Informationstechnologie (im Folgenden: Ministerium für Kommunikationstechnologie) angegliedert ist und den Regelungen des Gesetzes über die Aufgaben und Befugnisse dieses Ministeriums sowie ihrer eigenen Satzung unterliegt und nach diesem Gesetz und dieser Satzung organisiert ist. Nach dieser Satzung setzt die Klägerin u. a. die vom Ministerium für Kommunikationstechnologie festgelegten Ziele im Sektor des Funkverkehrs um und übt Regierungs-, Exekutiv- und Aufsichtsaufgaben und -befugnisse dieses Ministeriums aus. Die Haupttätigkeit der Klägerin besteht in der Regulierung, Verwaltung und Kontrolle des Frequenzraums in Iran. Die Klägerin ist dabei im Besonderen mit der Erteilung von Lizenzen für den Netzbetrieb an Telekommunikationsdienste und der Überwachung der Leistungen der Lizenznehmer betraut. Die Klägerin übt ferner eine normative Rolle aus, indem sie den zuständigen Behörden nationale Kommunikationsstandards sowie Instruktionen und Regelungen zur Verbindung von Telekommunikations- und Computernetzwerken untereinander unter dem Gesichtspunkt der Sicherheit der Verbindungen vorschlägt. Die Klägerin übt auch Aufgaben zum Schutz der Rechte der Nutzer von Telekommunikationsdiensten aus und nimmt die Vertretung der Islamischen Republik Iran in regionalen und internationalen Vereinigungen des Kommunikationssektors wahr.

3 Am 21. März 2011 nahm der Rat der Europäischen Union Schlussfolgerungen an, in denen es heißt, dass die Europäische Union angesichts der weiteren Verschlechterung der Menschenrechtslage in Iran tief besorgt sei. Der Rat lenkte die Aufmerksamkeit auf die systematische Repression gegen iranische Bürger, die Schikanen ausgesetzt seien und festgenommen würden, weil sie ihr legitimes Recht auf Meinungsfreiheit und friedliche Versammlung ausübten. Außerdem bekräftigte der Rat die Intention der Union, die Menschenrechtsverletzungen in Iran anzugehen, auch indem zügig gezielte restriktive Maßnahmen gegen diejenigen eingeleitet würden, die für schwerwiegende Verstöße gegen die Menschenrechte verantwortlich sind.

4 Am 12. April 2011 erließ der Rat den Beschluss 2011/235/GASP über restriktive Maßnahmen gegen bestimmte Personen und Organisationen angesichts der Lage in Iran (ABl. 2011, L 100, S. 51), der eine Reihe restriktiver Maßnahmen gegen Personen festlegt, die für die Anordnung oder Begehung schwerer Menschenrechtsverletzungen verantwortlich oder hieran beteiligt waren.

5 Der Beschluss 2011/235 wurde mit der auf der Grundlage von Art. 215 Abs. 2 AEUV erlassenen Verordnung (EU) Nr. 359/2011 des Rates vom 12. April 2011 über restriktive Maßnahmen gegen bestimmte Personen, Organisationen und Einrichtungen angesichts der Lage in Iran (ABl. 2011, L 100, S. 1) umgesetzt.

6 Art. 2 Abs. 1 und 2 der Verordnung Nr. 359/2011 bestimmt:

„(1) Sämtliche Gelder und wirtschaftlichen Ressourcen, die Eigentum oder Besitz der in Anhang I aufgeführten natürlichen und juristischen Personen, Organisationen und Einrichtungen sind oder von diesen gehalten oder kontrolliert werden, werden eingefroren.

(2) Den in Anhang I aufgeführten natürlichen und juristischen Personen, Organisationen und Einrichtungen dürfen weder unmittelbar noch mittelbar Gelder oder wirtschaftliche Ressourcen zur Verfügung gestellt werden oder zugutekommen."

7 Gemäß Art. 3 Abs. 1 und 2 der Verordnung Nr. 359/2011 werden die Personen, die vom Rat als für schwere Menschenrechtsverletzungen in Iran verantwortlich ermittelt worden sind, und die Personen, Organisationen und Einrichtungen, die mit ihnen in Verbindung stehen, in die Liste in Anhang I aufgenommen. Diese Liste enthält die Gründe für die Aufnahme.

8 Art. 12 Abs. 1 bis 3 der Verordnung Nr. 359/2011 bestimmt:

„(1) Beschließt der Rat, die in Artikel 2 Absatz 1 genannten Maßnahmen auf eine natürliche oder juristische Person, Organisation oder Einrichtung anzuwenden, so ändert er Anhang I entsprechend.

„(2) Der Rat setzt die natürlichen oder juristischen Personen, Organisationen oder Einrichtungen … von seinem Beschluss und den Gründen für ihre Aufnahme in die Liste in Kenntnis und gibt dabei diesen natürlichen oder juristischen Personen, Organisationen oder Einrichtungen Gelegenheit zur Stellungnahme.

(3) Wird eine Stellungnahme unterbreitet oder werden stichhaltige neue Beweise vorgelegt, so überprüft der Rat seinen Beschluss und unterrichtet die natürliche oder juristische Person, Organisation oder Einrichtung entsprechend."

9 Am 16. September 2022 verstarb Frau Mahsa Amini, eine 22-jährige Iranerin, im Krankenhaus, nachdem sie von der iranischen Sittenpolizei festgenommen worden war. Nach ihrem Tod kam es zu Massenprotesten, die von den iranischen Behörden unterdrückt wurden.

10 Am 25. September 2022 gab der Hohe Vertreter der Union für die Außen- und Sicherheitspolitik im Namen der Union eine Erklärung ab, in der er den weitverbreiteten und unverhältnismäßigen Einsatz von Gewalt seitens der iranischen Sicherheitskräfte gegen friedlich Demonstrierende bedauerte. In der Erklärung hieß es ferner, dass jede für die Tötung von Frau Amini verantwortliche Person zur Rechenschaft gezogen werden müsse. Die iranische Regierung wurde aufgefordert, dafür zu sorgen, dass im Zuge transparenter und glaubwürdiger Ermittlungen festgestellt wird, wie viele Menschen getötet und festgenommen worden sind, dass alle friedlich Demonstrierenden freigelassen werden und dass alle Inhaftierten ein ordnungsgemäßes Verfahren erhalten. Weiter wurde in der Erklärung betont, dass die Entscheidung Irans, den Internetzugang erheblich einzuschränken und Instant-Messaging-Plattformen zu blockieren, einen eklatanten Verstoß gegen das Recht auf freie Meinungsäußerung darstelle. Schließlich hieß es in der Erklärung, dass die Union alle ihr zur Verfügung stehenden Optionen prüfen werde, um auf die Tötung von Frau Amini und die Art und Weise, wie die iranischen Sicherheitskräfte mit den anschließenden Demonstrationen umgegangen seien, zu reagieren.

11 Am 23. Januar 2023 erließ der Rat den Durchführungsbeschluss (GASP) 2023/153 zur Durchführung des Beschlusses 2011/235 (ABl. 2023, L 20 I, S. 23). Der zweite Erwägungsgrund des Durchführungsbeschlusses 2023/153 verwies auf die Erklärung des Hohen Vertreters der Union für die Außenpolitik mit dem oben in Rn. 10 wiedergegebenen Wortlaut. Laut dem dritten Erwägungsgrund „[sollten v]or diesem Hintergrund und im Einklang mit der Zusage der Union, alle wichtigen Fragen, einschließlich der Menschenrechtslage, zusammen mit Iran anzugehen, … 18 Personen und 19 Organisation[en] in die im Anhang des Beschlusses 2011/235 enthaltene Liste der Personen und Organisationen, die restriktiven Maßnahmen unterliegen, aufgenommen werden“. Art. 1 des Durchführungsbeschlusses 2023/153 sah die Änderung des Anhangs des Beschlusses 2011/235 gemäß dem Anhang des Durchführungsbeschlusses 2023/153 vor.

12 In Zeile 15 der Liste der Organisationen im Anhang des Durchführungsbeschlusses 2023/153 wurden u. a. der Name der Klägerin sowie die Gründe für ihre Aufnahme mit folgenden Worten aufgenommen:

„Die Kommunikationsregulierungsbehörde (CRA) untersteht dem iranischen Ministerium für Informations- und Kommunikations-technologie. Die CRA setzt die Vorschrift der iranischen Regierung durch, Internet-Inhalte durch eine Spähsoftware mit Namen SIAM zu filtern.

Während der Proteste 2022 hat die CRA ihre Kontrolle über den Zugang zum Internet und über Mobiltelefone dazu genutzt, Protestteilnehmer nachzuverfolgen und der Regierung ein von ihr nach Belieben zu verwendendes detailliertes Bild der Aktivitäten von Dissidenten und Protestteilnehmern zu übermitteln[.] Die CRA ist somit verantwortlich für die Unterstützung der Unterdrückung von friedlichen Demonstranten, Journalisten, Menschenrechtsverteidigern, Studierenden und anderen Personen, die für ihre legitimen Rechte eintreten.

Die Kommunikationsregulierungsbehörde ist somit verantwortlich für schwere Menschenrechtsverletzungen in Iran.“

13 Am selben Tag erließ der Rat auf der Grundlage von Art. 12 Abs. 1 der Verordnung Nr. 359/2011 die angefochtene Verordnung. Der Wortlaut der Erwägungsgründe 2 und 3 der angefochtenen Verordnung und derjenige der Erwägungsgründe 2 und 3 des Durchführungsbeschlusses 2023/153 ist abgesehen davon, dass Erstere auf den Anhang I der Verordnung Nr. 359/2011 anstelle des Anhangs des Beschlusses 2011/235 verweisen, identisch. Art. 1 der angefochtenen Verordnung sah die Änderung des Anhangs I der Verordnung Nr. 359/2011 gemäß dem Anhang der angefochtenen Verordnung vor.

14 In Zeile 15 der im Anhang der angefochtenen Verordnung enthaltenen Liste der Organisationen wurden u. a. der Name der Klägerin sowie die Aufnahmegründe mit einem Wortlaut, der mit dem oben in Rn. 12 wiedergegebenen Wortlaut identisch ist, aufgenommen.

15 Am 24. Januar 2023 veröffentlichte der Rat im *Amtsblatt der Europäischen Union* eine Mitteilung an die Personen, Organisationen und Einrichtungen, die den Maßnahmen nach dem Beschluss 2011/235, durchgeführt durch den Durchführungsbeschluss 2023/153, und der Verordnung Nr. 359/2011, durchgeführt durch die angefochtene Verordnung, unterliegen (ABl. 2023, C 25, S. 8).

16 In dieser Mitteilung hieß es u. a., dass der Rat beschlossen habe, dass die fraglichen Personen und Organisationen in die Liste der Personen und Organisationen aufgenommen werden sollten, die den im Beschluss 2011/235 und in der Verordnung Nr. 359/2011 vorgesehenen restriktiven

Maßnahmen unterliegen, und dass diese Personen und Organisationen bei ihm unter Vorlage entsprechender Nachweise beantragen könnten, dass der Beschluss, sie in die genannten Listen aufzunehmen, überprüft wird. Entsprechende Anträge waren bis zum 15. Februar 2023 an die in dieser Mitteilung angegebene Anschrift zu richten.

Anträge der Parteien

17 Die Klägerin beantragt, die angefochtene Verordnung insoweit für nichtig zu erklären, als ihr Name in Anhang I der Verordnung Nr. 359/2011 aufgenommen wird.

18 Der Rat beantragt,

– die Klage abzuweisen;

– der Klägerin die Kosten aufzuerlegen.

Rechtliche Würdigung

19 Die Klägerin stützt ihre Klage auf vier Klagegründe: erstens im Wesentlichen einen Befugnismissbrauch, zweitens eine Verletzung der Begründungspflicht und des Rechts auf effektiven gerichtlichen Rechtsschutz, drittens im Wesentlichen die sachliche Unrichtigkeit des Sachverhalts und viertens einen Verstoß gegen den Verhältnismäßigkeitsgrundsatz.

20 Nach der Analyse dieser Klagegründe erweist es sich als sachdienlich, als Erstes den zweiten Klagegrund betreffend die Verletzung der Begründungspflicht und des Rechts auf effektiven gerichtlichen Rechtsschutz zu prüfen, als Zweites den dritten Klagegrund betreffend einen offensichtlichen Fehler bei der Beurteilung des Sachverhalts, als Drittes den vierten Klagegrund betreffend einen Verstoß gegen den Verhältnismäßigkeitsgrundsatz und sodann als Viertes den ersten Klagegrund betreffend einen Befugnismissbrauch.

Zum zweiten Klagegrund: Verletzung der Begründungspflicht und des Rechts auf effektiven gerichtlichen Rechtsschutz

21 Als Erstes macht die Klägerin geltend, der Rat habe, da er nicht gleichzeitig mit oder unmittelbar nach Erlass der angefochtenen Verordnung die Informationen oder Beweise, auf denen die Gründe für ihre Aufnahme in die in Anhang I der Verordnung Nr. 359/2011 enthaltene Liste beruhten, mitgeteilt habe, seine Pflicht, die Stichhaltigkeit dieser Gründe nachzuweisen, nicht erfüllt und folglich seine Begründungspflicht verletzt.

22 Als Zweites bringt die Klägerin vor, die Begründung der angefochtenen Verordnung bestehe, soweit sie sie betreffe, aus einer stereotypen Begründung, die sich aus drei kurzen Absätzen mit 15 Zeilen zusammensetze, in denen die Annahmen zusammengefasst würden, die der Rat aufgrund ihrer Eigenschaft als staatliche Stelle treffe. Solch eine Begründung stehe nicht im Einklang mit der Rechtsprechung, wonach die Begründung eines Rechtsakts es zum einen der von dem streitigen Rechtsakt betroffenen Person ermöglichen müsse, dessen Ungültigkeit bei Gericht in vollumfänglicher Kenntnis der gegen sie erhobenen Vorwürfe geltend zu machen, und zum anderen dem Gericht die Ausübung seiner Kontrolle des angefochtenen Rechtsakts ermöglichen müsse. Das Begründungserfordernis könne nicht durch den politischen Kontext, in

dem eine Maßnahme erlassen werde, aufgeweicht werden, zumal die Kontextualisierung die Klägerin nicht in die Lage versetze, die Tragweite der gegen sie verhängten restriktiven Maßnahmen zu verstehen, und entsprechend das Gericht nicht in die Lage versetze, die Prüfung der in Rede stehenden Maßnahme vorzunehmen. Der Rat könne daher seiner Begründungspflicht nicht nachkommen, indem er sich hinter sicherheits- und außenpolitischen Erwägungen „verstecke“.

23 Als Drittes rügt die Klägerin in der Erwiderung auf der Grundlage der Art. 47 und 48 der Charta der Grundrechte der Europäischen Union (im Folgenden: Charta), dass das Dokument, das der Rat dem Gericht zum Beweis der Gründe für die Aufnahme ihres Namens in Anhang I der Verordnung Nr. 359/2011 vorgelegt habe, nicht berücksichtigt werden dürfe. Sie bestreitet ferner die Relevanz und die Beweiskraft der in diesem Dokument enthaltenen Informationen.

24 Der Rat tritt dem Vorbringen der Klägerin entgegen.

25 Es ist darauf hinzuweisen, dass die Pflicht zur Begründung eines beschwerenden Rechtsakts, die aus dem Grundsatz der Wahrung der Verteidigungsrechte folgt, nach ständiger Rechtsprechung dem Zweck dient, den Betroffenen so ausreichend zu unterrichten, dass er erkennen kann, ob der Rechtsakt sachlich richtig oder eventuell mit einem Mangel behaftet ist, der seine Anfechtung vor den Unionsgerichten zulässt, und den Unionsgerichten die Prüfung der Rechtmäßigkeit dieses Rechtsakts zu ermöglichen (vgl. Urteil vom 15. November 2012, Rat/Bamba, C-417/11 P, EU:C:2012:718, Rn. 49 und die dort angeführte Rechtsprechung).

26 Ferner muss die nach Art. 296 AEUV und Art. 41 Abs. 2 Buchst. c der Charta vorgeschriebene Begründung der Natur des betreffenden Rechtsakts und dem Kontext, in dem er erlassen wurde, angepasst sein. Das Begründungserfordernis ist anhand der Umstände des Einzelfalls, insbesondere des Inhalts des Rechtsakts, der Art der angeführten Gründe und des Interesses zu beurteilen, das die Adressaten oder andere von dem Rechtsakt unmittelbar und individuell betroffene Personen an Erläuterungen haben können. In der Begründung brauchen nicht alle tatsächlich und rechtlich einschlägigen Gesichtspunkte genannt zu werden, da die Frage, ob eine Begründung ausreichend ist, nicht nur anhand des Wortlauts des Rechtsakts, sondern auch anhand seines Kontexts sowie sämtlicher Rechtsvorschriften auf dem betreffenden Gebiet zu beurteilen ist (vgl. Urteil vom 17. September 2020, Rosneft u. a./Rat, C-732/18 P, nicht veröffentlicht, EU:C:2020:727, Rn. 77 und die dort angeführte Rechtsprechung; Urteil vom 27. Juli 2022, RT France/Rat, T-125/22, EU:T:2022:483, Rn. 103).

27 Somit ist ein beschwerender Rechtsakt hinreichend begründet, wenn er in einem Kontext ergangen ist, der dem Betroffenen bekannt war und ihm gestattet, die Tragweite der ihm gegenüber getroffenen Maßnahme zu verstehen (vgl. Urteil vom 17. September 2020, Rosneft u. a./Rat, C-732/18 P, nicht veröffentlicht, EU:C:2020:727, Rn. 78 und die dort angeführte Rechtsprechung). Außerdem müssen die an die Genauigkeit der Begründung eines Rechtsakts zu stellenden Anforderungen den tatsächlichen Möglichkeiten sowie den technischen und zeitlichen Bedingungen angepasst werden, unter denen der Rechtsakt zu ergehen hat (vgl. Urteil vom 27. Juli 2022, RT France/Rat, T-125/22, EU:T:2022:483, Rn. 104 und die dort angeführte Rechtsprechung).

28 Nach der Rechtsprechung muss überdies in der Begründung eines Rechtsakts des Rates, mit dem eine restriktive Maßnahme verhängt wird, nicht nur die Rechtsgrundlage dieser Maßnahme genannt werden, sondern es müssen auch die besonderen und konkreten Gründe angegeben

werden, aus denen der Rat es in Ausübung seines Ermessens für angebracht hielt, den Betroffenen einer solchen Maßnahme zu unterwerfen (vgl. Urteil vom 27. Juli 2022, RT France/Rat, T-125/22, EU:T:2022:483, Rn. 105 und die dort angeführte Rechtsprechung).

29 Schließlich ist darauf hinzuweisen, dass es sich bei der Begründungspflicht um ein wesentliches Formerfordernis handelt, das von der Stichhaltigkeit der Gründe zu unterscheiden ist, die zur materiellen Rechtmäßigkeit des streitigen Rechtsakts gehört. Die Begründung eines Rechtsakts soll nämlich förmlich die Gründe zum Ausdruck bringen, auf denen dieser Rechtsakt beruht. Weisen die Gründe Fehler auf, so beeinträchtigen diese die materielle Rechtmäßigkeit des Rechtsakts, nicht aber dessen Begründung, die, obwohl sie fehlerhafte Gründe enthält, zureichend sein kann (vgl. in diesem Sinne Urteil vom 13. September 2013, Makhlouf/Rat, T-383/11, EU:T:2013:431, Rn. 73 und 74 und die dort angeführte Rechtsprechung).

30 Im vorliegenden Fall ist, was den Kontext der Aufnahme der Klägerin in Anhang I der Verordnung Nr. 359/2011 anbelangt, darauf hinzuweisen, dass der zweite Erwägungsgrund der angefochtenen Verordnung, wie der Rat zu Recht betont, auf die im Namen der Union abgegebene Erklärung des Hohen Vertreters der Union verwies, deren Wortlaut oben in Rn. 10 wiedergegeben ist.

31 Wie oben in Rn. 11 angegeben, geht aus dem dritten Erwägungsgrund der angefochtenen Verordnung zudem hervor, dass die Aufnahme von 19 Organisationen, u. a. der Klägerin, in die in Anhang I der Verordnung Nr. 359/2011 enthaltene Liste der natürlichen und juristischen Personen, Organisationen und Einrichtungen, die restriktiven Maßnahmen unterliegen, vor dem in Rn. 10 dargestellten Hintergrund und im Einklang mit der Zusage der Union erfolgt ist, alle wichtigen Fragen betreffend Iran, einschließlich der Menschenrechtslage, anzugehen.

32 Im Besonderen waren die Gründe, aus denen der Name der Klägerin in Anhang I der Verordnung Nr. 359/2011 aufgenommen wurde, im Anhang der angefochtenen Verordnung mit dem oben in Rn. 12 wiedergegebenen Wortlaut angegeben.

33 Eine derartige Begründung legt im Licht der in den Erwägungsgründen 2 und 3 der angefochtenen Verordnung genannten kontextuellen Aspekte die Gründe, aus denen der Rat es in Ausübung seines Ermessens für angebracht hielt, die Klägerin einer restriktiven Maßnahme zu unterwerfen, in hinreichender spezifischer und konkreter Weise dar.

34 Aus der Begründung der angefochtenen Verordnung ergibt sich nämlich, dass die Klägerin als für schwere Menschenrechtsverletzungen in Iran verantwortlich angesehen wurde, da sie die Anordnung der iranischen Regierung, Internet-Inhalte durch eine Spähsoftware mit Namen SIAM zu filtern, umgesetzt und im Besonderen bei den Protesten 2022 nach dem Tod von Frau Amini ihre Kontrolle über den Zugang zum Internet und über Mobiltelefone dazu genutzt hat, Protestteilnehmer nachzuverfolgen und der Regierung ein von dieser nach Belieben zu verwendendes detailliertes Bild der Aktivitäten von Dissidenten und Protestteilnehmern zu übermitteln, und damit die Unterdrückung der Demonstranten, die für ihre legitimen Rechte eintraten, unterstützt hat.

35 Überdies greift das Argument der Klägerin nicht durch, der Rat sei seiner Begründungspflicht nicht nachgekommen, weil er die Beweise, auf denen die für ihre Aufnahme in Anhang I der Verordnung Nr. 359/2011 angeführten Gründe beruhten, nicht gleichzeitig mit der angefochtenen Verordnung oder unmittelbar nach deren Erlass übermittelt und daher die Stichhaltigkeit dieser Gründe nicht nachgewiesen habe.

36 Soweit die Argumentation der Klägerin dahin geht, dass der Rat den Beweis für die Stichhaltigkeit der Gründe, die er in der angefochtenen Verordnung für ihre Aufnahme in Anhang I der Verordnung Nr. 359/2011 angeführt hat, nicht erbracht habe, ist diese Frage gemäß der oben in Rn. 29 angeführten Rechtsprechung von der Frage der Begründung der angefochtenen Verordnung zu unterscheiden, die die formelle Rechtmäßigkeit dieser Verordnung betrifft.

37 Soweit die Klägerin mit dieser Argumentation geltend machen möchte, dass der Rat ihre Verteidigungsrechte verletzt habe, weil er verpflichtet gewesen sei, ihr von Amts wegen Zugang zu den in seiner Akte enthaltenen Informationen zu gewähren, ist darauf hinzuweisen, dass die angefochtene Verordnung der Klägerin durch eine am 24. Januar 2023 im Amtsblatt veröffentlichten Mitteilung bekannt gegeben wurde, in der den betroffenen Personen und Organisationen Gelegenheit gegeben wurde, bis zum 15. Februar 2023 beim Rat die Überprüfung zu beantragen, und dass die Klägerin weder einen solchen Antrag gestellt noch den Rat außerhalb des vorliegenden Verfahrens um Zugang zu der sie betreffenden Akte ersucht hat.

38 Bei einer erstmaligen Aufnahme in die Liste der Personen und Einrichtungen, gegen die restriktive Maßnahmen erlassen werden, verpflichtet der Grundsatz der Wahrung der Verteidigungsrechte den Rat nicht, von sich aus Zugang zu den in seinen Akten enthaltenen Schriftstücken zu gewähren, wenn hinreichend genaue Informationen mitgeteilt wurden, die es der betroffenen Einrichtung ermöglichen, zu den ihr vom Rat zur Last gelegten Gesichtspunkten sachdienlich Stellung zu nehmen. Nur auf Antrag des Betroffenen hat er Einsicht in alle nicht vertraulichen Verwaltungsdokumente zu gewähren, die die in Rede stehende Maßnahme betreffen. Das Erfordernis, den Inhalt der Akte von sich aus mitzuteilen, ginge zu weit, da zum Zeitpunkt des Erlasses einer Maßnahme des Einfrierens von Geldern nicht sicher ist, dass die betroffene Einrichtung mittels Aktenzugang die tatsächlichen Umstände überprüfen will, auf die der Rat die ihr zur Last gelegten Punkte stützt (Urteile vom 14. Oktober 2009, Bank Melli Iran/Rat, T-390/08, EU:T:2009:401, Rn. 97, und vom 16. September 2013, Bank Kargoshaei u. a./Rat, T-8/11, nicht veröffentlicht, EU:T:2013:470, Rn. 68).

39 Im vorliegenden Fall ergibt sich aus dem Vorstehenden, dass die Klägerin durch die Begründung der angefochtenen Verordnung über hinreichend genaue Informationen verfügte, die es ihr erlaubten, zu den ihr vom Rat zur Last gelegten Gesichtspunkten Stellung zu nehmen. Daher war der Rat nicht verpflichtet, der Klägerin die in seiner Akte enthaltenen Informationen von Amts wegen mitzuteilen.

40 Ferner ist hervorzuheben, dass das Vorbringen der Klägerin in Bezug auf die Zulässigkeit des in der Anlage B.11 vorgelegten Dokuments und den Beweiswert der darin enthaltenen Informationen die Stichhaltigkeit der für die Aufnahme ihres Namens in Anhang I der Verordnung Nr. 359/2011 angeführten Gründe betrifft und somit für den Klagegrund, mit dem eine Verletzung der Begründungspflicht geltend gemacht wird, irrelevant ist. Dieses Vorbringen wird deshalb zusammen mit dem ähnlichen Vorbringen der Klägerin im Rahmen des dritten Klagegrundes geprüft, mit dem sie einen offensichtlichen Beurteilungsfehler geltend macht.

41 Folglich ist der zweite Klagegrund als unbegründet zurückzuweisen.

Zum dritten Klagegrund: sachliche Unrichtigkeit des Sachverhalts

42 Die Klägerin bringt vor, die angefochtene Verordnung sei, soweit sie sie betreffe, mit einem „offensichtlichen Fehler bei der Beurteilung des Sachverhalts“ behaftet, da sie zum einen nicht die rechtliche Fähigkeit besitze, die ihr vom Rat vorgeworfenen Handlungen zu begehen, und zum anderen auch nicht über die technischen Fähigkeiten verfüge, um die Tätigkeiten der Protestteilnehmer nachzuverfolgen oder ein „detailliertes Bild“ hiervon zu erstellen.

43 Daher macht die Klägerin erstens geltend, dass ihre Satzung es ihr nicht gestatte, eine massenhafte Überwachung der Bevölkerung vorzunehmen, und noch weniger, die Protestteilnehmer „nachzuverfolgen“. Nach ihrer Satzung habe die Klägerin die Rolle eines Regulators, Moderators oder auch Repräsentanten von Iran inne. Zudem könne sie, selbst wenn sie es wollte, keine Filterung einrichten, da eine solche Praxis rechtlichen Rahmenbedingungen unterliege. Entgegen dem Vorbringen des Rates sei die Sammlung von Daten durch zahlreiche Rechtstexte geregelt, u. a. Art. 25 der Verfassung, Art. 582 des iranischen Strafgesetzbuchs, ergänzt durch das „Gesetz über Cyberstraftraten“ vom 26. Mai 2009, und die Art. 104 und 150 der iranischen Strafprozessordnung. Dieser normative Rahmen stehe im Einklang mit der Entschließung des Rates vom 17. Januar 1995 über die rechtmäßige Überwachung des Fernmeldeverkehrs (ABl. 1996, C 329, S. 1). Ferner ergebe sich aus zwei Berichten eines Telekommunikationsunternehmens, dass die Anfragen der Klägerin entgegen dem Vorbringen des Rates nicht über die die herkömmlichen Anforderungen im Bereich der rechtmäßigen Überwachung hinausgingen.

44 Im Übrigen sei die Massenüberwachung von der individuellen Überwachung von Personen zu unterscheiden. Die Massenüberwachung könne in jeder Gesellschaft notwendig sein, um den Frieden und die öffentliche Ordnung aufrechtzuerhalten, insbesondere indem die Bewegungen von Personen und Menschenmengen, die sich versammelten, überwacht würden. Dies ermögliche es, bei öffentlichen Demonstrationen jegliche Ausschreitungen aus der Menge heraus zu verhindern. Über diese Überwachungsbefugnis verfüge jeder souveräne Staat, und von der Ausübung dieser Befugnis könne nicht auf individuelle Menschenrechtsverletzungen geschlossen werden. Diese Überwachungsbefugnis stelle ein Hoheitsrecht dar, das u. a. vom Europäischen Gerichtshof für Menschenrechte anerkannt sei.

45 Zweitens behauptet die Klägerin, die von ihr verwendete Software namens „SIAM“ oder in Farsi „Samaneh yekparche Estehlamate Mokhaberati“ verfüge nicht über Funktionen, die eine massenhafte oder individuelle Überwachung von Demonstrierenden auf iranischem Hoheitsgebiet ermöglichten.

46 Die Klägerin trägt vor, die Software SIAM sei eine Anwendungsprogrammierschnittstelle (Application Programming Interface, im Folgenden: API), d. h. ein Mechanismus, der die Rolle einer Brücke übernehme und es einem externen Kunden ermögliche, interne APIs und deren Dienste zu nutzen. In Iran griffen der Rote Halbmond, die Rettungsdienste, die Feuerwehr und die für Straßen und Krisenmanagement zuständigen Organisationen auf diese Software zurück. Die Software SIAM werde von den Leitstellen genutzt, insbesondere wenn sie von den Notfalldiensten angerufen würden. Die Leitstellen verwendeten diese Software, um die Mobilfunkbetreiber zu erreichen, die dann eine lediglich näherungsweise Lokalisierung der sich in einer Gefahrensituation befindenden Person mitteilen würden.

47 Im Übrigen betont die Klägerin, dass sie den Polizei- und Justizbehörden nicht unmittelbar Informationen über die Nutzer von Kommunikationsdiensten übermitteln könne, denn diese Informationen befänden sich in der Hand der Betreiber, die Lizenzen für den Netzbetrieb innehätten.

48 Schließlich tritt die Klägerin dem Vorbringen des Rates in dessen Klagebeantwortung bezüglich der angeblichen „Funktionskomponenten“ von Irans Überwachungssystem entgegen.

49 Die Klägerin macht insoweit geltend, dass der Rat sich in den Funktionalitäten der Software SIAM, „Force2GNumber“, „LocationCustomerList“, „GetCDR“, „GetIPDR“ und „ApplySusplp“, auf die er in der Klagebeantwortung Bezug nehme, täusche. Die Beschreibung dieser Funktionen durch den Rat, die allein auf dem Artikel des investigativen Onlinemagazins *The Intercept* beruhe, entspreche nicht der Realität. Es handele sich um klassische und übliche Befehle, die einem staatlichen Telekommunikationsregulierungsorgan zur Verfügung stünden, und alle Mitgliedstaaten der Union verfügten über ähnliche Instrumente. Entsprechendes gelte für die Systeme „Legal Intercept“ (LI), „Control Illegal Devices“ (CID), „SHAHKAR“ und „SHAMSA“.

50 Ferner rügt die Klägerin in der Erwiderung, dass der am 28. Oktober 2022 von *The Intercept* unter dem Titel „Hacked documents: How Iran track and control protesters phones“ veröffentlichte und vom Rat als Anlage B.11 vorgelegte Artikel (im Folgenden: Artikel von *The Intercept*) nicht berücksichtigt werden dürfe. Die in diesem Artikel behaupteten Tatsachen beruhten auf einer Reihe interner Dokumente eines iranischen Mobilfunkbetreibers, die in das Verfahren beim Gericht nicht eingeführt worden seien. Der Rat begnüge sich mit der Behauptung, dass die Autoren dieses Artikels Zugang zu Dokumenten gehabt hätten, die ihnen „von einer Person übermittelt wurden, [die behaupte], einen iranischen Mobilfunkbetreiber gehackt zu haben“. Dieser Artikel, der das Kernstück der Akte des Rates darstelle, sei daher ein bloßer Beweis vom Hörensagen. Nach der Rechtsprechung des Gerichtshofs zu den Art. 47 und 48 der Charta sowie der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte zu Art. 6 der am 4. November 1950 in Rom unterzeichneten Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten sei die Verwertung der Aussagen von in der späteren mündlichen Verhandlung nicht anwesenden Zeugen, die von der gegnerischen Partei nicht geprüft werden könnten, grundsätzlich verboten, es sei denn, es werde eine hinreichende Begründung vorgebracht, die die Notwendigkeit, die Zeugenaussagen zu verwerten, rechtfertige, dem Angeklagten würden andere Verfahrensgarantien gewährt und es lägen weitere ihn belastende Beweise vor. Der Gerichtshof habe außerdem in dem Urteil vom 8. Dezember 2022, HYA u. a. (Unmöglichkeit, Fragen an die Belastungszeugen zu stellen) (C-348/21, EU:C:2022:965), entschieden, dass die Beweiskraft der Aussagen von Belastungszeugen in Fällen, in denen es nicht möglich sei, Fragen an diese Zeugen zu stellen, relativiert werden müsse, auch wenn solche Zeugenaussagen zulässig seien.

51 Hieraus folge, dass der Rat unter Verstoß gegen die Art. 47 und 48 der Charta gehandelt habe, indem er die angefochtene Verordnung auf angebliche Aussagen einer unbekannten Person gestützt habe, so dass dieses Beweisangebot als unzulässig zurückzuweisen sei.

52 Die Klägerin macht in der Erwiderung außerdem geltend, dass das Gericht nach dem Grundsatz des kontradiktorischen Verfahrens nur die Verfahrensdokumente und Beweisstücke berücksichtigen dürfe, die die Parteien zur Kenntnis hätten nehmen und zu denen sie Stellung hätten nehmen können. Der Rat habe jedoch selbst eingeräumt, dass der in dem Artikel von *The Intercept* genannte iranische Mobilfunkbetreiber der Bitte der Journalisten um eine Stellungnahme nicht nachgekommen sei.

53 Der Rat tritt dem Vorbringen der Klägerin entgegen.

54 Es ist darauf hinzuweisen, dass die Klägerin im Rahmen des dritten Klagegrundes die sachliche Richtigkeit der für ihre Aufnahme in Anhang I der Verordnung Nr. 359/2011 angeführten Gründe bestreitet. Sie sei weder rechtlich noch technisch zu den ihr vorgeworfenen Handlungen befähigt.

55 Wie aus Rn. 23 oben hervorgeht, wirft die Klägerin dem Rat im Rahmen des zweiten Klagegrundes jedoch auch vor, die Art. 47 und 48 der Charta zu verletzen und die Beweislast umzukehren, indem er seine Beurteilung auf den Artikel von *The Intercept* stütze. Die in diesem Artikel angeführten Tatsachen und Aussagen stellten nämlich, nachdem die in dieser Publikation genannten Dokumente nicht zur Akte des vorliegenden Verfahrens gereicht worden seien, bloße Behauptungen dar, hinsichtlich derer der Klägerin die Möglichkeit genommen sei, ihre Verteidigungsrechte auszuüben. In ihrem Erwiderungsschriftsatz macht die Klägerin ferner geltend, dass der in Art. 85 Abs. 1 der Verfahrensordnung des Gerichts verankerte Grundsatz des kontradiktorischen Verfahrens missachtet werde, da im vorliegenden Verfahren keine Beweisstücke zur Akte gereicht worden seien. Die Klägerin hebt außerdem den fehlenden Beweiswert einer solchen Publikation hervor.

56 Das Vorbringen der Klägerin in Bezug auf die Verletzung der Art. 47 und 48 der Charta sowie der Verstoß gegen den Grundsatz des kontradiktorischen Verfahrens sind vor dem Vorbringen in Bezug auf den Beweiswert des Artikels von *The Intercept* und dem im Anschluss hieran zu behandelnden Vorbringen in Bezug auf einen „offensichtlichen Fehler bei der Beurteilung des Sachverhalts“ zu prüfen.

Zur Verletzung der Art. 47 und 48 der Charta und zum Verstoß gegen den Grundsatz des kontradiktorischen Verfahrens

57 Zunächst ist das Vorbringen der Klägerin zurückzuweisen, der vom Rat als Anlage B.11 zur Klagebeantwortung vorgelegte Artikel von *The Intercept* sei im Wesentlichen aus dem Grund als unzulässig zurückzuweisen, dass es der Klägerin nicht möglich sei, sich gegen bloße Behauptungen zu verteidigen, und daher ihre Rechte zur Verteidigung vor dem Gericht beeinträchtigt würden.

58 Hierzu ist darauf hinzuweisen, dass die Frage der Zulässigkeit von Beweisangeboten beim Gericht, die in Art. 85 der Verfahrensordnung geregelt ist, von der Frage der Beweiswürdigung durch die Unionsgerichte zu unterscheiden ist.

59 Nach der Rechtsprechung des Gerichtshofs müssen die Unionsgerichte bei der Kontrolle restriktiver Maßnahmen eine grundsätzlich umfassende Kontrolle der Rechtmäßigkeit sämtlicher Handlungen der Union im Hinblick auf die Grundrechte als Bestandteil der Unionsrechtsordnung gewährleisten (vgl. in diesem Sinne Urteile vom 18. Juli 2013, Kommission u. a./Kadi, C-584/10 P, C-593/10 P und C-595/10 P, EU:C:2013:518, Rn. 97, vom 28. November 2013, Rat/Fulmen und Mahmoudian, C-280/12 P, EU:C:2013:775, Rn. 58, und vom 28. März 2017, Rosneft, C-72/15, EU:C:2017:236, Rn. 106).

60 Grundrechtsrang haben u. a. das Recht auf Achtung der Verteidigungsrechte und das Recht auf effektiven gerichtlichen Rechtsschutz (vgl. Urteil vom 28. November 2013, Rat/Fulmen und Mahmoudian, C-280/12 P, EU:C:2013:775, Rn. 59 und die dort angeführte Rechtsprechung; Urteil vom 28. November 2013, Rat/Manufacturing Support & Procurement Kala Naft, C-348/12 P, EU:C:2013:776, Rn. 66).

61 Die durch Art. 47 der Charta gewährleistete Effektivität der gerichtlichen Kontrolle erfordert auch, dass sich das Unionsgericht, wenn es die Rechtmäßigkeit der einer Entscheidung, den Namen einer bestimmten Person oder Organisation in die Liste der Personen und Organisationen, gegen die restriktive Maßnahmen verhängt werden, aufzunehmen oder auf dieser Liste zu belassen, zugrunde liegenden Begründung prüft, vergewissert, dass diese Entscheidung, die eine individuelle Betroffenheit dieser Person bzw. Organisation begründet, auf einer hinreichend gesicherten tatsächlichen Grundlage beruht. Dies setzt eine Überprüfung der Tatsachen voraus, die in der dieser Entscheidung zugrunde liegenden Begründung angeführt werden, so dass sich die gerichtliche Kontrolle nicht auf die Beurteilung der abstrakten Wahrscheinlichkeit der angeführten Gründe beschränkt, sondern auf die Frage erstreckt, ob diese Gründe – oder zumindest einer von ihnen, der für sich genommen als ausreichend angesehen wird, um diese Rechtsakte zu stützen – erwiesen sind (vgl. in diesem Sinne Urteile vom 18. Juli 2013, Kommission u. a./Kadi, C-584/10 P, C-593/10 P und C-595/10 P, EU:C:2013:518, Rn. 119, vom 18. Juni 2015, Ipatau/Rat, C-535/14 P, EU:C:2015:407, Rn. 42, und vom 18. Februar 2016, Rat/Bank Mellat, C-176/13 P, EU:C:2016:96, Rn. 109).

62 In diesem Rahmen ist es im Streitfall nämlich Sache der zuständigen Unionsbehörde, die Stichhaltigkeit der gegen die betroffene Person oder Organisation vorliegenden Gründe nachzuweisen, und nicht Sache dieser Betroffenen, den negativen Nachweis zu erbringen, dass diese Gründe nicht stichhaltig sind (vgl. in diesem Sinne Urteil vom 18. Juli 2013, Kommission u. a./Kadi, C-584/10 P, C-593/10 P und C-595/10 P, EU:C:2013:518, Rn. 121).

63 Anders als die Klägerin meint, folgt hieraus jedoch nicht, dass das angebliche Unvermögen des Rates, die angeführten Gründe für die Aufnahme der Klägerin in Anhang I der Verordnung Nr. 359/2011 nachzuweisen, unterstellt man es als wahr, die Verteidigungsrechte der Klägerin beeinträchtigt.

64 Wie sich aus der oben in Rn. 61 angeführten Rechtsprechung ergibt, ist das Unionsgericht, weil die Wahrung der Effektivität von Art. 47 der Charta es erfordert, im Rahmen der Kontrolle der Rechtmäßigkeit der restriktiven Maßnahmen vielmehr verpflichtet, die Stichhaltigkeit der Gründe, auf denen diese Maßnahmen beruhen, und somit den Beweiswert der hier vom Rat vorgelegten Dokumente zu prüfen.

65 Sodann sind die von der Klägerin geltend gemachten Erwägungen, die im Urteil vom 8. Dezember 2022, HYA u. a. (Unmöglichkeit, Fragen an die Belastungszeugen zu stellen) (C-348/21, EU:C:2022:965), in dem der Gerichtshof mit der Auslegung von Art. 6 Abs. 1 und Art. 8 Abs. 1 der Richtlinie (EU) 2016/343 des Europäischen Parlaments und des Rates vom 9. März 2016 über die Stärkung bestimmter Aspekte der Unschuldsvermutung und des Rechts auf Anwesenheit in der Verhandlung in Strafverfahren (ABl. 2016, L 65, S. 1) sowie von Art. 47 Abs. 2 der Charta befasst war, angestellt wurden, mangels Relevanz für den vorliegenden Fall zurückzuweisen.

66 Es ist darauf hinzuweisen, dass der in Art. 6 Abs. 2 der Konvention zum Schutz der Menschenrechte und Grundfreiheiten und in Art. 48 Abs. 1 der Charta verankerte Grundsatz der Unschuldsvermutung ein Grundrecht darstellt, das dem Einzelnen oder von Einzelnen geführten Einheiten Rechte verleiht, deren Achtung die Unionsgerichte gewährleisten (vgl. Urteil vom 18. Mai 2017, Makhlouf/Rat, T-410/16, nicht veröffentlicht, EU:T:2017:349, Rn. 122 und die dort angeführte Rechtsprechung).

67 Der Grundsatz der Unschuldsvermutung, wonach jede Person, die einer Straftat angeklagt ist, bis zum gesetzlichen Beweis ihrer Schuld als unschuldig gilt, steht dem Erlass von Sicherungsmaßnahmen in Form des Einfrierens von Geldern insoweit nicht entgegen, als diese Maßnahmen nicht dem Ziel der Einleitung eines Strafverfahrens gegen die von ihnen erfassten Personen oder Organisationen dienen. Solche Maßnahmen müssen angesichts der Schwere des Eingriffs jedoch gesetzlich vorgesehen sein, von einer zuständigen Behörde erlassen werden und von begrenzter Dauer sein. Aus obiger Rn. 13 ergibt sich, dass diese ersten beiden Kriterien erfüllt sind. Was ferner die zeitliche Begrenzung anbelangt, ist festzustellen, dass Anhang I der Verordnung Nr. 359/2011 gemäß Art. 12 Abs. 3 und 4 dieser Verordnung in regelmäßigen Abständen, mindestens aber alle zwölf Monate überprüft wird, wobei die Aufnahme einer Person oder Einheit in diesen Anhang gegebenenfalls verlängert oder abgeändert werden kann. Die der Klägerin auferlegten Maßnahmen sind folglich zeitlich begrenzt (vgl. in diesem Sinne Urteil vom 18. Mai 2017, Makhlouf/Rat, T-410/16, nicht veröffentlicht, EU:T:2017:349, Rn. 123 und die dort angeführte Rechtsprechung).

68 Außerdem führen die in Rede stehenden restriktiven Maßnahmen nicht dazu, dass die Vermögenswerte der Klägerin als Erträge aus einer Straftat eingezogen werden, sondern sie werden vorsorglich eingefroren. Diese Maßnahmen sind daher keine Sanktion und enthalten im Übrigen keinen dahin gehenden Vorwurf (vgl. Urteil vom 18. Mai 2017, Makhlouf/Rat, T-410/16, nicht veröffentlicht, EU:T:2017:349, Rn. 124 und die dort angeführte Rechtsprechung).

69 Mit der angefochtenen Verordnung wurde, soweit sie die Klägerin betrifft, keine Feststellung getroffen, dass tatsächlich eine Straftat begangen wurde, sondern die Verordnung wurde im Rahmen und zum Zweck eines verwaltungsrechtlichen Verfahrens mit einer Sicherungsfunktion und dem alleinigen Ziel erlassen, dem Rat die Gewährleistung des Schutzes der Zivilbevölkerung zu ermöglichen (vgl. in diesem Sinne Urteil vom 18. Mai 2017, Makhlouf/Rat, T-410/16, nicht veröffentlicht, EU:T:2017:349, Rn. 125 und die dort angeführte Rechtsprechung).

70 Schließlich ist auch das Vorbringen der Klägerin zurückzuweisen, wonach der Artikel von *The Intercept* als unzulässig zurückzuweisen sei, weil die darin in Bezug genommenen Dokumente nicht zur Akte des vorliegenden Verfahrens gereicht worden seien und das Gericht nach dem Grundsatz des kontradiktorischen Verfahrens nur die Verfahrensdokumente und Beweisstücke berücksichtigen dürfe, die die Parteien zur Kenntnis nehmen und zu denen sie Stellung nehmen konnten. Insoweit genügt der Hinweis, dass die Klägerin Gelegenheit hatte, in ihrem Erwiderungsschriftsatz zu den vom Rat in der Anlage B.11 vorgelegten Beweisstücken, u. a. diesem Artikel, dessen Beweiswert sie im Übrigen bestreitet, Stellung zu nehmen.

71 Im Übrigen ist darauf hinzuweisen, dass die beiden Benutzerhandbücher der Software SIAM, eines in Farsi und das andere in englischer Sprache, direkt von dem Artikel von *The Intercept* aus über einen Hyperlink abrufbar waren, der sich auf S. 3 der vom Rat als Anlage B.11 zur Klagebeantwortung vorgelegten Akte WK 307/2023 INIT befindet.

72 Die Rügen der Klägerin, mit denen sie einen Verstoß gegen die Art. 47 und 48 der Charta und den Grundsatz des kontradiktorischen Verfahrens geltend macht, sind daher zurückzuweisen.

Zum Beweiswert des Artikels von The Intercept

73 Die Klägerin rügt, dass es sich bei dem Artikel von *The Intercept* um eine bloße journalistische Publikation handele, die lediglich nicht verifizierbare Behauptungen enthalte, und der deshalb keinerlei Beweiskraft zukomme.

74 Hierzu ist festzustellen, dass nach ständiger Rechtsprechung für den Gerichtshof und für das Gericht der Grundsatz der freien Beweiswürdigung gilt und dass für die Würdigung der vorgelegten Beweise allein ihre Glaubhaftigkeit maßgeblich ist. Zur Beurteilung des Beweiswerts eines Dokuments ist zudem die Wahrscheinlichkeit der darin enthaltenen Information zu untersuchen. Dabei sind insbesondere die Herkunft des Dokuments, die Umstände seiner Ausarbeitung und sein Adressat zu berücksichtigen, und es ist die Frage zu beantworten, ob es seinem Inhalt nach vernünftig und glaubhaft erscheint (vgl. Urteil vom 31. Mai 2018, Kaddour/Rat, T-461/16, EU:T:2018:316, Rn. 107 und die dort angeführte Rechtsprechung).

75 Da den Unionsbehörden in Drittstaaten keine Ermittlungsbefugnisse zustehen, müssen sie sich bei ihrer Beurteilung *de facto* auf öffentlich zugängliche Informationsquellen, Berichte, Presseartikel, Geheimdienstberichte oder andere ähnliche Informationsquellen stützen (Urteile vom 14. März 2018, Kim u. a./Rat und Kommission, T-533/15 und T-264/16, EU:T:2018:138, Rn. 107, und vom 1. Juni 2022, Prigozhin/Rat, T-723/20, nicht veröffentlicht, EU:T:2022:317, Rn. 59).

76 Vom Rat zu verlangen, dass er selbst vor Ort Ermittlungen hinsichtlich der Wahrheit der Tatsachen führt, die von zahlreichen Medien berichtet wurden, ginge zu weit und wäre unverhältnismäßig (Urteil vom 25. Januar 2017, Almaz-Antey Air and Space Defence/Rat, T-255/15, nicht veröffentlicht, EU:T:2017:25, Rn. 148).

77 Zum Beleg bestimmter Tatsachen darf daher auf Presseartikel zurückgegriffen werden, wenn diese aus mehreren unterschiedlichen Quellen stammen und hinreichend konkrete, präzise und übereinstimmende Angaben zu den darin beschriebenen Tatsachen enthalten (vgl. Urteil vom 11. September 2019, Topor-Gilka und WO Technopromexport/Rat, T-721/17 und T-722/17, nicht veröffentlicht, EU:T:2019:579, Rn. 137 und die dort angeführte Rechtsprechung).

78 Vorliegend hat der Rat die Aufnahme der Klägerin in Anhang I der Verordnung Nr. 359/2011 auf vier Dokumente der Akte WK 307/2023 INIT gestützt, die in der Anlage B.11 zur Klagebeantwortung enthalten sind.

79 Es handelt sich erstens um den Artikel von *The Intercept*, zweitens den am 31. Oktober 2022 von der spezialisierten Internetseite Commsrisk unter dem Titel „Hacker Leaks Manuals Showing How Iran Uses Mobile Networks to Track Protesters“ veröffentlichten Artikel, drittens den am 17. November 2022 auf der Internetseite der Vereinigung ARTICLE 19 unter dem Titel „Iran: New tactics for digital repression as protests continue“ veröffentlichten Artikel und viertens den am 3. November 2022 von dem investigativen Onlinemagazin *The Tech Monitor* unter dem Titel „Iran is using spyware to track citizens attending protests“ veröffentlichten Artikel.

80 Die Klägerin macht geltend, der Rat stütze die angefochtene Verordnung, soweit sie sie betreffe, ausschließlich auf die Behauptungen, die in dem Artikel von *The Intercept* enthalten und ihrerseits auf die Aussagen einer anonymen Person gestützt seien.

81 Hierzu ist anzumerken, dass der Artikel von *The Intercept* enthüllt, dass die Autoren dieses Artikels auf der Grundlage interner Dokumente eines iranischen Mobilfunkbetreibers, u. a. E-Mail-Verkehr mit den Führungspersonen der Klägerin und zwei Benutzerhandbücher einer Software namens SIAM, eines davon in englischer Sprache, eines in Farsi, herausgefunden haben, wie die iranischen Behörden über die Klägerin ein im Hintergrund der iranischen Mobilfunknetze agierendes System eingerichtet hatten, das es der iranischen Regierung ermöglichte, das Anrufverschlüsselungssystem zu umgehen, die Bewegungen eines sich an einem bestimmten Ort

befindenden Telefonnutzers zu verfolgen, alle Kontakte eines Telefonnutzers zu analysieren und die Internetverbindung des Nutzers zu unterbrechen oder zu verlangsamen, und das eingesetzt wurde, um die iranische Bevölkerung nach dem Tod von Frau Amini im Jahr 2022 zu unterdrücken und zu kontrollieren. Dieser Artikel erklärt ferner, dass laut der englischen Fassung des Benutzerhandbuchs der Software SIAM „[n]ach den Regeln und Vorschriften der [Klägerin] alle Telekommunikationsbetreiber [dieser] direkten Zugang zu ihrem System gewähren [müssen], um die Kundeninformationen abzufragen (*sic*) und ihre Dienste über den Webservice zu ändern“, und darüber hinaus technische Informationen zu den mächtigsten Befehlen enthält, die von der Software SIAM verwendet werden, um Daten über die Nutzer direkt bei den iranischen Mobilfunkbetreibern zu erfassen.

82 Ferner ist anzumerken, dass die Autoren des Artikels von *The Intercept* dafür Sorge getragen haben, zwei als Experten vorgestellte Personen zu befragen.

83 Die erste als Experte vorgestellte Person ist, anders als von der Klägerin behauptet, nicht „irgendjemand, den niemand kennt und der über keine besondere Legitimität zu verfügen scheint“. Aus der Akte ergibt sich vielmehr, dass diese erste Person Forscher beim CitizenLab Canada ist, einem interdisziplinären Labor an der Universität Toronto (Kanada), das auf die „Forschung, Entwicklung, Strategiepolitik auf hohem Niveau und rechtliches Engagement an der Schnittstelle der Informations- und Kommunikationstechnologien, der Menschenrechte und der globalen Sicherheit“ spezialisiert ist, und bereits in einem am 1. Februar 2022 von der renommierten Zeitung *The Guardian* veröffentlichten Artikel als Experte vorgestellt worden war.

84 Ebenso ergibt sich aus der Akte, dass sich die zweite in dem Artikel von *The Intercept* als Experte vorgestellte Person als Leiter des Bereichs Digitale Rechte und Sicherheit der MIAAN Group, einer Organisation mit Sitz in Texas (Vereinigte Staaten), die „die Menschenrechte in Iran verteidigt“, bezeichnet und zahlreiche Male von der internationalen Presseagentur Reuters in dieser Funktion vorgestellt wurde. Der bloße Umstand, dass „[es sich] bekanntermaßen [um] eine Person des öffentlichen Lebens [handelt], die sich offen und vorbehaltlos gegen die iranische Regierung engagiert“, führt entgegen der Ansicht der Klägerin nicht zwangsläufig dazu, dass den Aussagen dieser Person mit der Begründung, dass sie nicht neutral und unparteiisch sei, jegliche Relevanz abzusprechen wäre.

85 Die Erfahrung einer solchen Person, die auf die Verteidigung der Menschenrechte, insbesondere der digitalen Rechte, spezialisiert ist und die von der Klägerin selbst als Gegner des iranischen Regimes bezeichnet wird, ist für eine sachdienliche Beurteilung der Art und Weise, wie die iranischen Behörden ein System wie das in dem Artikel von *The Intercept* beschriebene einsetzen könnten, um diese Rechte zu beschneiden, von Relevanz.

86 Im Übrigen ist hervorzuheben, dass der auf der Seite von *The Intercept* veröffentlichte Artikel nicht bloße Behauptungen aufgestellt hat und nicht einmal lediglich Expertenmeinungen wiedergegeben hat, sondern darüber hinaus seine Behauptungen und Meinungen dadurch untermauert hat, dass er das Benutzerhandbuch der Software SIAM in englischer Sprache, dessen direkten Abruf er in einem Visualisierungsfenster ermöglicht hat, und das zweite, in Farsi verfasste Handbuch, das das Logo der Klägerin trug, zur Verfügung gestellt hat.

87 Was ferner die anderen in der Akte WK 307/2023 INIT enthaltenen Artikel anbelangt, ist darauf hinzuweisen, dass die Internetseite Commsrisk, die sich als „eine Website, die über die Risiken, denen Anbieter elektronischer Kommunikation und ihre Kunden ausgesetzt sind, berichtet“, beschreibt, und *The Tech Monitor*, der nach eigener Definition „Unternehmensleitungen,

IT-Verantwortlichen und politisch Verantwortlichen in einer von der Technologie bewegten und inspirierten Welt datenbasierte Informationen und verlässliche Analysen“ bieten soll, auf den Bereich der Telekommunikation spezialisierte Medien sind und dass die Vereinigung ARTICLE 19 mit Sitz in London (Vereinigtes Königreich) sich als „eine internationale Denkfabrik, die die Bewegung für die freie Meinungsäußerung auf lokaler und globaler Ebene unterstützt, um zu gewährleisten, dass alle Individuen die Macht ihrer Stimme verwirklichen“ beschreibt, so dass sie als relevante Informationsquellen in Bezug auf die Verwendung von Informations- und Kommunikationstechnologien im Zusammenhang mit der Ausübung der Grundrechte und insbesondere des Rechts auf freie Meinungsäußerung zu betrachten sind.

88 Die Artikel von Commsrisk, ARTICLE 19 und *The Tech Monitor* beziehen sich zwar alle drei auf den Artikel von *The Intercept*, der Artikel von Commsrisk berichtet jedoch auch von der Erfahrung seines Autors, der den Vertreter eines Technologieunternehmens getroffen haben soll, der versucht habe, Iran eine Software mit „seltsamerweise ähnlichen“ Funktionen wie denjenigen der Software SIAM zu verkaufen, und der ihm bereitwillig Informationen in Bezug auf diesen Verkauf geliefert habe.

89 Darüber hinaus ergibt sich aus dem Artikel der Vereinigung ARTICLE 19, dass diese das Ausmaß der Kontrolle, die in Iran über das Internet ausgeübt wird, seit mehreren Jahren beobachtet hat und dass sie in einem unter dem Titel „Iran Tightening the Net 2020“ veröffentlichten Bericht die Funktionsweise der Internetinfrastruktur in diesem Land und ihre Verwaltung durch die Behörden enthüllt hat. Insbesondere existiert danach ein zentralisiertes System, das es ermöglicht, den Internetzugang bei Demonstrationen abzuschalten, bei denen die Verwaltung und Kontrolle des Internets als eine Frage der nationalen Sicherheit betrachtet wird. Die Vereinigung ARTICLE 19 hat diesem Bericht zufolge herausgefunden, dass die Klägerin unter der Kontrolle des Ministeriums für Kommunikation, das in Wirklichkeit vom Nachrichtendienst kontrolliert werde, Überwachungs- und Zensurinstrumente auf der Ebene der Internetanbieter installiere und im Auftrag des Obersten Nationalen Sicherheitsrats Abschaltungen und andere Störungen des Internetzugangs anordne. Der Artikel der Vereinigung ARTICLE 19 berichtet ferner, dass die iranischen Behörden Technologien, die die Verwendung von Tools wie virtuellen privaten Netzwerken (VPN) blockieren, mit denen Internetbeschränkungen umgangen werden können, sowie Abschaltungen oder schwerwiegende Störungen der mobilen Internetverbindung als Taktiken digitaler Unterdrückung eingesetzt haben. Abschaltungen des mobilen Internetzugangs würden seit November 2019 immer häufiger eingesetzt. Derartige Abschaltungen seien insbesondere während der regionalen Demonstrationen seit 2021 bis zum gegenwärtigen Zeitpunkt genutzt worden. Die mobilen Internetverbindungen seien an zahlreichen Orten an den meisten Tagen, die auf die Demonstrationen nach dem Tod von Frau Amini folgten, deaktiviert worden. Diese Abschaltungen hätten die größten Anbieter des mobilen Internetzugangs im ganzen Land betroffen, was in einem Land, in dem das mobile Internet die Hauptquelle des Internetzugangs der Bevölkerung ist, negative Auswirkungen auf den Internetzugang gehabt habe.

90 Aus dem Vorstehenden ergibt sich somit, dass die in dem Artikel von *The Intercept* aufgestellten Behauptungen durch die anderen in der Akte WK 307/2023 INIT enthaltenen Beweisstücke bekräftigt werden und dass sich der Rat folglich entgegen dem Vorbringen der Klägerin nicht allein auf die in diesem Artikel aufgestellten Behauptungen gestützt hat. Mithin durften diese Behauptungen angesichts der Übereinstimmung der verschiedenen Beweisstücke und der oben genannten Umstände ihrer Entstehung berücksichtigt werden.

Zur materiellen Rechtmäßigkeit der Aufnahme des Namens der Klägerin

91 Vorab ist darauf hinzuweisen, dass die Klägerin zwar geltend macht, der Rat habe vorliegend einen „offensichtlichen Fehler bei der Beurteilung des Sachverhalts“ begangen, ihr diesbezügliches Vorbringen jedoch als Bestreiten der sachlichen Richtigkeit der ihr zur Last gelegten Tatsachen anzusehen ist. Aus der oben in Rn. 42 wiedergegebenen Argumentation, auf die die Klägerin den vorliegenden Klagegrund stützt, ergibt sich nämlich, dass die Klägerin sich nicht dagegen wendet, dass die ihr zur Last gelegten Tatsachen von den Aufnahmekriterien nach Art. 3 Abs. 1 und 2 der Verordnung (EU) Nr. 359/2011 gedeckt sein können, sondern geltend macht, diese Tatsachen entsprächen nicht der Realität.

92 Insoweit ergibt sich aus der oben in Rn. 62 angeführten Rechtsprechung, dass die Kontrolle durch die Unionsgerichte eine Überprüfung der Tatsachen voraussetzt, die in der der Entscheidung über die Verhängung restriktiver Maßnahmen gegen eine Organisation zugrunde liegenden Begründung angeführt sind, und dass diese Überprüfung sich nicht auf die Beurteilung der abstrakten Wahrscheinlichkeit der angeführten Gründe beschränkt, sondern sich auf die Frage erstreckt, ob diese Gründe – oder zumindest einer von ihnen, der für sich genommen als ausreichend angesehen wird, um diese Entscheidung zu stützen – erwiesen sind.

93 Bei der Beurteilung der Stichhaltigkeit dieser Gründe sind die Beweise und die Informationen nicht isoliert, sondern in dem Zusammenhang zu prüfen, in dem sie stehen. Der Rat erfüllt die ihm obliegende Beweislast, wenn er vor dem Unionsgericht auf ein Bündel von Indizien hinweist, die hinreichend konkret, genau und übereinstimmend sind und die Feststellung ermöglichen, dass eine hinreichende Verbindung zwischen der Person, die einer restriktiven Maßnahme unterworfen ist, und dem bekämpften Regime oder ganz allgemein den bekämpften Situationen besteht (vgl. in diesem Sinne Urteil vom 20. Juli 2017, Badica und Kardiam/Rat, T-619/15, EU:T:2017:532, Rn. 99 und die dort angeführte Rechtsprechung).

94 Im Licht dieser Erwägungen ist zu prüfen, ob der Rat bei Erlass der angefochtenen Verordnung zu Recht der Ansicht war, dass die Klägerin restriktiven Maßnahmen unterworfen werden durfte.

95 Erstens ist in Bezug auf die von der Klägerin angeführten Bestimmungen des iranischen Rechts, die belegen sollen, dass sie rechtlich daran gehindert sei, die Kommunikation der Nutzer der iranischen Mobilfunknetze zu überwachen und zu kontrollieren, darauf hinzuweisen, dass nach dem Wortlaut von Art. 25 der Verfassung der Islamischen Republik Iran „[d]ie Inspektion und die Nichtzustellung von Briefen, die Aufnahme und Offenlegung von Telefongesprächen, die Offenlegung von telegrafischer oder fernschriftlicher Kommunikation, die Zensur, … das heimliche Abhören und jede Form der Überwachung untersagt sind, es sei denn, sie erfolgen in Übereinstimmung mit dem Gesetz“.

96 Art. 582 des iranischen Strafgesetzbuchs bestimmt:

„Ein Staatsbediensteter oder Beamter, der sich in anderen als den gesetzlich erlaubten Fällen ohne die Erlaubnis des Eigentümers Zugang zu Briefen oder telegrafischer oder telefonischer Kommunikation von Personen verschafft oder sich dieser bemächtigt, sie vernichtet, inspiziert, aufnimmt oder überwacht oder ihren Inhalt offenlegt, wird mit Freiheitsstrafe von einem Jahr bis zu drei Jahren oder mit Geldstrafe von 6 bis 18 Mio. [R]ial bestraft.“

97 Art. 104 der iranischen Strafprozessordnung bestimmt:

„Die Kontrolle [(Überwachung)] der Telekommunikation von Privatpersonen ist untersagt, es sei denn, sie weist einen Bezug zur inneren oder äußeren Sicherheit des Landes auf oder wird als für die Ermittlung von Straftaten nach Art. 302 Buchst. a, b, c und d des vorliegenden Gesetzbuches notwendig erachtet. In diesem Fall wird die Überwachung mit Genehmigung des Präsidenten des Obersten Provinzgerichts durchgeführt und die Dauer und Häufigkeit der Überwachung festgelegt. Die Überwachung von Telefongesprächen der in Art. 307 des vorliegenden Gesetzbuchs genannten Personen und Beamten bedarf der Genehmigung des Präsidenten des Obersten Gerichtshofs, und diese Befugnis kann nicht auf andere Personen übertragen werden."

98 Aus diesen Bestimmungen ergibt sich, dass die Telekommunikationsüberwachung zwar grundsätzlich untersagt ist, jedoch u. a. „in Fällen, in denen sie einen Bezug zur inneren oder äußeren Sicherheit des Landes aufweist oder wegen [bestimmter Straftaten] als notwendig erachtet wird", oder, wenn „die Angelegenheit einen Bezug zur Sicherheit des Landes aufweist", rechtlich möglich bleibt. Überdies sind die Fälle, in denen die Telekommunikationsüberwachung rechtlich möglich ist, sehr weit gefasst.

99 Dem Vorbringen der Klägerin widerspricht zudem auch die englische Fassung des Benutzerhandbuchs der Software SIAM, deren Authentizität die Klägerin nicht in Frage stellt und worin es heißt, dass „[n]ach den Regeln und Vorschriften der [Klägerin] alle Telekommunikationsbetreiber [dieser] direkten Zugang zu ihrem System gewähren [müssen], um die Kundeninformationen abzufragen (*sic*) und ihre Dienste über den Webservice zu ändern".

100 Zweitens ist hinsichtlich der angeblich fehlenden technischen Fähigkeit der Klägerin, Operationen zur Überwachung und Kontrolle der Nutzer der iranischen Mobilfunknetze durchzuführen, festzustellen, dass dies nicht zutrifft.

101 Insoweit ist hervorzuheben, dass die Klägerin die Existenz der Software SIAM und auch die Existenz der Befehle „Force2GNumber", „LocationCustomerList", „GetCDR", „GetIPDR" und „ApplySusplp" sowie der Systeme „Legal Intercept" (LI), „Control Illegal Devices" (CID), „SHAHKAR" und „SHAMSA" nicht bestreitet. Die Klägerin bestreitet auch nicht, dass sie die Software SIAM sowie die genannten Systeme nutzt. Ebenso wenig bestreitet die Klägerin die Authentizität des E-Mail-Verkehrs zwischen ihren Führungspersonen und dem in dem Artikel von *The Intercept* genannten Mobilfunkbetreiber. Auch die Authentizität der beiden Benutzerhandbücher der Software SIAM in englischer Sprache und in Farsi bestreitet sie nicht.

102 Die Klägerin beschränkt sich vielmehr darauf, zum einen geltend zu machen, dass die Verwendung dieser Befehle entweder nicht die vom Rat beschriebene Wirkung habe oder einem legitimen Zweck entspreche, und zum anderen, dass der Einsatz der Systeme „Legal Intercept" (LI), „Control Illegal Devices" (CID), „SHAHKAR" und „SHAMSA" in den meisten Staaten verbreitet sei.

103 In dieser Hinsicht ist noch einmal zu wiederholen, dass es in der englischen Fassung des Benutzerhandbuchs der Software SIAM heißt, dass „[n]ach den Regeln und Vorschriften der [Klägerin] alle Telekommunikationsbetreiber [dieser] direkten Zugang zu ihrem System gewähren [müssen], um die Kundeninformationen abzufragen (*sic*) und ihre Dienste über den Webservice zu ändern".

104 Ferner ist darauf hinzuweisen, dass es in der Einleitung des Benutzerhandbuchs der Software SIAM in Farsi nach der vom Rat vorgelegten französischen Übersetzung heißt, dass es das Ziel dieser Software sei, „ein einziges zentralisiertes und zusammengeführtes System für Anfragen an die verschiedenen Server zu schaffen“ und „die Verwaltung und Kontrolle der Kommunikation und der Aktivitäten der Nutzer zu ermöglichen“.

105 Des Weiteren heißt es in dem Abschnitt „Kommunikationsgrundsätze“ dieses Handbuchs, dass „die Eingangsparameter in den von der Software SIAM gesandten Informationen zu jeder Methode (Funktion) der Anfrage an den Betreiber sind und [dass] die Ausgangsparameter die Daten der Antwort auf die Anfrage (und die Reihenfolge ihrer Klassifizierung) sind [und dass d]ie Betreiber die Antwort jeder angefragten Funktion genau in der Reihenfolge und Zusammensetzung an SIAM senden müssen, die in dem Abschnitt über die Ausgangsparameter der jeweiligen Funktion beschrieben sind“.

106 Ferner wird in diesem Handbuch ausgeführt, dass die Betreiber verpflichtet sind, „Anfragen der Software SIAM Tag und Nacht (24/7) zu beantworten“ und sich zu vergewissern, dass „die gesamte notwendige Ausstattung in den Bereichen Computer, Software, Netzwerkkommunikation und Sicherheit wie Datenredundanz (Redundancy), Lastverteilung (Road Balancing), Firewalls (Firewall) vorhanden und alle weiteren Voraussetzungen erfüllt sind“.

107 Aus diesen Feststellungen ergibt sich, dass die Befehle der Software SIAM an alle iranischen Mobilfunkbetreiber ergehen und dass diese verpflichtet sind, diese Befehle jederzeit in der vorgeschriebenen Weise auszuführen.

108 Im Licht dieser Feststellungen ist das Vorbringen der Klägerin in Bezug auf die Befehle der Software SIAM und die Systeme „Legal Intercept“ (LI), „Control Illegal Devices“ (CID), „SHAHKAR“ und „SHAMSA“ zu beurteilen.

109 Was den Befehl „LocationCustomerList“ anbelangt, trägt die Klägerin vor, dieser ermögliche es nicht, einem einzelnen Mobilfunknetznutzer präzise zu folgen, da dieser Befehl lediglich ermögliche, die Nutzer eines Mobilfunknetzes in einem Umkreis von 200 m bis 2 km eines GSM-Sendemasten zu identifizieren. Allerdings räumt die Klägerin ein, dass dieser Befehl die Identifizierung aller Nutzer eines Mobilfunknetzes, die sich in einem bestimmten – wenn auch nur näherungsweise umrissenen – geografischen Gebiet befinden, ermöglicht. Dies geht auch eindeutig aus der Beschreibung dieses Befehls in der englischen Fassung des Benutzerhandbuchs der Software SIAM hervor, worin es heißt, dass „diese Funktion, die einen Ortsparameter erhält, eine Liste der Nummern ausgeben soll, die sich an diesem Ort befinden“. Ferner ergibt sich aus dem in Farsi verfassten Handbuch, dass der Befehl „IdentitySearch“ die Betreiber verpflichtet, die Ergebnisse in Form einer „Tabelle“ zu übersenden, in der bei natürlichen Personen die Telefonnummer, der Vorname, der Name, der Vorname des Vaters, die Nummer der Geburtsurkunde, das Geburtsdatum, die Postleitzahl, die Staatsangehörigkeit, die Reisepassnummer, die Postanschrift(en), die Zahlungsart (Vorkasse/nachträgliche Zahlung), Verbindungstyp (SIM-Karte/Sonstiges), das Datum der Zuteilung, die IP-Adresse sowie der geografische Längengrad und der geografische Breitengrad der Adresse anzugeben sind.

110 Hinsichtlich des Befehls „Force2GNumber“ trägt die Klägerin vor, dass dieser entgegen dem Vorbringen des Rates das Risiko, dass die Kommunikation gehackt wird, nicht vergrößere. Allerdings stellt der Umstand, dass dieser Befehl das Risiko von Hacking nicht vergrößert – als wahr unterstellt –, die Feststellung nicht in Frage, dass ein solcher Befehl, der dazu dient, ein

Mobiltelefon zur Nutzung des 2G-Netzes anstelle der neueren 3G- und 4G-Netze zu zwingen, bewirkt, dass über dieses Telefon keine Videos angesehen und geteilt werden können, wie der Rat zu Recht anmerkt.

111 Was die Befehle „GetCDR“ und „GetIPDR“ anbelangt, dienen diese nach dem Vortrag der Klägerin im Fall von „GetCDR“ der Abfrage der Anrufhistorie eines Telefons und im Fall von „GetIPDR“ der Erlangung der IP-Adresse der Geräte, in denen eine bestimmte SIM-Karte aktiviert wurde. Diese Funktionen dienten ausschließlich der Erfüllung gerichtlicher Ermittlungsersuchen und seien essenzielle Instrumente, die den Gerichten zur Verfügung stünden, wie sich den Gerichtsbeschlüssen und polizeilichen Schreiben in der Anlage zur Erwiderung entnehmen lasse. Die Klägerin hat jedoch zum einen keinen tauglichen Beweis dafür angetreten, dass dieser Befehl ausschließlich zur Erfüllung rechtmäßiger Ersuchen der iranischen Gerichte und Polizeibehörden eingesetzt werden kann. Zum anderen sind die Fälle, in denen die Telekommunikationsüberwachung rechtlich möglich ist, wie bereits oben in Rn. 98 angemerkt, sehr weit gefasst.

112 Die Befehle „ApplySusp“ und „ApplySuspIP“ ermöglichen nach dem Vortrag der Klägerin die Sperrung von SIM-Karten, deren Verlust oder Diebstahl die Nutzer angezeigt haben oder die für verstorben erklärten Personen gehören. Die Klägerin hebt hervor, dass es sich dabei um eine Funktion handelt, die absoluter Standard und mit der von Regulierungsbehörden anderer Staaten wie Deutschland eingesetzten Funktion vergleichbar sei. Insoweit ergibt sich aus dem am 16. Januar 2015 von der kanadischen Immigrations- und Flüchtlingskommission unter dem Titel „Iran: Government surveillance capacity and control, including media censorship and surveillance of individual Internet activity““ („Iran: Überwachungskapazität der Regierung und von dieser ausgeübte Kontrolle, einschließlich Medienzensur und Überwachung der Internetnutzung“) veröffentlichten Bericht (Anlage B.8), aus dem von Amnesty International am 16. November 2020 veröffentlichten Bericht über die Demonstrationen von November 2019 in Iran und die Internet-Abschaltungen (Anlage B.10) und dem von der Presseagentur Human Rights Activists News Agency (HRANA) am 8. Dezember 2022 veröffentlichten Bericht, der eine statistische Untersuchung, Analyse und Synthese der ersten 82 Tage der Demonstrationen enthält und die geschätzte Zahl der Todesfälle und Festnahmen angibt (Anlage B.3), sowie dem von Freedom House veröffentlichten Bericht aus dem Jahr 2022, der sich mit der Internetfreiheit in Iran befasst (Anlage B.6), dass die Situation in Iran von regelmäßigen Protesten der Zivilgesellschaft gegen das Regime geprägt ist, die von den Behörden dieses Landes u. a. mit Hilfe von Mitteln der Internetüberwachung systematisch unterdrückt werden. Unter diesen Umständen kann, wie der Rat anmerkt, nicht ausgeschlossen werden, dass ursprünglich zu „legalen“ Zwecken entwickelte Befehle wie „ApplySusp“ und „ApplySuspIP“ von den iranischen Behörden zweckentfremdet und zu repressiven Zwecken eingesetzt werden.

113 Was die Funktionskomponenten des Kommunikationsüberwachungssystems von Iran anbelangt, führt die Klägerin aus, das System „SHAHKAR“ sei ein Netzwerk, das lediglich der Identitätsprüfung des Kommunikationsnutzers bei der SIM-Karten-Zuteilung zur Betrugsprävention diene. Dieses System stelle Informationen über die Person zusammen, der die jeweilige SIM-Karte oder Festnetzverbindung zugeordnet sei, und erstelle eine Datenbank, die zur Bekämpfung von Betrug, Belästigungen und anderen strafbaren Handlungen eingesetzt werde. Die Klägerin trägt allerdings auch vor, dass dieses System u. a. den iranischen Mobilfunkbetreibern ermögliche, die Identität der Nutzer von Kommunikationsdiensten zu verifizieren. Wie oben in Rn. 107 festgestellt, ergehen die Befehle der Software SIAM an alle iranischen Mobilfunkbetreiber und diese sind verpflichtet, sie jederzeit in der vorgeschriebenen Weise auszuführen und der Software SIAM permanenten Zugang zu den Daten, die sie über die

Nutzer besitzen, zu gewähren. Folglich vermag die Erklärung der Klägerin die Behauptung des Rates, das System „SHAHKAR“ stelle eine Funktionskomponente des Kommunikationsüberwachungssystems der iranischen Behörden dar, nicht zu entkräften.

114 Was das System „SHAMSA“ anbelangt, tritt die Klägerin dem Vorbringen des Rates entgegen, es handele sich dabei um eine „Schnittstelle für die Erfassung von Sprachdaten und SMS in großen Mengen (CDR) und von IP-Daten (IPDR)“. Der Klägerin zufolge handelt es sich um ein reines „Kommunikationsnetzwerk zwischen [ihr] und den [Mobilfunkb]etreibern, worüber Letztere durch die Eingabe von Codes und Befehlen interagieren“. Angesichts der oben in Rn. 107 getroffenen Feststellung, wonach die Befehle der Software an alle iranischen Mobilfunkbetreiber ergehen und diese sie jederzeit in der vorgeschriebenen Weise ausführen müssen, und angesichts dessen, dass im Inhaltsverzeichnis des in Farsi verfassten Benutzerhandbuchs der Software SIAM – nach der vom Rat eingereichten französischen Übersetzung – ein Befehl zur Weiterleitung von SMS an eine Nummer genannt ist, sind die Ausführungen der Klägerin jedoch wiederum wenig überzeugend.

115 Was das System „CID“ anbelangt, macht die Klägerin geltend, dieses ermögliche es, die Gerätenummer, Mobiltelefonnummer und SIM-Karten-Nummer in Übereinstimmung zu bringen. Die Funktion dieses Systems bestehe ausschließlich in der Identifizierung und Kontrolle der Rechtmäßigkeit des Imports von Mobiltelefonen und elektronischen Geräten, in die eine SIM-Karte eingelegt werden könne, um diese Informationen anschließend den Telekommunikationsbetreibern zu übermitteln. Nochmals ist darauf hinzuweisen, dass über das angegebene legitime Ziel hinaus die iranischen Mobilfunkbetreiber verpflichtet sind, der Klägerin über die Software SIAM permanenten Zugang zu den Informationen zu gewähren, die sie über ihre Nutzer besitzen, so dass die Klägerin auf diese Weise auf die von dem System „CID“ zusammengetragenen Daten zugreifen kann.

116 Was schließlich das System „LI“ anbelangt, räumt die Klägerin ein, dass es sich um ein Sicherheitssystem handelt, das es ermöglicht, einen Netzbetreiber zu ersuchen, abgefangene Kommunikationsvorgänge von Einzelpersonen oder Organisationen zu sammeln und den Ordnungskräften zur Verfügung zu stellen. Die Klägerin betont, dass dieses System durch die einschlägigen Vorschriften des iranischen Rechts an strenge Voraussetzungen gebunden sei. Allerdings ergibt sich, wie oben in Rn. 98 festgestellt, aus den Vorschriften des iranischen Rechts, die die Klägerin selbst anführt, dass die Fälle, in denen die Telekommunikationsüberwachung rechtlich möglich ist, sehr weit gefasst sind.

117 Angesichts der oben in den Rn. 95 bis 115 dargestellten Erwägungen hat der Rat vor dem Gericht auf ein Bündel von Indizien hingewiesen, die hinreichend konkret, genau und übereinstimmend sind und die Feststellung ermöglichen, dass im vorliegenden Fall eine hinreichende Verbindung zwischen der Klägerin und der bekämpften Situation, namentlich der Unterdrückung friedlicher Demonstranten, Journalisten, Menschenrechtsverteidiger, Studierender und anderer Personen durch die iranischen Behörden, besteht.

118 Demnach sind die Rügen zurückzuweisen, mit denen die Klägerin die sachliche Unrichtigkeit des Sachverhalts geltend macht.

119 Der dritte Klagegrund ist folglich in vollem Umfang als unbegründet zurückzuweisen.

Zum vierten Klagegrund: Verstoß gegen den Verhältnismäßigkeitsgrundsatz

120 Die Klägerin macht geltend, dass die restriktiven Maßnahmen, denen sie aufgrund ihrer Aufnahme in Anhang I der Verordnung Nr. 359/2011 unterworfen ist, gegen den Grundsatz der Verhältnismäßigkeit verstießen.

121 Insoweit trägt sie erstens vor, dass die in der Vergangenheit gegen Iran verhängten „internationalen Sanktionen“ dazu geführt hätten, dass ihr besonders nützliche Instrumente vorenthalten würden, von denen das eine verwendet werde, um eine Überschneidung zwischen iranischen Frequenzen und denen der Nachbarstaaten zu verhindern, und das andere, das Location Based System, für die genaue Lokalisierung verbundener Geräte. Darüber hinaus würden die Iran gegenwärtig auferlegten Sanktionen die Klägerin daran hindern, ihre Rolle in Bezug auf die Frequenzregulierung zu erfüllen und sicherzustellen, dass das nationale Telekommunikationsnetzwerk reibungslos funktioniere.

122 Zweitens trägt die Klägerin vor, dass die „Sanktionen“ sie an der Mitgliedschaft in der Global System for Mobile Communications Association (GSMA) hindern würden und dass sie daher das Register der GSMA nicht nutzen könne, um die Reparatur gefälschter und illegaler Geräte zu unterbinden. Dies ziehe mehrere schädliche Folgen nach sich, so könne Iran u. a. Betrug und die Schaffung eines Parallelmarkts für gestohlene Telefone nicht wirksam bekämpfen und sei nicht fähig, gestohlene Telefone ihren Eigentümern zurückzugeben.

123 Der Rat tritt dem Vorbringen der Klägerin entgegen.

124 Es ist darauf hinzuweisen, dass nach dem Grundsatz der Verhältnismäßigkeit, der zu den allgemeinen Grundsätzen des Unionsrechts gehört, die Rechtmäßigkeit des Verbots einer wirtschaftlichen Tätigkeit davon abhängt, dass die Verbotsmaßnahmen zur Erreichung der mit der fraglichen Regelung zulässigerweise verfolgten Ziele geeignet und erforderlich sind, wobei für den Fall, dass mehrere geeignete Maßnahmen zur Auswahl stehen, die am wenigsten belastende zu wählen ist und die verursachten Nachteile in angemessenem Verhältnis zu den angestrebten Zielen stehen müssen (vgl. Urteil vom 6. September 2013, Bank Melli Iran/Rat, T-35/10 und T-7/11, EU:T:2013:397, Rn. 179 und die dort angeführte Rechtsprechung).

125 Außerdem stellt die Achtung der Grundrechte zwar eine Rechtmäßigkeitsvoraussetzung der Unionsrechtsakte dar, diese Grundrechte genießen im Unionsrecht jedoch keinen uneingeschränkten Schutz, sondern sie müssen im Hinblick auf ihre gesellschaftliche Funktion gesehen werden. Folglich kann die Ausübung dieser Rechte Beschränkungen unterworfen werden, sofern diese tatsächlich dem Gemeinwohl dienenden Zielen der Union entsprechen und nicht einen im Hinblick auf den verfolgten Zweck unverhältnismäßigen und nicht tragbaren Eingriff darstellen, der die so gewährleisteten Rechte in ihrem Wesensgehalt antasten würde (vgl. Urteil vom 13. September 2013, Makhlouf/Rat, T-383/11, EU:T:2013:431, Rn. 97 und die dort angeführte Rechtsprechung; Urteil vom 16. Januar 2019, Haswani/Rat, T-477/17, nicht veröffentlicht, EU:T:2019:7, Rn. 74).

126 Vorliegend hat die Klägerin nicht dargetan, dass die von der Verordnung Nr. 359/2011 vorgesehen restriktiven Maßnahmen, denen sie aufgrund des Erlasses der angefochtenen Verordnung unterworfen ist, kein legitimes Ziel verfolgen, nicht erforderlich oder nicht angemessen sind, um dieses Ziel zu erreichen. Vielmehr macht sie im Wesentlichen lediglich geltend, dass sich die internationalen Sanktionen, die Iran in der Vergangenheit auferlegt worden

seien, auf ihre Fähigkeit, ihre Aufgaben zu erfüllen, nachteilig ausgewirkt hätten; den notwendigen Zusammenhang mit den von der Verordnung Nr. 359/2011 vorgesehenen Maßnahmen zeigt sie nicht auf.

127 Jedenfalls besteht eines der mit der Verordnung Nr. 359/2011 verfolgten Ziele, wie sich aus ihren Erwägungsgründen 1 und 2 im Wesentlichen ergibt, darin, auf bestimmte Personen und Organisationen, die für die Anordnung oder Begehung schwerer Menschenrechtsverletzungen im Zuge der Repression gegen friedliche Demonstranten, Journalisten, Menschenrechtsverteidiger, Studenten oder andere Menschen, die für ihre legitimen Rechte einschließlich des Rechts auf freie Meinungsäußerung eintreten, verantwortlich sind, Druck auszuüben, indem ihre Gelder und wirtschaftlichen Ressourcen eingefroren werden.

128 Dieses Ziel entspricht einem legitimen Ziel der Gemeinsamen Außen- und Sicherheitspolitik (GASP), nämlich dem in Art. 21 Abs. 2 Buchst. b EUV genannten Ziel, Demokratie, Rechtsstaatlichkeit, die Menschenrechte und die Grundsätze des Völkerrechts zu festigen und zu fördern.

129 Ferner können die in der Verordnung Nr. 359/2011 vorgesehenen restriktiven Maßnahmen angesichts der Schlüsselrolle der Klägerin bei der Umsetzung der Anordnungen der iranischen Regierung, Internet-Inhalte durch die Spähsoftware SIAM zu filtern, wie sie sich aus der Prüfung des dritten Klagegrundes ergibt, nicht als unangemessen angesehen werden.

130 Außerdem sind diese Maßnahmen als erforderlich anzusehen, da, worauf der Rat zu Recht hinweist, nicht dargetan ist, dass alternative, weniger einschneidende Maßnahmen wie ein System der vorherigen Genehmigung der Verwendung ausgezahlter Gelder oder eine nachträgliche Rechenschaftspflicht das verfolgte Ziel ebenso wirksam erreichen könnten.

131 Mithin ist der vierte Klagegrund als unbegründet zurückzuweisen.

Zum ersten Klagegrund: Befugnismissbrauch

132 Wenngleich die Klägerin die Zuständigkeit des Rates für den Erlass der angefochtenen Verordnung nicht in Frage stellt, macht sie geltend, dass diese Verordnung insofern fehlerbehaftet sei, als der Rat, was sie betreffe, seine Befugnisse überschritten habe. Diese Befugnisüberschreitung ergebe sich daraus, dass der wahre Grund, der den Rat veranlasst habe, ihren Namen in Anhang I der Verordnung Nr. 359/2011 aufzunehmen, darin bestehe, den iranischen Staat zu treffen.

133 Der Rat habe die Klägerin folglich – anders als in der angefochtenen Verordnung angegeben – nicht aufgrund ihrer Handlungen sanktioniert, sondern ausschließlich aufgrund ihrer Eigenschaft als Regierungsinstitution, die aus ihrer Angliederung an das Ministerium für Kommunikationstechnologie resultiere, wie in jedem anderen Land. Indem der Rat die Klägerin restriktiven Maßnahmen nach der Verordnung Nr. 359/2011 unterworfen habe, habe der Rat sie wegen dieser Angliederung sanktionieren und auf diese Weise die iranische Staatsmacht lähmen wollen.

134 Der rechtliche Status einer von restriktiven Maßnahmen erfassten Person oder eine rechtliche oder wirtschaftliche Verbindung zwischen dieser Person und der Regierung eines Landes könne zwar nach der Rechtsprechung ein Indiz darstellen, das beim Rat einen Verdacht entstehen lassen könne, vermöge jedoch für sich genommen den Erlass solcher Maßnahmen nicht zu rechtfertigen.

135 Die Identität der übrigen in Anhang I der Verordnung Nr. 359/2011 aufgenommenen Personen zeige ebenfalls, dass die Aufnahme der Klägerin in diesen Anhang exzessiv sei.

136 Die Klägerin hebt ferner hervor, dass die vom Rat erlassenen restriktiven Maßnahmen dem Vorbild der Maßnahmen des Office of Foreign Assets Control gefolgt seien und dies von politischen Ressentiments gegen die Islamische Republik Iran zeuge.

137 Der Rat tritt dem Vorbringen der Klägerin entgegen.

138 In dieser Hinsicht gilt, dass eine Rechtshandlung nach der Rechtsprechung des Gerichtshofs nur dann einen Befugnismissbrauch aufweist, wenn aufgrund objektiver, schlüssiger und übereinstimmender Indizien anzunehmen ist, dass sie ausschließlich oder zumindest vorwiegend zu anderen als den angegebenen Zwecken oder mit dem Ziel erlassen worden ist, ein Verfahren zu umgehen, das der Vertrag speziell vorsieht, um die konkrete Sachlage zu bewältigen (vgl. Urteil vom 31. Januar 2019, Islamic Republic of Iran Shipping Lines u. a./Rat, C-225/17 P, EU:C:2019:82, Rn. 115 und die dort angeführte Rechtsprechung).

139 Im vorliegenden Fall macht die Klägerin geltend, der Rat habe ihren Namen ausschließlich aufgrund ihrer Eigenschaft als Regierungsinstitution, die aus ihrer Angliederung an das Ministerium für Kommunikationstechnologie resultiere, in Anhang I der Verordnung Nr. 359/2011 aufgenommen und nicht aufgrund ihrer eigenen Handlungen.

140 Allerdings ergibt sich aus der Prüfung des zweiten Klagegrundes (siehe oben, Rn. 25 bis 34), dass die Aufnahme ihres Namens in Anhang I der Verordnung Nr. 359/2011 durch die angefochtene Verordnung nicht lediglich mit ihrer Angliederung an das Ministerium für Kommunikationstechnologie begründet wurde, sondern hauptsächlich damit, dass sie die Anordnung der iranischen Regierung umsetzt, Internet-Inhalte durch die Spähsoftware SIAM zu filtern, und insbesondere dass sie ihre Kontrolle über den Zugang zum Internet und über Mobiltelefone dazu genutzt hat, Protestteilnehmer nachzuverfolgen und ein detailliertes Bild der Aktivitäten von Dissidenten und Protestteilnehmern zu erstellen, das die Behörden während der Proteste nach dem Tod von Frau Amini im Jahr 2022 nach Belieben verwendet haben.

141 Ferner ergibt sich aus der Prüfung des dritten Klagegrundes, dass die Gründe, die der Rat für die Aufnahme des Namens der Klägerin in Anhang I der Verordnung Nr. 359/2011 durch die angefochtene Verordnung angeführt hat, auf einer hinreichend gesicherten Tatsachengrundlage beruhten.

142 Überdies legt die Klägerin nicht dar, inwiefern der Umstand, dass die Namen anderer Personen in Anhang I der Verordnung Nr. 359/2011, zu denen sie, wie sie selbst mitgeteilt hat, nicht Stellung nehmen möchte, oder die Tatsache, dass die Behörden der Vereinigten Staaten von Amerika ebenfalls entschieden haben, restriktive Maßnahmen gegen sie zu erlassen, von Bedeutung sein könnten, um darzutun, dass der Rat vorliegend seine Befugnisse im Sinne der oben in Rn. 138 angeführten Rechtsprechung missbraucht hat.

143 Der erste Klagegrund ist daher als unbegründet zurückzuweisen und die Klage damit insgesamt abzuweisen.

Kosten

144 Nach Art. 134 Abs. 1 der Verfahrensordnung ist die unterliegende Partei auf Antrag zur Tragung der Kosten zu verurteilen. Da die Klägerin hier unterlegen ist, sind ihr gemäß dem Antrag des Rates ihre eigenen Kosten sowie die Kosten des Rates aufzuerlegen.

Aus diesen Gründen hat

DAS GERICHT (Sechste Kammer)

für Recht erkannt und entschieden:

1. Die Klage wird abgewiesen.

2. Die Communications Regulatory Authority (CRA) trägt die Kosten.

Costeira Kancheva Öberg

Verkündet in öffentlicher Sitzung in Luxemburg am 16. Oktober 2024.

Unterschriften