BDI
Bundesverband der
Deutschen Industrie e.V.

STELLUNGNAHME

Die EU-Dual-Use-Reform: Der Verordnungsvorschlag der EU-Kommission COM(2016)0616

März 2017

Die EU-Kommission hat am 28. September 2016 über einen Reformvorschlag, COM(2016)0616 final, entschieden, der umfangreiche Änderungen der EG-Dual-Use-Verordnung vorsieht. In einem nächsten Schritt werden das Europäische Parlament und der Rat über den Verordnungsvorschlag der EU-Kommission beraten. Die zentralen Regelungsbereiche des Verordnungsvorschlags der EU-Kommission schießen über das eigentliche Reformziel hinaus. Dies könnte sich negativ auf die Entwicklung des Technologiestandortes Europa und Deutschland auswirken. Europäisches Parlament und Rat sind nun aufgerufen, im Gesetzgebungsverfahren Augenmaß walten zu lassen und offene Fragen zu klären.

- **Eine Überarbeitung des Verordnungsvorschlags ist dringend notwendig**

  Der Verordnungsvorschlag schafft in zentralen Bereichen keine Balance zwischen Effektivität und Effizienz. Das *impact assessment* der EU-Kommission ist lückenhaft, neue Regeln werden nicht hinreichend begründet. Hiermit genügt das *impact assessment* auch nicht den wichtigen Bestrebungen nach Bürokratieabbau in der EU, den sogenannten REFIT-Vorgaben. Durch die angekündigten EU-Leitlinien allein wird keine Rechtssicherheit geschaffen, da diese rechtlich nicht bindend sind.

- **Güter- und Länderlisten statt Catch-All-Regeln**

  Der BDI unterstützt den stärkeren Schutz von Menschenrechten in der Exportkontrolle. Striktere Exportkontrollen für Technologien der digitalen Überwachung können diesen Schutz verbessern, wenn die Kontrollen effektiv und effizient sind. Anstatt auf allgemeine Auffangregeln, sogenannte Catch-All-Regeln, sollte der Gesetzgeber auf präzise Güter- und Länderlisten setzen.

- **Keine Kriminalisierung digitaler Technologien: Definitionen schärfen**

  Die neuen Definitionen des Verordnungsvorschlags für Technologien der digitalen Überwachung erfassen auch Komponenten für die wichtige digitale öffentliche Infrastruktur. Digitale Technologien zum Monitoring smarter und komplexer Infrastruktur (u. a. Energie- und Wasserversorgung) sind unabkömmlich. Nur so kann ihre Funktionsweise aber auch ihr Schutz garantiert werden. Der Verordnungsvorschlag trägt diesem wichtigen Aspekt nicht ausreichend Rechnung.

Verena Kantel | Abteilung für Außenwirtschaftspolitik | T: +49 30 2028-1518 | V.Kantel@bdi.eu

Inhaltsverzeichnis

Ziele und Treiber der Reform

Die EU-Kommission beabsichtigt mit der Reform, die Exportkontrollen an das veränderte technologische und sicherheitspolitische Umfeld anzupassen. Die Generaldirektion Handel betont, dass dies im Rahmen einer wertebasierten Handelspolitik geschehen solle. Dual-Use-Exportkontrollen gelten bislang für Güter, die sowohl zivil als auch militärisch verwendet werden können und hauptsächlich im Zusammenhang mit ABC-Waffen oder den sie tragenden Flugkörpern stehen. Aus Sicht der EU-Kommission schaffen Sicherheits- und Überwachungstechnologien aber neuartige Gefahren, die striktere Exportkontrollen auch für diese Güter erfordern. Auch Mitglieder des Europäischen Parlaments verlangen von EU-Staaten und Unternehmen mehr Verantwortung beim Export bestimmter Sicherheits- und Überwachungstechnologien, die von Staaten etwa zur Überwachung von Regimegegnern eingesetzt werden können. Dies ist eine Reaktion auf die Demokratisierungsbewegungen des Arabischen Frühlings, als Menschenrechtsaktivisten und Journalisten mittels Sicherheits- und Überwachungstechnologien geortet und ihre Kommunikation in sozialen Netzwerken ausgelesen wurden. Presseberichten zufolge stammten diese Technologien auch aus der EU.

Die wertebasierte Handelspolitik ist Element der EU-*Trade for All*-Strategie und soll hohe Nachhaltigkeits-, Menschenrechts- und Demokratiestandards sicherstellen. Die EU-Kommission betont aber auch: Die Exportkontrolle solle mit der Reform effektiver (im Schutz vor Gefahren) und effizienter (in den Kontrollvorgängen) werden. Um eine wertebasierte Handelspolitik zu stärken, verankert die EU-Kommission zusätzlich das Konzept der menschlichen Sicherheit (den sogenannten *„human security approach“*) in der Exportkontrolle. Der Export von Sicherheits- und Überwachungstechnologien wird dafür durch neue Definitionen des Dual-Use-Gutes, neue Genehmigungspflichten und EU-autonome Güterlistungen restriktiver gestaltet. Ein weiteres Anliegen der EU-Kommission ist es, die EU-Exportkontrolle stärker zu harmonisieren. Unter anderem soll die Genehmigungspraxis der EU-Mitgliedstaaten durch einen zusätzlichen Informationsaustausch stärker aufeinander abgestimmt werden.

Schafft die Reform den Balanceakt zwischen Effektivität und Effizienz?

Der am 28. September 2016 vorgelegte Verordnungsentwurf COM(2016)0616 beinhaltet einige positive Ansätze für effizientere Kontrollen durch eine breitere Verwendung von Verfahrenserleichterungen in Form von EU-Allgemeingenehmigungen und Sammelausfuhrgenehmigungen/Globalgenehmigungen. Anstatt für eine Vielzahl gleicher Güterausfuhren aufwendige Einzelausfuhrgenehmigungen beantragen zu müssen, stellen Allgemeingenehmigungen bestimmte Güterexporte in unkritische Zielländer von einer Genehmigungspflicht von Amts wegen frei. Besonders vertrauenswürdige Ausführer können darüber hinaus eine Vielzahl weiterer Güterexporte in einem Antragsverfahren vorab genehmigen lassen. Im Gegenzug müssen die Ausführer sogenannte Nebenbestimmungen beachten, wie etwa Registrierungs- und Meldepflichten bei den EU-Allgemeingenehmigungen. Positiv im Verordnungsvorschlag sind die neuen EU-Allgemeingenehmigungen für Verschlüsselungstechnologien (EU 009), für geringwertige Sendungen (EU 007) und für die unternehmensinterne Weitergabe von Software und Technologie (EU 008). Letzteres ist gerade für weltweite Entwicklungsteams wichtig, die immer häufiger zeitversetzt und über Grenzen hinweg an Projekten arbeiten.

Negativ ist allerdings die zeitliche Befristung von Einzelausfuhrgenehmigungen und Globalgenehmigungen auf ein Jahr (Artikel 10 Abs. 3). Für Globalausfuhrgenehmigungen muss zudem ein internes Compliance-Programm (ICP) vorliegen (Artikel 10 Abs. 4). Ob bei der Beurteilung des unternehmensspezifischen ICPs die unterschiedlichen Organisationsstrukturen kleiner und großer Unternehmen ausreichend berücksichtigt werden, ist noch unklar. Schwer wiegen aus Sicht der Industrie eine Reihe grundlegender Regelungen. Hierzu gehören die Genehmigungspflichten über neue Catch-All-Regeln (Artikel 4 Abs. 1d, 1e), ungenaue neue Definitionen des Dual-Use-Gutes (Artikel 2 Abs. 1b, 21), extraterritoriale Wirkungen neuer Definitionen des Brokers und des Erbringers von technischer Unterstützung in Artikel 2 Abs. 7 und Abs. 9 sowie neue EU-autonome Listen (Art. 16).

Den *human security approach* der EU-Kommission stellt die deutsche Industrie nicht in Frage. Sowohl die jüngsten Änderungen in der Antifolterverordnung als auch die Neulistungen in den internationalen Exportkontrollregimen und die EU-Embargos, in denen Güter zur internen Repression gelistet wurden, trug die verfasste Industrie mit. Der BDI unterstützt ausdrücklich den stärkeren Schutz von Menschenrechten. Dem Gesetzgeber ist es aber bislang noch nicht gelungen, die kritischen Fälle konkret zu benennen und die Kontrollen auf den Schutz vor interner Repression in Drittländern maßzuschneidern. Unspezifische Auffangregeln, sogenannte „Catch-All-Regeln" können dies nicht leisten. Sie sind weder effektiv noch effizient. Konkrete Definitionen, Länder- und Güterlisten sind besser geeignet, dieses Ziel zu erreichen. Die EU-Kommission versäumt es, die zwei wichtigen Kriterien, nämlich die Wahrung eines globalen *level playing fields* und die Sicherung eines EU-internen *level playing fields,* ausreichend zu beachten.

Die Folgen der Rechtsunsicherheit können gravierend sein: Unpräzise Definitionen und unspezifische Catch-All-Regeln gefährden die Export- und Wettbewerbsfähigkeit der deutschen und europäischen Industrie, weil sie zu Unsicherheiten im Ausfuhrverfahren führen, Mitarbeiter aus Sorge vor haftungsrechtlichen Konsequenzen sogenannte Absicherungsanträge bei den Genehmigungsbehörden stellen und sich hierdurch Lieferzeiten teilweise unnötig verlängern. Wenn eine unspezifische Menschenrechts-Catch-All-Regelung Technologien für digitale Überwachung unter einen Exportgenehmigungsvorbehalt stellt, beträfe dies auch den Kernbereich von Industrie 4.0 und damit den Bereich, der für die wirtschaftliche Entwicklung der EU wesentlich ist. Daher ist eine klare und besonders sorgfältig abgewogene Regelung durch den Gesetzgeber erforderlich. Soft- und Hardware zur Überwachung und Auswertung von Datenströmen oder Prozessen sind inzwischen in fast allen Industrieanwendungen enthalten und erfüllen wichtige Funktionen:

1. **Intelligente Energie-, Wasser- und Gasversorgung.** Sicherheits- und Überwachungstechnologien dienen hier dem Schutz vor Angreifern und helfen, Sicherheitslücken aufzudecken. Auch Netzauslastungen werden ausgewertet, um den gewünschten Energiemix zu steuern.

2. **Intelligente Verkehrskonzepte.** Sicherheits- und Überwachungstechnologien ermöglichen intelligente Verkehrslenkungssysteme und helfen bei stärkerer Digitalisierung von Schiene, Straße, Luft- und Wasserwegen. Sie liefern einen wichtigen Beitrag zum Schutz vor Personenschäden.

3. **Industrieller Anlagenbau und *e-health*** nutzen Sicherheits- und Überwachungstechnologien verstärkt zur Datenanalyse, fehlerminimierter Steuerung und Ferndiagnose.

Besorgniserregend ist auch die Ankündigung, dass unklare Regeln des Verordnungsvorschlags erst in EU-Leitlinien nachgebessert würden. Aus Sicht der Industrie ist dies nicht akzeptabel. Leitlinien sind nicht bindend und gewährleisten keine Rechtssicherheit. Im Zuge der Überarbeitung sollte sich der Gesetzgeber immer wieder die Frage stellen, ob und inwiefern die Ziele über eine Änderung der Dual-Use-Verordnung erreichbar sind oder ob sich hierfür andere Mechanismen besser eignen. Eine Überarbeitung des Verordnungsvorschlags ist daher unerlässlich.

Kritik am Folgenabschätzungsprozess

Der im Oktober 2016 vorgelegte Folgenabschätzungsbericht erfüllt nicht seine bedeutende Filter- und Begründungsfunktion. Mitglieder des Europäischen Parlaments und Vertreter im Rat sollten daher in den anstehenden Beratungen von ihren Fragerechten Gebrauch machen und Begründungen einfordern. Die EU-Kommission muss sich an den eigens festgelegten Regeln im Rahmen der „besseren Rechtssetzung" und des REFIT-Programms messen lassen. Das EU-Bürokratieabbauprogramm REFIT sieht bei Reformen vor, dem EU-Bürger einen umfassenden Folgenabschätzungsbericht vorzulegen, der Gründe wie auch Kosten- und Verwaltungsaufwand neuer Regeln beschreibt. Für den vorliegenden Reformvorschlag gelten die Ergebnisse der Folgenabschätzungsanalyse SWD(2016) 315 final als wichtige Grundlage. Anzuerkennen ist, dass Faktenwissen über Genehmigungszahlen in den EU 28-Staaten dokumentiert wurde. Flächendeckende Informationen über Stärken

und Schwächen nationaler Umsetzung fehlen jedoch. Lücken der EU-Gesetzgebung werden nicht konkret benannt: Der schnelle technologische Wandel und die veränderte Sicherheitslage[1] werden zwar als „noch nicht geregelte“ Herausforderung und Grund für die Reform benannt, aber nicht näher erläutert.

Folgende Kernfragen sind im Bericht nicht beantwortet:

1. Welche Gefahr wollen wir bannen? Laut EU-Kommission gaben zahlreiche Presseberichte Anlass für eine striktere Exportkontrolle. Konkret ging es um Vorfälle interner Repression im Arabischen Frühling.[2] Der Bericht der EU-Kommission versäumt es aber, diese Fälle aufzulisten und konkret zu beschreiben. Ein einziger Fall wird explizit referenziert.[3] Im Übrigen wird nur sehr allgemein auf Berichte und Fälle verwiesen.[4] Diese Verweise beantworten allerdings nicht folgende Fragen: Was genau ist passiert? Welche Rechte wurden verletzt? Und welche Gefahren hätte das Unternehmen vorhersehen können? Gänzlich fehlt eine genaue Darstellung der kritischen Gütergruppen. Dass Definitionen und Regeln wie Catch-All-Regeln dann im Verordnungsvorschlag unpräzise sind, ist wenig überraschend.

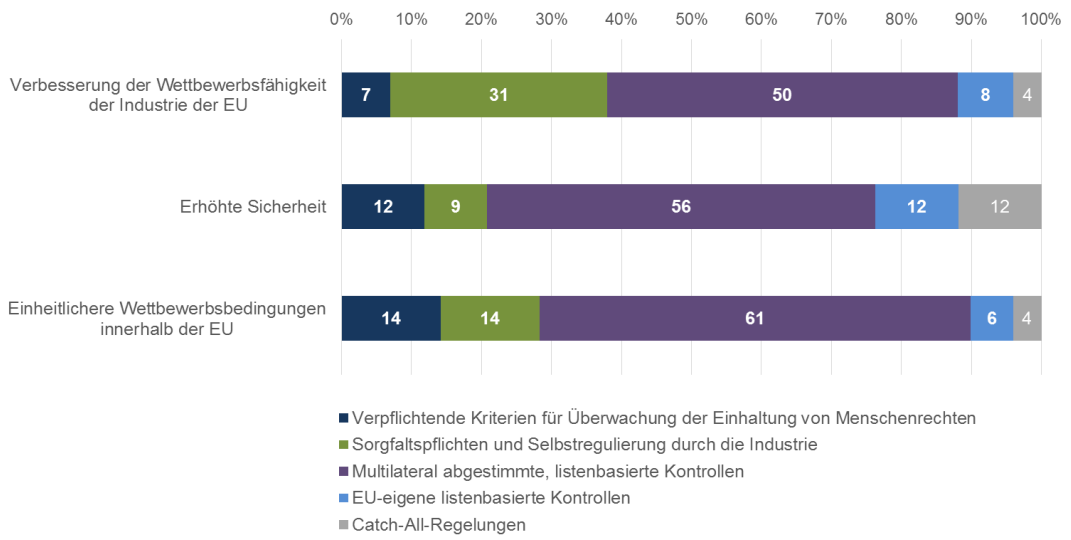
2. Welche kritischen Exportfälle sind nicht ausreichend geregelt? Die EU-Kommission bestätigt, dass die EU mit der aktuell gültigen EU-Dual-Use-Verordnung einen soliden Exportkontrollmechanismus bietet.[5] Gleichzeitig unterstreicht sie Regelungslücken für Cybertechnologien und betont, dass in vielen Fällen auch die Umsetzung der Exportkontrolle in den Mitgliedstaaten unzureichend sei. Beschrieben werden diese Umsetzungsversäumnisse allerdings nicht genau. Legislative Versäumnisse und Umsetzungsversäumnisse werden nicht unterschieden. Die Vorgaben des REFIT-Programms verlangen aber genau dies: Zunächst soll das Funktionieren der bisherigen Gesetzgebung überprüft werden, bevor neue Gesetze geschaffen werden. Vernachlässigt wird außerdem eine Analyse der jüngsten Gesetzesänderungen auf europäischer Ebene: Welchen kritischen Fällen haben die jüngsten Aktualisierungen der Güterlisten im Anhang I der Dual-Use-Verordnung bereits vorgebeugt? Welche weiteren Neulistungen werden aktuell schon in den internationalen Kontrollregimen diskutiert? Welche relevanten Fragen der Exportkontrolle werden nicht von den vier Regimen behandelt? Und: Welche Beispiele für gute nationale Exportkontrollregeln gibt es? Die Bestandsaufnahme bleibt unvollständig.

3. Warum weicht der Gesetzgeber vom gängigen Listenansatz ab? Die EU-Kommission empfiehlt Auffangregeln in Form von Catch-All-Regeln,[6] bricht hiermit jedoch mit dem bewährten Listenprinzip, das bislang eine solide Exportkontrolle ermöglichte. Begründet wird dies kaum. Unklar bleibt vor allem, warum Catch-All-Regeln effektiver sein sollen. Selbst die eigene Statistik der EU-Kommission zeigt: In der öffentlichen EU-Konsultation im Jahr 2015 bewerten die Befragten den Listenansatz als effektiveren Schutz der Sicherheit. Konkret fragte die EU-Kommission, wie wahrscheinlich es sei, dass der *human security approach* Auswirkungen auf eine erhöhte Sicherheit habe. Nur 12 Prozent der Befragten meinten, eine Catch-All-Regel entwickle überhaupt Effekte für eine erhöhte Sicherheit. Hingegen votierten 56 Prozent der Befragten, eine erhöhte Sicherheit sei über einen Listenansatz in internationalen Regimen zu erreichen. Die Handlungsalternativen werden so nicht vollständig abgewogen, obwohl es Sinn und Zweck des REFIT-Programms ist, unter Handlungsalternativen das effektivste und effizienteste Mittel aufzuzeigen. Zudem wurde keine Handlungsalternative aufgezeigt: Der gängige Güterlistenansatz kann mit einem Fast-Track-Verfahren kombiniert werden. Die Kontrolle wäre damit effektiver als eine Catch-All-Regel.

---

[1] EU-Kommission, *Impact Assessment, Report on the EU Export Control Policy Review*, SWD(2016)315 final, S. 5, 6.
[2] Ibid, S. 10.
[3] Ibid S. 11 („Hacking Team”).
[4] Ibid S. 10.
[5] Ibid S. 5.
[6] Ibid S. 37 ff.

Geringe Zustimmung für Catch-All-Regeln
„Würden Sie zustimmen, dass Maßnahmen, die den „*human security approach*" verfolgen, die folgenden Wirkungen haben?"



Quelle: EU-Kommission, *Impact Assessment, Report on the EU Export Control Policy Review*, SWD(2016)315 final, S. 35-38.

4. Warum hat es die EU bisher unterlassen, in den EU-Mitgliedstaaten für eine gleichmäßige und effektive Einhaltung des Exportkontrollrechts durch deren Unternehmen zu sorgen und diese Rechtseinhaltung zu kontrollieren, beziehungsweise Kontrollen zwingend vorzugeben? 20 von 28 Mitgliedstaaten sind einer Unternehmenserhebung nach nicht willens oder in der Lage, die Rechtseinhaltung ihrer Unternehmen zu kontrollieren. Eine vergleichbare Bestandsaufnahme hat das *impact assessment* versäumt. Es bleibt unklar, welche nationalen Kontrollen aktuell in Mitgliedstaaten durchgeführt werden. Eine Außenwirtschaftsprüfung gibt es beispielsweise in Deutschland und in Österreich. Wie aber ist die Lage in den anderen Ländern? Maßgabe muss auch in diesem Zusammenhang sein: Vor der Schaffung neuer Regelungen sollte dafür gesorgt werden, dass die bestehenden Regelungen einheitlich umgesetzt und eingehalten werden.

Klar ist: Der Gesetzgeber muss genau erläutern können, welchen Gefahren er vorbeugen will und warum kein anderes, weniger belastendes Mittel in Betracht kommt. Mitglieder des Europäischen Parlaments und die Vertreter im Rat sollten diese Fragen im Gesetzgebungsverfahren mit der EU-Kommission klären, da für die Reform alle drei EU-Institutionen die politische Verantwortung tragen.

Hohe Unsicherheiten für Unternehmen durch neue Catch-All-Regeln

Besorgniserregend sind die neuen Catch-All-Regeln; sie lassen große Effizienzverluste befürchten. Besondere Erwähnung verdienen die menschenrechtsbezogene Catch-All-Regel in Artikel 4 Abs. 1 d) und die Terrorismus-Catch-All-Regel in Artikel 4 Abs. 1 e). Da das bewährte Listenprinzip damit entwertet wird, muss die EU-Kommission ihre Maßnahmen besser begründen beziehungsweise Begründungen nachreichen. Unbestimmte Rechtsbegriffe sorgen für Rechtsunsicherheit. Aufgrund der Unsicherheit entsteht faktisch ein allgemeiner Genehmigungsvorbehalt, der nicht beabsichtigt war. Auch die Effektivität der Catch-All-Regelungen ist zweifelhaft. EU-Unternehmen können schließlich nur dann Einfluss auf verantwortungsvolle Lieferungen nehmen, wenn sie im Wettbewerb auf Auslandsmärkten gegenüber ihrer Konkurrenz bestehen.

In der aktuell gültigen Dual-Use-Verordnung (EG- VO Nr. 428/2009) werden Güter im Regelfall aufgrund ihrer technischen Parameter ausfuhrgenehmigungspflichtig. Sie sind dann im Anhang I der Dual-Use-Güter-Verordnung gelistet. Einen Auffangtatbestand in Form einer Catch-All-Lösung gibt es nur für mögliche Verwendungen im Bereich von ABC-Waffen und Trägertechnologien sowie im Fall einer einigermaßen konkret beschriebenen rüstungstechnischen Verwendung beschränkt auf Länder, gegen die ein Waffenembargo verhängt worden ist. Anstatt der technischen Parameter ist in diesen Catch-All-Regeln zwar ausnahmsweise der Verwendungsbezug entscheidend. Die kritische Verwendung ist den tatsächlichen Umständen nach aber beschrieben und erfordert keine rechtstechnische Einordnung. Aufgrund der faktenbasierten ausreichenden Konkretisierung kann die Wirtschaft mit dieser Regelung umgehen. Im Übrigen gilt der bewährte Listenansatz für Güter- und Länderlistungen.

Im Falle unspezifischer Catch-All-Regeln hingegen wäre die Unsicherheit in der Rechtsauslegung groß. Genau solche Unsicherheit entsteht aber in den vorgeschlagenen Catch-All-Regeln des Artikels 4 1d) und 1e).

Terrorismus-Catch-All-Regelung (Artikel 4 Absatz 1 e)

Der Kommissionsentwurf sieht vor, die sogenannte Catch-All-Kontrolle um das neue Kontrollziel „Terrorismus“ zu erweitern. Unternehmen müssten fortan verwendungskritische Fälle identifizieren, in denen die Gefahr besteht, dass Güter zu Zwecken terroristischer Handlungen missbräuchlich eingesetzt werden. Sie sollen damit teilweise Aufgaben und Risikoeinschätzungen wie Nachrichtendienste, Landes- oder Bundeskriminalämter vornehmen. Dies überfordert Unternehmen angesichts fehlender Beweislagen und nachrichtendienstlicher Erkenntnisse. Auch die rechtliche Bewertung ist alles andere als einfach. Die Definition der „terroristischen Handlungen“ ist äußerst komplex. Nicht umsonst verweist der Verordnungsvorschlag nur auf die Definition des Artikels 1 Abs. 3 des EU-Ratsbeschlusses 2001/931/GASP, die aus elf verschiedenen Handlungstypen besteht und Handlungsziele beschreibt.

Staatliche Organe dürfen ihre politische Verantwortung nicht auf die Unternehmen abwälzen. Bislang erstellt der Europäische Rat Sanktionslisten von natürlichen und juristischen Personen, wenn ausreichend Beweise den Schluss nahe legen, dass sie terroristische Organisationen unterstützen. Der Handel mit diesen Vertragspartnern ist verboten, das Bereitstellen finanzieller Mittel untersagt und unter Strafe gestellt (VO (EG) Nr.2580/2001 und Nr. 881/2002). In ihrer täglichen Exportkontroll-Compliance überprüfen Unternehmen ihre Vertragspartner effektiv anhand dieser Listen. Darüber hinaus verbieten Strafgesetze der Mitgliedstaaten strafbewehrt auch Beihilfe zu terroristischem Handeln und stellen Strafvereitelung unter Strafe. Auch andere Länder und überregionale Organisationen setzen im Zuge der Terror- und Gefahrenabwehr oder zur Durchsetzung von Sanktionen auf das bewährte Prinzip der Personenlistung: In den USA etwa gibt es die OFAC-SDN-List, die OFAC-FSE-List,[7] die BIS-Entity-List, die BIS-DPL-List und die BIS Unverified List.[8] Sowohl das Office of Foreign Asset Control (OFAC) als auch das Bureau of Industry and Security (BIS), welche die Listen erlassen, sind aber aus gutem Grund staatliche Einrichtungen, die ihre Listungen auf nachrichtendienstliche Erkenntnisse stützen. Die staatlichen Stellen nutzen Fachwissen, Fähigkeiten und Erkenntnisse der Ermittlungsbehörden und Geheimdienste. Die Listen schaffen auch Transparenz. Für Bürger und Unternehmen wird erkennbar, mit wem Geschäfte nicht durchgeführt werden dürfen. Die Vereinten Nationen listen im Zuge der Terrorsimusbekämpfung ebenfalls einzelne Personen in den einschlägigen Resolutionen des Sicherheitsrates.[9] Die Frage drängt sich auf: Warum soll eine unspezifische Catch-All-Regel effektiver als das Zusammenspiel von Terror-/Sanktionslisten und nationalem Strafrecht sein? Im *impact assessment* wurde diese Frage nicht thematisiert. Überhaupt finden sich im *impact assessment* keinerlei Begründungen und Abwägungen zu einer Terrorismus-Catch-All-Regelung. Dem

[7] U.S. Department of the Treasury, *Information on Financial Sanctions,* <https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/fse_list.aspx > (eingesehen am 18. Januar 2017).
[8] Bureau of Industry and Security (BIS), *Lists of Parties of Concern*, <https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list> (eingesehen am 18. Januar 2017).
[9] United Nations Security Council, *Sanctions*, <https://www.un.org/sc/suborg/en/sanctions/1267> (eingesehen am 18. Januar 2017).

REFIT- Ziel, Verordnungsvorschläge zu begründen, größere Transparenz und bessere Rechtssetzung zu gewährleisten, widerspricht dies.

Menschenrechts-Catch-All-Regelung (Artikel 4 Absatz 1 d)

Der Kommissionsentwurf sieht auch vor, die sogenannte Catch-All-Kontrolle um das Kontrollziel „Menschenrechte“ zu erweitern. Die Frage, wann eine Lieferung die Gefahr von Menschenrechtsverletzungen erhöht, ist für Unternehmen im konkreten Fall allerdings schwer zu beantworten, wenn es von einer eindeutigen staatlichen Stelle keine verbindlichen Hinweise auf sensible Zielländer und kritische Praktiken gibt. Zwar beabsichtigt die EU-Kommission in der neuen Catch-All-Regelung, dass es künftig (auch) auf den Hinweis von (über)-staatlichen Organisationen ankommen soll. Jedoch sind diese dem Namen nach nicht benannt. Auch ist unklar, ob diese Hinweise verbindlich sind und wo sie für jedermann zugänglich veröffentlicht würden. Die mögliche Filterfunktion entfällt zudem spätestens in der Tatbestandsvariante des Artikels 4 Abs. 2, in der es ausschließlich auf den subjektiven Kenntnismaßstab des Ausführers ankommt. Unternehmen ist deshalb unklar, auf der Grundlage welcher Informationsquellen sie beurteilen sollen, welche Überwachungstätigkeiten in Drittstaaten kritisch sind. Überwachungs- und Ermittlungstätigkeiten durch EU-Drittstaaten können schließlich nicht nur zur Überwachung unliebsamer Regimegegner, sondern auch zur notwendigen Gefahren- oder Terrorabwehr erfolgen. An einer funktionierenden Gefahren- und Terrorabwehr besteht ein weltweites sicherheitspolitisches Interesse. Unternehmen ist auch nicht klar, wessen Demokratiemaßstab bei dieser Bewertung gilt. Selbst innereuropäisch werden Maßnahmen der Gefahren- und Terrorabwehr unterschiedlich bewertet. Die Dauer der Einzelfallprüfungen in Unternehmen wäre nicht absehbar. Die übliche und effektive IT- und listenbasierte Risikokontrolle würde unmöglich. Unternehmen würden Einzelprüfungen durch Behörden nicht nur im Zweifelsfall beziehungsweise in eindeutigen Genehmigungsfällen, sondern zur Absicherung regelmäßig anstrengen. Staatliche Organe können besser beurteilen, welche Länder aufgrund von Menschrechtsverletzungen als sensibles Endbestimmungsland einzustufen sind. Sie verfügen über nachrichtendienstliche Erkenntnisse und können diese in politischen Prozessen im Rat bewerten, überprüfen und einem Konsens unterziehen. Sie sollten die Verantwortung politisch-rechtlicher Einschätzung nicht auf Unternehmen abwälzen.

Auch das Kriterium „Endbestimmungsland, benannt durch relevante öffentliche internationale Stellen oder zuständige europäische oder nationale Behörden“ ist nicht hinreichend bestimmt. Unklar ist, wer diese abstrakt beschriebenen Institutionen sind. Wo findet man ihre „Benennungen“ von menschenrechtskritischen Ländern? Werden sie im Europäischen Gesetzblatt wie Gesetze und formelle Mitteilungen der EU veröffentlicht?

Kritisch ist überdies, dass der güterbezogene Anwendungsbereich der Menschenrechts-Catch-All-Regelung anders als angekündigt, ausgeweitet wurde. Selbst im *impact assessment* wurden nur die Konsequenzen einer Catch-All untersucht, die sich auf den Güterkreis „Technologie für digitale Überwachung“ bezog.[10] Im Verordnungsvorschlag sind nun allerdings sämtliche Dual-Use-Güter oder nach anderer Lesart weitestgehend alle Güter von der Menschenrechts-Catch-All erfasst. Keineswegs beschränkt die EU-Kommission ihre Catch-All-Regelung auf den von ihr untersuchten Anwendungsbereich „Technologie für digitale Überwachung“. Gemessen an Maßstäben des REFIT-Prozesses ist dies nicht tragbar.

Effekte neuer Catch-All-Regelungen: Lange Lieferzeiten lähmen das Projekt- und Produktgeschäft

Wenn durch langwierige Einzelausfuhrgenehmigungsverfahren gerade das Ersatzteil- und Servicegeschäft erschwert würde, drohen europäische Unternehmen im gesamten Projekt- und Produktgeschäft weniger wettbewerbsfähig zu werden. Schon bei der Auftragsvergabe sind für den Kunden die Zusage für zügige Ferndiagnose, Reparatur oder auch Lieferung von Ersatzteilen mitentscheidend. Der Kunde will das Ausfallrisiko minimieren. Anlagen dürfen nicht stillstehen. Eine mehrmonatige Genehmigungsdauer bis zum Erhalt des Services

[10] Ibid, S.37.

wäre für ihn nicht zumutbar – und nicht effizient. Insgesamt würden deutsche und europäische Unternehmen an Wettbewerbsfähigkeit gegenüber ausländischen Herstellern einbüßen und an Marktmacht verlieren.

Die Empfehlung der Industrie:

- **Zum Schutz der Menschenrechte:** Die neue Catch-All-Regel des Artikels 4 Abs. 1 d) sollte gestrichen werden. Stattdessen sollten Unternehmen den Güterexport anhand von eindeutigen Güter- und Länderlisten überprüfen. Diese Listungen sollten in Anhang 1 der Verordnung per delegiertem Rechtsakt erfolgen. Falls eine Neulistung in den internationalen Regimen und damit in Anhang 1 A der Verordnung nicht gelingt, eine Kontrolle aber besonders dringlich ist, ist eine Neulistung im Anhang 1 B der Verordnung per Fast-Track-Verfahren effektiver und effizienter als eine Catch-All-Regelung. Das Fast-Track-Verfahren kann analog dem Verfahren in der jüngst beschlossenen Anti-Folterverordnung ausgestaltet werden. Eine autonome Listung sollte aber *ultima ratio* sein.

- **Zum Schutz vor terroristischen Gefahren:** Die neue Catch-All-Regel des Artikels 4 Abs. 1 e) sollte gestrichen werden. Stattdessen sollten Unternehmen ihre Vertragspartner auf Grundlage eindeutiger Personenlistungen des Europäischen Rates überprüfen müssen. Um zuverlässigere Personenlisten erstellen zu können, sollten europäische Nachrichtendienste ihre Erkenntnisse noch zielgerichteter zusammenführen.

- **Zu Organisationspflichten im Unternehmen:** Der Artikel 4 Abs. 2 sollte umformuliert werden. Organisations- und Sorgfaltspflichten müssen in der Catch-All-Regelung eindeutig auf die positive Kenntnis eines kritischen Exportes bezogen sein. Der Begriff der *„due diligence“* ist verwirrend und sollte gestrichen werden. Ziel muss es sein, dass das Unternehmen gewährleisten kann, den Export notfalls zu stoppen.

- **Zur Konsultation bei Einzeleingriffen:** Wenn Mitgliedstaaten eilige Einzeleingriffe vornehmen müssen, darf eine zwingende Konsultation aller Mitgliedstaaten nach Artikel 4 Abs. 4 die Reaktionsfähigkeit der nationalen Behörde nicht konterkarieren und Unternehmen nicht zu lange im Ungewissen über die Genehmigungsfähigkeit des Exports lassen. Auch muss den Wirtschaftsbeteiligten im Gegenzug ein Rechtsschutzmechanismus ermöglicht werden.

Definitionen schärfen: Das neue Dual-Use-Gut

In der Verordnung müssen Artikel 2 Abs. 1 a) und b) sowie Abs. 21 präzise definiert werden, was unter einem Dual-Use-Gut zu verstehen ist. Nur eine saubere und sinnvolle Definition kann effektive Exportkontrollen sichern. Die Definition legt den güterbezogenen Anwendungsbereich dieser Verordnung fest.

Die Definition erfüllt zwei zentrale Funktionen:

- **Rechts- und Planungssicherheit für Unternehmen im internationalen Wettbewerb:** Unternehmen und nationale Genehmigungsbehörden müssen anhand der Definition des Dual-Use-Gutes zuverlässig bestimmen können, für welche Güter sie beim Export eine Genehmigung beantragen müssen. Sofern sich die Genehmigungspflicht nicht aus der Güterlistung ergibt (Artikel 3 in Verbindung mit der Güterlistung in Anhang I, Sektion B), sind Unternehmen und Verwaltungen auf die allgemeine Definition des Artikels 2 angewiesen (Artikel 4 in Verbindung mit Artikel 2 Abs. 1 und 21). Über diese Verweisungskette wären auch nicht gelistete Güter ausnahmsweise genehmigungspflichtig. Die Definition darf aber nicht uferlos und ungenau sein. Sonst verlängert sich auch die Exportzeit von Gütern, die für zivile Verwendungszwecke wie *e-mobility* oder dem Schutz von Versorgungsanlagen eingesetzt werden.

Kontrolle durch das Europäische Parlament und den Rat: Die Definition des Dual-Use-Gutes nach Artikel 2 Abs. 1, 21 bestimmt, welche Güter die EU-Kommission künftig im Anhang I, Sektion B der Verordnung aufnehmen darf. Artikel 16 gibt ihr ein autonomes Listungsrecht. Da Parlament und Rat bei diesen neuen autonomen Güterlistungen per delegiertem Rechtsakt keine umfassende Kontrolle ausüben können, sollten sie Listungsmöglichkeiten vorab über die Definition eingrenzen.

Die neue Definition schärfen

Die Definition des Dual-Use-Gutes in Artikel 2 wurde um den Begriff der *„Technologie für digitale Überwachung“* in Artikel 2 Abs. 1b und 21 erweitert. Sie erstreckt Exportkontrollen und Güterlistungen damit künftig auf Güter der Sicherheits- und Überwachungstechnologie. Die Erweiterung entspricht jedoch nur in Teilen dem politischen Willen und den Zielen der Reform und schädigt für Unternehmen das globale *level playing field*. Die Definitionen schaffen Hürden nicht nur für kritische Exporte, welche die Gefahr interner Repression erhöhen, sondern auch für Technologien in umweltfreundlichen und für die Kommunikation wesentlichen Infrastrukturen. Die EU und ihre Bevölkerung haben ein strategisches Interesse daran, bei den für Industrie 4.0 und Massenkonsumgütermarkt wesentlichen Technologien wettbewerbsfähig zu sein und diese Güter von vertrauenswürdigen Unternehmen beziehen zu können. Güterkreis wie Verwendungszweck müssen deshalb konkretisiert werden. Auch aus Gründen des Versorgungsschutzes und des Verbraucherschutzes ist dies wichtig. Um etwa für den Kunden eine hohe Produktsicherheit auf dem Konsumgütermarkt zu gewährleisten, müssen Hersteller diejenigen IT-Verbindungen von Produkten in das Unternehmen sichern, über welche Kunden IT-Services abrufen. Ein Automobilhersteller muss so beispielsweise Clouddienste vor unbefugtem Zugriff Dritter schützen. Auch die Fahrassistenzsysteme und das autonome Fahren müssen vor Hackerangriffen sicher sein. Gleiches gilt für kritische Infrastrukturen. Dort gewährleisten sichere IT-Verbindungen die Versorgungssicherheit der Bevölkerung. Überwachungssysteme verringern hier die Wahrscheinlichkeit, dass Sicherheitslücken unentdeckt bleiben und Hackerangriffe großen Schaden anrichten.

- **Die Definition des Artikels 2 Abs. 1 b)** legt fest, dass „Technologie für digitale Überwachung“ exportkontrollrelevant ist, wenn sie „für die Begehung schwerwiegender Verletzungen der Menschenrechte oder des humanitären Völkerrechts verwendet werden oder eine Bedrohung für die internationale Sicherheit oder die wesentlichen Sicherheitsinteressen der Union und ihrer Mitgliedstaaten darstellen kann.“

  Da Abgeordnete des Europäischen Parlamentes ursprünglich bestimmten Fälle interner Repression in Drittstaaten vorbeugen wollten, sollten die Charakteristika der Fälle nun in den Tatbestandsmerkmalen der Definition genannt werden: Hierzu zählt der Schutz der Privatsphäre sowie der Schutz vor Meinungs- und Versammlungsfreiheit vor dem/beim Einsatz von Überwachungstechnologie. Der Anwendungsbereich sollte zudem auf „systematische und schwere“ Menschenrechtsverletzungen eingegrenzt werden. Unternehmen können unmöglich selbst gravierende Einzelfälle voraussehen. Wichtig sind daher Tatbestandsmerkmale, die Unterscheidungskriterien bieten, wann ein Drittstaat seiner Schutzpflicht gegenüber seinen Bürgern nicht mehr nachkommt und Rechtsstaatlichkeit nicht mehr gewährleistet ist. Mögliche Tatbestandsmerkmale sind hierfür etwa fehlende Richtervorbehalte in Ermittlungsverfahren, fehlende Klage- und Revisionsrechte sowie fehlende faire Verfahren. Falls besonders gravierende Einzelfälle dennoch ein Handeln notwendig erscheinen lassen, muss dies politisch bewertet und signalisiert werden.

- **Die Definition des Artikels 2 Abs. 21** versucht den Güterkreis der „Technologie für digitale Überwachung“ zu konkretisieren. Gelungen ist dies noch nicht. Die exemplarische Auflistung der allgemeinen Güter wie „Ausrüstung zum Abhören von mobiler Telekommunikation“, „Intrusion-Software“, „Überwachungszentren“, „digitale Forensik“ ist generisch, missverständlich und offen für Interpretation. Die Auflistung erfasst zudem Technologien, die für den Aufbau, die Sicherung und den Schutz von IT- und Kommunikationssystemen notwendig sind. Auch unkritische Verwendungszwecke sind erfasst. Die Technologien dienen auch zum Aufbau notwendiger Kommunikationsanlagen, öffentlicher Infrastruktur, Technologie zum Schutz des Unternehmens oder auch zum Schutz öffentlicher (Energie- und Wasser-) Versorgungsanlagen oder künftiger Verkehrslenkungssysteme vor Angriffen von außen.

Eine Eingrenzung des Verwendungszwecks gelingt über eine Negativabgrenzung und tatbestandliche Ausnahmen in Artikel 2 Abs. 21. In einem ersten Schritt müssen dafür die Tatbestandsausnahmen des Anhangs I, Sektion B in die Definition des Artikels 2 Abs. 21 übertragen werden. Sicherheits- und Überwachungstechnologien sind danach nicht tatbestandlich, wenn sie speziell konstruiert sind für folgende Zwecke*:* Abrechnung, Funktionen zur Datenerfassung innerhalb von Netzelementen (z. B. *Exchange* oder HLR), Dienstgüte des Netzwerks (*Quality of Service,* QoS) oder Nutzerzufriedenheit (*Quality of Experience,* QoE), Betrieb in Telekommunikationsunternehmen (Diensterbringern). Diese Formulierung sollte bereits Teil der Definition in der Verordnung und nicht nur des Anhangs sein. In einem zweiten Schritt sollten weitere unkritische und erstrebenswerte Verwendungszwecke als Tatbestandsausnahme formuliert werden, wie etwa, wenn die Technologie besonders konstruiert ist für: den Schutz öffentlicher digitaler Infrastruktur, den Schutz von Unternehmen vor Wirtschaftsspionage, den Schutz von Unternehmen und ihren Produkten vor Hackerangriffen, den Einsatz in unternehmenseigenen Compliance-Systemen zur Betrugs- und Bestechungsbekämpfung.

Im Übrigen muss auch eine ehrliche Debatte darüber geführt werden, dass nicht jede Datensammlung in Drittländern durch die EU-Dual-Use-Verordnung unterbunden werden kann. Datensammlungen und das Recht auf informationelle Selbstbestimmung, Schutz der Privatsphäre und der Meinungsfreiheit muss – genauso wie in der Europäischen Union – durch Datenschutzgesetze sowie ein entsprechendes materielles und prozessuales Strafrecht in den Drittländern geregelt werden. Hierzu können EU-Partnerprojekte beitragen, die Rechts- und Justizaufbau in Drittländern fördern. Die EU-Dual-Use-Verordnung darf nicht überfrachtet werden.

Die Empfehlung der Industrie:

Zur besseren Definition der Sicherheits- und Überwachungstechnologien:

- **Unkritische Verwendungszwecke anerkennen:** Unkritische Verwendungszwecke müssen von der Genehmigungspflicht ausgenommen werden. Die Ausnahmen des Anhangs I B der Verordnung sollten schon als tatbestandliche Ausnahme in die Definition des relevanten Cyber-Surveillance-Gutes in Artikel 2 Abs. 21 einfließen. Darüber hinaus muss Technologie freigestellt sein, die zum Schutz öffentlicher Infrastruktur, zum Schutz vor Wirtschaftsspionage in Unternehmen und zum Schutz der Verbraucher / Kunden eingesetzt wird.

- **Systematische Verletzungen von Schutzgütern berücksichtigen:** Der Gesetzgeber muss die Definition des Artikels 2 Abs. 1b) konkretisieren: Exportkontrollrelevant sollten Exporte sein, welche die Gefahr vor interner Repression erhöhen und eine Gefahr für die Meinungs- und Versammlungsfreiheit und den Schutz der Privatsphäre darstellen, wobei es dafür wesentlich darauf ankommt, ob funktionierende Rechtsschutzmechanismen grundsätzlich vorhanden sind oder fehlen (Richtervorbehalte in Ermittlungsverfahren, fehlende Klage- und Revisionsrechte sowie fehlende faire Verfahren**).**

Länderlisten schaffen Transparenz und eine effektive Kontrolle

Embargomaßnahmen und Länderlisten schaffen Klarheit und Transparenz, wenn Ausfuhrgeschäfte in sensible Länder verhindert werden sollen. Im Zuge der Exportkontrollreform sollten deshalb die unterschiedlichen Instrumente der Embargomaßnahmen und die Länderlisten in allgemeinen Exportkontrollregeln genauer betrachtet und stärker berücksichtigt werden. Für die allgemeine Dual-Use-Kontrolle sollten Länderlisten geschaffen werden, welche die drei Kontrollkriterien Exportgut, Endverwender und Endverwendung als Kontrollmittel ergänzen.

Gerade weil mit der Reform der Schutz vor Überwachungstechnologie in Ländern sichergestellt werden soll, in denen interne Repressionen von staatlichen Akteuren zu befürchten sind, wären strikte Positiv- oder Negativlisten oder aber auch graue Länderlisten („unverified lists“) das geeignete Mittel, um eine effektive Kontrolle durch Unternehmen und Behörden zu erreichen. Doch sowohl zum Mittel der Embargomaßnahmen als auch zu Beschränkungen durch Länderlisten trifft das *impact assessment* der EU-Kommission noch keine Aussage.

Embargopolitik

Sofern der Außenwirtschaftsverkehr mit einem Staat verboten oder beschränkt werden soll, weil der Zielstaat Völkerrecht verletzt hat, sind UN- und EU-Embargos das richtige Kontrollmittel. Die gewünschten Beschränkungen werden auf EU-Ebene im Rahmen der Gemeinsamen Außen- und Sicherheitspolitik (GASP) vom Europäischen Rat in einem Gemeinsamen Standpunkt und anschließend (meist) in einer EU-Verordnung erlassen. Der Beschluss des Rates bindet rechtlich die Mitgliedstaaten, die EU-Verordnung bindet auch die Unternehmen direkt und unmittelbar.

Durch Embargoverordnungen kann auch der Export von Gütern zur internen Repression sehr gezielt beschränkt werden, wie die EU-Verordnungen zu Iran, Lybien, Belarus oder Myanmar zeigen[11]. Die sogenannte Iran-Menschenrechtsverordnung (Verordnung (EG) Nr. 359/2011)[12] ist ein gutes Beispiel dafür, dass die Ausfuhr von diversen Gütern der Überwachungstechnologie effektiv verboten werden kann. Auch besonders kritische Endabnehmer wurden in der Verordnung explizit gelistet. Dies ist etwa der Fall bei dem sogenannten Informationsminister, der zum Zeitpunkt der Listung für Zensur und Kontrolle des Internets zuständig war. Eine solche Verordnung kann je nach landesinternen Umständen auch befristet oder aufgehoben werden. Mit dieser Verordnung kann also auch die EU-Kommission flexibel auf sich ändernde politische Umstände reagieren. Angesichts dieser Beispiele ist nicht nachvollziehbar, warum die Vorteile und Wirksamkeit dieser Maßnahmen nicht auch im *impact assessment* näher untersucht wurden.

Länderlisten

Auch Länderlisten im Anhang der Dual-Use-Verordnung könnten bestimmte Ausfuhrgeschäfte effektiv kontrollieren. Sie könnten von den EU-Institutionen per delegiertem Rechtsakt beschlossen werden. Dabei könnten drei verschiedene Arten von Länderlisten eine Abstufung der Verdachtsmomente erlauben. Je nach Beweislage über die jeweils vermeintlich kritischen Umstände in Drittstaaten, könnte die EU-Kommission positive, negative oder auch graue Listen vorschlagen. In Anlehnung an die US-amerikanischen *unverified lists* hätten gerade die grauen Listen den Vorteil, signalisieren zu können, dass im Drittstaat kritische Überwachungspraktiken nur vermutet werden, aber noch keineswegs feststehen. Welches listungswürdige, rechtsverletzende Überwachungspraktiken sind, könnten Parlament und Rat bereits im Verordnungsvorschlag festlegen. Der Vorteil ist klar: Länderlisten ermöglichen Unternehmen und Behörden einen Hinweis auf sensible Länder. Unnötig große Absicherungsanträge würden vermieden. Gelistete Staaten könnten auf Verdachtsmomente reagieren.

Verständlicherweise fällt es den politischen Institutionen schwer, das Verhalten von Drittstaaten öffentlich zu bewerten. So sind immer auch diplomatische Beziehungen zu beachten. Streng genommen beabsichtigt der Reformvorschlag aber genau diese politisch-rechtliche Bewertung drittstaatlichen Handels – nur eben hinter verschlossenen Türen. Eine wertebasierte Handelspolitik sollte der EU ermöglichen, über ihre Werte auch offen zu sprechen. Der Listenansatz bietet auch mehr Transparenz im Entscheidungsprozess.

---

[11] Bundesamt für Wirtschaft und Ausfuhrkontrolle, *Embargos*, <http://www.bafa.de/DE/Aussenwirtschaft/Ausfuhrkontrolle/Embargos/embargos_node.html> (eingesehen am 18. Januar 2017).
[12] Verordnung (EU) Nr. 264/2012 des Rates vom 23. März 2012 zur Änderung der Verordnung (EU) Nr. 359/2011 über restriktive Maßnahmen gegen bestimmte Personen, Organisationen und Einrichtungen angesichts der Lage in Iran, <http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32012R0264>.

Die Empfehlung der Industrie:

- **Negative Länderlisten** könnten in Anlehnung an die Embargopolitik den Export in bestimmte Länder beschränken, wenn Erkenntnisse und Beweise der 28 Nachrichtendienste auf eine hohe Wahrscheinlichkeit von bestimmten kritischen staatlichen Überwachungsmaßnahmen und daraus resultierenden Verletzungshandlungen schließen lassen.

- **Graue Länderlisten** könnten in Anlehnung an die *US-unverified lists/ entity lists* signalisieren, dass sich bestimmte Verdachtsmomente auf kritische Überwachungstechniken und Verletzungshandlungen von einer Mehrheit der 28 Nachrichtendienste erhärtet haben.

- **Positive Länderlisten** könnten in den Güterlistungen des Anhang I B als tatbestandliche Ausnahme formuliert werden. Die gelisteten Länder sind dann bei einem Exportvorbehalt aus Güterlistung als grundsätzlich unbedenklich eingestuft. Dieses auch national bewährte Mittel wird im Annex des Reformvorschlags bereits angedeutet und müsste konsequent fortgesetzt werden.

Die Kriterien für die Länderlistung müssten im Verordnungsvorschlag verankert werden. So können Europäisches Parlament und Rat die Entscheidungsbasis für kritische Fallgruppen definieren. Analog der Endverwendungskriterien in der Güterdefinition braucht es Tatbestandmerkmale für die kritische Überwachungspraxis.

Die Empfehlung der Industrie:

Eine kritische - rechtsverletzende - Überwachungspraxis im Sinne der Verordnung **liegt vor, wenn**

1. **in der Verfassung des Drittstaates, seinen Gesetzen, seiner höchstrichterlichen Rechtsprechung oder seinem Gewohnheitsrecht folgende Bürgerrechte nicht verankert oder als Bürgerrecht anerkannt sind:**

   - Schutz der Privatsphäre / Unverletzlichkeit der Wohnung (Schutz vor Abhörmaßnahmen)
   - Computer-Grundrecht
   - Meinungsfreiheit
   - Versammlungsfreiheit;

2. **bei typischerweise verdeckt erfolgenden Überwachungsmaßnahmen eine behördliche Überwachung zur Gefahrenabwehr oder Strafverfolgung auch ohne richterliche Anordnung möglich** ist, obwohl sie in die unter 1.) genannten Grundrechte eingreift;

3. **der Bürger gegen die ihn belastenden Maßnahmen keine ausreichenden Rechtsschutzmöglichkeiten hat,** mithilfe derer er die behördlichen Maßnahmen im Verwaltungswege oder vor (Verwaltungs-) Gerichten überprüfen und (auch im Nachhinhein) gegebenenfalls für unwirksam erklären lassen kann.

Schneller Ausfuhrstopp auch ohne neue Catch-All-Regeln möglich

Die Schlussfolgerungen des *impact assessments* der EU-Kommission suggerieren, EU-Staaten seien ohne neue Catch-All-Regeln nicht reaktionsfähig genug, um kurzfristig Güterlieferungen an sensible Endverwender zu stoppen. Dahinter steht die Annahme, dass rasante Änderungen des technologischen und politischen Umfelds, schnelle Reaktionen notwendig machen. Diese Sorge ist nachvollziehbar. Dabei wird jedoch die Fülle bewährter Kontrollmechanismen nicht ausreichend gewürdigt: Das gelungene Zusammenspiel von EU-Gesetzen und nationalem Verwaltungshandeln sichert schon heute die Reaktionsfähigkeit der Verwaltung auch in Zeiten des schnellen politischen und technologischen Wandels.

- **Exportkontrollregeln:** Auf Gesetzesebene sind die Embargovorschriften und zuvor beschriebenen Länder- und Güterlisten der allgemeinen EG-Dual-Use-Exportkontrolle das effektivste Mittel, um Warenlieferungen systematisch zu kontrollieren. Diese Listen sind Maßstab für die Kontrolle im Unternehmen sowie durch die nationalen Genehmigungs- und Zollbehörden.

- **Verwaltungshandeln:** Eine effektive Exportkontrolle wird außerdem durch das Verwaltungshandeln der nationalen Genehmigungsbehörden gesichert. Sie sind für die Durchsetzung der Exportkontrollregeln zuständig. Neben Bescheidungsbefugnissen im Antragsverfahren verfügen EU-Mitgliedstaaten auch über Eingriffskompetenzen außerhalb des Antragsverfahrens. Sie können die Warenausfuhr außerhalb eines Antragsverfahrens stoppen. Steht die Ware bereits an der Grenze, erfolgt dies mithilfe der Zollbehörde. Voraussetzung für den Stopp der Ausfuhr ist, dass für eine genehmigungspflichtige Ware keine Genehmigung erteilt wurde. Aber auch eine nicht genehmigungspflichtige Ware kann gestoppt werden. In diesem Fall muss die Genehmigungsbörde Anhaltspunkte dafür haben, dass durch die Ausfuhr und Lieferung an den Endverwender eine Gefahr für die öffentliche Sicherheit oder auch die Gefahr der Verletzung von Menschenrechten besteht. Rechtsgrundlage hierfür sind nationale Gesetze wie in Deutschland § 6 Außenwirtschaftsgesetz (AWG). Aber auch die Verordnung EG 428/2009 bietet den Genehmigungsbehörden mit Artikel 8 EG-Dual-Use Verordnung die Möglichkeit, die Ausfuhr zu verhindern.

  Insgesamt sind Einzeleingriffe sehr effektiv: staatliche (Genehmigungs-) Behörden können Hinweisen auf Menschenrechtsverletzungen nachgehen, diese mit den Erkenntnissen von Nachrichtendiensten abgleichen und schließlich in der Entscheidung über den Stopp der Warenausfuhr berücksichtigen. Unternehmen stehen die Erkenntnisse von Nachrichtendiensten hingegen nicht zur Verfügung.

Zu bemängeln ist, dass die EU-Kommission im *impact assessment* nicht untersucht hat, ob die Mitgliedstaaten von der Eingriffskompetenz tatsächlich Gebrauch machen. Möglicherweise fehlt es nur an einer effektiven EU-weiten Umsetzung bestehender Regeln. Der Außenwirtschaftsverkehr ist grundsätzlich frei und darf nicht ohne triftigen Grund durch Catch-All-Regeln eingeschränkt werden. Dies unterstrich Handelskommissarin Cecilia Malmström bereits in dem Reformvorhaben zur EU-Anti-Folterverordnung. Auch dort musste zwischen den Instrumenten Catch-All und Listenansatz abgewogen werden. Die Handelskommissarin sprach sich damals explizit gegen neue Catch-All Regeln aus.[13]

Die Empfehlung der Industrie:

- **Umsetzung und Durchsetzung der Regeln sichern:** Bevor der Gesetzgeber neue Regeln schafft, muss er untersuchen, ob Mitgliedstaaten von ihren Eingriffskompetenzen Gebrauch machen und inwiefern eine EU-weite Umsetzung und Durchsetzung bestehender Exportkontrollregeln gelingt.

[13] Europäisches Parlament, *Plenardebatten,* <http://www.europarl.europa.eu/sides/getDoc.do?type=CRE&reference=20151026&secondRef=ITEM-014&language=EN&ring=A8-2015-0267> (eingesehen am 14. März 2017).

Weitere kritische Elemente

Definitionen vereinheitlichen: Der Ausführer

Bei der Definition des Ausführers ist darauf zu achten, dass dieselbe Definition für Ausführer von exportgenehmigungspflichtigen Gütern auch in der europäischen Zollgesetzgebung gilt. Dies ist wichtig, da die Zollbehörden diejenigen Kontrollbehörden sind, die Gütersendungen an den Außengrenzen der Europäischen Union auch auf die Vollständigkeit ihrer Begleitpapiere und exportkontrollrechtlichen Genehmigungen überprüfen. Der Begriff des Ausführers in Artikel 2 Abs. 3 der künftigen Dual-Use-Verordnung muss daher mit der Definition des Ausführers im Unionszollkodex und seinen delegierten Rechtsakten harmonisiert werden.

Die Empfehlung der Industrie:

- **Die Definition des Ausführers vereinheitlichen:** Die Definition des Exporteurs sollte mit derjenigen im Zollrecht harmonisiert werden.

Wettbewerbsfähigkeit sichern: Vorsicht bei unilateralen und autonomen Listen der EU

Der Kommissionsentwurf sieht in Artikel 16 Abs. 1, 2b, 4, 5, 8 eine neue Ermächtigung der EU-Kommission vor. Hiermit kann die EU-Kommission per delegiertem Rechtsakt neue Güterlistungen im Bereich der Sicherheits- und Überwachungstechnologien vornehmen. Die Güterlistungen stehen dann in Anhang I, Sektion B.

Die autonome Listung ist bedenklich, weil die EU-Kommission Güterlistungsvorschläge im Alleingang ohne Vorabstimmung mit den EU-Mitgliedstaaten vornehmen kann. Die EU-Kommission verfügt aktuell nicht über die fachliche Kompetenz für Neulistungen in Anhang I, Sektion B. Hierdurch droht ein Absinken von Standards. Güterlistungen müssen technisch sauber und sinnvoll gestaltet sein. Vor Güterlistungen in internationalen Regimen beraten Fachgremien aus Regierungsvertretern der Mitgliedstaaten der Regime regelmäßig technische Güterklassifikationen, technische Beschreibungen und Risikoabschätzungen. Diese Qualitätsstandards sollten auf EU-Ebene nicht unterschritten werden. Die in Artikel 21 Abs. 3 für die EU-autonomen Listungen vorgesehene Einbindung der Mitgliedstaaten über die „*Dual Use Coordination Group*“ ist wenig systematisch und gewährleistet keine zwingende Berücksichtigung der Expertise aus den Mitgliedstaaten. Das spätere Einspruchsrecht des Rates im Verfahren des delegierten Rechtsaktes ist zu schwach und ist kein Gestaltungsrecht. Auch die Fachexperten der Unternehmen sollten für technologie- und marktbezogene Fragen systematisch einbezogen werden.

Alleingänge der EU ohne Abstimmung auf internationaler Ebene gefährden zudem das globale *level playing field* und die Wettbewerbsfähigkeit der europäischen Industrie. Zudem kann die EU-Kommission weniger Einfluss auf verantwortungsvolle Lieferungen in Drittländer nehmen. Eine unilatrale Güterlistung der EU sollte daher nur nachrangig gegenüber einer Güterlistung in den internationalen Regimen und als *ultima ratio* angewandt werden. Exportkontrollvorschriften sind nur dann nachhalttig, wenn gleiche Regelungen für alle gelten.

Die Empfehlung der Industrie:

- **Globale Wettbewerbsfähigkeit und verantwortungsvolle Lieferungen sichern:** Europäische Alleingänge sollte die EU vermeiden. Effektive Kontrollen können nur in Zusammenarbeit mit den Partnern der EU in den internationalen Exportkontrollregimen durchgeführt werden. Vorrangig sollte die EU kritische Güterlistungen auf internationaler Ebene in den bestehenden vier Exportkontrollregimen vorantreiben. Wenn Listungen von Sicherheits- und Überwachungstechnologie dort schwer erfasst werden können, sollte das Mandat dieser Regime ausgeweitet werden.

- **EU-Mitgliedstaaten einbeziehen**: Mitgliedstaaten sollten in die Entscheidungen über EU-autonome Listungen systematisch eingebunden werden. Falls Neulistungen zeitkritisch sind, kann das Fast-Track-Verfahren eingesetzt werden, das heute auch bei der Antifolterverordnung eingesetzt wird.

- **EU-autonomen Listungskompetenzen müssen Delistungskompetenzen gegenüberstehen:** Sofern die EU autonome Listungen vornehmen kann, muss sie auch Delistungen ermöglichen. Denn der schnelle technologische Wandel führt auch dazu, dass kritische Hochtechnologiegüter von heute Massenwaren von morgen sind. Sind Güter weltweit verfügbar oder leicht herstellbar, sind aufwendige Exportkontrollen weder effektiv noch effizient.

Vorsicht vor der Extraterritorialität von Regelungen

Der Broker und der Erbringer technischer Unterstützung

Der Kommissionsentwurf sieht vor, die Beschränkungen für Handels- und Vermittlungsgeschäfte (*brokering*) auch auf Unternehmen mit Sitz außerhalb der EU anzuwenden, wenn diese von einem EU-Unternehmen oder einer EU-Person kontrolliert werden (Artikel 2 Abs. 7). Eine gleiche Regelung wird für die Erbringer von technischer Unterstützung eingeführt (Artikel 2 Abs. 9). Diese Extraterritorialität ist politisch und völkerrechtlich fragwürdig und kaum administrierbar. Staatliches Handeln setzt einen Bezug zum eigenen Staatsgebiet voraus. Klassischerweise erfordert dies als Anknüpfungspunkt eine Handlung einer Person auf dem Hoheitsgebiet des Staates oder eine Handlung mit Wirkung auf das Hoheitsgebiet des Staates. Auch die Nationalität der Person kann Anknüpfungspunkt sein. Je schwächer der Bezugspunkt jedoch ist, desto schwieriger ist die extraterritoriale Wirkung des Rechts völkerrechtlich zu rechtfertigen, da die Extraterritorialität einem Drittstaat zumutet, dass fremdes Recht auch auf seinem Hoheitsgebiet Gültigkeit erlangt. Auch das Europäische Parlament und der Rat als Gesetzgeber über das EU-Hoheitsgebiet müssen beurteilen, ob es weitere (ausländische) Gesetzgeber neben sich gelten lassen möchte. Wenn sich die EU-Institutionen selbst dieses Recht in Bezug auf Drittstaaten einräumen, müssten sie dieses Recht auch ausländischen Gesetzgebern zugestehen.

Von der politisch-rechtlich schwierigen Fragestellung abgesehen ist der Bezugspunkt der Definitionen des Artikels 2 Abs. 7 und 9 unklar. Nicht eindeutig ist, wann die „Kontrolle über ein Unternehmen“ anzunehmen ist. Ab welchen Mehrheitsverhältnissen und Sperrminoritäten gelten sie? Wie wirkt sich die Regelung auf Investitionsmöglichkeiten von KMU im Ausland aus? Und welche ausländischen ICP-Regeln müssen wir in unseren Unternehmen künftig in der EU akzeptieren? Freiwillige interne Compliance Programme (ICPs) würden diese schwierigen Fragestellungen nicht aufwerfen. Die positiven Anreize für ICPs in den neuen EU-Allgemeingenehmigungen für Technologietransfer in verbundenen Unternehmen (Anhang II, Sektion H Nr. 3 als künftige EU008) sind ein effektives, aber weniger einschneidendes Mittel.

Die Empfehlung der Industrie:

- **Keine extraterritorialen Regeln:** Die EU darf nicht mit zweierlei Maß messen: Sie sollte keine verpflichtenden extraterritorialen Regeln schaffen, gegen die sie sich sonst gegenüber anderen Staaten, wie den USA, wehrt.

- **Positive Anreize für interne Compliance Systeme schaffen:** Über die EU-Allgemeingenehmigung für Technologietransfer in verbundenen Unternehmen kann die EU Unternehmen belohnen, die sich in ihren Niederlassungen weltweit für hohe Exportkontroll-Standards einsetzen.

Gültigkeit von Genehmigungen: Planungsfähigkeit sichern, Behörden nicht überlasten

Der Kommissionsentwurf sieht vor, die Gültigkeitsdauer der Exportgenehmigungen von zwei Jahren auf ein Jahr zu verkürzen. Artikel 10, Absatz 3 sieht diese kürzere Gültigkeitsdauer sowohl für die Einzelausfuhr- wie auch für Globalgenehmigungen vor. Die Industrie büßt dadurch Planungssicherheit ein. Auch drohen längere Bearbeitungszeiten in Antragsverfahren, da sich für die nationalen Genehmigungsbehörden das Antragsvolumen verdoppeln kann.

Die vorgeschlagenen Änderungen sind wettbewerbsschädlich. Attraktiv sind Anbieter nur, wenn sie gegenüber ihren Kunden (Liefer-) Zusagen einhalten können. Erscheint die Zuverlässigkeit eines Unternehmens zweifelhaft, ziehen Abnehmer Konkurrenten vor. Wird die Gültigkeit der Exportgenehmigungen von zwei Jahren auf ein Jahr verkürzt, können europäische Unternehmen keine langfristigen Lieferzusagen mehr treffen. Auch ihre Planungsfähigkeit im Projektgeschäft leidet erheblich.

Eine verkürzte Gültigkeitsdauer ist unnötig: Ändern sich die politischen Verhältnisse in einem Drittland und sind dort plötzlich Menschenrechtsverletzungen zu befürchten, kann der Export gleichwohl gestoppt werden. Genehmigungsbehörden können schon heute jede Genehmigung im Wege einer Rücknahme oder eines Widerrufes aufheben. In Deutschland etwa richtet sich dies nach den Bestimmungen des allgemeinen Verwaltungsrechts (§§ 48 und 49 Verwaltungsverfahrensgesetz, VwVfG). Gerade das Instrument des Widerrufes ermöglicht es, die verwaltungsrechtliche Entscheidung an die veränderte Sach- und Rechtslage anzupassen. Hierzu können auch die politisch-rechtlichen Umstände in einem Land zählen, sofern diese für die Erteilung der Exportgenehmigung zu berücksichtigen sind.

Die Empfehlung der Industrie:

- **Die zweijährige Gültigkeit von Genehmigungen erhalten:** Die Gültigkeit von Einzelausfuhr- und Globalgenehmigungen sollte weiterhin zwei Jahre betragen.

EU-Leitlinien schaffen keine Rechtssicherheit

Rechtssicherheit ist ein Eckpfeiler des Rechtsstaates, die Herrschaft des Rechts („*rule of law*“) ein wesentliches Prinzip auch der EU-Gesetzgebung. Der vorliegende Verordnungsentwurf stellt im Vergleich zur aktuell gültigen Fassung jedoch eine Verschlechterung der Rechtssicherheit dar. Gerade die neuen Catch-All-Regeln genügen nicht dem Bestimmtheitsgrundsatz; wesentliche Definitionen sind unklar. Die Kommission versucht diesen Umstand durch die Entwicklung von Leitlinien zu korrigieren[14] und kündigt an, diese „in enger Abstimmung mit den Mitgliedstaaten und Interessenträgern“ entwickeln zu wollen. Letzteres ist zu begrüßen, kann aber fehlende Rechtssicherheit nicht mindern, da EU-Leitlinien nicht verbindlich sind und keinen Gesetzescharakter haben. Leitlinien können sogar Umsetzungsunterschiede in Mitgliedstaaten befördern, da sich manche Mitgliedstaaten strikter an Leitlinien orientieren als andere. Das *level playing field* innerhalb der EU wird dadurch nicht gestärkt.

Die Bestimmungen des Verordnungstextes müssen auch ohne EU-Leitlinien eine sichere und effiziente Umsetzung erlauben. Leitlinien dürfen allenfalls als Sammlung guter Verwaltungspraxis verstanden werden und sollten unabhängig von diesem Gesetzgebungsprozess ständig geprüft und aktualisiert werden.

[14] EU-Kommission, Verordnungsvorschlag 2016/0295 (COD), Seite 5.

Quellenverzeichnis

Europäische Kommission (2016) Verordnungsvorschlag für eine Verordnung des Europäischen Parlaments und des Rats über eine Unionsregelung für die Kontrolle der Ausfuhr, der Verbringung, der Vermittlung, der technischen Unterstützung und der Durchfuhr betreffend Güter mit doppeltem Verwendungszweck (Neufassung), COM(2016)616 final

Europäische Kommission (2016). *Commission staff working document, Impact Assessment, Report on the EU Export Control Policy Review* SWD(2016)315 final

Impressum

Bundesverband der Deutschen Industrie e.V. (BDI)
Breite Straße 29, 10178 Berlin
www.bdi.eu
T: +49 30 2028-0

Redaktion

Dr. Stormy-Annika Mildner
T: +49 30 2028-1562
S.Mildner@bdi.eu

Verena Kantel
T: +49 30 2028-1518
V.Kantel@bdi.eu

Fabian Wendenburg
T: +49 30 2028-1421
F.Wendenburg@bdi.eu

D 0839