Amtsblatt
der Europäischen Union

DE
Reihe L

2024/2659

16.10.2024

EMPFEHLUNG (EU) 2024/2659 DER KOMMISSION

vom 11. Oktober 2024

zu Leitlinien für die Ausfuhr von Gütern für digitale Überwachung gemäß Artikel 5 der Verordnung (EU) 2021/821 des Europäischen Parlaments und des Rates

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 292,

in Erwägung nachstehender Gründe:

(1) Mit der Verordnung (EU) 2021/821 des Europäischen Parlaments und des Rates ([1]) wurde eine Unionsregelung für die Kontrolle der Ausfuhr, der Vermittlung, der technischen Unterstützung, der Durchfuhr und der Verbringung betreffend Güter mit doppeltem Verwendungszweck festgelegt.

(2) Mit der Verordnung (EU) 2021/821 wird dem Risiko begegnet, dass Güter für digitale Überwachung im Zusammenhang mit interner Repression und/oder der Begehung schwerwiegender Verstöße gegen die Menschenrechte und das humanitäre Völkerrecht verwendet werden.

(3) Gemäß Artikel 5 Absatz 2 und Artikel 26 Absatz 1 der Verordnung (EU) 2021/821 stellen die Kommission und der Rat Ausführern Leitlinien in Bezug auf nicht gelistete Güter für digitale Überwachung zur Verfügung, um die Effizienz der Ausfuhrkontrollregelung der Union im Hinblick auf die Cybersicherheit und die kohärente Durchführung der Verordnung (EU) 2021/821 zu gewährleisten.

(4) Diese Empfehlung und die ihr beigefügten Leitlinien zielen darauf ab, Ausführer bei der Durchführung von Kontrollen im Bereich der nicht gelisteten Güter für digitale Überwachung zu unterstützen, was unter anderem Maßnahmen im Rahmen der Sorgfaltspflicht zur Bewertung der Risiken im Zusammenhang mit der Ausfuhr solcher Güter einschließt.

(5) Die dieser Empfehlung beigefügten Leitlinien waren 2022 und 2023 Gegenstand umfassender Konsultationen in der Sachverständigengruppe für Überwachungstechnologie, und es wurden dabei Stellungnahmen berücksichtigt, die im zweiten Quartal 2023 bei einer öffentlichen Konsultation ([2]) eingegangen sind.

(6) Es sei darauf hingewiesen, dass diese Empfehlung und die beigefügten Leitlinien nicht bindend sind. Die Ausführer sollten daher weiterhin dafür verantwortlich sein, ihren Verpflichtungen gemäß der Verordnung (EU) 2021/821 nachzukommen, während die Kommission sicherstellen sollte, dass diese Empfehlung im Laufe der Zeit nicht an Relevanz verliert —

([1]) Verordnung (EU) 2021/821 des Europäischen Parlaments und des Rates vom 20. Mai 2021 über eine Unionsregelung für die Kontrolle der Ausfuhr, der Vermittlung, der technischen Unterstützung der Durchfuhr und der Verbringung betreffend Güter mit doppeltem Verwendungszweck (ABl. L 206 vom 11.6.2021, S. 1, ELI: http://data.europa.eu/eli/reg/2021/821/oj).

([2]) https://policy.trade.ec.europa.eu/consultations/guidelines-export-cyber-surveillance-items-under-article-5-regulation-eu-no-2021821_en.

HAT FOLGENDE EMPFEHLUNG ABGEGEBEN:

Den zuständigen Behörden der Mitgliedstaaten und den Ausführern wird geraten, die im Anhang dieser Empfehlung enthaltenen Leitlinien zu berücksichtigen, damit sie ihren Verpflichtungen gemäß Artikel 5 Absatz 2 der Verordnung (EU) 2021/821 nachkommen.

Brüssel, den 11. Oktober 2024

Für die Kommission
Valdis DOMBROVSKIS
Exekutiv-Vizepräsident

ANHANG

INHALT

Seite

Einleitung ... 4

1. Einschlägige Rechtsvorschriften, Begriffsbestimmungen und Schlüsselbegriffe ... 4

1.1. Überblick über die einschlägigen Rechtsvorschriften ... 4

1.2. Zentrale Begriffsbestimmungen ... 5

1.2.1. „Besonders konstruiert“ ... 5

1.2.2. „Verdeckte Überwachung“ ... 6

1.2.3. „Natürliche Personen“ ... 6

1.2.4. „Überwachung, Extraktion, Erhebung, Analyse von Daten“ ... 6

1.2.5. „Aus Informations- und Telekommunikationssystemen“ ... 7

1.2.6. „Kenntnis“ und „bestimmt sein für“ ... 7

1.3. Interne Repression, schwerwiegende Verstöße gegen die Menschenrechte und das humanitäre Völkerrecht ... 7

1.3.1. Interne Repression ... 8

1.3.2. Begehung schwerwiegender Verstöße gegen die Menschenrechte ... 8

1.3.3. Begehung schwerwiegender Verstöße gegen das humanitäre Völkerrecht ... 9

2. Technischer Anwendungsbereich ... 9

2.1. Gelistete Güter für digitale Überwachung ... 9

2.2. Potenzielle nicht gelistete Güter für digitale Überwachung ... 9

2.2.1. Gesichts- und Emotionserkennungstechnologie ... 10

2.2.2. Ortungsgeräte ... 10

2.2.3. Videoüberwachungssysteme ... 10

3. Maßnahmen im Rahmen der Sorgfaltspflicht ... 10

Anforderungen gemäß Artikel 5 Absatz 2 der Verordnung (EU) 2021/821 ... 12

4. Anlage ... 12

Gelistete Güter für digitale Überwachung, die gemäß Anhang I der Verordnung (EU) 2021/821 Kontrollen unterliegen ... 12

Systeme für das Abhören von Telekommunikation (5A001f) ... 12

Internet-Überwachungssysteme (5A001j) ... 13

„Intrusion-Software“ (4A005, 4D004 und damit verbundene Kontrollen nach den Unternummern 4E001a und 4E001c) 13

Kommunikationsüberwachungssoftware (5D001e) ... 14

Zur Ausführung der Kryptoanalyse verwendete Güter (5A004a) ... 14

Forensische Instrumente/Ermittlungsinstrumente (5A004b, 5D002a3b und 5D002c3b) ... 14

EINLEITUNG

Mit dem durch die Verordnung (EU) 2021/821 geschaffenen Ausfuhrkontrollrahmen der Union (im Folgenden „Verordnung“) soll sichergestellt werden, dass die internationalen Verpflichtungen und Zusagen der Union und ihrer Mitgliedstaaten, auch in Bezug auf Frieden, Sicherheit und Stabilität auf regionaler Ebene und die Achtung der Menschenrechte und des humanitären Völkerrechts, eingehalten werden. Die Union und ihre Mitgliedstaaten haben daher die im Rahmen der multilateralen Ausfuhrkontrollregelungen gefassten Beschlüsse umgesetzt und die EU-Ausfuhrkontrollliste in Anhang I der Verordnung entsprechend aktualisiert ([1]). Darüber hinaus hatten die zuständigen Behörden der Mitgliedstaaten bereits vor Anwendbarkeit des Artikels 5 der Verordnung die Ausfuhr bestimmter gelisteter Güter, die für Überwachungszwecke verwendet werden könnten, kontrolliert ([2]) und Risiken eines unter bestimmten besonderen Umständen möglichen Missbrauchs berücksichtigt. Bei Vorliegen besonders schwerwiegender Umstände hat die Union Sanktionen verhängt, die die Ausfuhr bestimmter Überwachungsausrüstung beschränken ([3]).

Die Verordnung spiegelt die Entschlossenheit der Union wider, wirksam gegen das Risiko vorzugehen, dass Güter für digitale Überwachung im Zusammenhang mit interner Repression und/oder der Begehung schwerwiegender Verstöße gegen die Menschenrechte und das humanitäre Völkerrecht verwendet werden. Mit der Verordnung werden insbesondere neue Bestimmungen für die Kontrolle der Ausfuhr nicht gelisteter Güter für digitale Überwachung eingeführt, einschließlich der Verpflichtung der Ausführer, die zuständige Behörde zu unterrichten, wenn ihnen aufgrund von im Rahmen ihrer Sorgfaltspflicht erlangten Erkenntnissen bekannt ist, dass nicht gelistete Güter für digitale Überwachung, die ausgeführt werden sollen, ganz oder teilweise zur Verwendung im Zusammenhang mit interner Repression und/oder der Begehung schwerwiegender Verstöße gegen die Menschenrechte und das humanitäre Völkerrecht bestimmt sind. In der Verordnung werden die Kommission und der Rat ferner aufgefordert, den Ausführern Leitlinien zur Verfügung zu stellen, um die wirksame Umsetzung der neuen Kontrollen für nicht gelistete Güter für digitale Überwachung zu unterstützen.

Diese Leitlinien zielen daher darauf ab, die Ausführer bei der Durchführung von Kontrollen nicht gelisteter Güter für digitale Überwachung zu unterstützen, unter anderem bei Maßnahmen im Rahmen der Sorgfaltspflicht zur Bewertung der Risiken im Zusammenhang mit der Ausfuhr solcher Güter zu Endverwendern und Endverwendungen gemäß den neuen Bestimmungen der Verordnung.

1. EINSCHLÄGIGE RECHTSVORSCHRIFTEN, BEGRIFFSBESTIMMUNGEN UND SCHLÜSSELBEGRIFFE

1.1. Überblick über die einschlägigen Rechtsvorschriften

Mit der Verordnung werden neue Bestimmungen eingeführt, die insbesondere Kontrollen für die Ausfuhr von nicht in Anhang I der Verordnung aufgeführten Gütern für digitale Überwachung vorsehen, die ganz oder teilweise für eine Verwendung im Zusammenhang mit interner Repression und/oder der Begehung schwerwiegender Verstöße gegen die Menschenrechte und das humanitäre Völkerrecht bestimmt sind oder sein könnten. Die maßgeblichen Erwägungsgründe und Artikel sind folgende:

a) Erwägungsgrund 8: „Um dem Risiko zu begegnen, dass gewisse aus dem Zollgebiet der Union ausgeführte nicht gelistete Güter für digitale Überwachung durch Personen missbraucht werden könnten, die an der Anordnung oder Begehung schwerwiegender Verstöße gegen die Menschenrechte oder das humanitäre Völkerrecht beteiligt oder dafür verantwortlich sind, ist es angezeigt, die Ausfuhr solcher Güter zu kontrollieren. Die damit verbundenen Risiken beziehen sich insbesondere auf Fälle, in denen Güter für digitale Überwachung besonders dafür konstruiert sind, das Eindringen in Informations- und Telekommunikationssysteme oder eine entsprechende tiefgreifende

([1]) Siehe insbesondere die Kontrollen betreffend Systeme für das Abhören von Telekommunikation (5A001f), Internetüberwachungssysteme (5A001j), Intrusion-Software (4A005, 4D004 und damit verbundene Kontrollen nach den Unternummern 4E001a und 4E001c) und Software für die Überwachung zur Verhütung oder Verfolgung von Straftaten oder zum Strafvollzug (5D001e). Siehe ferner auf der Grundlage einer Einzelfallbewertung Kontrollen betreffend bestimmte forensische Instrumente/Ermittlungsinstrumente (5A004b, 5D002a3b und 5D002c3b).

([2]) Insbesondere Systeme für Informationssicherheit.

([3]) Siehe angesichts der Lage in Belarus und der Rolle von Belarus im russischen Angriffskrieg gegen die Ukraine Verordnung (EG) Nr. 765/2006 des Rates vom 18. Mai 2006 (ABl. L 134 vom 20.5.2006, S. 1, ELI: http://data.europa.eu/eli/reg/2006/765/oj), 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. L 100 vom 14.4.2011, S. 1, ELI: http://data.europa.eu/eli/reg/2011/359/oj), Verordnung (EU) Nr. 36/2012 des Rates vom 18. Januar 2012 über restriktive Maßnahmen angesichts der Lage in Syrien und zur Aufhebung der Verordnung (EU) Nr. 442/2011 (ABl. L 16 vom 19.1.2012, S. 1, ELI: http://data.europa.eu/eli/reg/2012/36/oj), Verordnung (EU) Nr. 401/2013 des Rates vom 2. Mai 2013 über restriktive Maßnahmen gegen Myanmar/Birma und zur Aufhebung der Verordnung (EG) Nr. 194/2008 (ABl. L 121 vom 3.5.2013, S. 1, ELI: http://data.europa.eu/eli/reg/2013/401/oj) und Verordnung (EU) 2017/2063 des Rates vom 13. November 2017 über restriktive Maßnahmen angesichts der Lage in Venezuela (ABl. L 295 vom 14.11.2017, S. 21, ELI: http://data.europa.eu/eli/reg/2017/2063/oj).

Datenpaketanalyse (‚deep-packet inspection') zu ermöglichen, um natürliche Personen durch Überwachung, Extraktion, Erhebung oder Analyse von Daten, einschließlich biometrischer Daten, aus diesen Systemen verdeckt zu überwachen. Güter, die für eine rein kommerzielle Anwendung verwendet werden, etwa Rechnungsstellung, Marketing, Qualitätsdienste, Nutzerzufriedenheit oder Netzsicherheit, gelten im Allgemeinen als nicht mit derartigen Risiken behaftet."

b) Erwägungsgrund 9: „Im Hinblick auf eine wirksamere Kontrolle der Ausfuhr nicht gelisteter Güter für digitale Überwachung ist es von wesentlicher Bedeutung, die Anwendung von ‚Catch-all-Kontrollen' in diesem Bereich weiter zu harmonisieren. Zu diesem Zweck sind die Mitgliedstaaten verpflichtet, derartige Kontrollen zu unterstützen, indem sie untereinander und mit der Kommission Informationen austauschen, insbesondere über technologische Entwicklungen von Gütern für digitale Überwachung, und indem sie bei der Anwendung derartiger Kontrollen Wachsamkeit walten lassen, um einen Austausch auf Unionsebene zu fördern."

c) Artikel 2 Nummer 20, in dem der Begriff „Güter für digitale Überwachung" als „Güter mit doppeltem Verwendungszweck, die besonders dafür konstruiert sind, die verdeckte Überwachung natürlicher Personen durch Überwachung, Extraktion, Erhebung oder Analyse von Daten aus Informations- und Telekommunikationssystemen zu ermöglichen", definiert wird.

d) In Artikel 5 wird eine Genehmigungspflicht für die Ausfuhr von Gütern für digitale Überwachung eingeführt, wenn der Ausführer von der zuständigen Behörde davon unterrichtet worden ist, dass die betreffenden Güter ganz oder teilweise für eine Verwendung im Zusammenhang mit interner Repression und/oder der Begehung schwerwiegender Verstöße gegen die Menschenrechte und das humanitäre Völkerrecht bestimmt sind oder bestimmt sein können (Artikel 5 Absatz 1). Ferner sind Ausführer verpflichtet, die zuständige Behörde zu unterrichten, wenn ihnen aufgrund von im Rahmen ihrer Sorgfaltspflicht erlangten Erkenntnissen bekannt ist, dass Güter für digitale Überwachung ganz oder teilweise für eine Verwendung im Zusammenhang mit interner Repression und/oder der Begehung schwerwiegender Verstöße gegen die Menschenrechte und das humanitäre Völkerrecht bestimmt sind (Artikel 5 Absatz 2). Die zuständige Behörde muss entscheiden, ob die Ausfuhr dieser Güter genehmigungspflichtig sein soll.

e) In Artikel 5 Absatz 2 heißt es weiter: „Die Kommission und der Rat stellen den Ausführern Leitlinien gemäß Artikel 26 Absatz 1 zur Verfügung."

1.2. **Zentrale Begriffsbestimmungen**

Die Verordnung enthält spezielle Erwägungsgründe und Bestimmungen, in denen bestimmte Begriffe präzisiert werden, die für die Kontrolle der Ausfuhr nicht gelisteter Güter für digitale Überwachung relevant und für das Verständnis der Ausführer wichtig sind, um ihre Sorgfaltspflicht erfüllen und Kontrollen wirksam durchführen zu können. Von besonderer Relevanz ist Artikel 2 Nummer 20, der die folgende genaue Bestimmung des Begriffs „Güter für digitale Überwachung" enthält: „Güter mit doppeltem Verwendungszweck, die besonders dafür konstruiert sind, die verdeckte Überwachung natürlicher Personen durch Überwachung, Extraktion, Erhebung oder Analyse von Daten aus Informations- und Telekommunikationssystemen zu ermöglichen."

Für die Zwecke dieser Leitlinien sollten spezifische Aspekte dieser Begriffsbestimmung präzisiert werden.

1.2.1. *„Besonders konstruiert"*

Ein Gut ist für verdeckte Überwachung konstruiert, wenn sich seine technischen Merkmale für eine verdeckte Überwachung natürlicher Personen eignen und diese objektiv ermöglichen. Der Begriff „besonders konstruiert" bedeutet daher, dass das Produkt hauptsächlich zum Zweck der verdeckten Überwachung natürlicher Personen entwickelt und konstruiert worden sein muss. Der Begriff setzt jedoch nicht voraus, dass das Gut ausschließlich für die verdeckte Überwachung natürlicher Personen verwendbar ist.

Wie in Erwägungsgrund 8 der Verordnung klargestellt, sind Güter, die für eine rein kommerzielle Anwendung verwendet werden, etwa Rechnungsstellung, Marketing, Qualitätsdienste, Nutzerzufriedenheit oder Netzsicherheit, nicht besonders für die verdeckte Überwachung natürlicher Personen konstruiert und fallen daher nicht unter die Begriffsbestimmung von Gütern für digitale Überwachung. Selbst wenn beispielsweise Güter zur Überwachung von Betriebssystemen in der Industrie oder zur Überwachung des Nutzerverkehrs für Überwachungszwecke verwendet werden könnten, handelt es sich bei diesen Gütern nicht um Güter für digitale Überwachung im Sinne der Definition, da sie nicht besonders für die verdeckte Überwachung natürlicher Personen konstruiert sind.

1.2.2. *„Verdeckte Überwachung“*

Güter ermöglichen insbesondere dann eine verdeckte Überwachung, wenn die Überwachung für die betroffene natürliche Person nicht offensichtlich erkennbar ist. Dies wäre der Fall, wenn den betroffenen Personen nicht bekannt ist, dass Güter für digitale Überwachung vorhanden und/oder in Betrieb sind, und sie daher nicht die Möglichkeit haben, sich aus dem Überwachungsbereich zu entfernen oder zumindest ihr Verhalten entsprechend auszurichten. Selbst wenn die Überwachung mithilfe von im öffentlichen Raum installierten oder betriebenen Geräten erfolgt, kann die Erfassung von Daten in bestimmten Fällen als verdeckte Überwachung angesehen werden, insbesondere dann, wenn die erhobenen Daten für andere Zwecke umgeleitet, ausgewertet oder weiterverarbeitet werden können als die Zwecke, die der betroffenen natürlichen Person bekannt gemacht worden sind. Mit anderen Worten, wenn eine natürliche Person objektiv nicht davon ausgehen kann, dass sie überwacht wird, kann die Überwachung als verdeckt im Sinne von Artikel 2 Nummer 20 der Verordnung angesehen werden.

1.2.3. *„Natürliche Personen“*

Der Begriff „natürliche Person“ bezieht sich auf einen lebenden Menschen im Gegensatz zu juristischen Personen oder Organisationen, die folglich nicht den Bestimmungen unterliegen. Der Begriff umfasst nicht die Überwachung von Objekten, Standorten oder Maschinen.

1.2.4. *„Überwachung, Extraktion, Erhebung, Analyse von Daten“*

Laut dem Oxford English Dictionary haben die Wörter Überwachung, Extraktion, Erhebung und Analyse folgende sprachliche Bedeutung:

— „Überwachung“ bzw. „überwachen“: genau verfolgen, was jemand (der verdächtig ist) tut; jemanden, etwas durch ständiges Beobachten kontrollieren;

— „Extraktion“ bzw. „extrahieren“: [her]ausziehen;

— „Erhebung“ bzw. „erheben“: zusammentragen, sammeln;

— „Analyse“ (Duden — Das Fremdwörterbuch): systematische Untersuchung eines Gegenstandes oder Sachverhalts hinsichtlich aller einzelnen Komponenten oder Faktoren, die ihn bestimmen.

Diese Begriffe implizieren, dass die für die Überwachung eingesetzten Güter über präzise technische Datenverarbeitungsfähigkeiten verfügen sollten, um Daten überwachen, erheben, extrahieren oder analysieren zu können. Hierzu gehören z. B. die folgenden Güter:

a) Güter, die zur Überwachung von Daten aus Informations- und Telekommunikationssystemen verwendet werden ([4]) (z. B. Dateigröße oder Verkehr der in einem solchen System übertragenen Daten);

b) Güter, die Daten aus Informations- und Telekommunikationssystemen extrahieren, indem sie in die Systeme eindringen und Daten extrahieren (z. B. Intrusion-Software);

c) Güter, die eine Analyse der aus Informations- und Telekommunikationssystemen extrahierten Daten ermöglichen, einschließlich solcher, die in diesen Systemen gespeicherte Kamerabilder verarbeiten können (z. B. bestimmte Arten von Datenanalysetechnologien, die als Teil von Gesichtserkennungssystemen verwendet werden).

Güter, die zur einfachen Überwachung von Informationssystemen oder zur Beobachtung der Bevölkerung über Videoüberwachungskameras verwendet werden und es ermöglichen, Gespräche, den Austausch von Daten, Bewegungen und individuelle Verhaltensweisen zu erfassen, sind keine Güter für digitale Überwachung gemäß der Begriffsbestimmung der Verordnung, da sie nicht besonders für diesen Zweck konstruiert sind und da sie mit anderen Technologien wie künstlicher Intelligenz oder Big Data zusammenarbeiten müssen. Das gesamte System (in Zusammenarbeit mit anderen Technologien wie künstlicher Intelligenz oder Big-Data-Technologien) könnte jedoch möglicherweise ein Gut für digitale Überwachung gemäß der Begriffsbestimmung in Artikel 2 Nummer 20 der Verordnung sein.

Wichtig ist, dass zwar einige Beispiele zur Veranschaulichung genannt werden, damit jedoch keine Einschränkung der Begriffsbestimmung und der Bandbreite von Gütern für digitale Überwachung verbunden ist, da Artikel 5 darauf abzielt, eine wirksame Ausfuhrkontrolle bei nicht gelisteten Gütern zu ermöglichen.

([4]) Zur Begriffsbestimmung siehe 1.2.5.

Wie die Verwendung der Konjunktion „oder“ in der Begriffsbestimmung zeigt, sind die aufgeführten technischen Fähigkeiten als Alternativen zu betrachten, und es ist nicht erforderlich, dass ein Gut über alle diese technischen Fähigkeiten für die Überwachung, Extraktion, Erhebung oder Analyse von Daten verfügt. Mit anderen Worten, es genügt, dass ein Gut über eine dieser technischen Fähigkeiten verfügt, um unter die Bestimmung des Begriffs „Güter für digitale Überwachung“ in Artikel 2 Nummer 20 zu fallen.

1.2.5. *„Aus Informations- und Telekommunikationssystemen“*

Diese beiden Begriffe beziehen sich auf Systeme, die Informationen elektronisch verarbeiten, z. B. Programmierung/Kodierung, Betrieb von PC-Systemen (Hardware) und sonstige Informationsverwaltung, einschließlich Softwaretechnologie, Web-Technologie, Computertechnologie, Speichertechnologie usw., sowie auf einige Systeme, die Informationen über eine Distanz übertragen, z. B. technische Systeme, die Töne, Signale, Texte, sonstige Zeichen oder Bilder über drahtgebundene und drahtlose Kanäle, optische Fasern, Funk und andere elektromagnetische Systeme übertragen. Zusammen umfassen diese beiden Begriffe ein breites Spektrum von Systemen, die Informationen übermitteln oder verarbeiten. Es sei darauf hingewiesen, dass sich der Begriff auf Systeme und nicht auf Ausrüstung bezieht.

1.2.6. *„Kenntnis“ und „bestimmt sein für“*

Nach Artikel 5 Absatz 2 der Verordnung hat ein Ausführer die zuständige Behörde zu unterrichten, wenn ihm „bekannt“ ist, dass Güter für digitale Überwachung „für eine Verwendung im Zusammenhang mit interner Repression und/oder der Begehung schwerwiegender Verstöße gegen die Menschenrechte und das humanitäre Völkerrecht bestimmt sind oder bestimmt sein können.“

Der Begriff „bekannt“ ist kein neuer Rechtsbegriff, sondern wurde im Zusammenhang mit endverwendungsabhängigen Genehmigungspflichten (sogenannte „Catch-all-Kontrollen“) gemäß den Artikeln 4, 6, 7 und 8 der Verordnung verwendet. „Bekannt“ bedeutet, dass der Ausführer positive Kenntnis von dem beabsichtigten Missbrauch hat. Die bloße Möglichkeit eines solchen Risikos reicht nicht aus, um eine Kenntnis zu begründen. Der Begriff „Kenntnis“ kann jedoch nicht mit Passivität gleichgesetzt werden: Er setzt voraus, dass der Ausführer Schritte unternommen hat, um sich hinreichendes und angemessenes Wissen für die Bewertung der mit der Ausfuhr verbundenen Risiken zu verschaffen und die Einhaltung der Verordnung sicherzustellen.

Die Angabe, dass die Güter für eine relevante sensible Endverwendung „bestimmt“ sein müssen, bedeutet, dass der Ausführer die Endverwendung nach Lage des Einzelfalls unter Berücksichtigung der besonderen Umstände des Falls prüfen sollte. Im Umkehrschluss heißt dies, dass ein theoretisches, d. h. nicht auf eine konkrete Bewertung des Falls begründetes Risiko, dass die Güter in einer Weise verwendet werden könnten, die die Menschenrechte verletzt, nicht ausreicht, um davon auszugehen, dass sie für einen konkreten Missbrauch im Sinne von Artikel 5 „bestimmt sind“.

1.3. **Interne Repression, schwerwiegende Verstöße gegen die Menschenrechte und das humanitäre Völkerrecht**

Gemäß Artikel 15 der Verordnung, in dem die Erwägungen für die Entscheidung, ob eine Genehmigung erteilt wird, dargelegt sind, berücksichtigen die Mitgliedstaaten alle einschlägigen Erwägungen, einschließlich derjenigen, die durch den Gemeinsamen Standpunkt 2008/944/GASP des Rates ([5]) abgedeckt werden.

Durch Artikel 5 der Verordnung werden die Kontrollen der Ausfuhr nicht gelisteter Güter für digitale Überwachung ausgeweitet unter Einbeziehung des Risikos, dass sie im Zusammenhang mit interner Repression und/oder der Begehung schwerwiegender Verstöße gegen die Menschenrechte und das humanitäre Völkerrecht verwendet werden könnten. Der Gemeinsame Standpunkt 2008/944/GASP und der Leitfaden zur Anwendung des Gemeinsamen Standpunkts ([6]) bieten diesbezüglich nützliche Orientierungshilfen.

([5]) Gemeinsamer Standpunkt 2008/944/GASP des Rates vom 8. Dezember 2008 betreffend gemeinsame Regeln für die Kontrolle der Ausfuhr von Militärtechnologie und Militärgütern (ABl. L 335 vom 13.12.2008, S. 99, ELI: http://data.europa.eu/eli/compos/2008/944/oj).

([6]) Siehe Leitfaden zur Anwendung des Gemeinsamen Standpunkts 2008/944/GASP des Rates betreffend gemeinsame Regeln für die Kontrolle der Ausfuhr von Militärtechnologie und Militärgütern, https://www.parlament.gv.at/gegenstand/XXVI/EU/75074.

1.3.1. *Interne Repression*

Gemäß Artikel 2 Absatz 2 des Gemeinsamen Standpunkts 2008/944/GASP umfasst interne Repression „unter anderem Folter sowie andere grausame, unmenschliche und erniedrigende Behandlung oder Bestrafung, willkürliche oder Schnell-Hinrichtungen, das Verschwindenlassen von Personen, willkürliche Verhaftungen und andere schwere Verletzungen der Menschenrechte und Grundfreiheiten, wie sie in den einschlägigen Menschenrechtsübereinkünften, einschließlich der Allgemeinen Erklärung der Menschenrechte und des Internationalen Pakts über bürgerliche und politische Rechte, niedergelegt sind“ (IPBPR). Der Leitfaden zur Anwendung des Gemeinsamen Standpunkts 2008/944/GASP gibt Orientierungshilfe zu den Kriterien, die bei der Beurteilung durch den Ausführer zu berücksichtigen sind, darunter „das bisherige und das derzeitige Verhalten des vorgesehenen Endverwenders in Bezug auf die Achtung der Menschenrechte sowie die Haltung des Empfängerlandes generell in dieser Frage“.

1.3.2. *Begehung schwerwiegender Verstöße gegen die Menschenrechte*

Der Missbrauch nicht gelisteter Güter für digitale Überwachung kann negative Auswirkungen auf ein breites Spektrum von Menschenrechten haben und greift unmittelbar in das Recht auf Schutz der Privatsphäre und Datenschutz ein. Willkürliche oder unrechtmäßige Überwachung kann auch andere Menschenrechte verletzen, wie das Recht auf freie Meinungsäußerung, Vereinigungs- und Versammlungsfreiheit, Gedanken-, Gewissens- und Religionsfreiheit, das Recht auf Gleichbehandlung oder das Diskriminierungsverbot sowie das Recht auf freie, gleiche und geheime Wahlen. In besonderen Fällen kann die Überwachung, einschließlich der Beobachtung oder Einholung von Informationen über natürliche Personen wie Menschenrechtsverteidiger, Aktivisten, politische Persönlichkeiten, schutzbedürftige Bevölkerungsgruppen und Journalisten, zu Einschüchterung, Unterdrückung, willkürlichen Inhaftierungen, Folter oder sogar außergerichtlichen Hinrichtungen führen. Daher sollten die Ausführer diese Aspekte im Zusammenhang mit schwerwiegenden Verletzungen der Menschenrechte in ihre Bewertungen einbeziehen.

Die internationale Praxis zeigt, dass Einschränkungen der Menschenrechte „angemessen“ sein und mit den internationalen Menschenrechtsnormen im Einklang stehen müssen. In der Praxis bedeutet dies, dass angemessene Schutzmechanismen vorhanden sein müssen, die sicherstellen, dass Einschränkungen gesetzlich verankert sind und der Wesensgehalt der Rechte gewahrt bleibt. Unter Wahrung des Grundsatzes der Verhältnismäßigkeit dürfen Einschränkungen nur vorgenommen werden, wenn sie notwendig sind und tatsächlich einem legitimen Zweck dienen, z. B. der nationalen oder öffentlichen Sicherheit, der öffentlichen Ordnung, dem Schutz der öffentlichen Gesundheit oder dem Schutz der Rechte und Freiheiten anderer.

Güter für digitale Überwachung können legitime und regulierte Instrumente für Anwendungen in der Strafverfolgung umfassen, z. B. für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten, auch im Bereich der Terrorismusbekämpfung, oder die Vollstreckung strafrechtlicher Sanktionen. Gleichzeitig können Güter für digitale Überwachung jedoch auch für schwerwiegende Verstöße gegen die Menschenrechte und das humanitäre Völkerrecht missbraucht werden, wenn sie an repressive Regime oder private Endverwender und/oder in Konfliktgebiete ausgeführt werden.

Daher ist eine Bewertung der Umstände eines jeden Einzelfalls erforderlich, einschließlich der Anwendung der einschlägigen Vorschriften vor dem Hintergrund etwaiger Berichte der zuständigen Gremien der Vereinten Nationen, der Union oder des Europarats über schwere Menschenrechtsverletzungen. Die Anerkennung solcher Verstöße in Informationen, die von den zuständigen Gremien der Vereinten Nationen, von der Union oder dem Europarat veröffentlicht werden, kann ein Hinweis auf „schwerwiegende“ Verstöße gegen die Menschenrechte sein. Eine solch ausdrückliche Anerkennung durch diese Stellen ist keine unabdingbare Voraussetzung, stellt jedoch einen wichtigen Anhaltspunkt für die Erfüllung der Kriterien dar.

Gemäß Artikel 5 muss eine Menschenrechtsverletzung „schwerwiegend“ sein. Nützliche Hinweise zur Einstufung möglicher Menschenrechtsverletzungen als „schwerwiegend“ sind dem Leitfaden zur Anwendung des Gemeinsamen Standpunkts 2008/944/GASP zu entnehmen. Gemäß diesem Leitfaden sind die Art und Weise und die Folgen des Verstoßes entscheidend. Systematische und/oder weitverbreitete Menschenrechtsverletzungen werden regelmäßig als schwerwiegend angesehen. Aber auch Verstöße, die nicht systematisch oder weitverbreitet sind, können — beispielsweise aufgrund der Schwere der Folgen für die betroffenen Personen — als „schwerwiegend“ angesehen werden.

Anlage II des Leitfadens zur Anwendung des Gemeinsamen Standpunkts 2008/944/GASP enthält eine nicht erschöpfende Liste der wichtigsten internationalen und regionalen Menschenrechtsübereinkünfte, einschließlich des Internationalen Pakts über bürgerliche und politische Rechte (IPBPR), des Übereinkommens gegen Folter und andere grausame, unmenschliche oder erniedrigende Behandlung oder Strafe, der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (im Folgenden „Konvention“) und der Charta der Grundrechte (im Folgenden „Charta“), die als wichtige Orientierungshilfe für die Auslegung und Anwendung der Kriterien zur Unterstützung solider Bewertungen im Bereich der Menschenrechte dienen können. Diese Übereinkünfte und ihre jeweiligen Zusatzprotokolle stellen die wichtigsten internationalen Normen und Standards im Bereich der Menschenrechte und Grundfreiheiten dar.

1.3.3. *Begehung schwerwiegender Verstöße gegen das humanitäre Völkerrecht*

Das humanitäre Völkerrecht (auch als „Genfer Recht“ oder „Gesetz des bewaffneten Konflikts“ bezeichnet) wurde durch eine Reihe internationaler Verträge entwickelt, an erster Stelle die Haager Landkriegsordnung, die Genfer Abkommen sowie ihre beiden Zusatzprotokolle von 1977, und umfasst Regeln, mit denen das Ziel verfolgt wird, in Zeiten eines bewaffneten Konflikts Menschen zu schützen, die nicht oder nicht mehr an den Feindseligkeiten teilnehmen (z. B. Zivilpersonen und verletzte, kranke oder gefangen genommene Kombattanten), und die den Konfliktparteien Beschränkungen hinsichtlich der Mittel und Methoden der Kriegsführung auferlegen (Haager Recht).

Die Verwendung nicht gelisteter Güter für digitale Überwachung sollte im Einklang mit dem humanitären Völkerrecht stehen, wenn diese als Mittel und Methoden der Kriegsführung im Kontext eines bewaffneten Konflikts eingesetzt werden. Unter solchen Umständen ist dem Risiko schwerwiegender Verstöße gegen das humanitäre Völkerrecht gemäß der Verordnung Rechnung zu tragen und dieses sollte — wie bei der Begehung schwerwiegender Verstöße gegen die Menschenrechte — vor dem Hintergrund der beabsichtigten Endverwendung der Güter im konkreten Fall bewertet werden. Der Leitfaden zur Anwendung des Gemeinsamen Standpunkts 2008/944/GASP gibt Orientierungshilfe zu den zu berücksichtigenden Aspekten, darunter das bisherige und derzeitige Verhalten des Empfängers in Bezug auf die Achtung des humanitären Völkerrechts, durch förmliche Verpflichtungen zum Ausdruck gebrachte Absichten des Empfängers und die Fähigkeit des Empfängers, sicherzustellen, dass die Ausrüstung oder Technologie nach ihrer Weitergabe in einer mit dem humanitären Völkerrecht zu vereinbarenden Weise verwendet und nicht umgeleitet oder an andere Bestimmungsorte verbracht wird, wo sie für schwere Verletzungen des humanitären Völkerrechts verwendet werden könnte.

Nach Artikel 5 muss der Verstoß gegen das humanitäre Völkerrecht „schwerwiegend“ sein. Orientierungshilfe bietet der Leitfaden zur Anwendung des Gemeinsamen Standpunkts 2008/944/GASP, in dem anerkannt wird, dass „[e]inzelne Verletzungen des humanitären Völkerrechts (…) nicht zwangsläufig Ausdruck der Haltung des Empfängerlandes zum humanitären Völkerrecht“ sind, während, „wenn ein bestimmtes Muster von Verstößen festgestellt werden kann oder das Empfängerland keine geeigneten Schritte zur Ahndung von Verstößen unternommen hat, dies Anlass zu ernster Besorgnis“ geben sollte. Das Internationale Komitee vom Roten Kreuz (IKRK) hat Leitlinien für die Bewertung von Verstößen gegen das humanitäre Völkerrecht zum Zweck der Ausfuhrkontrolle festgelegt. Dem IKRK zufolge sind Verstöße gegen das humanitäre Völkerrecht schwerwiegend, „wenn sie geschützte Personen (z. B. Zivilpersonen, Kriegsgefangene, Verwundete und Kranke) oder Objekte (z. B. zivile Objekte oder Infrastrukturen) gefährden oder wichtige universelle Werte verletzen“. Kriegsverbrechen stellen beispielsweise schwere Verstöße gegen das humanitäre Völkerrecht dar. Das IKRK nennt ferner ähnliche zu berücksichtigende Faktoren, wie sie auch im Leitfaden zur Anwendung des Gemeinsamen Standpunkts 2008/944/GASP genannt sind, darunter förmliche Verpflichtungen zur Anwendung der Regeln des humanitären Völkerrechts, geeignete Maßnahmen zur Gewährleistung der Rechenschaftspflicht für Verstöße gegen das humanitäre Völkerrecht, Schulungen des Militärs im humanitären Völkerrecht und Verbot der Rekrutierung von Kindern für Streitkräfte.

2. **TECHNISCHER ANWENDUNGSBEREICH**

2.1. **Gelistete Güter für digitale Überwachung**

Die Anlage zu diesen Leitlinien enthält Informationen über in Anhang I der Verordnung aufgeführte Güter für digitale Überwachung, um Ausführer bei der Ermittlung potenzieller nicht gelisteter Güter für digitale Überwachung zu unterstützen.

2.2. **Potenzielle nicht gelistete Güter für digitale Überwachung**

Zwar ist es per definitionem nicht möglich, eine erschöpfende Liste der Produkte zu erstellen, die gemäß Artikel 5 als „nicht gelistete Güter“ kontrolliert werden können, jedoch könnten die folgenden Güter potenziell für eine Überwachung geeignet sein und daher eine besondere Wachsamkeit gemäß der Verordnung erfordern.

Wie in Erwägungsgrund 8 der Verordnung klargestellt, wird bei Gütern, die für rein kommerzielle Anwendungen wie Rechnungsstellung, Marketing, Qualitätsdienste, Nutzerzufriedenheit oder Netzsicherheit verwendet werden, im Allgemeinen davon ausgegangen, dass sie nicht mit Risiken eines Missbrauchs im Zusammenhang mit schwerwiegenden Verstößen gegen die Menschenrechte oder das humanitäre Völkerrecht behaftet sind, weshalb sie im Allgemeinen nicht der Kontrolle nach Artikel 5 unterliegen. Viele dieser Güter verfügen über Informationssicherheits-Funktionen (kryptografische oder sogar kryptoanalytische Funktionen), die den Kontrollparametern der Kategorie 5 Teil 2 der Beschreibung in Anhang I der Verordnung entsprechen. Sicherheits-Netzwerkausrüstung — einschließlich Router, Switches oder Repeater (relays), bei denen die Funktion der Informationssicherheit auf die Aufgaben von „Betrieb, Verwaltung oder Wartung“ beschränkt ist und die nur veröffentlichte oder kommerziell erhältliche kryptografische Standards anwenden — fällt ebenfalls nicht unter die Begriffsbestimmung von „Gütern für digitale Überwachung“, doch sollten die Ausführer angesichts verschiedener Berichte über den Missbrauch solcher Güter im Zusammenhang mit Menschenrechtsverletzungen wachsam bleiben.

2.2.1. *Gesichts- und Emotionserkennungstechnologie*

Technologien zur Gesichts- und Emotionserkennung haben neben der digitalen Überwachung vielfältige weitere Verwendungszwecke — z. B. zur Identifizierung oder Authentifizierung — und fallen nicht automatisch unter die Definition. Unter bestimmten Umständen können Technologien zur Gesichts- und Emotionserkennung jedoch in den Anwendungsbereich von Artikel 2 Nummer 20 der Verordnung fallen.

Technologien zur Gesichts- und Emotionserkennung, die verwendet werden können, um gespeicherte Videobilder zu überwachen oder zu analysieren, könnten unter die Bestimmung des Begriffs „Güter für digitale Überwachung" fallen. Doch selbst wenn die oben genannten Kriterien erfüllt sind, muss sorgfältig geprüft werden, ob die Software besonders für verdeckte Überwachung konstruiert ist.

2.2.2. *Ortungsgeräte*

Ortungsgeräte ermöglichen es, den physischen Standort eines Geräts über die Zeit zu verfolgen, und manche Ortungstechnologien werden seit einiger Zeit von Strafverfolgungs- und Nachrichtendiensten eingesetzt. Ihr Potenzial für den Einsatz zur gezielten Überwachung und Massenüberwachung hat sich erheblich weiterentwickelt, da die Tracking-Technologien immer weiter fortgeschritten sind — darunter satellitengestützte Ortung, Ortung über Mobilfunkmasten sowie WLAN- und Bluetooth-Transceiver — und „Ortungsgeräte" wie Smartphones und andere elektronische Geräte (z. B. bordeigene Systeme in Fahrzeugen) inzwischen weitverbreitet sind.

Ortungsgeräte werden beispielsweise von Strafverfolgungs- und Nachrichtendiensten verwendet, um Beweismittel im Laufe einer Ermittlung zu sammeln oder Verdächtige aufzuspüren, aber auch von Unternehmen zu kommerziellen Zwecken, z. B. zur Aufzeichnung von aggregierten Bewegungsmustern in Einkaufsstraßen, zur Ortung von im Außendienst arbeitenden Mitarbeitern oder für standortbezogene Werbung.

2.2.3. *Videoüberwachungssysteme*

Um die Ausführer darin zu unterstützen, potenzielle digitale Überwachung zu erkennen, ist es auch hilfreich klarzustellen, welche Güter nicht unter die Begriffsbestimmung fallen. In diesem Sinne fallen beispielsweise Videoüberwachungssysteme und Kameras — einschließlich hochauflösender Kameras —, die für das Filmen von Menschen im öffentlichen Raum eingesetzt werden, nicht unter die Begriffsbestimmung von Gütern für digitale Überwachung, da sie keine Daten aus Informations- und Telekommunikationssystemen überwachen oder erheben.

3. MAßNAHMEN IM RAHMEN DER SORGFALTSPFLICHT

In Erwägungsgrund 7 der Verordnung heißt es: „Ausführer ... leisten einen entscheidenden Beitrag zum übergeordneten Ziel von Handelskontrollen. Damit sie im Einklang mit dieser Verordnung handeln können, muss als Teil eines internen Programms für rechtskonformes Verhalten („internal compliance programme" — ICP) die Bewertung der Risiken im Zusammenhang mit Transaktionen, die unter diese Verordnung fallen, im Rahmen von transaktionsbezogenen Screening-Maßnahmen, auch bekannt als Grundsatz der Sorgfaltspflicht, durchgeführt werden."

In Artikel 2 Nummer 21 ist der Begriff internes Programm für rechtskonformes Verhalten oder ICP bestimmt als „laufende wirksame, geeignete und verhältnismäßige Strategien und Verfahren, die von Ausführern angenommen werden, um die Einhaltung der Bestimmungen und Ziele dieser Verordnung und der Bedingungen der gemäß dieser Verordnung erteilten Genehmigungen zu fördern, unter anderem Maßnahmen im Rahmen der Sorgfaltspflicht zur Bewertung der Risiken im Zusammenhang mit der Ausfuhr der Güter zu Endverwendern und Endverwendungen".

Die Empfehlung (EU) 2019/1318 der Kommission ([7]) bietet Ausführern einen Orientierungsrahmen, der ihnen helfen soll, Risiken im Zusammenhang mit der Kontrolle des Handels mit Gütern mit doppeltem Verwendungszweck zu ermitteln, zu steuern und zu verringern und die Einhaltung der einschlägigen Rechtsvorschriften der Union und der Mitgliedstaaten zu gewährleisten.

Diese Leitlinien können Ausführer bei der Durchführung von transaktionsbezogenen Screening-Maßnahmen, auch bekannt als Grundsatz der Sorgfaltspflicht, im Rahmen eines ICP unterstützen.

Nach Artikel 5 Absatz 2 der Verordnung (EU) 2021/821 sind Ausführer von nicht gelisteten Gütern für digitale Überwachung verpflichtet, ihrer Sorgfaltspflicht durch transaktionsbezogene Screening-Maßnahmen nachzukommen, d. h. Schritte zur Einstufung von Gütern und zur Bewertung des Risikos einer Transaktion zu unternehmen. In der Praxis sind die Ausführer dazu angehalten, Folgendes zu überprüfen:

([7]) Empfehlung (EU) 2019/1318 der Kommission vom 30. Juli 2019 zu internen Compliance-Programmen für die Kontrolle des Handels mit Gütern mit doppeltem Verwendungszweck (Dual-Use-Gütern) nach Maßgabe der Verordnung (EG) Nr. 428/2009 des Rates (ABl. L 205 vom 5.8.2019, S. 15, ELI: http://data.europa.eu/eli/reco/2019/1318/oj).

3.1. **Überprüfung, ob es sich bei dem zur Ausfuhr vorgesehenen, nicht gelisteten Gut um ein „Gut für digitale Überwachung" handeln könnte, d. h. es besonders konstruiert ist, um die verdeckte Überwachung natürlicher Personen durch Überwachung, Extraktion, Erhebung oder Analyse von Daten aus Informations- und Telekommunikationssystemen zu ermöglichen**

Dieser Schritt bezieht sich auf die Festlegung des Gutes gemäß den Bestimmungen über Güter für digitale Überwachung. Er umfasst eine Prüfung der technischen Merkmale der Güter auf der Grundlage der technischen Parameter, die für die in Anhang I der Verordnung aufgeführten Güter genannt sind, und unter Berücksichtigung der spezifischen Begriffe und Konzepte in der Begriffsbestimmung von Gütern für digitale Überwachung in Bezug auf nicht gelistete Güter sowie die anschließende Einstufung des Gutes (Waren, Technologie oder Software).

3.2. **Überprüfung der Fähigkeiten des betreffenden Gutes, um das Missbrauchspotenzial im Zusammenhang mit interner Repression und/oder der Begehung schwerwiegender Verstöße gegen die Menschenrechte und das humanitäre Völkerrecht durch ausländische Endverwender zu ermitteln**

Ausführer sollten eine Bewertung durchführen, um festzustellen, ob das Produkt zur internen Repression, zur Verletzung oder zum Missbrauch der Menschenrechte — einschließlich des Rechts auf Leben, des Verbots von Folter und unmenschlicher oder erniedrigender Behandlung, des Rechts auf Schutz der Privatsphäre, des Rechts auf freie Meinungsäußerung, der Vereinigungs- und Versammlungsfreiheit, der Gedanken-, Gewissens- und Religionsfreiheit, des Rechts auf Gleichbehandlung oder des Diskriminierungsverbots oder des Rechts auf freie, gleiche und geheime Wahlen — eingesetzt werden könnte.

Dies beinhaltet auch eine Bewertung, ob das Produkt als Teil oder Komponente eines Systems verwendet werden könnte, das zu denselben Verstößen und/oder demselben Missbrauch führen könnte.

Ausführer sollten bei ihrer Bewertung auf Warnsignale (sogenannte „Red Flags") achten, die sich auf ungewöhnliche Umstände einer Transaktion beziehen, welche darauf hindeuten, dass die Ausfuhr für eine Endverwendung, einen Endverwender oder einen Bestimmungsort, die Bedenken aufwerfen, vorgesehen sein könnte.

Warnsignale:

a) Das Produkt wird mit Informationen über seine mögliche Verwendung für verdeckte Überwachung in Verkehr gebracht;

b) Informationen, aus denen hervorgeht, dass ein ähnliches Gut im Zusammenhang mit interner Repression und/oder der Begehung schwerwiegender Verstöße gegen die Menschenrechte und das humanitäre Völkerrecht missbraucht wurde (siehe Abschnitt 1.3);

c) Informationen, aus denen hervorgeht, dass das Gut unrechtmäßig für Überwachungstätigkeiten gegen einen Mitgliedstaat oder im Zusammenhang mit der unrechtmäßigen Überwachung eines EU-Bürgers verwendet wurde;

d) Informationen, aus denen hervorgeht, dass die Transaktion Güter umfasst, die zur Einrichtung, Anpassung oder Konfiguration eines Systems verwendet werden könnten, das bekanntermaßen im Zusammenhang mit interner Repression und/oder schwerwiegenden Verstößen gegen die Menschenrechte und das humanitäre Völkerrecht missbraucht wurde (siehe Abschnitt 1.3);

e) das Gut oder ein ähnliches Gut findet sich auf der Liste, die gemäß Artikel 5 Absatz 6 der Verordnung in Reihe C des *Amtsblatts der Europäischen Union* veröffentlicht wird.

3.3. **Überprüfung — zur Unterstützung der zuständigen Behörden — der an der Transaktion beteiligten Akteure (einschließlich Endverwender und Empfänger wie z. B. Händler und Wiederverkäufer)**

Die Ausführer sollten zur Unterstützung der zuständigen Behörden im Rahmen des Möglichen

a) vor und während einer Transaktion anhand von Endverwendungserklärungen überprüfen, wie die Empfänger und/oder Endverwender das Produkt oder die Dienstleistung nutzen wollen;

b) sich mit der Lage am jeweiligen Bestimmungsort der Güter vertraut machen, insbesondere mit der allgemeinen Menschenrechtssituation, da dies ein wichtiger Indikator für die Gefahr schwerwiegender Verstöße gegen die Menschenrechte und das humanitäre Völkerrecht im Zusammenhang mit Ausfuhren ist;

c) anhand der nachstehend aufgeführten Warnsignale das Risiko bewerten, dass das Produkt oder die Dienstleistung an einen anderen unbefugten Endverwender umgeleitet wird.

Warnsignale:

a) Der Endverwender unterhält offenkundig eine Beziehung zu einer ausländischen Regierung, die nachweislich an internen Repressionen und/oder schwerwiegenden Verstößen gegen die Menschenrechte und das humanitäre Völkerrecht beteiligt ist;

b) der Endverwender ist strukturell Teil der Streitkräfte oder einer anderen an einem bewaffneten Konflikt beteiligten Gruppe, die an internen Repressionsmaßnahmen und/oder schwerwiegenden Verstößen gegen die Menschenrechte und das humanitäre Völkerrecht in der Vergangenheit beteiligt ist;

c) der Endverwender hat in der Vergangenheit Güter für digitale Überwachung in Länder ausgeführt, in denen die Verwendung dieser Güter zu interner Repression und/oder schwerwiegenden Verstößen gegen die Menschenrechte und das humanitäre Völkerrecht geführt hat.

3.4. **Nutzung der im Rahmen der Sorgfaltspflicht erlangten Erkenntnisse, um Pläne zur Vermeidung und Minderung potenzieller künftiger negativer Auswirkungen zu erstellen**

Die Ausführer sollten auf der Grundlage der im Rahmen ihrer Sorgfaltspflicht erlangten Erkenntnisse Tätigkeiten beenden, die negative Auswirkungen im Bereich der Menschenrechte verursachen oder begünstigen, und einen Abhilfemaßnahmenplan ausarbeiten und umsetzen. Die Maßnahmen in diesem Bereich umfassen unter anderem

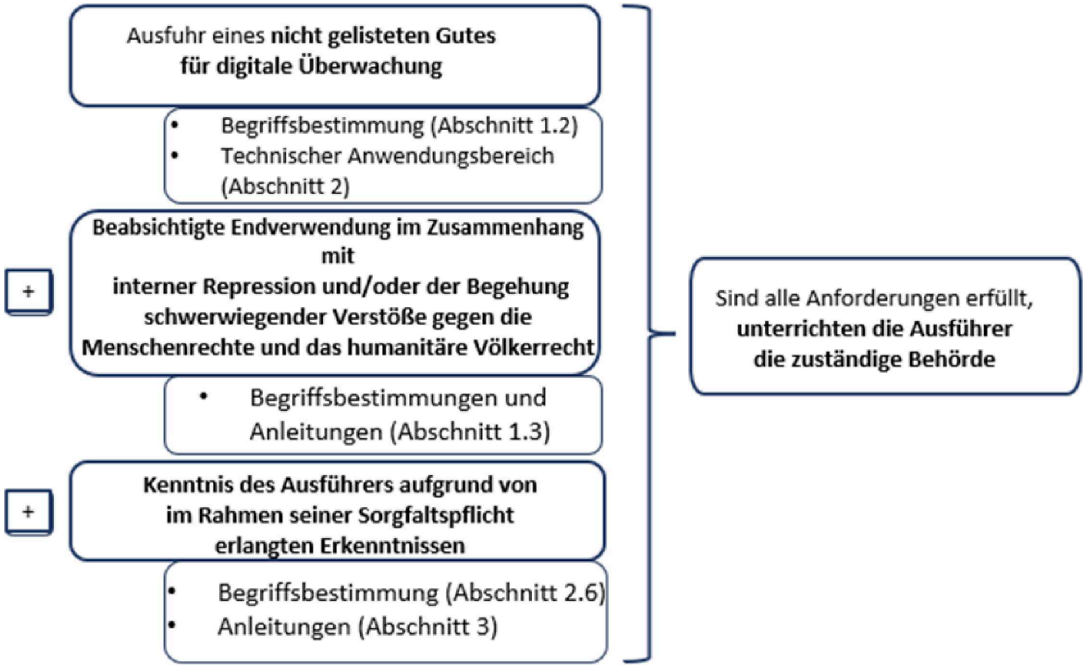
a) Aktualisierung der Strategien des Unternehmens, um Anleitungen zu geben, wie die negativen Auswirkungen in der Zukunft vermieden und angegangen werden können, und deren Umsetzung sicherzustellen;

b) Nutzung der im Rahmen der Risikobewertung erlangten Erkenntnisse, um die Managementsysteme zu aktualisieren und zu stärken, damit Informationen besser verfolgt und Risiken erkannt werden, bevor negative Auswirkungen eintreten;

c) Sammlung von Informationen, um die wichtigsten Risiken negativer Auswirkungen im betreffenden Sektor besser zu verstehen;

d) Unterrichtung der zuständigen Behörden der Mitgliedstaaten über die im Rahmen der Sorgfaltspflicht erlangten Erkenntnisse, um den Informationsfluss in Bezug auf bestimmte Güter, Endverwender und Bestimmungsorte zu erleichtern.

Anforderungen gemäß Artikel 5 Absatz 2 der Verordnung (EU) 2021/821



4. **ANLAGE**

Gelistete Güter für digitale Überwachung, die gemäß Anhang I der Verordnung (EU) 2021/821 Kontrollen unterliegen

— **Systeme für das Abhören von Telekommunikation (5A001f)**

In den meisten Ländern, einschließlich der Mitgliedstaaten, ist die Vertraulichkeit der Kommunikation gesetzlich geschützt, die verdeckte elektronische Überwachung der Kommunikation durch staatliche Behörden kann jedoch in einem rechtlichen Rahmen genehmigt werden (sogenannte rechtmäßige Überwachung — „Lawful Interception" — LI). Mit dem digitalen Zeitalter eröffnete sich jedoch die Möglichkeit, Abhörtechnologien in großem Maßstab einzusetzen. Der Einsatz von Überwachungsinstrumenten durch das libysche Regime hat deutlich gemacht, dass es möglich ist, diese Technologien in großem Maßstab einzusetzen, und führte 2012 zur Einführung von Ausfuhrkontrollen für Systeme für das Abhören von Telekommunikation.

Der Kontrolle unterliegt Ausrüstung, die für die Extraktion des Inhalts einer Nachricht (Sprache oder Daten) sowie von Teilnehmerkennungen oder anderen Metadaten, die über drahtlose Kommunikation übertragen werden, konstruiert ist, sowie Funkfrequenz-Überwachungsausrüstung. Die Kontrolle gilt beispielsweise für IMSI-Catcher (International Mobile Subscriber Identity), die den Mobilfunkverkehr abfangen und die Bewegungen von Mobiltelefonnutzern verfolgen, oder für Geräte, die gefälschte WLAN-Hotspots schaffen, mit denen IMSI-Nummern aus einem Telefon extrahiert werden können, sowie für bestimmte Arten von Gütern, die so besonders konstruiert sind, dass sie eine tiefgreifende Datenpaketanalyse („deep packet inspection") in Telekommunikationssystemen ermöglichen. Ausrüstung zur Störung der mobilen Telekommunikation fällt nicht unter Güter für digitale Überwachung, da keine Daten erfasst werden.

Zwar kann Technologie für allgemeine Anwendungen für den Aufbau solcher Systeme verwendet werden, doch hängen deren Fähigkeiten zum massenhaften Abhören von Kommunikation von spezifischen Teilen und Komponenten ab, einschließlich z. B. spezieller Software und fortgeschrittener oder anwendungsspezifischer integrierter Schaltungen (wie FGPAs, ASICs usw.), um die Anzahl der Pakete oder Kommunikationssitzungen, die pro Sekunde verarbeitet werden können, zu erhöhen.

— **Internet-Überwachungssysteme (5A001j)**

Obwohl ein Großteil der internetgestützten Kommunikation inzwischen standardmäßig verschlüsselt ist, kann das Abfangen von Verkehrsdaten (Metadaten) über die Kommunikation — wie IP-Adressen sowie Häufigkeit und Umfang des Datenaustauschs — noch immer dazu genutzt werden, um Verbindungen zwischen Personen und Domainnamen zu identifizieren. Regierungen können diese Systeme rechtmäßig und unter gerichtlicher Aufsicht für legitime Zwecke nutzen, z. B. zur Identifizierung von Personen, die Domains besuchen, die mit kriminellen oder terroristischen Inhalten in Zusammenhang stehen. Die Überwachung und Analyse des Internetverkehrs auf der Grundlage ethnischer, religiöser, politischer oder sozialer Merkmale kann jedoch zu einer umfassenden menschlichen und sozialen Kartierung eines Landes zum Zweck der Kontrolle und Unterdrückung der Bevölkerung sowie zu anderen Zwecken, z. B. zur Identifizierung politischer Dissidenten, führen. Neben Aspekten im Zusammenhang mit Menschenrechten und interner Repression können diese Güter auch zur Stärkung der sicherheitsbezogenen und militärischen Fähigkeiten beitragen.

Die Kontrolle nach Unternummer 5A001j gilt für Systeme zur Internetüberwachung, die in einem Carrier-Class Internet Protocol Network (z. B. nationales IP-Backbone) ausgeführt werden, um übertragene Metadateninhalte (Sprache, Video, Nachrichten, Anhänge) anhand von „harten Selektoren" zu analysieren, zu extrahieren und zu indexieren und das Beziehungsnetzwerk von Personen abzubilden. Dabei handelt es sich um Güter, die eine „verdeckte Überwachung" durchführen, da den Zielpersonen nicht bekannt ist, dass ihr Kommunikationsverkehr abgefangen wird. Dagegen zielen die Kontrollen nicht auf Systeme ab, in denen Nutzer oder Abonnenten Handlungen oder Interaktionen tätigen, und gelten beispielsweise nicht für soziale Netzwerke oder kommerzielle Suchmaschinen. Kontrollen unterliegen darüber hinaus Systeme, die Daten aus dem Kernnetz eines Internetanbieters verarbeiten, nicht aber soziale Netzwerke oder kommerzielle Suchmaschinen, die von Nutzern bereitgestellte Daten verarbeiten.

— **„Intrusion-Software" (4A005, 4D004 und damit verbundene Kontrollen nach den Unternummern 4E001a und 4E001c)**

Intrusion-Software ermöglicht es ihrem Bediener, verdeckt aus der Ferne auf elektronische Geräte wie Smartphones, Laptop, Server oder ein Gerät des Internets der Dinge zuzugreifen, darauf gespeicherte Daten zu erfassen, die Kommunikation über eine Kamera oder ein Mikrofon, die in dem Gerät eingebaut oder mit ihm verbunden sind, abzufangen und das Gerät als Trittbrett für Angriffe auf andere Geräte, die mit dem Gerät verbunden sind, oder auf Kontakte des Nutzers („Hacking über Geräte Dritter") zu nutzen. Zwar gibt es legitime Verwendungen ([8]) von Intrusion-Software, z. B. „Fernzugriffs-Software", die für die Fernwartung durch IT-Abteilungen verwendet wird, doch der verdeckte Charakter der Überwachung und das Ausmaß der möglicherweise gesammelten Informationen sind mit einem hohen Risiko behaftet, dass das Recht auf Schutz der Privatsphäre und personenbezogener Daten verletzt wird, und können das Recht auf freie Meinungsäußerung ernsthaft untergraben.

([8]) Zur Klarstellung: In Anhang I der Verordnung über Güter mit doppeltem Verwendungszweck aufgeführte Güter für digitale Überwachung benötigen, unabhängig davon, ob die Verwendung des Guts rechtmäßig ist, eine Genehmigung für die Ausfuhr in Drittländer.

Die Kontrolle nach Nummer 4A005 et al. schließt Software sowie Systeme, Ausrüstung, Bestandteile und zugehörige Technologie ein, die besonders für die Generierung und Steuerung oder Lieferung von „Intrusion-Software“ konstruiert oder geändert wurden, gilt jedoch nicht für die eigentliche „Intrusion-Software“, wie in Anhang I der Verordnung definiert. Diese Cyber-Tools werden unter Berücksichtigung ihres Potenzials für Störungen und Schäden kontrolliert, die sie verursachen können, wenn sie erfolgreich eingesetzt und ausgeführt werden; die Kontrollen sollen jedoch nicht die Tätigkeit der Forscher und der Industrie im Bereich der Cybersicherheit beeinträchtigen, da diese Informationen im Zusammenhang mit Intrusion-Software austauschen müssen, um Fehlerkorrekturen für ihre Produkte zu entwickeln und diese vor der öffentlichen Freigabe einer Schwachstelle zu installieren.

— **Kommunikationsüberwachungssoftware (5D001e)**

Diese Software ist für die Überwachung und Analyse von Daten durch ermächtigte Strafverfolgungsbehörden konzipiert, wobei die Daten durch gezielte Abfangmaßnahmen, zu denen ein Kommunikationsdienstleister aufgefordert wird, erhoben werden. Diese Software ermöglicht anhand von „harten Selektoren“ Suchen nach Kommunikationsinhalten oder Metadaten, indem eine Schnittstelle für die rechtmäßige Überwachung genutzt wird und das Beziehungsnetzwerk kartiert oder die Bewegungen von Zielpersonen auf der Grundlage der Suchergebnisse nachverfolgt werden. Die Software ist für die „verdeckte Überwachung“ bestimmt, da sie Daten verwendet, die bei der Überwachung des Kommunikationsverkehrs erhoben werden, ohne dass die Betroffenen davon Kenntnis haben. Darüber hinaus „analysiert“ sie Daten, die über „Telekommunikationssysteme“ erhoben werden. Die Software ist bei der staatlichen Behörde installiert (z. B. in der Überwachungseinrichtung der gesetzlich ermächtigten Behörde (Law Enforcement Monitoring Facility — LEMF)) und die Steuerung erfolgt unabhängig von den Compliance-Systemen für die rechtmäßige Überwachung (Lawful Interception — LI) (z. B. LI-Managementsysteme und Vermittlungsgeräte), die kommerziell entwickelt und beim Kommunikationsdienstleister installiert werden (z. B. integriert in das Kommunikationsnetz) und die der Dienstleister betreibt und instand hält. Wie in der Beschreibung klargestellt, unterliegt „Software“, die für rein kommerzielle Zwecke besonders konstruiert‘ oder geändert wurde, wie z. B. Rechnungsstellung, Dienstgüte des Netzwerks (Quality of Service — QoS), Nutzerzufriedenheit (Quality of Experience — QoE), Vermittlungsgeräte oder mobile Zahlungsdienste oder Bankanwendungen, keinen Kontrollen.

— **Zur Ausführung der Kryptoanalyse verwendete Güter (5A004a)**

Diese Kontrolle erfasst Güter, die zum Brechen kryptografischer Verfahren entwickelt wurden, um vertrauliche Variablen oder sensitive Daten einschließlich Klartext, Passwörter oder kryptografische Schlüssel abzuleiten. Kryptografie wird verwendet, um die Vertraulichkeit von Informationen bei der Übertragung und im Ruhezustand zu wahren. Kryptoanalyse wird dazu verwendet, diese Vertraulichkeit zu brechen, weshalb diese Technologie durch Überwachung, Extraktion, Sammlung oder Analyse von Daten aus Informations- und Telekommunikationssystemen eine verdeckte Überwachung ermöglicht.

— **Forensische Instrumente/Ermittlungsinstrumente (5A004b, 5D002a3b und 5D002c3b)**

Forensische Instrumente/Ermittlungsinstrumente wurden entwickelt, um Rohdaten so aus einem Gerät (z. B. Datenverarbeitung oder Kommunikation) zu extrahieren, dass die Daten für rechtliche Zwecke, d. h. für strafrechtliche Ermittlungen oder Gerichte, verwendet werden können, ohne manipuliert oder verfälscht zu werden. Mit diesen Produkten werden die „Authentifizierung“ oder Autorisierungskontrollen eines Geräts umgangen, sodass die Rohdaten aus dem Gerät extrahiert werden können. Diese Produkte werden von Regierungen und Strafverfolgungsbehörden, aber auch von Streitkräften verwendet, um Daten aus beschlagnahmten Geräten zu extrahieren und zu analysieren. Sie weisen zwar rechtmäßige Verwendungszwecke auf, können jedoch missbraucht werden und stellen somit ein Risiko für sensible oder kommerzielle Daten dar.

Forensische Instrumente/Ermittlungsinstrumente, die nicht für verdeckte Überwachung „besonders konstruiert“ sind, fallen jedoch nicht unter die Begriffsbestimmung von Gütern für digitale Überwachung in Artikel 2 Nummer 20. Außerdem werden forensische Instrumente/Ermittlungsinstrumente, die nur Nutzerdaten extrahieren oder bei denen die Daten auf dem Gerät ungeschützt sind, nicht von der Beschreibung in Unternummer 5A004b et al. erfasst. Gleichzeitig gelten die Kontrollen nicht für Produktions- oder Testausrüstungen des Herstellers, Systemadministratorwerkzeuge oder Produkte, die ausschließlich für den gewerblichen Einzelhandel bestimmt sind, wie z. B. Produkte zur Entsperrung von Mobiltelefonen. In Anbetracht der Vielfalt dieser Technologien hängt die Anwendung von Kontrollen daher von einer Einzelfallbewertung jedes einzelnen Produkts ab.

Abschließend sei darauf hingewiesen, dass andere überwachungsbezogene Güter, die in Anhang I der Verordnung aufgeführt sind, nicht als unter die Begriffsbestimmung von Gütern für digitale Überwachung fallend betrachtet werden sollten, z. B. Ausrüstung für das Stören von mobiler Kommunikation, die konstruiert wurde, um Kommunikation oder Systeme zu schädigen oder zu stören (5A001f), Intrusion-Software, die ein System verändert (4D004), und laser-akustische Detektionsausrüstung (6A005g), die Audiodaten mit einem Laser erfasst oder das Abhören von Gesprächen aus der Ferne ermöglicht (manchmal als „Lasermikrofon“ bezeichnet). Ebenso hätte die Verwendung gelisteter unbemannter Luftfahrzeuge für Überwachungszwecke nicht zur Folge, dass diese Güter unter die Begriffsbestimmung von Gütern für digitale Überwachung fallen.