

Vorschlag COM(2026) 16 vom 21. Januar 2026 für eine **Verordnung über digitale Netze**, zur Änderung der Verordnung (EU) 2015/2120, der Richtlinie 2002/58/EG und der Entscheidung Nr. 676/2002/EG sowie zur Aufhebung der Verordnung (EU) 2018/1971, der Richtlinie (EU) 2018/1972 und des Beschlusses Nr. 243/2012/EU

DIGITAL NETWORKS ACT (DNA) (TEIL 1)

cep**Analyse** Nr. 2/2026

LANGFASSUNG

A.	WESENTLICHE INHALTE DES EU-VORHABENS	2
1	Hintergrund und Ziele	2
2	Regelungssystematik	2
3	Neue Zielsetzungen des DNA	3
4	Neues Verfahren zur Allgemeingenehmigung und neues Passverfahren	4
5	Neuer Rahmen zur Stärkung von Resilienz und Vorsorge des Digitale-Netze-Sektors.....	5
B.	JURISTISCHER UND POLITISCHER KONTEXT	7
1	Stand der Gesetzgebung	7
2	Politische Einflussmöglichkeiten	7
3	Formalien.....	7
C.	BEWERTUNG	7
1	Ökonomische Folgenabschätzung	7
1.1	Regelungssystematik	7
1.2	Neue Zielsetzungen des DNA.....	8
1.3	Neues Verfahren zur Allgemeingenehmigung und neues Passverfahren	9
1.4	Neuer Rahmen zur Stärkung von Resilienz und Vorsorge des Digitale-Netze-Sektors.....	11
2	Juristische Bewertung	14
2.1	Kompetenz.....	14
2.2	Subsidiarität und Verhältnismäßigkeit gegenüber den Mitgliedstaaten	15
2.3	Sonstige Vereinbarkeit mit EU-Recht	15
D.	FAZIT	16

A. Wesentliche Inhalte des EU-Vorhabens

1 Hintergrund und Ziele

- ▶ Laut Kommission ist Konnektivität von entscheidender Bedeutung für die digitale Transformation Europas. Konnektivität lässt sich jedoch nur durch einen modernen und vereinfachten Rechtsrahmen sicherstellen, der z.B. Anreize zur Migration von kupferbasierten Netzen zu Glasfasernetzen und für den Ausbau hochwertiger 5G- und 6G-Netze oder cloudbasierter Infrastrukturen setzt und Größenvorteile über eine grenzüberschreitende Erbringung bzw. Bereitstellung von elektronischen Kommunikationsdiensten bzw. netzen ermöglicht. [S. 1]
- ▶ Die Kommission will mit dem Rechtsakt über digitale Netze (Digital Networks Act, DNA) einen solchen Rechtsrahmen etablieren. Er fußt, neben u.a. den Berichten von Draghi und Letta, auf den folgenden Vorarbeiten [S. 1]:
 - einer [Sondierungskonsultation](#) aus dem Frühjahr 2023 zur Zukunft des elektronischen Kommunikationssektors und seiner Infrastruktur,
 - einem [Weißbuch](#) vom Februar 2025 unter dem Titel „Wie kann der Bedarf an digitaler Infrastruktur in Europa gedeckt werden?“, sowie
 - einer weiteren [Sondierungskonsultation](#) aus dem Sommer 2025 zum avisierten DNA.
- ▶ Der DNA soll insbesondere [S. 1]
 - die Konnektivität fördern,
 - den Binnenmarkt für elektronische Kommunikation stärken,
 - die bestehenden regulatorischen Anforderungen vereinfachen, und
 - zur Erreichung zentraler politischer Ziele – z.B. Verbraucherwohlfahrt, Wettbewerbsfähigkeit, Resilienz, Sicherheit und Nachhaltigkeit – beitragen.
- ▶ Der DNA sieht insbesondere vor
 - eine neue Regelungssystematik durch eine Bündelung von Vorschriften,
 - eine veränderte Austarierung der Regulierungsziele im Konnektivitätssektor,
 - die Neugestaltung des Verfahrens zur Allgemeingenehmigung und die Etablierung eines EU-Passverfahrens,
 - die Etablierung eines Rahmens zur Stärkung von Resilienz und Vorsorge,
 - die Schaffung eines Rahmens für die Migration von Kupfer- zu Glasfasernetzen,
 - die weitgehende Aufrechterhaltung der asymmetrischen und Stärkung der symmetrischen Netzzugangsregulierung,
 - die weitergehende Europäisierung und Harmonisierung sowie Neuaustarierung der Funkfrequenzpolitik,
 - leichte Anpassungen der Vorschriften zur Netzneutralität und zur Dienstqualität,
 - die weitgehende Aufrechterhaltung der Rechte der Endnutzer,
 - die stärkere Vereinheitlichung der Regeln zu Universaldiensten und
 - die Etablierung von Vorgaben zu Kooperationen im digitalen Ökosystem, ohne jedoch „Fair-Share“-Abgaben vorzuschreiben.
- ▶ Diese **cepAnalyse** (Teil 1) beschäftigt sich mit
 - der neuen Regelungssystematik (Abschnitt 2),
 - der Neuaustarierung der Zielsetzungen (Abschnitt 3),
 - der Neugestaltung der Allgemeingenehmigung und der Etablierung eines EU-Passverfahrens (Abschnitt 4), und
 - der Etablierung des Rahmens zur Stärkung von Resilienz und Vorsorge (Abschnitt 5).

2 Regelungssystematik

- ▶ Der DNA ist als Verordnung konzipiert. Er legt Vorschriften für das „Konnektivitäts-Ökosystem“ fest. Dazu bündelt er mehrere bestehende EU-Vorschriften oder Teile davon unter einem Dach und passt diese teilweise an. Das sind [Erwägungsgrund 4]
 - die Richtlinie [\(EU\) 2018/1972](#) über den europäischen Kodex für die elektronische Kommunikation („EKEK“); mit dieser Richtlinie wurde ein harmonisierter Rahmen insbesondere für die Regulierung elektronischer Kommunikationsnetze und elektronischer Kommunikationsdienste errichtet;
 - die Verordnung [\(EU\) 2018/1971](#) zur Einrichtung des Gremiums europäischer Regulierungsstellen für elektronische Kommunikation (GEREK); mit dieser Verordnung wurde das GEREK und die Agentur zur Unterstützung des GEREK („GEREK-Büro“) etabliert;

- der Beschluss [Nr. 243/2012/EU](#) über ein Mehrjahresprogramm für die Funkfrequenzpolitik (RSPP); mit diesem Beschluss wurde ein Mehrjahresprogramm für die Funkfrequenzpolitik festgelegt;
- teilweise die Verordnung [\(EU\) 2015/2120](#) über Maßnahmen zum Zugang zum offenen Internet [...] (OIR); mit dieser Verordnung wurden u.a. Regeln zur Wahrung der gleichberechtigten und nichtdiskriminierenden Behandlung des Verkehrs bei der Bereitstellung von Internetzugangsdiensten festgelegt;
- teilweise die Richtlinie [2002/58/EG](#) über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (ePrivacy-Richtlinie).
- ▶ Ziel dieser Regelungssystematik und des Rückgriffs auf eine Verordnung für den DNA ist es [S. 7 und 8]
 - die bestehenden Vorschriften zu vereinfachen und besser aufeinander abzustimmen,
 - die bestehenden Binnenmarkthindernisse zu beseitigen,
 - zusätzliche Vorschriften auf nationaler Ebene (Gold-Plating) zu verhindern,
 - einen Flickenteppich an unterschiedlichen nationalen Vorschriften zu vermeiden, um so z.B. die Skalierung innovativer grenzüberschreitender Dienste zu erleichtern und Skaleneffekte besser zu nutzen.

3 Neue Zielsetzungen des DNA

- ▶ Status quo: Der noch geltende EKEK zielt insbesondere darauf ab [Art. 1 und 3, EKEK],
 - einen Binnenmarkt für elektronische Kommunikationsnetze und -dienste zu errichten,
 - die Konnektivität zu fördern,
 - den Ausbau und die Nutzung von „Netzen mit sehr hoher Kapazität“ zu unterstützen,
 - einen nachhaltigen Wettbewerb bei der Bereitstellung elektronischer Kommunikationsnetze und -dienste zu fördern,
 - die Interoperabilität elektronischer Kommunikationsdienste sicherzustellen,
 - die Sicherheit von Netzen und Diensten zu gewährleisten, und
 - die Interessen der Endnutzer zu wahren.
- ▶ Die Kommission will nun den Katalog an Zielen erweitern [S. 8]. Der Rechtsrahmen zielt künftig zusätzlich darauf ab
 - die Wettbewerbsfähigkeit des gesamten Konnektivitätssektors – d.h. Unternehmen des TK-Sektors sowie Unternehmen im digitalen Ökosystem – zu unterstützen [Erwägungsgrund 16 und Art. 3 Abs. 1 lit. a],
 - den Ausbau transeuropäischer digitaler Netze sowie die Bereitstellung europaweiter Satellitenkommunikationsdienste zu unterstützen [Erwägungsgrund 17 und Art. 3 Abs. 1 lit. b],
 - die Resilienz und Widerstandsfähigkeit von elektronischen Kommunikationsnetzen und -diensten zu stärken, um besser gegen Naturkatastrophen, von Menschen verursachte Bedrohungen und Krisen – z.B. Cyberattacken und hybride Angriffe – sowie Störungen von Netzwerken und Funksignalen gewappnet zu sein [Erwägungsgrund 18 und Art. 3 Abs. 1 lit. c],
 - die Nachhaltigkeit zu fördern, etwa durch Unterstützung von Investitionen in energieeffiziente und digitale Netze und Lösungen; dies sollte in Einklang stehen mit [Erwägungsgrund 23 und Art. 3 Abs. 1 lit. g]
 - dem EU-Regelwerk zur grünen Taxonomie [s. [hier](#)] und
 - dem Verhaltenskodex der Union für die Nachhaltigkeit von Telekommunikationsnetzen (s. [hier](#)).
- ▶ Der Rechtsrahmen zielt künftig darauf ab, die „breite Verfügbarkeit, den Zugang zu und die Nutzung von Gigabit-Netzen“ zu fördern, statt nur den „Zugang zu und die Nutzung von Netzen mit sehr hoher Kapazität“. Damit stellt er nun vordergründig auf elektronische Kommunikationsnetze ab, die [Erwägungsgrund 8, Art. 2 Ziff. 2 und 12, Art. 3 Abs. 1 lit. d]
 - „bis zum Netzabschlusspunkt“ vollständig aus Glasfaserelementen bestehen, d.h. bis zur Teilnehmeranschlussdose beim Endkunden („Fibre to the home, FTTH“), statt nur „bis zum Verteilerpunkt am Ort der Nutzung“, und
 - in der Lage sind, Datenraten von mindestens einem Gigabit pro Sekunde im Uplink und Downlink bereitzustellen.
- ▶ Eine Priorisierung der Ziele des Rechtsrahmens findet nicht statt, d. h. sie haben alle den gleichen Stellenwert. Im Rahmen ihrer jeweiligen Zuständigkeiten müssen sich die folgenden Akteure an den Zielen orientieren [Art. 3 Abs. 1]:
 - die Mitgliedstaaten,
 - die nationalen Regulierungsbehörden („NRBs“),
 - die anderen zuständigen nationalen Behörden,
 - das Gremium europäischer Regulierungsstellen für elektronische Kommunikation („GEREK“),
 - das Büro für Digitale Netze (Office for Digital Networks („ODN“), bisher: GEREK-Büro),
 - das Radio Spectrum Policy Body (RSPB, bisher: Radio Spectrum Policy Group (RSPG)), und
 - die Kommission.

- ▶ Die genannten Akteure müssen in ihrer Arbeit unparteiisch, objektiv, transparent, diskriminierungsfrei und verhältnismäßig handeln und beispielsweise darauf achten, dass sie den regulatorischen und administrativen Aufwand, der durch Regulierungsentscheidungen entsteht, so weit wie möglich begrenzen [Art. 3 Abs. 2].

4 Neues Verfahren zur Allgemeingenehmigung und neues Passverfahren

- ▶ Status quo: Bereits nach dem geltenden EKEK gibt es ein Verfahren für die Allgemeingenehmigung zur Bereitstellung von elektronischen Kommunikationsnetzen und -diensten. Diese basiert auf einer harmonisierten, aber maximalen Liste von Genehmigungsbedingungen. Die Mitgliedstaaten können flexibel bestimmen, [Erwägungsgrund 40, sowie Art. 12 EKEK]
 - welche der in der Liste aufgeführten Bedingungen auf ihrem Hoheitsgebiet erfüllt werden müssen,
 - wie sie diese auf nationaler Ebene weiter präzisieren, und
 - ob sie von den Anbietern vor der Bereitstellung der Netze bzw. Dienste eine deklaratorische Notifizierung verlangen.
- ▶ Laut Kommission führt dieser Ansatz dazu, dass Netzbetreiber, die in allen EU-Mitgliedstaaten tätig sind, zumindest potenziell „bis zu 1053“ nationale Auflagen erfüllen müssen [SWD(2026) 13, Part 1/3, S. 51].
- ▶ Der DNA etabliert nun ein stärker harmonisiertes Verfahren zur Allgemeingenehmigung der Bereitstellung von elektronischen Kommunikationsnetzen und -diensten [Art. 9]. Das Verfahren gilt für [Erwägungsgründe 42 und 43, Art. 9 Abs. 2 und 3]
 - Anbieter von öffentlichen elektronischen Kommunikationsdiensten (z.B. TK-Unternehmen, Internetzugangsanbieter), und
 - Anbieter von elektronischen Kommunikationsnetzen, sofern diese „ganz oder überwiegend“ der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder Dienste der Informationsgesellschaft dienen (z.B. Betreiber von Glasfaser oder Mobilfunknetzen).

Es gilt künftig für „alle Arten von elektronischen Kommunikationsnetzen“, die an der Bereitstellung öffentlich zugänglicher digitaler Dienste beteiligt sind [Erwägungsgrund 42].
- ▶ Das Verfahren gilt insbesondere nicht für Anbieter von [Erwägungsgründe 42, 43 und 45, Art. 9 Abs. 2 und 3, Art. 38 Abs. 2]
 - elektronischen Kommunikationsnetzen, die hauptsächlich für eine private, interne oder geschlossene, vorab festgelegte Benutzergruppen-Kommunikation genutzt werden,
 - nummernunabhängigen interpersonellen Kommunikationsdiensten (z.B. WhatsApp),
 - Satellitennetzen und Satellitenkommunikationsdiensten.
- ▶ Die Anbieter von elektronischen Kommunikationsnetzen und -diensten dürfen die Netze bzw. Dienste grundsätzlich in der gesamten EU bereitstellen. Die Mitgliedstaaten können diese Freiheit nur begründet und zur Wahrung der öffentlichen Ordnung, Sicherheit oder Gesundheit einschränken. [Art. 9 Abs. 1]
- ▶ Das Recht elektronische Kommunikationsnetze und -dienste erbringen zu dürfen, ist – im Rahmen einer Allgemeingenehmigung – abhängig von der Erfüllung einiger Bedingungen. So müssen die Anbieter, soweit für sie jeweils relevant, u.a. [Art. 9 Abs. 4]
 - die neu im DNA verankerten Vorgaben zur Wahrung der Resilienz und Vorsorge (s. Abschnitt 5) einhalten,
 - die neu im DNA verankerten Anforderungen zur Einhaltung von Bedingungen zur Nutzung von kritischen Kommunikationsdiensten bei Katastrophen größeren Ausmaßes oder nationalen Notfällen erfüllen,
 - Strafverfolgungs- und Justizbehörden den Zugang zu Daten ermöglichen, etwa zur legalen Überwachung von Telekommunikationsverbindungen sowie zur Vorratsdatenspeicherung; die diesbezüglichen Anforderungen können aus harmonisiertem EU-Recht oder nicht harmonisiertem nationalen Recht rühren,
 - die Integrität öffentlicher elektronischer Kommunikationsnetze wahren, etwa indem sie elektromagnetische Störungen zwischen Kommunikationsnetzen oder -diensten verhindern,
 - die im DNA verankerten Maßnahmen zur Zusammenschaltung ergreifen, und
 - Cybersicherheitsvorgaben einhalten.
- ▶ Die Einhaltung von Cybersicherheitsvorgaben umfasst auch die im Rahmen der Revision des Rechtsakts zur Cybersicherheit (Cyber Security Act 2, s. [COM\(2026\) 11](#)) vorgeschlagenen Regeln zur Sicherheit der IKT-Lieferkette. Dies bedeutet u.a., dass Unternehmen, die um eine Allgemeingenehmigung ersuchen, bestimmte IKT-Komponenten von Anbietern mit hohem Risiko nicht mehr nutzen dürfen.
- ▶ Die im DNA verankerte Liste an Bedingungen gilt dabei als abschließend. Die Mitgliedstaaten dürfen keine zusätzlichen Bedingungen festlegen. Die Anzahl an Bedingungen ist geringer als nach dem geltenden EKEK. [Erwägungsgrund 44, Art. 9 Abs. 4]

- ▶ Das GEREK veröffentlicht spätestens sechs Monate nach Inkrafttreten des DNA Leitlinien zu den Bedingungen, um eine kohärente, nichtdiskriminierende und verhältnismäßige Anwendung sicherzustellen [Art. 11 Abs. 1].
- ▶ Anbieter elektronischer Kommunikationsnetze oder -dienste, die Netze oder Dienste in einem oder mehreren Mitgliedstaaten bereitstellen wollen, müssen dies bei einer NRB eines dieser Mitgliedstaaten notifizieren, und zwar im Rahmen eines „einheitlichen Pass“-Verfahrens [Art. 10 Abs. 1]. Hierfür müssen sie ein Notifizierungsformular nutzen, welches das GEREK bereitstellt [Art. 10 Abs. 3].
- ▶ NRBs müssen auch Online-Notifizierungen ermöglichen. Falls vorgeschrieben, sollte dies auch über harmonisierte digitale Lösungen wie etwa europäische Unternehmensbrieftaschen („European Business Wallets“, s. [COM\(2025\) 838](#)) möglich sein. [Erwägungsgrund 49]
- ▶ Anbieter, die ihre Netze oder Dienste zu einem Zeitpunkt vor sechs Monate nach Inkrafttreten des DNA bereits notifiziert haben, benötigen keine erneute Notifizierung [Art. 10 Abs. 9].
- ▶ Die NRB, bei der die Notifizierung eingeht, informiert das ODN. Das ODN informiert ggf. andere zuständige Behörden, in denen der Anbieter ebenfalls tätig werden will. [Art. 10 Abs. 4]
- ▶ Der Anbieter elektronischer Kommunikationsnetze oder -dienste kann die aus einer Allgemeingenehmigung abgeleiteten Rechte ausüben, ohne dass es hierfür einer Entscheidung oder eines Verwaltungsakts der notifizierten Behörde bedarf [Art. 10 Abs. 2]. Die Behörde muss dem Anbieter nur binnen einer Woche nach Notifizierung bestätigen, dass er die Rechte ausüben kann. Sobald die Bestätigung vorliegt, kann der Anbieter die Tätigkeit aufnehmen. [Art. 10 Abs. 6 und 7]
- ▶ Die notifizierte NRB kann bei Verstößen gegen die Genehmigungsbedingungen Sanktionen verhängen. Bei schwerwiegenden Verstößen kann sie auch die Betriebsgenehmigung entziehen, und zwar ggf. auch in den Mitgliedstaaten, für die der einheitliche Pass gilt. Ist eine andere, nicht-notifizierte NRB der Auffassung, dass ein Verstoß gegen die Genehmigungsbedingungen „schwerwiegende negative Auswirkungen“ aus Gründen der nationalen Sicherheit oder des öffentlichen Interesses in ihrem Hoheitsgebiet haben könnte, kann auch sie ggf. Sanktionen verhängen. [Art. 11 Abs. 4 und 5]

5 Neuer Rahmen zur Stärkung von Resilienz und Vorsorge des Digitale-Netze-Sektors

- ▶ Der DNA etabliert – zur Stärkung der strategischen Autonomie der EU und der Reaktionsfähigkeit der Gesellschaft auf Krisen – einen neuen sektorspezifischen Rahmen zur Stärkung der Resilienz und zur Abwehrbereitschaft von elektronischen Kommunikationsnetzen und -diensten und anderen digitalen Infrastrukturen gegenüber natürlichen oder von Menschen verursachten Störungen, Krisen oder Fällen höherer Gewalt, die sich negativ auf die Bevölkerung auswirken oder die Funktionsfähigkeit des Binnenmarkts beeinträchtigen können [Erwägungsgrund 18, Teil II].
- ▶ Das GEREK erstellt zu dem Rahmen einen „Unionsvorsorgeplan für digitale Infrastrukturen“ und verabschiedet diesen spätestens ein Jahr nach Inkrafttreten des DNA. Der Plan enthält u.a. [Art. 6 Abs. 1 und 2]
 - eine Bewertung der Architekturen, Kapazitäten, Fähigkeiten und der Nutzung der Netze, inklusive der Analyse u.a. von potenziellen Engpässen oder Ausfallpunkten, wobei die bereitgestellten Informationen keine Geolokalisierung sensibler Anlagen ermöglichen soll,
 - operative Empfehlungen zur Wahrung der Netzausfallsicherheit, etwa in Situationen erhöhter Nachfrage, Netzüberlastung oder bei natürlichen oder vom Menschen verursachten (vorsätzlichen schädlichen) Störungen, sowie
 - Verfahren zum Krisenmanagement; das umfasst u.a. Koordinierungsvereinbarungen und operative Protokolle, die von den NRBs und anderen zuständigen Behörden im Krisenfall anzuwenden sind.
 Der Plan soll zu einem EU-weit einheitlichen Ansatz für die Stärkung der Resilienz beitragen, u.a. internationale Verbindungen, Aggregationsnetze, Kern- und Backbone-Netze, Unterseekabel, Content-Delivery-Networks berücksichtigen und auch „Finanzierungsmechanismen“ miteinbeziehen [Erwägungsgründe 32 und 33].
- ▶ Der Plan wird vom „Office for Digital Networks, ODN“ (ehemals „GEREK Office“) für das GEREK entworfen. Das ODN soll zur Stärkung der Resilienz des Sektors eine „zentrale Koordinierungsrolle“ übernehmen. Es wird dabei unterstützt von [Erwägungsgrund 26, Art. 7 Abs. 1]
 - der Kommission,
 - der „Kooperationsgruppe“; d.h. einem Gremium aus Vertretern der Mitgliedstaaten, der Kommission und der ENISA, welches die Zusammenarbeit und den Informationsaustausch zwischen den Mitgliedstaaten zur Wahrung eines hohen Cybersicherheitsniveau unterstützen soll,
 - ggf. der ENISA und Krisenreaktions- und Katastrophenschutzkoordinierungsbehörden, und
 - falls angemessen, von internationalen Organisationen (z.B. NATO).

- ▶ Das ODN muss die bestehenden Rollen dieser Einrichtungen „uneingeschränkt“ achten. Zudem muss es sich konzentrieren auf [Erwägungsgrund 26 und 27]
 - die systemweite Vorsorge,
 - die Interoperabilität der digitalen Infrastrukturen,
 - die Kontinuität der transeuropäischen Netze und Dienste und
 - die koordinierte Krisenreaktion.
- ▶ Die NRBs müssen zur Unterstützung der Ausarbeitung des Plans alle zwei Jahre Informationen erheben zu den Architekturen, Kapazitäten, Fähigkeiten und zur Nutzung von [Art. 7 Abs. 2]
 - öffentlichen elektronischen Kommunikationsnetzen,
 - öffentlich zugänglichen elektronischen Kommunikationsdiensten und,
 - ggf. von Netzen, die ganz oder überwiegend für die Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder Dienste der Informationsgesellschaft genutzt werden.

Jede Erhebung muss sich auf das unbedingt erforderliche Maß beschränken und ist hinfällig, wenn die Informationen bereits anderweitig bereitgestellt wurden [Art. 7 Abs. 2 und 3].
- ▶ Die Anbieter von elektronischen Kommunikationsnetzen oder -diensten müssen einen Beitrag zur Antizipation, Prävention, Vorsorge und Bewältigung der genannten Störungen, Krisen oder Fällen höherer Gewalt, die sich negativ auf die Bevölkerung auswirken können, leisten. Diesen Beitrag müssen sie leisten [Art. 4]
 - im Rahmen ihrer Zuständigkeiten,
 - gemeinsam mit (a) dem GEREK, (b) dem ODN, (c) den NRBs, (d) den nationalen Cybersicherheitsbehörden und (e) den nationalen Krisenmanagement- und Katastrophenschutzbehörden, und
 - durch die Erfüllung der im DNA verankerten Verpflichtungen.
- ▶ Die genannten Anbieter, Gremien und Behörden müssen zusammenarbeiten, um sicherzustellen, dass [Art. 5 Abs. 1]
 - elektronische Kommunikationsnetze und -dienste kontinuierlich verfügbar sind, und
 - es keine Fähigkeitslücke im Hinblick auf die Vorhersage, Prävention und Bewältigung der genannten Störungen, Krisen oder Fälle höherer Gewalt gibt.

Sie müssen hierfür den oben genannten Plan der GEREK weitestgehend berücksichtigen [Art. 5 Abs. 1].
- ▶ Die genannten Anbieter sowie Notrufabfragestellen („PSAPs“) müssen bei Auftreten der genannten Störungen, Krisen oder Fälle höherer Gewalt sicherstellen [Art. 5 Abs. 2]
 - die ununterbrochene Verfügbarkeit kritischer Kommunikationsdienste und Notrufe, und
 - die ununterbrochene Übermittlung öffentlicher Warnungen.

Sie müssen hierfür den Plan der GEREK berücksichtigen [Art. 5 Abs. 2].
- ▶ Die Anbieter von öffentlichen elektronischen Kommunikationsnetzen und von öffentlich zugänglichen elektronischen Kommunikationsdiensten sowie von PSAPs müssen die Verfügbarkeit von Notruf- und öffentlichen Warnsystemen auch dann gewährleisten, wenn sie neue Technologien implementieren [Art. 5 Abs. 2]. Die beiden erstgenannten Anbieter müssen zudem u.a. die Endnutzer darüber informieren, wenn eine Migration zu einer neuen Netzwerktechnologie zur Einstellung von Diensten auf den Endgeräten der Nutzer führen wird. Sie müssen dies mindestens zwei Jahre im Voraus „durch Vorlage eines Fahrplans, der den Migrationsprozess widerspiegelt“ tun. [Art. 5 Abs. 4]
- ▶ Die Kommission drängt, zur Stärkung der Resilienz, zudem auf [Erwägungsgründe 31 und 35]
 - die Einführung von Technologien wie der sich entwickelnden Quantenkommunikationstechnologien, wobei sie den „Übergang zur Post-Quanten-Kryptografie“ für erforderlich hält,
 - den Rückgriff auf „spezialisierte Dienste“ für Anwendungsfälle mit erhöhten Anforderungen an Sicherheit, Zuverlässigkeit und Latenz; hier nennt sie u.a. den Betrieb unbemannter Flugsysteme (z.B. Drohnen), und
 - die schrittweise Weiterentwicklung der „zellulare[n] Sensorik“ als ergänzendes Erkennungssystem für zivile und militärische Anwendungen.

B. Juristischer und politischer Kontext

1 Stand der Gesetzgebung

21.01.26 Annahme durch Kommission

Offen Annahme durch Europäisches Parlament und Rat, Veröffentlichung im Amtsblatt, Inkrafttreten

2 Politische Einflussmöglichkeiten

Generaldirektionen: GD Kommunikationsnetze, Inhalte und Technologien

Ausschüsse des Europäischen Parlaments: Industrie, Forschung und Energie (ITRE), Berichterstatter: Michał Andrzej Kobosko (Renew Europe, Polen)

Bundesministerien: Digitales und Staatsmodernisierung (federführend)

Ausschüsse des Deutschen Bundestags: Digitales und Staatsmodernisierung (federführend)

Entscheidungsmodus im Rat: Qualifizierte Mehrheit (Annahme durch 55% der Mitgliedstaaten, die 65% der EU-Bevölkerung ausmachen)

3 Formalien

Kompetenznorm: Art. 114 AEUV (Binnenmarkt)

Art der Gesetzgebungszuständigkeit: Geteilte Zuständigkeit (Art. 4 Abs. 2 AEUV)

Verfahrensart: Art. 294 AEUV (ordentliches Gesetzgebungsverfahren)

C. Bewertung

1 Ökonomische Folgenabschätzung

1.1 Regelungssystematik

Die Etablierung des DNA als EU-Verordnung, die keiner nationalen Umsetzung bedarf und mehrere bestehende EU-Rechtsakte in einem Rechtsakt bündelt, ist aus mehreren Gründen sachgerecht. Denn sie ermöglicht eine bessere Verzahnung von eng verwandten Vorschriften, was die Rechtssicherheit fördert, die Rechtskonsistenz stärkt und die Rechtsanwendung vereinfacht. Ferner erschwert bzw. verunmöglicht die Regelungssystematik schädliches Gold-Plating-Verhalten der Mitgliedstaaten, das regelmäßig für hohen Aufwände und Kosten sorgt, insbesondere für Marktteilnehmer, die grenzüberschreitend tätig sind oder sein wollen. Dass der DNA als Verordnung konzipiert ist, ist mithin ein wichtiger Beitrag zur Vertiefung bzw. Vollendung des digitalen Binnenmarkts und eine wichtige Basis u.a. für einen Ausbau grenzüberschreitender Tätigkeiten und die Erzielung von Skaleneffekten. Auch die regelmäßigen Verzögerungen, die bei der Umsetzung des EKEK durch zahlreiche Mitgliedstaaten zu beobachten waren, und so für mangelnde Planungssicherheit gesorgt haben, sprechen für ein einheitliches Regelwerk, welches für alle Mitgliedstaaten zu einem einheitlichen Datum Anwendung findet.

Ungeachtet der grundsätzlichen Zustimmung zu der neuen Regelungssystematik sei dennoch auf einige Fallstricke, insbesondere mit Blick auf die Bündelung von Rechtsakten, hingewiesen. Erstens ist mit dieser noch nicht viel gewonnen, wenn sich die hinter den Rechtsakten stehenden Vorschriften nicht gleichzeitig wandeln und an die heutigen Notwendigkeiten – etwa mit Blick auf eine Vereinfachung der Regulierung – angepasst werden.¹ Letztlich sollte auch ein gebündelter Rechtsakt – wie der DNA – nur jene Vorschriften enthalten, die künftig tatsächlich erforderlich und zweckmäßig sind.² Zweitens birgt die Strategie der Bündelung einige politökonomische Risiken. Denn wenn im Gesetzgebungsverfahren nun über eine größere Anzahl von verschiedenen Regelungsbereichen verhandelt werden muss, schafft dies zusätzlichen Raum für im Zweifel wenig sachdienliche

¹ Auch nach der vermeintlichen Vereinfachung hat der DNA stolze 343 Seiten in der englischen Fassung und besteht aus 416 Erwägungsgründen und 210 Artikeln.

² Ob eine solche Anpassung stattfindet, wird in weiteren Abschnitten und cepAnalysen zum DNA ausgeführt.

Paketlösungen. Und drittens bedeutet ein umfangreicheres Regelwerk für den TK- und Digitalsektor, dass künftig gezielte Anpassungen, die nur einen kleinen Teil des Regelwerks betreffen würden, – auch wenn sie aufgrund des grundsätzlich dynamischen Charakters der Digitale-Netze-Sektor geboten erscheinen – schwerer würden. Denn jede Öffnung des DNA an einer oder wenigen Stellen würde sogleich die Tür auch für Änderungen an anderen Stellen öffnen, und so das hohe Gut der regulatorischen Stabilität gefährden und damit eine wichtige Voraussetzung für Investitions- und Innovationsaktivitäten.

Die Einschränkung der mitgliedstaatlichen Spielräume ist erklärtes Ziel jeder Verordnung, und dieser Weg ist prinzipiell auch der Richtige. Dennoch erscheint es geboten, innerhalb des DNA noch stärker zu konkretisieren, welche Vorgaben als abschließend bzw. vollharmonisiert gelten und bei welchem Sachverhalten noch Raum für eigenständige mitgliedstaatliche Politiken verbleiben sollen. So dürfte es mit Blick auf einzelne Regelungsbereiche – auch wenn dies dem Binnenmarktgedanken widersprechen mag – auch künftig notwendig sein, nationale Besonderheiten aufgrund unterschiedlicher Marktgegebenheiten zu berücksichtigen. So sollte z.B. ein EU-Regime zur Kupfer-Glas-Migration³ auch künftig Spielräume bei den Mitgliedstaaten und den NRBs belassen, da die Ausgangslagen zwischen und innerhalb der Mitgliedstaaten sehr verschieden sind und eine uneinheitliche Herangehensweise daher auch sachdienlich sein kann.

1.2 Neue Zielsetzungen des DNA

Mit der Erweiterung des Katalogs an Zielen, die der DNA – als neuer EU-Rechtsrahmen für den TK-Sektor sowie teilweise für das weitere digitale Netze-Ökosystem – im Vergleich zum bestehenden Recht verfolgen will, reagiert die Kommission auf neue geo- und sicherheitspolitische Herausforderungen und auf die breite Erwartung, Fortschritte bei der digitalen Transformation und dem Übergang zu einer nachhaltigen Wirtschaft erzielen zu wollen. So soll ein breiter Kreis an Akteuren, von den NRBs über das GEREK bis hin zur EU-Kommission in ihrem jeweiligen (Aufsichts-)Handeln nun – zusätzlich zu einem bereits umfangreichen Kreis an Zielen – auch auf die Stärkung der Wettbewerbsfähigkeit, die Förderung von Resilienz und Widerstandsfähigkeit und auf die Förderung nachhaltiger TK-Netze achten.

Doch auch wenn die Zieleerweiterung zunächst nachvollziehbar und als politisch opportun erscheint, ist sie verfehlt. Erstens führt die Vielzahl von Zielen zu einer relativen Entwertung der einzelnen Ziele, insbesondere da keine Hierarchisierung der Ziele vorgesehen ist. Diese Entwertung führt dazu, dass bestimmte Ziele, die bisher als maßgeblich betrachtet wurden und diesen Status auch künftig haben sollten – insbesondere die Förderung eines nachhaltigen Wettbewerbs oder der Rechte der Endnutzer – an Gewicht verlieren werden. Werden zu viele Ziele verfolgt, wird am Ende keines mehr verfolgt. Zweitens besteht die Gefahr, dass verstärkt aus industriepolitisch motivierten Gründen in Marktprozesse eingegriffen und so Wettbewerbsverzerrungen Vorschub geleistet wird. Drittens werden, über die auch im bisherigen Rechtsrahmen bestehenden Zielkonflikte hinaus, noch weitere solcher Konflikte geschaffen. So könnten NRBs künftig beispielsweise aus Gründen der Unterstützung der Wettbewerbsfähigkeit der Digital-Netze-Wirtschaft von einer Netzzugangsregulierung absehen, obgleich sie aus reinen Wettbewerbsgesichtspunkten (noch) geboten wäre. Auch könnten Maßnahmen und Entscheidungen zur Stärkung von Resilienz und Vorsorge mit den Nachhaltigkeitszielen nicht in Einklang zu bringen sein. Wie die involvierten Akteure in diesen Fällen eine adäquate Abwägung vornehmen sollen, bleibt offen. Viertens steht der umfangreiche Zielkatalog für eine Erhöhung der Regulierungskomplexität. So müssen etwa die Kommission und die NRBs bei anstehenden Entscheidungen über Netzzugangsverpflichtungen zusätzliche Aspekte berücksichtigen, was nicht nur den Entscheidungsprozess verlangsamen, sondern auch zu neuen administrativen Aufwänden führen dürfte. Die Vorhersehbarkeit der Regulierung bzw. von behördlichem Handeln in der Praxis, würde leiden und die Rechtssicherheit schwächen, was mittelbar auch die Investitionsbereitschaft ausbremsen, statt anregen könnte. Die Zieleaufstockung steht somit auch der sonstigen Agenda der Kommission zur Vereinfachung von EU-Regulierung entgegen. Fünftens sollte beachtet werden, dass ein nachhaltiger Wettbewerb in der Regel eine Quelle von Wettbewerbsfähigkeit darstellt und letzteres mithin durch ersteres bereits unterstützt wird. Denn Wettbewerb gilt als treibende Kraft für Effizienz, Innovation, Wachstum und die Förderung der Verbraucherwohlfahrt, und Branchen, die einem intensiveren Wettbewerb ausgesetzt sind, verzeichnen üblicherweise auch ein stärkeres Produktivitätswachstum⁴. Sechstens ist fraglich, ob alle Ziele – bestehende und neue –

³ In dieser cepAnalyse wird nicht spezifisch auf die neuen Vorgaben zur Kupfer-Glas-Migration eingegangen. Dies soll in einer weiteren cepAnalyse erfolgen.

⁴ S. dazu auch: European Central Bank (2024), Competition policy in a changing world, Speech by Christine Lagarde, President of the ECB, at an event to mark the 15th anniversary of the Autorité de la concurrence Paris, 5 November 2024, und EU Commission (2024), Protecting competition in a changing world: Evidence on the evolution of competition in the EU during the past 25 years, Publications Office of the European Union, 2024.

im Hinblick auf die Vielzahl an Regelungsbereichen, die der DNA künftig abdecken soll – Resilienzrahmen, Kupfer-Glas-Migration, Netzzugangsregulierung, Funkfrequenzpolitik, Netzneutralität, Kooperationen im digitalen Ökosystem etc. – immer denselben Stellenwert haben sollten. Wie nun vorgesehen, ist weder eine Hierarchisierung der Ziele avisiert, noch sollen bestimmte Ziele für einzelne Regelungsbereiche keine oder nur eine untergeordnete Rolle spielen. Für eine effiziente Politik sollten die prioritären Ziele jedoch jeweils klar benannt werden – und zwar für jeden dieser Regelungsbereiche einzeln.⁵ Ein überlegenswerter Ansatz zur Zielfestlegung wäre jener, der in der Verordnung zur grünen Taxonomie Anwendung findet⁶. Dabei würden für die Regelungsbereiche des DNA jeweils primäre Ziele festgelegt, zu denen Maßnahmen und Entscheidungen im Rahmen der Anwendung der Verordnung einen wesentlichen Beitrag leisten müssen, wobei diese Maßnahmen gleichzeitig nicht zu einer (erheblichen) Beeinträchtigung anderer eher sekundärer Ziele führen dürften.

Verfehlt sind darüber hinaus, auch die Anpassungen mit Blick auf das Ziel der Förderung der Verfügbarkeit von, dem Zugang zu und der Nutzung von bestimmten TK-Netzen. Bereits der EKEK sah hier eine Bevorzugung von „Netzen von hoher Kapazität“ vor. Nun sollen explizit solche Netze in den Vordergrund gerückt werden, die zu den „Gigabit-Netzen“ zählen und die bis zum Netzabschlusspunkt vollständig aus Glasfaserelementen bestehen (FTTH-Netze). Gerade auf den Ausbau und die Nutzung solcher FTTH-Netze soll der Fokus gerichtet werden. Es ist jedoch nicht Aufgabe der Politik bzw. von (Regulierungs-)Behörden darüber zu entscheiden, welche Netztechnologie heute und in Zukunft die vermeintlich beste und unterstützungswürdigste Technologie darstellt. Darüber sollten die Marktakteure ein eigenständiges Urteil fällen. Gibt es im Markt eine Präferenz für FTTH-Netze werden diese sich auch regelmäßig durchsetzen. Das Postulat der Kommission, wonach FTTH die „zukunftssicherste Lösung“ sei⁷, ist jedenfalls eine Anmaßung von Wissen und ihre explizite Bevorzugung ein Bruch mit dem Primat der Technologieneutralität. Unabhängig von der Frage der „idealen“ Technologie, ist auch der Eingriff in die Souveränität der Verbraucher fragwürdig. Dieser weist paternalistische Züge auf. Denn ob und, wenn ja, welche Dienste auf Basis welcher Netze Verbraucher nachfragen, sollte allein ihnen überlassen sein. Das Abzielen auf eine möglichst hohe Nutzung von Gigabit-Netzen sollte jedenfalls kein explizites Regulierungsziel darstellen.

1.3 Neues Verfahren zur Allgemeingenehmigung und neues Passverfahren

Die Etablierung eines neuen Verfahrens zur Allgemeingenehmigung, welches stärker harmonisierte, einheitliche und in seiner Anzahl limitierte Bedingungen und Anforderungen vorsieht, sowie die Schaffung eines Pass-Regimes auf Grundlage des Herkunftslandprinzips senken Markteintrittsbarrieren, fördern den Wettbewerb, reduzieren administrative Aufwände und erleichtern die grenzüberschreitende Erbringung von elektronischen Kommunikationsdiensten. Sie können mithin einen Beitrag zur Förderung des Binnenmarkts leisten. Gleichwohl dürfte dieser Beitrag gering ausfallen. Denn auch wenn das derzeit bestehende Rechtsgefüge stark fragmentiert ist und die Mitgliedstaaten eine Vielzahl unterschiedlicher Ansätze verfolgen, stellt die Allgemeingenehmigung für sich genommen üblicherweise keine unüberwindbare Hürde für Betreiber von elektronischen Kommunikationsnetzen und Anbieter von elektronischen Kommunikationsdiensten dar.⁸ Denn bei dieser handelt es sich bisher, erstens, um ein freiwilliges Instrument; einige Mitgliedstaaten verzichten ganz darauf. Und zweitens hat es eher deklaratorischen Charakter und ist kein klassisches Zulassungsverfahren, sodass Betreiber bzw. Anbieter auch ohne eine aktive Zustimmung einer zuständigen Behörde Netzinfrastrukturen betreiben und Dienste erbringen dürfen. Die positiven Effekte einer stärkeren Harmonisierung und Zentralisierung dürften somit zwar bestehen, sollten jedoch nicht überschätzt werden. Die bedeutendsten Hürden für einen Telekommunikationsbinnenmarkt liegen woanders und entfalten sich in der Regel erst nachgelagert zu einer Allgemeingenehmigung bzw. zur Möglichkeit des Rückgriffs auf einen EU-Pass.

Dass die Liste an Bedingungen für eine Allgemeingenehmigung künftig als abschließend gelten soll, die Mitgliedstaaten keine zusätzlichen Anforderungen festlegen dürfen, das GEREK mittels Leitlinien für eine einheitliche Anwendung sorgen soll und der Katalog an zu erfüllenden Bedingungen gerade für Unternehmen, die in

⁵ Es erschließt sich beispielsweise nicht, warum der Schutz eines wirksamen Wettbewerbs oder die Nachhaltigkeit im neuen Rahmen zur Stärkung der Resilienz des Digitale Netze-Sektors denselben Stellenwert genießen sollen wie die Resilienz selbst.

⁶ Verordnung (EU) 2020/852 vom 18. Juni 2020 über die Einrichtung eines Rahmens zur Erleichterung nachhaltiger Investitionen und zur Änderung der Verordnung (EU) 2019/2088.

⁷ So schreibt die Kommission, dass „Glasfasernetze bis zum Endkunden („FTTH“) [...] die zukunftssicherste Möglichkeit dar[stellen]“, um „sichere, zuverlässige und energieeffiziente Festnetzverbindungen bereitzustellen, die den Zielen der Union im Bereich der digitalen Transformation und des Klimaschutzes gerecht werden und gleichzeitig die Wartungs- und Betriebskosten für die Betreiber senken“ [Erwägungsgrund 146].

⁸ Die Neuregelungen vereinfachen etwas, was bereits einfach war, insbesondere durch eine Zentralisierung von Verfahren und Vereinfachung von formalen Auflagen [Gambardella Luigi (2026), The “Single Passport” is not the Single Market: Europe confuses forms with borders, LinkedIn post, 21. Januar 2026].

mehreren Mitgliedstaaten tätig werden wollen, oftmals kleiner werden soll, ist ein wichtiges Signal zur Verwaltungsvereinfachung, zur Schaffung von Planungs- und Rechtssicherheit und zur Erleichterung des grenzüberschreitenden Marktzugangs. Die vorgenommenen Anpassungen stellen in jedem Fall einen Mehrwert im Vergleich zum Status quo dar. Festzuhalten ist gleichwohl, erstens, dass der einheitliche Katalog an Bedingungen nun auch Bedingungen enthalten wird, die die bisherigen Kataloge nicht enthalten. Dies gilt etwa für das Erfordernis zur Erfüllung von Anforderungen an Resilienz und Vorsorge sowie zur (Cyber-)Sicherheit in der IKT-Lieferkette nach der vorgeschlagenen Überarbeitung des Rechtsakts zur Cybersicherheit (CSA 2). Zweitens bleibt eine vollständige Vereinheitlichung aus. So müssen die Anbieter beispielsweise auch künftig z.B. nationale Vorgaben zur Vorratsdatenspeicherung oder – nach der NIS-2-Richtlinie unterschiedlich umgesetzte– Anforderungen zur Cybersicherheit beachten und die Mitgliedstaaten dürfen Einschränkungen für ein Tätigwerden aus Gründen der Wahrung der öffentlichen Ordnung, Sicherheit oder Gesundheit beschließen bzw. aufrechterhalten. Es werden mithin auch mit der Reform einige (teils nachvollziehbare) Hürden verbleiben und neue geschaffen, welche als Markteintrittshürden wirken und einer administrativen Erleichterung entgegenwirken werden. Des Weiteren ist, drittens, zwar sinnvoll, dass mittels Leitlinien für eine kohärente, nichtdiskriminierende und verhältnismäßige Anwendung der Genehmigungsbedingungen gesorgt werden soll. Ob das GEREK dies jedoch allein in zufriedenstellender Weise tun kann, ist fraglich. Denn teilweise betreffen die Genehmigungsbedingungen Sachverhalte, mit denen GEREK gar nicht primär betraut ist und wo es dem GEREK mithin an Kompetenzen und Fähigkeiten mangelt. Stattdessen haben hier andere Behörden, die etwa für Cybersicherheits- oder Vorratsdatenspeicherungsthemen zuständig sind, viel tiefere Einblicke. Sollten diese spezifischen Bedingungen daher Teil der abschließenden Liste an Bedingungen bleiben, sollte über eine engere Einbindung weiterer Aufsichtsinstanzen nachgedacht werden.

Neben der Ausgestaltung der Notifizierung dürfte auch die Frage sein, wer die Verantwortung dafür tragen wird, zu prüfen, dass die an eine Allgemeingenehmigung geknüpften Bedingungen in der Praxis auch eingehalten werden. Hierzu ist zunächst festzuhalten: Die Hauptverantwortung soll laut dem Kommissionsvorschlag die notifizierte NRB tragen, während die NRBs von Aufnahmemitgliedstaaten nur dann eingreifen dürfen sollen, sollten sich schwerwiegende negative Auswirkungen für die nationale Sicherheit oder das öffentliche Interesse abzeichnen. Dieser Regulierungsansatz birgt jedoch Risiken, und zwar in mehrerlei Hinsicht. Erstens ist fraglich, ob die hauptverantwortliche NRB immer in der Lage ist bzw. die Fähigkeiten und Kapazitäten dafür besitzt, die Befolgung der Anforderungen in anderen Mitgliedstaaten zu überwachen und sicherzustellen. Zweitens ist zu bezweifeln, dass das Aufsichtsinteresse für die Inlands- und die Auslandstätigkeiten eines Netzbetreibers oder Diensteanbieters gleichermaßen ausgeprägt sein wird oder, ob nicht zu erwarten ist, dass sie einen Schwerpunkt auf die Aktivitäten im Inland setzen wird. Und drittens könnten Netzbetreiber und Diensteanbieter, als Folge dieses Regulierungsansatzes, den Anreiz verspüren, sich jene NRB zur Notifizierung auszusuchen, die ihre Aufsichts- und Kontrollfunktion vermeintlich am wenigsten ernst zu nehmen verspricht. Im Sinne einer wirksamen Durchsetzung der Genehmigungsbedingungen sollten NRBs in den Aufnahmemitgliedstaaten daher frühzeitiger eingreifen können, und nicht erst bei schwerwiegenden negativen Auswirkungen.

Und nicht zuletzt, schafft die Kommission veritable Rechtsunsicherheiten mit Blick auf den Geltungsbereich von Allgemeingenehmigungen. Denn dieser könnte so verstanden werden, dass künftig neben klassischen Telekommunikationsdiensten beispielsweise auch Cloud-Dienste und Content Delivery Networks (CDNs) erfasst sind. Eine solche Lesart ergibt sich etwa bei der Lektüre von Art. 9 Abs. 2 und Erwägungsgrund 42⁹ und würde auch der Logik folgen, wonach die Kommission eine zunehmende Konvergenz zwischen elektronischen Kommunikationsnetzen und Cloud-/Edge-Computing erkennt. Gleichzeitig erklärt die Kommission, dass sie mit dem DNA nicht das Ziel verfolgt, Cloud-Dienste zu regulieren¹⁰, und erläutert auch eine etwaige Erweiterung des Geltungsbereichs des Verfahrens zur Allgemeingenehmigung auf z.B. Cloud-Dienste und CDNs an keiner Stelle hinreichend. Unabhängig davon, ob eine solche Ausdehnung sachgerecht wäre, sollte erstens klargestellt werden, ob diese überhaupt gewünscht ist, zweitens müsste sie dann explizit begründet werden, und drittens sollte erläutert werden, welche Erwartungen an eine solche Erweiterung geknüpft wären. In seiner jetzigen Form sind die vorgeschlagenen Anpassungen am Anwendungsbereich jedenfalls unklar und bedürfen der Klarstellung und Präzisierung.

⁹ Diese schreiben vor, dass das Verfahren zu Allgemeingenehmigungen auch für Anbieter von elektronischen Kommunikationsnetzen gelten soll, sofern diese „ganz oder überwiegend“ der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder Dienste der Informationsgesellschaft dienen, und künftig alle Arten von elektronischen Kommunikationsnetzen erfassen soll, die an der Bereitstellung öffentlich zugänglicher digitaler Dienste beteiligt sind.

¹⁰ Siehe Seite 3 des Kommissionsvorschlags

1.4 Neuer Rahmen zur Stärkung von Resilienz und Vorsorge des Digitale-Netze-Sektors

In den vergangenen Jahren hat die EU bereits eine Vielzahl von Anstrengungen zur Stärkung der Resilienz und Vorsorge der europäischen Wirtschaft und insbesondere von (Betreibern von) kritischen Infrastrukturen unternommen. Zu den getroffenen Maßnahmen zählen neben nicht-legislativen Schritten wie der Strategie zur Stärkung der wirtschaftlichen Sicherheit der EU [[JOIN\(2025\) 977](#), s. [cepInput](#)] und der Europäischen Strategie für eine Union der Krisenvorsorge [[JOIN\(2025\) 130](#)] auch die Etablierung bzw. Verschärfung einiger sektorübergreifender Rechtsvorschriften, die auch auf die Digitale-Netze-Sektoren Anwendung finden. Zu nennen sind hier, erstens, die überarbeitete Richtlinie zur Netz- und Informationssicherheit (NIS-2-Richtlinie [[\(EU\) 2022/2555](#), s. [cepAdhoc](#)], welche bereits bestehenden Verpflichtungen zur Cybersicherheit verschärft, zweitens, die CER-Richtlinie [[\(EU\) 2022/2557](#)], die vordergründig die physische Resilienz kritischer Einrichtungen adressiert, sowie, drittens, der Cyber Resilience Act [CRA, [\(EU\) 2024/2847](#), s. [cepAnalyse](#)], der horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen etablierte. Darüber hinaus kann auch die im Januar 2026 vorgeschlagene Überarbeitung des Rechtsakts zur Cybersicherheit [CSA 2, [COM\(2026\) 11](#)] in diesen Kanon aufgenommen werden, sieht sie doch strenge Maßnahmen zur Verringerung von Risiken in der IKT-Lieferkette vor, und insbesondere auch den mittelfristig verbindlichen Ausschluss von IKT-Komponenten aus Netzinfrastrukturen, sofern diese ihre Ursprung in bestimmten Hochrisiko-Drittstaaten haben¹¹.

Angesichts dieser Fülle an legislativen wie nicht-legislativen Maßnahmen könnte man versucht sein zu argumentieren, dass es keiner weiterer Schritte zur Förderung von Resilienz und Vorsorge bedarf, zumal einige der Maßnahmen ihre volle Wirkung noch gar nicht entfalten konnten, entweder, da sie erst kurze Zeit oder weil sie noch gar nicht Anwendung finden. Eine solche Argumentation greift jedoch zu kurz.

Zahlreiche Ereignisse in den vergangenen Monaten und Jahren verdeutlichen, dass hier weitergehende Anstrengungen vonnöten sind. Hier sind nicht nur die zahlreichen Angriffe auf Unterseekabel zu nennen, wie etwa jene vom Oktober 2022, als Glasfaserkabel bei Marseille an mehreren Stellen durchtrennt und in Schottland zwei Kabel beschädigt wurden, mit enormen Auswirkungen für die Verfügbarkeit des Internets.¹² Auch ein fehlerhaftes Update des CrowdStrike Falcon Sensors sorgte im Juli 2024 für massive IT-Ausfälle, ging mit schwerwiegenden Störungen der Kommunikationsinfrastruktur einher und bedeutete für eine Vielzahl von betroffenen Firmen, dass sie ihren Betrieb einstellen mussten.¹³ Ein Cyberangriff aus dem September 2025, der die Check-in-Systeme und damit wichtige IKT-Dienste betraf, sorgte für erhebliche Störung des Flugverkehrs in mehreren großen europäischen Städten.¹⁴ Allein im Jahr 2024 wurden der ENISA 188 Vorfälle von den TK-Aufsichtsbehörden gemeldet, die als schwerwiegend einzustufen sind.^{15,16} Ein Jahr zuvor waren es noch 156 Vorfälle. Bei 60% der 188 signifikanten Vorfälle, über die der Telekommunikationssektor Meldungen erstattete, handelte es sich um Systemausfälle, gefolgt von menschlichem Versagen (35 Vorfälle bzw. 19%) und Naturereignisse (25 Vorfälle oder 12%). Nur 12 Vorfälle oder 8% entfielen auf böswillige Handlungen, wobei hier Kabeldurchtrennungen mit allein 7 Vorfällen besonders hervorstechen (2023 gab es keinen solchen gemeldeten Vorfall). Diese Zahlen liefern jedoch wohl kein vollständiges Bild, da die Behörden nicht immer alle Vorfälle tatsächlich melden¹⁷. Fakt ist, dass wir uns einer fragilen, unsicheren und unvorhersehbaren geopolitischen Lage konfrontiert sehen, es große Abhängigkeiten der EU bei IKT-Vermögenswerten gegenüber nicht immer wohlgesinnten Drittstaaten wie China und zunehmend den USA gibt und die in der EU genutzte IKT etwa auch vielfach als veraltet betrachtet werden kann.¹⁸

¹¹ Die vorgeschlagenen strengen Maßnahmen zum Ausschluss von IKT-Komponenten sind auch eine Reaktion auf die aus Sicht der Kommission schleppende und unzureichende Umsetzung der sogenannten „5G-Toolbox“. Diese fordert von den Mitgliedstaaten die Umsetzung von Maßnahmen zur Verbesserung der Sicherheit und Resilienz von 5G-Netzen. Im Juni 2023 beklagte die Kommission in einer [Mitteilung](#) die mangelhafte Umsetzung der Toolbox und verlangte nach konkreten Schritten insbesondere in Bezug auf Hochrisikoanbieter.

¹² Anselm Küsters (2022), Europas verwundbares Rückgrat, Warum die EU digitale kritische Infrastruktur besser schützen muss, [cepAdhoc](#) Nr. 13 | 2022, Oktober 2022, abrufbar [hier](#).

¹³ Bitkom (2024), CrowdStrike: Welche Folgen der IT-Ausfall für deutsche Unternehmen hatte, 19. September 2024, s. [hier](#).

¹⁴ European Federation of Engineering Consultancy Associations (EFCA) (2025), Engineering Resilience – Current Challenges, Risks and Recommendations for the Information and Communication Technology Sector in Europe, Dezember 2025.

¹⁵ An den Meldungen der Vorfälle beteiligten sich für das Jahr 2025 insgesamt 25 EU-Mitgliedstaaten und zwei EFTA-Länder.

¹⁶ ENISA (2025), Telecom Security Incidents 2024. Juli 2025, abrufbar [hier](#).

¹⁷ S. [hier](#).

¹⁸ European Federation of Engineering Consultancy Associations (EFCA) (2025).

Wie nicht zuletzt in einem Statement der G7-Staaten vom Mai 2023¹⁹ und im so sogenannten Nevers Call aus dem März 2022²⁰ hervorgehoben, bedarf es weiterer Schritte, um die ganze Bandbreite an kritischen Infrastrukturen im IKT-Ökosystem (z.B. TK-Netze, Unterseekabel, Cloud-Infrastrukturen) sicherer und widerstandsfähiger zu machen und sich diesbezüglich stärker unter den relevanten Unternehmen, den einschlägigen Behörden und sonstigen Entscheidungsträgern zu vernetzen und zu kooperieren. Denn diese Infrastrukturen sind heutzutage ein Eckpfeiler für die Funktionsfähigkeit europäischer Gesellschaften und stellen eine „Lebensader der europäischen und transatlantischen Informationsgesellschaft“²¹ dar. Anfälligkeiten und Störungen haben oftmals nicht nur Auswirkungen für den Sektor und die spezifischen Marktteilnehmer selbst. Vielmehr bestehen eine Vielzahl von Interdependenzen, Abhängigkeiten und sonstigen sektorübergreifenden Verbindungen, die schwerwiegenden Kaskadeneffekten den Weg bereiten und neben der wirtschaftlichen Stabilität auch die nationale Sicherheit bedrohen können. Es bedarf angesichts der geopolitischen und geoökonomischen Verwerfungen und der anhaltend angespannten Sicherheitslage zusätzliche Anstrengungen, welche, angesichts der zunehmenden Vernetzung vieler Infrastrukturen und ihres Ökosystem-Charakters nicht an mitgliedstaatlichen Grenzen Halt machen sollten, sondern auch auf EU-Ebene erfolgen sollten.

Bei den bereits in Angriff genommenen Maßnahmen stehen zu bleiben, hieße ferner, sich auf rein sektorübergreifende Verpflichtungen zu verlassen, welche den Besonderheiten, Risiken und Vulnerabilitäten des Digitale Netze-Sektors nicht immer gebührend Rechnung tragen und die relevanten Aufsichtsinstanzen nur unzureichend Möglichkeiten gewährt, adäquat und angemessen zu reagieren. Auch hieße es auf eine enge und potenziell wertvolle Kooperation und Koordination zwischen relevanten sektorübergreifend tätigen Aufsichtsinstanzen, Gremien und Notfallteams – z.B. ENISA²², CSIRTs-Netzwerk²³, EU CyCLONe²⁴ – und sektorspezifischen – z.B. GEREK bzw. ODN – Aufsichtsinstanzen zu verzichten, obwohl sie im Fall von Krisen dazu beitragen könnten, diese schneller und effektiver einzudämmen und zu bewältigen. Ferner ist ein engerer Austausch zwischen staatlichen Stellen, sowohl auf europäischer als auch auf nationaler Ebene, und den Marktteilnehmern zwingend, da die einzelnen Akteure für sich genommen in der Regel nicht in der Lage sind, alle Risiken und Bedrohungen zu überblicken und sie diese Risiken und Bedrohungen auch nicht immer in ihr Entscheidungskalkül einbeziehen, da etwaige Kosten nicht bei ihnen selbst, sondern bei Dritten anfallen.

Die Etablierung eines Resilienz- und Vorsorgerahmens speziell für des Digitale Netze-Sektors ist daher grundsätzlich zu begrüßen. Der von der Kommission vorgeschlagene Ansatz geht dabei in die richtige Richtung, indem er neben einem umfassenden Lagebild auch auf konkrete Handlungsempfehlungen und die Etablierung von wirksamen Koordinierungsmechanismen und den Austausch zwischen wichtigen Instanzen abzielt.

Bei der konkreten Ausgestaltung des Resilienz- und Vorsorgerahmens sollten jedoch mehrere Aspekte Beachtung finden. Klar ist zunächst, dass der Rahmen insbesondere dem Vereinfachungsparadigma der Kommission, welches auf dringend notwendige regulatorische Erleichterungen für die europäische Wirtschaft dringt, entgegensteht, und sowohl für weitere Berichtsansforderungen und administrative Lasten als auch zu zusätzlichen Investitionserfordernissen und Kosten führen wird. Zusätzliche (personelle) Ressourcen werden nicht nur zur Steigerung der Fähigkeiten und Kapazitäten zum besseren Schutz von Netzinfrastrukturen benötigt werden, sondern etwa auch, um die Koordinierungserfordernisse adäquat abbilden und den Bedarfen der verschiedenen Aufsichtsinstanzen gerecht werden zu können. All dies wird insbesondere für kleinere Marktakteure eine Herausforderung darstellen. Es gilt mithin den Rahmen – stärker wie bisher vorgesehen – so auszugestalten, dass er einem risikobasierten Ansatz folgt und die Verhältnismäßigkeit gewahrt bleibt. Dass die für die Pläne des GEREK von den NRBs zu erhebenden Daten sich auf das unbedingt erforderliche Maß beschränken und die NRBs, falls möglich, immer auf bereits vorhandene Informationen zurückgreifen sollen, weist hier in die richtige Richtung. Für die Erhebungsfrequenz sollte jedoch ein Mechanismus greifen, der sich, statt verpflichtend und unterschiedslos alle zwei Jahre, stärker an der volkswirtschaftlichen Bedeutung und Kritikalität einer Netzinfrastruktur bzw.

¹⁹ G7 Leaders' Statement on Economic Resilience and Economic Security, May 20, 2023, siehe [hier](#).

²⁰ Informal Meeting of the Telecommunications Ministers, Nevers Call to Reinforce the EU's Cybersecurity Capabilities, Nevers, March 9, 2022, siehe [hier](#).

²¹ Anselm Küsters, André Wolf und Eleonora Poli (2024), Challenges to Transatlantic Digital Infrastructure: An EU Perspective. Istituto Affari Internazionali (IAI), Februar 2024, abrufbar [hier](#).

²² Die ENISA ist die EU-Agentur für Cybersicherheit und fungiert als Instanz, die u.a. die EU-Institutionen und die Mitgliedstaaten bei der Identifizierung, Vorbeugung und Abwehr von Cyberrisiken und -bedrohungen unterstützt.

²³ Das sogenannte CSIRTs-Netzwerk ist ein Netzwerk aus nationalen Computer-Notfallteams, welches von der ENISA koordiniert wird und insbesondere zur operativen Zusammenarbeit und koordinierten Reaktion auf Sicherheitsvorfälle etabliert wurde.

²⁴ EU CyCLONe ist ein europäisches Netzwerk, welches bei groß angelegten Cybersicherheitsvorfälle auf operativer Ebene unterstützend und koordinierend tätig wird, gemeinsame Lagebild erstellt, die Auswirkungen analysiert und mögliche Abhilfemaßnahmen diskutiert.

einzelner Netzkomponenten sowie der „systemischen Relevanz“ des Betreibers der Netze orientiert. Es muss das Ziel sein, dass Aufwand und Ertrag in einem angemessenen Verhältnis stehen und der Rahmen zu keiner reinen Compliance-Übung wird.

Außerdem weist der Kommissionsvorschlag Lücken mit Blick auf die unterschiedlichen Rollen der zahlreichen involvierten Behörden, Gremien und Aufseher auf. Bereits derzeit existiert ein komplexes Geflecht an Einrichtungen, die bei der Stärkung bzw. Wahrung der Sicherheit von kritischen Infrastrukturen, inklusive von Netzinfrastrukturen, unterstützen sollen, angelegt sowohl auf EU-Ebene als auch auf nationaler Ebene. In dieses Geflecht wird nun insbesondere noch zusätzlich das GEREK, das ODN und die NRBs eingewoben. Diese zusätzliche „Behördenschicht“ wird zu einer Etablierung zusätzlicher Koordinierungs- und Kooperationsprozesse führen. Um ein „Behördenwirrwarr“ zu verhindern, bedarf es mithin einer klaren Rollenverteilung, der Zuweisung von eindeutigen Verantwortlichkeiten und möglichst schlanker und tragfähiger Strukturen. Beispielsweise ist fraglich, ob das ODN in der Praxis eine zentrale Koordinierungsrolle zur Stärkung der Resilienz des Digitale-Netze-Sektors spielen kann, wenn es gleichzeitig die bestehenden Rollen anderer Einrichtungen „uneingeschränkt“ zu achten hat. So könnte die ENISA bei Attacken, die die Cybersicherheit betreffen und Auswirkungen auf den Digitale-Netze-Sektor haben, für sich eine hervorgehobene Rolle beanspruchen und damit in Konflikt zu den Ambitionen des ODN stehen, welche die Cybersicherheit auch als einen maßgeblichen Resilienzfaktor verstehen dürfte. Wenn die verschiedenen Einrichtungen sich jedoch in ihrem komplexen und unübersichtlichen Geflecht an Zuständigkeiten, Kompetenzen und Verfahren verfangen sollten, droht der Mehrwert des avisierten Resilienz- und Vorsorgerahmens zu verpuffen. Hier gilt es mithin nachzubessern und konkreter zu werden.

Der vorgeschlagene Resilienz- und Vorsorgerahmen lässt zudem eine zentrale Frage unbeantwortet. Wie bereits erwähnt, ist mehr Widerstandsfähigkeit und zusätzliche Prävention nicht kostenlos zu haben. Es bleibt jedoch im Vorschlag zum DNA weithin unklar, wer für die zusätzlichen Kosten aufkommen soll. Ohne Konkretisierungen im DNA dürften in erster Linie der Digitale Netze-Sektor selbst und die Kunden der Unternehmen des Sektors belastet werden. Jedoch stellt sich die Frage, ob diese allein für die Güter „Resilienz“ und „Vorsorge“ bezahlen sollten. Denn Investitionen in diese Güter erzeugen regelmäßig positive externe Effekte, sodass auch branchenfremde Akteure, ob Verbraucher, Unternehmen oder staatliche Einrichtungen, von diesen Investitionen profitieren. Es gibt mithin gute Gründe dafür, auch (vermeintlich) „unbeteiligte Dritte“ an der Finanzierung zumindest zu beteiligen – etwa über die öffentlichen Haushalte –, ohne die Akteure des Digitale-Netze-Sektors von finanziellen Verantwortlichkeiten zu befreien. Denn auch sie haben ein Eigeninteresse an stabilen und ausfallsicheren Netzen. Zudem stünde eine alleinige Finanzierung durch den Sektor in Konflikt zum postulierten Regulierungsziel, den Ausbau von Gigabitnetzen zu unterstützen und diesbezügliche Investitionen anzuregen. Zu diesem Sachverhalt bedarf es daher in jedem Fall weiterer Konkretisierungen innerhalb des DNA. Der vage Ansatz, dem GEREK zu ermöglichen, in seinem „EU-Vorsorgeplan für digitale Infrastrukturen“ auch „Finanzierungsmechanismen“ mitzudenken, ist der falsche. Sachverhalte mit solch großer finanzieller Tragweite sollten die EU-Gesetzgeber selbst klären, zumal auch unklar bleibt, welche praktische Relevanz bzw. Bindungskraft vom GEREK vorgeschlagene Mechanismen hätten.

Die Kommission drängt, insbesondere über die Vorlage eines „EU-Vorsorgeplans für digitale Infrastrukturen“ zu EU-weit einheitlichen Ansätzen zur Stärkung der Resilienz. Diese sollen für alle relevanten Akteure eine Leitlinie für ihr Handeln sein. So werden die Akteure etwa verpflichtet, die in einem solchen Plan verankerten Empfehlungen (weitgehend) zu berücksichtigen. Dies zielt, sinnvollerweise, auf ein möglichst einheitliches Agieren im Binnenmarkt. Gleichwohl gilt es sicherzustellen, dass die Mitgliedstaaten oder die zuständigen nationalen Behörden auch eigenständige, ggfs. abweichende und, falls nötig, weitergehende Resilienz- und Vorsorgestärkungspolitiken implementieren können. Denn, zum einen, ist das GEREK nicht vor Fehleinschätzungen gefeit und, zum anderen, können solche nationalen Politiken etwa aus Gründen der Aufrechterhaltung wesentlicher gesellschaftlicher Funktionen geboten sein. Mit dem diskretionären Handlungsspielraum für die nationale Ebene sollte gleichwohl die Verantwortung einhergehen, von redundanten, ähnlich gelagerten Maßnahmen Abstand zu nehmen und sinnvolle EU-Ansätze nicht als reine Ergänzung, sondern vordergründig als Ersatz zu werten. Doppelbelastungen, die aus einer nicht dringend notwendigen Aufrechterhaltung nationaler Maßnahmen resultieren, gilt es zu vermeiden.

Wichtig erscheint ferner, mit Blick auf die Umsetzung der in den Plänen des GEREK vorgeschlagenen Resilienz- und Vorsorgemaßnahmen, konkretere Vorgaben zu machen. Dies gilt etwa in Bezug auf die Vorgabe von Zeitplänen für deren Implementierung, zur Nachverfolgung und zum Monitoring der angegangenen Maßnahmen und zu potenziellen Konsequenzen, die bei einer fehlenden oder unzureichenden Umsetzung drohen. Ansonsten ist zu befürchten, dass dem Resilienz- und Vorsorgerahmen ein ähnliches Schicksal droht wie der 5G-Toolbox, welche nur widerwillig und in unterschiedlicher Weise von den Mitgliedstaaten umgesetzt wurde.

Parallel zu den Verhandlungen über die Vorschläge zum DNA für einen Resilienz- und Vorsorgerahmen sollte die Kommission zudem den bereits laufenden Prozess der Eignungsprüfung der EU-Digitalgesetzgebung („Digital Fitness Check“, s. [cepAdhoc](#)) nutzen, um zu untersuchen, ob die bestehenden, verwandten EU-Vorschriften (NIS 2-Richtlinie, Cyber Resilience Act, etc.) gut ineinandergreifen, keine Doppelbelastungen erzeugen und kohärent zueinander ausgestaltet sind. Es sollte vermieden werden, dass mit dem neuen Rahmen nur eine weitere „Regulierungsschicht“ geschaffen wird, welche die Regulierungslandschaft weiter unnötig verkompliziert und Rechtsunsicherheiten Vorschub leistet. Es gilt etwaigen Inkongruenzen und Überschneidungen frühzeitig zu begegnen und sie möglichst vor der Verabschiedung des DNA aufzulösen, um einen wirksamen und effizienten EU-Rechtsrahmen zum Schutz digitaler Netzinfrastrukturen in der EU sicherzustellen. Dies gilt insbesondere in Abgrenzung zu den Vorgaben der NIS-2- und der CER-Richtlinie. Unabhängig von der Eignungsprüfung bereits existierender EU-Digitalvorschriften sollte das Zusammenspiel mit diesen Vorschriften innerhalb des DNA klar definiert werden. Hier gilt es u.a. Doppelregulierung und -strukturen zu vermeiden, Berichtsanforderungen aufeinander abzustimmen und zu vermeiden, dass sich die Marktakteure mit konfligierenden Anforderungen oder widersprüchlichem Aufsichtshandeln konfrontiert sehen.

Die neuen Vorgaben zur Stärkung der Transparenz über Migrationsprozesse zu neuen Technologien, welche Gefahren für die Aufrechterhaltung der Funktionsfähigkeit von Notruf- und öffentlichen Warnsystemen bergen könnten, sind sachgerecht. Frühzeitige Informationen können spätere Diskontinuitäten verhindern, die Vorhersehbarkeit steigern und zusätzliche Planungssicherheit schaffen. Fraglich ist jedoch, ob die Frist von mindestens zwei Jahren für jede Form des Technologiewechsels als ausreichend betrachtet werden kann, insbesondere, wenn die Vorschrift so zu verstehen ist, dass die Migration ab Notifizierung binnen zwei Jahren abgeschlossen sein soll. Denn es ist zu bezweifeln, dass die Umstellungsprozesse in jedem Fall so zügig erfolgen können. Um den Anbietern genügend Zeit für die nötigen Anpassungen zu lassen, sollten Informationen über avisierte Migrationsprozesse mithin möglichst noch früher bereitgestellt werden.

2 Juristische Bewertung

Hinweis: Die juristische Bewertung beschränkt sich hier allein auf die in dieser cepAnalyse adressierten Themenbereiche.

2.1 Kompetenz

Die Verordnung wird zu Recht auf Art. 114 AEUV (Binnenmarkt) gestützt. Für den Kernbestand des Regelwerks ist diese Rechtsgrundlage vertretbar. Beim Regelungskomplex des Resilienzrahmens ist die Kompetenzgrundlage jedoch rechtlich nicht selbstverständlich.

Der Resilienzrahmen (Teil II) berührt den nationalen Sicherheitsvorbehalt nach Art. 4 Abs. 2 Satz 3 EUV, wonach nationale Sicherheit in der alleinigen Verantwortung der Mitgliedstaaten verbleibt.²⁵ Art. 3 Abs. 1 lit. c DNA benennt als allgemeines Ziel der Verordnung die Stärkung der Resilienz einschließlich der der „Sicherheits- und Verteidigungsinteressen der Union und ihrer Mitgliedstaaten“. Art. 5 Abs. 2 verpflichtet Anbieter öffentlicher Kommunikationsnetze und -dienste sowie Notrufabfragestellen (PSAPs), dazu „alle erforderlichen Maßnahmen“ zu ergreifen, um die ununterbrochene Verfügbarkeit kritischer Kommunikationsdienste und Notrufe sowie die ununterbrochene Übermittlung öffentlicher Warnungen in Krisen- und Katastrophenlagen sicherzustellen. Art. 6 Abs. 2 lit. c ordnet an, dass der GEREK-Vorsorgeplan „Krisenmanagementpraktiken“ enthält, die ausdrücklich vereinheitlichte Verfahren, Koordinierungsvereinbarungen und operative Protokolle für den Krisenfall umfassen und sich unmittelbar an nationale Regulierungs- und Kompetenzbehörden richten. Diese Normen greifen strukturell in die Organisation staatlicher Schutzinfrastruktur und des Katastrophenschutzes ein.²⁶ Hinzu kommt, dass Erwägungsgrund 35 die „zellulare Sensorik“ als ergänzendes Erkennungssystem für „zivile und militärische Anwendungen“ adressiert. Militärische Anwendungen sind der EU-Kompetenz nach Art. 4 Abs. 2 EUV in Verbindung mit Art. 42 EUV grundsätzlich entzogen.

Die Kommission operiert im Resilienzrahmen mit den Begriffen „Resilienz“, „Abwehrbereitschaft“, „Vorsorge“ und „Krisenreaktion“, aber nicht direkt mit dem Begriff „nationaler Sicherheit“. Dies ist höchstwahrscheinlich keine zufällige Wortwahl, sondern eine Strategie, um zu verhindern, dass der Regelungsgegenstand unter den Sicherheitsbegriff des Art. 4 Abs. 2 EUV fällt. Der EuGH hat jedoch in seiner Rechtsprechung betont, dass die rechtliche Einordnung einer Maßnahme von ihrem tatsächlichen Regelungsgegenstand und ihrer Wirkung

²⁵ Pechstein, Die Achtung nationaler Identität, ZaöRV 70 (2010), S. 707 ff.

²⁶ Vgl. Kietz D. & Ondarza N. (2016). Sicherheit delegieren: EU-Agenturen in der inneren und äußeren Sicherheit. (SWP-Studie, 6/2016). Berlin: Stiftung Wissenschaft und Politik -SWP- Deutsches Institut für Internationale Politik und Sicherheit. S. 13 ff.

abhängt, nicht von ihrer Bezeichnung („substance over form“).²⁷ Ob „koordinierte Krisenreaktion für Notfallkommunikation“ kompetenzrechtlich wesentlich anders zu behandeln ist als „nationale Sicherheit“, ist eine offene Rechtsfrage. Somit bleibt die Kompetenzgrundlage Art. 114 AEUV in diesem Bereich fraglich. Eine Anfechtung durch Mitgliedstaaten vor dem EuGH erscheint denkbar. Das Risiko der Teilnichtigkeit von Teil II des Kommissionsvorschlags zum DNA ist nicht zu vernachlässigen.

2.2 Subsidiarität und Verhältnismäßigkeit gegenüber den Mitgliedstaaten

Die Kommission begründet EU-Handlungsbedarf mit der Fragmentierung des Binnenmarktes infolge divergierender nationaler Umsetzungen der EKEK-Richtlinie.²⁸ Dies ist empirisch gestützt: Divergente Genehmigungsbedingungen, unterschiedliche Endnutzerregeln und verspätete 5G-Auktionen auf veralteter Rechtsgrundlage sind belegte Tatbestände. Die daraus gezogene Schlussfolgerung, dass eine Verordnung mit der vorliegenden Zentralisierungstiefe erforderlich ist, ist jedoch subsidiaritätsrechtlich angreifbar.

Nach Art. 5 Abs. 3 EUV ist maßgeblich, ob die Ziele der geplanten Maßnahme auf EU-Ebene besser verwirklicht werden können als durch die Mitgliedstaaten. Dieses Positivkriterium des „besser“ erfordert eine Bewertung der Effektivität des Unionshandelns, insbesondere unter Berücksichtigung der Größenordnung und des grenzüberschreitenden Charakters des Problems sowie der Folgen eines Unterlassens unionsrechtlicher Maßnahmen.²⁹ Die Prüfung muss ergeben, dass die Maßnahme aufgrund ihrer breiteren Wirkung der Zielverwirklichung näherkommt als einzelstaatliches Handeln. Maßgeblich ist hingegen nicht, ob Mitgliedstaaten ihre Pflichten in der Vergangenheit unzureichend erfüllt haben.³⁰ Dies zeigt sich auch in der Begründung der Kommission zum DNA, wonach der bisherige Rechtsrahmen in Form einer Richtlinie zu einer Fragmentierung des Binnenmarkts geführt habe und daher keinen einheitlichen Markt gewährleisten konnte.³¹ Das geeignete Instrument zur Sanktionierung schlechter Richtlinienumsetzung ist das Vertragsverletzungsverfahren nach Art. 258 AEUV³², nicht der Formwechsel. Würde die schlechte Umsetzungsbilanz einen Wechsel zur Verordnung rechtfertigen, ließe sich jede Richtlinie in eine Verordnung umwandeln, sobald die Umsetzung unbefriedigend ausfällt. Damit würde der primärrechtliche Unterschied zwischen beiden Instrumenten entwertet. Vor diesem Hintergrund entsteht der Eindruck, dass die Kommission das Subsidiaritätskriterium teilweise eher normativ voraussetzt als empirisch nachweist. Insbesondere bleibt es unklar, auf welcher Grundlage die behauptete Ineffektivität nationaler Regelungsansätze beruht. Darüber hinaus lässt eine Verordnung keinen Spielraum für die erheblichen strukturellen Unterschiede der nationalen Märkte hinsichtlich Marktstrukturen, geographischer Bedingungen, Investitionszyklen und regulatorischer Kapazitäten.³³

2.3 Sonstige Vereinbarkeit mit EU-Recht

Die Normkohärenz mit bestehendem EU-Recht ist teilweise ungenügend gesichert. Problematisch ist das Verhältnis zur NIS-2-Richtlinie (2022/2555/EU). Art. 4 des DNA verweist auf Art. 8 Abs. 1 und Art. 9 Abs. 1 NIS-2-Richtlinie und bezieht die dortigen nationalen Cybersicherheits- und Krisenreaktionsbehörden in den Kooperationsrahmen ein. Art. 5 Abs. 2 enthält den Vorbehalt „unbeschadet der Richtlinie (EU) 2022/2555“. Diese Formulierung sagt lediglich, dass die NIS-2-Richtlinie nicht verdrängt wird. Sie bestimmt nicht, welches Regime bei widersprüchlichen Anforderungen Vorrang hat, welche Behörde zuständig ist, wenn eine NRB und eine nationale Cybersicherheitsbehörde gleichzeitig tätig werden, und wie Unternehmen verfahren sollen, wenn sie von beiden Behörden divergierende Anweisungen erhalten. Ein Telekommunikationsanbieter, der einen Sicherheitsvorfall erlebt, hat nach der NIS-2-Richtlinie eine 24-Stunden-Erstmeldepflicht gegenüber der Cybersicherheitsbehörde; nach dem DNA-Resilienzrahmen bestehen Verfügbarkeits- und Kooperationspflichten gegenüber der NRB. Beide

²⁷ EuGH, 16.06.2015, Gauweiler u.a., C-62/14, para. 70; EuGH, 05.10.2000, Bundesrepublik Deutschland gegen Europäisches Parlament und Rat der Europäischen Union, C-376/98, C-74/99, para 83.

²⁸ Erwägungsgrund 4 des DANN-Kommissionsvorschlags.

²⁹ Vgl. Calliess/Ruffert EUV Kommentar, Art. 5 EUV Rn. 40 ff.

³⁰ Fründ, F., Subsidiarität – Recht und Kontrolle: Eine Untersuchung zur gerichtlichen Kontrolldichte des Art. 5 Abs. 3 EUV. Schriften zum Europäischen Recht. Band 205, Duncker & Humblot 2021. S. 37 ff.

³¹ Siehe Seiten 1 und 7 des Kommissionsvorschlags.

³² Gemäß Art. 259 AEUV sind die Mitgliedstaaten berechtigt, gegen einen anderen Mitgliedstaat eine Vertragsverletzungsklage zu erheben. In der Praxis wird von dieser Möglichkeit jedoch nur selten Gebrauch gemacht. S. Cremer, in: Calliess/Ruffert, EUV/AEUV, 6. Aufl. 2022, Art. 259 AEUV, Rn. 1.

³³ Selbst BEREC hat sich kritisch zu einer tiefgreifende Zentralisierung ausgesprochen, S. BEREC (2026), Early BEREC Assessment of the Digital Networks Act, 30 March 2026, BoR (26) 52, S. 4 ff.

Behörden können im Krisenfall Anweisungen erteilen; welche Anweisung Vorrang hat, wenn sie kollidieren, ist im DNA nicht geregelt.

Für den Finanzsektor hat die EU mit der DORA-Verordnung (2022/2554/EU) (s. [cepAnalyse](#)) explizite Abgrenzungsregeln gegenüber der NIS 2-Richtlinie (s. [cepAdhoc](#)) vorgesehen. Nach der DORA-Verordnung gilt die NIS-2-Richtlinie zwar grundsätzlich weiter für DORA-Normadressaten, jedoch verhindert eine Vorrangklausel im Sinne der Spezialregelung (lex specialis) in der DORA-Verordnung die Überschneidung: Die DORA-Verordnung hat Vorrang gegenüber NIS-2-Richtlinie für die erfassten Finanzunternehmen. Eine vergleichbare Lösung für den Telekommunikationssektor fehlt jedoch. Das Aufsichten eines weiteren Resilienzrahmens auf eine noch nicht vollständig transponierte Grundlage³⁴ verstärkt die Rechtsunsicherheit. Ähnliche, wenn auch weniger akute Überschneidungsprobleme bestehen mit dem Cyber Resilience Act (2024/2847/EU, s. [cepAnalyse](#)), dem Data Act (2023/2854/EU) (s. [cepInput](#)) und dem AI Act (2024/1689/EU), mit denen der DNA interagiert, ohne systematische Abgrenzungsregeln vorzusehen. Solche ungeklärte Normschnittstellen laufen dem erklärten Vereinfachungsziel des DNA unmittelbar zuwider.

D. Fazit

Nach vielen Monaten und Jahren der intensiven und kontroversen Diskussionen, an denen sich auch das cep aktiv beteiligte (s. [cepAnalyse](#)), legte die Kommission zu Beginn des Jahres mit dem DNA ein umfangreiches neues Regelwerk zur Regulierung des Konnektivitätssektors vor. Diese **cepAnalyse**, die zunächst vier Teilaspekte des Kommissionsvorschlags – Regelungssystematik, Regulierungsziele, Allgemeingenehmigung/EU-Pass sowie neuer Resilienz- und Vorsorgerahmen – in den Blick nimmt, zieht ein gemischtes Fazit:

Die Etablierung des DNA als Verordnung, die zudem mehrere sektorspezifische EU-Rechtsakte bündelt, stärkt die Rechtssicherheit und -konsistenz, erschwert unerwünschtes Gold-Plating-Verhalten und fördert den Binnenmarkt. Gleichwohl birgt die neue Regelungssystematik politökonomische Fallstricke, etwa die Gefahr von wenig sachdienlichen Paketlösungen oder höhere Hürde für gezielte Anpassungen des Regelwerks in der Zukunft.

Die Erweiterung des Zielekatalogs erscheint politisch geboten, ist jedoch abzulehnen. Denn werden zu viele Ziele verfolgt, wird am Ende keines mehr verfolgt. Auch steigt die Gefahr industriepolitisch motivierter Eingriffe in Marktprozesse. Zudem wird zusätzlichen Zielkonflikten Vorschub geleistet. Ferner steigt die Regulierungskomplexität und die Vorhersehbarkeit der Regulierung leidet. Dies steht im Widerspruch zur Vereinfachungsagenda der Kommission.

Die regulatorische Bevorzugung von Netzen, die zu den „Gigabit-Netzen“ zählen und die bis zum Netzabschlusspunkt vollständig aus Glasfaserelementen bestehen (FFTH-Netze), ist verfehlt. Es ist nicht Aufgabe der Politik bzw. von (Regulierungs-)Behörden darüber zu entscheiden, welche Netztechnologie die vermeintlich beste und unterstützungswürdigste Technologie darstellt. Das Postulat der Kommission, wonach FTTH die „zukunftsstärkste Lösung“ sei, ist eine Anmaßung von Wissen und ein Bruch mit dem Primat der Technologieneutralität.

Das neue Verfahren zur Allgemeingenehmigung und die Etablierung eines EU-Pass-Regimes senken Markteintrittsbarrieren, fördern den Wettbewerb, reduzieren administrative Aufwände und stärken den Binnenmarkt. Die positiven Effekte dürften jedoch gering ausfallen. Darüber hinaus bergen die Vorgaben zur Durchsetzung der Genehmigungsbedingungen Risiken mit Blick auf Arbitrageverhalten und eine mangelnde Kontrolle in Aufnahmemitgliedstaaten. Ferner bedarf es Klarstellungen beim Geltungsbereich, um Rechtsunsicherheiten zu mindern.

Die Etablierung eines sektorspezifischen Resilienz- und Vorsorgerahmens ist, obgleich bereits eine Fülle von (nicht-)legislativen Maßnahmen ergriffen wurden, angesichts geopolitischer Spannungen und der derzeitigen Sicherheitslage zu begrüßen. Er sollte jedoch stärker wie bisher vorgesehen einem risikobasierten Ansatz folgen. Auch lässt er bisher die zentrale Frage der Finanzierung unbeantwortet. Es gibt jedenfalls gute Gründe dafür, auch (vermeintlich) „unbeteiligte Dritte“ an der Finanzierung zu beteiligen.

Die neuen Vorgaben zur Stärkung der Transparenz über Migrationsprozesse zu neuen Technologien sind sachgerecht. Sie können dazu beitragen, spätere Diskontinuitäten zu verhindern, die Vorhersehbarkeit zu steigern und zusätzliche Planungssicherheit schaffen. Die Frist von „mindestens zwei Jahren“ ist jedoch zu kurz und sollte ausgedehnt werden.

³⁴ Die Kommission schlug am 20. Januar 2026 – zeitgleich mit der Vorlage des DNA-Entwurfs – gezielte Änderungen der NIS2-Richtlinie vor.