

The Draft Reform of the European Telecommunications Framework: How Its Interaction with the CSA2 Proposal Risks Breaching the Treaties and Constitutional Principles

Abstract

The European Commission's proposal for a regulation COM(2026)16 (procedure 2026/0013 COD) (the Digital Networks Act, or DNA), aimed at reforming and harmonising the regulatory framework for the electronic communications sector, presents numerous potential interactions with the ongoing cybersecurity reform, whose proposal for a regulation COM(2026)11, also known as the Cybersecurity Act "CSA2", is currently under discussion before the Union's co-legislators.

Although the DNA proposal does not, in its stated objectives, seek to establish a differentiated market-access regime for suppliers based on non-technical criteria, a point of contact with the draft CSA2 cybersecurity reform emerges from the outset, first and foremost in Part III of the proposal, where the provisions on authorisation and spectrum rights are made conditional on compliance with cybersecurity rules.

This provision presents significant legal concerns, as it links access to the electronic communications networks and services market to compliance with ICT supply-chain security requirements set out in the CSA2, whose scrutiny in light of Article 114 TFEU and the principles of legal certainty, proportionality and non-discrimination is not free from significant doubts as to its compatibility with EU law, with the allocation of competences between the EU and the Member States, and with the constitutional principles of the Italian legal order. These doubts find significant confirmation in Advocate General Ćapeta's Opinion of 19 March 2026 in Case C-354/24, *Elisa Eesti AS*, concerning the restriction, on national security grounds, of the use of telecommunications equipment, which — while acknowledging the legitimacy in principle of such restrictions — makes their compatibility with the Treaties conditional on rigorous proportionality scrutiny and on subjection to effective judicial review.

*

I. The DNA–CSA2 Linkage: From Cybersecurity Compliance to Market Access

I.1 Regulatory Context

The European Union's integration process is undergoing a period of significant change in the fields of cybersecurity regulation and telecommunications, where two major legislative proposals are currently under discussion: the proposed regulation COM(2026)16, known as the Digital Networks Act (DNA), and the proposed regulation COM(2026)11, also known as the Cybersecurity Act (CSA2).

Both measures, proposed by the Commission, are subject to the ordinary legislative procedure and are currently under examination before the Council and the European Parliament.

- a) The proposed regulation COM(2026)16, known as the Digital Networks Act (DNA) and based on Article 114 TFEU, seeks to bring about a thorough rationalisation of the sector and to

overcome the fragmentation of national markets. It provides for the repeal of the European Electronic Communications Code (EECC), of the regulation establishing BEREC, and of the Decision on the Radio Spectrum Policy Programme (RSPP), while also incorporating parts of the Open Internet Regulation and amending the ePrivacy Directive.

- b) The proposed regulation COM(2026)11, known as CSA2, for its part seeks to repeal and replace the current Cybersecurity Act (Regulation (EU) 2019/881), forming part of the Commission's REFIT programme and pursuing two declared general objectives: strengthening the Union's cybersecurity capabilities and resilience, and preventing internal-market fragmentation caused by divergent national regimes.

More specifically, and as relevant here, it introduces, among other things, a new ECCF certification system that is potentially selective of providers based on technical and non-technical security criteria alike (Arts. 85 and 100). The proposal also introduces a self-standing framework for the security of the information and communication technology (ICT) supply chain: coordinated Union-level security risk assessments (Article 99), the designation of third countries raising cybersecurity concerns (Article 100), the identification of critical ICT assets (Article 102), mitigation measures applicable to supply chains, including a prohibition on the use of ICT components from high-risk suppliers (Article 103), the identification of high-risk suppliers (Article 104), and, specifically for the mobile, fixed and satellite electronic communications sectors, the ex lege phased removal of components traceable to high-risk suppliers from critical ICT assets (Articles 110 and 111).

Although the two legislative drafts are intended to regulate distinct subject matters, they do not operate on parallel tracks but end up interlocking with one another. Through its authorisation and enforcement provisions, the DNA incorporates the supply-chain requirements laid down by the CSA2 into the regulatory framework governing the provision of electronic communications networks and services. The linking provisions relevant for this purpose are, in particular, four: Article 9(4)(d), Article 20(2)(d), Article 181(4) and Article 196(10).

Article 9(4)(d) of the DNA makes the right to provide electronic communications networks and services, under the general authorisation regime, conditional on compliance with cybersecurity rules, *"including ICT supply-chain requirements under the cybersecurity law that will replace Regulation (EU) 2019/881"*.

Article 20(2)(d) reproduces the same condition with regard to the general authorisation for the use of radio spectrum, providing that undertakings authorised to use radio spectrum are required to comply with the same cybersecurity rules contained in the CSA2, currently under adoption.

Article 181(4) completes the mechanism on the supervisory side, providing that the national regulatory authority of the place where the networks and services are provided may request *"the competent authority designated under the cybersecurity law intended to replace Regulation (EU) 2019/881 to verify compliance with ICT supply-chain security requirements and to share the*

results, where such verification is necessary for the purposes of assessing compliance with the general authorisation conditions under Article 9(4)(d) and Article 20”.

To these provisions is added, on the enforcement side, Article 196(10), which requires the national regulatory authority to revoke the right to provide networks and services, at the request of the competent authority under the CSA2, where the provider fails to comply with the supply-chain security requirements — a mechanism examined in greater detail in Section V, devoted to proportionality and procedural safeguards.

I.2 The Legal Effects of the Linkage Mechanism

I.2.1 The system just described produces a set of interlocking effects, the first of which is the shift from an ongoing compliance obligation to a market-access condition.

Rather than operating as ongoing technical regulatory obligations — to be complied with in the course of business and liable to ex post sanction in the event of breach — cybersecurity obligations become, by virtue of the reference made in Articles 9(4)(d) and 20(2)(d), preconditions for the grant and continued holding of the authorisation to operate on the telecommunications market. The dividing line between ex post regulation of an operator's conduct and ex ante regulation of market access is thereby significantly blurred. In this context, the operational functions assigned to ENISA by the CSA2 and referred to in the DNA at Articles 181(4) and 196(10) become relevant, with an evident risk of overlap with the competences of national authorities and a danger of creating uncertainty in the management of incidents and critical issues.

It should be added that Article 11(4) grants the authorities the power to revoke the right to operate across the entire single market in the event of a “serious breach” of the conditions — a revocation which, from a proportionality standpoint, should remain a measure of last resort (see § V.3 below).

I.2.2 From a different angle, there is a shift in how exclusion risk is assessed, leaving the provider unable to foresee future geopolitical decisions that may affect its market position.

The criteria governing, under Article 100 of the CSA2, the designation of third countries raising cybersecurity concerns — such as the existence of laws requiring the disclosure to state authorities of software or hardware vulnerabilities, or the absence of effective judicial remedies and independent, democratic oversight mechanisms — do not concern verifiable technical vulnerabilities of the individual product or ICT component, but rather whether the provider's ownership and control structure is traceable to a third country regarded as unreliable (see Article 104 of the CSA2).

Factors of this kind, plainly non-technical in nature, can translate, through Articles 110 and 111, into the mandatory replacement of equipment and the progressive exclusion of economic operators from the market — an exclusion that may apply from the outset or arise later, upon the country's inclusion among those deemed unreliable, penalising smaller providers above all.

I.2.3 Third, the mechanism brings about a shift from coordination to centralisation of security-related decision-making.

The designation of high-risk suppliers and the mitigation measures, adopted by the Commission through implementing acts under Articles 103 and 104 of the CSA2, produce, through the reference made by the DNA, direct effects on the right to operate in the internal market for electronic communications.

The result is an at least potential compression of the Member States' ability to determine autonomously the threats to their own national security and to adopt the measures best suited to address them — a danger heightened by the European Commission's excessive recourse to delegated and implementing acts, potentially exceeding the limits set by Articles 290 and 291 TFEU.

I.2.4 Finally, this gives rise to a situation of dynamic legal uncertainty. The content and scope of the authorisation obligations set out in the DNA depend on an instrument — the CSA2 — that is still under adoption, as well as on subsequent secondary legislation (implementing acts under Articles 100, 103 and 104 of the CSA2) that will define its content in concrete terms. The absence of objective, transparent technical criteria may further entail the risk that lists of unreliable entities come to rest on discretionary geopolitical assessments, with attendant risks of indirect discrimination and distortions of competition in the European digital market.

Taken together, these four effects form the premise for the systemic concerns examined in the sections that follow: the soundness of the legal basis under Article 114 TFEU (Section II), respect for the Member States' competence over national security under Article 4(2) TEU (Section III), and the issues of subsidiarity, proportionality, legal certainty and effective judicial protection (Sections IV and V).

*

II. Article 114 TFEU: The Limits of Internal-Market Harmonisation

II.1 The Limits of Article 114 TFEU in the Case Law of the Court of Justice

According to the settled case law of the Court of Justice of the European Union, Article 114 TFEU constitutes the legal basis enabling the Union institutions to adopt harmonisation measures aimed at removing actual or foreseeable obstacles to free movement and at preventing appreciable distortions of competition. It is, however, a functional rather than a general legal basis: as the Court made clear in *Tobacco Advertising I* (Case C-376/98), to interpret Article 114 TFEU "*as meaning that it vests the [Union] legislature with a general power to regulate the internal market would not only be contrary to the very wording of the provisions cited, but would also be*

incompatible with the principle [...] that the [Union's] powers are limited to those specifically conferred on it”¹.

Two corollaries follow from this principle, both relevant for the purposes of this analysis.

The first is that the mere finding of disparities between national rules, or the abstract risk of obstacles to fundamental freedoms, is not enough to justify recourse to Article 114 TFEU: the regulatory divergences must be such as to have a direct effect on the functioning of the internal market, or to create appreciable distortions of competition.²

The second is that, where the measure is intended to prevent future obstacles to trade resulting from the heterogeneous development of national legislation, the emergence of such obstacles must be likely, and the measure must specifically be designed to prevent them.³

The case law on the two Tobacco Advertising cases remains paradigmatic on this point. In Case C-376/98, the Court annulled Directive 98/43/EC for lacking a sufficient connection with the internal market, finding that its real aim was the protection of public health. In the subsequent Case C-380/03, by contrast, the Court held Directive 2003/33/EC to be lawful, since it was confined to forms of advertising with a genuine cross-border dimension and therefore capable of affecting trade and competition. The criterion distinguishing the two outcomes is the now well-established “centre of gravity” test: review of the correctness of the legal basis rests on objective factors, including the aim and content of the measure itself,⁴ and recourse to Article 114 TFEU is lawful only where the internal market constitutes the true centre of gravity of the legislative intervention.

II.2 The Centre of Gravity of the Linkage Mechanism and Non-Technical Criteria

Applying this framework to the linkage mechanism described in Section I, a first element of tension emerges.

The DNA, taken as a whole, pursues objectives proper to internal-market harmonisation: standardising authorisation conditions, reducing fragmentation in spectrum management, and simplifying multi-State access through the single passport. The conditions listed in Article 9(4) are, in their generality, technical or organisational in nature: network resilience, technical standards, interconnection, and efficient use of resources.

Points (d) of Articles 9(4) and 20(2), however, do not merely refer to cybersecurity requirements in the technical sense. Through their reference to the CSA2, they do nothing other than import into the DNA's authorisation regime the non-technical reliability-assessment criteria set out in

¹Court of Justice of the European Union, judgment of 5 October 2000, Case C-376/98, Germany v Parliament and Council, ECR I-8419, paragraph 83.

²Court of Justice, Case C-58/08, Vodafone, paragraph 32; Case C-380/03, Tobacco Advertising II, paragraphs 37 et seq.; Case C-376/98, Tobacco Advertising I, paragraphs 84 and 106.

³Court of Justice of the European Union, judgment of 13 July 1995, Case C-350/92, Spain v Council, ECR I-1985, paragraph 35; judgment of 9 October 2001, Case C-377/98, Netherlands v Parliament and Council, ECR I-7079, paragraph 15.

⁴Court of Justice, Case C-376/98, Tobacco Advertising I, paragraph 83.

Article 100 of the CSA2, by which the cybersecurity draft regulation proposes to identify the third countries deemed unreliable to which an economic operator may be found to be connected.

This is, to use a formula already employed in the analysis of the CSA2, a “politico-institutional” judgment on the reliability of a foreign legal order, not a technical assessment of a product, a component, or an economic operator.

Where restrictions on access to the electronic communications market rest, through the DNA's cross-reference, predominantly on nationality, ownership structure, the third country's regulatory framework, or geopolitical assessments, the centre of gravity of the regulatory intervention risks shifting beyond ordinary internal-market harmonisation. In other words, while the core of the DNA remains firmly anchored in internal-market logic, the specific portion of the authorisation regime that absorbs, by reference, the CSA2's non-technical criteria is exposed to the very same doubt as to the legitimacy of the legal basis that arises, upstream, for the CSA2 itself.

II.3 Harmonising Cybersecurity — Competence over National Security

In light of the foregoing, it may be said that, while Article 114 TFEU is not in itself a bar to establishing a common cybersecurity framework, the principles underpinning the European legal order prevent any legislative intervention from using cybersecurity as a vehicle for introducing market-access criteria based on geopolitical reliability assessments.

In light of the case law cited, uniform technical resilience standards, security requirements for ICT products and services, and risk-management obligations fall, without strain, within the harmonising function of Article 114 TFEU, as they concern technical vulnerabilities that are objectively verifiable and common to the internal market.

The position is different where the same legal basis is used to condition market access on geopolitical reliability assessments of a supplier or a third country, and to derive from these direct consequences for the right to operate in the electronic communications market. Competence over national security has not been conferred on the Union by the Treaties — it remains, as will be seen in Section III, reserved exclusively to the Member States under Article 4(2) TEU — and Article 114 TFEU cannot, by definition, make up for that absence of conferral.

The risk, for the DNA as already for the CSA2, is that the breadth of the formula “internal-market harmonisation” is stretched to cover an intervention which, by its content and purpose, belongs to a different, non-conferred area of competence.

*

III. National Security as the Sole Responsibility of the Member States

III.1 The Limit of Competence under Article 4(2) TEU and the Principle of Conferral under Article 5 TEU

Having established this, the DNA regulation proposed by the Commission, as supplemented by the rules under adoption in the CSA2 proposal, raises concerns with regard to the principle of conferral.

Article 4(2) TEU provides that the Union shall respect the essential State functions, *"including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security"*, and states expressis verbis that *"in particular, national security remains the sole responsibility of each Member State"*. This is a competence that the Treaties have not conferred on the Union and that, by virtue of the principle of conferral under Article 5(2) TEU already referred to, the Union cannot exercise, whatever legal basis is formally invoked.

A second, procedural element must be added to this. Should determinations on high-risk suppliers and third countries go beyond the nature of technical requirements and qualify — by their substantive content — as foreign and security policy decisions, they would fall within the scope of the Common Foreign and Security Policy (CFSP), governed by Title V TEU, which provides for a decision-making mechanism specific to, and distinct from, the Community method: a mechanism based on intergovernmental cooperation, in which unanimity within the Council remains the general rule (Articles 24 and 31 TEU), subject to the limited exceptions provided for therein.

Recourse, for the same determinations, to Commission implementing acts adopted by qualified majority under the examination procedure — as occurs for the designation of problematic third countries under Article 100 of the CSA2 and for the identification of high-risk suppliers under Article 104 — therefore risks circumventing not only the allocation of competences between the Union and the Member States, but also the decision-making mechanism that the Treaties reserve specifically for determinations of a politico-strategic nature in security matters.

III.2 National Security and the Principle of Proportionality: The Need for Judicial Review

Even assuming, for the sake of argument, that a measure restricting access to the electronic communications market could legitimately be justified by security requirements — along the lines of the derogations under Article 52(1) TFEU, itself referred to in Article 9(1) of the DNA — such a measure would nonetheless remain subject to the ordinary test of necessity and proportionality developed by the case law of the Court of Justice.⁵

Under that case law, reliance on grounds of security or public order cannot justify measures that in reality pursue industrial-policy objectives or the protection of the internal market; and a restriction based on generic, geopolitical, non-technical criteria, absent any concrete demonstration of a link between the provider's origin and an actual risk to network security, is liable to be disproportionate.

⁵Court of Justice, Case C-331/88, Fedesa, paragraph 13; Case C-58/08, Vodafone, paragraph 51.

In this respect, the combined provisions of the DNA and the CSA2 outline a set of measures that are excessive in relation to the objectives pursued, since they are based on criteria not directly related to technical risks and could be replaced by less restrictive instruments.

Moreover, this proportionality review cannot be separated from effective judicial protection. For a measure restricting market access or the use of an asset to be lawful, it must remain subject to judicial review, which must assess not only the measure's procedural compliance but also its substantive proportionality in relation to the risk actually established.

III.3 Advocate General Ćapeta's Opinion in Elisa Eesti

A recent test of these principles is offered by the Opinion of Advocate General Ćapeta of 19 March 2026 in Case C-354/24, *Elisa Eesti AS v Estonian Government Security Committee*,⁶ concerning the limitation, on security grounds, of an authorisation granted to a provider to use certain hardware and software.

The Advocate General's Opinion confirms, first of all, a matter of principle: Member States may, in principle, restrict the use of specific telecommunications equipment on grounds of national security — which presupposes, consistently with what was observed in the preceding section, that such an assessment falls in the first instance to the competent national authority, rather than to the Commission through the centralised designation of a supplier or a third country.

Such a decision, however, cannot rest on generalised suspicion directed at a supplier as such, or at its origin in a given third country. It must instead be based on an assessment of the specific equipment concerned, its position within the network, its intended use, and the risks concretely associated with it — and must in any event remain subject to effective judicial review, including a proportionality assessment. This is also the direction taken by the Advocate General's statement that, in reviewing the measure, the national court may take into account risk assessments carried out both by the Union institutions and by national bodies, where their respective security interests converge⁷ — which presupposes, upstream, that it is in any event the national court, and not a Commission implementing act, that is called upon to decide on the individual restrictive measure. The contrast with the architecture of the CSA2 is, at this point, difficult to overlook. The mechanism under Articles 100 and 104 of the CSA2 designates entire third countries and entire suppliers on the basis of structural, non-technical criteria — including the identified absence of effective judicial remedies or of independent, democratic oversight mechanisms in the country of origin, and the supplier's ownership or control structure — rather than on the basis of a case-by-case assessment of the risk posed by the individual component or item of equipment in the specific

⁶Opinion of Advocate General Ćapeta of 19 March 2026, Case C-354/24, *Elisa Eesti AS v Estonian Government Security Committee* (case pending before the Court of Justice).

⁷Opinion of AG Ćapeta, Case C-354/24, cited above, § 115: «Where, as in the present case, there is a convergence between the security interests concerned at Union and at national level, a national court may also take into account — within the framework of judicial review of the measure at issue — the risk assessments carried out by the institutions and bodies of the Union as well as by national bodies.»

context in which it is intended to operate. This is precisely the approach that the Advocate General's reasoning in *Elisa Eesti* appears to place in tension with the principle of proportionality. And since, by virtue of the linkage mechanism described in Section I, that centralised designation automatically translates — through Articles 9(4)(d), 20(2)(d) and 110-111 of the CSA2 — into a condition for access to the electronic communications market, the deficit of individualisation found upstream, in the CSA2 designation, is transmitted in full downstream, into the DNA's authorisation regime.

*

IV. Subsidiarity and the Existing Italian Framework

IV.1 The Possible Breach of the Principle of Subsidiarity

From a different angle, similar concerns arise with regard to the principle of subsidiarity, enshrined in Article 5(3) TEU.

That principle, as is well known, requires that, in areas which do not fall within its exclusive competence, the Union act only if and insofar as the objectives of the proposed action cannot be sufficiently achieved by the Member States, but can — by reason of the scale or effects of the action — be better achieved at Union level. The subsidiarity test therefore requires a twofold verification: the necessity of EU action, on the one hand, and the added value that such action would bring compared with the instruments already available at national level, on the other.

As to the first aspect, it has not been shown that such a centralised intervention is necessary in view of the competences and instruments already available at national level, as indeed noted by the XIV Committee of the Chamber of Deputies, which criticised the choice of a Regulation over a Directive, considering it detrimental to the flexibility needed to manage the profound differences between national markets, particularly in sensitive areas such as security and lawful interception. As to the second aspect, there are numerous examples of legislation and/or regulatory instruments effectively adopted at national level in this field. One example above all is the French regime governing the use of the special share instrument, commonly known as the *golden share*, which forms part of the legal arsenal adopted to complete control over strategic assets by combining administrative control instruments with corporate-law ones.

On this point, the existing Italian regulatory framework on the security of electronic communications networks likewise merits closer examination.

IV.2 The Golden Power Regime and Its Extension to 5G

The Italian legal system has long had an instrument specifically designed to subject to State control transactions and contracts capable of affecting the security of strategic infrastructure: the special powers regime ("golden power"), introduced by Decree-Law No. 21 of 15 March 2012, converted with amendments by Law No. 56 of 11 May 2012.

This regime, originally conceived for the defence and national-security sectors and for energy, transport and communications infrastructure, has been progressively extended to high-technology sectors (see Decree-Law No. 148 of 16 October 2017).

With Decree-Law No. 105 of 25 September 2019, converted by Law No. 133 of 18 November 2019, the legislature introduced rules specifically dedicated to 5G technology, requiring operators of electronic communications networks to notify the Prime Minister's Office of their intention to enter into contracts or agreements for the acquisition of goods or services relating to the design, implementation, maintenance or management of networks connected with the roll-out of 5G technology, where the contracting counterparty is an entity established outside the European Union.

At the end of the review process, the Government may, by decree of the Prime Minister adopted on a resolution of the Council of Ministers, exercise a power of veto over the individual contract, or — and this is the aspect of greatest interest for the present analysis — impose specific conditions and requirements on the individual contract, calibrated to the component or equipment concerned, to the network function it is intended for, and to the risk actually identified during the review.

The exercise of this power is not entrusted to a single authority, but is distributed among several bodies, each with a distinct and complementary role. The Prime Minister's Office holds political responsibility and the final decision-making power on golden power matters, adopted by prime ministerial decree at the conclusion of the review process, coordinated by the inter-ministerial group established for that purpose within the Office itself. The Ministry of Enterprises and Made in Italy (MIMIT), as successor to the former Ministry of Economic Development, retains an investigative and liaison role with operators in the electronic communications sector, in addition to its general competence over industrial policy for the sector. The National Cybersecurity Agency (ACN), established by Decree-Law No. 82 of 14 June 2021 as the national reference authority for cybersecurity, provides the technical risk assessment within the 5G golden power review, and simultaneously administers the National Cybersecurity Perimeter under the aforementioned Decree-Law No. 105/2019, which identifies public and private entities operating in strategic sectors and subjects their most critical ICT assets to a preventive security assessment. AGCOM, lastly, remains the regulatory authority for the electronic communications sector proper — the Italian equivalent of the national regulatory authority referred to in the DNA — competent for the general authorisation regime, spectrum assignment and market analysis, but without a direct role in assessing national-security matters, which is reserved to the bodies indicated above.

IV.3 A Model Calibrated to the Individual Case

What matters, for present purposes, is the very structure of the mechanism thus outlined.

The Italian regime does not operate by general categories — that is, it does not exclude a supplier from the entire market on account of its nationality or origin — but instead allows the competent

authority to intervene on the individual contract, component and network function concerned, on the basis of the risk actually identified at the conclusion of the review.

Alongside an outright prohibition, the measures available to the Government include a range of intermediate requirements — enhanced security conditions, monitoring obligations, functional limitations — allowing for a proportionate, tailored response, rather than the indiscriminate exclusion of an entire supplier from every segment of the market.

It is, in other words, a model that displays exactly the features of individualisation and proportionality referred to in Section III with regard to the position taken by the Advocate General in *Elisa Eesti*: an assessment anchored to the contract, the equipment, its function within the network and the specific risk, rather than to a structural, category-based designation of the supplier or its country of origin.

IV.4 The Implications of Golden Power for Subsidiarity

If the Italian legal system already has an instrument capable of pursuing the objective of network security through a selective, proportionate and institutionally tested mechanism — involving, in a coordinated design, the Prime Minister's Office, MIMIT, the ACN and, for ordinary regulatory matters, AGCOM — it becomes necessary to ask seriously what added value the centralised designation mechanism provided for by the CSA2, and incorporated into the DNA through Articles 9(4)(d), 20(2)(d) and 181(4), would be capable of bringing compared with the national instruments already in operation.

Otherwise, the risk is that the Union's intervention will not merely fill a regulatory gap, but will superimpose on the national assessment — case-specific and proportionate to the particular concern — a structural, category-based designation that the Italian legal order has thus far deliberately avoided adopting as its exclusive model. Such an overlap would raise not only a problem of duplicated administrative burdens for operators, who would have to contend with two layers of control not necessarily coordinated with one another, but also a more fundamental question as to compliance with the necessity criterion for EU action, where the declared objective — the security of electronic communications networks — is already being adequately pursued at national level through more targeted instruments.

*

V. Proportionality, Legal Certainty and Judicial Safeguards

V.1 Suitability and Necessity

The principle of proportionality, as developed by the settled case law of the Court of Justice, requires a three-tier assessment: the suitability of the measure to achieve the objective pursued, its necessity — understood as the absence of equally effective, less restrictive alternatives — and

proportionality in the strict sense, that is, the correct balance between the burdens imposed and the benefits pursued.⁸

Applied to the DNA-CSA2 linkage mechanism, this three-tier test requires the cybersecurity benefits pursued to be weighed against a range of competing interests: internal-market freedoms (Arts. 34-36 TFEU), the freedom to conduct a business and the right to property protected by Articles 16 and 17 of the Charter, the sunk costs already incurred by operators, the costs of accelerated replacement imposed by rigid timetables, and the risk — paradoxical in light of the stated objective — of a concentration of supply in favour of a handful of “approved” suppliers, to the detriment of supply-chain diversification.

One aspect that deserves particular attention concerns the allocation of the economic costs of any forced replacement of suppliers. The question arises whether such costs should fall on suppliers, network operators, consumers, the budgets of the Member States, or the Union.

The text of the legislation offers a significant indication on this point.

Article 195 of the DNA recognises, as a general rule, that holders of spectrum-use rights revoked before expiry are entitled to adequate compensation for the direct costs of migration or spectrum reassignment, in accordance with national law — but does so “*without prejudice to Article 196(10) and (11)*”, thereby expressly excluding from that guarantee precisely those cases of revocation connected with a breach of the CSA2 supply-chain security requirements.

It follows that, should the DNA-CSA2 framework require Italy to implement a mandatory supplier phase-out without any Union-level cost-sharing, compensation or financial-support mechanism being provided, the resulting burdens — compensation claims by operators, litigation, and any national support measures — risk ultimately falling on the Italian public budget.

Even leaving aside whether the measure should be classified as expropriatory — a classification which, as seen in Section III with reference to the Advocate General's Opinion in *Elisa Eesti*, the European approach tends in any event to exclude, preferring instead the category of limitation on use — the costs of replacement may nonetheless generate broader public-finance effects and social costs: through State support measures for affected operators, through reduced network investment resulting from the need to devote resources to forced replacement rather than infrastructure development, through delays in the roll-out of next-generation networks — in tension with the very Gigabit and Digital Decade objectives that the DNA claims to pursue — and, ultimately, through higher consumer prices.

V.2 Legal Certainty

The issue of legal certainty, already addressed with reference to the “moving clause” nature of Articles 9(4)(d) and 20(2)(d) of the DNA, is compounded at this stage of the analysis by a further concern: the overlap of two distinct bodies of secondary legislation, both still in the making.

⁸See footnote 5 above.

On the one hand, the substantive content of the authorisation obligations depends on the implementing acts which the CSA2 confers on the Commission for the designation of problematic third countries (Article 100), the identification of high-risk suppliers (Article 104) and the definition of phase-out periods for fixed and satellite networks (Article 110(4) and (5)). On the other hand, the DNA itself confers on the Commission a broad catalogue of delegations — including, by way of example, those under Articles 22(3), 39(4)(f), 82(1), 103(5), 106(8) and 114 — granted, under Article 198, for a period of five years, tacitly renewable unless opposed by the European Parliament or the Council.

This dual and concurrent layering of secondary legislation makes it particularly difficult for an operator to assess *ex ante* the actual scope of its authorisation obligations and, consequently, to plan its investments with an adequate degree of predictability — precisely the predictability that the Court's case law requires for rules affecting the exercise of fundamental freedoms.

The risk, already flagged by the 14th Committee of the Italian Chamber of Deputies, is that the systematic use of delegated and implementing acts may exceed the limits set by Articles 290 and 291 TFEU, shifting to fora that lack the participatory and transparency safeguards of the ordinary legislative procedure the task of defining elements that directly affect the right to operate on the market.

V.3 Procedural Safeguards and Effective Judicial Protection

Article 196 of the DNA sets out, as a general rule, a procedural sequence that is in the abstract respectful of the right to be heard, consisting of a finding of non-compliance, notification to the undertaking, an opportunity for the latter to submit observations, a formal notice to cease the breach and, only as a measure of last resort in cases of serious or repeated breaches, suspension or revocation of rights.

Paragraph 10 of the same article, however, appears to depart from that sequence: at the request of the competent authority designated under the future cybersecurity law, the national regulatory authority *"shall revoke the right to provide networks and services under a general authorisation or individual rights of use of radio spectrum [...] where the provider fails to comply with ICT supply-chain security requirements"*. The wording used — a duty to revoke, not a discretionary power — deprives the national regulatory authority of the discretion needed to assess, in the specific case, the proportionality of the measure or the suitability of less restrictive mitigation solutions, such as audits, remediation plans or scheduled replacements.

This automatism also has repercussions for judicial protection.

Article 197 of the DNA grants any undertaking affected by a decision of the competent authority the right to lodge an appeal before an independent body; it specifies, however, that *"pending the outcome of the appeal, the decision of the competent authority shall remain in force, unless interim measures are granted in accordance with national law"*.

The provision, in other words, does not guarantee an automatic suspensive effect at the level of Union law, but leaves entirely to national law — with the resulting divergence between Member States that this may produce — the decision whether or not to grant interim protection in the meantime. In a capital-intensive sector such as electronic communications, the immediate enforceability of a revocation based on Article 196(10) thus exposes the undertaking to the risk of irreversible economic harm even before the court has ruled on the merits of the dispute.

The connection with what was observed in Section III regarding the Advocate General's Opinion in *Elisa Eesti* is unmistakable.

If judicial review of a restrictive measure based on security grounds must genuinely be capable of extending to a substantive proportionality assessment — and if that assessment presupposes that the authority adopting the measure has itself exercised a margin of discretionary judgment in the specific case — the automatism introduced by Article 196(10) of the DNA risks hollowing out that review at its root: there is, upstream, no discretion on the part of the national regulatory authority over which the court could exercise its proportionality scrutiny, since the revocation appears to follow, almost automatically, from the mere request of the authority designated under the CSA2.

*

VI. Italy's Qualified Position and Stakeholder Views

VI.1 The Chamber of Deputies and the Senate

Under Article 12 TEU, the Italian Parliament has begun examining the DNA proposal in order to verify its compliance with the principles of subsidiarity and proportionality.

The XIV Standing Committee (European Union Policies) of the Chamber of Deputies concluded its examination at the sitting of 4 June 2026, approving an assessment document that showed cross-party agreement, on the part of almost all political groups, on the concerns identified.

The document adopted acknowledges, in principle, the value of coordinated action at Union level in the electronic communications sector, but does not translate into unconditional endorsement of the proposal's overall design.

The main reservations concern: the choice of legislative instrument — a directly applicable Regulation, rather than a Directive, which was considered better suited to preserving the flexibility needed to manage the profound differences between national markets, particularly in sensitive areas such as security and lawful interception; the excessive use of delegated and implementing acts to define substantive elements of the framework, with a resulting reduction in legal certainty for operators; the centralisation of spectrum and numbering-resource management, which would diminish the role of national regulatory authorities and divert resources from Member States' budgets; the rigidity of the copper switch-off obligation by 2035; and the need to update the net-neutrality paradigm. With specific reference to the cross-reference made by Article 9(4)(d), the

Chamber also expressed concern about the assignment to ENISA of operational functions potentially overlapping with those of national authorities, and called — perhaps the point of greatest relevance for the present contribution — for objective, transparent technical criteria for the designation of high-risk suppliers, in order to prevent such lists from resting on discretionary geopolitical assessments, with the attendant risk of indirect discrimination and distortions of competition in the European digital market, as well as for a revision of the timetables for replacing components from high-risk suppliers (36 months for mobile networks), considered more restrictive than the national golden power regime and potentially liable to impose disproportionate economic burdens on undertakings, particularly SMEs.

VI.2 Discussions within the Council

Within the Council, technical examination of the proposal continues within the competent working party. At present, what is documented is that several national delegations — including France, Germany and Italy — have already expressed reservations about the need to preserve national flexibility, calling for the choice of legislative instrument to be reconsidered in favour of the more flexible Directive; neither the European Parliament nor the Council has yet approved the text of the proposal at first reading.

The issues that, by their nature, appear set to form the backbone of the discussion within the working party fall into categories largely already identified in the preceding sections, in particular: the allocation of competences between the Union and the Member States, with specific regard to national security; the proportionality of the measures envisaged, particularly as regards the absence of risk gradation by network segment; the interaction between the DNA and the other instruments of the cyber package, in particular the CSA2 and the NIS2 Directive, in respect of which there is a need for coherence and non-duplication of compliance burdens; and the extent of recourse to secondary legislation, a theme common to the reservations expressed at national level and one that appears set to be the subject of negotiation within the Council.

VI.3 Stakeholders Positions

Similar reservations have been expressed by numerous stakeholders in the hearings conducted by the Italian Parliament.

The Italian Internet Providers Association (AIIP) submitted a position paper to the XIV Committee of the Chamber of Deputies on 22 May 2026. AIIP — which represents more than 60 undertakings, mostly small and medium-sized, with a strong territorial presence — noted that the DNA brings about a centralisation of powers in the hands of the Commission to the detriment of the Member States, national regulatory authorities and the market, through a “pre-packaged and rigid” framework lacking adequate consideration of the specific features of individual national markets, and criticised, among other things, the undifferentiated copper switch-off obligation by 2035 and the removal of spectrum management from the jurisdiction of the Member States.

With specific reference to the linkage with the CSA2, the position expressed by AIIP converges significantly with the central thesis of this contribution. The Association observed, in its own words, that *"the identification of vendors designated as high-risk is not truly a cybersecurity measure, which is based on technological criteria and elements, but rather one of national security, based on geopolitical assessments, and as such, in application of the principle of subsidiarity, should be judged by each Member State rather than by the Commission (which, in this respect, would not have the necessary powers)"*.⁹ AIIP proposed, as its primary position, the adoption of a Directive rather than a Regulation, and, in the alternative, an amendment to the text restoring greater discretion to the Member States and national regulatory authorities. Lastly, the Association expressed concern about the introduction, among the DNA's objectives, of a new "competitiveness" criterion that risks degrading competition to a mere instrument rather than an end in itself, favouring market-concentration dynamics to the detriment of SMEs in the sector.

*

VII. Conclusions

VII.1 In light of the foregoing considerations, it may be concluded that the cross-references between the DNA and the CSA2 do not merely impose on market operators compliance with requirements of a purely technical nature. As set out in Section I, through Articles 9(4)(d), 20(2)(d), 181(4), and — on the enforcement side — 196(10) of the DNA, supply-chain determinations adopted under Articles 100, 104, 110 and 111 of the CSA2 may translate into direct legal restrictions on market access, on spectrum-use rights and on business continuity, based on assessments of a political nature.

The linkage mechanism thus described is not, therefore, a mere technique of normative cross-reference between two sectoral instruments of neutral scope, but rather a regulatory framework that allows the Commission to affect national security assessments reserved to the Member States (§ III), shifting the centre of gravity of the decision — and, with it, the allocation of power — from the national level to that of the Union.

VII.2 It has been noted that the DNA should refer exclusively to cybersecurity obligations that are already in force, sufficiently precise, and legally binding. As observed in Sections I and V, the current wording of Article 9(4)(d) constitutes a "moving clause" whose content depends on an instrument — the CSA2 — that is still under negotiation, as well as on subsequent secondary legislation that is no less uncertain.

A reference of this kind undermines the predictability of the rule for operators in the sector and exposes them to a regulatory risk they cannot assess ex ante. The dynamic incorporation of an unstable legal framework should therefore be avoided, in favour of a reference to primary-law

⁹Italian Internet Providers Association (AIIP), position paper submitted to the XIV Committee (European Union Policies) of the Chamber of Deputies, 22 May 2026.

provisions already consolidated within the Union legal order, which remain preferable to second-tier regulatory instruments that end up curtailing democratic control mechanisms.

VII.3 National security must remain the exclusive responsibility of the Member States. As set out in Section III, Article 4(2) TEU reserves to the Member States the ultimate assessment of whether a threat to their national security exists, as well as the final decision whether to impose restrictions on suppliers or require the removal of specific equipment on the basis of that assessment. The existing Italian regulatory framework — the golden power regime, discussed in Section IV, and the coordinated role of the Prime Minister's Office, MIMIT, ACN and AGCOM — demonstrates that this responsibility can be effectively exercised at national level, with a degree of calibration that a centralised designation could hardly replicate.

Insofar as such measures amount, in substance, to foreign and security policy determinations, they should fall within the scope of the CFSP and be adopted unanimously, as the Treaties provide for that field.

VII.4 Restrictions should be based on risk assessments referring to the individual asset and the individual function, not on category-based designations or lists drawn up according to political evaluation criteria. As emerges from the position taken by the Advocate General in the *Elisa Eesti* case, examined in Section III, and as is confirmed, consistently, by the very structure of the Italian golden power regime examined in Section IV, any restrictive measure should be anchored to the specific component, the network function concerned, the context of use and the risk concretely demonstrated — not to nationality, ownership structure, or affiliation with a third country considered as such. It is precisely the absence of this individualisation — inherent in the category-based designation mechanism provided for by Articles 100 and 104 of the CSA2 — that constitutes, as shown in Section V, the principal point of friction with the principle of proportionality and with the fundamental principles of the EU legal order.

VII.5 Substantive political determinations concerning third countries and high-risk suppliers should require a unanimous decision within the Council. Since these are assessments of an essentially geopolitical rather than technical nature, their adoption through implementing acts by qualified majority appears difficult to reconcile with the nature of the underlying subject matter and with the Treaties.

Consistently with Article 24 TEU, only unanimity would ensure that choices of such political significance receive the endorsement of all Member States, rather than that of a mere qualified majority within an implementing committee.

VII.6 In light of the foregoing considerations, it appears desirable to remove the DNA provisions that establish the linkage with the CSA2, insofar as such linkage may give rise to barriers for operators based on non-technical assessments. This would entail the deletion of Article 9(4)(d); Article 20(2)(d); Article 181(4); and, consequently, of the reference to those same

provisions contained in Article 196(10) of the DNA, insofar as it underpins the enforcement apparatus.

A mere reformulation of the reference to the cybersecurity framework would not suffice to eliminate the structural defect identified above, since it would continue to link an instrument of market harmonisation (the DNA) to a framework (the CSA2) that appears centred on objectives of a political nature going beyond the mere functioning of the market.

Absent such intervention, the risk is extensive litigation on multiple fronts: before the Court of Justice, under Article 263 TFEU, for lack of competence arising from a distorted use of Article 114 TFEU; by way of preliminary reference, under Article 267 TFEU, in the context of disputes pending before national courts; and, not least, on the plane of fundamental rights enshrined in the Charter and the ECHR, given that the CSA2 measures could affect the freedom to conduct a business, the right to property and the principle of non-discrimination, with possible review by national courts and, ultimately, by the ECtHR. This is without even accounting for possible issues of unconstitutionality under the domestic law of the Member States.

From this perspective, the model currently outlined appears to move away from the multilevel system in which the Union stands alongside — without wholly displacing — the national legal orders, which remain the linchpin of industrial and security policy, in an arrangement more consistent with the Treaties and more respectful of national specificities. The reform of the DNA should therefore pursue a balance between the Union level and the national level, grounded in horizontal cooperation and in regulatory instruments suited to the transnational nature of digital phenomena, rather than in a purely centralising direction.

Avv. Giuseppe Libutti

Avv. Michele Trotta

Prof. Avv. Sergio Santoro