EUROPEAN LAW BLOG
NEWS AND COMMENTS ON EU LAW

ELB Blogpost 6/2023, 1 February 2023
Tags: cybersecurity, EU competence, market harmonisation
Topics: Data Protection and Digital Governance

Cybersecurity for Europe without a legal basis?

By Giacomo Delinavelli

As the European Commission is committed to ensure the digital transformation of Europe by 2030, cybersecurity policy is taking a special place. As part of this effort, recently, the Network and Information Security (NIS2), Digital Operational Resilience Act (DORA), the Resilience of Critical Entities (RCE) have entered in force and the Cyber Resilience Act (CRA) has been proposed. However, in consideration of the conferred nature of the supranational powers, it is worth discussing to what extent the EU has the mandate to act in this field without a proper cybersecurity competence being stated in the Treaties. The new cybersecurity legislation has been proposed and approved by relying on the 'internal market harmonisation' legal basis, i.e., Art. 114 TFEU. However, in consideration of the proactive approach the Commission has taken in this field and the complex nature of cybersecurity policy, I argue that, although the legitimacy of such legislation is hard to be disputed, the attribution of a specific competence to be conferred to the EU, even by amending the Treaties, would clarify – and better justify – the prominent role that the EU has taken in this area.

Policy background

Cybersecurity aims at ensuring the integrity of information and networks, and in a digitised society, this means to ensure its continuous functioning. Securing information and networks has effects on (almost) every aspect of our society: from healthcare to private communications, from education to defence, etc. From an external or geopolitical perspective, a high level of cybersecurity means ensuring protection against cyber-attacks coming from hostile nations, as well as providing for a high level of autonomy for important and critical infrastructures and (knowledge) systems. The scope of cybersecurity policy in a digitised society concerns

investments in infrastructures and systems, the development of digital capabilities and specific technical skills, as well as cross border coordination and common regulatory frameworks.

The Commission's efforts for the broader digitisation of Europe are outlined in its policy initiative 'Europe's Digital Decade 2030'. The language used in this communication clearly pitches 'Europe' as paving its own way to the digital realm on a variety of topics, from Artificial Intelligence to data sharing, from hyper connected devices to quantum computing. Europe's decade is juxtaposed to developments in, say, the USA and China. The underlying idea is that only a united Europe, with a holistic approach to digital development, can and will be able to cope in the global arena.

In this context, cybersecurity is a key enabler of the European Digital Decade. And the legislation mentioned above is a key piece of the puzzle. These cybersecurity laws cover information networks and digital products and impose security requirements and mandatory conducts on manufactures of digital products and Member States for their "critical entities". These laws have as their main policy objective the enhancement of European cybersecurity, which the Commission is *proactively* leading. And despite the fact that these instruments have all been proposed on a market harmonisation rationale and, for that matter, on Art. 114 TFEU, it would be reductive to justify this legislation only with the aim of removing (or preventing likely) obstacles to the freedoms enshrined in the Treaties.

The use and limits of Art. 114 TFEU for cybersecurity

The need to specify a legal basis for the proposition of new legislation derives from the principle of conferral of powers, as stated in Art. 5(2) TEU. Accordingly, the Union can only legislate when the Member States have vested the EU with the power to do so, in correspondence of a specific policy area envisaged in the Treaties. In the EU legal system, some legal bases are linked to rather specific policy areas, e.g. environment at Art, 11 and 191-193 TFEU and transportation at Art. 90-100 TFUE, whereas others, also known as *functional competences*, lend themselves to a more general scope of measures, such as the 'internal market' competence at Art. 114 TFEU or the residual competence at Art. 352 TFEU.

Due to its broad wording and interpretation, and its procedural advantages, Art. 114 TFEU has become the go to legal basis for a variety of legislative actions. In 70 years of EU law, the substantive limits of this legal basis have been put to the test several times. And it was not until the *Tobacco Advertising case* that the European Court of Justice set the general (abstract) limits for the use of this legal basis. The Court affirmed that a simple disparity in national laws would theoretically not be enough to justify the use of the internal market competence. The disparity must either constitute an obstacle to trade across the Union or lead to some appreciable distortion of competition. And although Art. 114 TFEU can be used to address future disparities, 'the emergence of such obstacles must be likely and the measure in question must be designed to prevent them' [Tobacco Advertising, para. 86].

Moreover, Art. 114 TFEU has been already used to – indirectly – address security issues across the Union. For instance, the Directive on control of the acquisition and possession of weapons is

based on Art. 114 TFEU, as well as the invalidated electronic communications data retention Directive from 2006, also relied on it.

The use of Art. 114 TFEU to pursue cybersecurity initiatives did not come without controversy. In 2006, the United Kingdom contested the use of the internal market competence for the establishment of the European Network and Information Security Agency (ENISA). At the time, the UK pointed out that Art. 114 TFEU (previously, Art. 95 EC) confers "the power to harmonise national laws and not one which is aimed at setting up Community bodies and conferring tasks upon such bodies." However, **according to the Court of Justice, the Treaty intended to confer on the Community legislature a discretion when using Art. 114 TFEU, in particular in fields with complex technical features** (para 43). Moreover, in considering that the area of technology is rapidly expanding, divergences from Member States are to be expected (para 61), and preventing the emergence of disparities likely to create obstacles to the smooth functioning of the internal market in the area (para. 62) justifies the use of Art. 114 TFEU. Yet, in 2019, ENISA received a fresh mandate on the Cybersecurity Act to deal with cybersecurity attacks that increasingly occur across national borders. Unsurprisingly, also this mandate relies on Art. 114 TFEU as legal basis.

During the years, Member States have pointed out the limits of Art. 114 TFEU to pursue additional policy objectives other than the harmonisation of the internal market. Often, Art. 352 TFEU was proposed as a possible alternative to the use of 114 TFEU. Indeed, the "residual competence" of the EU is meant to be used for the adoption of acts necessary to attain objectives laid down in the Treaties, when the necessary powers of action are not (explicitly) provided for in the Treaties. Nevertheless, this legal basis requires the Council to act unanimously and, to point out the lack of an explicit legal basis for the pursuit of certain policies, including health, working time, or setting up a cybersecurity agency, has been a way for Member States to limit the expansion of powers from the European Union.

However, as explained by Weatherill in his investigation of how the European Court of Justice (ECJ) guards the limits of Art. 114 TFEU, he concludes that the ECJ´s generous interpretation is mainly due to the language adopted in the Treaties and the concept of internal market, which is simply broad. How concretely the new cybersecurity legislation has an effect on the removal of actual legislative barriers for the smooth functioning of the internal market, or have the likely effect to prevent the emergence of new ones, is still (and hard) to be demonstrated.

NIS2, DORA, RCE and CRA

The new cybersecurity legislation, namely NIS2 Directive, DORA and RCE Directive, is primarily aimed at enhancing the resilience of critical entities from cyber-attacks. The **NIS2 Directive** mandates Member States to identify critical and important entities and to establish for the identified organisations a set of mandatory security and reporting obligations. Compared to the previous NIS Directive, adopted in 2016, the scope of the legislation is broader, touching upon several critical sectors, such as energy; transport; banking; financial market infrastructures; health, drinking water; waste water; digital infrastructure; public administration and space.

DORA is another piece of cybersecurity legislation, which can be considered as a subset of NIS2. It specifically concerns security of ICT systems used by financial entities such as banks, insurance companies and investment firms. This regulation provides for a common framework to ensure "digital resilience" of the system that ensures monetary exchanges across Europe and beyond. Finally, the **Resilience of Critical Entities Directive** mandates Member States to establish a cyber security strategy that provides for the identification of critical infrastructures.

An additional paradigmatic case is represented by the proposed **Cyber Resilience Act**, which combines a consumer protection rationale (i.e. improving consumers' confidence with better information and safeguards to enhance the functioning of the internal market), with broader cybersecurity ambitions, which regard risk identification and life-cycle risk management. This proposal sets common cybersecurity requirements for digital products, as its main goal is to improve security in Europe, for consumers and society at large.

For all these laws, according to the European co-legislators, the use of 114 TFEU as legal basis is (allegedly) entirely justified by the fact that the entities subject to the envisaged cybersecurity provisions still provide services on the internal market, thus by harmonising mandatory (cybersecurity) requirements distortions of market competition are avoided. For instance, in the CRA, digital products traded on the internal market will – to a large extent – all be subject to the same cybersecurity requirements. Nevertheless, these legislations have a broader scope than setting up common requirements for products harmonisation. In this regard, the ECJ stated that the Treaties do not authorise a measure which has only the incidental effect of harmonizing market conditions within the Union (para. 19). Put another way, the EU may intervene to cure diversity between national laws only where that diversity is shown to be harmful to the achievement of the EU's internal market.

Conclusion

In consideration of the fact that in the last years the Commission has made cybersecurity a priority, the fact that the Treaties do not provide the EU with an explicit cybersecurity competence may undermine this effort, and confuse the role that the EU should have *vis-á-vis* Member States when it comes to ensuring the digital security of the European citizens and organisations.

Although the impact of common requirements for digital products and service providers is surely beneficial to the "smooth functioning of the internal market", imposing general cybersecurity obligations, even mandating Member States to implement a cybersecurity strategy, hides - in plain sight - broader ambition than internal market harmonisation.

Discussing the legal basis for enacting cybersecurity policy in Europe, far from being a mere formalist argument, would help to clarify the policy debate and enhance political accountability. And by clarifying the limits of the EU, it would help to call on Member States to take their own responsibilities.