NEWSLETTER CVA

CYBER RESILIENCE ACT, A FAR-OFF PROPOSAL?

Executive Summary

In September 2022, the European Commission (EC) presented a proposal to complement the already comprehensive European regulation on the cybersecurity of products consisting of or containing digital elements.

In this newsletter, we analyse the proposal, which is in the phase of negotiations within the "trilogue" between the European Parliament, the Council of Ministers of the EU and the European Commission, in the framework of the ordinary legislative procedure.

This is a very important piece of legislation, especially considering the growing concerns about security within the internal market arising from the fact that, in its present form – after the EP 1st lecture – it may harm the functioning of the internal market, whose preservation and integrity is, however, its intended goal.

The telecommunications sector (TELCO) in the EU is characterised by a free and competitive market, based on the rule of law. National security issues are, as spelled out in article 4 n.2 of the Treaty of the European Union, a sole competence of the Member States, who bear a relevant part of the responsibility to react against threats that concern their national security.

Av. Duque de Ávila, 141-4Dto
Edifício OMNI
1050-081 Lisboa-Portugal

info@cruzvilaca.eu
+351 211 609 524

If it makes sense that the EC promotes a certain degree of harmonisation throughout the internal market of the conditions under which certain prohibitions or restrictions in the Telco sector are admissible, those measures must be necessary, appropriate and proportionate in view of the objectives pursued. Otherwise, the effects of such interventions could be exactly the opposite.

We will focus our attention, namely, on the provisions applicable to the so-called "High-risk Vendors". In this field, the political aspect of security assessments may be exacerbated and go beyond the proportionality required by both European and national laws. The effectiveness of judicial protection may also be jeopardised.

Identical considerations apply to the coexistence of technical and non-technical restrictions regarding the assessment of security risk alleged posed by specific products.

Moreover, the proposal gives the EC, alongside the Member States, a number of powers that may bring into question the principle of conferral.

With this provision, we analyse in this newsletter, competition may be harmed, innovation reduced and prices soared. And the internal market may be harmed.

Introduction

In September 2022, the European Commission (EC) presented a proposal to complement the already comprehensive European regulation on the cybersecurity of products consisting of or containing digital elements.

The proposed legislation, nicknamed Cyber Resilience Act (CRA), is called "Regulation on horizontal cybersecurity requirements for products with digital elements amending Regulation (EU) 2019/1020". It was approved by the European Parliament´s (EP) ITRE committee at first reading last July and confirmed at the institution's plenary session in September. Interinstitutional negotiations between the EP, the Council of Ministers (CM) and the EC, known in EU jargon as "trilogue", will take place over the next few months.

In this newsletter we analyse the CRA proposal, its *raison d'être*, and what we consider its strengths, weaknesses, and potential flaws. We also highlight the doubts and controversial issues that may arise from the proposal.

But first of all, it is important to define the issue itself: what is cybersecurity and why is there a need for this piece of legislation, which is horizontal in nature and sets requirements for the whole of the EU? And why, as many believe, has it been long awaited by many institutional quarters, policy makers and stakeholders from different industries, political

Av. Duque de Ávila, 141-4Dto
Edifício OMNI
1050-081 Lisboa-Portugal

info@cruzvilaca.eu
+351 211 609 524

sectors, specialised media and opinion makers in Europe?

Europe has been at the forefront of technological development, trying to cope from a regulatory point of view with a rapidly changing digital environment affecting markets and businesses.

The pace and depth of this change has given rise, at least in the last decade (if not before), to a greater number of increasingly frequent and sophisticated threats, such as the theft of credit card data to be sold for criminal purposes on the digital black market.

In fact, different technologies, a lack of digital literacy or failure to comply with minimum security standards are responsible for the sharp rise in the global cost of a data breach to organisations. Estimates put the cost of cybercrime in 2021 at around 6 trillion euro – and rising. A cybersecurity market indicator, 'Estimated Cost of Cybercrime', predicts a steady increase between 2023 and 2028 to a total of 5,7 trillion dollars, an increase of 70%.

Cybersecurity is therefore about protecting organisations, systems and information networks from digital attacks. While it is true that threats are constantly increasing as a result of the ever-accelerating pace of technological and digital innovation, it is also true that the development of comprehensive strategies, based on best practices and the use of artificial intelligence, combined with in-depth knowledge of the issues involved, expertise and advanced analytics, can be an effective way to prevent, if possible, and mitigate the damage caused by digital attacks.

Regulation is the other side of the coin. But when you look at it in the context of a multi-layered, multi-market, multi-national and very complex international environment, there are many issues to consider. They may be political or economic; they almost always raise complex legal issues.

This is all the truer in the case of the EU, an organisation that combines national sovereignty with a supranational legal and regulatory capacity.

I. The CRA - what it aims to achieve and what it can change

The Commission presents the case as follows: regulatory and market failures with regard to effective cybersecurity of products with digital elements threaten the integrity of the internal market, which is the main foundation of European integration. It can also jeopardise the fundamental rights and security of individuals.

The objective is to address these shortcomings and the lack of regulation **by establishing horizontal criteria and obligations in the field of cybersecurity for products with**

Av. Duque de Ávila, 141-4Dto
Edifício OMNI
1050-081 Lisboa-Portugal

info@cruzvilaca.eu
+351 211 609 524

digital elements (namely, the Internet of Things).

It is also a fundamental tool to enhance the potential of the internal market and (still) open economic relations worldwide (within the framework and scope of WTO), while avoiding security risks that are, or could be (the subtle distinction between these verbs is one of the issues raised by the CRA proposal) posed by high-risk providers (or, in the wording of the proposal, high-risk vendors – HRV).

In a nutshell, as mentioned above, the proposal establishes rules for the placing on the market of these products, including requirements for their design, development, and production.

It sets out the obligations and responsibilities of economic operators, from a cybersecurity perspective.

It defines the essential requirements and includes the responsibility for addressing the vulnerabilities inherent in handling these products, and the processes involved throughout the production cycle.

It also lays down the rules for monitoring and enforcing all these requirements and obligations.

Ideally, and theoretically, CRA should focus on the uniform requirements of different products and the level of security risk they may present. It is in fact important that its rules concern technical criteria, in order to make sure that CRA respects the principles of legality, legal security and the certainty of law, as in any other regulations on compliance.

The proposal, whose legal basis is Article 114 of the Treaty on the Functioning of the European Union (TFEU), has apparently been put on the fast track of the EU legislative process. Presented in mid-2022, it is already being discussed in the “trialogue” and many actors in the process have expressed the urgency to adopt this legislation.

The big question is whether it will be possible to adopt it before the – inevitable – gap in terms of legislative (and executive) delivery of decisions and actions, during election period: European elections are due in June 2024, and there will be a period, between then and January 2025, during which new leaders will have to be appointed, notably a new EC.

In any case, and despite the fact that this is a very complex piece of legislation, there is considerable pressure from various quarters to speed up the process. Everything will also depend on the degree of convergence that can be achieved in the “trialogue”, particularly between the national delegations (and especially the larger and more influential ones).

Av. Duque de Ávila, 141-4Dto
Edifício OMNI
1050-081 Lisboa-Portugal

info@cruzvilaca.eu
+351 211 609 524

II. CRA - General considerations, framework, potential problems

a) Geopolitical considerations

It is impossible to underestimate the importance of the political processes that concern and influence the international behaviour of the various parties involved in digital innovation, including cybersecurity, with the intertwining of the different geostrategies of the relevant actors, be they national, political or corporate.

In this sense, there seems to be a link between the current proposal, particularly reinforced in the amendments introduced by the EP in its first reading, and the broader geopolitical tensions between Western countries, namely the United States, and China.

These tensions seem to be on the rise, as the war in Ukraine could lead the world as a whole to a new division between two political and economic blocs, with the EU siding with its Western allies – but also with its own geostrategic interests, of which the concept (and the discussion around it) of a "strategic autonomy" is particularly illustrative.

In this sense, this initiative, which is obviously complex, involves considerations other than security, be they economic, technological, or political. **It is convenient for European partners within the EU to try to reconcile security requirements with the safeguard of its internal market and infrastructures.**

The debate is ongoing and future elections, both nationally (as usual, several countries will hold elections within the next 12 months, and the current political trends balance between a more protectionist and security approach to international relations and more liberal agendas) and within the EU, as mentioned above, may be decisive.

b) Internal market in question

The fact that **the main objective of this legislation is expressly the integrity of the internal market** – Article 114 TFEU – creates a paradox.

According to the proposal, the exclusion of a certain product can be initiated by the EC, either under the watered-down formulas of informing "the relevant market surveillance authorities" and issuing "targeted recommendations to economic operators aimed at ensuring that appropriate corrective actions are put in place" (Article 45(2)) or, at the Union level, through implementing acts (subject to a review procedure by a committee composed of representatives of the Member States, which decides by qualified majority).

In between, ENISA can be consulted and will carry out its own evaluation and risk assessment.

Av. Duque de Ávila, 141-4Dto
Edifício OMNI
1050-081 Lisboa-Portugal

info@cruzvilaca.eu
+351 211 609 524

Member States retain their prerogative to take measures to safeguard their own national security – in compliance with Union law – and may also impose additional measures on products with digital elements that are used for military, defence or national security purposes.

Thus, the constitutionality (compatibility with the Treaties) of the intervention of the EC, as proposed, seems very questionable and should be revised.

But in addition, and to illustrate the contradiction between the objectives pursued - in particular, the defence of the internal market - and the situation that could arise from the application of this legislation, it suffices to mention the possibility of the Commission imposing a ban on certain products under its proposed new powers, while Member States, in the legitimate exercise of their competences, impose similar bans on other products, for reasons of national security.

The cacophony in the internal market will increase and its integrity and proper functioning could be jeopardised, contrary to what was intended.

The fact that the EC, ENISA, the Examination Committee, probably the ECM and the regulators and authorities of the Member States, are all involved in deciding what is to be considered a risk, who is an HRV, which products should be excluded, which non-technical factors are relevant – always in specific and concrete cases – will inevitably create an imbalance in the market.

Legislation designed to protect the internal market can therefore, simply by following its own rules, endanger it.

All the more so if we consider that the possible exclusion of some suppliers with an established and legal activity within the internal market – or of their products, which are considered to be high risk, without an adequate judicial guarantee (see point II.d) – may lead to breach constitutional principles and rules, such as non-discrimination, competition, and proportionality (see point II.c).

To sum up, the ban restricts competition in the EU market. The exclusion of major digital products providers may reduce competition, potentially leading to higher prices for consumers and limiting innovation.

This will of course hinder the potential and proper functioning of the internal market, thus jeopardising the very objective pursued.

Av. Duque de Ávila, 141-4Dto
Edifício OMNI
1050-081 Lisboa-Portugal

info@cruzvilaca.eu
+351 211 609 524

c) Principles of proportionality and subsidiarity

In exercising (or using) the powers conferred on them by the Treaties, the European institutions must also comply with rules and principles designed to prevent the abusive, disproportionate or meaningless use of those powers. Fundamental principles of European law apply to the exercise of the Union's competences, in particular the principles of proportionality and subsidiarity.

Put simply, **the subsidiarity principle** means that rules should only be adopted at European level if their objectives cannot be better (or equally well) pursued by decisions at national level. It can be argued that, in the case of this regulation and in view of the nature of the matter, they cannot – but there is a reason for the existence of Article 4 of the TEU, and the multitude of actors foreseen in this legislation may even put in question the main objective, ie. the integrity of the internal market (as seen in point II.b).

Considering that subsidiarity applies (but the legal moment to act may have already been passed), it would give back to Member States the exclusive power to act, even if within the framework of programs, reports, tool-boxes, incentives and harmonized objectives within the context of EU institutions and Member States cooperation.

Proportionality, constitutionalised in Article 5 of the TEU, is probably the most paramount issue concerning CRA. Public authorities, if they are competent to act, cannot do it in such a manner that exceeds the limits of what is necessary to achieve the objectives of public interest that they pursue. It applies to Member States when implementing EU measures, and is of paramount importance when fundamental rights, EU principles or policies (e.g., the internal market or public security) are at stake.

Commenting the decision by the Portuguese cybersecurity authority to potentially exclude some suppliers and manufacturers of 5G equipment's – still under the former EC 5G toolbox -, Thierry Breton, internal market commissioner, recently stated that there would be no problem if the Portuguese authorities followed the rules, and, referring the case of a specific manufacturer, specified that "*there are some pieces of equipment that don't have any problems, but others may have some problems and it's up to the Member States to decide and [...] fulfil the commitment that everyone has made to respect the toolbox*".

This goes straight to the issue of proportionality, which is a fundamental principle of EU law that binds the Member States when applying EU law. As laid down in Article 5 TEU and already recalled above, any measures intended to fulfil a legitimate objective should be necessary and appropriate to that end, and (proportionality stricto sensu) must not impose a cost or a burden on someone, which is excessive in relation to the objective pursued. Singling out and discriminating against certain providers, or a provider's complete set of products not only goes beyond what is necessary to achieve the objectives of the proposed

Av. Duque de Ávila, 141-4Dto
Edifício OMNI
1050-081 Lisboa-Portugal

info@cruzvilaca.eu
+351 211 609 524

regulation, but also imposes an excessive and disproportionate burden on those providers.

Subsidiarity and proportionality principles in EU law concern the way a certain competence is exercised – not if it exists (which is a matter of the competence gap, hereabove).

d) Judicial protection

A major problem in the CRA proposal, in our view, is the absence - or inadequacy - of provisions to ensure that the decisions of the competent authorities (whether the EC, in particular when exercising the powers granted to it by Articles 45 and 46 of the proposal, in the EP version, as well as the evaluation by ENISA, a European agency, or even the national authorities) are based on transparent and informed procedures that guarantee the rights of the parties involved.

The proposal seems to lack adequate provisions on the right to effective judicial protection.

It would be advisable for these provisions to be duly adopted, taking into account the rights guaranteed by the Charter of Fundamental Rights of the European Union.

e) The competence gaps

In the constitutional organisation of the EU, the competences relating to the power to legislate are distributed between the EU itself and its Member States. Some competences remain national, others have been (or may be) transferred to the EU, according to the principle of conferral.

Today, after the Lisbon Treaty, the fundamental law of the EU, confirming a well-established doctrine as well as case law, explicitly establishes three types of EU competences: those exclusive to the EU, those shared between the EU and the Member States, and those which support, coordinate or complement national action.

Relevant for the CRA case on national security, Article 4(2) TEU clearly states that "*national security remains the sole responsibility of each Member State*." If this is the case, the question that arises is: on which basis can the EU legislate on such matters, with the scope and intensity as provided for in Articles 45 and 46 of the proposed regulation?

This also raises the issue of the legal basis to adopt the current regulation (see below point II.i).

A second level of competence gaps, this time within the framework of the EU decision-making process, concerns the level of power granted to the EC by Articles 45 and 46 of the proposal.

Av. Duque de Ávila, 141-4Dto
Edifício OMNI
1050-081 Lisboa-Portugal

info@cruzvilaca.eu
+351 211 609 524

This appears particularly worrying, when such a power – already alluded to above, in particular in points II.d and II.f) – goes as far as: "*The European Commission is given the right to enforce laws through implementing regulations when digital products comply with CRA technical specifications but have cyber security risks*" (Article 46(4) of the CRA proposal).

What are the risks alluded to? Ultimately, the main risk may be subjectivity, analogous to the considerations on non-technical specifications (see point II.f, here below). It must be acknowledged that such decisions also directly affect national security, thus raising the issue of the EU competence.

f) Non-technical factors raise serious problems of accountability

The mention of non-technical factors as a risk that can lead to the exclusion of suppliers – included in the version that will be submitted to the "trialogue" negotiations -, is of great concern, especially because of the subjective nature of these factors.

For example, what does the reference to "undue influence on suppliers by third countries" (recital 33) mean? Which criteria apply? Who has the burden of proof? How can these criteria – if they can be minimally objectified - be harmonised across the EU? How can the use of non-technical justifications (for exclusion) be assessed against principles such as legality and proportionality? How can "political" contamination be avoided?

And so on. These and other doubts, despite the efforts of the EC and the EP in their explanatory memoranda and part of the recitals, must necessarily be addressed and resolved in order to avoid a serious violation of the rule of law, a pillar of European integration.

Indeed, non-technical considerations should not fall within the competence of the EC. Decisions to exclude suppliers on the basis of non-technical factors should remain the sole responsibility of individual Member States, subject to review by national and European courts. In this context, the principle of conferral, which governs the limits of Union competences (Article 5(1) of the TEU should in any case be respected.

g) Inappropriateness of High-risk Vendor references

The qualification of a company as HRV raises several relevant legal issues that should be considered in the final version of the CRA. In the proposal's version after the EP 1st reading, a reference to HRV has been introduced in the following terms:

"*The Union needs to maximise the benefits of its economic openness while minimising the risks from economic dependencies on high-risk vendors, through a common strategic framework for Union economic security*" (recital 34a).

Av. Duque de Ávila, 141-4Dto
Edifício OMNI
1050-081 Lisboa-Portugal

info@cruzvilaca.eu
+351 211 609 524

This reference is inappropriate, to say the least, for a number of reasons:

First, there is of course the important question of who decides that a supplier is a high-risk vendor. There is a relevant legal difference whether the decision is taken by the EC or by a Member State. Indeed, it is highly questionable whether the EC is entitled to make this decision, given the competence gap highlighted in point II.e, hereabove.

Secondly, in view of the relevant consequences of this decision, the designation of a provider as high risk should only be acceptable if very clear and consistent facts are established, the burden of proof is very well defined, the decision-making process is at least transparent to those concerned and the right to effective judicial protection is guaranteed.

On the other hand, it does not make sense for the reference to a dependence "on high-risk vendors" to be made only in the recitals, in a single instance, without any consequent operationalisation (which, incidentally, would be highly questionable, as explained above in this point).

In fact, qualifying any supplier as a HRV by means of simple administrative and regulatory acts, except for very well established and proven cases (which fall under other legal provisions – espionage, interference, aggression, all of which are criminal in nature) would create a very strong stigma that could permanently damage a company's reputation. Mere political considerations are of a different nature.

h) Confusion between aims

Besides the specific internal market paradox mentioned hereabove (in item II.b), a ban affecting certain providers may be counter effective. Simple considerations, impossible to delve into in this instance, can illustrate that fact:

- *Economy*. It may have economic repercussions, disrupting existing contracts and investments made by European telecom operators with those providers, as well as affecting the business interests of European companies operating in other countries, potentially leading to retaliatory measures. Banning companies from supplying the European market may have severe long-term economic costs.

- *Supply diversity*. Banning a group of important TELCO providers may result in a higher degree of reliance on a small number of suppliers, from other geographies, less effective or more expensive, making the EU more vulnerable to supply chain disruptions, price fluctuations, and limited choices. There are just a few manufacturers who produce essential equipment. The exclusion of some of them will necessarily slow down the deployment of networks in the EU, for the lack of alternative suppliers or because replacing existing infrastructure can be time-consuming and costly.

Av. Duque de Ávila, 141-4Dto
Edifício OMNI
1050-081 Lisboa-Portugal

info@cruzvilaca.eu
+351 211 609 524

- *Technological Advancement.* The exclusion of specific providers may hinder the EU's access to cutting-edge technology and delay the implementation of advanced applications, namely concerning the Internet of Things and autonomous vehicles, which rely on robust 5G networks. Often, innovation and research are a two-way road that can be eroded by radical decisions.

- *Political imbalance.* The idea that the European security depends on this regulation implies that the alignment with the strategic interest of partners overseas is essential for that purpose. What guarantees Europe that one or more of those partners do not, in pursuit of their national interests, disregard prohibitions or establish their own agreements with a view to economic, commercial or technological gain? It is nothing that hasn't happened before.

i) Legal basis

This is a crucial aspect. The choice of the legal path in the EU legal framework is based on the content. **The main basis of CRA is the internal market and its protection:**

"T*he legal basis for this proposal is Article 114 TFEU, which provides for the adoption of measures to ensure the establishing and functioning of the internal market. The purpose of the proposal is to harmonise cybersecurity requirements for products with digital elements in all Member States and to remove obstacles to the free movement of goods*" (explanatory memorandum, EC, 15/09/2022).

The legal basis of legislative acts under European law is based on their content, within the aforementioned principle of conferral. There are proposals - and this may be the case - **where a double or triple legal basis is required**, implying different procedures, either the more usual ordinary legislative procedure (as in the present proposal), based on a double majority and the participation of the three institutions in the decision-making process, or special procedures, where unanimity is the rule. Problems arise when the various legal bases require different legislative procedures which are incompatible with each other. Then, the only legitimate solution is to split the single proposal in as many proposals according to the specific legal basis.

As said before, there is a legal reason for national security issues to be kept in the national sphere. This proposal seems to go too far in using exclusively article 114 as a legal basis to approve all the measures it contains – despite the EC explanations, and the *exposé de motifs* of the other institutions involved.

The fact that the present choice of legal basis has as the inevitable consequence that any final decision on the legislative procedure is taken by a qualified majority vote, thus avoiding the need to ensure unanimity of all Member States.

Av. Duque de Ávila, 141-4Dto
Edifício OMNI
1050-081 Lisboa-Portugal

info@cruzvilaca.eu
+351 211 609 524

III. Conclusion

It is undeniable that security is essential and the threats to the integrity of States, businesses and individuals have been growing constantly.

It also seems obvious that the European internal market is one of the potential victims of the realisation of those threats, and thus should be protected.

The EC, as the guardian of the Treaties, has, in first place, the responsibility to preserve and defend it.

A careful assessment of the current legislative proposal reveals a number of inconsistencies which may ultimately combine to reduce its effectiveness or even contribute to the exact opposite of its stated objective: the integrity of the internal market.

Moreover, in its current form, the proposal may violate a number of fundamental principles and rules of the EU legal order.

However, it is still time to change what needs to be changed, especially as regards the excesses of intervention at EC level, the lack of judicial guarantees and the transparency gap. As the old saying goes, it is important not to "throw the baby out with the bathwater".

Av. Duque de Ávila, 141-4Dto
Edifício OMNI
1050-081 Lisboa-Portugal

info@cruzvilaca.eu
+351 211 609 524