LEITARTIKEL 1:

Mira Burri / Zaira Zihlmann
The Cyber Resilience Act -
An appraisal and contextualization

LEITARTIKEL 2:

Okan Yildiz / Rolf H. Weber
Market Definition and Market
Power in the Era of Blockchain

The EU Cyber Resilience Act – An appraisal and contextualization

Mira Burri/Zaira Zihlmann*

Table of contents

A.   Introduction

The onset of a "fourth industrial revolution" was heralded a few years ago, a term coined to describe the advancing fusion of technologies that blurs the lines between the physical, digital, and biological realms.[1] Crucial part in this transformation is played by the Internet of Things (IoT)[2] as "a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies."[3] The number of devices connected to the IoT is huge and growing. There are currently more IoT devices than there are humans on the planet,[4] and it is estimated that by 2025 there will be 30.9 billion IoT devices worldwide, with 4.3 billion of those in the European Union (EU).[5] Yet, a large number of these connected devices come with a low level of cybersecurity.[6] This raises serious concerns as more unsecured products also mean an extended attack surface and heightened cybersecurity risks for their users.[7] This becomes even more problematic as connected products by means of interlinked systems of sensors and actuators interact seamlessly with the physical realm in which they operate. Thus, the

---

[1]   Schwab Klaus, The Fourth Industrial Revolution, Geneva 2016, 12.

[2]   Carr Madeline/Lesniewska Feja, Internet of Things, Cybersecurity and Governing Wicked Problems: Learning from Climate Change Governance, International Relations 2020, 392.

[3]   Definition according to the International Telecommunication Union. ITU, Recommendation Y.2060, Overview of the Internet of Things, 2012, <https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.2060-201206-I!!PDF-E&type=items>.

[4]   Tasheva Iva/Kunkel Ilana, In a Hyperconnected World, Is the EU Cybersecurity Framework Connected?, European View 2022, 187.

[5]   Statista, Internet of Things (IoT) and Non-IoT Active Device Connections Worldwide from 2010 to 2025, September 2022, <https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/>.

[6]   Studies have shown that between 57% and 68% IoT devices have critical vulnerabilities. Roberts Paul F., Smart Toys Are Still Hackable (We Just Don't Talk about It), Forbes, 28 December 2022, <https://www.forbes.com/sites/paulfroberts/2022/12/28/smart-toys-are-still-hackable-we-just-dont-talk-about-it/>.

[7]   Cf. Johnson Shane D. et al., Crime and the Consumer Internet of Things, in: Gill Martin (ed.), The Handbook of Security, Cham 2022, 707.

security of these products is directly related to safety.[8] Moreover, given the strong cross-border nature of connected devices, an incident that initially affects a single entity or an EU Member State can often spread across organizations, industries and multiple Member States, and this within minutes.[9] To put it in the words of the European Commission's President Ursula von der Leyen: "[i]f everything is connected, everything can be hacked."[10] Following up on this expressed concern in her 2021 State of the Union address, she declared the EU's intention to take a leading role in cybersecurity and announced the project of a Cyber Resilience Act (CRA) – as a complement to EU's cybersecurity acquis with horizontal cybersecurity requirements for all products with digital elements[11] and the "first ever EU-wide legislation of its kind."[12] The CRA project advanced rapidly and was adopted by the Commission on 15 September 2022.[13]

If enacted, the CRA would allow, among other things, the banning of devices with digital elements that do not meet the requirements of the EU market. Given that the CRA may also apply to non-EU manufacturers' digital products once placed on the EU market, the CRA could have an impact on cybersecurity standards for such products beyond the EU borders. Indeed, non-EU operators might find it convenient to follow the CRA's rules as a default framework for their global operations instead of developing different products or processes for different markets.[14] Consequently, the EU might emerge as

---

[8] Chiara Pier Giorgio, The Cyber Resilience Act: The EU Commission's Proposal for a Horizontal Regulation on Cybersecurity for Products with Digital Elements, International Cybersecurity Law Review 2022 (cit.: Chiara, Cyber Resilience Act), 256.

[9] European Commission Staff Working Document, Impact Assessment Report accompanying the Document Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, SWD(2022) 282 final, 15 September 2022, part 1/3 (cit.: Impact Assessment Report, part 1), 1.

[10] von der Leyen Ursula, 2021 State of the Union Address by President von der Leyen, September 2021, <https://ec.europa.eu/commission/presscorner/api/files/document/print/ov/speech_21_4701/SPEECH_21_4701_OV.pdf>.

[11] Chiara, Cyber Resilience Act (fn 8), 255.

[12] European Commission, Cyber Resilience Act: New EU Cybersecurity Rules Ensure More Secure Hardware and Software Products, September 2022, <https://data.europa.eu/doi/10.2759/543836>.

[13] Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM(2022) 454 final, 15 September 2022 [hereinafter CRA or CRA Proposal].

[14] Car Polona/De Luca Stefano, EU Cyber-resilience Act, European Parliamentary Research Service, PE 739.259, December 2022, 6.

the international reference point for cybersecurity of connected devices – triggering the so-called "Brussels effect" – similarly as in the area of data protection by means of the General Data Protection Regulation (GDPR).[15]

Following this brief introduction, the goal of this article is threefold: (1) to contextualize the CRA by outlining the drivers of its adoption against the broader picture of EU's role (and ambitions) in the cybersecurity domain as well as the EU's dynamic legislative landscape (Section B); (2) to provide an overview of the rules of the proposed CRA and critically evaluate selected aspects (Section C). Based on the analyses, we seek in the final Section (D) to assess whether and to what extent the CRA project would be successful in attaining its objectives and what the consequences of this could be.[16]

B.   Drivers of a horizontal cybersecurity regulation

When examining the drivers of the proposed EU Cyber Resilience Act, it is apt to focus not only on the rationale of the regulatory initiative, namely the creation of an Internet of Secure Things, but to view this in the somewhat broader context of the EU's growing ambition to become a cybersecurity champion and its striving for digital sovereignty. We look in turn at these rationales behind the CRA in the next two sections.

I.   Creating an Internet of Secure Things through harmonization and mandatory requirements

As stated at the outset, one of the focal points of cybersecurity challenges in the EU has been the Internet of Things, as its employment is characterized by a large number of vulnerabilities and a cross-border nature. This can potentially not only threaten the proper functioning of the internal market but also

---

[15]   Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ (2016) L 119/1 [hereinafter GDPR].

[16]   It should be noted that the subsequent observations refer to the proposal of 15 September 2022. Discussions on this draft have meanwhile gained momentum in the Council of EU Ministers, and it is reported that the Swedish Presidency circulated a new compromise text on 27 January 2023, which was recently subject to discussion in the Horizontal Working Group on Cyber Issues, the technical body of the EU Council that prepares for adoption by the Ministers. See e.g., Bertuzzi Luca, EU Council Moves to Adjust Product Life-cycle, Reporting in New Cybersecurity Law, EURACTIV.com, 1 February 2023, <https://www.euractiv.com/section/cybersecurity/news/eu-council-moves-to-adjust-product-lifecycle-reporting-in-new-cybersecurity-law/> (cit.: Bertuzzi, February 2023).

fundamental rights and the security of EU citizens. Aware of this problematic interplay, the EU announced in its Cybersecurity Strategy for the Digital Decade[17] aiming to tackle this issue by inter alia incentivizing secure products and services in order to ensure an Internet of Secure Things.[18] One of the critical building blocks towards this goal is the proposed CRA.[19]

According to the CRA proposal, there are two major problems with respect to cybersecurity in products with digital elements: (1) products have low levels of cybersecurity; and (2) users are prevented from selecting products with adequate cybersecurity properties or using them in a secure manner due to insufficient understanding and access to information.[20]

1. Protecting consumers by imposing mandatory requirements for all connected devices

The first problem stems from the lack of incentives for manufacturers to take security seriously,[21] as well as the fierce competition from products coming at a much lower price, notably from China.[22] Indeed, although manufacturers of products with digital elements sometimes face reputational damage if their products are not secure enough, the costs of security breaches are mainly borne by consumers.[23] Besides, security vulnerabilities often do not lead users to actually switch products, due to the inherent network effects.[24] Consequently, manufacturers have little incentive to invest in the design and development of secure products and to provide security updates.[25] They also typically prioritize rapid market access through new feature development and compatibility with existing products over the development of security

---

[17] Joint Communication to the European Parliament and the Council, The EU's Cybersecurity Strategy for the Digital Decade, JOIN(2020) 18 final, 16 December 2020 (cit.: EU's Cybersecurity Strategy for the Digital Decade).

[18] EU's Cybersecurity Strategy for the Digital Decade (fn 17), 9.

[19] Cf. Car/De Luca (fn 14), 2 et seq.

[20] Recital 1 CRA Proposal.

[21] Impact Assessment Report, part 1 (fn 9), 9.

[22] Most infected IoT devices come from China and Taiwan, the world's leading hardware manufacturers. Rodríguez Elsa et al., Superspreaders: Quantifying the Role of IoT Manufacturers in Device Infections, 20th Annual Workshop on the Economics of Information Security WEIS 2021, <https://weis2021.econinfosec.org/wp-content/uploads/sites/9/2021/06/weis21-rodriguez.pdf>, 13.

[23] European Economic and Social Committee, Opinion, Cyber Resilience Act, INT/999, adopted on 14 December 2022, 4.

[24] Impact Assessment Report, part 1 (fn 9), 10.

[25] European Economic and Social Committee (fn 23), 4.

properties.[26] Especially cheap devices exacerbate the issue, as they often stem from non-EU manufacturers that ship an entire series of products with a default password, such as 123456.[27]

Another important aspect is that the insecurity of devices is not just a local technical issue. Rather, such devices, notably sensors, are embedded in devices and systems that are managed by people who lack awareness of the potential vulnerabilities – for example, manufacturers of smart toys are familiar with the safe use of plastics but may lack awareness of cybersecurity and privacy threats to children.[28]

Additionally, users are often unaware of the security risks associated with products with digital elements and usually have no knowledge of a product's internal workings, so making purchasing decisions based on these features can be very difficult for them.[29] Accordingly, in many cases, cybersecurity incidents may be attributed to users selecting products that are inappropriate for their purposes or having hardware and software misconfigured,[30] thereby raising the security risk of their device or network unnecessarily.[31] The primary cause of this issue, as identified in the CRA Impact Assessment, is that manufacturers do not provide adequate information about security features, vulnerabilities, and how to use a device safely.[32] But even if users are familiar with the parameters of the product or service they purchase, they are unable to predict flaws that may show up later, especially since many vulnerabilities are only discovered years after a particular technology was developed. Also, the emergence of some vulnerabilities may not have been foreseeable at the time of product launch, as the assessment of the degree of security of a particular technology may change over time.[33]

---

[26] Johnson et al. (fn 7), 706; Chiara, Cyber Resilience Act (fn 8), 256.

[27] Gregersen Carsten Rhod, EU Cyber Resilience Act: The GDPR for IoT, embedded, 20 December 2022, <https://www.embedded.com/eu-cyber-resilience-act-the-gdpr-for-iot/#:~:text=The_Cyber_Resilience_Act_is,elements_throughout_their_whole_lifecycle>. According to Hernández-Ramos José L. et al., Toward a Data-Driven Society: A Technological Perspective on the Development of Cybersecurity and Data-Protection Policies, IEEE Security & Privacy 2020, 30, there is also the possibility that devices are put on the market that have default passwords, which are never changed during their life-cycle.

[28] Carr/Lesniewska (fn 2), 397.

[29] Impact Assessment Report, part 1 (fn 9), 10.

[30] European Economic and Social Committee (fn 23), 4.

[31] Impact Assessment Report, part 1 (fn 9), 8.

[32] Impact Assessment Report, part 1 (fn 9), 14.

[33] Banasinski Cezary/Rojszczak Marcin, Cybersecurity of Consumer Products against the Background of the EU Model of Cyberspace Protection, Journal of Cybersecurity 2021, 2.

In order to address the problem of low level of cybersecurity of products with digital elements marketed in the Union, the CRA imposes mandatory minimum-security requirements for all connected devices.[34] Against the problem of insufficient understanding among users and in order to enable organizations and consumers to use products with digital elements securely, the CRA proposal seeks to enhance transparency in various aspects.[35] The CRA essential cybersecurity requirements are also meant to contribute to strengthened protection of personal data and privacy of individuals. In this sense, cybersecurity is seen as a core element in the protection of fundamental rights and freedoms.[36]

2. Ensuring a coherent cybersecurity framework via horizontal regulation

The second driver behind the CRA adoption has been the fragmentation of the existing EU legal framework.[37] As a gap analysis study[38] showed, there is presently no piece of EU legislation that requires comprehensive cyber-security requirements for all products with digital elements.[39] Rather, the current legislation comprises several sets of horizontal rules that address certain aspects linked to cybersecurity – yet from different angles.[40] While the Cybersecurity Act[41] as well as the Network and Information Security Directive (NIS Directive)[42] do come with measures to improve the security of the digital supply chain, they set no mandatory requirements for the security of products

---

[34] Chiara, Cyber Resilience Act (fn 8), 257.

[35] Impact Assessment Report, part 1 (fn 9), 21.

[36] Chiara, Cyber Resilience Act (fn 8), 271.

[37] Impact Assessment Report, part 1 (fn 9), 11.

[38] Annex 13 of the Commission Staff Working Document, Impact Assessment Report, Annexes to the Impact Assessment Report accompanying the document Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, SWD(2022) 282 final, 15 September 2022, part 2/3.

[39] Impact Assessment Report, part 1 (fn 9), 11.

[40] Explanatory Memorandum to the CRA Proposal, 2.

[41] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ (2019) L 151/15 [hereinafter CSA].

[42] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ (2016) L 194/1 [hereinafter NIS Directive].

with digital elements.[43] According to the CRA Impact Assessment this bears the risk of Member States adopting diverging national regulation.[44] Germany is a proof of this, having introduced first (non-binding) measures to enhance the security of products with digital elements.[45] Such initiatives may undermine the internal market, creating legal uncertainty for both manufacturers and users, as well as placing unnecessary burdens on economic operators to meet overlapping requirements for similar types of devices[46] – a state that is certainly not along the lines of the EU Strategy for a Digital Single Market.[47]

In order to avoid regulatory fragmentation and ensure a coherent cybersecurity framework, the CRA aims to streamline the EU's fragmented cybersecurity regulatory landscape by introducing horizontal cybersecurity requirements for products with digital elements.[48] The means of a Regulation over a Directive ensures this in a more immediate way and gives a level of legal certainty that a Directive, considering the leeway given for its implementation at the Member State level, could not achieve.[49]

II.   Strengthening digital sovereignty via cybersecurity regulation

The CRA must also be seen in the context of concerted efforts of the EU to become a leading actor in the domain of cybersecurity and its interlinked striving, through a set of regulatory initiatives, to assert the EU's "digital sovereignty" and render it sustainable over time.

1.   EU's cybersecurity activities

With regard to the former, it is evident that the last two decades have witnessed the emergence of cybersecurity as one of the most critical, as well as contentious, topics on regulatory agendas. This new strategic importance is intrinsically linked to the striving of various actors (states as well as international and supranational organizations) to shape and influence the

---

[43]   Recital 3 CRA Proposal.

[44]   Impact Assessment Report, part 1 (fn 9), 16 et seq.

[45]   Impact Assessment Report, part 1 (fn 9), 19.

[46]   Impact Assessment Report, part 1 (fn 9), 16 et seq.; Chiara, Cyber Resilience Act (fn 8), 257.

[47]   Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe, COM(2015) 192 final, 6 May 2015.

[48]   Cf. Vikolainen Vera, Strengthening Cyber Resilience, European Parliament Research Service, PE 734.708, December 2022, 1.

[49]   Explanatory Memorandum to the CRA Proposal, 5.

governance of cyberspace.[50] Among them is the EU, for which cybersecurity is now one of the top priorities[51] and which aspires to position itself as a central cybersecurity actor.[52] EU's heightened prioritization of cybersecurity comes after a period of inaction, as, although the issue of safeguarding cyberspace has been on the EU institutional agenda for some 20 years now, almost no binding provisions were adopted.[53] Yet, against the backdrop of major cyberattacks and incidents, the EU accelerated its regulatory activity[54] and with the 2013 EU Cybersecurity Strategy[55] introduced cybersecurity as a new policy area.[56] The Cybersecurity Strategy is closely linked to the 2015 EU Digital Single Market Strategy as cybersecurity is an important instrument to prevent economic damage and enhance consumer trust.[57]

---

[50]   Backman Sarah, Risk vs. Threat-based Cybersecurity: The Case of the EU, European Security 2022, 1.

[51]   Carrapico Helena/Barrinha André, European Union Cyber Security as an Emerging Research and Policy Field, European Politics and Society 2018, 300.

[52]   Gao Xinchuchu/Chen Xuechen, Role Enactment and the Contestation of Global Cybersecurity Governance, Defence Studies 2022, 689.

[53]   Banasinski/Rojszczak (fn 33), 3. A comprehensive overview on how the topic of cybersecurity has evolved from its absence to its prominence on the European agenda is provided by Brandão Ana Paula/Camisão Isabel, Playing the Market Card: The Commission's Strategy to Shape EU Cybersecurity Policy, JCMS 2022, 1339 et seqq.

[54]   Today there are numerous EU legal instruments relevant to cybersecurity and given that cybersecurity is a cross-cutting issue, there are not only laws on information society and cyber resilience, but also EU legal acts on cyber deterrence and defense. Given the limited space, in the following only selected policies are highlighted. For more details on the cybersecurity regulatory landscape, cf.: Kasper Agnes/Antonov Alexander, Towards Conceptualizing EU Cybersecurity Law, ZEI Discussion Paper 2019, <https://www.zei.uni-bonn.de/de/publikationen/medien/zei-dp/zei-dp-253-2019.pdf>; European Court of Auditors, Challenges to Effective EU Cybersecurity Policy, Briefing Paper, March 2019, <https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf>, 9; Wessel Ramses A., Cybersecurity in the European Union: Resilience through Regulation?, in: Conde Elena/Yaneva Zhaklin/Scopelliti Marzia (eds.), Routledge Handbook of EU Security Law and Policy, Abingdon 2019.

[55]   Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013) 1 final, 7 February 2013.

[56]   Fuster Gloria González/Jasmontaite Lina, Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights, in: Christen Markus/Gordijn Bert/Loi Michele (eds.), The Ethics of Cybersecurity, Cham 2020, 98.

[57]   Bendiek Annegret/Pander Maat Eva, The EU's Regulatory Approach to Cybersecurity, German Institute for international and Security Affairs, WP NR. 02 2019, <https://www.swp-berlin.org/publications/products/arbeitspapiere/WP_Bendiek_Pander_Maat_EU_Approach_Cybersecurity.pdf>, 4 et seq.

The main pillar of the 2013 Cybersecurity Strategy was the NIS Directive that came into effect in 2016 and was the first EU-wide horizontal instrument, i.e., cross-sectoral instrument, to regulate cybersecurity.[58] The NIS Directive aimed to ensure a high level of network and information security at the EU level by setting security and incident reporting obligations for operators of essential services and digital service providers,[59] as well as achieve a minimum level harmonization across the Member States.[60] The GDPR, adopted also in 2016, approaches cybersecurity from the angle of data protection, and sets out technical requirements for security of personal data and a breach notification regime.[61]

The second Cybersecurity Strategy was proposed in 2017[62] and resulted in the proposal for the EU Cybersecurity Act, which was adopted on 12 March 2019.[63] The Cybersecurity Act was a significant step forward in the EU's approach to cybersecurity as it introduced an EU-wide cybersecurity certification framework for products and services as well as granted the European Union Agency for Cybersecurity (ENISA) a permanent mandate.[64] The follow-up and presently applying "Cybersecurity Strategy for the Digital Decade" of 2020 focuses on three areas: (1) resilience, technological sovereignty and leadership; (2) operational capacity to prevent, deter and respond; (3) a global and open cyberspace. The revised NIS Directive (NIS2 Directive),[65] which entered into

---

[58] Markopouloua Dimitra/Papakonstantinou Vagelis/De Hert Paul, The New EU Cybersecurity Framework: The NIS Directive, ENISA's Role and the General Data Protection Regulation, Computer Law & Security Review 2019, 1; Schmitz-Berndt Sandra/Cole Mark D., Towards an Efficient and Coherent Regulatory Framework on Cybersecurity in the EU: The Proposals for a NIS 2.0 Directive and a Cyber Resilience Act, ACIG 2022, 5.

[59] Carrapico/Barrinha (fn 51), 300; Hernández-Ramos et al. (fn 27), 32.

[60] European Court of Auditors (fn 54), 13.

[61] Arts. 32–34 GDPR. Kasper/Antonov (fn 54), 34; Bederna Zsolt/Rajnai Zoltan, Analysis of the Cybersecurity Ecosystem in the European Union, International Cybersecurity Law Review 2022, 39 et seq. A comprehensive overview of the cybersecurity obligations of the GDPR provide Mantelero Alessandro et al., The Common EU Approach to Personal Data and Cybersecurity Regulation, International Journal of Law and Information Technology 2020, 306.

[62] Joint Communication to the European Parliament and the Council, Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, Brussels, JOIN(2017) 450 final, 13 September 2017.

[63] Chiara Pier Giorgio, The IoT and the New EU Cybersecurity Regulatory Landscape, International Review of Law, Computers & Technology 2022 (cit.: Chiara, IoT), 119 et seq.

[64] Bendiek/Pander (fn 57), 12 et seq.; Hernández-Ramos et al. (fn 27), 32.

[65] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), OJ (2022) L 333/80 [hereinafter NIS2 Directive].

force in January 2023, accordingly aims to enhance the level of cyber resilience by requiring all public and private entities across the single market that perform important functions for the economy and society as a whole to adopt appropriate cybersecurity measures. It also seeks to strengthen the cyber-security risk management and improve cooperation between the relevant competent authorities.[66]

Importantly, the Cybersecurity Strategy for the Digital Decade also announced new horizontal rules to improve the cybersecurity of products with digital elements. This triggered the legislative process[67] and ultimately led to the Commission's CRA proposal of 15 September 2022.[68] The CRA forms part of a large number of EU legal acts in the digital domain, such as on AI, data spaces, online platforms, that affect but also go beyond cybersecurity.[69] This regulatory activism can be well understood in the context of the EU's pursuit of "digital sovereignty", also dubbed as a process of "re-sovereignization".[70]

2.   Digital sovereignty and EU's re-sovereignization

The term "digital sovereignty" expresses the idea that "states should reassert their authority over the internet and protect their citizens and businesses from the manifold challenges to self-determination in the digital sphere."[71] Yet, the term lacks a uniform definition and is used inconsistently in EU policy documents. Indeed, even essential elements are unclear, such as whether digital sovereignty is something that the EU already possesses, or whether it is a goal that the EU should aspire to.[72] Nevertheless, the term "sovereignty" has been increasingly used since 2019, notably by Ursula von der Leyen's

---

[66]   Bederna/Rajnai (fn 61), 39 et seq.; Schmitz-Berndt Sandra, Cybersecurity Is Gaining Momentum - NIS 2.0 Is on Its Way, European Data Protection Law Review 2021, 582 et seq.

[67]   Council of the European Union, Council conclusions on the development of the European Union's cyber posture - Council conclusions approved by the Council at its meeting on 23 May 2022, Brussels, 23 May 2022, 6.

[68]   Further on the legislative history of the CRA: Car/De Luca (fn 14), 4 et seqq.

[69]   Codagnone Cristiano/Weigl Linda, Leading the Charge on Digital Regulation: The More, the Better, or Policy Bubble?, Digital Society 2023, 7 et seq.

[70]   Bendiek Annegret/Stürzer Isabella, Advancing European Internal and External Digital Sovereignty: The Brussels Effect and the EU-US Trade and Technology Council, German Institute for international and Security Affairs, SWP Comment 2022, <https://www.swp-berlin.org/publications/products/comments/2022C20_European DigitalSovereignty.pdf>, 8.

[71]   Pohle Julia/Thiel Thorsten, Digital Sovereignty, Internet Policy Review 2020, 2.

[72]   Roberts Huw et al., Safeguarding European Values with Digital Sovereignty: An Analysis of Statements and Policies, Internet Policy Review 2021, 12.

Geopolitical Commission, which urged the EU to be at the forefront of key technologies and future-proof infrastructure, with common standards, gigabit networks and secure current and next-generation clouds.[73] The President of the European Council, Charles Michel, has also constructed digital sovereignty as a strategy, in the sense that the EU sets its own rules, makes autonomous technological choices and develops its own digital solutions.[74] Similarly, the European Commission has announced the years 2020–2030 as Europe's "digital decade" and stated that securing Europe's "technological sovereignty" and "digital sovereignty" are key strategic objectives during this period.[75]

Cybersecurity appears as a core pillar of the EU's digital sovereignty, as strong cybersecurity is seen as a prerequisite for other policy areas, since the security of data, infrastructure and economic entities are necessary for a functional and competitive EU digital economy as well as for the safeguarding of EU values.[76] Consequently, there are various legislative initiatives that seek to strengthen the EU's digital sovereignty by making it a standard-setter in the field of cybersecurity,[77] such as the above-mentioned NIS2 Directive, the Cybersecurity Act as well as the GDPR, together with the EU Cybersecurity Strategy, which highlights the need for technological sovereignty too. The CRA only adds to this package, in particular in the domain of cybersecurity standard-setting for all products with digital elements.

In this context and making the link to the "Brussels effect", whereby the EU, as a regulatory superpower, "exports" its standards and they become the global ones,[78] the CRA can arguably be seen as the "GDPR for IoT".[79] If this effect, in analogy to global data protection, eventually materializes would very much depend on the level and type of obligations, the material

---

[73] von der Leyen Ursula, Speech in the European Parliament Plenary Session, November 2019, <https://ec.europa.eu/commission/presscorner/api/files/attachment/858838/Speech by President-elect von der Leyen at the EP - as delivered in EN-FR-DE.pdf>, 9.

[74] Barrinha André/Christou George, Speaking Sovereignty: The EU in the Cyber Domain, European Security 2022, 362.

[75] Bendiek Annegret/Stürzer Isabella, The Brussels Effect, European Regulatory Power and Political Capital: Evidence for Mutually Reinforcing Internal and External Dimensions of the Brussels Effect from the European Digital Policy Debate, Digital Society 2023, 4.

[76] Roberts et al. (fn 72), 12.

[77] Madiega Tambiama, Digital Sovereignty for Europe, European Parliamentary Research Service, PE 651.992, July 2020, 4; Barrinha/Christou (fn 74), 429.

[78] Anu Bradford, The Brussels Effect, Northwestern University Law Review (2012), 1; Anu Bradford, The Brussels Effect: How The European Union Rules the World, Oxford 2020; Fahey Elaine, EU as a Global Digital Actor: Institutionalising Global Data Protection, Trade, and Cybersecurity, London 2022.

[79] Gregersen (fn 27).

scope and extra-territorial reach of the CRA, its stringency of monitoring and enforcement, among other things.[80] The "Brussels effect", although admittedly not a form of international cooperation but a case of unilateral standard-setting, could also have positive impact – in that it "may ultimately contribute to the enhancement of global cyber resilience".[81]

The following section looks more closely at key aspects of the proposed CRA, which gives us also the basis to test to what extent the regulatory rationales driving the CRA's adoption find an appropriate reflection in its legal provisions and contribute to EU's digital sovereignty and the multiplication of the "Brussels effect".

C.   The proposed Cyber Resilience Act: Analysis of selected key aspects

Consisting of 71 Recitals, 57 Articles and 6 Annexes (for an overview, see Table 1 below), the proposed Cyber Resilience Act aims to create a coherent cybersecurity framework by requiring that products with digital elements are secure along the supply chain and throughout their life-cycle, as well as by enabling users to take cybersecurity into account when selecting and using products with digital elements.[82]

The CRA subject matter consists of four general elements, listed in Art. 1: (1) rules for the placing on the market of products with digital elements to ensure the cybersecurity of such products; (2) essential requirements for the design, development and production of products with digital elements, and obligations for economic operators in relation to these products with respect to cybersecurity; (3) essential requirements for the vulnerability handling processes put in place by manufacturers to ensure the cybersecurity of products with digital elements during the whole life-cycle, and obligations for economic operators in relation to these processes; and (4) rules on market surveillance and enforcement of the above-mentioned rules and require-ments.

---

[80]   Bendiek/Pander (fn 57), 8.

[81]   Saalman Lora/Su Fei/Saveleva Dovgal Larisa, Cyber Posture Trends in China, Russia, the United States and the European Union, December 2022, <https://www.sipri.org/sites/default/files/2022-12/2212_cyber_postures_0.pdf>, 22.

[82]   Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/102 - Progress Report, 18 November 2022 (cit.: Council of the European Union, Progress Report), 2.

However, these elements cannot be allocated to individual chapters of the regulation. Yet, it may be difficult to link these core regulatory elements with discrete chapters and/or annexes of the CRA. Rather, these aspects recur throughout the entire regulation, including the Annexes, and the related rights and obligations need to be taken as appropriately together. The chapters of the proposed CRA and its Annexes are structured as follows:

Chapter I: General Provisions	Arts. 1 – 9
Chapter II: Obligations of Economic Operators	Arts. 10 – 17
Chapter III: Conformity of the Product with Digital Elements	Arts. 18 – 24
Chapter IV: Notification of Conformity Assessment Bodies	Arts. 25 – 40
Chapter V: Market Surveillance and Enforcement	Arts. 41 – 49
Chapter VI: Delegated Powers and Committee Procedure	Arts. 50 – 51
Chapter VII: Confidentiality and Penalties	Arts. 52 – 53
Chapter VIII: Transitional and Final Provisions	Arts. 54 – 57

Annex I: Essential Cybersecurity Requirements
1. Security Requirements Relating to the Properties of Products with Digital Elements
2. Vulnerability Handling Requirements

Annex II: Information and Instructions to the User

Annex III: Critical Products with Digital Elements

Annex IV: EU Declaration of Conformity

Annex V: Contents of the Technical Documentation

Annex VI: Conformity Assessment Procedures
– Conformity Assessment Procedure Based on Internal Control (Based on Module A)
– EU-type Examination (Based on Module B)
– Conformity to Type Based on Internal Production Control (Based on Module C)
– Conformity Based on Full Quality Assurance (Based on Module H)

Table 1: Overview of the CRA's chapters and annexes

In the following, we analyze in more detail: (1) the nature and scope of the CRA; (2) the risk-based classification of products; (3) the economic operators' obligations; (4) the monitoring and enforcement mechanism; and (5) the fines for non-compliance.

I. Horizontal regulatory intervention with a broad scope of application

1. Regulatory intervention based on Art. 114 TFEU

Art. 114 of the Treaty on the Functioning of the European Union (TFEU)[83] gives the legal basis for the CRA.[84] This is linked to the now common practice of using the catch-all provision of Art. 114 TFEU, i.e., the political and legal mandate to regulate the internal market, to adopt policies and legislation on cybersecurity.[85] This path is aptly chosen, given that cybersecurity remains a legal competence of the Member States and the EU constitutional law provides no unified legal basis for the Union to regulate cybersecurity.[86] The market-security nexus opens a door for the EU legislator in the cybersecurity context and this has been the case also with NIS Directive.[87] While there is no jurisprudence specifically on cybersecurity, the CJEU has confirmed internal market regulation as the proper legal basis for regulating cyberspace.[88]

Views on the soundness of this approach differ. Some authors have referred to this interventionist top-down approach, especially in the field of technology regulation, that introduces new concepts, principles and governmental mechanisms into the legal systems of the Member States, as "regulatory brutality"[89] that is likely to ignore Member States' particularities and is not

---

[83] Consolidated version of the Treaty on the Functioning of the European Union, OJ (2012) C 326/47, 26 October 2012.

[84] Explanatory Memorandum to the CRA Proposal, 3 et seq.

[85] Miadzvetskaya Yuliya/Wessel Ramses A., The Externalisation of the EU's Cybersecurity Regime: The Cyber Diplomacy Toolbox, European Papers 2021, 419.

[86] Bendiek/Pander (fn 57), 3; Wessel Ramses A., European Law and Cyberspace, in: Tsagourias Nicholas/Buchan Russell (eds.), Research Handbook on International Law and Cyberspace, Cheltenham 2021.

[87] Brandão/Camisão (fn 53), 1338; Fuster/Jasmontaite (fn 56), 107.

[88] Bendiek/Pander (fn 57), 7; Miadzvetskaya/Wessel (fn 85), 419; cf. Case C-217/04 United Kingdom vs. European Parliament and Council ECLI:EU:C:2006:279 and Joined Cases C-293/12 and C-594/12 Digital Rights Ireland Ltd ECLI:EU:C:2014:238.

[89] Papakonstantinou Vagelis/De Hert Paul, The Regulation of Digital Technologies in the EU: The Law-making Phenomena of "actification", "GDPR mimesis" and "EU law brutality", TechReg 2022, 56.

about harmonization but rather about implanting of entirely new regimes. With regard to the CRA, such a deep type of intervention – as will be shown in more detail below – is likely to occur in some but not all affected domains.

2.   Extensive material scope

The proposed CRA comes with a wide material scope as it applies to all "products with digital elements whose intended or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network."[90] "Products with digital elements" are defined as "any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately."[91] Due to the use of "or", the definition of "products with digital elements" can be read to include software as a separate product from the hardware.[92] This reading seems to be confirmed by Recital 46 CRA, which refers to "software products" as well as by the fact that, according to the Explanatory Memorandum, non-embedded software is also covered, as it is often exposed to vulnerabilities.[93]

Furthermore, the CRA seems to not only encompass "finished" software and hardware products but also components thereof, as Art. 3(2) also refers to "software and hardware components to be placed on the market separately". Accordingly, the scope of protection not only covers end devices like smartphones, smart speakers, sensors, smart meters, routers, industrial control systems as well as software like desktop applications, video games and operating systems but also components such as computer processing units (CPUs) and software libraries.[94] Covered are also artificial intelligence (AI) systems, including products with digital elements that are classified as high-risk AI systems.[95]

Overall, the CRA's scope of application is very broad and basically all products with digital elements are covered.[96] This appears well justified since potentially all products with digital elements integrated in or connected to a larger electronic information system can serve as an entry point for attack by

---

[90]   Art. 2(1) CRA Proposal.
[91]   Art. 3 point (1) CRA Proposal.
[92]   Chiara, Cyber Resilience Act (fn 8), 258.
[93]   Explanatory Memorandum to the CRA Proposal, 7.
[94]   Impact Assessment Report, part 1 (fn 9), 2.
[95]   Car/De Luca (fn 14), 6.
[96]   European Economic and Social Committee (fn 23), 2; Chiara, Cyber Resilience Act (fn 8), 257 et seq.

malicious actors,[97] and that vulnerabilities are found not only in end products, but also in intermediate software components.[98] Despite subscribing to this all-encompassing approach along the lines of "[c]ybersecurity of the entire ecosystem is ensured only if all its components are cyber-secure,"[99] the European Commission also takes into account that not all products with digital elements are equally critical and therefore introduces a graduated series of obligations, as shown below.

Some products are also explicitly excluded from the CRA's scope of application. First of all, the CRA does not apply to products with digital elements that already fall under specific sectoral regulation with correspond-ing cybersecurity requirements,[100] such as medical devices[101] and in vitro diagnostic medical devices,[102] as well as products covered by the Vehicle General Safety Regulation[103] and the Regulation on common rules in civil

---

[97] Cf. Recital 7 CRA Proposal.

[98] Cf. Impact Assessment Report, part 1 (fn 9), 7.

[99] Explanatory Memorandum to the CRA Proposal, 2.

[100] Cf. Recitals 12 and 13 and Art. 2(2 and 3) CRA Proposal; Chiara, Cyber Resilience Act (fn 8), 259.

[101] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC, OJ (2017) L 117/1.

[102] Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU, OJ (2017) L 117/176.

[103] Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166, OJ (2019) L 325/1.

aviation.[104] The European Data Protection Supervisor (EDPS) has noted however that the Regulation on medical devices is not detailed and specific enough to meet the cybersecurity standards of the CRA, contrary to what is purported in Recital 12 CRA. The EDPS thus recommends that this particular Regulation should be deleted from the list of legislation excluded from the scope of the CRA.[105]

Additionally, Art. 2(5) CRA excludes products with digital elements developed exclusively for national security or military purposes and products specifically designed to process classified information from its scope of application. However, a large share of products used in the defence sector are civil and dual-use products with digital elements[106] and are accordingly subject to the CRA.

A further exception can be found in Recital 10 CRA, which stipulates that "free and open source software developed or supplied outside the course of a commercial activity" should not be covered by the CRA to avoid hampering innovation and research. While the objective of this exemption is to be welcomed, it merits clarity. First of all, the CRA does not define relevant terms such as "free software", "open source software" and "free and open source software".[107] Further is the scope of "commercial activity" unclear as according to Recital 10, a commercial activity can be characterized not only by charging a price for a product but for instance also by charging a price for technical support services. Should the scope of Recital 10 CRA remain unclear, there are concerns that the certification process and the fines that could be applied under the adopted CRA could impede the development of open source software and cause open source products to be withdrawn from the internal

---

104   Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/9, OJ (2018) L 212/1.

105   European Data Protection Supervisor, Opinion 23/2022 on the Proposal for a Regulation of the European Parliament and of the Council on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulation (EU) 2019/1020, November 2022, <https://edps.europa.eu/system/files/2022-11/2022-0921_d2649_opinion_en.pdf>, 8.

106   High Representative of the Union for Foreign Affairs and Security Policy, Joint Communication to the European Parliament and the Council, EU Policy on Cyber Defence, JOIN(2022) 49 final, 10 November 2022, 11.

107   European Data Protection Supervisor (fn 105), 10.

market, which could affect innovation in Europe.[108] Yet, it should be borne in mind that often commercial software relies on open source components and such components might exhibit vulnerabilities,[109] just as recently seen with Log4Shell, a zero-day vulnerability in Log4j.[110] The open source library Log4j is used by many major software manufacturers and the vulnerability thus led to security incidents around the world.[111] It is therefore necessary to formulate an exception that provides clarity as well as an appropriate balance in terms of responsibility.

Another exception is formulated in Recital 9 CRA. It indicates that Software-as-a-Service (SaaS) is not covered by the CRA, except for "remote data processing solutions relating to a product with digital elements". This exception is intended to ensure that there is no overlap resulting from SaaS already covered by the NIS2 Directive and the catch-all scope of application of the CRA.[112] However, as products that rely on "remote data processing" are not excluded by Recital 9, it is possible that SaaS is nonetheless, at least partially, included in CRA's scope, given that virtually all SaaS products rely on "remote data processing".[113] Clarification in this respect seems to be underway, as it is reported that the new version of the CRA text from the Czech presidency, dated 2 December 2022, clearly excludes SaaS from the scope of the CRA.[114] The text also clarifies that websites would not qualify as remote data processing solutions of web browsers, because they are not developed under the control of the browser manufacturer, and the browser would not be prevented from functioning if single website were absent.[115]

---

[108]   Car/De Luca (fn 14), 9; Ilkka Turunen, Europe's Cyber Security Strategy Must Be Clear about Open Source, Computer Weekly.com, 12 January 2023, <https://www.computerweekly.com/opinion/Europes-cyber-security-strategy-must-be-clear-about-open-source>.

[109]   Kazakova Anastasiya/Kumagin Igor, The EU's Upcoming Cyber Resilience Act Should Set New Rules for the Game, June 2022, <https://www.kaspersky.com/about/policy-blog/index/the-eus-upcoming-cyber-resilience-act-should-set-new-rules-for-the-game>.

[110]   Wortley Free/Thompson Chris/Allison Forrest, Log4Shell: RCE 0-Day Exploit Found in log4j, a Popular Java Logging Package, December 2021, <https://www.lunasec.io/docs/blog/log4j-zero-day/>.

[111]   Impact Assessment Report, part 1 (fn 9), 7.

[112]   Explanatory Memorandum to the CRA Proposal, 2 et seq.

[113]   Chiara, Cyber Resilience Act (fn 8), 259.

[114]   Bertuzzi Luca, EU Council Moves to Exclude Software-as-a-Service from New Cybersecurity Law, EURACTIV.com, 9 December 2022, <https://www.euractiv.com/section/cybersecurity/news/eu-council-moves-to-exclude-software-as-a-service-from-new-cybersecurity-law/> (cit.: Bertuzzi, December 2022).

[115]   Bertuzzi, December 2022 (fn 114).

Overall, more clarification on the scope of the proposal is clearly needed[116] and this is likely to be addressed in the next legislative steps of adopting the CRA.

3.   Complex interplay with other regulations

The above definitional dilemmas are also indicative of the problem that, due to the broad scope of the CRA, there may be overlaps with other laws in the field and the respective scopes of application may not be clearly distinguishable from one another. As the CRA is seen as "the missing piece of the puzzle completing the picture of EU cybersecurity policies",[117] it is critical that it dovetails with the existing as well as the proposed legislation in the digital domain addressing products' cybersecurity, either directly or indirectly.

The interplay between the CRA and other legislation prescribing cybersecurity requirements for products with digital elements is addressed by Art. 2(4).[118] Next to the above-mentioned exemptions, Art. 2(4) can be seen as operational-izing "a rule of prevalence", as it provides criteria to determine whether other legal acts, which address all or some of the risks covered by the essential requirements laid down in Annex I of the CRA, may prevail over the CRA.[119] Having some criteria in place is paramount in light of the fact that Recital 14 states that sectoral or product-specific Union legislation may be introduced – i.e., there is a possibility that after enactment of the CRA, further sector-specific legislation may follow, whose interplay with the CRA would need to be clarified.

The CRA does provide also explicit guidance on its interplay with certain existing pieces of legislation – such as the Cybersecurity Act, the NIS2 Directive, the GDPR, as well as the proposed AI Act[120]. In relation to the Cybersecurity Act, the CRA aims to exploit synergies mainly with regard to the conformity assessment process.[121] Pursuant to Article 18(3) and (4) CRA, the relationship between the CRA and the Cybersecurity Act is such that

---

[116]   Council of the European Union, Progress Report (fn 82), 5.

[117]   Impact Assessment Report, part 1 (fn 9), 4.

[118]   Chiara, Cyber Resilience Act (fn 8), 266.

[119]   Chiara, Cyber Resilience Act (fn 8), 266. According to Art. 2(4) the application of the CRA may be limited or excluded where such a limitation or exclusion is consistent with the overall regulatory framework applying to those products and if the sectoral rules achieve the same level of protection as the one provided for by the CRA.

[120]   Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM(2021) 206, 21 April 2021 [hereinafter AI Act].

[121]   Car/De Luca (fn 14), 8.

digital products that comply with the voluntary cybersecurity certification schemes are deemed to comply with the CRA's conformity assessment.[122] With respect to the NIS2 Directive, the CRA intends to complement it in that it seeks to make it easier for digital infrastructure providers to meet the supply chain requirements under the NIS2 Directive by ensuring that the products with digital elements that they use to deliver their services are developed in a secure manner and that they have access to timely security updates for those products.[123] Similarly to the NIS2 Directive, the CRA aims to complement the GDPR[124] and exploit synergies. Pursuant to Recital 17, the CRA should be without prejudice to the GDPR. Rather the CRA is intended to contribute to the protection of personal data and privacy of individuals and to create synergies in both standardization and certification on cybersecurity, as well as in the area of market surveillance and enforcement.[125] However, the EDPS has observed that the governance provisions of Recital 17 are not fully mirrored in the operative part of the CRA. In the absence of clear provisions, the EDPS is concerned that synergies are unlikely to be achieved in practice and recommends inter alia specifying the synergies between the CRA and the GDPR in the area of market surveillance and enforcement.[126]

Finally, with respect to the proposed AI Act the general rule is that for products with digital elements covered by the CRA that are simultaneously classified as "high-risk AI systems" under the AI proposal, the CRA's conformity assessment procedure shall apply to demonstrate their compliance with the security requirements of the proposed AI Act.[127] Exceptions apply for certain AI critical products.[128]

There are further provisions on the CRA's interface[129] that include: clarification on the interplay between the CRA and the General Product Safety Regulation

---

[122] Car/De Luca (fn 14), 8.

[123] Recital 11 CRA Proposal. For more details: Chiara, Cyber Resilience Act (fn 8), 270 and Schmitz-Berndt/Cole (fn 58), 12 et seq.

[124] For general observations on the relationship between cybersecurity and data protection, cf. Kuner Christopher et al., The Rise of Cybersecurity and Its Impact on Data Protection, International Data Privacy Law 2017, 73.

[125] Recital 17 CRA Proposal.

[126] European Data Protection Supervisor (fn 105), 8.

[127] Art. 8 and Recital 29 CRA Proposal; European Economic and Social Committee (fn 23), 3.

[128] Car/De Luca (fn 14), 8.

[129] Besides the ones mentioned, there are also some provisions in Recitals 30 and 31 CRA Proposal.

(Art. 7);[130] CRA's interface with the Machinery Regulation Proposal (Art. 9);[131] and with the Delegated Act to the Radio Equipment Directive (RED) (Recital 15).[132]. As regards the latter, it should be noted that to avoid a regulatory overlap, it is planned that the Commission would repeal or amend the RED delegated regulation with respect to the radio equipment covered by the CRA, so that the latter one would apply to it.[133]

Yet, despite all these clarifications on the interplay with other regulations one can find in the CRA, there is a possibility that its broad horizontal scope will not straightforwardly lead to a streamlined regulatory landscape. Given the complex legal landscape, and considering that further regulations are in the making, it would be desirable that the Commission develops guidelines to provide better guidance to manufacturers and consumers on the exact rules and procedures that apply in practice.[134] Otherwise, there is a risk that the CRA will fall short of its objective for coherent regulation by merely adding an additional layer of requirements, thereby making it even more complicated for addressees to navigate the legislative landscape and exacerbating the problems that it is indeed intended to tackle.[135]

4.   Addressees along the supply chain

The CRA not only has a wide scope of material application, but also its personal scope is comprehensive, as the CRA addresses all market participants involved in the supply chain: from manufacturers to distributors and importers.[136] This is new and remarkable in the field of EU cybersecurity law.[137] Depending on the classification as either manufacturer, importer or distributor, economic operators are subject to different obligations,[138] which are discussed below.

---

[130]   For more details: Chiara, Cyber Resilience Act (fn 8), 267.

[131]   For more details: Chiara, Cyber Resilience Act (fn 8), 268.

[132]   For more details: Chiara, Cyber Resilience Act (fn 8), 268.

[133]   Explanatory Memorandum to the CRA Proposal, 4.

[134]   Cf. European Economic and Social Committee (fn 23), 1.

[135]   Cf. Digitaleurope, Building Blocks for a Scalable Cyber Resilience Act, May 2022, <https://digital-europe-website-v1.s3.fr-par.scw.cloud/uploads/2022/05/Building-blocks-for-a-scalable-Cyber-Resilience-Act.pdf>, 5.

[136]   Cf. Art. 3 point (17) CRA Proposal.

[137]   Chiara, Cyber Resilience Act (fn 8), 260; Kipker Dennis-Kenji, Der EU "Cyber Resilience Act" kommt – und mit ihm die umfassendsten Compliance-Pflichten in der IT-Sicherheit, die es jemals gab, MMR-Aktuell 2022.

[138]   Section C.III.

According to Art. 3(18) CRA, a manufacturer is a natural or legal person who develops or manufactures a product with digital elements himself, or who has such products designed, developed or manufactured by third parties and then markets these products under his own name or trademark, irrespective of whether this is done for a fee or free of charge.[139] An importer is a natural or legal person established in the EU who places on the market a product with digital elements that bears the name or trademark of a natural or legal person established outside the EU.[140] "Placing on the market" means thereby the first making available on the Union market.[141] A natural or legal person in the supply chain, other than the manufacturer or the importer, that supplies product with digital elements for distribution or use on the Union market in the course of a commercial activity without affecting the devices properties is deemed to be a distributor.[142]

It should be noted that the CRA, like other cybersecurity legislation,[143] does not grant rights to individuals and they are not addressees of the regulation. However, users may still fall within the scope of the CRA. This is the case if Art. 16 CRA comes into play. This provision stipulates that a "natural or legal person, other than the manufacturer, the importer or the distributor, that carries out a substantial modification of the product with digital elements shall be considered a manufacturer". "Substantial modifications" are any changes to the product that affect the product's compliance with the essential cybersecurity requirements of Section 1 of Annex I, or results in a change of its intended use.[144] Pursuant to Recital 24 refurbishing, maintaining as well as repairing a product with digital elements are not to considered as substantial modifications, as long as the intended use and functionalities remain unchanged and the level of risk unaffected. Yet, if functional upgrades are made in the course of these activities, a substantial change may occur.[145] So to put it simply, if users (be it natural or legal persons) elevate themselves to a position similar to the role of manufacturer by making substantial changes to a product they may be subject to individual manufacturer obligations.[146] The consequence of this is that the person is, pursuant to Art. 16 CRA, "subject to

---

[139]   Art. 3 point (18) CRA Proposal.
[140]   Art. 3 point (20) CRA Proposal.
[141]   Art. 3 point (22) CRA Proposal.
[142]   Art. 3 point (21) CRA Proposal in connection with Art. 3 point (23) CRA Proposal.
[143]   Cf. Markopouloua/Papakonstantinou/De Hert (fn 58), 11.
[144]   Art. 3 point (31) CRA Proposal.
[145]   Zirnstein Yannick, Der Entwurf des Cyber Resilience Act, Computer und Recht 2022, 711 et seq.
[146]   Zirnstein (fn 145), 711.

the obligations of the manufacturer set out in Articles 10 and 11(1), (2), (4) and (7), for the part of the product that is affected by the substantial modification or, if the substantial modification has an impact on the cybersecurity of the product with digital elements as a whole, for the entire product". Bearing in mind the burdensome obligations the manufacturer has to fulfil[147] and the heavy fines that can be imposed in the case of non-compliance,[148] as well as the consumer protection rationale inherent in the CRA, one can reasonably ask if Art. 16 goes too far.[149] Some of this excess possibility seems acknowledged by the CRA, as it states in Recital 66 that when fining persons, their economic situation as well as the general level of income in the respective Member State should be taken into account.

5.   CRA's territorial scope

The CRA does not contain any explicit provisions on the territorial scope of its application.[150] However, the various references to products with digital elements that are "placed on the EU market" or "made available on the market" indicate that the CRA applies to such products that are offered for sale or use in the Union.[151] In particular Art. 1(a) states that the CRA lays down "rules for the placing on the market for products with digital elements".[152] "Placing on the market" means making available on the EU market for the first time, which is the supply of a product with digital elements for distribution or use on the EU market in the course of a commercial activity, regardless of whether this is done for payment or free of charge.[153] It appears that it is this particular link with the EU market that triggers the CRA's application.

At the same time, if one looks at the various definitions of the different economic operators, it is noticeable that the definition of the manufacturer,

---

[147]   Section C.III.1.

[148]   Section C.V.

[149]   Cf. Zußner Matthias, Das Inverkehrbringen von Produkten mit digitalen Elementen nach dem Vorschlag der EU-Kommission für eine Verordnung über horizontale Cybersicherheitsanforderungen, Austrian Law Journal 2022, 196 et seq.

[150]   Zirnstein (fn 145), 709.

[151]   Tuninetti Ferrari Andrea et al., EU Cyber Resilience Act - Proposed Cyber-Security Rules for Connected Products, Clifford Chance Briefing, November 2022, <https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2022/11/EU-Cyber-Resilience-Act-Proposed-Cyber-Security-Rules-for-Connected-Products.pdf>, 2.

[152]   In the same sense Recital 1 reads: "It is necessary to improve the functioning of the internal market by laying down a uniform legal framework for essential cybersecurity requirements for placing products with digital elements on the Union market."

[153]   Art. 3 point (22) and (23) CRA Proposal.

unlike that of importer and distributor, does not make reference to the Union. According to Zirnstein, this is an indication that the CRA strives for an extra-territorial application since although manufacturers could disregard the CRA's safety requirements if they are based outside the Union, importers would not be allowed to import any of these products into the European market, as they must attest that manufacturers' products ensure compliance with the requirements of Annex I CRA. In other words, the scope of the Regulation extends beyond the EU borders as any manufacturer based outside the EU exporting to EU Member States is subject to the legislation in the sense that its importer and (less so) distributor are liable for their compliance.[154]

Given that the CRA is likely to also apply to digital products from non-EU manufacturers once they are placed on the EU market, the CRA would impact cybersecurity standards for such products beyond the EU's borders. As earlier mentioned, non-EU operators striving for efficiency might follow the CRA's rules as a default framework for their global operations – thus fueling the "Brussels effect" in an important manner and establishing the EU as the global standard-setter for the cybersecurity of connected devices.[155]

II. Risk-based classification of products

As seen before, the CRA covers a broad range of products. However, based on their level of risk, the CRA splits these products in two main categories: (1) default non-critical products, i.e., hardware and software with a low level of criticality[156] and (2) "critical products". The latter are products listed in Annex III, as well as products that have the core functionality of a category that is listed in Annex III.[157] Reflecting their inherent level of cybersecurity risk, the critical products are then divided into class I and class II as set out in Annex III.[158] This risk-based approach is typical for many of the CRA's rules but is certainly not unique to it.[159] It has indeed become a feature of EU's regulation

---

[154] Cf. Sections C.III.2. and C.III.3 below for further clarification.

[155] Car/De Luca (fn 14), 6; Bertuzzi Luca, Commission Expects to Set the World's Cybersecurity Standards for Connected Devices, EURACTIV.com, 27 September 2022, <https://www.euractiv.com/section/cybersecurity/news/commission-expects-to-set-the-worlds-cybersecurity-standards-for-connected-devices/> (cit.: Bertuzzi, September 2022).

[156] Car/De Luca (fn 14), 6.

[157] Art. 6(1) CRA Proposal.

[158] Art. 6(1) CRA Proposal.

[159] Chiara, Cyber Resilience Act (fn 8), 259.

of new technologies and is prominently showcased by the GDPR,[160] as well as by recent legislative developments, such as the proposed AI Act and the 2022 Digital Services Act (DSA).[161]

Following the risk-based approach, manufacturers must assess the cybersecurity risks associated with a product category and take this into account during the planning, design, development, manufacturing, distribution and maintenance of the product with digital elements.[162] While all products, regardless of their classification, must meet the essential cybersecurity requirements of Annex I, depending on their classification, products are subject to different conformity assessment procedures,[163] as we show below.

The EU estimates that the vast majority of products with digital elements (90%) will fall into the "default" category and only 10% are going to be classified as "critical".[164] The "default" category contains products such as photo-editing software, video games, smart speakers and hard drives.[165] Pursuant to Annex III, critical "class I" products with digital elements are password managers, network interfaces, firewalls, and microcontrollers.[166] Highly critical products, i.e., critical "class II" products are among others operating systems for servers, desktops and mobile devices, smart meters, CPUs and robot controllers.[167]

Annex III is however not conceived as an exhaustive list. Rather, the European Commission is empowered to adopt delegated acts to amend it,[168] and so

---

[160] De Gregorio Giovanni/Dunn Pietro, The European Risk-based Approaches: Connecting Constitutional Dots in the Digital Age, Common Market Law Review 2022, 476.

[161] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ (2022) L 277/1 [hereinafter DSA]. However, those regulations differ in their approach towards risk regulation; De Gregorio/Dunn (fn 160), 477.

[162] Chiara, Cyber Resilience Act (fn 8), 261.

[163] Chiara, Cyber Resilience Act (fn 8), 260.

[164] European Commission, Directorate-General for Communications Networks, Content and Technology, Cyber Resilience Act: New EU Cybersecurity Rules Ensure More Secure Hardware and Software Products, September 2022, <https://data.europa.eu/doi/10.2759/543836>.

[165] European Commission, Directorate-General for Communications Networks, Content and Technology (fn 164).

[166] Annex III of the CRA Proposal; cf. European Commission, Directorate-General for Communications Networks, Content and Technology (fn 164).

[167] Annex III of the CRA Proposal; European Commission, Directorate-General for Communications Networks, Content and Technology (fn 164).

[168] Art. 6(2) CRA Proposal.

if needed, take into account technical innovations. In view of the rapid technological developments and the related possibility that the risks of the products may change, the list will probably need to be continuously reviewed.[169] However, it is doubtful whether the proposed review process can accommodate all developments. Already now the list of Annex III seems somewhat incomplete, given that tangible and intangible products with digital elements that perform cryptographic operations are not listed, while such products are of importance for effective information security, cybersecurity, data protection and privacy, and might be exposed to attacks.[170]

Another critical issue with the listing of Annex III is that it is unclear which criteria the Commission applied to identify and classify the listed products.[171] This could change insofar as Art. 6(3) CRA indicates that the Commission shall specify the characteristics of the product categories listed in Annex III in a delegated act to provide operators with guidance on how to determine with certainty whether and how their products are to be classified. Moreover, Recital 25 and Art. 6(2) CRA provide some criteria for determining if a product with digital elements is to be deemed "critical". Pursuant to Recital 25 "[p]roducts with digital elements should be considered critical if the negative impact of the exploitation of potential cybersecurity vulnerabilities in the product can be severe due to, amongst others, the cybersecurity-related functionality, or the intended use." Accordingly, one criterion for assessing the level of the cybersecurity risk of a product is whether it runs with privilege, privileged access, or performs a function critical to trust,[172] as such attributes can lead to a propagation of security issues throughout the supply chain.[173] Further criteria are the intended use in sensitive environments such as in industrial settings[174] or the intended use for the processing of personal data,[175] as well as the potential impact of an incident, in particular its ability to affect a large number of people.[176] That last criterion seems to be linked to the market share of a product. But this again runs the danger that products that are

---

Cf. Brass Irina/Sowell Jesse H., Adaptive Governance for the Internet of Things: Coping with Emerging Security Risks, Regulation & Governance 2021, 1102.

[170] Cf. European Data Protection Supervisor (fn 105), 7.

[171] Cf. TÜV Verband, Position Paper on the EU Commission Proposal for a Cyber Resilience Act, December 2022, <https://www.tuev-verband.de/index.php?eID=dumpFile&t=f&f=2933&token=b28683b4eaf5f0c41236b49c3373ea6852eaa17d>, 4.

[172] Art 6(2) point a) CRA Proposal.

[173] Recital 25 CRA Proposal.

[174] Explanatory Memorandum to the CRA Proposal, 9 et seq.

[175] Art. 6(2) point c) CRA Proposal.

[176] Art. 6(2) point d) CRA Proposal.

not bestsellers would be deemed to be less risky merely because they have a smaller market share and therefore lesser ability to affect many people in case of an incident.

It is furthermore noteworthy that most of the criteria seem to mainly focus on the industrial side.[177] The classification in Annex III, respectively the classification of certain products as "non-critical" appears to indicate that the Commission deems industrial IoT more critical than consumer IoT, such as for instance smart speakers. This approach, however, may underestimate the fact that certain products should be treated as riskier since they are used to keep the user safe in the physical world, such as smart homes and security alarms, may process privacy-relevant data and/or are used by children.[178] Also, as the CRA classifies categories of products, it may unduly disregard the "operational environment" in which a product will be placed, even though threats and related risks of products can be extremely different depending on where they are used.[179] For instance, smart LED bulbs would likely be classified as non-critical products. However, if a smart LED light bulb is compromised, it can serve as a gateway into the network it is connected to and the threat can spread to an entire network.[180] If a smart LED bulb is used in a private home network, the ramifications of its compromise may be less problematic. However, if such a light bulb is in use in a factory and can thus be exploited as an entry point into the factory's network and for example be used to shut down the factory's production, the consequences could be much more widespread. Yet, this can also be the case in reverse, in particular in that industrial components are used for non-critical purposes.[181] Consequently, it is questionable if the "list-based" approach of Annex III is sufficiently robust to reflect the risks posed by products with digital elements under different circumstances.

---

[177] Cf. Euroconsumers, EU Cyber Resilience Act: Will the Hackable Home Finally Be Secured?, September 2022, <https://www.euroconsumers.org/activities/cyber-resilience-act-will-hackable-home-be-secured>.

[178] TÜV Verband (fn 171), 5; Bertuzzi, September 2022 (fn 155).

[179] Cf. Digitaleurope (fn 135), 6.

[180] Cf. Interagency International Cybersecurity Standardization Working Group (IICS WG), Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things (IoT), November 2018, <https://csrc.nist.gov/publications/detail/nistir/8200/fina>, 13 et seq.; cf. Johnson et al. (fn 7), 721.

[181] Cf. VDMA, Uniform Cybersecurity Requirements Are the Only Right Way Forward, September 2022, <https://www.vdma.org/viewer/-/v2article/render/67648803>; ZVEI Germany's Electro and Digital Industry, Cyber Resilience Act: Important Step for More Cyber Security, September 2022, <https://www.zvei.org/en/press-media/pressarea/cyber-resilience-act-important-step-for-more-cyber-security>.

Some of the above points of critique appear to be addressed by a recently shared new compromise text of the Swedish presidency of the EU Council of Ministers. It is reported that this compromise comes with significant changes on the classification of critical and highly critical products and sheds some light on why and which products qualify as critical class I or class II products. Furthermore, the list of products was revised in that, inter alia, class I and class II products were divided into subgroups and consumer products such as smart locks and alarm systems were included.[182]

III. Obligations of economic operators along the supply chain and throughout the life-cycle of products

As noted earlier, the addressees of the CRA are the economic operators, in particular manufacturers, importers and distributors of products with digital elements.[183] These economic operators – depending on their role and responsibility within the supply chain – have to fulfil several obligations before and during the placing on the market of a product.[184] As the next sections show, there is a sliding scale of regulatory burden, starting with manufacturers at the top towards distributors at the scale's bottom.

1. Extensive obligations of manufacturers

A large number of obligations of the CRA are imposed primarily on manufacturers. This can arguably be based on the assumption that manufacturers form the beginning of the supply chain, thus having usually the most influence on the conception, design and development of their products.[185]

First of all, it is the obligation of the manufacturer to ensure that, when placing a product with digital elements on the market, it has been designed, developed and produced in accordance with the essential requirements set out in Section 1 of Annex I.[186] Those include the obligation to design, develop and produce products with digital elements in such a way that they ensure an appropriate level of cybersecurity based on their risks. Furthermore, they should not be delivered with known exploitable vulnerabilities, must be

---

[182] Bertuzzi Luca, EU Council Reconsiders Critical Products in New Cybersecurity Law, EURACTIV.com, 15 February 2023, <https://www.euractiv.com/section/cybersecurity/news/eu-council-reconsiders-critical-products-in-new-cybersecurity-law/>.

[183] Section C.I.4.

[184] Car/De Luca (fn 14), 7.

[185] Zirnstein (fn 145), 710.

[186] Art. 10(1) CRA Proposal.

delivered with a secure by default configuration, must protect the confidentiality and integrity of the data they process and only process data, personal or other, that are strictly necessary to the functioning of the product.[187] Yet again, the list in Section 1 of Annex I is not to be understood as exhaustive.[188] While the manufacturers have to comply with all essential requirements related to vulnerability handling and have to ensure that they deliver their products without any known exploitable vulnerability, with respect to the other essential requirements manufacturers have to determine themselves which of them are relevant for the respective type of product.[189] In this sense, manufacturers must take a holistic view of whether the implementation of these requirements alone leads to an appropriate level of cybersecurity of their product or if they have to take additional case-specific measures.[190] This is reminiscent of Art. 32 GDPR in the context of personal data protection that also sets out a non-exhaustive list of security measures to ensure a level of security appropriate to the risk.[191]

Next to requirements that the products be designed, developed, and produced in such a way that they ensure an appropriate level of cybersecurity, the CRA follows the principle of security by design and makes it mandatory.[192] The basic idea behind security by design is that products should be designed with threats to security in mind and that vulnerabilities should be adequately addressed throughout a product's life-cycle.[193] In other words, products should be secure right from the moment they are made available, and they should be secure during their operational phase and remain secure during and after maintenance operations, such as updates. Moreover, once the product has reached its end-of-life, its secure disposal or recycling, especially the

---

[187]   European Economic and Social Committee (fn 23), 2; Car/De Luca (fn 14), 7.
[188]   Zirnstein (fn 145), 710.
[189]   Recital 32 CRA Proposal.
[190]   Zirnstein Yannick/Lee Yue Lin/Ge Amanda, Evolving Cybersecurity Landscape – Comparing the Regulatory Approaches in the EU, in China and in Singapore — An Analysis of Legislative Approaches to Key Issues in Tackling a Global Phenomenon, Computer Law Review International 2022, 167.
[191]   Cf. Haber Eldar/Tamò-Larrieux Aurelia, Privacy and Security by Design: Comparing the EU and Israeli Approaches to Embedding Privacy and Security, Computer Law & Security Review 2020, 4.
[192]   Section 1 (3a) of Annex I of the CRA Proposal. Schmitz-Berndt/Cole (fn 58), 11; cf. Car/De Luca (fn 14), 7.
[193]   Center for Security Studies, Governance Approaches to the Security of Digital Products - A Comparative Analysis, November 2021, <https://genevadialogue.ch/wp-content/uploads/Governance-Approaches-to-the-Security-of-Digital-Products-Report-2021-Geneva-Dialogue-and-EHTZ-CSS.pdf>, 19.

deletion of personal data that it contains, must be provided.[194] The security-by-design model is not new to cybersecurity, as it first emerged from computer engineering principles and was later proposed as a way to mitigate the security vulnerabilities presented by the IoT.[195] Since then, it has been reflected in cybersecurity law,[196] for instance in the NIS Directive and its update, in the Cybersecurity Act as well as in newer EU data governance legislation, such as the proposed AI Act and the Data Act.[197] In light of these similarities in approach, the EDPS has sought to interface the GDPR with the CRA and strongly recommends including data protection by design and by default in the essential cybersecurity requirements for products with digital elements.[198]

While the security-by-design approach set out in Annex I Section 1 is to be welcomed,[199] the requirement that "products with digital elements shall be delivered without any known exploitable vulnerability" might be over-ambitious, considering that for example the vulnerability in Log4j, the case discussed earlier, existed since 2013 and remained unnoticed until the end of 2021, even though Log4j has been highly popular and with widespread use. Ellul et al. argue that software-based products and services are inherently delivered with vulnerabilities, despite the increasing capabilities and ongoing development of technical assurances. This has to do with the common practice of ensuring that no software is released without undergoing testing – that is, the process of evaluating and validating software by running it in a controlled environment. While this practice seems relatively straightforward, the actual process is not. According to Ellul et al. it is not always easy to know what constitutes an appropriate test, and whether a test suite adequately captures the possible behaviour of the system. In addition, it is difficult to simulate the environment in which the system will operate during a test, especially in environments with malicious actors.[200] In this context, it appears that the initial text of the CRA is now being adapted in that the obligation not to place products with known exploitable vulnerabilities on the EU internal

---

[194] van der Schaaf Koen/Tekinerdogan Bedir/Catal Cagatay, A Feature-based Approach for Guiding the Selection of Internet of Things Cybersecurity Standards Using Text Mining, Concurrency and Computation: Practice and Experience 2021, 7 et seq.

[195] Bygrave Lee A., Security by Design: Aspirations and Realities in a Regulatory Context, Oslo Law Review 2021 (cit.: Bygrave, Security by Design), 126.

[196] Bygrave, Security by Design (fn 195), 137 et seq.

[197] Bygrave, Security by Design (fn 195), 138.

[198] European Data Protection Supervisor (fn 105), 7.

[199] European Data Protection Supervisor (fn 105), 2.

[200] Ellul Joshua et al., When Is Good Enough Good Enough? On Software Assurances, ERA Forum 2023.

market will depend on the manufacturer's risk assessment. This means that if manufacturers assess the risk of a vulnerability as very low, the product can still be marketed. This amendment is intended to reduce bureaucracy and take into account cases in which a vulnerability can later be fixed by a security update.[201]

Another obligation towards manufacturers, given the emphasis put on the supply chain security, is the due diligence obligation, when manufacturers source third-party components for their products with digital elements and need to ensure that such components do not compromise the product's cybersecurity.[202] Furthermore, in order to ascertain and demonstrate compliance of their product with the essential cybersecurity requirements, manufacturers are required to undertake an assessment of the cybersecurity risks associated with a product with digital elements.[203] The CRA provides via Chapters III and IV and Annex VI for a rather extensive guidance on the conformity assessment, especially with respect to the procedure as well as on the conformity assessment bodies. Three aspects should be pointed out here: First, under certain conditions, there is a presumption of conformity for products with digital elements and processes put in place by the manufacturer.[204] This is the case, for instance, where European harmonization standards already exist for a particular area[205] and the product in question complies with these standards.[206] A second aspect worth highlighting is the fact that a manufacturer's choice for a conformity assessment procedure set out in Annex VI depends on the risk classification of his product.[207] For non-

---

[201]   Bertuzzi, February 2023 (fn 16).

[202]   Tuninetti Ferrari et al. (fn 151), 3; cf. Chiara, IoT (fn 63), 129.

[203]   Art. 10(2) CRA Proposal. However, under certain conditions, manufacturers are permitted under Recital 20 and Art. 4(3) CRA to release software for testing purposes before subjecting their product to a conformity assessment. Further on this as well as on the research and development indications of the CRA: Rosal Santos Isabela, Horizontal Cybersecurity Requirements: What Does the New European Proposal for Products with Digital Elements Add to R&D?, KU Leuven CiTiP Blog, 17 January 2023, <https://www.law.kuleuven.be/citip/blog/horizontal-cybersecurity-requirements-what-does-the-new-european-proposal-for-products-with-digital-elements-add-to-rd/>.

[204]   Cf. Art. 18 CRA Proposal.

[205]   Further on European cybersecurity certification schemes under the Cybersecurity Act: Kamara Irene, Misaligned Union Laws? A Comparative Analysis of Certification in the Cybersecurity Act and the General Data Protection Regulation, in: Hallinan Dara/Leenes Ronald/De Hert Paul (eds.), Privacy and Data Protection: Artificial Intelligence, Oxford 2020.

[206]   Art. 18(1) CRA Proposal.

[207]   Chiara, Cyber Resilience Act (fn 8), 260.

critical products, manufacturers can exercise a self-assessment, declaring that their products satisfy the essential security requirements of Annex I.[208] Manufacturers of critical product of class I and II however have to demonstrate conformity through an EU-type examination[209] or by full quality assurance[210], the latter involving a third-party.[211] In this sense, the risk-based approach in the product classification is also clearly reflected here. Considering that estimated 90% of the products with digital elements are likely to be classified as non-critical and will not trigger an external assessment, but a self-assessment by manufacturers,[212] this raises some doubts as to whether an adequate level of cybersecurity and a consistently high level of protection in a rapidly changing cybersecurity threat environment would be ensured.[213] And finally, the manufacturer has to provide a declaration of conformity according to Art. 20 CRA and digital products demonstrating compliance must be properly CE marked and may only be placed on the market with such marking.[214] Once a product receives a CE marking, it can be deployed in and move freely within the internal EU market,[215] thus fostering the functioning of the single market for products with digital elements.[216]

Manufacturers have also several documentation obligations. Following Art. 23 they need to draw up a comprehensive technical documentation before the product is placed on the market,[217] with the minimum requirements for this documentation specified in Annex V. Furthermore Art. 10(10) CRA obliges manufacturers to ensure that products are accompanied by the information and instructions set out in Annex II. The information should be provided in an electronic or physical form and the language should be clear, understandable, intelligible and legible.

---

[208]   Car/De Luca (fn 14), 7 et seq.

[209]   Annex VI, Module B CRA Proposal.

[210]   Annex VI, Module H CRA Proposal.

[211]   Explanatory Memorandum to the CRA Proposal, 10 et seq.; Car/De Luca (fn 14), 7 et seq.

[212]   TIC Council, TIC Council Welcomes the European Commission's Proposal for a Cyber Resilience Act, September 2022, <https://www.tic-council.org/news-and-events/news/press-release-tic-council-welcomes-european-commissions-proposal-cyber-resilience-act>; Euroconsumers, (fn 177).

[213]   TÜV Verband (fn 171), 4.

[214]   Arts. 21 and 22 CRA Proposal.

[215]   Art. 4(1) CRA Proposal.

[216]   Zußner (fn 149), 194.

[217]   Chiara, Cyber Resilience Act (fn 8), 261.

Article 10(6) CRA imposes further the obligation on manufacturers, upon placing a product with digital elements on the market, to ensure that vulnerabilities of that product are addressed effectively and in accordance with the essential requirements of Section 2 of Annex I of the CRA during the expected lifetime of the product or during a period of five years from the date on which the product is placed on the market, whichever is shorter. Consequently, during the maximal period of five years manufacturers have to continuously test whether their products still comply with the legal requirements and if this is not the case, they must take all necessary measures to restore compliance.[218]

One finds no explanation in the CRA why the period of five years was chosen.[219] Considering the fact that many products have a longer lifetime, this period may be inadequate, especially since the EU strives for sustainability of products.[220] If products no longer receive security updates after the five years have expired, they can easily turn into a dangerous gateway for attacks.[221] There is a related concern also for products that are already on the market for some time and the five year period has almost expired – let us say after four and half years on the market. Although in this example the user would still benefit from security updates for six months, he may continue to use the product for years afterwards without further receiving security updates. While admittedly, users are provided with the information on the period up to which the manufacturer offers security support as per the information obligations of Art. 10(10) in connection with Annex II, this does not change the potential risk situation for the product, especially as used products can easily be resold on existing auction and other platforms.

These concerns fortunately appear to be addressed in a subsequently agreed upon amendment of the CRA proposal. It is reported that the compromise will be amended in that manufacturers shall ensure the security of their products "for a period of time after the placing on the market, appropriate to the type

---

218 Zirnstein (fn 145), 710.
219 Cf. Kipker (fn 137).
220 Inter alia EU's New Consumer Agenda (Communication from the Commission to the European Parliament and the Council, New Consumer Agenda, COM(2020) 696 final, 13 November 2020) and the Circular Economy Action Plan (Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A New Circular Economy Action Plan, COM(2020) 98 final, 11 March 2020) aim at promoting repair and encouraging more sustainable products.
221 Zirnstein (fn 145), 710 et seq.; cf. Euroconsumers (fn 177).

of product and its expected lifetime."[222] This adequately takes into account now that each product has a different life-cycle, which the manufacturer has to assess himself, based on the time that users reasonably expect to receive security updates, considering the functionality and the intended use of the product. Further, the manufacturer has a duty of care to provide security updates for at least 10 years. The same period applies if the manufacturer becomes aware or has reason to believe that his product no longer complies with the security requirements of the CRA.[223]

Still, there is a concern as to how the end of the update obligation is to be assessed in light of the idea of security by design, which entails a life-cycle approach. The CRA seems to follow this life-cycle approach for most parts as Art. 10(1) demands products to be designed, developed and produced in accordance with the essential cybersecurity requirements and Art. 10(6) lays down essential requirements for vulnerability handling. Apart from the above noted dilemmas around a product's operation phase and the associated with it obligations, at some point, the product will reach its end of lifespan. Yet, one finds no security requirements in the CRA that would address how to ensure products' cybersecurity at the end of its life-cycle. The secure disposal of a device, especially the secure removal of information in the device, is at the same time absolutely key.[224] Information erasing is also elemental where the device is not completely decommissioned but reused or refurbished.[225] Furthermore, the big question looms of how all these obligations are to be realized in practice.[226] In reality, it is common that the manufacturer does not know the end user because the product with digital elements is not sold directly by the manufacturer but through distributors, or the product has been resold.

Finally, manufacturers carry certain reporting obligations. Pursuant to Art. 11 CRA, the manufacturer must report any actively exploited vulnerability of a product with digital elements and any incident affecting its security to ENISA without delay, but within 24 hours of becoming aware of them. The

---

[222]   Bertuzzi, February 2023 (fn 16).

[223]   Bertuzzi, February 2023 (fn 16).

[224]   European Union Agency for Cybersecurity, Guidelines for Securing the Internet of Things, Secure Supply Chain for IoT, November 2020, <https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things/@@download/fullReport>, 12; van der Schaaf/Tekinerdogan/Catal (fn 194), 7 et seq.

[225]   European Union Agency for Cybersecurity (fn 224), 12.

[226]   Cf. Nai Fovino Igor et al., Cybersecurity, Our Digital Anchor, June 2020, <https://publications.jrc.ec.europa.eu/repository/bitstream/JRC121051/cybersecurity_online.pdf>, 90.

manufacturer must also notify without delay the users of the product, irrespective of the risk, and inform them of corrective measures they can take.[227] Here, the CRA seems to diverge from the GDPR, which, based on its risk-based approach, requires data breach notification of users, respectively data subjects, only if the breach is likely to result in a high risk to the rights and freedoms of natural persons.[228] Also the NIS2 Directive only requires a notification to users in case of "significant incidents that are likely to adversely affect the provision of the services" of the entities.[229]

While swift reporting of incidents seems sensible, given that security incidents can spread within minutes, the formulation "any incident" in Art. 11(2) CRA can be understood as that every vulnerability, even if it poses no noticeable impact on the security of a product, triggers the reporting obligation of the manufacturer. Furthermore, the CRA reporting obligations are not aligned with processes that are already in place – for instance, the timeframe of 24 hours differs from the 72 hours given under the GDPR and the NIS2 Directive.[230]

As with previous concerns, these seem to be recognized and there is an effort to tackle them. A newly reached compromise strives in this sense to align the CRA reporting obligation with the NIS2 Directive, shifting also the reporting from ENISA to the national Computer Security Incident Response Team (CSIRT).[231]

2.   Importers as watchdogs

While importers themselves are not responsible for ensuring that products meet the essential cybersecurity requirements set out in Section 1 of Annex I, they are not permitted to import products into the European market that do not meet the respective requirements.[232] In case an importer considers or has reason to believe that a product is non-compliant, he should refrain from placing the product on the market until it has been brought into conformity by the manufacturer.[233] Consequently, in order to avoid infringing their own obligations, it will be imperative for importers to carry out a full inspection

---

[227]   Art. 11(1) and (2) CRA Proposal.

[228]   Cf. Haber/Tamò-Larrieux (fn 191), 4.

[229]   Art. 23(1) NIS2 Directive.

[230]   Art. 32(1) GDPR; Art. 23(4) NIS2 Directive.

[231]   Bertuzzi, February 2023 (fn 16).

[232]   Art. 13(1) CRA Proposal.

[233]   Art. 13(3) CRA Proposal.

of every product that they wish to import,[234] although Art. 13(2) CRA only obliges them to ensure that the manufacturer has carried out the appropriate conformity assessment procedures and has drawn up the technical documentation. Furthermore, they have to check that the product bears the CE marking and is accompanied by the instructions and information set out in Annex II.

By imposing such obligations on the importer, in particular to verify that the manufacturer is complying with his obligations under Section I of Annex I, Art. 13 assigns a "watchdog" function to the importer vis-à-vis the manufacturer. This role is also observable in Art. 13(6) CRA, which obliges the importer to support manufacturers in their vulnerability management and inform the manufacturer immediately if they become aware of a vulnerability. In addition, if the respective product poses a significant cybersecurity risk from the importer's perspective, importers must also inform the market surveillance authority.[235] Apart from this "watchdog" role, importers carry certain transparency related duties and must provide their contact details in the way specified in Art. 13(4) CRA.

3.   Few duties for distributors

Unlike the importer, the distributor does not have to verify whether a manufacturer's products comply with the essential cybersecurity requirements. Before making the product available on the market, the distributor only has to check whether the product bears the CE marking and whether the manufacturer and the importer have complied with the obligations set out respectively in Arts. 10(10), 10(11) and 13(4)[236] – that is, whether the manufacturer has provided the required information according to Annex II as well as the declaration of conformity and, in the case of the importer, whether the name and contact information are provided.

These "light" obligations of the distributor, compared to the ones of the manufacturer and importer, can be explained by the fact that the distributor forms the end of the supply chain and as such has no relevant influence on the development, manufacturing and upstream distribution process.[237] Still, the distributor seems to be assigned also with some watchdog functions in that, like the importer, the distributor may not (or no longer) place a product on the market in case he believes or has reason to believe that a product is not in

---

[234]   Zirnstein (fn 145), 711.

[235]   Art. 13(3) CRA Proposal.

[236]   Art. 14(2) CRA Proposal.

[237]   Zirnstein (fn 145), 711.

conformity with the essential cybersecurity requirements.[238] The distributor must also inform the manufacturer, as well as the market surveillance authority, if a products poses a significant cybersecurity risk.[239]

IV. Comprehensive market surveillance and enforcement mechanisms

The CRA grants the European Commission, ENISA as well as national market surveillance authorities comprehensive market surveillance, investigation and ordering competences. Market surveillance for products with digital elements was already introduced with Regulation (EU) 2019/1020[240] on market surveillance and compliance of products by relevant authorities.[241] Member States may designate one or more existing authorities as market surveillance authorities or establish new ones.[242] However, for products with digital elements under the CRA that are classified as high-risk AI systems according to the AI Act, it is the market surveillance authorities pursuant to the AI Act that are responsible.[243]

Market surveillance authorities carry out market surveillance in the territory of the respective Member State. As far as necessary, they must be in constant exchange with their counterparts in other Member States as well as with data protection supervisory authorities.[244] In contrast to the GDPR and the Digital Services Act, the CRA does not create a one-stop-shop mechanism to address cross-border infringements.[245] It does, however, aim to establish a dedicated administrative cooperation group (ADCO) to ensure CRA's uniform application.[246] This ADCO is to be composed of representatives of the market surveillance authorities and representatives of single liaison offices.[247]

---

[238] Art. 14(3) CRA Proposal; cf. Tuninetti Ferrari et al. (fn 151), 5 et seq.

[239] Art. 14(3) CRA Proposal.

[240] Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011, OJ (2019) L 169/1.

[241] Explanatory Memorandum to the CRA Proposal, 11.

[242] Art. 41(2) CRA Proposal.

[243] Art. 41(10) CRA Proposal.

[244] Art. 41(4) and (5) CRA Proposal.

[245] Tuninetti Ferrari et al. (fn 151), 6.

[246] Recital 56 CRA Proposal.

[247] Art. 41(11) CRA Proposal.

The purpose of the national market surveillance authorities is to ensure the effective implementation of the CRA.[248] In order to do so they may initiate investigations following Art. 43 if they have sufficient reason to consider that a product with digital elements presents a significant cybersecurity risk.[249] To be able to evaluate the conformity of products, the authority shall be granted access to the data that it needs to assess the design, development, production and vulnerability handling, including also related internal documentation.[250] Where the market surveillance authority reaches the conclusion that the product does not comply with the requirements of the CRA, it may, commensurate with the nature of the risk, order the relevant operator to take all necessary measures to make the product compliant, to withdraw it from the market or to recall it.[251] If the operator does not take the corrective actions within the given timeframe, the authority shall take the appropriate measure.[252]

In case the Commission has reasons to consider that a product with digital elements is non-compliant with the CRA, the Commission can request the respective national market surveillance authority to carry out an evaluation according to Art. 43.[253] However, it is also possible that the Commission requests ENISA to carry out an evaluation of compliance.[254] This is the case where the exceptional circumstances justify an immediate intervention, there is sufficient reason to consider that the product remains non-compliant, and no effective measures have been taken by the relevant market surveillance authority.[255] Pursuant to Recital 59 CRA, an "exceptional circumstance" is present, for instance where a non-compliant product is made available throughout several Member States, used also in key sectors, and contains known and already exploited vulnerabilities for which the manufacturer does not provide patches. The Commission may intervene, based on ENISA's evaluation, by adopting implementing acts to decide on measures at the Union level, which may include ordering the withdrawal of the product or recalling it.[256]

---

[248]   Art. 41(2) CRA Proposal.
[249]   Zirnstein/Lee/Ge (fn 190), 170.
[250]   Art. 42 CRA Proposal.
[251]   Art. 43(1), (4) and (5) CRA Proposal.
[252]   Chiara, Cyber Resilience Act (fn 8), 265.
[253]   Art. 45(1) CRA Proposal.
[254]   Chiara, Cyber Resilience Act (fn 8), 265.
[255]   Art. 45(2) CRA Proposal.
[256]   Art. 45(3) and (4) CRA Proposal.

Even where products comply with the CRA, market surveillance authorities have the power to intervene via Art. 46. The prerequisite for this is that the product poses a significant cybersecurity risk despite its compliance with the cybersecurity requirements and the product furthermore poses a risk to particular rights or goods,[257] such as the health or safety of persons, compliance risks in relation to fundamental rights or other aspects of the protection of public interests.[258] The criterion "other aspects of the protection of public interests", however, seems rather broad and vague given the fact that if the prerequisites are met, Art. 46(1) provides the market surveillance authority to take the same measures as the authority has in case of non-compliant products, i.e., the authority might even demand the recall of compliant products.[259] It is also with regard to compliant products, where the Commission is provided with the possibility to intervene and establish corrective or restrictive measures, similarly to those under Art. 45 concerning the EU-level procedure for products with digital elements presenting a significant cybersecurity risk.[260]

Apart from these intervention possibilities, following Art. 48 CRA several market surveillance authorities can also agree to carry out joint activities to verify compliance and identify cybersecurity risks of products with digital elements that are often found to present such risks.[261] Joint activities might also be proposed by the Commission or ENISA.[262] Particularly drastic joint activities are the so-called "sweeps".[263] These are simultaneous coordinated control actions of certain products or categories thereof in order to check their compliance with the CRA.[264] In other words, market surveillance authorities can simulate area-wide and cross-border cyberattacks on products that are already on the market and in use.[265] According to Recital 61 CRA, sweeps should particularly be conducted "where market trends, consumer complaints or other indications suggest that certain product categories are often found to present cybersecurity risks." Given that sweeps are an intensive intervention with respect to the rights and freedoms of market participants and users, it can be noted that these criteria are again

---

[257] Zirnstein/Lee/Ge (fn 190), 170.
[258] Art. 46(1) CRA Proposal.
[259] Art. 46(1) CRA Proposal.
[260] Cf. Art. 48(6 et seqq.) CRA Proposal.
[261] Cf. Recital 60 CRA Proposal.
[262] Art. 48(2) CRA Proposal.
[263] Zirnstein (fn 145), 713.
[264] Art. 49(1) CRA Proposal.
[265] Zirnstein (fn 145), 713.

somewhat broad and vague.[266] If clearer criteria not only on the deployment but also on the process of such control actions can be established, such sweeps can be a viable way to verify that a product is secure in practice.[267]

Overall, the monitoring and oversight over the compliance with the CRA is considerable and complex.[268] This can be in practice linked to problems of coordination between the different national authorities.[269] There is also a risk of fragmentation of surveillance resulting from the unclear wording in Art. 43(1), which states that a market surveillance authority may initiate investigations if it considers a product to present a "significant cybersecurity risk". Consequently Art. 43(1) leaves it to the discretion of the market surveillance authority which products are to be investigated or not. This may result in inconsistent procedures within the EU.[270] Asymmetry between national market surveillance authorities may also unfold as a result of different set of resources and institutions that an authority may use. In this sense, the varying levels of cybersecurity preparedness among Member States may present an obstacle to harmonization, mutual recognition, and convergence.[271] Accordingly, the requirement in Art. 41(6) CRA, whereby Member States must provide adequate resources, is particularly important and ultimately critical for the CRA's efficiency on the ground and throughout the Union.[272]

V. Significant administrative fines

The power to set rules on penalties is delegated to the Member States. Yet, the Member States' discretions are relative,[273] as Art. 53 already sets certain parameters. In general, all penalties imposed must be effective, proportionate and dissuasive.[274] More concretely: in case of a failure to comply with the essential requirements of Annex I and the obligations set out in Arts. 10 and 11 market surveillance authorities may impose fines of either €15 million or 2.5% of the total annual turnover of the previous business year, whichever is

---

[266]   Zirnstein (fn 145), 713.

[267]   Cf. Ludvigsen Kaspar Rosager/Nagaraja Shishir, The Opportunity to Regulate Cybersecurity in the EU (and the World): Recommendations for the Cybersecurity Resilience Act, <https://arxiv.org/abs/2205.13196>, 17.

[268]   European Economic and Social Committee (fn 23), 1.

[269]   European Economic and Social Committee (fn 23), 5.

[270]   Chiara, IoT (fn 63), 127 et seq.

[271]   Christou George, Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy, London 2016, 177.

[272]   European Economic and Social Committee (fn 23), 1.

[273]   Chiara, Cyber Resilience Act (fn 8), 265.

[274]   Art. 53(1) CRA Proposal.

higher.[275] The bulk of risking fines is therefore borne by the manufacturer and other persons who are deemed to be manufacturers.[276] For non-compliance with other obligations of the CRA, market surveillance authorities can impose administrative fines of up to €10 million or 2% of global annual turnover for the previous fiscal year, whichever is higher.[277] This risk is borne by all economic operators – manufacturers, importers, as well as distributors.[278] For the supply of incorrect, incomplete or misleading information to market surveillance authorities in connection with an official investigation, a fine of €5 million or 1% of the total worldwide annual turnover for the previous fiscal year, whichever is higher, may be imposed.[279]

When deciding on the amount of the administrative fine in each individual case, the market surveillance authority should take into account all relevant circumstances of the specific situation and as a minimum the nature, gravity, duration and consequence of the infringement; whether other authorities have already imposed fines for similar infringements; and the size and market share of the operator.[280]

At a first glance, one may well conclude that the CRA follows the fines model of recent EU law, such as the GDPR as well as the proposed AI Act.[281] Yet, it remains to be seen whether the fines will amount to similar sums as those imposed under the GDPR and whether differences in the authorities' approaches to fines will also materialize in case of the CRA.[282] It should be borne in mind that, as shown above, the market surveillance authorities also have the option of banning products on the market, which can be an important tool of intervention. The interplay between these two mechanisms (fines vs. barring from the EU market) is so far not clarified in the CRA and may need additional attention before its final adoption.

D.   Concluding observations and outlook

The article provided an enquiry into the EU proposal for a Cyber Resilience Act and attempted above all two things – on the one hand, to analyze more

---

275   Art. 53(3) CRA Proposal.
276   Zirnstein/Lee/Ge (fn 190), 170.
277   Art. 53(4) CRA Proposal.
278   Car/De Luca (fn 14), 8.
279   Art. 53(5) CRA Proposal.
280   Recital 65 and Art. 53(6) CRA Proposal.
281   Zirnstein/Lee/Ge (fn 190), 170.
282   Zirnstein/Lee/Ge (fn 190), 170; Ludvigsen/Nagaraja (fn 267), 11.

closely some of the key CRA provisions and on the other, to put the reform that the CRA will bring about into the broader context of EU's legal, policy as well as geopolitical activities in the digital domain in general and cybersecurity in particular. It is evident from the above that the CRA, when adopted, would cause a major stir and trigger a series of obligations for all actors engaged along the life-cycle of products with digital elements, create new competences for EU and Member State agencies and generate new interfaces with existing EU regulation in the domain of cybersecurity but also in other areas, such data protection and AI.

The ambitious regulatory project of the CRA and its potential far-reaching implications can be linked in general terms to its approach to cybersecurity as a cross-sectoral issue and the underlying conceptualization of cyber resilience as not merely a technical but a much wider topic of immediate societal relevance.[283] In more concrete terms, the regulatory sway of the CRA comes from its broad and comprehensive scope of application, the detailed catalogue of obligations (especially for manufactures of products with digital elements), as well as the potentially impactful market surveillance and enforcement mechanisms. Crucial for the effective approach of the CRA is also the inclusion of the entire value chain of digital products along their life-cycle, which is a new legal approach that duly takes into account both the dynamics of technological innovation as well as the premise of cyber resilience, whereby cyber threats are the rule rather than the exception.[284] While the CRA does take cyber resilience seriously, it also seeks to ensure that the single market for digital products is not unduly compromised and adopts a risk-based approach with varied regulatory burden across types of products and types of actors.

Despite the promise of the CRA and its regulatory potence, many questions remain still unanswered. These questions are of different nature and their answers will ultimately be quite different. Some of the definitional problems, lack of clarity and guidance in the CRA proposal, as well as the coordination problems with existing (and forthcoming) pieces of EU legislation can certainly be solved – either through compromises made during the still ongoing legislative process, through additional guidelines by the Commission or if somewhat less swiftly, through follow-up jurisprudence. There are however bigger questions and our contextualization of the CRA in the beginning of

---

283 Kipker (fn 137); Nai Fovino et al. (fn 226), 93; Bygrave Lee, Cyber Resilience versus Cybersecurity as Legal Aspiration, 14th International Conference on Cyber Conflict: Keep Moving 2022 (cit.: Bygrave, Cyber Resilience), 27.

284 Bygrave, Cyber Resilience (fn 284), 27.

the article speaks to them. The first important issue is whether the CRA, despite its virtues, could effectively lead to an Internet of Secure Things in Europe. Some of the concerns in this regard stem from endogenous to the CRA issues, such as that most digital products will be classified as low risk, the sliding scale of obligations, the possible divergences in surveillance practices and fines across responsible agencies. Others stem from even harder problems linked to the CRA's implementation in practice. In this context, it remains to be seen whether the CRA is adaptable enough to keep up with the rapidly evolving threat environment inherent to connected devices. Here one can consider for instance the fact that cybercriminals increasingly use malicious AI to support attacks, often to thwart intrusion detection algorithms within the IoT, or to attack beneficial AI in a way that causes the AI to work against its own system.[285] Also, given that the sophisticated AI application ChatGPT (with others to join it) can be used to proficiently write computer code, virtually anyone could exploit this to create their own malware to spy on user activity, steal data, spread ransomware or undertake any other malicious cyberattack.[286] Another big unknown in this dynamic context are users. While it appears that consumers would be willing to pay more for secure IoT devices,[287] the problem of informational asymmetry in the marketplace remains.[288] Similarly, the big question mark around user literacy and to what extent users are able and willing to react when faced with insecure digital products is unaddressed and may in reality reduce the CRA's efficacy despite the huge regulatory burden placed on the supply side. In this and the overall implementation context of the CRA, it would be particularly interesting, and potentially fruitful for policy makers, to observe and detect parallels with the implementation of the GDPR as another grand EU regulatory project.

Some of the critique points that can be expressed towards the CRA are of exogenous nature and can be linked to the CRA's underlying rationale to boost EU's role as a global cybersecurity standard-setter and a vector for safeguarding and sustaining its digital sovereignty – the second discrete topic that this article picked up at its outset. From the perspective of the Union, such a "digital sovereignty"-oriented strategy and the therewith related

---

[285] Kuzlu Murat/Fair Corinne/Guler Ozgur, Role of Artificial Intelligence in the Internet of Things (IoT) Cybersecurity, Discover Internet of Things 2021.

[286] Marr Bernard, How Dangerous Are ChatGPT and Natural Language Technology for Cybersecurity?, Forbes, 25 January 2023, <https://www.forbes.com/sites/bernardmarr/2023/01/25/how-dangerous-are-chatgpt-and-natural-language-technology-for-cybersecurity/?sh=52b374864aa6>.

[287] Johnson et al. (fn 7), 721.

[288] Johnson et al. (fn 7), 722.

regulatory activism in cybersecurity and beyond make lots of sense and can be easily politically justified. Yet, the EU, despite its sizeable market, is still part of the even larger landscape of the world and the datafication of economies and societies as a whole has only increased connectedness and interdependence between and across actors. After a period of relatively liberal stance towards cyberspace, in recent years and absent an international legal framework governing data, national legislators have adopted far-reaching rules on data protection, cybersecurity, competition, consumer protection, etc., often with an extra-territorial effect. It can be maintained that the EU has even been the regulatory champion in this regard. Yet, this leads to a profound fragmentation in the global data governance framework that we should be aware of.[289] Whether the "Brussels effect" of the CRA will unfold is still unknown but it too can contribute to exacerbating this fragmentation, as well as to increasing geopolitical tensions and strategic competition across different policy areas, which ultimately contribute little to a functioning, seamless data economy and a corresponding optimal legal design.[290]

Against this backdrop, it remains to be seen to what extent and how the CRA will manage to find its place in the complex puzzle and navigate the different trade-offs – such as between cybersecurity and market freedom, between protectionism and openness, between unilateral action and international cooperation.

---

[289]   Arner Douglas W./Castellano Giuliano G./Selga Eriks K., The Transnational Data Governance Problem, Berkeley Technology Law Journal 2023, 623.

[290]   Arner/Castellani/Selga (fn 290); also Aaronson Susan, What Are We Talking about When We Talk about Digital Protectionism?, World Trade Review 2018, 541; Bonefeld-Dahl Cecilia, European Sovereignty or a Shadow of Protectionism?, EURACTIV.com, 25 August 2022, <https://www.euractiv.com/section/digital/opinion/european-sovereignty-or-a-shadow-of-protectionism/>.

Market Definition and Market Power in the Era of Blockchain

Okan Yildiz/Rolf H. Weber*

Table of Contents

---

*   Okan Yildiz, MLaw, PhD candidate, Law Faculty, University of Zurich;
    Prof. Dr. Rolf H. Weber, professor of Business Law at University of Zurich and attorney in
    Zurich (Bratschi AG).

A.   Introduction

During the last decade, competition authorities had to increasingly deal with digital business models (often described as operating in "digital markets").[1] While scholars and authorities were in the process of understanding how to adapt competition law in the context of digitalization, the next technological leap started to emerge. This article does not investigate the digital markets in general but the newly appearing infrastructure, the distributed ledger technology (DLT). With the DLT, once again particular markets are evolving; therefore, it is important to address the features of those new markets which are based on the DLT.

In contrast to the World Wide Web, which is the "internet of information", DLT and blockchain[2] have been transforming the internet to the so called "internet of value". Consequently, in DLT and blockchain, the digitally represented values, their ownership, access to them and transactions with these values are of importance.

DLT is not fully unknown to the Swiss[3] as well as the European[4] regulators. Both authorities already reacted with the development of a normative framework for financial markets. In principle, policy and law intend to ensure optimal conditions for business activities with the aim that new technologies can meet the needs of society and markets. In the last few years, competition

---

[1]   In fact, *one* specific digital market does not exist; this terminology is a paraphrase for markets in the digital economy. However, authorities as well as the literature regularly speak of "digital markets" (e.g., *Digital Markets* Act in the European Union).

[2]   See section B.I. for the terminological differences between these two.

[3]   Federal Law on the Adaptation of Federal Law to Developments in the Distributed Ledger Technology, 27 November 2019, BBl 2020, 233 et seqq.

[4]   Proposal for a Regulation of the European Parliament and of the council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, COM(2020) 593 final, 2020/0265(COD). The trilogues between the legislative bodies have already ended in a formal agreement; the provisional agreement of MiCA is subject to approval by the Council and the European Parliament before going through the formal adoption procedure (see Council of the EU, Digital finance: agreement reached on European crypto-assets regulation (MiCA) – Press release of 30.06.2022, available at <https://www.consilium.europa.eu/en/press/press-releases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica/>).

law academics started to shift their focus to DLT and blockchain issues and to also raise respective concerns.[5]

The topic of DLT and blockchain is still very much in progress, both technologically and legally, but a more in-depth exploration of the normative regulatory framework proves to be appropriate. This paper aims to understand the implications of DLT and blockchain on Swiss and European competition law. In order to assess those implications, the first section explains the fundamental technological features, i.e., section B. addresses the technology itself by setting the technical foundation (B.I.), showing the objectives of blockchain (B.II.), examining different types of blockchain (B.III.), pointing out the multi-layered architecture of blockchain (B.IV.) and taking a closer look at the main concepts of blockchain (B.V.).

In section C. the focus lies on the main implications of DLT/blockchain on substantive Swiss and European competition law. In this context, the chapters examine the concept of an "undertaking" under the applicable law and investigate possible consequences for blockchain business models (C.I.). Furthermore, the application of existing market definition tools to blockchain markets (C.II.) is of fundamental importance. In addition, the calculation and evaluation of market power also need some adaptation in the context of DLT and blockchain (C.III.). Lastly, section D. concludes this article and gives an outlook.

B.   Distributed ledger technology (DLT) and blockchain

This section examines the technological characteristics of DLT and blockchain in detail. In this regard, it is important to clarify the functioning of the technology itself because the subsequent competition law related considerations require a conceptual understanding of DLT and blockchain.[6]

---

[5]   Schrepel Thibault, Blockchain + Antitrust: The Decentralization Formula, Cheltenham/ Northampton 2021 (cit. Schrepel, Blockchain + Antitrust); Schrepel Thibault/Buterin Vitalik, Blockchain Code as Antitrust, Berkeley Technology Law Journal 2021, 1 et seqq; Deuflhard Florian/Heller C.-Philipp, Antitrust Economics of Cryptocurrency Mining, available at <https://ssrn.com/abstract=3917012>; Schrepel Thibault, Libra: A Concentrate of "Blockchain Antitrust", Michigan Law Review 2020, 160 et seqq.; Schrepel Thibault, Collusion by Blockchain and Smart Contracts, Harvard Journal of Law and Technology 2019, 117 et seqq.; Schrepel Thibault, Is Blockchain the Death of Antitrust Law? The Blockchain Antitrust Paradox, Georgetown Law Technology Review 2019, 281 et seqq.

[6]   The following section is based on Weber Rolf H., DLT-Handelsplattformen: Spannungsfeld von Technologie und Recht, Zürich 2022 (cit. Weber, DLT-Handelsplattformen). This publication is not further referenced below.

I.   Terminology

DLT refers to a concept that allows data to be recorded and shared across distributed ledgers. It enables the recording, sharing and synchronization of transactions and data across a distributed network with participants all over the world, hence it is built on a peer-to-peer basis and operates without intermediaries, i.e., without centralized control.[7]

Blockchain (literally a chain of data blocks) is a special type of data structure used in some distributed ledgers. New data (usually transactions) – after being validated by the participants – are stored on the blockchain, block by block and chronologically, and are thus linked together in a digital chain.[8] Blockchains use cryptographic and algorithmic methods to record and synchronize data across their networks; hence, the blocks are connected by cryptographic hashes.[9] Each newly added block refers to the previous block; in this way, the technology ensures that a unique and traceable chain of blocks is created.[10]

"Distributed ledger" is a broader terminology describing distributed, synchronized, and cryptographically secured databases.[11] Therefore, in some situations it is necessary to speak of distributed ledgers rather than

---

[7]   Baker Colleen/Werbach Kevin, Blockchain in Financial Services, in: Madir Jelena (ed.), FinTech, Law and Regulation, Cheltenham/Northampton 2019, 123 et seqq., marginal nos. 6.05 et seq. (cit. Baker/Werbach, Blockchain in Financial Services); Maull Roger et al., Distributed Ledger Technology: Applications and Implications, Strategic Change 2017, 481 et seqq., 483 et seq. (cit. Maull et al., Strategic Change 2017).

[8]   Baker/Werbach, Blockchain in Financial Services, marginal no. 6.07; Ganne Emmanuelle, Can Blockchain revolutionize international trade?, Geneva 2018, 6 (cit. Ganne, Can Blockchain revolutionize); Tapscott Don/Tapscott Alex, The Blockchain Revolution, How the Technology Behind Bitcoin is Changing Money, Business, and the World, Toronto 2016, 75; Weber Rolf H./Baumann Simone, FinTech – Schweizer Finanzmarktregulierung im Lichte disruptiver Technologien, Jusletter 21. September 2015, marginal no. 26.

[9]   A cryptographic hash is a cryptographic fingerprint. When generating a hash, the algorithm receives a data input of arbitrary length and generates a deterministic result of predetermined length. For a specific input, the resulting hash value always remains the same and is verifiable by anyone using the same hash algorithm. Computationally, it is impossible to provoke a collision, i.e., it is impossible to generate the same cryptographic fingerprint with two different inputs (Antonopoulos Andreas M., Mastering Bitcoin, Programming the Open Blockchain, 2nd ed. Beijing 2017, 228).

[10]   Low Kelvin F.K./Mik Eliza, Pause the Blockchain Legal Revolution, International & Comparative Law Quarterly 2020, 135 et seqq., 137 et seq. (cit. Low/Mik, International & Comparative Law Quarterly 2020); Baker/Werbach, Blockchain in Financial Services, marginal no. 6.07; Weber Rolf H., Regulatory Environment of the Ledger Technology, CRi 2017, 1 et seqq.

[11]   Maull et al., Strategic Change 2017, 483.

blockchain, since not all distributed ledgers record and store data in interconnected chains of blocks. In these cases, the distributed ledgers do not have the same so-called "immutability" as some blockchains.[12]

II.   Fundamental objectives of blockchain

The blockchain technology being called the "internet of values" focuses on digitally represented assets. Unlike on the World Wide Web, the rightful owner of any asset can be conclusively determined on the blockchain.[13]

In addition, the assets or property rights on the blockchain are transferred in atomic transactions and not copied. The blockchain automatically ensures that a value on the blockchain (or on any other distributed ledger) exists only once and is assigned to a precisely identifiable owner. Due to the lack of a centralized authority, the data is (simultaneously) stored on the different decentralized nodes.[14]

III.   Types of blockchain

In relation to the authorization to validate, the accessibility to the blockchain and the possibility to participate on the blockchain, two main distinctions are necessary.

Firstly, blockchains can be qualified as permissioned or permissionless networks. The main difference between these two types of blockchain is whether anyone can validate a new block or whether doing that requires some kind of permission. Permissionless blockchains are of particular interest because on permissionless systems, anyone can create and validate the blocks

---

[12]   Low Kelvin F.K., Confronting Cryptomania: Can Equity Tame the Blockchain?, Legal Studies Research Paper No. 2020-01, Hong Kong 2020, 7 (cit. Low, Confronting Cryptomania); Low/ Mik, International & Comparative Law Quarterly 2020, 138 with further details (esp. footnote 23).

[13]   Rutishauser Daniel/Kubli Ralf/Weber Rolf H., Grundlagen, in: Weber Rolf H./Kuhn Hans (eds.), Entwicklungen im Schweizer Blockchain-Recht, Basel 2021, 9 et seqq., marginal no. 4 (cit. Rutishauser/Kubli/Weber, Grundlagen).

[14]   Rutishauser/Kubli/Weber, Grundlagen, marginal nos. 4 et seq.

or add transactions. Hence, the validators can be numerous.[15] On permissioned systems, execution and validation is limited to the authorized participants. On these systems, a hierarchy (i.e., by defining different permissions for each group of participants) among the participants exists. It is necessary to pre-define the nodes in each group.[16] These restrictions to certain nodes are applied by a controlling firm or by a consortium of firms (so called consortium blockchain).[17]

Secondly, blockchains can be categorized into private and public blockchains depending on whether everybody or only the participating nodes in the network are able to access the blockchain. On public blockchains there is no restriction to access the blockchain itself; anyone can participate on the blockchain while keeping the anonymity. No specific user is given special authorization on any decisions as the validation of transactions relies on a pre-defined consensus mechanism.[18] On private blockchains, only authorized parties can view the transaction history. In addition, access to the system is restricted and the participants are in principle identifiable. Only a limited

---

[15] Ganne Emmanuelle, Blockchain's Practical and Legal Implications for Global Trade and Global Trade Law, in: Burri Mira (ed.), Big Data and Global Trade Law, Cambridge 2021, 128 et seqq., 130 (cit. Ganne, Blockchain's Practical and Legal Implications); Low, Confronting Cryptomania, 7 et seq.; Low/Mik, International & Comparative Law Quarterly 2020, 138 et seqq.; Nascimento Susana/Pólvora Alexandre (eds.), Blockchain now and tomorrow: assessing multidimensional impacts of distributed ledger technologies, Luxembourg 2019, 14 (cit. Nascimento/Pólvora, Blockchain now and tomorrow); Rauchs Michel et al., Distributed Ledger Technology Systems: A Conceptual Framework, Cambridge 2018, 24 (cit. Rauchs et al., Distributed Ledger Technology Systems).

[16] Massarotto Giovanna, Using Blockchain-Based Smart Contracts To Enforce the Antitrust Consent, 11, available at <https://ssrn.com/abstract=4016740>; Ganne, Blockchain's Practical and Legal Implications, 130; Low, Confronting Cryptomania, 7 et seq.; Low/Mik, International & Comparative Law Quarterly 2020, 138 et seqq.; Nascimento/Pólvora, Blockchain now and tomorrow, 14.

[17] Pike Chris/Capobianco Antonio, Antitrust and the trust machine, OECD Blockchain Policy Series, 4 et seq., available at <https://www.oecd.org/daf/competition/antitrust-and-the-trust-machine-2020.pdf> (cit. Pike/Capobianco, OECD Blockchain Policy Series); Rauchs et al., Distributed Ledger Technology Systems, 54; Ganne, Can Blockchain revolutionize, 11.

[18] See section B.V.3. Consensus mechanisms. Rutishauser/Kubli/Weber, Grundlagen, marginal nos. 20 et seq.; Pike/Capobianco, OECD Blockchain Policy Series, 5; Nascimento/Pólvora, Blockchain now and tomorrow, 14 et seq.; Salmon John/Myers Gordon, Blockchain and Associated Legal Issues for Emerging Markets, EMcompass 2019, 1 et seqq., 1 et seq. (cit. Salmon/Myers, EMcompass 2019); Ganne, Can Blockchain revolutionize, 9.

number of nodes are allowed to participate in the verification process. In this constellation, the system is protected not only technologically, but also organizationally by comprehensive sets of contracts and rules.[19]

These two main distinctions can also be found in tech as well as law literature addressing blockchain but the terminologies are not always used consistently.[20] Finally, the categorization of blockchains presented here is not exhaustive; hybrid systems in particular also exist in the real world.

IV.   Multi-layered architecture of blockchain

Blockchains usually use a multi-layered architecture with distinct purposes of each layer. In the context of the internet, for example, a distinction between the infrastructure layer, the data layer, the software layer, and the application layer is applied. In the context of blockchain,[21] Decentralized Finance (DeFi) is a good example for the multi-layered architecture because DeFi consists of five different layers, namely the settlement layer, the asset layer, the protocol layer, the application layer, and the aggregation layer.[22] For the purpose of

---

[19]   Rutishauser/Kubli/Weber, Grundlagen, marginal nos. 20 et seq.; Pike/Capobianco, OECD Blockchain Policy Series, 5; Nascimento/Pólvora, Blockchain now and tomorrow, 14 et seq.; Salmon/Myers, EMcompass 2019, 1 et seq.; Ganne, Can Blockchain revolutionize, 10; Kaulartz Markus, Die Blockchain-Technologie, CR 2016, 474 et seqq., 475.

[20]   See Deng Robert /Lee David Kuo Chuen, Handbook of Blockchain, Digital Finance, and Inclusion, Vol. 2, Cambridge MA 2017, 147; Low/Mik, International & Comparative Law Quarterly 2020, 138; see also World Bank Group, Distributed Ledger Technology (DLT) and Blockchain, FinTech Note, No. 1, Washington 2017, IV and 11 et seqq., available at <https://documents1.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf> with an explicit distinction between permissioned/permissionless and private/public blockchains.

[21]   For other examples of multi-layered architecture in blockchain, see Pajooh Houshyar Honar et al. Multi-Layer Blockchain-Based Security Architecture for Internet of Things, sensors 2021, 772, 1 et seqq., 6 et seqq.; López David/Farooq Bilal, A multi-layered blockchain framework for smart mobility datamarkets, Transportation Research Part C 2020, 588 et seqq., 590 et seqq.

[22]   For the internet layers, see Weber Rolf H., Zivilrechtliche Haftung auf dem Information Highway, in: Hilty Reto M. (ed.), Information Highway. Beiträge zu rechtlichen und tatsächlichen Fragen, Bern 1996, 531 et seqq. For the example of DeFi, see Schär Fabian, Decentralized Finance: On Blockchain- and Smart Contract-based Financial Markets, Federal Reserve Bank of St. Louis Review 2021, 153 et seqq., 155 et seqq. (cit. Schär, Federal Reserve Bank of St. Louis Review 2021).

this article, only the settlement layer, asset layer and application layer will be discussed.[23]

The settlement layer of DeFi represents the used blockchain for the system. Hence, the settlement layer consists of the blockchain and the native protocol asset (e.g., Bitcoin on the Bitcoin network or Ether on the Ethereum network). The settlement layer can be understood as the foundation.[24]

The asset layer encompasses all assets issued on the settlement layer. Besides the native protocol assets, the asset layer also consists of tokens, which are digital assets that have not been issued on the native protocol.[25]

On the application layer, user-oriented applications are created. These applications connect different protocols and provide a user-friendly experience. The application layer usually is closely linked to the user interface as it facilitates the interaction with the smart contract, and as a result, the protocols are easier to use.[26]

V.   Main characteristics of blockchain

Various blockchains are often considered secure because of the lack of potentially "untrustworthy" intermediaries. In the following, the most important concepts and technological foundations of blockchain are explained in order to create a basic understanding for the legal analysis of blockchain in context of competition law.[27]

1.   Distributed ledgers

In distributed ledgers, as mentioned above, neither a single party ever has control over the entire ledgers nor is the data ever stored centrally in one place; rather, various mirrors with the same information are distributed across several nodes. Therefore, these nodes replace to role of a central party in

---

[23]   For a comprehensive explication of all layers on DeFi, see Schär, Federal Reserve Bank of St. Louis Review 2021, 155 et seqq.

[24]   Schär, Federal Reserve Bank of St. Louis Review 2021, 155 et seq.

[25]   Schär, Federal Reserve Bank of St. Louis Review 2021, 156; Roth Jakob/Schär Fabian/ Schöpfer Aljoscha, The Tokenization of Assets: Using Blockchains for Equity Crowdfunding, in: Wendt Karen (ed.), Theory of Change: Change Leadership Tools, Models and Applications for Investing in Sustainable Development, Cham 2021, 329 et seqq., 332.

[26]   Schär, Federal Reserve Bank of St. Louis Review 2021, 156.

[27]   See also Schär Fabian/Berentsen Aleksander, Bitcoin, Blockchain, and Cryptoassets, Cambridge MA/London 2020, 31 seqq. (cit. Schär/Berentsen, Bitcoin, Blockchain, and Cryptoassets).

a "traditional" setting with intermediaries.[28] With this concept, a consensus mechanism is necessary: the participants themselves are responsible for verifying and validating the data blocks using this mechanism,[29] which replaces trust in the counterparty. The activity of all participants is based on a protocol that contains instructions for the entire network. Usually, this code is "open source", i.e., it can be viewed and understood by all participants.[30]

2. Decentralized structure without intermediaries

According to the description as "internet of values", one of the main functions of transactions on the blockchain is how much (and what kind of) value has been transferred from one party to another. The data of each transaction or bundle of transactions can be represented as a block on the blockchain. Each block has a header, which contains all the information necessary to classify and validate a block, and a body, which describes the transaction to be re-registered. Since each block in the chain builds on the previous block, it is possible to trace the entire chain; a newly created block contains the hash of the previous block.[31]

3. Consensus mechanisms

There are two types of users on the blockchain: those who only register transactions and those who provide the computing power to validate a transaction. The participants of the second group are responsible for finding the consensus – based on a specific pre-selected consensus mechanism. The consensus mechanisms are – contrary to the name – not of a democratic nature, but fully automated, deterministic, and algorithm-driven validation processes. Validation thus depends on the fulfilment of certain technological conditions; in principle, a node or the person behind it cannot decide for

---

[28] Low, Confronting Cryptomania, 7; Ganne, Can Blockchain revolutionize, 6.

[29] Weber Rolf H., Handel mit digitalen Aktiven, in: Weber Rolf H./Kuhn Hans (eds.), Entwicklungen im Schweizer Blockchain-Recht, Basel 2021, 165 et seqq., marginal no. 11; Low, Confronting Cryptomania, 7; Ganne, Can Blockchain revolutionize, 5 et seqq.; Maull et al., Strategic Change 2017, 483 et seq.

[30] Rutishauser/Kubli/Weber, Grundlagen, marginal no. 15.

[31] Rutishauser/Kubli/Weber, Grundlagen, marginal no. 16.

itself whether to reject a transaction that fulfils all validation criteria or to accept a transaction that does not fulfil the validation criteria.[32] In practice, the following two methods are established consensus mechanisms:[33]

a)   *Proof of Work*

If the blockchain opted for proof of work, all participants attempt to solve a complex proof of work instance (a complex calculation).[34] Proof of work builds on the asymmetry of calculation and verification, because the calculation requires immense computing power, while the verification of the solution is simple. The first party to find the solution receives a reward and the other participants can simply verify the solution. This described verification process is called mining, because after the verification a new block is added to the blockchain. Proof of work is an established method for reaching consensus (e.g., used in the Bitcoin network).[35]

b)   *Proof of Stake*

When using proof of stake, validation is not carried out via the computing power of the participants, but via deposited cryptocurrencies (so far generally not via cryptoassets). Proof of stake systems consist of validators who lock their assets (staked coins) and those who merely hold the cryptocurrency of the corresponding system. Validators propose the potentially next valid block through a weighted random selection, which is determined by the participation time and/or the percentage relation to the deposited cryptocurrencies and vote on its validity. The voting power of the validators depends on the size of their deposited portfolio.[36]

Staking is complemented by slashing. Slashing is used to punish unfair or malicious behavior of validators. Hence, validators are exposed to the risk

---

[32]   Low/Mik, International & Comparative Law Quarterly 2020, 140 et seq.

[33]   Rutishauser/Kubli/Weber, Grundlagen, marginal nos. 22 et seqq.; Schär/Berentsen, Bitcoin, Blockchain, and Cryptoassets, 139 et seqq.

[34]   Strictly speaking, this is not a common mathematical calculation, but a complex procedure, see Gervais Arthur et al., On the Security and Performance of Proof of Work Blockchains, CCS '16: Proceedings of the 2016 ACM SIGSAC, Vienna 2016, 3 et seqq., 4 et seq.

[35]   Nakamoto Satoshi, Bitcoin: A Peer-to-Peer Electronic Cash System, available at <https://bitcoin.org/bitcoin.pdf>.

[36]   Antonopoulos Andreas M./Wood Gavin, Mastering Ethereum, Building Smart Contracts and DApps, Beijing 2019, 321 (cit. Antonopoulos/Wood, Mastering Ethereum).

of losing their entire deposit or parts of the staked cryptocurrencies.[37] But validators also receive a small reward proportional to their staked coins; this reward-punishment mechanism forces validators to act honestly and follow the consensus protocol.[38]

Furthermore, proof of stake is supposed to be substantially less energy intensive. It is said that the Ethereum Merge in mid-September 2022 (a software upgrade swapping the platforms consensus mechanism from proof of work to proof of stake) will speed up the execution of transactions on the blockchain and significantly reduce energy consumption (estimations of 99% energy reduction).[39]

C.   Implications of blockchain on competition law

The following section analyses the implications of blockchain on competition law based on Art. 102 TFEU[40] and Art. 7 CartA[41] in particular. It focuses on fundamental questions regarding the application of competition law in a blockchain environment. First, an overview of the concept of an undertaking and how blockchain might affect the approach to define an undertaking is necessary. Furthermore, the market definition of blockchain business models needs further investigation. Then, the determination of market power in the context of blockchain will be discussed and the last part addresses possible examples of abuse of power.

---

[37] Rutishauser/Kubli/Weber, Grundlagen, marginal nos. 22 et seqq.; Chentouf Fatima Zahrae/Bouchkaren Said, Blockchain for Cybersecurity in IoT, in: Maleh Yassine et al. (eds.), Artificial Intelligence and Blockchain for Future Cybersecurity Applications, Cham 2021, 61 et seqq., 74; Bitcoinsuisse, What is Staking?, Zug 2020, 1 et seq. available at <https://www.bitcoinsuisse.com/learn/what-is-staking>.

[38] Antonopoulos/Wood, Mastering Ethereum, 321.

[39] Born Mathias, Ethereum senkt Stromverbrauch: Wie Bitcoin, nur bio, Tages-Anzeiger of 15.09.2022, available at <https://www.tagesanzeiger.ch/die-zweitgroesste-kryptowaehrung-wird-oekologischer-652418632805>; Fulterer Ruth, Ethereum löst auf einen Schlag sein Energieproblem. Das geht nicht ohne Risiko. Die sieben wichtigsten Fragen, NZZ of 29.08.2022, available at <https://www.nzz.ch/technologie/der-merge-bei-ethereum-7-fragen-zum-gruenen-umbau-der-blockchain-ld.1695122>.

[40] Consolidated version of the Treaty on the Functioning of the European Union, OJ C 326, 26.10.2012, 47–390.

[41] Federal Act on Cartels and other Restraints of Competition of 6 October 1995 (CC 251; Status as of 1 January 2022).

I.   The concept of "undertaking"

In competition law, various articles apply to "undertakings" (e.g. TFEU Title VII, Chapter 1, Section 1: Rules applying to undertakings). Art. 101 and 102 TFEU explicitly mention the undertakings. In Swiss competition law, Art. 2 para. 1 CartA clearly states the scope of the Act which "*applies to private or public undertakings* that are parties to cartels or to other agreements affecting competition, which exercise market power or which participate in concentrations of undertakings".[42] The structure of blockchain[43] inherently contains some implications on the concept of the undertaking. First, in a distributed ledger, which blockchain is a part of, one single party never has control over the whole structure. Further, the consensus mechanisms allow to make certain decisions within the blockchain. These two circumstances together raise concerns over who controls an economic entity and who is with which assets liable for actions taken by this economic entity, be it an undertaking or a firm.

The concept of undertakings in the context of blockchain has already been discussed in detail by *Schrepel* and *Lianos*.[44] It is especially important to also consider the "firm" besides defining the concept of "undertaking". For this purpose, *Schrepel* has developed a theory of granularity. He distinguishes between different participants and defines a "nucleus". According to *Schrepel*, the nucleus is "a group of participants [that] may achieve a form of control over the blockchain by collaborating, by circumventing (some of) the constraints imposed on them, and by changing them in the long run."[45] Therefore, this nucleus should "become a legal fiction that can be liable for anticompetitive practices, but also able to claim damages."[46] Hereinafter this view of *Lianos* and *Schrepel* related to the concept of undertaking is applied.

---

[42]   With emphasis added.

[43]   See section B.V. Main characteristics of blockchain.

[44]   Schrepel, Blockchain + Antitrust, 80 et seqq. with special focus on the "firm" (esp. 109 et seqq.); Lianos Ioannis, Blockchain Competition, Centre for Law, Economics and Society Research Paper Series 4/2018, 77 et seqq. (cit. Lianos, Blockchain Competition).

[45]   Schrepel, Blockchain + Antitrust, 123.

[46]   Schrepel, Blockchain + Antitrust, 124; similarly, Lianos, Blockchain Competition, 79 et seq.

II. Market definition

1. Overview

The definition of the market requires a twofold approach: First, this section explains why a market definition is still necessary even though in the 2010s an increasing number of papers discussed the abandonment of market definition.[47] Then, the current state of market definition in the European Union and in Switzerland is described in order to demonstrate this article's approach to "blockchain markets".[48]

When defining markets in the context of blockchain, the characteristics of this new infrastructure need to be considered. First of all, a distinction between public/private and permissionless/permissioned blockchains is necessary. Secondly, the type of validation on the blockchain plays an important role in delineating the market. Furthermore, when developing a market definition,

---

[47] Especially the papers by Kaplow were influential: Kaplow Louis, Market definition: impossible and counterproductive, Antitrust Law Journal 2013, 361 et seqq.; Kaplow Louis, Why (Ever) Define Markets?, Harward Law Review 2010, 437 et seqq., 517 (cit. Kaplow, Harv. L. Rev. 2010); see also Pike Chris, Part I. Introduction and key findings, in: OECD (ed.), Rethinking Antitrust Tools for Multi-Sided Platforms, Paris 2018, 9 et seqq. (cit. Pike, Part I) stating "market definition is often unnecessary and can be counterproductive." (see Pike, Part I, 13); Smith Rhonda L./Duke Arlen, Platform business and market definition, ECJ 2021, 93 et seqq. (footnote 1 with further information; cit. Smith/Duke, ECJ 2021); Nazzini Renato, Online Platforms and Antitrust: Where Do We Go From Here?, Italian Antitrust Review 2018, 5 et seqq., 13 et seqq.; Schweitzer Heike et al., Modernisierung der Missbrauchsaufsicht für marktmächtige Unternehmen, Endbericht, Projekt im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi) Projekt Nr. 66/17, Düsseldorf 2018, 30 et seqq.; Podszun Rupprecht/Franz Benjamin, Was ist ein Markt? – Unentgeltliche Leistungsbeziehungen im Kartellrecht, NZKart 2015, 121 et seqq., 126; Crane Daniel A., Market Power Without Market Definition, Notre Dame Law Review 2014, 31 et seqq.; Zimmer Daniel, Differenzierte Produkte, nichtkoordinierte Effekte und das Upward Pricing-Pressure-Konzept: Wird die Marktabgrenzung in Fusionskontrollverfahren entbehrlich?, WuW 2013, 928 et seqq. with further information.

[48] In fact, a "blockchain market" per se does not exist. In the context of competition law, there is no such thing as *one* "blockchain market", *one* "digital market" or *one* "multi-sided market"; it is misleading to assume that there is a single, predetermined market for blockchain in general. Moreover, those terminologies might help to orient one towards a general description of a specific market structure. Once this is established, competition authorities are able to define markets for each case separately while considering all peculiarities of each market.

the authorities need to always assess the multi-layered architecture of the blockchain. Lastly, as a comprehensive and reoccurring topic, the general concept of blockchain must be reflected in the market definition.

2. Current state of market definition

According to *Kaplow* "the market definition process is incoherent as a matter of basic economic principles and hence should be abandoned entirely".[49] *Kaplow* is, in particular, of the opinion that the market definition is useful in a market with homogenous products but useless if applied in redefined markets.[50] Furthermore, he argues that the market definition is the first step in antitrust proceedings which is used to assess the market share of a firm or undertaking. From this share, then, one (automatically) infers the degree of market power.[51]

This line of argumentation does not work in the context of European and Swiss law. While the market definition is a tool for determining market power, the authorities are still obliged to analyze the market position of the undertaking under investigation. This market analysis considers market shares but does not automatically infer any market power from it. Instead, the authorities also take the market structure (i.e., potential competition, barriers to entry), the company structure (i.e., economies of scale, technological lead) and the general market behavior into account.[52] Even though extraordinary market shares are an indicator for market power in the European Union and in Switzerland,[53] their authorities only consider the market share among other

---

[49] Kaplow, Harv. L. Rev. 2010, 437.

[50] Kaplow, Harv. L. Rev. 2010, 441.

[51] Kaplow, Harv. L. Rev. 2010, 439.

[52] LMRKM Kartellrecht, Kommentar zum Deutschen und Europäischen Recht, Loewenheim Ulrich et al. (eds.), 4th ed., Munich 2020, LMRKM Kartellrecht-Bergmann/Fiedler, Art. 102 marginal nos. 117 et seqq. (cit. LMRKM Kartellrecht-Editor). The dispatch of the Federal Council explicitly states that there is not a numerus clausus of possible factors to consider for the determination of market power, it rather is necessary to consider all specific circumstances of the individual case (Dispatch of the Federal Council on the Federal Act on Cartels and other Restraints of Competition of 23 November 1994, Swiss Federal Gazette 1995 I 468 et seqq.).

[53] LMRKM Kartellrecht-Bergmann/Fiedler, Art. 102 marginal nos. 118 et seq. In Switzerland, the Federal Supreme Court of Switzerland states that high market shares are a strong indicator for market power but does not necessarily mean that there is no effective competition (TF 130 II 459 E. 5.7.2).

important factors. In the digital economy, in particular, the market share starts to lose importance because of the dynamic and innovative markets; this is not different in markets based on blockchain.

Therefore, the authorities of the European Union and of Switzerland still hold on to a market definition; their methods remained constant for decades and the market definition still is a prerequisite for analyzing market power. Both authorities usually consider the demand side substitutability and the SSNIP test. The former has even been codified in the Merger Control Ordinance (MCO), according to Art. 11 para. 3 lit. a MCO, "[t]he [relevant] product market comprises all those goods or services that are regarded as interchangeable by consumers on the one hand and by suppliers on the other hand".[54]

According to the demand side substitutability, products and services which are interchangeable based on their characteristics, the price level and the intended use belong to the same market. The focus is on the functional interchangeability of the goods from the point of view of the market counterparty. Price, quality, availability, consumer preferences and barriers to market entry must be considered.[55]

The SSNIP test examines how consumers would react to a hypothetical, small but significant and non-transitory price increase of 5%-10%. If consumers switch to other goods or services, the next best substitute is also included in the analysis. Then it is again examined whether a hypothetical price increase of 5%-10% of these two goods or services would be profitable for the undertaking. If this is the case, these two goods form the relevant product market. This test is usually conducted until the price increase of the identified group of products or services would no longer lead to a switch to another product or service.[56]

3. Market definition based on type of blockchain

One possible method of defining a market is by differentiating the various types of blockchain (e.g., having a market for public blockchain and a market for private blockchain). Especially the private blockchains can be of sig-

---

[54] Ordinance on the Control of Concentrations of Undertakings (MCO) of 17 June 1996 (CC 251.1; Status as of 1 January 2013).

[55] Basler Kommentar zum Kartellgesetz, Amstutz Marc/Reinert Mani (eds.), 2nd ed. Basel 2022, BSK-Reinert/Wälchli, Art. 4 para. 2, marginal no. 102 (cit. BSK-Author); LMRKM Kartellrecht-Bergmann/Fiedler, Art. 102 marginal no. 38.

[56] BSK-Reinert/Wälchli, Art. 4 para. 2, marginal nos. 116 et seqq.; LMRKM Kartellrecht-Bergmann/Fiedler, Art. 102 marginal no. 41.

nificance for competition authorities because they could conduct anticompetitive practices by excluding certain users (in this context, comparisons to sporting associations may be appropriate). It is easily possible that – if a user is excluded from accessing the infrastructure of a blockchain – an infrastructure is regarded as essential facility if there are no suitable alternatives and the infrastructure can deny access. This issue, however, only concerns private and/or permissioned blockchains which are much less in use compared to public/permissionless blockchains.

Nevertheless, the distinction between these types of blockchain raises another question: Can a product or service be interchangeable if offered on opposing types of blockchain? Similar to online and offline markets, this question cannot be answered generally. Rather, one must conduct a "traditional" market definition (with demand side substitutability or the SSNIP test) to infer whether any two products or services (be it on public or private blockchain) are interchangeable. Therefore, it is theoretically possible that two products or services are interchangeable based on their characteristics, the price level, and the intended use even though one is on a public blockchain and the other is on a private blockchain. However, price, quality, availability, consumer preferences and barriers to market entry must also be considered. Consequently, the substitutability equally depends on the level of privatization of the blockchain.

4. Market definition based on block validation

The still limited literature on competition law in the context of blockchain suggests delineating markets based on block validation.[57] It is surprising that the authors assume separate markets based on consensus mechanisms without providing any explanation as to why.[58] Based on that assumption, they apply the SSNIP test to these "markets". It is, however, questionable if those markets do even exist because of the difficulty to grasp the fact that a type of internal organization is being analyzed in these cases. As mentioned above, these consensus mechanisms are an inherent part of distributed ledgers (thus also blockchains) because of the lack of intermediaries and the need of trust

---

[57]   Deuflhard Florian/Heller C.-Philipp, Defining Relevant Markets in the Crypto Economy, TechREG CHRONICLE February 2022, 1 et seqq., 4 et seqq. (cit. Deuflhard/Heller, Defining Relevant Markets).

[58]   "The markets for the two consensus mechanisms are likely separate." (Deuflhard/Heller, Defining Relevant Markets, 4).

towards the counterparties. Therefore, the consensus mechanisms do not provide any insight in interchangeability or – more generally – in competitive constraints.

The main goal of the market definition is to define the framework for the antitrust analysis. It aims to determining the competitive constraints concerning the undertaking under investigation. The competitive constraints, however, cannot be identified based on internal organizational structure. The consensus mechanisms can be compared to (internal) decision-making mechanisms in different types of undertakings (e.g., a voting in the general assembly of a shareholder company where they decide on internal matters without any influence to the market definition in competition law). In traditional competition law, one does not define markets based on the type of company (e.g., public stock company, limited company etc.). Competition authorities rather consider the economic activities of these undertakings and then decide that different types of companies belong to the same market. The same logic should apply to blockchains.

Therefore, it is not convincing to base market definition on block validation types.

5.   Market definition based on the layers of the blockchain

As mentioned, blockchains use a multi-layered architecture. This architecture has important effects on the approach of market definition. For the purpose of a market definition, it is important to distinguish the different layers and identify the layer that is impacted.[59] Most likely, products and services on each layer are not interchangeable with products and services on other layers as they do not provide functional interchangeability and/or consumers could not change to a product or service on another layer.

a)   Market definition on the base layer

The base layer of blockchain (in the context of DeFi, it is called the settlement layer) must be considered at the beginning. As explained above, the base layer provides the infrastructure on which everything relies on. In the case of blockchain, the base layer usually contains the used blockchain for the system, thus the base layer consists of the blockchain itself and the native protocol asset. Regarded as the foundation, everything bases on the Bitcoin network or Ethereum network (or any other network).

---

[59]   See also Schrepel, Blockchain + Antitrust, 185.

This base layer of the blockchain can be compared to the infrastructure layer of the internet. The internet (or its infrastructure) can be seen as a network of networks that is linked together.[60] While competition authorities have dealt with a myriad of cases regarding the internet (more specifically based on the internet), the question of defining a market along the infrastructure never came up. The same thought process can be applied to the base layer of blockchain.

Even though there are different protocols and infrastructures of blockchain (as mentioned Bitcoin network, Ethereum network, but also Tezos network and others), they are mainly public blockchain networks.[61] Similar to the internet infrastructure, these public and/or permissionless blockchain infrastructures do not present any problems.[62] Therefore, at least for the time being, this base layer does not seem to pose any difficulties regarding market definition.

Even if the blockchain infrastructure is viewed as a platform, hence as its own ecosystem, it is questionable whether it may constitute its own market. Even with digital ecosystems, authorities tend to struggle when defining "ecosystem markets", with good reasons. While at first sight, ecosystems might seem to be competing against each other, a general definition of ecosystem markets may lead to erroneous markets, especially when keeping in mind that the goal of the market definition is to consider competing, substitutable *products and services* from the point of view of the consumers. It is rare that consumers will consider whole ecosystems as interchangeable; they rather care about single products in an ecosystem.

A similar approach is necessary when analyzing blockchains. It is not reasonable to view whole blockchain infrastructures (or ecosystems) as general substitutes. In this case, it would be more accurate to investigate each application on the blockchain.[63]

Another point of view is the qualification of a blockchain as a platform.[64] This approach has the advantage of being (comparatively) easy to understand as it bases its core logic on platform theories of digital businesses. According to *Pike/Capobianco*, blockchains "compete to attract both users and validators"

---

[60]   Krol Ed/Hoffman Ellen S., FYI on "What is the Internet?", May 1993, available at <https://www.rfc-editor.org/rfc/rfc1462.html>, 1 et seqq.

[61]   See section B.III. Types of blockchain.

[62]   See section B.III. Types of blockchain.

[63]   See section C.II.5.b). Market definition based on the layers of the blockchain.

[64]   Pike/Capobianco, OECD Blockchain Policy Series, 6; Hoffer Raoul/Mirtchev Kristina, Erfordert die Blockchain ein neues Kartellrecht?, Neue Zeitschrift für Kartellrecht 2019, 239 et seqq., 241 (cit. Hoffer/Mirtchev, NZKart 2019).

while the blockchain itself "should be seen as platform products". As mentioned above, the blockchain is not a product nor does it intend to be one. The blockchain is just one type of distributed ledger that provides an infrastructure for new types of applications with self-regulation as described hereinafter.

Such a concept of self-regulation needs further explanation. According to *Tombs*, regulation ensures the absence of chaos. Without regulation, actors of society – or for that matter of any environment – tend to cheat. Therefore, regulation suppresses and avoids these actors or these behaviors;[65] self-regulation aims to do the same as governmental regulation with the difference that the decisions to self-regulate stem from the community itself. Self-regulation has several advantages: the rules created by the participants of a given community are fundamentally efficient, as they respond to real needs, reflect technology, and offer the possibility to flexibly adapt the legal framework to the changing environment. Since self-regulation is negotiated by the stakeholders involved, there is a high probability that such rules will be widely accepted.[66]

On the blockchain, self-regulation is an integral part of the concept itself. The participants of any blockchain (and application on the blockchain) may – depending on the structure of the blockchain[67] and the content of the smart contract[68] – also regulate business decisions acting as something similar to the general assembly of a company (more specific as the shareholders of a company). Therefore, it is wrongful to treat a blockchain as a platform product; for that reason, this comparison is flawed.

Furthermore, the core idea of digital platforms is having the function of a central party, the so-called intermediary, while the whole structure of blockchains is based on the lack of intermediaries. Therefore, this comparison is misleading as well.

However, if ever a market definition on the base layer is necessary, the approach of *Schrepel* comes closest of being applicable. He identifies

---

[65]   Tombs Steve, Understanding Regulation?, Social & Legal Studies 2002, 113 et seqq., 114.

[66]   Weber Rolf H., Sectoral Self-Regulation as Viable Tool, in: Mathis Klaus/Tor Avishalom (eds.), Law and Economics of Regulation, Cham 2021, 25 et seqq., 26; Weber Rolf H., Realizing a New Global Cyberspace Framework, Normative Foundations and Guiding Principles, Zurich 2014, 27; similar basic principles are applicable to the blockchain as well.

[67]   For detailed explanation of the structure of the blockchain, see section B.V. Main characteristics of blockchain.

[68]   See footnote 71 for further remarks on the smart contract.

substitutable blockchains on the demand side based on their nucleus.[69] While this method is possible, it may result in a too narrow view of markets. It is correct that the nucleus of a blockchain has to some extent control over the blockchain and may impose constraints on the blockchain. Even so, this should not be the approach when considering the whole infrastructure.

If authorities need to define markets on the infrastructure layer, it is important to find the opposite market side.[70] On the infrastructure layer, the opposite market side are the undertakings that seek the service of the infrastructure which is the use of the blockchain. All blockchain networks provide the same service – a blockchain. Here, a broader approach may be necessary because first of all, authorities need to decide whether blockchains and other distributed ledgers are interchangeable. As mentioned above, the special characteristic of blockchains is the chronological linkage of blocks which are connected by cryptographic hashes and constitute a unique and traceable chain. Other distributed ledgers may have fundamentally different structures which may not be favorable for certain use cases. Hence, depending on the exact use case, the substitutability of blockchains with other distributed ledgers needs to be evaluated.

Once this is determined, in a second step, the question of private/ permissioned and public/permissionless blockchain arises. Here again, depending on the exact use case of the blockchain, it is possible that all types are substitutable. But if an undertaking (or a state) needs to use a specific type of blockchain to be able to hold control, only private or permissioned blockchains may be substitutes.

b)   *Market definition on the application layer*

The actual challenge for a market definition on the blockchain is at the application layer that can remotely be compared to different websites on the internet (or even different applications on different "app stores"). An

---

69   Schrepel, Blockchain + Antitrust, 130.

70   Market definition is conducted from the perspective of the opposite market side (BSK-Reinert/Wälchli, Art. 4 para. 2, marginal no. 102; LMRKM Kartellrecht-Bergmann/Fiedler, Art. 102 marginal no. 35). The opposite market side often are the consumer, but depending on the perspective, the consumer may change.

application runs on the base layer and are a user-friendly interface that allow interaction with the smart contract[71] and other protocols of the blockchain.

On the application layer, again, different distinctions are necessary. Firstly, only applications on one specific blockchain network may be substitutes. Then, one may view all applications on public or private blockchains as substitutes. Lastly, it is also possible to assume interchangeability of applications independent of the blockchain network they are based on (only based on their products or services).

The first approach needs to be rejected. It is not reasonable to narrow the substitutes of an application to its existence on any specific blockchain network. The reasoning here is twofold: Firstly, market delineation on the base layer usually only concerns the undertakings deciding on which blockchain network they are willing to build their application. Secondly, users of the applications are seeking the services of said application and not the blockchain the application is based on. Therefore, it is not right to discard all applications on other blockchain infrastructures from the very beginning without conducting any reasonable market definition.

The second approach is more intricate. While there is some truth in the fact that private/permissioned and public/permissionless blockchains may not be interchangeable to some users, this question usually regards the undertakings building their applications on a specific blockchain network. From the perspective of the end users, however, the actual product or service of the application itself is of importance. Therefore, private/permissioned and public/permissionless blockchains may be considered to the extent that they constitute an inherent part of their product or service. Hence, competition authorities should not delineate markets for applications just on the mere fact that they are built on private/permissioned or public/permissionless blockchains.

---

71   The smart contract is based on predetermined rules (if-then rules); if the smart contract is stored on the blockchain and a predefined scenario occurs, then the contract is automatically executed – according to the predetermined consequences. Therefore, the execution of the smart contract does not necessarily require a "common" consensus in the legal sense, but merely the occurrence of the predefined event (this event itself may require a consensus but does not have to). In this respect, smart contracts are not contracts in the legal sense, but programs that automate process flows on a blockchain and ensure the correct execution of contractual relationships (for further details, see Schär, Federal Reserve Bank of St. Louis Review 2021, 154; Schär Fabian/Hübner Philipp, Blockchain und Smart Contracts im Kontext der Prozessautomatisierung, in: Bruhn Manfred/Hadwich Karsten (eds.), Automatisierung und Personalisierung von Dienstleistungen, Berlin 2020, 297 et seqq., 305).

The last approach will be – in most cases – a suitable approach. Applications shall not be excluded in advance from the scope of the market definition because of the network they are based on or because of the type of blockchain they are part of.[72]

When defining the market on the application layer, the demand side substitutability provides satisfying results. Here, comparisons to multi-sided markets[73] need to be prevented. While applications on the blockchain may provide similar services to applications on the digital economy, their fundamental structure is different. Applications in the digital economy are based on multi-sidedness with the application (or the platform) as the intermediary of the business. On the blockchain, this is logically not possible. Blockchains do not have any intermediary that is connecting two (or more) sides together. The blockchain, as a distributed ledger, is typically a public database distributed across multiple locations, countries, and institutions. Each computer interacting with the blockchain constitutes an own node that cannot be allocated to any side. Hence, the application itself, as a whole, needs other applications as substitutes which constitute the market.[74]

On this level of market definition, the use of the SSNIP test is possible too. The approach of applying the SSNIP test on this layer of the blockchain can be situated between its applications on "traditional" markets and digital markets. On digital markets, the SSNIP test tends to meet problems with the small but significant and non-transitory *increase of price* because most of these services are free of charge. To overcome this issue, it has been suggested to have a SSNDQ test (small but significant and non-transitory *decrease of quality*)[75] or that "the SSNIP should be applied to the (weighted) average competitive price applicable to the particular platform business".[76]

Applications on the blockchain, however, are not fully comparable to these platform businesses; for competition authorities, it may even be easier to define markets for the application layer on the blockchain. The SSNIP test needs no adaptation of the method itself but only on where it is applied. The general use of an application is mostly free of charge on the blockchain,

---

[72]   Similarly, Pike/Capobianco, OECD Blockchain Policy Series, 6.

[73]   To some extend Pike/Capobianco, OECD Blockchain Policy Series, 6.

[74]   Not entirely matching, but with a similar thought process Pike/Capobianco, OECD Blockchain Policy Series, 6.

[75]   Filistrucchi Lapo, Market Definition in Multi-Sided Markets, in: OECD (ed.), Rethinking Antitrust Tools for Multi-Sided Platforms, 37 et seqq., 47 et seq.; Smith/Duke, ECJ 2021, 104 et seq.

[76]   Smith/Duke, ECJ 2021, 104 et seq.

but as mentioned in the introduction, the blockchain can be seen as the internet of values. The blockchain focuses on digitally represented assets, their ownership, access to them, and transactions with these assets. The latter concept is the foundation to the other use cases. A digitally represented asset, its ownership, and access to it only is useful if a transaction proceeds them.

Therefore, any use of an application usually intends to conduct a transaction at some point. Hence, it is possible to assess the SSNIP test on said transactions. Depending on the blockchain network and the application that is being used, users need to pay a certain fee for such transaction, in most cases the native token of the application. These amounts are either measured at a percentage rate of the whole transaction or are a fixed amount. Here, the SSNIP test is applicable because a small but significant and non-transitory increase of price (here the price of each transaction) is very much possible.

Again, it is not reasonable to differentiate the applications based on the consensus mechanism.[77] The consensus mechanisms are in fact important for internal matters of each application, but this is usually of no importance to the users. The users seek the service (or product) of said application. As mentioned above, this can be compared to the internal structure of any given undertaking in the "traditional" markets. When deciding whether any two products (or services) are substitutes, it is not of any relevance whether the undertaking providing the product (or service) is a limited company or a public stock company. Similarly, it cannot be of importance whether decisions made on applications are based on proof of work or proof of stake, even if they are fundamental decisions on what product an undertaking should provide. It is possible that an application – based on the voting – decides to change its product (or service) which in return would lead to it not being part of said relevant market anymore. However, it is not necessary to exclude any application from the very beginning.

III.   Market power

The way of determining market power has been discussed and questioned in the past. Because the calculation of market power is difficult, competition authorities usually use a two-step method. First, the relevant market is

---

[77]   For the consensus mechanisms, see section B.V.3.

defined, then the potentially dominant position is determined comparing all undertakings of that market.[78] Logically, a narrower market definition tends to have more powerful undertakings.

In traditional markets, the most common method of calculating market power is based on market shares. Market shares are therefore also the starting point for analyzing whether a company is dominant. However, market shares are not as indicative on the blockchain because of their special architecture and may not be used as a proxy. Especially when considering the first layer, market shares are not a useful tool of comparison because of the differences in the value of the concerned cryptocurrency of each blockchain.[79]

1.   Existing methods

As mentioned above, the market share is an important factor when ascertaining market power.[80] In the context of blockchain, it is not clear how an authority would calculate market shares. Several approaches seem to have emerged in the past which need further clarification.

One method examines market power based on the consensus mechanisms.[81] *Hoffer/Mirtchev* suggest two different ways of identifying market power.[82] According to their first method, market power on a blockchain based on proof of stake[83] could be measured by the ownership of the issued tokens, especially if one or several users have a high volume of ownership in view of the issued tokens.[84] While this approach is able to determine who has a say in said blockchain ecosystems, it does not reveal anything on market power. This fact is rather comparable to majority shareholders in a company acting in a "traditional" market. When determining whether a company has market power (and is abusing that power), competition authorities do not need to know whether someone has a majority stake in the company or not.

---

[78]   See EGC, Judgment of 6 July 2000, Case T-62/98, ECLI:EU:T:2000:180 – Volkswagen v Commission, marginal no. 230; see also ECJ, Judgement of 14 February 1978, Case 27/76, ECLI:EU:C:1978:22 – United Brands v Commission, marginal no. 10; ECJ, Judgement of 21 February 1973, Case 6-72, ECLI:EU:C:1973:22 – Europemballage v Commission, marginal nos. 29–35.

[79]   Similarly, Schrepel, Blockchain + Antitrust, 187.

[80]   See section C.II.2. Current state of market definition.

[81]   See section B.V.3. for the consensus mechanisms.

[82]   Hoffer/Mirtchev, NZKart 2019, 244.

[83]   For a detailed description of proof of stake, see B.V.III.b).

[84]   Hoffer/Mirtchev, NZKart 2019, 244.

As specified above, the indirect method of calculating market power determines the market power of different undertakings in one defined market. *Hoffer's* and *Mirtchev's* method, however, does not consider different undertakings in a defined market, but only examines the internal matters within a blockchain infrastructure (or application) which is of no interest for competition law.

According to these authors, the other way of establishing the domination of a relevant market is by evaluating the hashing power in a proof of work.[85] As they state correctly, there is a hypothetical chance of controlling a blockchain when a group of miners can control more than 50% of the hashing power. Consequently, miners would be able to control the consensus on a network. From that, they deduce market power through these miners.[86] However, this again does not establish any market power and just describes the circumstances within a blockchain infrastructure as it just concerns the internal matters of an undertaking (i.e., control of an undertaking). This method does not allow to compare any two undertakings for antitrust proceedings.

Therefore, these existing methods are impractical and do not grant any reliable insight on market power or dominant position of an undertaking in a defined market. Hence, it is necessary to provide an appropriate proxy or approach for calculating market power on the blockchain.

2. Alternative approach for the determination of market power on the blockchain

Because the market share cannot be used as a proxy when determining market power on the blockchain, another approach is necessary. One possible solution would be to establish market power through the number of participating nodes. As mentioned, blockchains consist of different nodes forming the distributed network.[87]

One challenge of this method consists in the control over the nodes because in public/permissionless blockchains everybody is allowed to "connect" to the blockchain, i.e., to create an own node. In consequence, this situation allows to have "unused" nodes on the application. Therefore, plainly determining market power by the existing nodes does not provide satisfying results. While using

---

[85]   For a detailed description of proof of work, see B.V.III.a).

[86]   Hoffer/Mirtchev, NZKart 2019, 244; further details on the 51% attack, see Weber, DLT-Handelsplattformen, 88.

[87]   See sections B.I. Terminology, B.II. Fundamental objectives of blockchain, and B.V.2. Decentralized structure without intermediaries.

nodes as a proxy for market power might have some advantages, authorities need to further investigate the exact behavior of these nodes, i.e., investigate their activity on the application (passive users generally do not provide any added value to the system). The activity of the nodes can be determined by different factors such as participation on consensus-building, participation on the blockchain, conducting transactions or even search queries where applicable.[88]

Another interesting way of deducing the activity on a blockchain is by analyzing the hashing power spent for any one validation of a block. The faster a community is able to validate a block (thus the more hashing power they spend) the more active this community is. Hence, this blockchain (or application) usually also is more attractive than other competing blockchains (or applications).[89]

Again, another way of calculating market power on a blockchain might be to rely on the number of transactions recorded on a blockchain (or application). This, however, may lead to inaccurate results because just a high number of transactions does not equal to high market power. This method needs to be combined with the volume of transactions conducted on said blockchain. Because the blockchain is regarded as the internet of values, the number of transactions combined with the volume of those transactions may provide valuable insight on market power. When considering the volume of a transaction, further problems may arise, especially the high fluctuation of the value of tokens[90] on the blockchain.[91] There are, however, possibilities to circumvent this problem. Even though *Schrepel* also brings up the problem of high fluctuation, he disregards the fact that, when analyzing different blockchain structures, authorities do not necessarily need to convert the value of a token to fiat money. It is easily possible to calculate the value of tokens on the blockchain based on an "anchor token". Then, there is a lot less fluctuation of the tokens under investigation and the analysis is kept in the blockchain environment without outside world influences.

Due to the fact that transactions are of great importance on the blockchain the generated revenue on the blockchain or the applications may also be one of many indicators on its market power.

---

[88]   Similarly, Schrepel, Blockchain + Antitrust, 190; Lianos, Blockchain Competition, 86.

[89]   Lianos, Blockchain Competition, 86.

[90]   A token in the context of distributed ledgers is considered a digital representation of a good and can be traded like assets that are part of the underlying protocol.

[91]   See also Schrepel, Blockchain + Antitrust, 189.

In contrast to the already existing ways of determining market power on the blockchain, this method comprehensively captures the (economic) activity on a blockchain and not the internal organization of it. In addition, the activity of the nodes can compare different applications regardless of whether the investigated undertakings are based on a public/permissionless or private/ permissioned blockchains.

D.   Outlook

As two core elements of antitrust proceedings, market definition and market power have always been an object of competition law literature. This most probably will not change with the challenges of the blockchain developments. Even though this topic is still to be fully explored by informatics, business, law, and other scholars, it seems to be important to take first actions where possible.

Similar to the developments in the context of the regulation of financial markets, it remains to be seen what importance blockchain architecture will have for authorities. There has not been any antitrust case concerning the blockchain so far. Nonetheless, first discussions on this topic seem to show that a correct application of the already known (and with the digital developments expanded methods) usually appear to be able to seize the challenges faced with blockchain.

In view of market definition, this article suggests distinguishing between each layer of the blockchain architecture. The base layer is comparable to the infrastructure layer of the internet. As for the internet, the infrastructure layer usually is not part of antitrust proceedings. Authorities are more concerned with what happens on this infrastructure. Similarly, in the context of blockchain, authorities will most probably deal with applications that are created on said infrastructure. It is imperative that competition authorities do not differentiate from the very beginning between markets based on the blockchain network itself and markets based on the type of blockchain (public/permissionless or private/permissioned). When looking at the application layer, a market for the application as a whole can be constituted by applying the concept demand side substitutability. Furthermore, it is possible to define a market based on the SSNIP test as every application conducts a transaction. Such a transaction is coupled with a fee, be it at a percentage rate or a fixed amount, which can serve as the price that needs to be increased.

In the past, it has been suggested that market power may be calculated through ownership in tokens on a proof of work or control of more than 50%

on a proof of stake system. Both methods, however, do not provide sufficient knowledge on market power, but only on internal control of an undertaking which is of no relevance for competition law. Therefore, this article suggests determining market power through the activity of nodes in any blockchain network or application. The activity of nodes is a valuable indicator on active usage of the network or application.

As shown, there is no need to adapt the antitrust laws themselves because selectively adapting the approach to market definition and calculation of market power seems sufficient. This would also be in line with the desirability of making regulations technologically neutral when regulating DLT and blockchain law.

This article has not touched on various other problems regarding competition law in the blockchain environment which need further investigation. Once market definition and market power are established, authorities have to look at anti-competitive practices by undertakings. But in the context of blockchain, it is important to first acquire insights on what layer of the blockchain is of interest and on what exactly constitutes the undertaking (or on what this undertaking consists of). The theory of granularity lays the ground for that analysis.

EuZ
ZEITSCHRIFT FÜR EUROPARECHT

25. Jahrgang