eLaw

No 2019/007 - ELAW– 31 October 2019

(Re-) Defining Software Defined Networks under the European Electronic Communications Code

Serge J.H. Gijrath

Universiteit Leiden
eLaw

(Re-)Defining Software Defined Networks under the European Electronic Communications Code

Prof. dr. Serge J.H. Gijrath, eLaw@Leiden University, the Netherlands

Abstract — This article assesses prospective regulation of Software Defined Networks (SDN) and Network Functional Virtualization (NFV) in the European Union (EU). The overall research for this article focuses on the re-regulation of the European Electronic Communications Code ('EECC') and the Commission's desire to promote innovation to better compete on the global communications and technology market. After a concise technological introduction, this Article discusses three regulatory & legal issues: (1) the qualification of SDN and access to fixed networks and network elements of electronic communications networks (ECN) by either software suppliers or electronic communications service providers (ECS); (2) the asymmetry in network elements sharing by ECNs and (mobile) virtual network operators (MVNOs); and (3) the allocation of responsibility for network and information security. Following up on BEREC's recommendations of 2016, this Article touches upon whether and, if so, how innovation policy objectives in the EECC could be translated in sustainable regulation.

Key words – *Access regulation; BEREC; Convergence fixed/mobile networks; European Electronic Communications Code (EECC); Electronic Communications Networks (ECN); 5G frequencies; Incentives for innovation; Network Function Virtualization (NFV); Network and Information Security; OSI-model; Software Defined Networks (SDN); Technology Standards.*

(Re-) Defining Software Defined Networks under

I. A Concise Description of SDN and NFV

1. Great expectations

A major shift in the configuration of telecommunications networks has been ongoing gradually. Governments across the globe have expressed high expectations on the commercial take-off of 5G, including the virtualization of network functions and the uncoupling of service layers. Both Software Defined Networks (SDN) and Network Function Virtualization (NFV) transform the way that network operators design and operate networks.

These new technologies are as important as the introduction of IP networks.[1] The take-off of IP technology in many networks of telecom operators has brought both planes together. The basis for SDN is the separation of the control and user data planes. BEREC 2016 describes SDN as: "*a new architecture where network control is logically centralized (decoupling of control and data planes), directly programmable and the underlying network infrastructure is abstracted from the applications*."[2] The decoupling of the control and data planes allows SDN to centralize the control plane functions in a single entity (the SDN controller). The SDN controller thus is capable of providing a centralized view of the available resources and making the network more dynamic and reactive than a distributed control plane. The SDN controller may also operate an abstraction layer. This layer is designed to hide the infrastructure characteristics of the operator. It makes the

[1] *"*BEREC Input paper on Potential Regulatory Implications of Software-Defined Networking and Network Functions Virtualisation*", BoR (16) 97* referring to Little, A.D., Bell Labs, *Reshaping the future with NFV and SDN. The impact of new technologies on carriers and their networks*, 2015 (Little 2015) http://sdn.ieee.org/images/pdf/adl_belllabs_2015_reshapingthefuture.pdf.

[2] BEREC 2016, Annex 1. Normally, a communications network is a medium to which many nodes can be connected, on which every node has an address and which permits nodes connected to it to transfer messages to other nodes connected to it.

electronic communications network (ECN) programmable through an API independent of the technology.[3]

NFV uses software which can dynamically be moved to, or instantiated in, various locations in the network layers as required, without the need for installing new equipment.[4] SDN and NFV are complementary, but SDN does not have to use NFV. Conversely, NFV cannot always function without SDN, because it enables vertical separation of the ECN functions. In the context of 5G ECN operators may profit from "*unprecedented programmability, automation, and network control, enabling them to build highly scalable, flexible networks that readily adapt to changing business needs.*"[5] A wide variety of eco-systems emerges and network openness is enhanced. Additionally, SDN supports multi-tenancy.[6] Research suggests that SDN/NFV are likely to reduce CAPEX and OPEX and the risk of sunk costs. SDN/NFV enhances innovative electronic communications services (ECS).[7]

The primary objectives of the enhanced regulation remain the promotion of competition, the internal market and end-user interests. Still, the regulatory focus could have an impact on SDN and NFV services provision. The EECC focuses on achieving that ECNs and ECS contribute to the widespread access to and take-up of very high capacity networks for all EU citizens and businesses on the basis of reasonable price and choice. The considerations of the EECC first of all reiterate the

---

[3] *A survey of 5g technologies: regulatory, standardization and industrial perspectives*, Chongqing University of Posts and Telecommunications, Elsevier B.V. 2017.

[4] *Network Functions Virtualisation*, Introductory White Paper (ETSI 2012): http://portal.etsi.org/NFV/NFV_White_Paper.pdf; ETSI GS NFV 001, *Network Functions Virtualisation (NFV); Use Cases*, *V1.1.1*, Oct. 2013; (ETSI 2013); http://www.etsi.org/deliver/etsi_gs/NFV/001_099/001/01.01.01_60/gs_NFV001v010101p.pdf
ETSI GS NFV 002, *Network Functions Virtualisation (NFV); Architectural Framework, V1.2.1*, Dec. 2014 (ETSI 2014);
http://www.etsi.org/deliver/etsi_gs/NFV/001_099/002/01.02.01_60/gs_NFV002v010201p.pdf
ETSI GS NFV-EVE 005, *Network Functions Virtualisation (NFV); Ecosystem;*
Report on SDN Usage in NFV Architectural Framework, V1.1.1, Dec. 2015
http://www.etsi.org/deliver/etsi_gs/NFV-EVE/001_099/005/01.01.01_60/gs_NFV-EVE005v010101p.pdf (ETSI 2015).

[5] BEREC 2016, p. 6 and figure 1.

[6] Infra, para. III.3.

[7] *Infra*, figure 1. 'ECS' (art. 2 (4) and 'ECN' (art. 2 (1)) are defined terms in the EECC.

objectives of effective and fair competition, open innovation, efficient use of radio spectrum, common rules, predictable regulatory approaches in the internal market and the necessary sector-specific rules to safeguard end-user interests. In addition, the connectivity objective aims at promoting the highest capacity networks and services economically sustainable in a given area, and, the pursuit of convergence in capacity available in different geographic areas – in particular rural areas.[8] The EECC places more obligations on the Member States, the national regulatory and other competent authorities and the stakeholders to achieve the connectivity objective.

The expectation is that 5G frequencies will perform significantly better than 4G and other predecessors on such performance indicators as latency, data rates and energy usage. The regulatory framework is intended to cover the use of radio spectrum by all ECNs, including the emerging self-use of radio spectrum.[9] What makes SDN truly innovative in the current regulatory environment is that the ECN operator has a broader menu of choice with respect to 5G infrastructure configuration and deployment. The ECN operator may choose between: (i) logically centralized network control; (ii) open APIs, i.e., interfaces that can be programmed to support the independent evolution of software used on the infrastructure; (iii) a standardized switch protocol; or (iv) an implementation of third party network services and virtualization of the logical networks – the latter two requiring the use of NFV.

The EECC acknowledges SDN. It prescribes the adjustment of definitions to: "(…) *ensure that they are in line with the principle of technology neutrality and to keep pace with technological development, including new forms of network management such as through software emulation or software-defined networks* (…)."[10]

---

[8] EECC, Consideration (23).

[9] EECC, Considerations (12) and (24) express the Commission's desire to warrant the availability of uninterrupted 5G coverage for urban areas and major terrestrial transport paths, and the availability to all households in each Member State of ECNs which are capable of providing at least 100 Mbps, and which are promptly upgradeable to gigabit speeds.

[10] EECC, Consideration (14).

When SDN technology increases infrastructure agility this begs the question how it fits in the Open Systems Interconnection (OSI) model.[11] Simply put, the OSI model functions as a universal language for computer networking. The OSI model partitions various communications systems into abstraction layers. The seven layers are often characterized similarly, although there are some nuances.[12] The models distinguish between media and host layers. Clearly, the take-off of the Internet Protocol (IP) and the use of the Transmission Control Protocol (TCP) in networks impacted the network layers significantly. Figure 1 shows a traditional and slightly reworked representation of the model with the physical network layer at the bottom.[13]

Figure 1. OSI Model[14]

Layer			Protocol data unit	Function
Host layers	7	Application	Data	The application layer closest to the end-user. This layer and the user interact directly with the software application. This layer typically also includes identifying communications parties, determining identity and availability.
	6	Presentation		The presentation layer establishes the context between the application layer entities (layer 7) in which the application layer entities may use different syntax and semantics.
	5	Session		The session layer controls the connections between the systems. Connections between local & remote applications are established, managed and terminated. This layer also establishes procedures for checkpointing, suspending, restarting or terminating a session. The TCP handles this at the transport layer in the IP suite.

[11] The OSI model conceptualizes different standard protocols that enable various communications systems to interconnect and, thus, achieve network and functional interoperability. Hubert Zimmermann first defined the OSI Model in raw form in Washington, DC in February 1978. A refined standard was published by the ISO in 1984, ISO/IEC 7498. See, i.a., "OSI: the Internet That Wasn't". *IEEE Spectrum*. March 2017.

[12] Gijrath, S.J.H, *Interconnection Regulation and Contract Law*, Amstelveen, DeLex, 2006 (Gijrath, 2006), p. 119-120; Palfrey, J., Gasser, U., *Interop, the promise and perils of highly interconnected systems*, Basic Books, New York, 2013.

[13] The International Organization for Standardization.

[14] Reworked for this Article by the author.

	4	Transport	Segment, Datagram	The transport layer provides the functional and procedural means of transferring variable-length data sequences (packets) from a source to a destination host, whilst maintaining the quality of service (QoS) functions.
Media layers	3	Network	Packet	The network layer provides for the functional and procedural means of transferring variable-length data sequences (packets) from one node to another in various networks.
	2	Data link	Frame	The data link layer provides node-to-node transfer. This is a link between two directly connected nodes. The link detects and possibly corrects errors that may occur in the physical layer.
	1	Physical	Symbol	The physical layer provides for the transmission and reception of unstructured, raw data between the device and the physical transmission medium. Simply put: the physical layer converts digital bits into electrical, radio or optical signals.

A notable distinction between SDN and NFV is that SDN impacts the network configuration layers, whereas NFV does not necessarily. The SDN is likely to be configurated in the media layers. NFV is virtually part of different layers, including the data layers. NFV is aimed more at the optimizing of the ECN's resources. The various communications protocols enable the SDN controllers to use different types of application programming interfaces (API's) downwards. This enables ECN operators to modify their network specifications more flexibly. The technology can be applied upwards to communicate better with different customer applications. The core network (including data) can be excluded from the infrastructure, making active network sharing arrangements between competing operators more attractive as well.

NFV supports MVNOs in customizing user needs at all layers. They may compete directly with the ECN operator who will host them on the quality of service levels (QoS).[15] Consequently, the ECN operator will be able to consolidate its network infrastructure. Network functionality can be managed virtually. This brings both cost savings and a more efficient administration of networks. In an SDN environment, the MVNOs no longer need full access to an ECN. SDN enables access of third parties

[15] MVNOs do not operate their own network infrastructure. See also Wazir, F., *Can NL trust 5G? A conceptual model for of cybersecurity supervision in the Netherlands*, 2019.

to network control functions, whilst controlling their own physical and virtual core network elements. Radio Access Network (RAN) equipment can be configured in new ways to allow for shared use, even though no active equipment is shared. NFV enables the ECN operators to manage the various network traffic events. This way, the network control plane can be separated from the traffic control (voice, data). NFV's key innovation is that it enables certain network functionality to be translated into software, which can run on cheaper, generic, hardware elements which can be added to the ECN.[16] NFV uses various IT technologies to virtualize entire classes of network node functions, in order that the *same* infrastructure can run different systems and applications software functions for ECS providers (e.g., the MVNOs discussed above).

Nevertheless, in 2017, there were also voices that while SDN/NFV could offer the same functionality as some existing access and interconnection products, the physical infrastructure, to which most telecommunication regulation applies, would remain unchanged.[17]

2. Scope of research

SDN and NFV may potentially be affected by the EECC.[18] In 2017, when SDN/ NFV were still subject to scrutiny by regulatory authorities, it was difficult to predict the specific effects of developing policies or regulation. The methodology is aimed at

---

[16] Alexiades, P., Shortall, T. 'The Advent of 5G: Should Technological Evolution Lead to Regulatory Revolution?' Paper, *Competition Policy International*, November 2016 (G. Alexiades, P., Shortall, 2016); Brownsword, R., Goodwin, M., *Law and Technologies of the Twenty-First Century*, Cambridge University Press, Cambridge, UK, 2012; see also TSM Proposal 2016, p. 1.

[17] See ECTA's response to BEREC's work programme 2016, p. 19: "In ECTA's view, such technological developments do not seem prima facie to affect the physical network layer and thus would not affect the need to retain regulation in market 3a. The same is likely the case for Layer 2 transport as such, and hence it would not affect the need to retain regulation in markets 3b and 4."

[18] Soft law initiatives will not be discussed in detail. These include such regulations and recommendations coming from the International Telecommunications Union (ITU) , the Internet Engineering Task Force, (IETF), the Third Generation Partnership Project (3GPP), the authoritative Institute of Electrical and Electronic Engineers for standards (IEEE), the Fifth generation partnership project (5G-PPP). All of these initiatives are likely to have a decisive influence on the architecture of 5G, including SDN and NFV elements. The Body of European Regulators for Electronic Communications (BEREC) has different role: it has to promote greater regulatory coordination and consistency in the Member States.

using various regulations to determine the place of SDN/NFV. There will be less focus on NFV in light of the nature of the technology.

Following a short discussion on prospective network innovation policy, this Article discusses three regulatory aspects surrounding SDN/NFV from an EU perspective: (1) the legal qualification of SDN/NFV under the EECC and access rights; (2) the asymmetry between traditional network operators versus virtual network operators; and (3) network and information security responsibilities, including cost allocation.[19] For this reason, this Article alludes to the NIS Directive,[20] and the Cybersecurity Act that entered into force on 27 June 2019.[21] Some reference is made to the relevant provisions in the General Data Protection Regulation (GDPR).[22] This Article leaves open other legal questions, such as SDN and intellectual property and the role of NRA's.

3. Structure and methodology

This Article is structured as follows. Para. II discusses the EECC high-level in the context of governments' desires to innovate networks further, whilst focusing on public policy needs and regulation. This para. describes symmetric regulation. Para. III analyses the three legal questions set forth above. Para. IV. contains final remarks. The input for the three regulatory issues in this Article has been drawn mostly from extensive desk research.

---

[19] Scott-Hayward, S. Natarjan, S. & Sezer, S., *A Survey of Security in Software Defined Networks. IEEE Communications Surveys and Tutorials*, 18(1), 623-654, provide an overview of the characteristics of SDN in light of security aspects. DOI: 10.1109/COMST.2015.2453114, 2016 (Scott-Hayward, S. Natarjan, S. & Sezer, S., 2016) para. II. Another feature they mention is centralized monitoring units, but, these are not specific to SDN architecture, see p. 4, sub-para. 6. Open Network Foundation, *Principles and Practices for Securing Software Defined Networks*, ONF Paper TR-511, January 2015.

[20] Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union *OJ L 194, 19.7.2016* (NIS Directive).

[21] 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). The Cybersecurity Act was preceded by the now repealed ENISA Regulation of 2013.

[22] Regulation (EU) 2016/679 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* L 119/1.

II. SDN: Shifting Policy and Regulatory Perspectives?

1. A tale of two (or more) competitors

Both very high-speed broadband networks and 5G deployment could benefit from SDN technology.[23] Application of SDN will blur the distinction between network and services interoperability further. While 'transmission of signals' remains an important parameter for determining the services falling into the scope of the EECC, it aims to cover any services that enable communication.[24] This is reflected in the definition of the 'interpersonal communications service'. This definition is ubiquitous in the EECC's considerations.[25] By adding the definition of interpersonal communication service to EECC the scope of ECS is broadened.[26] The Commission expects a significant enhancement of infrastructure competition as a result of the implementation of innovative solutions in telecommunications networks and bringing new services to within the scope of the EECC is a way to control them.[27] The definition of ECN has not been updated significantly. This is due to the addition of the new notion of 'very high capacity network'. This separate definition reveals the level of detail the EECC desires in terms of converging very high capacity with

---

[23] *Supra*, EECC, Consideration (14).

[24] EECC, Consideration (15).

[25] Definition of Interpersonal Communication Services (Art. 2 sub 5 EECC): "'*interpersonal communications service' means a service normally provided for remuneration that enables direct interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons, whereby the persons initiating or participating in the communication determine its recipient(s) and does not include services which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service*'".

[26] Art. 2 sub 4 EECC.

[27] See also Recast Proposal for a Directive of the European Parliament and the Council Establishing the European Electronic Communications Code, *COM(2016) 590 final, 2016/0288 (COD)*, Brussels 14.9.2016 (TSM Proposal 2016). See also: EU Workplan to achieve smart and sustainable growth: Horizon2020, 2017, 'Work Programme 2018-2020', unauthorized version. In the EU, the designated frequency bands 700 MHz, 3,6 GHz and most likely 26 GHz.

advanced mobile networks.[28] The next para. will analyse whether SDN/NFV could qualify as an ECS.

2. Innovation policy objectives

In the run up to the EECC, DG Connect commissioned an extensive and thorough study into the technological, economic, and regulatory implications of both SDN and NFV.[29] According to these studies, SDN suggests a number of regulatory issues. The BEREC 2016 report alluded to the potential regulatory implications of SDN and NFV.[30] The BEREC 2016 report looked at which adaptations of the regulatory framework could be needed.[31] The BEREC 2016 report on SDN/NFV was

[28] Art. 2 sub (1) EECC defines ECN. It is supplemented by the more specific definition in art. 2 sub (2), which defines the 'very high capacity network' as: "*either an electronic communications network which consists wholly of optical fibre elements at least up to the distribution point at the serving location, or an electronic communications network which is capable of delivering, under usual peak-time conditions, similar network performance in terms of available downlink and uplink bandwidth, resilience, error-related parameters, and latency and its variation; network performance can be considered similar regardless of whether the end-user experience varies due to the inherently different characteristics of the medium by which the network ultimately connects with the network termination point.*"

[29] On the various aspects and regulatory issues: *i.a.*, Assessment of the need to review the BEREC Common Positions on Markets 3a, 3b and 4 BoR (18) 24; R. Arnold et al. *Implications of the emerging technologies Software-Defined Networking and Network Function Virtualisation on the future Telecommunications Landscape*" (Study prepared for the European Commission DG Communications Networks, Content & Technology, p. 1-222) Last updated: 11 May 2017 (Arnold et al. 2017, hereinafter: '2017 DG Connect Study'); J. Garay et. al. "Service description in the NFV revolution: Trends, challenges and a way forward", *IEEE Communications Magazine*, vol. 54, issue, March 2016 (Garay et al. 2016*);* BEREC 2017*;*
T. van der Vorst et al., *The impact of network virtualization on the Dutch telecommunications ecosystem: An exploratory study*, p. 1-87, 2016 (Van der Vorst et al. 2016); S. Iyer, "Virtualisation of Network Functions and the SDN: Improving the Economics of the Network", *Journal of Telecommunications and the Digital Economy (AJTDE)* - Vol 2, No 2 - May 2014 (Iyer 2014); ITU, *Workshop on Software Defined Networking (SDN) Standardization Landscape,* Geneva, Switzerland, 4 June 2013 (ITU 2013); ETSI (various contributors), *Network Function Virtualisation – Introductory White Paper*, 2012 (ETSI 2012).

[30] BEREC 2016, p. 5.

[31] This Article revitalizes some of BEREC's research in the context of the EECC.

issued prior to the 2018 new European Electronic Communications Code (EECC)[32] and its conclusions were reticent.

The EECC is aimed at simplifying regulation by merging various Directives and Regulations and enhancing electronic communications regulation.[33] The findings of the 2017 DG Connect Study supported that SDN and NFV could have positive effects on the cost structure of network connectivity provision. SDN could also bring a shift from operators focusing more on the provision of wholesale services instead of end-user services. In such a scenario, ECN operators could profit economically from developing novel services that require SDN/NFV.

The 2017 DG Connect Study referred to prior studies and underlined that SDN and NFV represented technologies at an early stage of development and deployment.[34] 4G frequencies enabled an all IP based, packet switched core network, moving networks further away from traditional circuit switching. But 5G enables handling a hundred times higher data rates and a hundred times higher traffic density. 5G also offers greater network reliability, a factor of fifty lower latency, connectivity for more than hundred times more devices per area and a hundred times lower energy usage in support of applications.

---

[32] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, *OJ L 321,* 17.12.2018, p. 36–214 (EECC or Telecom Code). It entered into force on 21 December 2018 and it must be implemented by the Member States of the EU by 21 December 2021.

[33] The tools to test the effectiveness and sustainability are defined in the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Regulatory Fitness and Performance (REFIT): Results and Next Steps, *COM (2013) 685 final*, Brussels, 2.10.2013 (REFIT 2013). The Commission also published three accompanying documents with assessments of the impact on the market of the proposed EECC: Commission Staff Working Document, Impact Assessment, Accompanying the document Proposals for a Directive of the European Parliament and of the Council establishing the European Electronic Communications Code (Recast) and a Regulation of the European Parliament and of the Council establishing the Body of European Regulators for Electronic Communications, Brussels, 14.9.2016 *SWD(2016) 303 final*, (in 3 parts, hereinafter: 'Impact Assessment'). See also: Amendola, G., Gassot, Y., Lebourges, M., Stumpf, U., 'Re-thinking the EU telecom regulation', *DigiWorld Economic Journal*, no. 93, 1st quarter 2014, p. 17-35 (Amendola, G., Gassot, Y., Lebourges, M., Stumpf, U., 2014).

[34] BEREC 2017, p. 59*ff*; Van der Vorst, T.; Naudts, B.; de Bijl, P.; Verbrugge, s. & Brennenraedts, R. (2016): *The impact of network virtualisation on the Dutch telecommunications ecosystem: An exploratory study*. A study commissioned by the Dutch Ministry of Economic Affairs. Project 2016.024. Utrecht: Radican Economics, iMinds, dialogic (Radican et al. 2016).

Consequently, the general idea is that the deployment of SDN will have a profound impact on how ECN mobile operators roll-out, implement, use and offer the new generation of RAN equipment once they have obtained 5G frequency licenses. With its vast amount of applications and services, the 5G landscape will span from end-user devices to the RAN, to the mobile core network and the Internet. Where the 5G network functions as a utility or critical infrastructure the security threats are likely to increase. Given the vastly increasing numbers of applications and services, the 5G threat landscape will span from end-user devices to the RAN, to the mobile core network and the Internet. Conversely, SDN may offer expanded security solutions, including possibilities for Deep Packet Inspection (DPI) of data traffic of operators and service providers alike.[35]

In terms of new features, the 2017 DG Connect Study on SDN mentioned that the probable most likely network use options would be: (1) the virtualisation of mobile core networks, (2) the virtualisation of content delivery networks, and (3) the virtual network platform as a service (VNPaaS).[36] In addition to the above applications, academics identified other innovations that could impact ECNs. These would include device-centric architectures, millimetre wave, massive multiple input/multiple output (MIMO), smarter devices, and native support for machine-to-machine communications.[37] The Commission conducted a SWOT Analysis on whether or not to implement specific regulation, where the focus of attention was the option of access regulation.[38]

---

[35]Scott-Hayward, S. Natarjan, S. & Sezer, S., 2016, p. 4, give a technical description of SDN and NFV in the context of securing these networks.

[36] 2017 DG Connect Study, p. 30-48 on the business potential and p. 59-84 on policy and regulatory implications.

[37] Boccardi, F. Heath, R.W., Lozano, A. Marzetta, T.L., Popovsk, P. "Five Disruptive Technology Directions for 5G," *IEEE Communications Magazine,* vol. 52, no. 2, pp. 74 - 80, February 2014.

[38] *2017 DG Connect Study*, page 60, Figure 7-1; see underlining studies: Kim, J, Kim, Y., Gaston, N., Lestage, R. Kim, Y., Flacher, D., (Kim et al 2011), "Access regulation and infrastructure investment in the mobile telecommunications industry", *Telecommunications Policy***,** Vol**.** 35, Issue 11, December 2011, Pages 907-919; Bourreau, M., Cambini, C., Hoernig, S., "Ex ante regulation and co-**i**nvestment in the transition to next generation access", *Telecommunications Policy***,** Vol**.** 36, Issue 5, June 2012, Pages 399-406.

It is important that wholesale-only operators can focus on the roll-out of fibre infrastructure and the related wholesale offers for third parties. To this effect, the Commission adopted a co-investment approach. It provides that co-investment models are exempted from cost-oriented pricing under certain cumulative conditions; as long as the access conditions are transparent and non-discriminating for third parties, it considers high capacity network elements to be useful. The starting point is that competition conditions must not deteriorate. The Commission has considered to exempt wholesale-only operators from price regulation, even when they possess significant market power.

There is some room for subsidizing innovation. The Commission rolled out modest packages intended to stimulate SDN/NFV. The H2020 initiative offers a host of subsidies to market parties for network improvement.[39] The initiative also stimulates strongly R&D and innovation activities on telecommunications issues.[40] Yet it remains to be seen whether mobile ECN operators are incentivized enough under the EECC to innovate their networks fundamentally.[41] This is tricky where ECNs focus on different network elements sharing options.[42] Economic research point at a light regulatory and pro-investment approach to drive SDN/NFV and deployment.

3. Symmetric v. asymmetric regulation

The mobile electronic communications sector remains atypical in comparison with other network sectors in that it is subject to recurring significant investment issues,

---

[39] WP2018-2020.

[40] Commission (2018), A guide to ICT-related activities in WP2018-20 (WP2018-20). See also Granieri, M., Renda, A., *Innovation Law and Policy in the European Union, Towards Horizon2020*, Springer, 2012 (Granieri M., Renda, A., 2012);

[41] Gijrath, S.J.H., 'Telecommunications Networks in the EU: Towards Smarter Regulation and Contracts?', *CRNI*, 2017, vol. 18 (3-4), 2018, p. 175-197 (Gijrath 2017); from the same author: "Infrastructure Innovation in India: What can be inferred from EU Regulation?", 14/1 *Indian Journal of Law and Technology*, 2018, p. 41-60 (Gijrath 2018-2).

[42] Gijrath, S.J.H., 'Negotiating and Performing Infrastructure Sharing Agreements under the European Electronic Communications Code' 2018, 24 *C.T.L.*R. issue 4 (Gijrath 2018-3). Consideration (111) alludes to facilitating the sharing of radio spectrum. See reference to CEPT under Decision No 676/2002/EC and standardisation requests to standardisation bodies, such as the European Telecommunications Standards Institute (ETSI).

when frequency licence terms expire. The specificity of asset investments has been identified as the most important rationale for vertical integration. This rationale applies directly to the infrastructure investments necessary to provide ECS. The mobile ECN operator must strike a balance between addressing the demand of increased network capacity and excess capacity versus avoiding unnecessary duplicate investments.[43] To address this, the EECC contains a new provision ordering Member States to match the duration of the radio spectrum for an appropriate period for investment amortization.[44] This paragraph discusses to what extent the EECC could include regulation of either ECNs or SDN/software suppliers.[45] The starting point is determining the place of SDN/NFV in the EECC. The mere scope of the regulation begs the question whether and how it can be achieved to ensure that the EECC will remain sustainable and able to ensure investment whilst also being able to regulate where this is required.[46] Arguably, the EECC could still cause a "*regulatory distortion of competition*", which could inhibit investments.[47] A difference between fixed and mobile markets is that in the latter market mandated inefficiencies occur as a result of the prices realized in the allocation of spectrum; these are so high that these costs may have a negative

---

[43] Art. 3, para. 4 sub (d) EECC instructs NRA's, *inter alia*, to promote efficient investment and innovation in new and enhanced infrastructures and permit various cooperative arrangements.

[44] Art. 49 para. 1 EECC.

[45] Cave, M., 'Encouraging Infrastructure Competition Via the Ladder of Investment', *Telecommunications Policy*, 30, pp. 223-237 (Cave, M. 2006); Vogelsang, I., 'Incentive Regulation, Investments and Technological Change, in: G.R. Faulhaber, G. Madden, J. Petchey, *Regulation and the Performance of Communications and Information Networks*, Edward Elgar, 2012 (Vogelsang, I., 2012) p. 1; Guthrie, G., 'Regulating infrastructure: The impact on risk and investment', *Journal of Economic Literature*, 44(4), pp. 925-972.

[46] The EECC entered into force in all Member States on 21 December 2018 without any special consideration for SDN/NFV legal issues. It alludes to the Interinstitutional Agreement of 13 April 2016 on Better Law-Making, *OJ* L 123, 12.5.2016, p. 1. The EECC merges 10 pieces of regulation into one. This has resulted in a code that consists of 127 provisions, 12 Annexes and 326 explanatory considerations.

[47] Allouët, A-M, Le Franc, S., Marques, M-N, Rossi, L., 'Achieving a Level Playing Field between the Players of the Internet Value Chain', in: Bock, W.D., Wilms, M., Soos, P., Roeber, B. (2014), Reforming Europe's Telecoms Regulation to Enable the Digital Single Market' p. 99-118 (Allouët, A-M, Le Franc, S., Marques, M-N, Rossi, L., 2014); Boston Consulting Group, *Reforming Europe's Telecoms Regulation to Enable the Digital Single Market*, report for ETNO 2012 (Boston Consulting Group 2012).

impact on the speed of 5G roll-out. This impediment does not benefit end-users. Yet, following the BEREC Report of 2016, the EECC has remained reticent on defining the importance and scope of access to the market of new technologies such as SDN/NFV. Defining SDN seems to have been a matter of concern.[48] The EECC appears to create legal space to bring SDN under the scope of both asymmetrical (*i.e.* aimed at the incumbent ECN operator)[49] *and* symmetrical regulation when needed. The EECC, but the EECC does not redefine SDN; it appears to keep its options open for symmetric regulation.[50] Typical for the EU's policy to harmonize rules across the Union, the Commission's approach is more and more institutional. The EECC leaves it to the national regulatory authorities (NRAs) of the Member States to pursue the general and high-level objectives set forth in the EECC and to apply the (new) rules in detail.[51] The emphasis on the role of institutions underlines the Commission's need to cater for the uncertainties of network innovation. This is very much reflected in the 2017 DG Connect Study. Not all the draft tasks bestowed on the NRAs made the final text of the EECC.[52] In sum, it is unclear to what extent market parties can expect symmetric regulation.

---

[48] EECC, Consideration (14): "*Definitions need to be adjusted to ensure that they are in line with the principle of technology neutrality and to keep pace with technological development, including new forms of network management such as through software emulation or software-defined networks*."

[49] *E.g.*, Art. 17 para. 1 sub (a) and (b), which used to apply to companies with significant market power only. The EECC stipulates that all ECN and ECS companies must keep separate accounts; but the Member States can apply a minimum threshold for this requirement of EUR 50M. Another measure requires all ECN and ECS companies to provide information to the regulatory authorities, but here the SMP parties have stronger obligations regarding the submission of accounting data upon request.

[50] *Cf.* the main provision in art. 76, and 67, 79, and Annex IV EECC, which describes the criteria for signing off on co-investment initiatives.

[51] Art. 3, sub 2, paras. (a)-(d) of the EECC.

[52] Art. 5, first para. EECC. Initially, the NRA's were mandated to (i) further stimulate efficient competition at the infrastructure level; (ii) stimulate access to and take-up of very high speed broadband networks by all EU citizens and companies; (iii) remove the remaining obstacles and the creation of convergent conditions for the investment in and the delivery of ECN, associated facilities and services and (iv) assure that EU citizens will take up the widespread high fixed and mobile capacity and the underlying ECS and realization of the maximal advantages in terms of choice, price and quality.

III. SDN/NFV: Three Legal Issues

1.1 *The qualification of SDN/NFV*

To determine the possible regulatory aspects affecting SDN/NFV an analysis of the stakeholders' business must made under the EECC. This paragraph describes the qualification from the perspective of the SDN/NFV provider. The question whether a provider qualifies an ECN, an ECS or an undefined entity is relevant because varying rights and obligations apply dependent upon the legal status of the provider. Given that SDN/NFV do not require the exploitation of an ECN, the focus will be on whether SDN/NFV could qualify as an ECS as defined in art. 2 (4) EECC.[53] In any case, then the general authorisation regime will take effect.[54] In that case the SDN provider may be required to notify the NRA in the jurisdiction where the services are provided.[55] The notification requirement is part of the general art. 12*ff*. EECC. If the SDN supplier qualifies – partly or wholly – as an ECS provider, then this brings certain legal obligations to the SDN supplier. Examples are end-user obligations including transparency on the service, the obligation to afford for tapping, e-Privacy, net neutrality, and network and information security.[56]

Three criteria are decisive for assessing whether a telecom service qualifies as an ECS.[57] In 2019, the CJEU issued two judgements on the qualification of ECS

---

[53] Art. 2 (4) EECC reads: '*electronic communications service' means a service normally provided for remuneration via electronic communications networks, which encompasses, with the exception of services providing, or exercising editorial control over, content transmitted using electronic communications networks and services, the following types of services: (a) 'internet access service' as defined in point (2) of the second paragraph of Article 2 of Regulation (EU) 2015/2120; (b) interpersonal communications service; and (c) services consisting wholly or mainly in the conveyance of signals such as transmission services used for the provision of machine-to-machine services and for broadcasting*.'

[54] Art. 2 (22) EECCC defines the general authorisation.

[55] Previously art. 6 of Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive) (OJ L 108, 24.4.2002, p. 21).

[56] On network and information security, *Infra,* para. III.3.

[57] Part II, chapters 3 en 4 in: S.J.H. Gijrath, S. van der Hof, A.R. Lodder, G-J Zwenne (eds)., *Concise European Data Protection, E-Commerce and IT Law*, 3rd ed., Kluwer Law International, 2018. Gijrath, S.J.H., "Skype and Google", ECS or not? *Mediaforum* 2019-4, p. 122*ff*. [in Dutch] (Gijrath 2019).

involving prejudicial queries to the highest EU Court.[58] The first criterion dictates that there is a "*transmission of signals*". The first criterion is broken down into three sub-elements. These elements require that the service: (a) "(...) *consists wholly or mainly* (...)" of the transmission of signals and (b) that the transmission occurs [generally] "(...) *via electronic communication, including telecommunications services and transmission services* (...)," and (c) that the provider "*is liable*" for the signal transmission that enables the end-user to purchase the service.[59] The second criterion requires an assessment as to whether the service is "*usually offered for remuneration.*" This criterion originates from the EU Electronic Commerce Directive. The term "usual" suggests that payment for the service is the norm, but that it is not decisive. The practice on digital platforms that offer free services is different. In any event, the compensation does not require a cash payment; as such the provision of data by the end-user could fall under the term. The third criterion mentioned in the definition is the "*internet access service"*. This definition is included in art. 2, para. 2 of the Open Internet Regulation (OIV) under the definition of Internet access service : "(…) *a public telecommunications service which provides access to the Internet and therefore connectivity to virtually all endpoints of the Internet, regardless of the network technology and terminal equipment*."[60] The EECC contains definitions on the prior unregulated Internet Protocol (IP) technology. The Commission reasons that nature of IP-based services is bidirectional – enabling both parties to communicate – and, consequently, similar to traditional communication and it that sense, it could have an impact on SDN. Again, it all depends on the services scope, which must be determined on case-by-

---

[58] CJEU 5 June 2019, ECLI: EU: C: 2019: 460 (*Skype / Commission*) and CJEU 13 June 2019, ECLI:EU:C:2019: 498 (*Google / Commission*).

[59] CJEU 7 November 2013 ECLI: EU: C: 2013: 709 (*UPC / Hilversum*), CJEU 30 April 2014 ECLI: EU: C: 2014: 285 (*UPC / DTH).*

[60] Emphasis added. Regulation 2015/2120/EU of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on Universal Service and Users' Rights relating to electronic communications networks and services and regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union, [2015] OJ L 310/1 (Open Internet Regulation "OIR", also known as the Net Neutrality Regulation.

case manner.[61] As with the first element sub (c), it is relevant whether the provider is "*liable*" for the service provided to the end-user.

The qualification as an internet access service provider (IAP) will impact the IAP's offer even though they do not otherwise qualify as an ECS or an ECN. The EECC defines a new category of service providers, aimed at bringing parties who do not operate an ECN into the definition of ECS. The new definition of interpersonal communications services could be used to support disruptive models offered by parties who offer packet switched data services only into the fray of the EECC.[62]

The Skype and Gmail judgments demonstrate that the technical parameters of the SDN are decisive for the scope of regulation. In both the Skype and the Google case, the transmission of signals appears to have been the prevailing element. The Court also had an eye for assessing the network topology and innovative software services. The Skype decision supports symmetrical regulation in the extended definition of ECS.[63] Conditions for the provision of a service must be separated from the actual definitional elements of a voice communications service. In terms of SDN/ NFV, it seems that the default is that a party supplying predominantly software is probably not going to fall under the definition of an ECS as there is no transmission of signals by the SDN. There may be overlap in standard software services and SDN that could be defined as ECS. Examples could be services involving an automated data transfer between devices or software-based applications with limited or no human interaction. This, clearly is a service scope that points at an ECS. Furthermore, where the SDN provider enters into a direct agreement with its end-users and where it can be considered to be liable for the functioning of the SDN elements on an ECN, then perhaps the outcome falls the other way. Another

---

[61] EECC, consideration (44), these "*do not benefit from the use of public numbering resources and do not participate in a publicly assured interoperable ecosystem*." Hence, if the SDN services qualifies as a number-independent interpersonal communications services, then it is exempted.

[62] Art. 2 para. (5) which introduces a new notion in the term, which provides that: *"'interpersonal communications service' means a service normally provided for remuneration that enables direct interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons, whereby the persons initiating or participating in the communication determine its recipient(s) and does not include services which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service*;"

[63] *Supra*, para. I sub 2.

possible qualification as an ECS is where the SDN provider also is an IAP. Having read through the EECC – in particular its considerations – it seems that the Commission wants to keep all options open and leave the qualification to the market: the SDN supplier needs to negotiate with the ECN or ECS provider.

In principle, an SDN provider who wants access to specific network elements to enable service provision could benefit from the ECS provider stamp to invoke, e.g., a right: (1) of access to network elements,[64] or (2) to engage in a (passive) infrastructure sharing arrangement with an ECN operator.[65]

The EECC may want to keep its options open for Member States to introduce more symmetrical regulation. Until then, pure software providers are likely to be exempt from regulation under the EECC.

1.2 Access rights to electronic communications networks

In terms of SDN, the Commission's starting point for access is that mandating access to network infrastructure can be justified as a means of increasing competition, provided that NRA's need to balance the rights of an ECN operator to exploit its infrastructure for its own benefit with the rights of other service providers to access facilities that are essential for the provision of competing services. In this context, the goal of promoting interoperability as mentioned in art. 61 (1) EECC emerges.[66]

The answer to the question whether operators or service providers who want to use an ECN virtually have an access right to the ECN cannot be found in the broadened scope of the definition of access in the EECC. 'Access' is redefined in art. 2 (27) EECC. Besides access to physical infrastructure, new network elements such as SDN are relevant.[67] The definition includes access to "*relevant software*

[64] EECC, consideration (105) refers to Competent authorities being able to impose the sharing of network elements and associated facilities. The consideration mentions ducts, conduits, masts, manholes, cabinets, antennae, towers and other supporting constructions, buildings or entries into buildings, and a better coordination of civil works on environmental or other public policy grounds.

[65] *Infra*, para. III-2.

[66] Art. 61.1 EECC refers to Consideration (189).

[67] Access to physical infrastructure on the basis of Directive 2014/61/EU.

systems."[68] It suggests that ECN operators should have access to the software systems. Does this perhaps intend to mean the reverse as well? Should an SDN have access to ECN by law, even where its service portfolio does not contain elements of an ECS? Where an NRA imposes obligations on providers requiring them to meet reasonable requests for access to and use of networks elements and associated facilities, these requests should be refused only on the basis of objective criteria. Possible criteria could be technical feasibility or the need to maintain network integrity. A company with mandated access obligations cannot be required to provide types of access which it is not within its power to provide, according to the EECC.[69]

The imposition by NRA's of mandated access that increases competition in the short term should not reduce incentives for competitors to invest in alternative facilities that will secure more sustainable competition or higher performance and end-user benefits in the long term. NRA's should be able to impose technical and operational conditions on the provider or beneficiaries of mandated access in accordance with EU.[70] In any event, the considerations of the EECC stipulate that the provisions should provide access for competing virtual operators who wish to employ SDN/NFV as well as obtaining access to an ECN. If the operator would have to grant access to its ECN, then access to its software elements could be included. How this works in practice depends on the scope of the software architecture.

A manner to deal with this is where the competent authorities in the Member States have the freedom to attach conditions on individual rights of use for radio

[68] Art. 2, para. (27) defines Access as: "(…) *the making available of facilities or services to another undertaking, under defined conditions, either on an exclusive or a non-exclusive basis, for the purpose of providing electronic communications services, including when they are used for the delivery of information society services or broadcast content services; it covers, inter alia: access to network elements and associated facilities, which may involve the connection of equipment, by fixed or non- fixed means (in particular this includes access to the local loop and to facilities and services necessary to provide services over the local loop); access to physical infrastructure including buildings, ducts and masts; access to relevant software systems including operational support systems; access to information systems or databases for pre-ordering, provisioning, ordering, maintaining and repair requests, and billing; access to number translation or systems offering equivalent functionality; access to fixed and mobile networks, in particular for roaming; access to conditional access systems for digital television services and access to virtual network services.*" [emphasis added].

[69] EECC Consideration (191).

[70] See, in particular, Directive (EU) 2015/1535.

spectrum and they could include obligations to allow SDN providers.[71] Generic or more specific innovation obligations could be part of the terms of the frequency license. Thus, the use of SDN or NFV could be imposed as part thereof. EU regulation of frequency allocation procedures entails that the Member States must describe their innovation goals in a clear manner in the allocation instrument; where possible, the responsible Minister or (other) regulatory authority must calculate in advance the cost of such measures both at the national and the EU level.[72] The same applies to infrastructure sharing agreements.[73] Competent authorities may impose such obligations only where this possibility is clearly provided for when granting the rights of use for radio spectrum and where justified on the grounds that, in the area subject to such obligations, the market-driven deployment of infrastructure for the provision of networks or services which rely on the use of radio spectrum is subject to insurmountable economic or physical obstacles and therefore access to networks or services by end-users is severely deficient or absent.

No matter the concreteness of the Commission's policy objectives in terms of promoting infrastructure innovation to stimulate the economy, the regulatory climate requires a careful weighting of the factors that are influenced by industry specific features, firm behaviour and regulatory incentives. Because prices are often determined after the investments have been made, the EU regulator's desire to maintain and create further regulation that contains provisions imposing SDN/NFV access obligations on ECN operators could create a conflict with its desire to stimulate innovative investments.[74]

This begs the question whether the EECC brings regulation that could be onerous on the ECN operators or on SDN providers. Does the Commission have enough confidence in the workings of the free market to allow for long-term economically viable contracts between ECN operators and SDN providers? For the time being the

---

[71] *Cf.* Art. 15 (2) (a): the right to negotiate access and art. 47 EECC.

[72] See also TSM Proposal, art. 54, second para. sub (d).

[73] *Infra*, para. III.2.

[74] Arve, M., Zwart, G. 'Optimal Procurement and Investment in New Technologies under Uncertainty', *TILEC Discussion Paper*, DP 2014-028 (Arve, Zwart 2014); Brito, D., Pereira, P., Vareda, J., 'Can Two-Part Tariffs Promote Efficient Investment on Next Generation Networks?' Mimeo 2008 (Brito, D., Pereira, P. , Vareda, J., 2008); Granieri, M., Renda, A., 2012.

regulatory focus remains on access regulation on the ECN; not on the ECN purchasing SDN/NFV features maintenance provision. The EECC is not concerned with the need to have clear and enforceable contracts for the viability of SDN deployment. The reason for the focus on generic access rights, rather than on (access to) detailed network elements, is that the regulation still aims predominantly at restricting anti-competitive behaviour. A recent example can be found in the Netherlands, where the Dutch NRA found that the roll-out of new glass-fibre networks was suffering significant delays. The NRA investigated these solely where it involved fibre-to-the-home (FttH).[75] ACM described that competition between market parties in the outlying areas resulted in an accelerated roll-out of fibre optics, but that in urban areas and the immediately adjacent neighbouring areas there was a delay or reduction in fibre roll-out.

2. Asymmetry in network elements sharing by ECNs & MVNOs?

Under the *ex-ante* approach to EU electronic communications market regulation, markets are defined *a priori* to facilitate the process of determining significant market power (SMP). Ex ante regulation focuses on the ECN not the SDN provider. Hence, this paragraph focuses on the perspective of the ECN. The underpinning of SMP regulation is to evaluate what would be the cost for a new entrant to build an alternative network to be able to supply similar services.[76] Unlike fixed networks, *ex ante* market regulation of mobile ECN operators is not very probable.[77] This is due to the circumstance that (most) mobile players are not considered easily to have SMP (a past exception being the market for mobile terminating tariffs). Consequently, there is a rather weak legal basis for regulatory intervention in 5G and SDN network rollout on mobile-only networks.

---

[75] ACM, Market study into the roll-out of fiber optic networks in the Netherlands (FttH market study), 21 October 2019 (ACM 2019).

[76] Hauge, J.A., Sappington, D.E.M., 'Pricing in Network Industries', in: R. Baldwin, M. Cave, M. Lodge (eds.), *Oxford Handbook of Regulation*, Oxford 2010 (Hauge, J.A., Sappington, D.E.M., 2010), p. 462-499.

[77] Gruber, H., Koutroumpis, P., 'Competition enhancing regulation and diffusion of innovation: the case of broadband networks', *Journal of Regulatory Economics*, Vol. 43, issue 2, 2013, p. 168-195 (Gruber, Koutroumpis 2012), p.2.

What are the alternatives for mobile ECN operators who wish to be subjected as little as possible to access regulation and who are open to SDN? An option could be infrastructure sharing.[78] It should be borne in mind that infrastructure arrangements are more common in the (less-regulated) mobile ECN and ECS markets. Roughly speaking, we can distinguish between different models, such as passive, active infrastructure sharing or spectrum sharing.[79]

A first option is passive sharing of infrastructure elements: masts, sites, cabinets, racks, power or conditioning; also known as site sharing, this is the lightest (and from a competition law perspective least worrisome) form of cooperation. *Prima facie*, there appears to be less incentive for mobile operators to enter into sharing agreements with new entrants, OTTs and even direct competitors, voluntarily. Besides, the party gaining access to existing network elements of the other party is unlikely to get access to the competitive facilities of that party. Hence, it is not included in art. 47 EECC.

A second option of infrastructure sharing includes active sharing of antennae, nodes, and, possibly the RAN. This form of cooperation may include sharing of the backhaul that goes to the different Radio Network Controls (RNC). The implementation of SDN/NFV will make this approach feasible and sustainable for competitors who wish to share. In fact, SDN could imply that traditional hardware suppliers will come to the fore and be an important partner in such arrangements. Hence this form of cooperation approach can vary even more than with passive sharing, but it can also be expected to raise more concerns with (national) competition authorities. These authorities are likely to require strong Chinese walls between the core network and the shared elements. The option of spectrum sharing does not, *prima facie*, lends itself to cooperation between ECNs and SDN providers.

Network fragmentation brings various options for network element sharing and software driven infrastructure comes into sight. Some of the proposed measures are built on the expectation that 5G roll-out and the implementation of SDN and NFV

[78] Art. 47 para. 2 sub (a) EECC.

[79] Gijrath 2018-3; BEREC/RSPG (2011), 'Infrastructure and spectrum sharing in mobile wireless networks', *RSPG11-374* final, 2011; Art. 47 para. 2 sub (c) also considers joint roll-out agreements.

shall result in several, sometimes multilateral, agreements. An ECN operator could enter into various co-sourcing agreements. Such agreements could involve direct competitors or new entrants, or the network equipment and/or SDN providers. Thus, the mobile ECN providers and their counterpart need to revaluate their agreements.

Art. 61 (4) EECC prescribes the Member States to ensure that competent authorities have the power to impose on undertakings providing or authorised to provide ECN obligations in relation to the sharing of passive infrastructure or obligations to conclude localised roaming access agreements, in both cases if directly necessary for the local provision of services which rely on the use of radio spectrum, in accordance with EU law. This obligation is applicable where there are no viable and similar alternative means of access to end-users on fair and reasonable terms and conditions. In those circumstances where access and sharing of passive infrastructure alone does not suffice to address the situation, national regulatory authorities may impose obligations on sharing of active infrastructure.

There is not yet enough data available on the long-term economic and legal advantages of these types of arrangements involving SDN. The arrangements could well lead to competition law concerns at a different level, and, most certainly raise a host of issues between the parties regarding the division and exploitation of intellectual property rights in new products. It would be best to see this form of cooperation more as a business and organization offer and deal with it as such in the contract terms; this is likely to make the arrangements more workable and more sustainable.

Having established this, it is likely that sharing arrangements can offer the parties more flexibility and freedom in creating opportunities for both incremental and fundamental infrastructure investments. ECN operators who will prepare for their networks or infrastructure to be shared with others are likely to be the first to reap the benefits of these arrangements. They can make a head start when it comes to crossing borders in light of the use of SDN. Even in the blockchain era, contracting to fend-off intervention is likely very much alive. In sum, it should be further investigated what types of passive infrastructure sharing arrangements can be used with SDN/NFV. Since the NRAs are supposed to be independent agencies from the issuing ministry, the question is why the Commission leaves the stimulation of

innovation for mobile networks to the national governments. In all likelihood, the reason is instrumental: only a national government is competent to issue specific regulations together with the rules for frequency allocation and subsequent licenses.[80]

In the coming years, the NRAs are expected to supervise the cooperation between ECN operators in the mobile and the fixed infrastructure markets. The NRAs are likely to be asked to determine their position on SDN and NFV, with a clear view of how these network software applications impact network topology and influence infrastructure competition. Broadband access will be an important building block at the wholesale level for providing internet access to end-users.

Imposing and enforcing detailed technological interoperability standards is not an easy task. Administrative courts that will rule on (often contractual) conflicts relating to measures imposed by a supervisory body will have an even more extensive duty to investigate the case and its circumstances and motivate their rulings. Moreover, the duty to investigate crosses borders: supervisory bodies must consider convergent conditions for the entire EU. Yet, there is no clear coordinating role for BEREC. Besides, what would be the remedy imposed by the NRA – termination of the licence appears to be disproportionate. In my research I did not find empirical analysis of the effects of combining innovations obligations in the frequency licence with either penalties under the licence or administrative penalties, if the licence holder would fail to satisfy the innovation obligation. In sum, sharing arrangements between ECN operators and SDN providers is left to the parties for now; but is not a done deal.

4. **The allocation of responsibility for network and information security**

[80] An example of imposing innovation through the process of allocating a frequency license occurred in the Netherlands in 2011 and again in 2017. The Minister in charge of the allocation and renewal of licenses for commercial radio frequencies required the licence holders to safeguard that digital radio reception (DAB+) would become available throughout the Netherlands. The Minister wanted the licence holders to invest in digital radio, in addition to their continued analogue wireless broadcast. However, this approach also had a downside, which the Minister did not investigate *a priori*. The digitization requirement could serve as an unassailable hurdle for new entrants to a very competitive market with an atypical business model. Commercial radio stations generate nearly all their income through advertising deals.

The Commission attaches great importance to network security, albeit that the regulatory focus remains on incident notification.[81] A 5G network infrastructure which employs SDN/NFV will be more open and programmable, new regulatory challenges to security issues arise. SDN and NFV in particular raise concerns on the security of the communication between the control and data planes, and the security and isolation of dedicated network slicing. With digitisation and connectivity becoming core features of an ECN an extremely high number of connected digital devices are expected to be deployed during the next decade. The Commission is convinced that the increased digitisation and connectivity increase cybersecurity risks. This affects society at large. Where an increasing number of devices is connected to the internet, the Commission also has serious doubts as regards the security and resilience of networks. Probably for this reason, the Commission attaches great importance to certification which enables users to obtain sufficient information about the cybersecurity features of ECN's and the ECS.[82]

The question in this paragraph is whether tailored SDN security regulation is required, and, if it is, will it be sustainable? This question requires answers to two preliminary questions: (1) to what extent do perceived network and information security threats fit in existing regulation? and (2) could SDN providers fall under the definition of network security and services under the EECC even if they are not an ECS?

First, what is regulated already in terms of network and information security and how does it fit in? In the Commission's view, the implementation of SDN/NFV arrangements could increase network and information security threats. A survey of security in SDN produced the following risks: (i) unauthorized access, when multiple controllers may access the "data plane of the network"; (ii) "data leakage", (iii) undesirable data modification when the controller is hijacked; (iv) integration of "malicious or compromised applications;" (v) DoS issues; (vi) configuration issues;

---

[81] Art. 2 (21) EECC defines security of networks and services as: '*the ability of electronic communications networks and services to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of those networks and services, of stored or transmitted or processed data, or of the related services offered by, or accessible via, those electronic communications networks or services;*'

[82] Cybersecurity Act 2019, Recitals.

(vii) “system level SDN security.” These findings are not unknown or untested risks. Nevertheless, given the specific functions of SDN/NFV, the authors of the survey on security of SDN consider the warranting network security to be a daunting challenge for regulators.[83]

The starting point for considering specific SDN regulation, in the EECC or other relevant regulation, is for the Commission to determine whether there is (appears to be) a regulatory gap in terms of warranting network security when SDN/NFV is implemented. Although they do not address SDN directly, the Cybersecurity Act, the NIS Directive and the GDPR contain a few high-level material provisions which may be relevant to regulating SDN operators and their suppliers. The notion of ‘*security of network and information systems*’ has remained essentially unchanged since the definition of ‘network and information security’ (NIS), in the first NIS Directive Proposal in 2001.[84] As can be seen in conjunction with para. 1, the only difference is that the definition now covers processed data as well.[85]

A proposal for a new Cybersecurity Act was launched in 2017.[86] SDN was not addressed as such, and software was relegated to being mentioned only in Recital 34. The new Cybersecurity Act 2019 is unlikely to apply to specific SDN and NFV security issues. The Cybersecurity Act is institutional not material regulation.

---

[83] Scott-Hayward, S. Natarjan, S. & Sezer, S., 2016, p. 8.

[84] Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, Network and Information Security: Proposal for A European Policy Approach, COM(2001) 298 final, Chapter 2.

[85] According to the GDPR in its Art. 4(2): “‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;”

[86] Proposal for a regulation of the European Parliament and of the council on ENISA, the "EU cybersecurity agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act").

That brings us to GDPR.[87] Neither the GDPR nor the proposal for an e-Privacy Regulation[88] contains a definition for 'security'. Art. para. 2 of the NIS Directive contains a definition of 'security': "(2) '*security of network and information systems' means the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems*;" However, the NIS Directive is aimed at the Member States and not directly at SDN operators.

Both the EECC and Recital 2a of the draft e-Privacy Regulation clarify that the GDPR applies next to the EECC and the e-Privacy Regulation. The GDPR does not deal with software, but with personal data. The generic norm for secure data processing is laid down in art. 32, para. 1 GDPR.[89] It will apply directly both to the traditional mobile ECN operators and to the providers of the software for the SDN, who may be considered processors.[90] That is not surprising. Examples of protection measures given by art. 32 GDPR are: (i) (a) the pseudonymisation and encryption of personal data; (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (iii) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

---

[87] Regulation (EU) 2016/679 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, OJ L 119/1, 4 May 2016, General Data Protection Regulation, enters into force on 25 May 2018.

[88] By November 2019, the e-Privacy Regulation was still under discussion. See Proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC, revised Brussels 5 December 2017, 2017/0003 (COD) and amended versions.

[89] Art. 32, para. 1 GDPR provides: "*Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk*."

[90] Art. 28 GDPR.

If and once the e-Privacy Regulation enters into force, it should be analysed whether there may be a case for arguing that the new Regulation covers measures to be taken to protect ECN. The scope may be rather generic, the obligations attached to being a party placing 'software permitting electronic communications' on the market, are even more. Art. 8(1) sub (e) e-Privacy Regulation allows these providers to install security updates in the systems, provided that these do not modify end-users' privacy settings.

This brings us to the second question: could SDN providers fall under the definition of network security and services under the EECC even if they are not an ECS? The starting point seems to be the converse, where art. 40 places the onus on the public ECN operator or ECS provider – where it was established above that these do not, necessarily apply to SDN providers.[91] Recital (50) of the NIS Directive states the following: "*Operators of essential services and digital service providers should ensure the security of the network and information systems which they use.*" ECN operators do not qualify as such. Bear in mind that ECN operators are regulated predominantly in the EECC even though the NIS Directive applies to them as well.

It is unclear how the suppliers of SDN and NFV will be looked at under the new EECC and Cybersecurity Act. As with ECN operators, these suppliers are not considered essential services or digital services providers under the NIS Directive. In addition, software suppliers are excluded from the scope of the NIS Directive.

Thus, when comparing mandatory measures with the risks perceived and solutions suggested by SDN experts, it is likely that SDN and NVF providers may warrant specific consideration. The Commission should investigate whether and how these measures will enhance SDN and NVF security. It is probably up to the Commission to come up with a patch in the NIS Directive or to devise another regulatory instrument specifically aimed at SDN security.

---

[91] Art. 40 EECC directs the Member States to ensure that providers of public ECN or of publicly available ECS: "*take appropriate and proportionate technical and organisational measures to appropriately manage the risks posed to the security of networks and services. Having regard to the state of the art, those measures shall ensure a level of security appropriate to the risk presented. In particular, measures, including encryption where appropriate, shall be taken to prevent and minimise the impact of security incidents on users and on other networks and services*."

Finally, a word on notification. The EECC extends the notification provision regards to threats.[92] Unfortunately, none of the instruments provide a definition of "significant" or threshold values to determine it. Implementing acts sometimes supplement primary legislation such as Art. 4.1 of Regulation 2018/151[93] concerning Art. 16 of the NIS Directive regarding when an incident shall be considered as having a substantial impact.[94]

IV. Final Remarks

It is likely that SDN/NFV will bring electronic communications network and services innovation. The deployment of SDN/NFV can stimulate economic growth. The EECC does not intervene in the provision of SDN/NFV. Nor does the Commission cater for either stimulating or facilitating SDN as a tool for network and services innovation.

This Article focused first on the question how SDN/NFV fit under the new EECC. It was established that it is not entirely excluded that SDN/NFV providers could fall under the scope of the EECC. However, this depends on the qualification of SDN/NFV under the EECC. The ramifications of access regulation on ECN operators were also discussed in the context of SDN. It is uncertain whether threats of regulation will bring competitors to agree a form of co-sharing infrastructure with SDN providers voluntarily. Although NRAs must consider technological innovation in market analysis, it is by no means clear whether such an exercise will enhance innovation through SDN. This approach still clashes with the market parties' desire

[92] Member States shall ensure that in case of a particular and significant threat of a security incident in public communications networks or publicly available electronic communications services, providers of such networks or services shall inform their users potentially affected by such a threat of any possible protective measures or remedies which can be taken by the users. Where appropriate, providers should inform their users also of the threat itself (Art 40(3) EECC).

[93] Which is a *lex specialis* to the NIS Directive.

[94] An incident shall be considered as having a substantial impact where at least one of the following situations has taken place: (a) the service provided by a digital service provider was unavailable for more than 5M user-hours whereby the term user-hour refers to the number of affected users in the Union for a duration of 60 minutes; (b) the incident has resulted in a loss of integrity, authenticity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via a network and information system of the digital service provider affecting more than 100.000 users in the EU; (c) the incident has created a risk to public safety, public security or of loss of life; (d) the incident has caused material damage to at least one user in the Union where the damage caused to that user exceeds EUR 1.000.000.

for deregulation, as was evident from the BEREC 2016 Input Paper and the 2017 DG Connect Study. Perhaps a more holistic approach – with incentives for parties willing to innovate through co-sourcing SDN – is more effective than including SDN deployment obligations in frequency licences.

Second, just as with infrastructure sharing, co-sourcing, using SDN can take very different forms, going as far as parties agreeing on joint ownership of certain network elements that can serve to balance their needs, while also sharing financial risks that will occur during the period of investment. In the event of a form of joint ownership of infrastructure elements, this should affect the level playing field positively, as the parties will truly share the risks of the innovative investments on an *ex ante* basis. Such arrangements are likely to be agreed once the new frequencies have been allocated. This entails that the party controlling the infrastructure will have to give up some of its first-mover advantage for the benefit of the party entering the sharing arrangement.

A third issue was: who pays the bill for preserving network and information security (NIS)? Catering for NIS become more complex when multiple suppliers, providers and operators cooperate in SDN arrangements. The EU regulation governing network security is inconveniently high-level to cater for security concerns. Conversely, this means that the parties are free to determine both the scope and cost of security measures. Besides, it could be argued there is more contractual freedom in the network control elements of SDN if the services are implemented at a network level that does involve the processing of personal data. Much will depend on how the SDN/NFV fit within the OSI model.

Contractual arrangements regarding the onus of liability may be scrutinized by NRA's or courts, when there is a serious breach of security. This means that disclaimers could risk being set aside.

Another issue is how the regulator can ensure that governance structures for SDN/NFV and network and information security are in place. What is needed to make a governance structure efficient? There must be fair and transparent process for decision making, for instance, on incentive regulation. The EECC aims at coordinating the diverse practices for network innovation in the Member States by standardising the conditions for frequency allocation in the Member States. But

there is no political consensus in the EU on the coordination of 5G allocation and considerations on SDN and NFV opportunities are not on the table.[95]

All things considered, redefining SDN is needed before any policy objective can be applied to its advent. Additionally, the policy objectives are very high-level. This is good in that it could lead to more sustainable regulation – with the focus remaining on preventing market distortions. There is not a strong case for proposing innovation measures to stimulate the take-off of SDN and NFV, but there may be some onus on the ECN operator unwilling to grant SDN suppliers a podium. The focus could perhaps be on self-regulation through co-sourcing arrangements. That could promote legal certainty for parties wishing to deploy SDN/NFV. Finally, generic regulation of network and information security is likely to extend to SDN to some extent, but the question who will pay for that is probably a matter of commercial discussions.

[95] ECJ, Case C-687/15 on the competencies with regard to the ITU spectrum policy, 25 October 2017, ECLI:EU:C:2017:803 (*Commission/Council*).