Commission Delegated Regulation (EU) 2022/30 Supplementing Directive 2014/53/EU on Radio Equipment: Strengthening Cybersecurity, Privacy and Personal Data Protection of Wireless Devices

*Pier Giorgio Chiara**

I. Introduction

Since consumer products are increasingly connected to the internet (the number is estimated to rise to 7.43 billion in the EU by 2030), concerns are arising as to whether these devices – including machines, sensors and networks that make up the Internet of Things (IoT) – are sufficiently secure to ensure that users' personal data and networks are protected, their privacy respected, and frauds avoided.[1] The Commission started in 2019 a public consultation to address the issue in a holistic manner, by taking into account the possible impacts for society (eg. consumers and economic operators) and the effectiveness of national authorities, the common market access conditions and the implementation of, or synergies with, additional pieces of EU legislation, in particular those relating to (cyber)security, data protection and privacy.[2]

Directive 2014/53/EU on radio equipment (RED) establishes a regulatory framework for the making available of radio equipment on the EU single market.[3] The RED aligned the previous Directive, the Radio and telecommunication terminal equipment Directive (1999/5/EC) with the New Legislative Framework principles[4] for the marketing of products and for improved market surveillance.[5] The Directive defines 'radio equipment' as an "electrical or electronic product, which intentionally emits and/or receives radio waves for the purpose of radio communication"[6].

Article 3 lays down the 'essential requirements' radio equipment shall comply with.[7] Pursuant to Article 3(1) RED radio equipment shall be constructed so as to ensure on the one hand the protection of health and safety of persons, domestic animals and property (letter 'a') and, on the other hand, an adequate level of electromagnetic compatibility as set out in Directive 2014/30/EU (letter 'b'). Further, Article 3(2) RED mandates that radio equipment shall both effectively use and support the efficient use of radio spectrum in order to avoid harmful interference.

DOI: 10.21552/edpl/2022/1/15

* The author is a PhD Candidate in the programme 'Law, Science and Technology, Rights of Internet of Everything' at the University of Luxembourg, University of Bologna and University of Turin, <https://last-jd-rioe.eu/pier-giorgio-chiara.html>. For correspondence <piergiorgio.chiara@uni.lu>. This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie ITN EJD "Law, Science and Technology Rights of Internet of Everything" grant agreement No 814177.

1 Chiara Giovanni and Frederico Silva, 'Cybersecurity for Connected Products - ANEC BEUC Position Paper' (2018) 4; OECD, 'Consumer Product Safety in the Internet of Things' (2018) 267 OECD Digital Economy Papers, 18 and ff.

2 European Commission, 'Commission Staff Working Document Imapct Assessment Report Accompanying the Document Commission Delegated Regulation Supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive' (2021) Annex II, 62 <https://ec.europa.eu/growth/system/files/2021-10/SWD%282021%29 302_EN_impact_assessment_part1_v3.pdf>.

3 RED, Article 1(1).

4 The 'New Legislative Framework' (NLF) updated the foundational principles of the 'New Approach' (dating back to the 80s) vis-à-vis the EU model of governance of product safety. The NLF consists of Regulation (EC) 765/2008 setting out the requirements for accreditation and the market surveillance of products; Decision 768/2008 on a common framework for the marketing of products, which includes reference provisions to be incorporated whenever product legislation is revised; and Regulation (EU) 2019/1020 on market surveillance and compliance of products.

5 In particular, the 'EU declaration of conformity' (RED, Annex IV), issued by the manufacturer, introduces a traceability system based on the identification of radio equipment in order to facilitate national market surveillance authorities' task of tracing economic operators (i.e., manufacturers, importers and distributors) who made non-compliant radio equipment available on the market (RED, recital 37).

6 Directive 2014/53/EU, Art 2(1).

7 Pursuant to Art 17(2) RED, manufacturers shall demonstrate compliance of radio equipment with the essential requirements set out in Article 3(1) using any of the following conformity assessment procedures: (a) internal production control set out in Annex II; (b) EU-type examination that is followed by the conformity to type based on internal production control set out in Annex III; (c) conformity based on full quality assurance set out in Annex IV.

Importantly, Article 44 empowers the Commission to adopt delegated acts to specify which categories or classes of radio equipment are concerned by each of the *additional* essential safety requirements laid down in Article 3(3). In order to address the problem of unsecure devices vis-à-vis different elements related to cybersecurity, such as network protection, safeguards for the protection of personal data and privacy, and protection from fraud, the Commission focused on three essential requirements, namely Article 3(3)(d) on network protection[8], Article 3(3)(e) on personal data protection and privacy[9] and Article 3(3)(f) on protection from fraud[10].

So-called 'smart' appliances of everyday use, like smart cameras, alarm systems and many other internet-connected radio equipment are devices at risk of hacking and of privacy and data protection issues when connected to the internet. Moreover, wearable radio equipment (eg. fitness trackers, headsets, etc.) collect, process and re-transmit a vast number of users' sensitive data over time (eg. position, temperature, blood pressure, heart rate), not only over the internet, but also through insecure short range communication technologies.[11]

Against this backdrop, the question is ultimately which classes or categories of internet-connected radio equipment are concerned by the requirements set out in Article 3(3)(d), (e) and (f) RED, regardless of whether they communicate over the internet *directly* through a wireless network (such as Wi-fi) or router, or *indirectly* through a Bluetooth connection or via a link between an IoT device and a mobile phone application.

This contribution highlights how the Delegated Regulation (EU) 2022/30 activating the essential requirements of Article 3(3)(d), (e) and (f) RED will enhance and complement existing cybersecurity and privacy and data protection EU legal frameworks while strengthening the (cyber)security of wireless devices.

II. EU Commission Delegated Act activating RED Article 3(3)(d), (e) and (f)

The Commission adopted the Delegated Regulation (EU) 2022/30 on 29 October 2021[12]. As mentioned above, the objective of the Delegated Act is to specify to which categories or classes of radio equipment the essential requirements set out in Article 3(3)(d), (e) and (f) of the RED apply.

Article 1(1) of the Delegated Act concerns the 'network-preservation' requirement of Article 3(3)(d) RED. This essential requirement "shall apply to any radio equipment that can communicate itself over the internet, whether it communicates directly or via any other equipment ('internet-connected radio equipment')"[13].

Conversely, the 'privacy & data protection' essential requirement of Article 3(3)(e) RED is applicable also to radio equipment, capable of processing[14] personal data[15] and traffic[16] and location[17] data, which is generally internet-connected (Article 1(2)(a) Delegated Act); designed or intended exclusively for childcare (Article 1(2)(b) Delegated Act); radio equipment covered by Directive 2009/48/EC, that is, on the safety of toys (Article 1(2)(c) Delegated Act); and radio equipment designed or intended, whether exclusively or not exclusively, to be worn on, strapped to, or hung from (i) any part of the human body, and (ii) any clothing which is worn by human beings (Article 1(2)(d)). In particular, the inclusion of 'connected toys' is well substantiated, as the *Cayla* doll case[18] showed that national Market Surveillance Authori-

8 Art 3(3)(d) RED mandates that radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service.

9 Art 3(3)(e) RED prescribes that radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected.

10 Art 3(3)(f) RED requires that radio equipment supports certain features ensuring protection from fraud.

11 European Commission, 'Explanatory Memorandum to the Commission Delegated Regulation 2022/30 of 29.10.2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive' C(2021) 7672 final, 2.

12 Commission Delegated Regulation (EU) 2022/30 of 29.10.2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive.

13 RED Delegated Act, Art 1(1).

14 As defined in Art 4(2) GDPR.

15 As defined in Art 4(1) GDPR.

16 As defined in Art 2(b) ePrivacy Directive.

17 As defined in Art 2(c) ePrivacy Directive.

18 Steve Mansfield-Devine, 'Weaponising the Internet of Things' (2017) Network Security 13; Stefan Hessel, '"My friend Cayla" - eine nach § 90 TKG verbotene Sendeanlage?' (2017) 13 JurPC Web-Dok <https://www.jurpc.de/jurpc/show?id=20170013> accessed 15 February 2022.

ties[19] struggled to remove the product from the market, even though various security flaws and vulnerabilities had been exposed.[20]

Finally, Article 1(3) of the Delegated Regulation mandates that the essential requirement set out in Article 3(3)(f) RED shall apply to any internet-connected radio equipment, if that equipment enables the holder or user to transfer money, monetary value or virtual currency as defined in Article 2 (d) of Directive (EU) 2019/713[21].

Article 2(1) of the Delegated Act derogates from Article 1 by excluding from the scope of all the RED essential requirements under scrutiny medical and in-vitro devices, that is, Regulation (EU) 2017/745[22] and Regulation (EU) 2017/746[23] respectively. In addition, the essential requirements regarding the protection of privacy and personal data (Article 3(3)(e)) and protection against fraud (Article 3(3)(f)) shall not apply to radio equipment already covered by other Union legal acts. These are: Regulation (EU) 2019/2144 on safety requirements for motor vehicles[24]; Regulation (EU) 2018/1139 on common rules in the field of civil aviation[25]; and Directive (EU) 2019/520 on electronic road toll systems[26]. Accordingly, the cybersecurity requirement of Article 3(3)(d) against networks harm and misuse would still be applicable to these pieces of legislation.

The Delegated Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union and shall apply from 1 August 2024.[27]

III. The Relevance of the Delegated Regulation for the IoT market

The Delegated Regulation, which brings into the scope of Article 3(3) RED the majority of IoT devices[28], enhances and complements the existing EU legal framework in the field of cybersecurity, privacy and data protection. Yet, it serves as an example of the common EU approach towards these three areas , with cybersecurity being essential for upholding privacy and data protection.[29] Key definitions such as personal data, processing, location and traffic data are aligned with EU legislation already in place, that is, the GDPR and the e-Privacy Directive, thus ensuring coherence within the EU legal landscape.

A first important legal consequence of this convergence is that manufacturers of internet-connected and wearable radio equipment will have to design and develop devices taking into account baseline (cyber)security and data protection principles such as

19 Germany resorted to a longstanding legal act on espionage to remove the product on the market; See <https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2017/14012017_cayla.html?nn=690686> accessed 25 January 2022.

20 European Commission (n 2) 27.

21 Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA.

22 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.

23 Regulation (EU) 2017/746 on 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.

24 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.

25 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 3922/91.

26 Directive (EU) 2019/520 of the European Parliament and of the Council of 19 March 2019 on the interoperability of electronic road toll systems and facilitating cross-border exchange of information on the failure to pay road fees in the Union.

27 RED Delegated Act, Art 3.

28 Pier Giorgio Chiara, 'The IoT and the new EU cybersecurity regulatory landscape' (2022) 36 International Review of Law, Computers and Technology 2, forthcoming.

29 European Commission and the High Representatitve of the Union for Foreign Affairs and Security Policy, 'Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade' (2020) <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2020:18:FIN> accessed 7 February 2022, 4.

'security by design' and 'data protection by design'[30] as a pre-condition for market access: "arguably, a further benefit is that by making all manufacturers of internet-connected RE and wearable RE directly responsible for ensuring data protection and privacy (even if they do not intend to collect personal data themselves), it could overcome uncertainty within the value chain as regards how GDPR compliance applies to manufacturers, technology providers, and third-party service providers"[31].

A second legal challenge addressed in the impact assessment is the lack of obligations for manufacturers to consider security and data protection by design principles, if there is no intention to collect any personal data[32]. The risk to overlook GDPR's security considerations is exacerbated in a scenario where an internet-connected radio equipment, allegedly collecting, generating, or sharing non-personal data, processes personal data pursuant to the broad definition of Article 4(1) GDPR and the identifiability test of Recital 26[33], and relevant case-law[34]. Synergies will then be ensured between the product safety legislation perspective, which targets economic operators, with higher burdens on manufacturers regardless of any personal data processing, and the horizontal GDPR perspective, which lays out obligations on data controllers and processors.

It follows, therefore, that national competent authorities will be able to remove internet-connected radio equipment from the Single Market if they fail, *inter alia,* to provide safeguards to protect users' privacy and personal data protection. Moreover, this policy option favours the harmonisation of the Union market vis-à-vis the products under scrutiny, as it will be "unhampered by diverging local or national regulations that increase administrative burdens for smaller companies in particular"[35].

Conversely, Article 3(3)(d) RED tackles more explicitly 'cybersecurity' since internet-connected radio equipment will have to embed security measures or controls to avoid harm to the network or its functioning or misuse of network resources. Recital 9 of the Delegated Act further clarifies that the 'network security' requirement shall be interpreted broadly to cover the main cybersecurity threats[36], such as DDoS attacks. The rationale underpinning an 'absolutist' understanding of "harm to network" is to be found in the more complex, extensive and dynamic threat landscape – with 5G being a major driver of such expansion of threat vectors.[37] Therefore, Article 3(3)(d) RED would not only take into account the 'expected' use of the network by radio equipment but also the harmful consequences to the network arising from insufficient security, that is, insufficient authentication, against cyberattacks.[38] In other words, the Delegated Regulation would complement the network and information systems security framework established by the NIS Directive[39], ensuring that not only the networks *per se* are secure, but also that the connected radio equipment does not harm them.[40]

IV. Conclusive Remarks

In accordance with the 'New Legislative Approach' principles, the European Commission has issued a standardisation mandate to the European Standardisation Organisations (ESOs). ESOs will have to develop harmonised technical standards which might then be used by manufacturers to demonstrate compliance with the essential requirements under scrutiny. The 2022 'annual Union work programme for European standardisation' outlines as a deliverable the development and revision of European standards in

30 EDPB, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default' (2020) <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en> accessed 7 February 2022.

31 CSES, "Executive Summary - Impact Assessment on Increased Protection of Internet-Connected Radio Equipment and Wearable Radio Equipment" (2020) <https://ec.europa.eu/docsroom/documents/40763> accessed 7 February 2022, 5.

32 ibid 35.

33 Michèle Finck and Frank Pallas, 'They Who Must Not Be Identified — Distinguishing Personal from Non-Personal Data under the GDPR' (2020) 10 International Data Privacy Law 11, 11.

34 CJEU, Case C-582/14, Patrick Breyer v Bundesrepublik Deutschland [2016] ECLI:EU:C:2016:779; CJEU, Case C-434/16 Peter Nowak v Data Protection Commissioner [2017] ECLI:EU:C:2017:994.

35 European Commission (n 11) 3.

36 RED Delegated Act, recital 9: "an attacker may maliciously flood the internet network to prevent legitimate network traffic, disrupt the connections between two radio products, thus preventing access to a service, prevent a particular person from accessing a service".

37 ENISA, 'ENISA Threat Landscape for 5G Networks' (2019) <https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks> accessed 26 January 2022.

38 European Commission (n 2) 12–17.

39 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.

40 ibid 5.

support of cybersecurity requirements for wireless connected products under the RED.[41]

This action will avoid disproportionate actions since there are already existing solutions that can be adopted. As pointed out by the Commission, the GDPR "security by design" principle and payments security can already be addressed through specific standards. As regards networks security, "there is already a pool of best practices and standards that stem from the implementation of the NIS Directive which can be taken as a benchmark and mirrored, where appropriate, into the design of equipment"[42].

In the 2021 ENISA cybersecurity standardisation conference, relevant stakeholders stressed the need for "open" standardisation requests under the RED Delegated Act, that is, *performance-based* and *technology-neutral*. As a result, these standards may benefit the future horizontal legislation on cybersecurity for connected products[43], which has been mentioned in the new Cybersecurity Strategy of the Commission[44], preceded by the Council conclusions[45] and as called for by many industrial associations[46].

The strengthening of an 'ecosystem of trust', which stems from the synergies of all related pieces of EU law concerning protection of networks and privacy as well as directed against fraud, is the key objective underpinning this initiative.[47] Furthermore, the Delegated Act is expected to be complemented by a Cyber Resilience Act, recently announced by President von der Leyen in the State of the Union speech, which would aim to cover more products, looking at their whole life cycle.[48]

41 European Commission, 'Annex to the Commission Notice: The 2022 annual Union work programme for European standardisation' C(2022) 546 final, <https://ec.europa.eu/docsroom/documents/48601> accessed 8 February 2022, 33.

42 European Commission (n 2) 52–53.

43 Dieter Wegener, 'Proposal for a realistic way to implement a "Cybersecurity regulation in Europe"' (2021) ENISA Cybersecurity Standardization Conference, panel 1: Cybersecurity and Radio Equipment Directive – setting up the scene and future work, <https://www.enisa.europa.eu/events/cybersecurity_standardisation_2021/presentations/01-06-wegener> accessed 7 February 2022.

44 European Commission and the High Representatitve of the Union for Foreign Affairs and Security Policy (n 24) 9.

45 Council of the European Union, 'Council Conclusions on the cybersecurity of connected devices' (2020) 13629/20 <https://www.consilium.europa.eu/en/press/press-releases/2020/12/02/cybersecurity-of-connected-devices-council-adopts-conclusions/> accessed 26 January 2022, 4-6.

46 Orgalim, 'Proposal for a Horizontal Legislation on Cybersecurity for Networkable Products within the New Legislative Framework' (2020) <https://orgalim.eu/sites/default/files/attachment/Proposal for a horizontal legislation on cybersecurity for networkable products within the New Legislative Framework 091120 %28003%29.pdf> accessed 26 January 2022; BDI, DIN and DKE, 'EU-wide Cybersecurity Requirements - Introduction of horizontal cybersecurity requirements based on the New Legislative Framework and bridge to the EU Cybersecurity Act' (2021) <https://www.dke.de/resource/blob/2021296/f9708b36c89b2e527bcb1a66f523827a/position-eu-wide-cybersecurity-requirements---pdf-data.pdf> accessed 26 January 2022. See also Wavestone - CEPS - CARSA - ICF, 'Study on the Need of Cybersecurity Requirements for ICT Products - No. 2020-0715: Final Study Report' (2021) 256–257 <https://digital-strategy.ec.europa.eu/en/library/study-need-cybersecurity-requirements-ict-products> accessed 26 January 2022.

47 European Commission (n 2) 23.

48 European Commission, 'Commission strengthens cybersecurity of wireless devices and products' (2021) <https://ec.europa.eu/commission/presscorner/detail/en/IP_21_5634> accessed 7 February 2022.