Int. Cybersecur. Law Rev.
https://doi.org/10.1365/s43439-022-00064-9

Vulnerability management as compliance requirement in product security regulation—a game changer for producers' liability and consequential improvement of the level of security in the Internet of Things?

Roman Dickmann

Received: 20 July 2022 / Accepted: 16 August 2022

Abstract The article outlines the European Union (EU) regulation of information technology (IT) security in Internet of Things products from a consumer and end user perspective. It starts with civil law and the necessity to address security requirements and specifications in individual contractual terms. Data and consumer protection laws have not helped much, mainly because of missing definitions and levels of applicable security. Two new EU directives reforming the law of obligations may improve the situation for consumers since security is now a named quality requirement, especially for the sale of (digital) goods. Also introduced is the provision of security updates as a contractual duty. But both rule sets address only the traders, not the producers. This is different with the activation of clauses in the radio equipment directive, which sets IT security measures as requirements to be compliant for CE labeling. An important element is the introduction of a vulnerability management system. Details can be found in the draft of technical standard ETSI/EN 303645. The work concludes with a look at the EU's efforts regarding certification schemes and the interaction of all regulation elements, with more liability for insecure products plus the hope for effectiveness.

Keywords Vulnerability disclosure · Radio equipment · CE mark · Sale of goods with digital elements directive · Product safety

Roman Dickmann (✉)
https://www.radickmann.de
E-Mail: rd@radickmann.de

Published online: 16 September 2022

Schwachstellen-Management als Konformitätsanforderung im Produktsicherheitsrecht – Impulsgeber für schärfere Produkthaftung und ein resultierendes höheres Sicherheitsniveau im Internet der Dinge?

Zusammenfassung Der Artikel stellt die die Regulierung der Eropäischen Union (EU) im Bereich von Produkten des Internets der Dinge (Internet of Things, IoT) aus Sicht von Verbrauchern und Endnutzern dar. Eingangs wird die Notwendigkeit im Zivilrecht zu expliziten Abreden über Sicherheitsanforderungen und Spezifikationen herausgestellt. Daten- und Verbraucherschutzrecht haben insbesondere wegen fehlenden Definitionen und einem fehlenden Mindestsicherheitsniveau wenig zu mehr Klarheit beigetragen. Zwei neue EU-Richtlinien als Motor der (digitalen) Schuldrechtsreform könnten nun mit der Benennung von Sicherheit als Produktanforderung zu einer Verbesserung führen. Wesentlicher Faktor ist dabei die Einführung von Sicherheitsupdates als vertragliche Pflicht. Diese obliegt jedoch nur den Händlern und nicht den Herstellern. Adressiert werden Letztere jedoch durch die Aktivierung mehrerer Regelungen in der Funkanlagenrichtlinie. Mit dieser wird IT-Sicherheit zu einer Anforderung für das Anbringen des CE-Kennzeichens. Wesentliches Element ist dabei die Einführung eines Schwachstellen-Managements. Details dazu finden sich im Entwurf des technischen Standards ETSI/EN 303645. Abschließend wird ein Blick auf die EU-Regulierung der IT-Sicherheit mittels Zertifizierungsanforderungen und das Zusammenwirken der Einzelregelungen geworfen. Es ist durchaus mit einer schärferen Haftung für unsichere Produkte zu rechnen und auf die Effektivität der neuen Normen zu hoffen.

Schlüsselwörter Schwachstellenveröffentlichung · Funkanlagen · CE-Kennzeichen · Digitale-Inhalte-Richtlinie · Produktsicherheit

Wireless connections to other devices and the internet have become the norm, making cable an anachronistic anchor to a grounded infrastructure. Radio ports in almost every piece of portable equipment allow apparently boundless use. But as a downside, they also allow remote attacks and misuse. Missing or ineffective technical precautions and vulnerabilities, mainly in software, facilitate this possibility, resulting in a poor level of the interconnected world's security. The laws of the European Union (EU) and its member states may provide new impetus to change that.

1 Until recently, the only leverage: concessions or individual contractual terms

In civil law, the parties need to agree upon certain information technology (IT) security specifications for goods and services.[1] Those may be found (at least for

[1] Especially the Internet of Things: physical objects with embedded software to exchange data with other connected devices. For the legal context, see Bräutigam in Bräutigam and Kraul, *Internet of Things*, 2021, § 1, pp. 2.

serial products) in referenced technical standards or internal specifications from the producer. For products with wireless network connectivity, such provisions—for example, the radio transmission encryption protocols—are a bare minimum.[2] Certain features and/or a particular level of IT security are generally not required by law (other than mandates in harmonized fields for certain product categories).[3] So the term "secure" is in most cases not specific enough to allow a clear legal finding of a product fault, especially if not even defined.[4] Besides the security features to be implemented in hardware and software, there are external factors, such as cloud functions and preventive or loss-minimizing processes, that are not physically bound to the goods. An example is vulnerability management[5] as a process by the producer involving the supply and delivery chain. If the parties do not precisely list requirements with risk spheres and their boundaries, a complemental interpretation of unclear or incomplete contractual terms is a difficult task.[6]

With the ever-evolving digitalization fueled lately by the COVID-19 pandemic, IT security is not regarded as an option anymore but has been promoted to a core feature. A general definition of security is not to be found.[7] Rules for consumer protection actually intervene only sporadically with requirements for consent, information obligations, and secondary rights.[8] Article 32 of the General Data Protection Regulation (GDPR) requests technical and organizational measures to ensure a risk-appropriate level of security, and Article 25 of the GDPR calls for data protection by design and by default. These duties bind only the data controller and processor but not the producer of the used IT. Only personal data are naturally protected.[9] The harmonized product liability law derives from a time when the focus was on analog faults in operating and controlling or incorrect use. The according directive

[2] Such as WEP, WPA, WPA2, and WPA3; see Schäfers/Walde, *WLAN Hacking*, 2018, pp. 69. For vulnerabilities, see Forshaw, *Attacking Network Protocols*, 2018, pp. 207.

[3] For examples in German KRITIS sectors, see Hornung and Schallbruch, *IT-Sicherheitsrecht*, § 21, rec. 53 ff.; § 22, rec. 62 ff.; § 23, rec. 9 ff.; § 24, rec. 19 ff.

[4] This is so even though the main security flaws in software over the years have consistently been buffer overflows, weak authentication, unauthorized code execution or elevation of user privileges, weak or faulty implementation of encryption, and lack of encryption of data transfer and storage; see Howard et al., 24 Sins of Software, *Security*, 2009, pp. 89. With interconnection, special forms have been added; see Gebeshuber et al., *Exploit*, 2019, pp. 51, and for vulnerabilities in application programming interfaces, see Ully, *iX*, July 2022, p. 52.

[5] A process to deal internally or externally with vulnerabilities in hardware and software, from detection/notification, reception by prepared staff, evaluation of criticality with prioritizing and instant mitigation, investigation of the technical background and root cause, and communication with other parties involved, to the development/testing/rollout of patches and updates or other mitigation measures plus documentation, lessons learned, and improvement cycle.

[6] For example, via the legal concept of the "least/cheapest cost avoider," see Finkenauer in *MüKoBGB*, 9th edn. 2022, German Civil Code (BGB) § 313 rec. 69.

[7] And with its relative nature, it is hard to create. Compare, for example, Eckert, *IT-Sicherheit*, 10th edn. 2018, Chap. 1.2; Bundesamt für Sicherheit in der Informationstechnik (BSI), glossary keyword "Sicherheitsanforderung," https://www.bsi.bund.de; NIST, glossary term "information security" with cross references to different sources, https://csrc.nist.gov/glossary.

[8] For German law, see the rules on sales to consumers in §§ 474 ff. BGB with the timely limited shift of the burden of proof for a product fault at the time of transfer of perils.

[9] Hartung in Kühling and Buchner, *DS-GVO*, 3rd edn. 2020, Art. 25, rec. 12 f. with further references.

does not exclude the digital world completely, but data are not intrinsically property and therefore are only captured via storage or software control of hardware.[10] Comparison of the use of terms in different languages and technical terminologies brings up blurring definitions plus different understandings by legal practitioners, programmers, and engineers.[11] In Anglo-American countries there is a differentiation between "safety" and "security," while, for example, in Germany "Sicherheit" is the single combined term.[12] With the growing field of the Internet of Things (IoT), protection from potentially malicious misuse of hardware and software, along with the need to identify specific safety and security objectives, becomes a priority. Absolute safety and security, such as fault-free software (at least from a quickly reached complex level on), does not exist in reality. As an instantaneous relative condition (even better, a steady process), security requires agreement about a certain level. To approximate or even reach such a goal, the tools include continuous risk assessment, resulting adjustments, preconcerted effective measures, and product specifications that are actually met. Factors such as missing technical understanding and risk unawareness, information asymmetry, and lack of transparency often lead to the absence of relevant contract terms. The resulting software has an unclear security condition and maintenance status, keeping both over the software's life cycle and beyond. The negative effects of miserable software quality are an externality, as vulnerabilities have been for decades, resulting in the current state of IT insecurity.[13]

2 Two directives may change a lot for consumers, but they address only traders

The transfer of the digital content and digital services directive[14] and its sister, the sale of goods with digital elements directive,[15] led to a reform of the national laws of obligations. The scope of the directives requires an exchange between the parties[16] and excludes, under certain circumstances, free and open software.[17] Information

[10] See Wagner in *MüKoBGB*, 8th edn. 2020, ProdHaftG § 2, rec. 21 ff.; Lenz, *Produkthaftung*, 2nd edn. 2022, § 3, rec. 298; Förster in BeckOK BGB, 61st edn. 1 February 2022, ProdHaftG § 2, rec. 22 ff. with further references.

[11] See Anderson, *Security Engineering*, 3rd edn. 2020, pp. 1044.; Pietre-Cambacedes and Chaudret, AIC '09: Proceedings of the 9th WSEAS International Conference on Applied Informatics and Communications, August 2009, pp. 156.

[12] Functional protection of the outside world and, on the other hand, protection against interference/attacks (protection of the object). See Anderson, *Security Engineering*, 3rd edn. 2020, p. 16.; Hornung and Schallbruch, *IT-Sicherheitsrecht*, 2021, § 1, rec. 12; Schucht, *NVwZ,* 2021, 532.

[13] See Anderson, *Security Engineering*, 3rd edn. 2020, pp. 277.

[14] Directive (EU) 2019/770.

[15] Directive (EU) 2019/771.

[16] A price in the form of, for example, money or personal data. See directive Art. 3 (5) f) (EU) 2019/770 and recital 25 with an exclusion for collecting personal data without a price "for the sole purpose of meeting legal requirements," such as "cases where the registration of the consumer is required by applicable laws for security and identification purposes" (compare Art. 6 (1) c) GDPR).

[17] See directive (EU) 2019/770 recital 32.

technology security becomes a named objective conformity requirement for digital goods.[18] A definition is not provided. For the applicable level of security, the law refers, in the absence of an individual concession or agreement,[19] to "objective requirements for conformity."[20] Key are the security features and quality that are "normal for goods of the same type which the consumer may reasonably expect given the nature of the goods." How the consumer's expectations shall be determined is a question unanswered by the directives or national law.[21] Published producer notes and documentation of the product's security scope with the applied threat model and resulting protection measures may help, but they are a rarity and tough to understand for the ordinary IT user.[22] Court decisions and further harmonizing efforts may construct a framework.[23] An agreement of an IT security level below expectations may be legally binding in favor of the trader only in rare circumstances, especially with regard to the required comprehensive, technically transparent presales information and qualified consent by the consumer. Secondary duties following a breach of contract due to a security-related product fault bind only the trader, who may often be a different person than the producer. Concerning vulnerabilities, this is the wrong addressee, since the producer as controller of the flawed software code may be the only actor to fix it. Vulnerability management is not focused on a fault in an individual (serial) product but rather on the producer's portfolio.

The implementation of security updates in sale contracts as, so far, a one-time exchange of goods for (traditionally) money inserts a dynamic and continuous factor that was formerly found only in continuing obligations such as rentals. Transfer of perils is no longer the only point in time for a change in risk allocation. The traders need to monitor the security status, identify the need for updates, provide them, and inform the consumer to stay in conformity. It is then up to the consumer to install them. Remaining to be solved are foreseeable issues and conflicts concerning

[18] See directive (EU) 2019/770 in Art. 8 (1) (b) and recital 50 for transparency requests to the traders ("should").

[19] The directives declare (unless otherwise provided) a contractual agreement to the consumer's detriment on a substandard level of IT security not binding to the consumer (especially before the consumer's knowledge of the lesser protection provided). An agreement after the consumer brings the lack of conformity to the seller's attention may be binding. See Art. 21 directive (EU) 2019/771; Art. 22 directive (EU) 2019/770. For a critical view, see Kipker and Walkusz, *RDi*, 2021, 30 (doubting, rightfully for most cases, an informed consent).

[20] See Art. 7 (1) directive (EU) 2019/771; Art. 8 (1) directive (EU) 2019/770. In German law, §§ 327 (3) sentence 1 no. 2; 434 (3) sentence 2 BGB, and for the interpretation directive, (EU) 2019/770 recital 45 ff. and directive (EU) 2019/771 recital 24 ff. For the interpretation of "normal use" with reference to technical standards, see Schulze and Staudenmayer, *EU Digital Law*, 2020, pp. 137.

[21] To be clarified by (CJEU) case law. A path could be a combination of surveys/polls (empirical data concerning market penetration of security features, advertising statements, and specifications as well as the ever-evolving state of technology) and risk assessment/loss analysis provided by court-appointed experts. The perspective is that of the consumer/end user and is time critical. For the concept of reasonable expectations emphasizing the back reference to the parties' statements of intentions, see Schulze and Zoll, *European Contract Law*, 3rd edn. 2021, pp. 41; Schulze and Staudenmayer, *EU Digital Law*, 2020, pp. 144.

[22] See Shostack, *Threat Modeling*, 2014, pp. 34.

[23] Directive (EU) 2019/771 recital 25 demands full harmonization to achieve clarity.

- requirements for (continuous) monitoring and identification of update necessities
- timeliness of the provision, information, and installation of an update
- requirements for complete and flawless information, e.g., concerning installation procedures, configuration and risks, test requirements,[24] and incompatibilities
- faulty or ineffective updates
- faulty or ineffective installations
- end-of-life cycles of products, components, online services, and technologies
- required conformity in the fields of compatibility, functionality, usability, performance or power/storage consumption (including follow-up problems in connected systems)

An update may not be provided or may fail because of collisions and conflicts, especially in cases of insufficient performance or storage space. A central open question is whether the technical requirements for updates can be foreseen so that the hardware and software have enough reserve. Even with sufficient reserve, required source code may be inaccessible—for example, due to contractual restrictions or data loss in the supply chain, resulting in the personal or absolute inability to provide an update. For consumers and commercial end users, the code of closed-source software is a black box, including its history. With every update, closed-source software may be changed unnoticeably, inserting new flaws with consequences for usage instantly or later. Code sovereigns may delete, cover, or manipulate tracks of, for example, flaws and data loss via (automatic) updates. The information asymmetry and difficulties for consumers and end users in obtaining evidence are obvious.[25] The courts will have to handle such cases of fallout.[26]

Especially for long-lasting goods such as cars, the courts will also need to decide about the appropriate support periods and range. Traders are not obliged before the transfer of perils to inform about the minimum time span of support, but it obviously needs to be longer than the warranty period since market expectations grow for security updates. Because online features relying on a steady web connection have become the norm, security updates will be a necessity to keep cars technically compliant with road traffic licensing regulations and thus securely operational.[27] Remote attacks while someone is driving may result in mass crashes, and other scenarios can be imagined.[28] Security updates are key, as well as a pricing factor for secondary and follow-up sales. The producer will also have to decide whether the bundling of functionality and security, e.g., to sell subscriptions for "premium features," is worth the risks of intermingling software and hardware modules and

[24] See, for example, § 327e (3) sentence 1 no. 3 BGB.

[25] A solution could be court-appointed experts as data trustees with granted access to source code. For the burden of proof, see Art. 12 directive (EU) 2019/770, and in general, see Schulze and Zoll, *European Contract Law*, 3rd edn. 2021, pp. 249.

[26] For Dutch cases prior to the two directives, see *Wolters Computer Law & Security Review*, vol. 35, issue 3, May 2019, 295.

[27] See Vellinga, *International Review of Law, Computers & Technology*, published online 4 April 2022, pp. 5 https://doi.org/10.1080/13600869.2022.2060472.

[28] For a fictional approach, see Doctorow, *Attack Surface*, 2020.

raising the complexity level. The demand and expectation for (security) updates will be, from today's perspective, for more than 10 years for a newly purchased car. Leasing may become the norm, allowing the car manufacturers and traders more flexible terms and conditions. Closed-source software will also mean a closed shop for maintenance and repairs, and consequently perhaps even for reselling.[29] With more and more dependencies on online connectivity, a switch to get to an offline or even air-gap mode seems to be utopian.[30] But especially with regard to sustainability, the question remains: Will security flaws take an otherwise functioning car to the recycling facility or junkyard?[31]

Currently the producer is only a downstream debtor in the liability chain, especially because lawmakers often do not pay enough attention to pure financial loss and because of the increasing relevance of the right to use over ownership. For the claimant, it is difficult to prove the existence and causality of digital flaws, especially in closed-source products. A fortiori this is the case if end users want to check for vulnerabilities to prevent a loss. Product liability in tort sets duties to monitor, warn, and possibly recall, with many leading court decisions only from analog times. Because of the mentioned black-box effect, the only investigation opportunities for the consumer or commercial end user are via monitoring the software's run time or manipulating the data input and observing the output. Insight into the code is denied because of intellectual property rights or business secrets. General contract terms often even effectively forbid in-depth security testing since typical measures such as fuzzing and decompiling are not allowed.[32] The end user is forced to blindly rely on the willingness of the producer to fix vulnerabilities. Consumer protection may find a solution in extending the legal framework for IT security researchers and allowing penetration testing not hindered by liability or one-sided intellectual property rights.[33] Long overdue is the establishment of product liability for software.[34] But all of these are measures to address the aftermath of IT insecurity.

A best practice for how producers are supposed to handle notifications of (potential) vulnerabilities from end users and IT security researchers needs to be es-

[29] The right to repair or tinker with end-of-life products (for example, to publish source code under a free open-source license or make boot loaders/ROM/firmware accessible/changeable to allow community-driven projects) is difficult to enforce for complex products such as cars that have many technology layers and component interactions. On the other hand, a right to repair is environmentally sustainable and should not be rejected by denying support via updates to promote a paid upgrade rather than allowing repairs outside of the producer's economic sphere.

[30] See ENISA Advisory Group, Opinion Consumers and IoT security, September 2019, pp. 8 https://www.enisa.europa.eu.

[31] See Schneier, Click here to kill everybody, 2018, pp. 37; Van Gool and Michel, EuCML 2021, 136.

[32] See Balaban et al., *Whitepaper zur Rechtslage der IT-Sicherheitsforschung*, v. 1.0, 2021, pp. 27 https://sec4research.de.

[33] For (potential) criminal charges in Germany, see BVerfG decision from 18.05.2009, matter 2 BvR 2233/07; 2 BvR 1151/08; 2 BvR 1524/08, plus BVerfG decision from 30.03.2022, matter 1 BvR 2821/16 plus BGH MMR 2021, 441. For the United States, see van Buren v. United States, U.S. Supreme Court, case no. 19-783, decision from 3 June 2021; for an in-depth analysis, see Mackey/Opsahl, blog entry on 3 June 2021, https://www.eff.org. For blocking effects of IP, see Dickmann in Balaban et al., *Whitepaper zur Rechtslage der IT-Sicherheitsforschung*, v. 1.0 ,2021, pp. 20 https://sec4research.de.

[34] See Schneier, Click here to kill everybody, 2018, pp. 131.

tablished. For bigger companies, processes and an ISO standard for coordinated vulnerability disclosure (CVD) have been developed.[35] The driver here is mainly compliance[36] and less the protection of end users, with strong impetus from the U.S. Federal Trade Commission.[37] Details of such procedures mostly remain publicly unknown. Notifiers and especially researchers cannot be sure that producers will seriously take on the task in time or at all and with a fix as the goal. In addition, there is no end user's right to enforce effective IT vulnerability management. Even if basic security features such as password protection and data traffic encryption are not implemented, the consequence may only be claims for supplementary performance or damages. Otherwise, the consumer may only refuse to buy such a flawed product. But for some products and services, there may not be affordable, productive, or reliable alternatives on the market, posing a dilemma. The same applies for nonconsumers who do not benefit from the new rights such as updates, even though national lawmakers may include them as a protected group.[38] Since small and medium-sized businesses in particular are, as end users, often in a similar situation as consumers, their inclusion would boost IT security, and the protection would scale up with the sheer number of IoT devices in their service.

3 Product safety regulation as stimulus for an improved level of IoT security

The earliest opportunity to regulate at least a baseline level of security and loss prevention is before allowing products to enter the market.[39] A major regulation vehicle in the EU is the duty to mark products in certain categories. The label on the product is a producer's declaration of conformity with certain technical requirements according to the legal status at the time it was placed on the market. Subsequent stricter requirements do not result in an illegal market entrance. Derived from an

[35] ISO/IEC 29147:2018 plus for multiparty cases ISO/IEC TR 5895. For a historic placement, see Dickmann in Balaban et al., *Whitepaper zur Rechtslage der IT-Sicherheitsforschung*, v. 1.0 2021, pp. 39 https://sec4research.de.

[36] For product compliance, see Wagner et al., CCZ 2020, 1, and for the IT security niche, see Schmidl in Hauschka et al., *Corporate Compliance*, 3rd edn. 2016, Sect. 2, Chap. 4, § 28, rec. 1 ff.; Fortmann r+s 2021, 549, 552.

[37] For example, Federal Trade Commission [FTC] v. Equifax, Inc.; matter 172 3203, FTC v. Zoom Video Communications, Inc.; matter 192 3167; FTC v. Guess?, Inc./Guess.com, Inc.; matter 022 3260; https://www.ftc.gov. For U.S. regulation, see Whittle, *Impact Assessment on Increased Protection of Internet-Connected Radio Equipment and Wearable Radio Equipment,* final report, April 2020, Sect. 3.3.7, and Kitchen et al., *Duquesne Law Review*, vol. 59 no. 2 (2021), p. 274 ff. For equipment authorization between the United States and the EU, see agreement on mutal recognition (MRA; OJ L 31, 04.02.1999 with successive amendments, pp. 3–80), including acceptance of telecommunications equipment conformity.

[38] See Riehm, *RDi*, 2022, p. 209.

[39] Addressees are (component) producers and importers. Concerning the position of traders, see Schucht, *CCZ*, 2020, p. 322.

analog perspective with functional fixed hardware,[40] this regulation has up to now been static and focused on individual features. Breaches may result in penalties, authorities may deny or revoke the market entry of goods, and competitors may send a warning letter to an infringer.[41]

Such a declaration of conformity for radio equipment as products with specific harmonized technical requirements is the CE mark.[42] For labeled goods there is an assumption for the actual fulfillment[43] that may be refuted, for example if there is only compliance with out-of-date standards. If the producer does not comply with the typical standards, this does not result in an assumption of noncompliance.[44] But the producer needs to prove conformity on its own, making this an unexplored path. Until now, IT security has not been a named factor in the conformity check-up.

4 Activation of clauses in the radio equipment directive

For the future, the activation of Article 3, paragraph 3, sentence 1 d–f) of the radio equipment directive[45] may be a game changer, at least for goods with wireless or optional wireless connectivity.[46] It will have to be applied from 1 August 2024 onward. The mentioned article with IT security requirements was incorporated into the directive in 2014. But without the delegated act by the European Commission, the

[40] This has changed since software has come to more and more define (dynamically) hardware functionality, e.g., field programmable gate arrays. See Mencer et al., *Communications of the ACM*, vol. 63, issue 10, pp. 36, https://doi.org/10.1145/3410669.

[41] See §§ 7 (1/2), 28 (1) no. 5/6 ProdSG; Art. 16 (1) b) regulation (EU) 2019/1020; §§ 8, 9, 10 UWG. For more details, see Schütte in Ehring and Taeger, *ProdukthaftungsR- und ProduktsicherheitsR*, 2022, § 7 ProdSG, rec. 35 ff.

[42] See Art. 30 regulation (EG) 765/2008 plus for radio equipment directive (EU) 2014/53 recital 43 ff. It could be rated as an officially not checked assertion by the producer. For the perception by the market, see Lenz, *Produkthaftung*, 2nd edn. 2022, § 8, rec. 68 ff. For compliance procedures for radio equipment, see Williams, EMC for product designers, 5. Edt. 2017, pp. 53.

[43] If necessary, combined with a to be added EU conformity declaration. For radio equipment directive (EU), see 2014/53 recital 38; § 17 FuAG (German transfer). See also regulation (EU) 2022/30 recital 17 plus Schucht, *NVwZ*, 2021, 532, 533.

[44] Kapoor and Klindt, *NVwZ*, 2012, 719; Schucht, *NVwZ* ,2015, 852; Bauer, *Das Recht des technischen Produkts*, 2018, p. 174.

[45] Radio equipment directive (EU) 2014/53. Technology is neutral for products with wireless transmitter/receiver functionality such as routers or smartphones as well as Bluetooth watches, "smart" toys with online based speech recognition, or baby monitors controlled via WLAN.

[46] For the history, see https://ec.europa.eu/growth/sectors/electrical-and-electronic-engineering-industries-eei/radio-equipment-directive-red_en and Chiara, *International Review of Law, Computers & Technology*, published online 7 May 2022, p. 6 https://doi.org/10.1080/13600869.2022.2060468.

[47] Art. 3 (3) sentence 2, Art. 44 directive (EU) 2014/53; delegated regulation (EU) 2022/30 by the Commission dated 29.10.2021, official journal of the EU (DE) dated 12.01.2022, p. 6 ff.; in force since 02/01/2022. Also see the documentation of the Commission dated 29.10.2021, reference C (2021) 7672 final. Regarding no objection by the EU parliament and the council, see Art. 3 (3) p. 2; 44 directive (EU) 2014/53.

scope of application was missing.[47] Article 1 includes in paragraph 2 the categories of radio equipment[48] that

- is directly or indirectly[49] connected with the internet (concerning protection of the network and its functioning against misuse of network resources resulting in an unacceptable degradation of service) and/or processes personal/traffic/location data (concerning protection of privacy/personal data)[50]
- is designed or intended exclusively for childcare and processes personal/traffic/location data (concerning protection of privacy/personal data)[51]
- is a component of a toy or is a toy itself and processes personal/traffic/location data (concerning protection of privacy/personal data)[52]
- is a component of a wearable or is a wearable itself and processes personal/traffic/location data (concerning protection of privacy/personal data)[53]
- is directly or indirectly connected with the internet and enables the holder or user to transfer money, monetary value, or virtual currency (concerning the protection against fraud)[54]

Not in the scope of application is radio equipment to which one or more of the following also apply:

- The medical devices regulation[55]
- The in vitro diagnostic medical devices regulation[56]
- The aviation basic regulation (partial exclusion)[57]
- The type-approval requirements for motor vehicles regulation (partial exclusion)[58]
- The electronic road toll systems directive (partial exclusion)[59]

The essential requirements addressing IT security laid down in the radio equipment directive call for the following:

[48] For details on the categories, see Whittle, *Impact Assessment on Increased Protection of Internet-Connected Radio Equipment and Wearable Radio Equipment*, final report, April 2020, pp. 18.

[49] See regulation (EU) 2022/30 recital 5.

[50] Art. 1 (1) respectively (2a) regulation (EU) 2022/30.

[51] Art. 1 (2b) regulation (EU) 2022/30.

[52] Radio equipment that applies to regulation (EG) 2009/48 (safety/security of toys), Art. 1 (2c) regulation (EU) 2022/30. See also Hessel and Rebmann, *Int. Cybersecur. Law Rev.* (2020), vol. 1, issue 1–2, p. 27.

[53] Art. 1 (2d) regulation (EU) 2022/30.

[54] Art. 1 (3) regulation (EU) 2022/30, and for the definition of fraud protection, see Whittle, *Impact Assessment on Increased Protection of Internet-Connected Radio Equipment and Wearable Radio Equipment,* final report, April 2020, Sect. 1.3.4. and 3.3.4.

[55] Art. 2 (1a) regulation (EU) 2022/30 with reference to regulation (EU) 2017/745.

[56] Art. 2 (1b) regulation (EU) 2022/30 with reference to regulation (EU) 2017/746.

[57] Art. 2 (2a) regulation (EU) 2022/30 with reference to regulation (EU) 2018/1139 ("equipment to control unmanned aircraft remotely as well as non-airborne specific radio equipment that may be installed on aircrafts"); exclusion only for Art. 3 (3) sentence 1 e) and f) directive (EU) 2014/53.

[58] Art. 2 (2b) regulation (EU) 2022/30 with reference to regulation (EU) 2019/2144; exclusion only for Art. 3 (3) sentence 1 e) and f) directive (EU) 2014/53.

[59] Art. 2 (2c) regulation (EU) 2022/30 with reference to directive (EU) 2019/520; exclusion only for Art. 3 (3) sentence 1 e) and f) directive (EU) 2014/53.

- Neither harming the network or its functioning nor misusing network resources, thereby causing an unacceptable degradation of service[60]
- Incorporating safeguards to ensure that the personal data and privacy of the user and the subscriber are protected[61]
- Supporting certain features ensuring protection from fraud[62]

The radio equipment directive's scope of application is not limited to products for consumers.[63] Its regulation begins with the conception and construction of hardware and software[64] in order to avoid the misuse of certain locally stored data or data to be transferred and of network resources via radio, since wireless ports are harder to secure. How and via which port an internet connection is established is irrelevant. Especially concerning the protection of privacy, a connection is not even necessary. The IT security requirements are not limited to radio-specific functions but apply to the product from a holistic standpoint.[65] With regard to technical neutrality, producers are free in their choice of tools for implementation, but the result needs to be effective. The European Commission refers to the impact assessment previously published, which demands a vulnerability management system to deal, for example, with notifications from security researchers.[66]

The quite abstract requirements call for a concretion in harmonized technical standards. Such a body of work has to be created by a European standardization committee mandated by the Commission and is published in the official journal of the EU.[67] In this context, the European Telecommunications Standards Institute (ETSI) has already drafted ETSI/EN 303645.[68] This technical standard frames specifications for the IT security of consumer IoT.[69] The scope has much overlap with the radio equipment directive's activated categories, even though it is not limited to products with radio connectivity.[70] It covers the full product life cycle, whereas

[60] Art. 3 (3) sentence 1 d) directive (EU) 2014/53. See also regulation (EU) 2022/30 recital 9.

[61] Art. 3 (3) sentence 1 e) directive (EU) 2014/53. See also regulation (EU) 2022/30 recital 10 f.

[62] Art. 3 (3) sentence 1 f) directive (EU) 2014/53. See also regulation (EU) 2022/30 recital 13 f.

[63] See Art. 1 (1) regulation (EU) 2014/53.

[64] Regulation (EU) 2022/30 recital 2; Art. 4 directive (EU) 2014/53. See Schucht, *NVwZ*, 2021, 532, 535 ("To prevent attacks instructions do not seem to be effective").

[65] Regulation (EU) 2022/30 recital 8 and 12.

[66] Impact Assessment on Increased Protection of Internet-Connected Radio Equipment and Wearable Radio Equipment, https://ec.europa.eu/docsroom/documents/40763 and Whittle, Final Report, April 2020, pp. 25.

[67] For a listing, see https://ec.europa.eu/growth/single-market/european-standards/harmonised-standards_de.

[68] For the up-to-date draft, see v. 2.1.0, June 2020, *Cyber Security for Consumer Internet of Things: Baseline Requirements*, https://www.etsi.org. Compare also ENISA, *Good Practices for Security of Internet of Things*, November 2018, https://www.enisa.europa.eu.

[69] For the threat landscape in IoT, see Chantzis et al., Practical IoT Hacking, 2021, pp. 3; specifically for radio hacking, see pp. 239.

[70] ETSI/EN 303645 V2.1.1 (2020-06), p. 6, 11.

the directive's formal influence ends with the product's placement on the market.[71] Important to note is that the standard focuses on typical remote attacks, with no physical access required.[72] The cybersecurity provisions for consumer IoT range from a secure default setup in the delivery state, secure updates, and encryption of stored data, plus connections, usability, input validation, and resilience against outages to secure delete functions.[73] Also included are provisions for data protection, such as transparent information about the usage of personal data, obtaining of user consent, and minimization of telemetry data.[74] Implied measures do not stop with implementations in a product's hardware and software but also include external processes. One such demand is for IT vulnerability management.[75] This consists of a published self-binding policy for a coordinated disclosure process with duties to react on notifications within an appropriate time limit, with a ready-to-roll-out patch/update if possible.[76]

ETSI/EN 303645 assumes in Sect. 5.2 a contact of notifier and producer on par, resulting in respectful and fair communication.[77] In reality, conflicts often arise because of, for instance, fear[78] or missing experience.[79] A transparent CVD process allows management of expectations on all sides involved, such as concerning time frames or feedback loops, and avoids publishing vulnerability information or even an exploit without a mitigation process at hand (full disclosure). In practice, the involved parties may agree on an extension of the period to work on a proper patch or mitigation, especially if the technical background and coordination are complex. Such handling is based on already established trust. Fair treatment and the will to mitigate will give the producer adequate time for development plus rollout and will give the notifier merit for the effort (if desired).[80]

Since mostly larger technology-oriented companies have already established a disclosure process, it will be an intermediate goal to reach a significant number of smaller IoT producers, even from outside the European single market. Acceptance

[71] This timely limitation does not block the demand for updates and vulnerability management processes since the technical/procedural seeds need to be implemented before the placement.

[72] ETSI/EN 303645 V2.1.1 (2020-06), p. 5. The regulation (EU) 2022/30 identifies with the impact assessment the risks of "physical penetration."

[73] See ETSI/EN 303645 V2.1.1 (2020-06), cybersecurity provisions (no. 5).

[74] See ETSI/EN 303645 V2.1.1 (2020-06), data protection provisions (no. 6).

[75] ETSI/EN 303645 V2.1.1 (2020-06), p. 14 f. (provision 5.2-1 ff.).

[76] For VDP, see Goerke et al. in Balaban et al., *Whitepaper zur Rechtslage der IT-Sicherheitsforschung*, v. 1.0 2021, pp. 54 https://sec4research.de. For the status quo in the EU member states, see ENISA, Coordinated Vulnerability Disclosure Policies in the EU, April 2022, https://www.enisa.europe.eu.

[77] For the actors and their incentives/behavior in the disclosure process, see ENISA, Economics of vulnerability disclosure, December 2018, pp. 10 and pp. 26 https://www.enisa.europa.eu.

[78] Such as because of liability, penalties, or negative economic impact/publicity.

[79] See ETSI/EN 303645 V2.1.1 (2020-06), p. 14 ("In the IoT industry, CVD is currently not well-established as some companies are reticent about dealing with security researchers").

[80] For example, in the form of a publication, a presentation from a conference, an honorable mention in a press release, or other rewarding gestures.

[81] Arguments: notifications as gifts of valuable information that allow product improvement, diminish liability risks by mitigation, and creation of positive public relations after a successful CVD.

is key[81] and includes preparation via training courses, selection of (technical) staff, and documentation of distributed hardware and software from conception onward.[82] This along with dry-run testing would be the baseline to be able to move to more complex scenarios such as

- involvement of many parties in a (layered) supply and/or delivery chain[83]
- vulnerabilities in classes of products[84]
- unclear maintenance responsibilities or end-of-life legacy code
- inaccessible software code
- insolvency of parties
- conflicts due to nondisclosure agreements or obligations of confidentiality by law
- blocking effects by intellectual property rights
- hoax/malicious notifications[85]
- parallel notifications
- conflicts due to mandatory notifications[86]

ETSI/EN 303645 mentions as favored behavior direct notification of the vulnerability by the finder to the producer.[87] But it does not stand against (central) notification authorities as an alternative way to launch the CVD process.[88] As a mediator to avoid or arbitrate disputes and help with the identification of producers, or in cases of unclear responsibilities, such an authority could add value in the form of practical experience, expert knowledge, or a network of contacts.

Like the new rules for sales or service contracts for digital goods with the obligation to provide updates,[89] activation of the radio equipment directive implements a dynamic and continuous component. With a focus not on functionality but on IT security, this change calls for a specific kind of maintenance in the product's life cycle and maybe beyond. Neither set of rules results in unlimited implied warranty through the back door. The directives for the law of obligations have not set absolute limitations in time for the provision of updates but instead rely on the consumer's reasonable expectation. This is in itself a dynamic factor that may change over time with evolving technology and deeper technical understanding, especially of security mechanisms and their effectiveness. In this field of the law, there is no demand to the trader for self-commitment to a minimum support period. Even though many commentators have criticized this, it is at least understandable because the addressee

[82] ETSI/EN 303645 V2.1.1 (2020-06), p. 15 (Provision 5.2-3; Software Bill of Materials (SBOM)). See Anderson, *Security Engineering*, 3rd edn. 2020, p. 498, with the reminder on "good engineering."

[83] See ISO/IEC TR 5895. On the security issues in supply chains, see ENISA, Guideline for securing the Internet of Things, Secure supply chain for IoT, November 2020, https://www.enisa.europa.eu. Conflicts may arise from difference in interests concerning finding a mitigation (and admitting faults) and securing potential recourse claims in the chains; see Art. 20 directive (EU) 2019/770 and Art. 18 directive (EU) 2019/771.

[84] See Schneier, Click here to kill everybody, 2018, pp. 31, 95.

[85] For example, by competitors to bind resources.

[86] For example, concerning prioritization, allocation of resources, transparency, and information flow.

[87] ETSI/EN 303645 V2.1.1 (2020-06), p. 15.

[88] ETSI/EN 303645 V2.1.1 (2020-06), p. 15 ("reporting to national authorities").

[89] See §§ 327 f, 475b (4) no. 2 BGB.

is not the producer with hands on the code.[90] The regulation of product security on the other side allows the producer to define the time of support but requests information to the public for the minimum period when placing the product on the market.[91] Product security regulation does not include a right for updates, only for a process to deal with vulnerabilities that may lead to a fix (or not). A breach may result in a tort claim if absent or ineffective vulnerability management brings harm to end users because a security flaw could have been fixed and therefore avoided (e.g., a loss via a ransomware attack). Severe obstacles remain for the claimant, since causality plus a concrete loss need to be proven.

Another path of regulation has to be kept in mind. This is the non–sector specific and more general direction via the EU Cybersecurity Act (CSA),[92] the Cyber Resilience Act (CRA),[93] and the to-be-reformed directive concerning measures for a high common level of security of network and information systems across the EU (NIS).[94] Key elements of interest here are certification schemes and processes[95] to allow validation of compliance with technical requirements for the producers. The earliest starting point would be with the conception of new products with regard to security by design and default, including supply and delivery chains. To be avoided is a last-minute or even postmarket entry evaluation of the actual product security, with end users and security researchers identifying vulnerabilities that should have been tracked down and eliminated (as low-hanging fruit) in the development and testing phases. These regulations aim to encourage early-on investments and approaches. They are not focused on individual products but reach for a global lead in the development, application, and evolution of IT security standards as well as guaranteeing a market with only compliant products. For the individual consumer, the regulation therefore has more indirect effects. Whether such high-flying plans materialize as actual betterment of IT security in hardware and software needs to

[90] See Artz in Staudinger and Artz, *Neues Kaufrecht und Verträge über digitale Produkte*, 2022, rec. 158; Schulze and Staudenmayer, *EU Digital Law*, 2020, pp. 155 with further references.

[91] Publication of the point in time after which security updates or mitigation information will no longer be provided for a specific product.

[92] Regulation (EU) 881/2019. For the strategy to enforce the act, see ENISA, A trusted and cyber secure Europe, June 2020, https://www.enisa.europa.eu.

[93] See Kipker, *MMR-Aktuell*, 2022, 447353.

[94] For a commentary on the draft of NIS2 as a reformed version of directive (EU) 1148/2016, see Kipker et al., *MMR*, 2021, 214; Chiara, *Int. Review of Law, Computers & Technology*, published online 7 May 2022, p. 9 https://doi.org/10.1080/13600869.2022.2060468.

[95] It is important to understand that there is a difference between compliance with a scheme/process and an actual secure product (one that reaches the required security level applicable for its type). Certification processes should be kept free of conflicts of interest and false incentives, for example, letting the mandating company pay vendors for licensing or conformity assessment bodies. See *Anderson, Security Engineering*, 3rd edn. 2020, p. 1026.

be watched closely.[96] Hopefully, they will not end in legal fragmentation with many overlaps and unclear competence boundaries.[97]

When zooming out and taking the consumer's perspective, there is a blind spot. The original trader is bound to provide updates but this is limited in cases of impossibility or financial unreasonableness. This may cause many potential conflicts if the trader is different to the producer.[98] Since there is no direct primary claim against the producer for updates, it is unclear what will happen in secondary and follow-up markets, especially for highly durable goods such as cars. The follow-up buyers will have no contractual relationship with the producer.[99] In some cases a guarantee might fill gaps, but it is a voluntary extra with limited scope, obligations, positions/amounts, and exclusions. Product liability in tort does not provide entitlement to claims for performance, not even through the back door.[100] This may argue against implementation of a dynamic and continuous obligation to provide updates in a reform of product liability regulation.[101] On the other hand, why not insert a timely limited obligation for the producer to provide updates to the current user? This may improve the overall level of IT security in products[102] with additional pressure from the insurance industry.[103] From an ecological perspective, this may result in longer product life cycles and increased sustainability.

[96] Important factors are, for example, the scope of covered industries and products, the inclusion of business-to-business relations, a balanced mix of mandatory and voluntary measures, clear wording of sufficient in-depth requirements, common understanding by all actors, quick adjustment cycles, checks of actual effective compliance (not only to processes) in the field, and strict enforcement at least of the core elements.

[97] Also in the fields of data protection and privacy. See Chiara, *International Review of Law, Computers & Technology*, published online 7 May 2022, p. 10 https://doi.org/10.1080/13600869.2022.2060468

[98] For example, certain features could be provided to the original buyer only (as a measure to increase "customer loyalty"), even if such contractual terms may be invalid under consumer protection laws. Are such rights transferable, and if so, under which conditions? Does the original buyer have claims against the trader to transfer rights against the producer (even to follow-up buyers)? Even if one supports this, there is a lack of transparency and asymmetry of knowledge concerning the contracts between trader and producer. Do nondisclosure agreements and business secrets block claims for information?

[99] There may be one if the producer offers "premium features" on a subscription basis, but it is then limited to exactly this service (including the warranty).

[100] From a German perspective, see Lenz, *Produkthaftung*, 2. Aufl. 2022, § 3, rec. 155 (cumulus principle) and § 3, rec. 171 ff. (necessity for a breach of integrity interests). Under German law, a product fault is not a breach of property rights concerning this individual product since at the time of transfer of perils, the owner received a product including seeds of the fault. This understanding may now change with the dynamic continuous factor of security updates.

[101] Reform of directive (EEC) 374/1985 (plus directives (EC) 34/1999 and (EC) 42/2016). See the Commission's report to the Parliament on safety and liability implications of artificial intelligence, IoT, and robotics from 19 February 2020, matter COM (2020) 64 final, https://eur-lex.europa.eu for possible directions in regulation. For the historical development, see Wagner in *MüKoBGB*, ProdHaftG vor § 1 rec. 7; Riehm and Meier, *EuCML*, 2019, 161.

[102] At least concerning the provided features; the users still need to activate and configure them securely.

[103] For example, for general liability, (extended) product liability, product protection, and recall policies, as well as for errors and omissions, professional liability, and directors and officers coverage. For the phenomenon of silent cyber in conventional policies, see Bertsch and Fortmann, *r+s,* 2021, 485; *r+s* 2021, 549. Many insurers have reacted with exclusions, limits, deductibles, and zeroing clauses to exclusively concentrate risks in certain (cyber) policies generally covering only pure financial loss. For the General Association of the German Insurance Industry (GDV) muster wording (April 2017) from https://www.gdv.

5 Liability risks and chances

An unjustified affix of a CE marking is a product fault if there is no compliance with the harmonized requirements for IT security.[104] It is doubtful that the producers will have adopted all of their products by 1 August 2024. But at least the baseline security requirements will have been met, making them mandatory (partly dynamic) features. Costs are not an argument against this since at least those for a minimum security level are not prohibitive and demand implementation only in the development and construction/programming phases. Ignoring this has to be costly for the producers in order to be a regulation with teeth.[105] This also affects product liability insurance, in which more secure products mean lower premiums. A positive development may also bring extended coverage for pure financial loss, which is especially needed by IT service providers that program and install software and hardware.

In addition, a breach of the implementation of the tightened radio equipment directive may result in claims in tort under national law.[106] This is at least the case with the activation in the directive coming into effect that establishes new objectives.[107] Such goals are the protection against misuse of network resources and personal data as well as against the violation of privacy and fraud. In scope and protected not only as a reflex are users and participants. Their trust in the actual technical compliance by the producers has to be preserved.

An omitted establishment of vulnerability management does not bear the assumption that the product is vulnerable and therefore faulty. The omission becomes relevant if a vulnerability is detected and exploited. This raises the question of whether effective vulnerability management would have resulted in a patch/update being installed before the exploit. An installation that was done in time could be

de, see AVB Cyber A1-17.6 (exclusion for vehicles), A3-2 (exclusion for contractual performance), and A3-7.1 (zeroing for recall), and (of limited interest concerning our topic) for consumer cyber policies, see Fortmann, *Verbraucher-Cyberversicherung*, 2022.

[104] Under German law, a breach of §§ 434 (1) or 633 (1) BGB, likewise Schütte in Ehring and Taeger, *Produkthaftungs- und ProduktsicherheitsR*, 2022, § 7 ProdSG, rec. 46. For divergent German court decisions concerning construction materials, see LG Mönchengladbach BeckRS 2015, 12238; LG Flensburg BeckRS 2022, 8216, and OLG Oldenburg NJW 2019, 863, with comment by Ziegler, plus CJEU NZBau 2021, 100 (decision from 17.12.2020, C-475/19 P, C-688/19 p).

[105] The positive effect on the market may be a squeeze out of products not meeting baseline security requirements and no new developments in this (lowest price) category strengthening the market position of those who already have implemented the features. For the economic impact, see Whittle, *Impact Assessment on Increased Protection of Internet-Connected Radio Equipment and Wearable Radio Equipment*, final report, April 2020, pp. 117. For the economics in general, see Anderson, *Security Engineering*, 3rd edn. 2020, pp. 293.

[106] Under German law, a breach of § 823 (2) BGB and § 7 (2) ProdSG. For a different opinion with regard to the legal status before the reform of the law of obligations, see Schütte in Ehring and Taeger, *Produkthaftungs- und ProduktsicherheitsR*, 2022, § 7 ProdSG, rec. 43 with further references. For cases involving conformity assessment bodies, see CJEU NJW 2017, 1161 (decision from 16.02.2017, C-219/15, especially rec. 60) for medical products but with general relevance for the consumer trust in the CE mark. See also BGH NJW 2020, 1514 (PIP breast implants; court of second instance needs to revaluate potential liability in tort). For similar court actions in France, see Becklink 2021967, available at https://beck-online.beck.de.

[107] See directive (EU) 2014/53 recital 44 ("Important for the Information of Consumers and Public Authorities").

assumed in favor of the claimant, but proving the causality chain from the exploit to the loss is a high burden. Adducing evidence may be easier when an end user fell victim to a ransomware campaign for which the path of an exploit had already been investigated. Sources for pertinent knowledge are press articles, forensic findings, information leaks, breach notifications, official investigations, and answers to claims for information. If the producer had sufficient time for development and rollout of a patch/update or another mitigation (at least via a warning) but failed to provide it, this may result in liability.

Time will tell if a combination of the law of obligations and product security law leads to significance concerning the liability of producers for IT security flaws. A crossroads will be reached if courts rule differently on technical details of the IT security requirements in both fields. Market expectations tend to exceed minimum requirements. Hopefully, the producers do not see vulnerability management as pure red tape but see notifications from IT security researchers as gifts and chances for improvement.

Roman Dickmann Specialist solicitor in insurance law, LL.M., University of Münster; Europajurist, University of Würzburg