# Conceptualising the Legal Notion of 'State of the Art' in the Context of IT Security

Sandra Schmitz-Berndt

# Conceptualising the Legal Notion of 'State of the Art' in the Context of IT Security

Sandra Schmitz[1][0000-0001-9443-9206]

[1] Université du Luxembourg, 6, Avenue de la Fonte, 4264 Esch-sur-Alzette, Luxembourg

sandra.schmitz@uni.lu

**Abstract.** In the context of IT security, legal instruments commonly demand that IT security is brought up to the level of 'state of the art'.
As the first horizontal instrument on cybersecurity at EU level, the NIS Directive requires that Member States shall ensure that operators of essential services (OESs) and digital service providers (DSPs) take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations, or in the context of offering specific services. Having regard to the 'state of the art', those measures shall ensure a level of security of NIS appropriate to the risk posed. Similarly, the GDPR requires data controllers, and to some extent processors, to take 'state of the art' into account when implementing appropriate technical and organisational measures to mitigate the risks caused by their data processing activities. The same applies to public electronic communications networks or services regarding the security of their networks and services under the EECC.
Although the notion is widely referred to in legal texts, there is no standard legal definition of the notion.
This paper, based on a workshop held at the 14th IFIP summer school, analyses the contexts in which the notion 'state of the art' is being used in legislation. Briefly, the reasons for abstaining from clear technical guidance are addressed. Following an introduction to the three-step theory developed by the German constitutional court, where 'state of the art' is located between the 'generally accepted rules of technology' and the 'state of science and technology', this paper argues that this approach can also be applied at EU level in the context of IT security.

**Keywords:** State of the Art, NIS Directive, GDPR.

## 1 State of the Art in Legal Interventions

### 1.1 'State of the Art' as Protection Goal

In the context of IT security, EU legal instruments commonly demand that IT security is brought up to the level of 'state of the art'. Both, national and EU legislators, however, refrain from defining what 'state of the art' in IT security exactly means.

Commonly, the notion refers to the highest level of general development achieved at a particular time. In law, the notion has some tradition in patent law[1] as well as in tort law[2]. As regards the latter, it may be used as a legal defence, meaning that for instance a manufacturer cannot be held liable if he can prove that the state of technical and scientific knowledge, at the time when the product was put in circulation, was not such as to enable the existence of a certain defect to be discovered. In patent law, state of the art is used in the process of assessing and asserting the novelty of an invention.

With increasing regulation of technology and in particular information technology, the notion of state of the art gained in importance.

As the first horizontal instrument on cybersecurity at EU level, the NIS Directive[3] requires that Member States shall ensure that operators of essential services (OESs) and digital service providers (DSPs) take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations, or as regards DSPs in the context of offering services referred to in Annex III of the Directive.[4] Having regard to the 'state of the art', those measures shall ensure a level of security of NIS appropriate to the risk posed.[5] Similarly, Arts. 25 and 32 GDPR[6] require data controllers, and to some extent processors, to take the 'state of the art' into account when implementing appropriate technical and organisational measures to mitigate the risks caused by their data processing activities. According to Art. 40(1) EECC[7], the same applies to public electronic communications networks or services regarding the security of their networks and services. None of these legal interventions provides a binding legal definition of the concept of 'state of the art' in the context of IT security.

If one consults the vast body of EU legislation, the notion 'state of the art' is widely referred to in legal texts relating to environment and technology such as for instance

[1] Cf. for instance Art. 54 Convention on the Grant of European Patents (European Patent Convention).

[2] Cf. for instance Art. 7(e) Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (Product Liability Directive) [1985] OJ L 210/29.

[3] 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 [2016] OJ L 194/1.

[4] Arts. 14(1) and 16(1) NIS Directive.

[5] Ibid.

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data,and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/ 1.

[7] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code [2018] OJ L 321/36 (EEEC).

the Medical Devices Regulation[8], the Radio Equipment Directive[9], or the Machinery Directive[10]. Similar as in the aforementioned acts, none of these acts provides a standard legal definition of 'state of the art'. Legal scholars thus refer to the notion as an indefinite, abstract general notion [1], or undetermined legal concept [2]. The objective behind using such a concept instead of referring to given standards is obvious: the legislator is keen on retaining options open to accommodate improvements over time. In particular in the field of technology, requiring a certain set level of technology would mean that a legal provision is likely to become outdated in no time.

### 1.2 State of the Art vs. Best Available Techniques

Besides 'state of the art', legal norms may require that the level of technology corresponds to the 'best available techniques'. In particular in environmental law, 'best available techniques' constitutes a substantial tool to regulate industrial emissions. At EU level, this notion was first introduced by the Integrated Pollution Prevention and Control Directive[11].

Art. 3(10) of Directive 2010/75/EU[12], which replaced the aforementioned Directive, provides a definition of 'best available techniques' in the context of emissions as meaning 'the most effective and advanced stage in the development of activities and their methods of operation which indicates the practical suitability of particular techniques for providing the basis for emission limit values and other permit conditions designed to prevent an, where that is not practicable, to reduce emissions and the impact on the environment as a whole: (a) 'techniques' includes both the technology used and the way in which the installation is designed, built, maintained, operated and decommissioned; (b) 'available techniques' means those developed on a scale which allows implementation in the relevant industrial sector, under economically and technically viable conditions, taking into consideration the costs and advantages, whether or not the techniques are used or produced inside the Member State in question, as long as they are reasonably accessible to the operator; (c) 'best' means most effective in achieving a high general level of protection of the environment as a whole.'

---

[8] 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 [2017] OJ L 117/1.

[9] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC [2014] OJ L 153/62.

[10] Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC [2006] OJ L 157/24.

[11] Council Directive 96/61/EC of 24 September 1996 concerning integrated pollution prevention and control [1996] OJ L 257/26.

[12] Directive 2010/75/EU of the European Parliament and of the Council of 24 November 2010 on industrial emissions (integrated pollution prevention and control) [2010] OJ L 334/17.

The national implementation of Directive 2010/75/EU into German law, the Federal Immission Control Act (BImSchG[13]), uses the notions 'state of the art' ('Stand der Technik'[14]) and 'best available techniques' ('beste verfügbare Techniken'[15]) suggesting that they are not identical but closely connected. There seems to be consensus that in this context state of the art at least corresponds to best available techniques [3] [4] [5]. Accordingly, the minimum basis for state of the art in that context is the best available technique.

### 1.3 The Deployment of State of the Art in the Context of IT/Data Security Regulation

Although best available technique is almost equally vague as state of art, it clarifies that the technology must be 'available'. However, this leads to further questions, namely, whether the technology must be available in general on the market, and/or available to the individual operator.

The NIS Directive requires operators or essential services and digital service providers to ensure the security of the network and information systems which they use and 'having regard to the state of the art, those measures shall ensure a level of security' 'appropriate to the risk posed'. Recital 53, which may support the interpretation of the operative part, stipulates that disproportionate financial and administrative burdens on operators should be avoided by requiring measures proportionate to the risk presented. Arts. 25 and 32 GDPR require the data controller to take into account state of the art, the cost of implementation and the nature, scope, context and purpose of processing as well as the risks for rights and freedoms of data subjects posed by the processing, when implementing appropriate technical and organisational measures. GDPR and NIS Directive (and corresponding IT security regulation) follow a risk-based approach, meaning that the appropriateness of a security measure depends on the risk level. Since both instruments refer to the cost of implementation as a factor to be considered beside state of the art technology, this implies that 'availability' of a technology seems to be a mere objective criterion, meaning that the technology must be available in general on the market. Any further methodological guidance on how to comply with the state of the art requirement is lacking.

---

[13] Gesetz zum Schutz vor schädlichen Umwelteinwirkungen durch Luftverunreinigungen, Geräusche, Erschütterungen und ähnliche Vorgänge (BImSchG) (Act on the prevention of harmful effects on the environment caused by air pollution, noise, vibration and similar phenomena).

[14] § 3 sec. 6 BIsmSchG: 'State of the art as used herein shall mean the state of development of advanced processes, facilities or modes of operation which is deemed to indicate the practical suitability of a particular technique for restricting emission levels. When determining the state of the art, special consideration shall be given to comparable processes, facilities or modes of operation that have been successfully proven in practical operation'. Translation provided by Inter Nationes, available at https://germanlawarchive.iuscomp.org/?p=315, last accessed 202/01/24.

[15] § 3 sec. 6d BImschG.

In order to respond to requests for guidance and to achieve an overall high level of security, some national legislators allow for ministerial orders to set security rules that should fulfill the state of the art criterion[16] or for the national competent NIS authority to approve security standards for specific sectors suggested by operators of critical infrastructures and their industry associations[17]. As regards the latter, in Germany, the national competent NIS authority further issued a guide to the contents and requirements of security standards for specific sectors [6]. Soft law instruments or ministerial orders allow for timely updates and thus greater flexibility as there is no lengthy legislative process. However, where industry associations set security standards for specific sectors, this does not necessarily mean that there is transparency as to which criteria have been used to determine the level of state of the art [cf. 7 p. 8]. Realistically speaking, industry associations have an interest to have approved what they consider to be best practice. Best practice in turn does not necessarily have to amount to state of the art.

## 2 A Three-Step-Test to Determine State of the Art Technology

### 2.1 The Development of the Three-Step-Test

The abstention from defining state of the art is not unique to EU law. As already mentioned, national legislation is equally reluctant to provide a definition of state of the art within the meaning of technology in general and IT security legislation in particular.

Against this background, it is not surprising that as early as 1978 the German Constitutional Court had been confronted with determining state of the art in context of atomic energy.

In its Kalkar decision[18], the German Constitutional Court approached the question irrespective from the particular context. The Court located state of the art between the 'generally accepted rules of technology' ('allgemein anerkannte Regeln der Technik') and the 'state of science and technology' ('Stand der Wissenschaft und Technik').

The generally accepted rules of technology can be identified by determining the prevailing opinion among practitioners.[19] Generally accepted rules of technology require that a certain technology has stood the test of practice and is generally accepted amongst the majority of experts, however, it does not have to be the best technology available [8]. This notion derives historically from building/construction law and the notion of generally accepted rules of architecture describing the dominating opinion of technical experts. There is a (rebuttable) presumption that technical standards such as DIN-norms

[16] Cf. France: Art. 10 Décret no 2018-384 du 23 mai 2018 relatif à la sécurité des reseaux et sytèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique (Decree No. 1018-384 of 23 May 2018 on the security of the networks and information systems of critical service operators and digital service providers).

[17] Cf. Germany: § 8a Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) (Act on the Federal Office for information security).

[18] BVerGE 49, 89 (135 et seq.).

[19] Ibid.

amount to generally accepted rules [9]. In contrast, state of science and technology relates to a very high level of protection, that requires to take into account the latest scientific knowledge regardless of whether it is technically feasible and available [8] [10].[20]

Placing state of the art in between these two notions at normative level confirms the aforementioned finding that state of the art corresponds at least to the best technique available to the operator in question. The legal benchmark of what constitutes state of the art is thus shifted to the front of technical development, since general recognition and practical validation alone are not decisive for the state of the art of a technology.

### 2.2 The Dynamic Function of Technical Measures

What renders the determination of state of the art somehow 'tricky' is its dynamic function. Technical measures that today form part of the latest scientific knowledge may in no time become state of the art technology. State of the art state is regularly achieved when market maturity is reached and the technology is launched on the market. Equally the generally accepted rules may become outdated as their degree of innovation diminishes [7]. TeleTrust [7] summarises the innovative shift as follows:

'1. A measure will initially reach the "existing scientific knowledge and research" stage at its origin. 2. When introduced on the market, it will pass to the "state of the art" stage, 3. and as it is distributed and recognised more widely on the market, it will at some point be assigned to "generally accepted rules of technology." 4. if recognition is lost, this measure can no longer be used.'. Bearing in mind this product lifecycle, the border between state of the art and generally accepted rules of technology can be fluent and difficult to determine, meaning that a court or authority has to enter into technicians' controversies.

The dynamic nature also comes into play with regard to the aspect of when a technical measure has to amount to state of the art.

In the context of the GDPR, it has been argued [10] that data controllers are required to adapt their privacy measures regularly to advances in technology. The dynamic reference thus has the potential to enhance innovation, when data controllers are required to constantly adapt their protection measures [2]. In that regard Art. 25(1) GDPR requires that in the context of data protection by design or default, state of the art must be taken into account 'both at the time of the determination of the means for processing and at the time of processing itself'. Compliance with Art. 25 GDPR thus requires constant monitoring of the evolvement of state of the art which also needs to be taken into consideration by certification schemes. It has to be ensured that the certification body examines whether the data controller (or processor) keeps track with technological progress [2].

Although the NIS Directive lacks a determination of the time when state of the art must be taken into account, the ratio of the security provisions implies that the OESs or DSPS have to adapt the security measures to ensure a level of security of NIS appropriate to the risks posed.

[20] Cf. also BVerGE 49, 89 (135 et seq.).

### 2.3 The Objective Nature of the State of the Art Criterion and the Principle of Proportionality

As already indicated, the state of the art criterion is purely objective and does not take into account the individual means of the operator. State of the art can thus be described as 'the procedures, equipment or operating methods available in the trade in goods and services for which the application thereof is most effective in achieving the respective legal protection objectives' [11]. Accordingly, subjective elements such as high costs will justify a derivation from this. One may argue, that proprietary tools that are only offered by a single vendor to competitors under abusive conditions may not amount to methods that are 'available' in a strict sense. However, the state of the art criterion always has to be placed in context. Legal interventions commonly require that the technical measure that respects the state of the art is inter alia 'appropriate' (e.g. to the risks posed), 'proportionate to the cost of implementation', take into account the 'nature, scope, context and purpose of [data] processing' (GDPR) and/or risks. As regards for instance the NIS Directive, Recital 53 specifies that in order to avoid imposing a disproportionate financial and administrative burden on OESs and DSPs, the requirements should be proportionate to the risk presented by the NIS concerned. This is in line with the 'state of the art' requiring economically and technically feasible measures in corresponding legal interventions.

## 3 Conclusion

The determination of whether a particular technology amounts to state of the art can be a challenge for technicians and lawyers alike. The three-step-test introduced by the German Constitutional Court in the 1970s supports the translation from legal to technical requirements in that it clarifies the location of state of the art in between the highest innovative level of research and science and the generally accepted rules of technology which have stood the test of practice. This distinction takes into account the product lifecycle and the dynamic nature of technology. Due to the abstract nature of the three-step-test, i.e. that it is independent of the context, the test can be applied to all fields of technology. Further, the test is also feasible at the level of EU law.

Since the state of the art criterion in legal interventions is of an objective nature, the financial, administrative and technical means available to the individual operators are not to be considered in first place. Commonly the legal interventions will in that regard provide guidance as to what in terms of expenses, manpower etc. can be expected. Assessing state of the art in the context of a specific legal norm often also refers to appropriateness in terms of risk levels and thus has to be determined on a case-by-case basis. Data controllers (GDPR) and other addressees of the requirement of state of the art technology are advised to closely collaborate with regulators to determine appropriate measures.

**Acknowledgements.** The research for this article was funded by the Luxembourg National Research Fund (FNR) C18/IS/12639666/EnCaViBS/Cole[21].

## References

1. Martini, M.: Art. 25 DS-GVO, marginal no. 39a. In: Paal, B., Pauly, D. (eds.): DS-GVO BDSG. 3rd edn. Beck, München (2021).
2. Von Grafenstein, M.: Co-Regulation and the Competitive Advantage in the GDPR: Data Protection Certification Mechanisms, Codes of Conduct and the 'State of the Art' of Data Protection-by-Design. In: González Fuster, G., van Brakel, R., de Hert, P.: Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics, pp. 398–427. Edward Elgar Publishing (2022).
3. Schulte M., Michalk, K.: § 3 BImSchG marginal no. 98. In: Giesberts, L., Reinhardt, M. (eds.): BeckOK Umweltrecht. 57th edn. Beck, München (2020).
4. Deutscher Bundestag, BT-Drs. 14/4599, p. 126.
5. Deutscher Bundestag, BT-Drs. 17/8125, p. 3.
6. BSI: Orientierungshilfe zu Inhalten und Anforderungen an branchenspezifische Sicherheitsstandards (B3S) gemäß § 8a Absatz 2 BSIG, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/b3s_orientierungshilfe.pdf?__blob=publicationFile&v=4, last accessed 2022/01/24.
7. IT Security Association Germany (TeleTrust) in co-operation with ENISA: IT Security Act (Germany) and EU General Data Protection Regulation: Guideline "State of the art", Technical and organizational measures (2021), https://www.teletrust.de/fileadmin/user_upload/2021-09_TeleTrusT_Guideline_State_of_the_art_in_IT_security_EN.pdf, last accessed 2022/01/26.
8. Jarass, H.: § 3 BImSchG, marginal no. 115. In: Jarasss, H. (ed.): BImSchG, Bundes-Immissionsschutzgesetz. 13th edn.Beck, München (2020).
9. Seibel, M.: Abgrenzung der "allgemein anerkannten Regeln der Technik" vom „Stand der Technik". In: NJW, pp. 3000 – 3004 (2013).
10. Martini, M.: Art. 25 DS-GVO, marginal no. 39d. In: Paal, B., Pauly, D. (eds.): DS-GVO BDSG. 3rd edn. Beck, München (2021).
11. Bartels, K., Backer, M.: Die Berücksichtigung des Stands der Technik in der DSGVO. In: DuD, pp. 214 – (2018).

[21] https://www.fnr.lu/projects/the-eu-nis-directive-enhancingcybersecurity-across-vital-business-sectors-encavibs/