UM SISTEMA DE SAÚDE DIGITAL NA ALEMANHA – CIBERSEGURANÇA, PROTEÇÃO DE DADOS E INTELIGÊNCIA ARTIFICIAL[1]

A DIGITAL HEALTHCARE SYSTEM IN GERMANY – CYBERSECURITY, DATA PROTECTION AND ARTIFICIAL INTELLIGENCE

Sebastian Bretthauer

Professor de Direito Público na Universidade EBS, em Wiesbaden, Alemanha. Assistente acadêmico da Profª. Drª. Inda Spiecker gen. Döhmann na Universidade Goethe de Frankfurt a.M. Diretor de Projetos no Instituto de Pesquisa sobre Proteção de Dados na mesma universidade. Colaborador do Instituto de Política de Saúde e Direito Social na Europa (ineges). sebastian.bretthauer@ebs.edu.

Resumo: A digitalização do setor da saúde é um dos desafios centrais do presente e do futuro. Ela afeta todos os atores do sistema de saúde e, portanto, nada menos que 82 milhões de pessoas na Alemanha que se beneficiam de um sistema de saúde moderno e sustentável. Há algum tempo o legislador nacional vem fazendo esforços consideráveis para enquadrar juridicamente os desafios associados a essa questão. Numerosas leis abordam a digitalização e temas específicos ligados a ela, como o reforço da cibersegurança, a proteção de dados na pesquisa com dados de saúde ou a utilização de inteligência artificial na avaliação de dados de saúde. O artigo oferece uma visão geral das regulamentações mais importantes e as toma como ensejo para uma análise jurídica crítica.

Palavras-chave: Direito à saúde. Proteção de dados pessoais. Inteligência artificial.

Abstract: The digitization of the healthcare sector is one of the central challenges of the present and future. It affects all actors in the healthcare system and, therefore, no less than 82 million people in Germany who benefit from a modern and sustainable healthcare system. For some time now, the legislator has been making considerable efforts to legally frame the associated challenges. Numerous laws address digitization and specific topics related to it, such as strengthening cybersecurity, protecting data in health data research, and the use of artificial intelligence in health data evaluation. The article provides an overview of the most important regulations and uses them as a basis for a critical legal analysis.

Keywords: Right to health. Personal data protection. Artificial intelligence.

[1] Tradução de Luiz Sander e revisão de Hannah Alff. Este artigo se baseia substancialmente em duas publicações do autor (Bretthauer, NVwZ, no prelo, e Bretthauer, *Die Verwaltung*, v. 54, p. 411 ss., 2021). A presente publicação conta com o apoio financeiro do Conselho Nacional de Desenvolvimento Científico e Tecnológico – CNPq, Chamada MCTIC/CNPq nº 28/2018 – Universal/Faixa C Processo: 433383/2018-6.

A Introdução

A digitalização do sistema de saúde vem sendo impulsionada no direito alemão por numerosas leis novas, muitas vezes muito extensas e difíceis de compreender. Desde 2016, o legislador federal alemão aprovou pelo menos sete desses conjuntos de regras. Estas incluem, entre outras, a Lei E-Health ou Lei da Saúde Digital,[2] a Lei do Atendimento Médico Digital,[3] a Lei da Proteção de Dados dos Pacientes,[4] a Lei do Futuro Hospitalar[5] e a Lei da Modernização do Atendimento e dos Cuidados Digitais.[6] Com a Lei Digital[7] e a Lei da Utilização de Dados de Saúde,[8] foram aprovados, em fins de 2023, mais dois conjuntos centrais de regras para acelerar a digitalização do sistema de saúde.

A Lei da Saúde Digital, que regulamenta a introdução de aplicações médicas digitais no sistema de saúde pela substituição de processos baseados em papel,[9] definiu fundamentalmente as balizas para um sistema de saúde digitalizado. Com a Lei de Atendimento Médico Digital, o governo federal promulgou amplas medidas para melhorar o atendimento aos segurados de planos de saúde, que visam, especialmente, introduzir rapidamente aplicativos digitais de saúde no atendimento, simplificar os processos administrativos por meio da digitalização e possibilitar

2 BUNDESGESETZBLATT. *Bundesgesetzblatt Teil I* [= Diário Oficial Federal]. Disponível em: https://www.recht.bund.de/de/bundesgesetzblatt/bgbl-1/bgbl-1_node.html. Acesso em: 10 jul. 2024. p. 2408.

3 BUNDESGESETZBLATT. *Bundesgesetzblatt Teil I* [= Diário Oficial Federal]. Disponível em: https://www.recht.bund.de/de/bundesgesetzblatt/bgbl-1/bgbl-1_node.html. Acesso em: 10 jul. 2024. p. 2562.

4 BUNDESGESETZBLATT. *Bundesgesetzblatt Teil I* [= Diário Oficial Federal]. Disponível em: https://www.recht.bund.de/de/bundesgesetzblatt/bgbl-1/bgbl-1_node.html. Acesso em: 10 jul. 2024. p. 2115.

5 BUNDESGESETZBLATT. *Bundesgesetzblatt Teil I* [= Diário Oficial Federal]. Disponível em: https://www.recht.bund.de/de/bundesgesetzblatt/bgbl-1/bgbl-1_node.html. Acesso em: 10 jul. 2024. p. 1454, 1469.

6 BUNDESGESETZBLATT. *Bundesgesetzblatt Teil I* [= Diário Oficial Federal]. Disponível em: https://www.recht.bund.de/de/bundesgesetzblatt/bgbl-1/bgbl-1_node.html. Acesso em: 10 jul. 2024. p. 1309.

7 DEUTSCHER BUNDESTAG. *Entwurf eines Gesetzes zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG) 20/9048*. [Publicações do Parlamento Federal] n. 20/9048. 2023.

8 DEUTSCHER BUNDESTAG. *Entwurf eines Gesetzes zur verbesserten Nutzung von Gesundheitsdaten (Gesundheitsdatennutzungsgesetz – GDNG) 20/9046*. [Publicações do Parlamento Federal] n. 20/9046. 2023.

9 DEUTSCHER BUNDESTAG. *Entwurf eines Gesetzes für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen 18/5293*. [Publicações do Parlamento Federal] n. 18/5293. 2015. p. 1 s.

um melhor aproveitamento dos dados de saúde para fins de pesquisa.[10] A Lei da Proteção de Dados dos Pacientes, por sua vez, fortalece a configuração do prontuário eletrônico dos pacientes, fazendo com que, entre outras coisas, ocorra seu emprego específico no tocante ao conteúdo e uso, bem como às autorizações de processamento e à concepção e acesso, seja aumentada a dinâmica na introdução das aplicações médicas da infraestrutura telemática através de incentivos e prazos vinculantes e sejam regulamentados de maneira diferenciada o processamento de dados e as responsabilidades jurídicas pela proteção de dados na infraestrutura telemática, no que diz respeito às normas de proteção de dados.[11] A Lei do Futuro Hospitalar promove a digitalização e o uso de equipamentos tecnologicamente modernos nos hospitais.[12] Com a Lei da Modernização do Atendimento e dos Cuidados Digitais, expande-se o atendimento médico, com aplicações digitais, e se ampliam as estruturas e ofertas já criadas.[13] Por último, a Lei da Utilização de Dados de Saúde atualiza principalmente o marco jurídico para o intercâmbio e a utilização de dados de saúde para um atendimento de alta qualidade e, neste sentido, aborda particularmente a área da utilização secundária de dados de saúde,[14] enquanto o objeto da Lei Digital consiste principalmente em promover a utilização de aplicações digitais e, neste sentido, enfatiza especialmente o aspecto da facilidade de uso e a segurança.[15]

Este artigo enfoca três desdobramentos selecionados que ilustram o avanço da digitalização no setor de saúde alemão. Para este fim, ele examina a Lei Digital aprovada em fins de 2023 com suas novas regras sobre interoperabilidade e cibersegurança (B), a Lei do Atendimento Médico Digital e a Lei da Proteção de Dados dos Pacientes com suas normas sobre proteção de dados na pesquisa de dados de saúde (C), bem como a proposta de regulamentação da Comissão

[10] DEUTSCHER BUNDESTAG. *Entwurf eines Gesetzes für eine bessere Versorgung durch Digitalisierung und Innovation (Digitale-Versorgung-Gesetz – DVG) 19/13438*. [Publicações do Parlamento Federal] n. 19/13438. 2015. p. 2.

[11] DEUTSCHER BUNDESTAG. *Entwurf eines Gesetzes für eine bessere Versorgung durch Digitalisierung und Innovation (Digitale-Versorgung-Gesetz – DVG) 19/18793*. [Publicações do Parlamento Federal] n. 19/18793. 2020. p. 2.

[12] DEUTSCHER BUNDESTAG. *Entwurf eines Gesetzes für ein Zukunftsprogramm Krankenhäuser (Krankenhauszukunftsgesetz – KHZG) 19/22126*. [Publicações do Parlamento Federal] n. 19/22126. 2020. p. 1.

[13] DEUTSCHER BUNDESTAG. *Entwurf eines Gesetzes zur digitalen Modernisierung von Versorgung und Pflege (Digitale-Versorgung-und-Pflege-Modernisierungs-Gesetz – DVPMG) 19/27652*. [Publicações do Parlamento Federal] n. 19/27652. 2021. p. 2.

[14] DEUTSCHER BUNDESRAT. *Entwurf eines Gesetzes zur verbesserten Nutzung von Gesundheitsdaten (Gesundheitsdatennutzungsgesetz – GDNG) 434/23*. [Publicações do Parlamento Federal] n. 434/23. 2023. p. 1 ss.

[15] DEUTSCHER BUNDESRAT. *Entwurf eines Gesetzes zur verbesserten Nutzung von Gesundheitsdaten (Gesundheitsdatennutzungsgesetz – GDNG) 434/23*. [Publicações do Parlamento Federal] n. 434/23. 2023. p. 1.

Europeia de Inteligência Artificial com suas regras para a utilização de inteligência artificial na avaliação de dados de saúde (D). O artigo termina com uma conclusão e perspectivas (E).

B Cibersegurança e interoperabilidade no sistema de saúde

Em dezembro de 2023, o Parlamento Federal aprovou a Lei da Aceleração da Digitalização do Sistema de Saúde (DigiG, na sigla em alemão).[16] A DigiG pretende promover a utilização de aplicações digitais e dar especial ênfase ao aspecto da facilidade de utilização e segurança.[17] Isto diz respeito, em particular, à melhoria da interoperabilidade através da centralização e da procedimentalização, bem como ao aumento da cibersegurança pelo fortalecimento da consciência da segurança por parte dos usuários da tecnologia.

I Melhoria da interoperabilidade

Um sistema de saúde moderno e digitalizado só poderá ter sucesso se se garantir a interoperabilidade dos sistemas de informação nele implicados,[18] pois uma troca de informações eficiente e eficaz entre os atores envolvidos é um pressuposto básico para um sistema de saúde funcional que esteja a serviço do bem-estar dos segurados e dos pacientes.

1 Carência de regulamentação necessária devido à fragmentação pregressa

As normas até agora em vigor para a interoperabilidade dos sistemas de tecnologia da informação[19] no sistema da saúde se encontravam em diferentes

[16] DEUTSCHER BUNDESRAT. *Entwurf eines Gesetzes zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG) 435/23*. [Publicações do Parlamento Federal] n. 435/23. 2023.

[17] DEUTSCHER BUNDESRAT. *Entwurf eines Gesetzes zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG) 435/23*. [Publicações do Parlamento Federal] n. 435/23. 2023. p. 1.

[18] DEUTSCHER BUNDESRAT. *Entwurf eines Gesetzes zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG) 435/23*. [Publicações do Parlamento Federal] n. 435/23. 2023. p. 3.

[19] Cf., quanto ao conceito, BVerfGE [*Entscheidungen des Bundesverfassungsgerichts* = Decisões do Tribunal Constitucional Federal]: BUNDESVERFASSUNGSGERICHT. *BVerfGE*: Entscheidungen des

passagens do Código Social V,[20] eram distribuídas entre diferentes atores e havia uma total falta de normas uniformes para a implementação dos requisitos.[21] A isso se acrescentavam uma coordenação insuficiente, ausência de uma priorização abrangente de especificações e fragmentação excessiva de competências com um grande número de atores diferentes no sistema de saúde.[22] Isto resultou, inevitavelmente, em incompatibilidades, contradições e especificações múltiplas, bem como em diferenças de qualidade nos respectivos sistemas de tecnologia da informação. Com as novas regulamentações nos §§385-388 e seguintes do SGB V, pretende-se agora enfrentar e delimitar esses problemas. Por isso, as regulamentações preveem diversas medidas para melhorar a interoperabilidade.

2 Reforço do Centro de Competência em Interoperabilidade

Inicialmente, o §385 do SGB V define de forma abrangente as tarefas do Centro de Competência em Interoperabilidade no sistema de saúde montado junto à Sociedade de Telemática (gematik) (§385, 1 do SGB V). Com o Centro de Competência, cria-se uma agência central para coletar, agrupar e priorizar necessidades de padronização ou desenvolvimento de interfaces.[23] Assim, ao Centro de Competência são atribuídas tarefas como identificar e priorizar a necessidade de padrões técnicos, semânticos e sintáticos, perfis e diretrizes (§385, 1, 2, n. 1 do SGB V), recomendá-los para áreas específicas ou para todo o sistema de saúde (§385, 1, 2, n. 3 do SGB V) e também para desenvolvê-los por conta própria (§385, 1, 2, n. 6 do SGB V), verificar a concordância com os requisitos de interoperabilidade através da avaliação de conformidade de acordo com o §387 do SGB V (§385, 1, 2, n. 7 do SGB V), acompanhar comunicacionalmente as tarefas do Centro de

Bundesverfassungsgerichts. [Decisões do Tribunal Constitucional Federal], 120, 274-350. Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227_1bvr037007.html. Acesso em: 07 jul. 2024.

[20] O Código da Segurança Social (*Sozialgesetzbuch*, SGB, na sigla em alemão) é a codificação do Direito Social. Ele está subdividido em uma parte geral (SGB I) e 13 outros livros. O SGB V contém normas sobre a obrigatoriedade do seguro de saúde e serviços dos planos de saúde regulamentados por lei, bem como suas relações jurídicas com outros prestadores de serviços (médicos, dentistas, farmacêuticos etc.).

[21] DEUTSCHER BUNDESRAT. *Entwurf eines Gesetzes zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG) 435/23*. [Publicações do Parlamento Federal] n. 435/23. 2023. p. 151.

[22] DEUTSCHER BUNDESRAT. *Entwurf eines Gesetzes zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG) 435/23*. [Publicações do Parlamento Federal] n. 435/23. 2023. p. 151.

[23] DEUTSCHER BUNDESRAT. *Entwurf eines Gesetzes zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG) 435/23*. [Publicações do Parlamento Federal] n. 435/23. 2023. p. 151.

Competência com recursos de relações públicas (§385, 1, 2, n. 8 do SGB V) e apoiar o Governo Federal no marco de projetos e comitês para promover a interoperabilidade no sistema de saúde em nível federal e europeu (§385, 1, 2, n. 9 do SGB V). A criação e organização do Centro de Competência, bem como do Comitê de Especialistas por ele instituído, são regulamentadas concretamente por portaria administrativa sem o consentimento do Conselho Federal (§385, 1, 1 do SGB V).

Portanto, no futuro, o Centro de Competências assumirá uma função diretiva central na área da interação digital dos numerosos atores no sistema de saúde. Ele deve resumir e coordenar os diferentes requisitos dos atores na esfera da saúde e, com base nisso, rever as interfaces e normas necessárias e estruturar mais concretamente os requisitos de interoperabilidade.[24] Nesse sentido, as especificações devem se basear em normas internacionais abertas, a fim de que, já de início, uma conexão com o espaço europeu de dados de saúde[25] seja garantida.[26] No tocante aos detalhes estruturais, o regulamento não é muito preciso porque os requisitos específicos só são definidos em uma portaria administrativa. O quadro de pessoal do Centro de Competência não fica claro. Uma definição mais precisa de quais atores devem ser incluídos e do número de pessoas envolvidas deveria ocorrer, pelo menos, no marco de um processo legislativo formal.[27] Em todo, pelo menos a portaria deve conter pelo menos normas detalhadas sobre quais especialidades estão representados no Centro de Competência e no Comitê de Especialistas criado, para que se garanta que as pessoas atuantes no Centro de Competência representem as respectivas particularidades setoriais com base na experiência.[28] No entanto, o cumprimento destas extensas tarefas só pode ser bem-sucedido

[24] Posição crítica quanto a isso se encontra em GEMATIK. *Stellungnahme der gematik zum Referentenentwurf eines Gesetzes zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG).* Disponível em: https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/Gesetze_und_Verordnungen/Stellungnahmen_WP20/DigiG/stellungnahme_gematik.pdf. Acesso em: 07 jul. 2024, já que não se devem prescrever os padrões ou normas, e sim criar estímulos para sua utilização.

[25] Cf., quanto a isso, EUROPEAN COMISSION. *European Health Data Space*. Disponível em: https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en. Acesso em: 10 jul. 2024.

[26] Essa é também a posição de GEMATIK. *Stellungnahme der gematik zum Referentenentwurf eines Gesetzes zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG).* Disponível em: https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/Gesetze_und_Verordnungen/Stellungnahmen_WP20/DigiG/stellungnahme_gematik.pdf. Acesso em: 07 jul. 2024.

[27] Essa já era a posição de BITKOM. *Stellungnahme zum Referentenentwurf eines Gesetzes zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz).* Berlin, 2023. Disponível em: https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/Gesetze_und_Verordnungen/Stellungnahmen_WP20/DigiG/stellungnahme_bitkom.pdf. Acesso em: 10 jul. 2024.

[28] KASSENÄRTZLICHE BUNDESVEREINIGUNG. *Entwurf eines gesetzes zur beschleunigung der digitalisierung des gesundheitswesens (Digital-Gesetz – DIGIG).* Disponível em: https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/Gesetze_und_Verordnungen/Stellungnahmen_WP20/DigiG/stellungnahme_kbv.pdf. Acesso em: 10 jul. 2024.

se se disponibilizarem para o Centro de Competência os recursos de pessoal e materiais necessários para realizar eficazmente sua tarefa.

3 Requisitos para a circulação de sistemas de tecnologia da informação

O §388 do SGB V regulamenta os requisitos para a circulação de sistemas de tecnologia da informação no sistema de saúde que processam dados pessoais de saúde. Assim, a partir de 1º.1.2025, só poderão ser colocados em circulação sistemas que cumpram os requisitos vinculativos de interoperabilidade (§388, 1 do SGB V). O que entra em cogitação na área ambulatorial são sistemas de gestão de consultórios e sistemas de informação clínica no setor de internação.[29] Contudo, estão isentos da necessidade de uma avaliação de conformidade os sistemas que forem desenvolvidos no marco da pesquisa científica, para fins de utilidade pública ou por entidades jurídicas de direito público no cumprimento de uma incumbência legal (§388, 2 do SGB V). Finalmente, pode ser requisitado a omitir-se de colocar em circulação o produtor ou fornecedor que viole as obrigações de avaliação da conformidade (§388, 3 do SGB V).

O sistema de tecnologia da informação como referência de tipicidade ou suporte fático acarreta uma esfera de aplicação muito ampla da norma, de modo que *wearables* e aplicativos de saúde também são abrangidos por ela.[30] Por razões de esclarecimento e delimitação da norma, algumas definições mais precisas são necessárias neste ponto, p. ex., mediante a inclusão de exemplos-padrão. Além disso, é preciso esclarecer o que acontece com produtos que já estejam no mercado, pois a colocação em circulação designa a disponibilização de um produto, com exceção de produtos de teste, pela primeira vez no mercado da União.[31] Deve-se,

[29] DEUTSCHER BUNDESRAT. *Entwurf eines Gesetzes zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG) 435/23*. [Publicações do Parlamento Federal] n. 435/23. 2023. p. 162.

[30] GEMATIK. *Stellungnahme der gematik zum Referentenentwurf eines Gesetzes zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG)*. Disponível em: https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/Gesetze_und_Verordnungen/Stellungnahmen_WP20/DigiG/stellungnahme_gematik.pdf. Acesso em: 07 jul. 2024.

[31] Art. 2, nº 28, UNIÃO EUROPEIA. *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 (Text with EEA relevance.)*. Disponível em: https://eur-lex.europa.eu/eli/reg/2017/745/oj. Acesso em: 30 jun. 2024.

portanto, acrescentar igualmente um esclarecimento no sentido de que isto também inclui produtos que já foram disponibilizados no mercado.[32]

Para atingir o objetivo da interoperabilidade abrangente, é imperativo reforçar os mecanismos vinculativos,[33] embora a regulamentação possa levar a restrições de mercado e, assim, processos de inovação sejam impedidos.[34]

Ainda que a regulamentação da interoperabilidade afete a liberdade de exercício da profissão (§12º, n. 1 da Lei Fundamental [GG, na sigla em alemão]) dos produtores de TI e fornecedores de tais sistemas,[35] a obrigação de avaliar a conformidade é necessária e adequada, levando-se em conta a grande importância de uma interoperabilidade efetivamente funcional dos sistemas de TI disponibilizados para o sistema de saúde e para a tutela dos bens juridicamente protegidos dos pacientes.[36] É adequada, antes de mais nada, porque deve haver uma troca sem problemas de informações entre todos os sistemas permitidos e esta é a única maneira de salvaguardar o direito dos segurados e dos pacientes a que os seus dados sejam divulgados em um formato interoperável.[37] Por meio dos padrões unificados para a garantia da interoperabilidade, impulsionam-se o desenvolvimento de um sistema de saúde moderno e digitalizado. Ao mesmo tempo, assegura-se que o direito à transmissão de dados (cf. §386, 2, 2 do SGB V) possa ser exercido adequadamente. Além disso, também é preciso criar a interoperabilidade porque os mecanismos pregressos não levaram à promoção da interoperabilidade necessária.[38]

---

[32] Posição igual em BITKOM. *Stellungnahme zum Referentenentwurf eines Gesetzes zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz)*. Berlin, 2023. Disponível em: https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/Gesetze_und_Verordnungen/Stellungnahmen_WP20/DigiG/stellungnahme_bitkom.pdf. Acesso em: 10 jul. 2024.

[33] Art. 2, n. 28, UNIÃO EUROPEIA. *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 (Text with EEA relevance.)*. Disponível em: https://eur-lex.europa.eu/eli/reg/2017/745/oj. Acesso em: 30 jun. 2024.

[34] Essa é a posição, p. ex., de DEUTSCHE KRANKENHAUSGESELLSCHAFT. *Branchenspezifischer Sicherheitsstandard "Medizinische Versorgung"*. Version 1.2, 2022. Disponível em: https://www.dkgev.de/fileadmin/default/Mediapool/2_Themen/2.1_Digitalisierung_Daten/2.1.4._IT-Sicherheit_und_technischer_Datenschutz/2.1.4.1._IT-Sicherheit_im_Krankenhaus/Branchenspezifischer_Sicherheitsstandard_Medizinische_Versorgung_v1.2_Stand_2022-12-08.pdf. Acesso em: 07 jul. 2024. p. 25.

[35] DEUTSCHER BUNDESRAT. *Entwurf eines Gesetzes zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG) 435/23*. [Publicações do Parlamento Federal] n. 435/23. 2023. p. 162.

[36] Essa é também a posição que se encontra em DEUTSCHER BUNDESRAT. *Entwurf eines Gesetzes zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG) 435/23*. [Publicações do Parlamento Federal] n. 435/23. 2023. p. 162.

[37] DEUTSCHER BUNDESRAT. *Entwurf eines Gesetzes zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG) 435/23*. [Publicações do Parlamento Federal] n. 435/23. 2023. p. 163.

[38] DEUTSCHER BUNDESRAT. *Entwurf eines Gesetzes zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG) 435/23*. [Publicações do Parlamento Federal] n. 435/23. 2023. p. 163.

Medidas menos incisivas em termos de intervenção, que se baseiam, em particular, em compromissos voluntários por parte dos produtores e fornecedores de TI, não levaram, ao menos até agora, ao sucesso desejado. Aliás, uma potencial autodeclaração sobre o cumprimento de normas se revela inadequada, devido à pluralidade de motivos de produtores e fornecedores.[39] Por isso, um processo centralizado e procedimentalizado para produzir a interoperabilidade é apropriado para expandir ainda mais um sistema de saúde moderno e digitalizado.

4 Procedimentos de avaliação da conformidade

O disposto no §387 do SGB V obriga o Centro de Competência ou outro órgão credenciado[40] (cf. §385, 8 do SGB V) a realizar uma avaliação de conformidade a pedido de um produtor ou fornecedor de sistemas de TI que serão usados no setor de saúde e a verificar se o sistema está em conformidade com os requisitos de interoperabilidade vigentes (§387, 1 do SGB V). No procedimento de conformidade se constata se os requisitos de interoperabilidade relevantes em cada caso para um sistema de TI são cumpridos (§384, n. 8 do SGB V). Trata-se de um procedimento extenso e, em particular, de caráter muito técnico, cujas origens residem na legislação sobre segurança dos produtos.[41]

Até agora existiam vários procedimentos para verificar o cumprimento das normas de interoperabilidade para sistemas de TI no setor da saúde. Assim, por exemplo, a Associação Federal dos Planos de Saúde (KBV, na sigla em alemão) realizava as certificações para sistemas de gestão de consultórios e a Sociedade de Telemática, as certificações para sistemas de IT em hospitais.[42] Agora, com o Centro de Competência, cria-se um órgão central e a fragmentação pregressa é neutralizada. Após a conclusão do procedimento, o Centro de Competência apresenta um relatório do teste, de modo que o requerente possa corrigir os erros caso o resultado do teste seja negativo; caso contrário, emite-se um certificado de exame positivo (§387, 3 do SGB V).

[39] DEUTSCHER BUNDESRAT. *Entwurf eines Gesetzes zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG) 435/23*. [Publicações do Parlamento Federal] n. 435/23. 2023. p. 163.

[40] Este atua, via de regra, como contratado ou terceirizado. Cf. DEUTSCHER BUNDESRAT. *Entwurf eines Gesetzes zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG) 435/23*. [Publicações do Parlamento Federal] n. 435/23. 2023. p. 158.

[41] Cf. Diretiva 2001/95/CE do Parlamento Europeu e do Conselho, de 3 de dezembro de 2001, relativa à segurança geral dos produtos.

[42] DEUTSCHER BUNDESRAT. *Entwurf eines Gesetzes zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG) 435/23*. [Publicações do Parlamento Federal] n. 435/23. 2023. p.160.

O procedimento de avaliação da conformidade implica padrões uniformes para os sistemas de TI utilizados no setor da saúde e, portanto, também uma comparabilidade desses sistemas. No entanto, esforços adicionais se fazem necessários porque tal procedimento muitas vezes ainda não existe em certos setores – como na área dos planos de saúde odontológicos.[43] Nessas áreas, o procedimento de conformidade ainda precisa ser implementado. Contudo, os requisitos específicos dos respectivos atores precisam sempre ser levados em conta porque as soluções clássicas do tipo *one-size-fits-all* (de tamanho único) não podem ser eficazes em um mercado tão heterogêneo.

5 Direito à interoperabilidade

Por fim, o §386 do SGB V normatiza pela primeira vez um direito à interoperabilidade. Este direito é muito semelhante ao direito ao acesso e à informação, proveniente do direito referente aos dados pessoais, bem como ao direito à portabilidade dos dados.[44] Os segurados têm direito à divulgação de seus dados pessoais (cf. §386, 2, 1 do SGB V) em relação aos prestadores de serviços ou responsáveis pelo processamento de dados de um aplicativo da área de saúde (cf. §33a do SGB V) ou um de aplicativo digital da área de assistência ou cuidados de saúde (cf. §40a do SGB XI) e também podem exigir que os dados pessoais de saúde armazenados sejam transmitidos diretamente entre os atores de saúde envolvidos (§386, 2, 2 do SGB V). O direito à portabilidade de dados, que foi juridicamente consagrado pela primeira vez no artigo 20º do Regulamento Geral de Proteção de Dados (RGPD), é um elemento ainda recente e particularmente moderno de regulamentação jurídica e representa interconexões entre a proteção de dados, a defesa do consumidor e o direito da concorrência.[45] Para fazer valer esses direitos basta uma simples

[43] KASSENÄRTZLICHE BUNDESVEREINIGUNG. *Entwurf eines gesetzes zur beschleunigung der digitalisierung des gesundheitswesens (Digital-Gesetz – DIGIG)*. Disponível em: https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/Gesetze_und_Verordnungen/Stellungnahmen_WP20/DigiG/stellungnahme_kbv.pdf. Acesso em: 10 jul. 2024. p. 9.

[44] Há uma exposição extensa sobre o direito à portabilidade dos dados em FIX, Alexander Daniel. *Das Recht auf Datenportabilität*: Art. 20 DSGVO als Schnittstelle zwischen Wettbewerbsförderung und Datenschutz. Peter Lang: Berlim, 2022.

[45] Essa posição quanto ao Art. 20º do RGPD se encontra em Simitis; Hornung; Spiecker gen. Döhmann; Dix, *Datenschutzrecht*, 2019, Art. 20, Rn. 1; Jülicher; Röttgen; von Schönfeld, ZD, 2016, 358 (360); posição crítica em Kühling; Martini, EuZW, 2016, 448 (450 s.) e Dehmel; Hullen, ZD, 2013, 147 (153), que contestam a relação do direito à portabilidade de dados com o Direito de proteção de dados.

solicitação em forma de texto, sendo desnecessária uma justificativa.[46] Em todo, um pedido transmitido verbalmente durante uma consulta do paciente não é suficiente.[47]

A regulamentação serve para fortalecer a soberania e a autodeterminação dos segurados e reforça seu direito a seus dados.[48] Ela consagra, assim, na legislação ordinária, o postulado do princípio da soberania dos dados dos pacientes no sistema de saúde.[49] Por isso, a transparência e o controle como expressão da autodeterminação informacional[50] são imprescindíveis também na melhoria da interoperabilidade. Neste sentido, é responsabilidade dos planos de saúde apoiar os segurados no acompanhamento de suas reivindicações (§386, 4 do SGB V), pois o desequilíbrio de poder existente entre os prestadores de serviços e os segurados em detrimento destes últimos pode ter um efeito dissuasório para fazer valer seus direitos.[51] A pessoa que tema ficar sujeita a riscos ou desvantagens em consequência do exercício de seus direitos pode optar por abrir mão disso. Entretanto, isto não afeta apenas a liberdade de desenvolvimento do indivíduo, mas também o bem comum, porque a autodeterminação é uma condição elementar para o funcionamento de uma coletividade livre e democrática baseada na capacidade de ação e participação de seus cidadãos.[52] Portanto, as seguradoras de saúde devem apoiar, como serviço prestado gratuitamente, os segurados no exercício de seus

[46] DEUTSCHER BUNDESRAT. *Entwurf eines Gesetzes zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG) 435/23*. [Publicações do Parlamento Federal] n. 435/23. 2023. p. 159.

[47] DEUTSCHER BUNDESRAT. *Entwurf eines Gesetzes zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG) 435/23*. [Publicações do Parlamento Federal] n. 435/23. 2023. p. 159.

[48] DEUTSCHER BUNDESRAT. *Entwurf eines Gesetzes zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG) 435/23*. [Publicações do Parlamento Federal] n. 435/23. 2023. p. 159.

[49] Quanto à questão da soberania sobre os dados no sistema de saúde, cf. KELBER, Ulrich. Datensouveränität und Digitalisierung. *Soziale Sicherheit*, n. 3, 2022. p. 107; BRETTHAUER, Sebastian; APPENZELLER, Arno; BIRNSTILL, Pascal. Datensouveränität für Patienten im Gesundheitswesen: Eine Chance für die medizinische Forschung und den Datenschutz. *Datenschutz und Datensicherheit (DuD)*, v. 45, n. 3, p. 173-179, 2021. p. 173; *Kolb; Robers, Zeitschrift für Verwaltung, 2021, 405*; THÜSING, Gregor; ROMBEY, Sebastian. Forschung im Gesundheitswesen: Anforderungen an einen passgenauen Datenschutz. *Neue Zeitschrift für Sozialrecht*, p. 201-205, 2019. p. 201-204; detalhes também em DEUTSCHER ETHIKRAT. *Big Data und Gesundheit*: Datensouveränität als informationelle Freiheitsgestaltung. 2018. Disponível em: https://www.ethikrat.org/fileadmin/Publikationen/Stellungnahmen/deutsch/stellungnahme-big-data-und-gesundheit.pdf. Acesso em: 07 jul. 2024.

[50] BRETTHAUER, Sebastian; APPENZELLER, Arno; BIRNSTILL, Pascal. Datensouveränität für Patienten im Gesundheitswesen: Eine Chance für die medizinische Forschung und den Datenschutz. *Datenschutz und Datensicherheit (DuD)*, v. 45, n. 3, p. 173-179, 2021. p. 173-174.

[51] DEUTSCHER BUNDESRAT. *Entwurf eines Gesetzes zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG) 435/23*. [Publicações do Parlamento Federal] n. 435/23. 2023. p.159.

[52] Essa já era a posição que se encontra em BUNDESVERFASSUNGSGERICHT. *BVerfGE, 65, 1 (43)*. Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1983/12/rs19831215_1bvr020983.html. Acesso em: 12 jul. 2024.

direitos e podem solicitar elas próprias a divulgação dos dados.[53] Neste tocante, seria coerente formular a regulamentação não apenas como um desiderato (§386, 4, 2 do SGB V), mas também obrigar os planos a prestar apoio, pois, de acordo com a regulamentação em vigor, as seguradoras de saúde podem, ao menos, abster-se de prestar apoio se houver um motivo importante ou em casos avulsos atípicos. Isto se aplica especialmente a situações em que o exercício do direito à interoperabilidade venha a ocorrer de maneira abusiva,[54] o que já parece merecer discussão em casos de solicitações repetidas.

6 Conclusão provisória

O objetivo da Lei Digital de promover e assegurar a interoperabilidade dos sistemas de TI necessários no sistema da saúde é amplamente alcançado através de uma forte centralização e procedimentalização. O Centro de Competência para a Interoperabilidade é, como ator principal, responsável por garantir sistemas de TI interoperáveis. Com isto se faz frente à fragmentação pregressa nessa área. Por meio do procedimento de avaliação da conformidade regulamentado por lei, cria-se mais transparência e rastreabilidade no setor da saúde, porque os produtores e fornecedores de TI precisam cumprir os requisitos relevantes. Da mesma maneira, a uniformização também fortalece a concorrência entre produtores e fornecedores de TI, porque eles podem otimizar e oferecer seus produtos dentro dos limites dos requisitos legais sobre segurança de TI. Por fim, sobretudo os direitos dos pacientes e dos segurados são substancialmente reforçados pelo direito à interoperabilidade, embora a adequação prática desse direito ainda precise de ser demonstrada.[55]

[53] DEUTSCHER BUNDESRAT. *Entwurf eines Gesetzes zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG) 435/23*. [Publicações do Parlamento Federal] n. 435/23. 2023. p. 159; posição crítica quanto a isso em DEUTSCHE KRANKENHAUSGESELLSCHAFT. *Stellungnahme der Deutschen Krankenhausgesellschaft zum Referentenentwurf eines Gesetzes zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz)*. 2023. Disponível em: https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/Gesetze_und_Verordnungen/Stellungnahmen_WP20/DigiG/stellungnahme_dkg.pdf. Acesso em: 07 jul. 2024, porque a normatização da prestação do serviço significa o estabelecimento e a manutenção de processos tecnológicos dispendiosos cuja frequência de utilização não pode ser percebida.

[54] STELKENS, Paul; BONK, Heiz Joachim; SACHS, Michael. *VwVfG*: Verwaltungsverfahrengesetz. 10 ed. München: C.H. Beck, 2023. §40, nota de rodapé 27; SCHOCH, Friedrich; SCHNEIDER, Jens-Peter. *Verwaltungsrecht VwVfG*: 3. Ergänzungslieferung. München: C.H. Beck, 2022. §40, nota de rodapé 26; *BverwGE. Entscheidungen des Bundesverwaltungsgerichts* [= *Decisões do Tribunal Administrativo Federal*]*, 42, 26 (28); BverwGE. Entscheidungen des Bundesverwaltungsgerichts* [= *Decisões do Tribunal Administrativo Federal*]*, 49, 16 (23).*

[55] Quanto à implementação técnica da portabilidade de dados, veja especialmente FIX, Alexander Daniel. *Das Recht auf Datenportabilität*: Art. 20 DSGVO als Schnittstelle zwischen Wettbewerbsförderung und Datenschutz. Peter Lang: Berlim, 2022. p. 275 ss.

II Aumento da cibersegurança

Além de melhorar a interoperabilidade, o aumento da cibersegurança é outra preocupação fundamental da Lei Digital, pois ataques cibernéticos no setor da saúde vêm aumentando constantemente nos últimos anos,[56] de modo que se faz necessário, para todos os atores envolvidos, um nível mínimo de proteção, garantido por regulamento.

1 Riscos de ameaças no setor da saúde

O setor da saúde e seus atores são alvo, com particular frequência, ataques cibernéticos, como se depreende, no passado recente, dos relatórios da Agência Europeia de Cibersegurança (ENISA, na sigla em inglês) e da Agência de Segurança na Tecnologia da Informação (BSI, na sigla em alemão).[57] Os ataques virtuais são amplos e incluem hospitais,[58] planos de saúde, serviços sociais e prestadores de serviços de TI.[59] Além de restringir os sistemas de gestão de TI – o que muitas vezes é o objetivo principal dos invasores – esses ataques podem, na pior das hipóteses, também levar à morte de pacientes.[60] Pense-se, p. ex., em uma situação em que os sistemas de TI vitais na sala de operações caem em um hospital, em

[56] Cf., p. ex., BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK. *Die Lage der IT-Sicherheit in Deutschland 2023*. Disponível em: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.pdf?__blob=publicationFile&v=7. Acesso em: 07 jul. 2024. p. 58 s., 62; BUNDESKRIMINALAMT. *Cybercrime*: Bundeslagebild 2021. Disponível em: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2021.pdf?__blob=publicationFile&v=6. Acesso em: 10 jul. 2024. p. 1; MACHO, Andreas. *"Hacker-Angriffe auf Kliniken nehmen zu"* – obwohl sie Leben kosten. Disponível em: https://www.welt.de/wirtschaft/article246400880/Krankenhaeuser-Hacker-Angriffe-nehmen-zu-obwohl-sie-Leben-kosten.html. Acesso em: 12 jul. 2024.

[57] EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA). *ENISA threat landscape*: Health Sector. 2023. Disponível em: https://www.enisa.europa.eu/publications/health-threat-landscape/@@download/fullReport. Acesso em: 07 jul. 2024. p. 58 s., 62; de modo geral cf., quanto a isso, também BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK. *Lagebild Gesundheit*: Cyber-Sicherheit im Gesundheitswesen 2022. Disponível em: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Lagebild_Gesundheit_2022.pdf?__blob=publicationFile&v=6. Acesso em: 10 jul. 2024.

[58] Veja, mais recentemente, os ataques cibernéticos a clínicas na Renânia do Norte-Westfália: HEISE ONLINE. *Cyberangriff auf Kliniken in Ostwestfalen*. Disponível em: https://www.heise.de/news/Cyberangriff-auf-Kliniken-in-Ostwestfalen-9582719.html. Acesso em: 10 jul. 2024.

[59] EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA). *ENISA threat landscape*: Health Sector. 2023. Disponível em: https://www.enisa.europa.eu/publications/health-threat-landscape/@@download/fullReport. Acesso em: 07 jul. 2024.

[60] KERKMANN, Christof; NAGEL, Lars-Marten. *Todesfall nach Hackerangriff auf Uni-Klinik Düsseldorf*. Disponível em: https://www.handelsblatt.com/technik/cycberkriminalitaet-todesfall-nach-hackerangriff-auf-uni-klinik-duesseldorf/26198688.html. Acesso em: 10 jul. 2024.

que *hackers* têm acesso a marca-passos, ou em que dispositivos de infusão de medicamentos ou o prontuário de um paciente são manipulados.

Por isso, há necessário, sobretudo, tomar medidas tecnológicas e organizacionais para reforçar a resiliência dos sistemas de TI no setor da saúde. Ao mesmo tempo, as pessoas que entram diariamente em contato com esses sistemas também devem ser sensibilizadas e a sua consciência de segurança (*security awareness*)[61] deve ser reforçada.

2 Regulamentação da segurança de TI no setor da saúde

As normas centrais para regulamentar a segurança de TI se encontram agora nos §§390 – 392 do SGB V e no §103a do SGB XI. Elas se dirigem aos principais atores no setor da saúde, a saber, os envolvidos no atendimento médico e dentário dos planos de saúde (§390 do SGB V), os hospitais (§391 do SGB V), as seguradoras de saúde (§392 do SGB V) e os planos de prestação de assistência para pessoas doentes ou necessitadas de cuidados (§103a do SGB XI). Neste sentido, as normas anteriormente vigentes para a segurança de TI no atendimento de planos de saúde e odontológicos (§75b do SGB V aF) e em hospitais (§75c SGB V aF) são reformuladas em §§390, 391 SGB V e seu conteúdo é amplamente adotado.[62] Novas são as adições do §Secção 392 do SGB V e §103a do SGB XI, que abordam a segurança de TI dos planos de atendimento médico e de assistência a doentes.

3 Medidas tecnológicas e organizacionais

Devido à sua complexidade e à velocidade com que se desenvolve, a segurança da TI faz com que o marco jurídico seja constantemente desafiado e precise reagir com precisão e rapidez às novas tecnologias e situações de ameaça.[63] Por isso o legislador fornece apenas um marco jurídico abstrato nas normas mais importantes

[61] Cf., quanto a esse conceito, WEBER, Kristin; SCHÜTZ, Andreas E.; FERTIG, Tobias. *Grundlagen und Anwendung von Information Security Awareness*: Mitarbeiter zielgerichtet für Informationssicherheit sensibiliesieren. Wiesbaden: Springer Vieweg, 2019. p. 9 ss.; HELISCH, Michael; POKOYSKI, Dietmar (Orgs.). *Security Awareness*: Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung. Wiesbaden: Vieweg & Teubner, 2009. p. 10 ss.

[62] DEUTSCHER BUNDESRAT. *Entwurf eines Gesetzes zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG) 435/23*. [Publicações do Parlamento Federal] n. 435/23. 2023. p.164 s.

[63] Quanto às particularidades e aos desafios da segurança na TI, cf. LASSAHN, Philipp; POSCHER, Ralf. §7. *In*: HORNUNG, Gerrit; SCHALLBRUCH, Martin (Orgs.). *IT-Sicherheitsrecht*: Praxishandbuch. Baden-Baden: Nomos, 2021. §7, nota de rodapé 14 ss.

de segurança em TI, que deve ser preenchido através de diretrizes ou instrumentos comparáveis com a ajuda de outros atores – como, p. ex., a Agência Federal de Segurança na Tecnologia da Informação (BSI). Ao fazê-lo, ele cumpre seu dever de proteger os direitos fundamentais de proteção, criando agências e atribuindo-lhes a tarefa de elaborar padrões e orientações materiais sobre a segurança da TI.[64] Tendo em vista a efemeridade dos sistemas de TI informáticos e da segurança dessa tecnologia, a definição de normas de conteúdo pelos legisladores e reguladores parlamentares não é um meio adequado para alcançar um nível sempre atualizado e suficiente de segurança em TI.[65] Em todo caso, este tipo de regulamentação no setor de TI não constitui uma violação do princípio da significância,[66] pois questões regulatórias muito marcantes são regularmente concretizadas em normas infralegais.[67] Com isso, alcança-se um alívio para o legislador, garante-se a flexibilidade necessária, integram-se os conhecimentos especializados da administração pública, promove-se a participação das pessoas afetadas e alcança-se uma harmonização e coordenação da aplicação das normas.[68] Em particular, o alívio para o legislador e a maior flexibilidade na estruturação específica da segurança da TI e sua garantia jurídica no sistema de saúde possibilitam adaptar rapidamente o marco jurídico a novas ameaças para a cibersegurança.

a) Segurança de TI no atendimento médico e dentário das seguradoras

Para a área de assistência médica e odontológica obrigatória dos planos de saúde, tanto a Associação Nacional dos Médicos de Planos de Saúde quanto a Associação Nacional dos Dentistas de Planos de Saúde já estabeleceram os requisitos para garantir a segurança de TNI em diretivas próprias.[69] Neste sentido, os requisitos a serem atendidos se orientam pelo tamanho do consultório e diferenciam

[64] LASSAHN, Philipp; POSCHER, Ralf. §7. *In*: HORNUNG, Gerrit; SCHALLBRUCH, Martin (Orgs.). *IT-Sicherheitsrecht*: Praxishandbuch. Baden-Baden: Nomos, 2021. §7, nota de rodapé 42.

[65] LASSAHN, Philipp; POSCHER, Ralf. §7. *In*: HORNUNG, Gerrit; SCHALLBRUCH, Martin (Orgs.). *IT-Sicherheitsrecht*: Praxishandbuch. Baden-Baden: Nomos, 2021. §7, nota de rodapé 42.

[66] Veja, porém, quanto à atribuição da característica "operador de infraestruturas críticas", segundo o §10 da BUNDESMINISTERIUM DER JUSTIZ. *Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG).* Disponível em: https://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html. Acesso em: 07 jul. 2024. [= Lei sobre a Agência Federal de Segurança na Tecnologia da Informação], no contexto da teoria da significância, HEINICKEL, Caroline; FEILER, Lukas. Der Entwurf für ein IT-Sicherheitsgesetz – europarechtlicher Kontext und die (eigentlichen) Bedürfnisse der Praxis. *Computer und Recht*, n. 11, p. 708-714, 2014. p. 708 – 713 s.

[67] Kahl; Ludwigs; Bickenbach, *Handbuch des Verwaltungsrechts* – Band 2, 2023, §132, Rn. 24; cf., a título de exemplo, quanto ao Direito ambiental, Hoffmann, *Verwaltungskooperative Standardsetzung,* 2023.

[68] KAHL, Wolfgang; LUDWIGS, Markus. *Handbuch des Verwaltungsrechts*. Heidelberg: C.F. Müller, 2023. §132, nota de rodapé. 25 ss.

[69] KASSENÄRTZLICHE BUNDESVEREINIGUNG. *Richtlinie nach §75b SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit.* 2020. Disponível em: https://www.kbv.de/media/sp/RiLi___75b_SGB_V_Anforderungen_Gewaehrleistung_IT-Sicherheit.pdf. Acesso em: 10 jul. 2024.

entre consultórios pequenos, médios e grandes. Assim, p. ex., ao utilizar produtos do Office, os dados pessoais não devem ser armazenados na nuvem, ao utilizar dispositivos finais, deve ser feita regularmente uma cópia de segurança dos dados, e a transição da intranet para a internet deve ser protegida por um *firewall*. Em comparação com o regulamento anterior do §75b do SGB V aF,[70] a norma contém apenas – com exceção do reforço da *security awareness*[71] – revisões editoriais e não introduz qualquer alteração no que diz respeito ao conteúdo dos requisitos que devem ser preenchidos pela diretriz sobre a segurança da TI.[72]

b) Segurança de TI em hospitais e nos planos de saúde e assistência

Os hospitais, planos de saúde e assistência a doentes ou pessoas necessitadas de cuidados são obrigados a tomar precauções organizacionais e técnicas adequadas com base no estado atual da tecnologia para evitar rupturas na disponibilidade, integridade e confidencialidade de seus sistemas, componentes ou processos de TI (cf. §§391, 1, 392, 1 do SGB V, §103a, 1 do SGB XI). Os atores podem cumprir essas obrigações aplicando um padrão de segurança específico do setor para os sistemas de TI em suas respectivas instituições, sendo que sua adequação deve ser constatada pela Agência Federal de Segurança da Tecnologia da Informação (BSI) de acordo com o §8a II da BSIG (cf. §§391, 4, 392, 3 da SGB V, §103a, 3 da SGB XI).

Em hospitais, utiliza-se o padrão de segurança específico do setor (B3S), "Medizinische Versorgung [= Atendimento Médico]", cuja adequação já foi constatada pelo BSI.[73] Além de informações básicas e indicações sobre o âmbito de aplicação, o padrão contém especificações para determinar a situação de risco específica (capítulo 4) e extensos requisitos e recomendações, daí derivados, para a implementação de medidas concretas (capítulos 6 e 7).[74]

---

70 Cf., quanto a isso, DITTRICH, Tilmann; IPPACH, Jan. IT-Sicherheit betrifft nicht nur Großkrankenhäuser – die Regulierung der IT-Sicherheit im ambulanten und stationären Bereich. *GesundhaeitsRecht*, n. 5, p. 285 ss., 2021.

71 Veja, quanto a isso, detalhes em IV. 4.

72 DEUTSCHER BUNDESRAT. *Entwurf eines Gesetzes zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG) 435/23*. [Publicações do Parlamento Federal] n. 435/23. 2023. p. 164.

73 DEUTSCHE KRANKENHAUSGESELLSCHAFT. *Branchenspezifischer Sicherheitsstandard "Medizinische Versorgung"*. Version 1.2, 2022. Disponível em: https://www.dkgev.de/fileadmin/default/Mediapool/2_Themen/2.1_Digitalisierung_Daten/2.1.4._IT-Sicherheit_und_technischer_Datenschutz/2.1.4.1._IT-Sicherheit_im_Krankenhaus/Branchenspezifischer_Sicherheitsstandard_Medizinische_Versorgung_v1.2_Stand_2022-12-08.pdf. Acesso em: 07 jul. 2024.

74 Já presentes na versão anterior, HÄNLEIN, Andreas; SCHULER, Rolf. *Sozialgesetzbuch V*: Gesetzliche Krankenversicherung. 6. ed. Baden-Baden: Nomos, 2022. §75c, nota de rodapé 10.

No futuro, tal padrão também se aplicará às seguradoras de saúde e assistência a doentes (cf. §392, 3 do SGB V e §103a, 3 do SGB XI). Elas são obrigadas a tomar precauções organizacionais e técnicas adequadas com base no estado atual da tecnologia para evitar rupturas na disponibilidade, integridade e confidencialidade de seus sistemas, componentes ou processos de TI que sejam decisivos para a funcionalidade do respectivo plano de saúde ou de assistência e para a segurança das informações dos segurados processadas (§392, 1 do SGB V, §103a do SGB XI). As precauções são adequadas sempre que o dispêndio exigido não for desproporcional às consequências de uma falha ou comprometimento dos processos operacionais da seguradora de saúde ou de assistência ou da segurança das informações processadas dos segurados (§392, 2 do SGB X, §103a, 2 do SGB XI). Estas precauções devem ser tomadas por todos os planos de saúde e assistência – de modo semelhante à área de hospitais (cf. §391, 5 do SGB V ou §75c, 3 do SGB V aF) – a menos que, de qualquer modo, como operadores de infraestruturas críticas de acordo com o §da BSIG já devam tomar tais precauções (§392, 5 do SGB V, §103a, 5 do SGB XI).[75]

As seguradoras de saúde e de assistência a doentes podem utilizar o padrão de segurança – específico do setor – B3S-GKV/PV, cuja adequação foi constatada pelo BSI no início de 2023.[76] Neste tocante, o B3S-GKV/PV leva especialmente em consideração os requisitos que vão além da ISO 27001[77] [78] e precisam ser levados em conta em um setor tão particularmente vulnerável.

É lógico e coerente que, além dos requisitos jurídicos pregressos de segurança de TI no atendimento de médicos e dentistas credenciados, bem como em hospitais (§75 b e §75 c do SGB V aF), o legislador estenda agora estes requisitos também à área de planos de saúde e assistência, pois a segurança de TI afeta todos os atores envolvidos no sistema de saúde.

---

[75] Isso se refere a §10 I 1 BSIG em associação com §6 BSI-KritisV em associação com Anlage 5 sobre BSI-KritisV.

[76] UP KRITIS. *Branchenspezifischer Sicherheitsstandard für gesetzliche Kranken- und Pflegeversicherer B3S-GKV/PV*. 2023. Disponível em: https://www.vdek.com/Service/brachenspezifischer-sicherheitsstandard-b3s-gkv-pv/_jcr_content/par/download/file.res/B3S_GKV-PV_V.1.3.28_final.pdf. Acesso em: 12 jul. 2024.

[77] Cf. INFORMATION SECURITY MANAGEMENT. *ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements*. Disponível em: https://pecb.com/whitepaper/iso-27001-information-technology--security-techniques-information-security--management-systems---requirements. Acesso em: 07 jul. 2024, que especifica os requisitos para a instalação, implementação, manutenção e melhoria contínua de uma gestão documentada de sistemas de segurança de informações levando em conta o contexto de uma organização.

[78] UP KRITIS. *Branchenspezifischer Sicherheitsstandard für gesetzliche Kranken- und Pflegeversicherer B3S-GKV/PV*. 2023. Disponível em: https://www.vdek.com/Service/brachenspezifischer-sicherheitsstandard-b3s-gkv-pv/_jcr_content/par/download/file.res/B3S_GKV-PV_V.1.3.28_final.pdf. Acesso em: 12 jul. 2024. p. 5.

4 Aumento da *security awareness*

A fim de melhorar a resiliência dos sistemas de informação no setor da saúde e reduzir os riscos, os atores do sistema de saúde precisam tomar medidas organizacionais e técnicas. Um fator essencial são os usuários de sistemas de TI, que muitas vezes representam involuntariamente um risco de segurança. É, portanto, necessário que medidas para aumentar a *security awareness* – a consciência de segurança – dos usuários sejam ampliadas,[79] pois incidentes de segurança críticos para a TI são frequentemente o resultado de falha humana, avaliação equivocada de riscos e perigos ou falta de conhecimento ao lidar com sistemas de TI. Por conseguinte, é coerente que os atores relevantes no setor da saúde devam agora também tomar medidas para aumentar a consciência de segurança de seus funcionários (cf. §390, 2, 2, 391, 2, 392, 4, do SGB V, §103a, 4, 1 do SGB XI). Por isso, as diretrizes relevantes em matéria de segurança de TI precisam também especificar meios concretos para aumentar a consciência de segurança no futuro. Neste sentido, as medidas cogitadas devem ser adaptadas ao ator para quem serão utilizadas. Elas também dependem fortemente do respectivo nível de sensibilização na instituição específica. Estendem-se desde meros materiais e brochuras informativos até cursos de formação e "ataques" simulados ou demonstrativos.[80]

a) Consciência de segurança no atendimento médico e odontológico

No atendimento prestado por médicos e dentistas credenciados, as medidas de conscientização atingem os consultórios médicos e dentários. Em consonância com a diferenciação – de qualquer modo já vigente nessa área – baseada no tamanho dos consultórios e nos diferentes requisitos a ele associados para garantir a segurança de TI, as medidas de conscientização também devem ser diferenciadas por esse critério. Assim, medidas aplicadas em um consultório pequeno, no qual apenas cinco pessoas lidam constantemente com o processamento de dados, devem ser diferentes das aplicadas em um consultório em que mais de 20 pessoas lidam regularmente com o processamento de dados.[81] Neste tocante, a conscientização deve começar já na contratação de funcionários e levar em conta os diferentes

[79] DEUTSCHER BUNDESRAT. *Entwurf eines Gesetzes zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG) 435/23*. [Publicações do Parlamento Federal] n. 435/23. 2023. p. 72.

[80] DEUTSCHER BUNDESRAT. *Entwurf eines Gesetzes zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG) 435/23*. [Publicações do Parlamento Federal] n. 435/23. 2023. p. 165.

[81] Cf., quanto a essa diferenciação por tamanho, KASSENÄRTZLICHE BUNDESVEREINIGUNG. *Richtlinie nach §75b SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit*. 2020. Disponível em: https://www.kbv.de/media/sp/RiLi___75b_SGB_V_Anforderungen_Gewaehrleistung_IT-Sicherheit.pdf. Acesso em: 10 jul. 2024..

grupos-alvo com suas capacidades, processos de trabalho e recursos necessários.[82] Da mesma maneira, um exercício de emergência na área de TI também deve ser realizado em intervalos regulares. Assim, pode-se terminar um dia de atendimento normal no consultório mais cedo para realizar o exercício de emergência durante o restante da jornada de trabalho.[83] No entanto, isto não parece muito prático sob as atuais circunstâncias e condições no sistema e no atendimento de saúde, razão pela qual deve-se pensar sobre outras possibilidades.

b) Consciência de segurança em hospitais, incluindo aparelhos ou dispositivos médicos

Em comparação com os consultórios de médicos e dentistas, as medidas de conscientização nos hospitais são mais complexas porque existem numerosos outros atores a considerar. Além de médicos, pacientes e equipes de enfermagem, também devem ser levados em consideração funcionários externos, empresas e fornecedores que possam ter contato com o processamento de dados, de modo que estes também precisam ser conscientizados sobre como lidar com dados de pacientes.

No hospital as medidas de conscientização também precisam ser adaptadas às diferentes funções ou papéis. Assim, os grupos de pessoas que têm contato regular com informações dos pacientes devem ser capacitados de modo diferente dos grupos de pessoas que tenham pouco contato com essas informações. Quanto maior a relação com o processamento de dados dos pacientes, tanto melhor e mais abrangente deve ser a capacitação dos funcionários e tanto mais devem estar cientes de suas responsabilidades.[84] Neste contexto, diferentes temas devem ser abordados.[85] Deve-se pensar, p. ex., na política de segurança do hospital, em possíveis efeitos de um ciberataque ao hospital, na forma de lidar com senhas, no comportamento ao usar o computador e na navegação na internet, no uso de dispositivos móveis, nas responsabilidades em matéria de proteção de dados e

[82] DARMS, Martin; HAβFELD, Stefan; FEDTKE, Stephen. *IT-Sicherheit und Datenschutz im Gesundheitswesen*: Leitfaden für Ärzte, Apotheker, Informatiker und Geschäftsführer in Klinik und Praxis. Wiesbaden: Springer Vieweg, 2019. p. 148.

[83] Essa é a posição que se encontra, p. ex., em DARMS, Martin; HAβFELD, Stefan; FEDTKE, Stephen. *IT-Sicherheit und Datenschutz im Gesundheitswesen*: Leitfaden für Ärzte, Apotheker, Informatiker und Geschäftsführer in Klinik und Praxis. Wiesbaden: Springer Vieweg, 2019. p. 148.

[84] DARMS, Martin; HAβFELD, Stefan; FEDTKE, Stephen. *IT-Sicherheit und Datenschutz im Gesundheitswesen*: Leitfaden für Ärzte, Apotheker, Informatiker und Geschäftsführer in Klinik und Praxis. Wiesbaden: Springer Vieweg, 2019. p. 188.

[85] Segundo DARMS, Martin; HAβFELD, Stefan; FEDTKE, Stephen. *IT-Sicherheit und Datenschutz im Gesundheitswesen*: Leitfaden für Ärzte, Apotheker, Informatiker und Geschäftsführer in Klinik und Praxis. Wiesbaden: Springer Vieweg, 2019. p. 191 s.

segurança de TI, bem como nas instâncias responsáveis para relatar incidentes ou anomalias.

Além disso, os aparelhos ou dispositivos médicos também desempenham um papel central, de modo que os funcionários devem ter se conscientizado de que esses aparelhos podem processar informações confidenciais dos pacientes e que os sistemas só devem ser utilizados para o uso indicado e só então fornecem os resultados pertinentes.[86] No que diz respeito às medidas de conscientização para dispositivos médicos, deve-se lembrar, p. ex., que não se instalem *softwares* de terceiros, os aparelhos só sejam utilizados para a finalidade específica do produto médico e o comportamento incomum seja imediatamente comunicado à equipe de apoio técnico ou ao fabricante.[87]

c) Consciência de segurança nos planos de saúde e de assistência

Os planos de saúde e de assistência a doentes ou pessoas necessitadas de cuidados, por sua vez, têm de definir um foco diferente no tocante às medidas de conscientização a serem concretamente tomadas, pois neles, em comparação com os consultórios de médicos e dentistas e hospitais, outros parâmetros desempenham um papel substancial. Neste caso, é a segurança das informações dos segurados que está em primeiro plano. Portanto, os sistemas de TI utilizados devem ser protegidos e os funcionários devem ser capacitados sobre como lidar com eles. Neste sentido não basta que sejam realizadas medidas de conscientização de qualquer forma, pois elas também precisam ser bem-sucedidas. Isto pressupõe, em particular, que haja preparação e organização profissional, que não se despertem receios entre os funcionários, que se transmitam conteúdos de capacitação bem direcionados e passíveis de implementação, que novas formas de comportamento sejam continuamente treinadas e que seja dado *feedback*, além de levar em consideração peculiaridades culturais.[88] Também neste caso se podem cogitar diferentes medidas: campanhas sobre *phishing* para aumentar a consciência

[86] Exposição extensa quanto a isso se encontra em DARMS, Martin; HAβFELD, Stefan; FEDTKE, Stephen. *IT-Sicherheit und Datenschutz im Gesundheitswesen*: Leitfaden für Ärzte, Apotheker, Informatiker und Geschäftsführer in Klinik und Praxis. Wiesbaden: Springer Vieweg, 2019. p. 126.

[87] Segundo DARMS, Martin; HAβFELD, Stefan; FEDTKE, Stephen. *IT-Sicherheit und Datenschutz im Gesundheitswesen*: Leitfaden für Ärzte, Apotheker, Informatiker und Geschäftsführer in Klinik und Praxis. Wiesbaden: Springer Vieweg, 2019. p. 127.

[88] WEBER, Kristin; SCHÜTZ, Andreas E.; FERTIG, Tobias. *Grundlagen und Anwendung von Information Security Awareness*: Mitarbeiter zielgerichtet für Informationssicherheit sensibiliesieren. Wiesbaden: Springer Vieweg, 2019. p. 20.

dos funcionários,[89] a utilização de URLs de reencaminhamento em *e-mails*,[90] a criação de medidas eficazes de conscientização para a segurança de senhas[91] ou a utilização de ferramentas de conscientização sobre segurança especificamente talhadas para planos de saúde e de assistência a doentes.[92]

5 Conclusão provisória

O aumento da cibersegurança é outro componente essencial no caminho para um sistema de saúde digitalizado. É coerente que os requisitos de segurança de TI também sejam estendidos às seguradoras de saúde e de assistência a pessoas doentes ou necessitadas de cuidados e que a concretização dos requisitos técnicos específicos seja elaborada pelos atores responsáveis em cada caso, pois são eles que melhor conhecem os requisitos específicos. Não obstante, sobretudo os médicos e dentistas credenciados, os hospitais e os planos de saúde e de assistência são colocados diante de novos desafios pelo novo marco jurídico. Para cumprir os requisitos legalmente consagrados em matéria de segurança em TI e para aumentar a *security awareness*, é necessário um dispêndio considerável em termos de recursos humanos e financeiros, pois a implementação dos requisitos não pode ser deixada sob a responsabilidade da equipe médica. Da mesma maneira, deve-se fazer frente de modo eficaz ao risco de uma burocratização adicional do sistema de saúde. Por fim, o aumento fundamentalmente necessário da consciência da segurança entre os atores da área médica não deve ocorrer à custa dos segurados e dos pacientes. Portanto, o dispêndio para as instalações e equipamentos de saúde deve ser reduzido a um nível necessário.[93]

[89] Veja, quanto a isso, VOLKAMER, Melanie; SASSE, Martina A.; BOEHM, Franziska. Phishing: Kampagnen zur Steigerung der Mitarbeiter-Awareness. *Datenschcutz und Datensicherheit – DuD*, v. 44, p. 518-521, 2020. p. 518.

[90] Veja, quanto a isso, MÜLLMANN, Dirk; VEIT, Maxime; VOLKAMER, Melanie. Weiterleitungs-URLs in e-mails. *Datenschcutz und Datensicherheit – DuD*, n. 5, p. 275 ss., 2023. p. 275.

[91] Veja, quanto a isso, MAYER, Peter; BALLREICH, Fabian; DÜZGÜN; SCHWARTZ, Christian; VOLKAMER, Melanie. Erstellung von effektiven Sensibilisierungsmaterialien zur Passwortsicherheit. *Datenschcutz und Datensicherheit – DuD*, v. 44, p. 522-527, 2020. p. 522.

[92] MARKUS, Heike; MEUCHE, Thomas. *Auf dem Weg zur digitalen Verwaltung*: Ein ganzheitliches Konzept für eine gelingende Digitalisierung in der öffentlichen Verwaltung. Wiesbaden: Springer Gabler, 2022. p. 211.

[93] BUNDESMINISTERIUM FÜR GESUNDHEIT. *Stellungnahme der Gesellschaft für Qualitätsmanagement in der Gesundheitsversorgung e.V. (GQMG) zum Referentenentwurf des Bundesministeriums für Gesundheit über das Gesetz zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG)*. Disponível em: https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/Gesetze_und_Verordnungen/Stellungnahmen_WP20/DigiG/stellungnahme_gqmg.pdf. Acesso em: 07 jul. 2024.

C Proteção de dados na pesquisa em saúde

A pesquisa que utiliza dados dos atores num sistema de saúde digitalizado também se tornará fundamentalmente mais importante no futuro. Em particular, são os dados fornecidos pelos segurados e pelos pacientes que representam um enorme tesouro de dados. Podem ser utilizados para investigar e desenvolver novas terapias, melhorar e otimizar procedimentos médicos e adaptar o sistema de saúde de forma muito mais eficiente e precisa às necessidades das pessoas afetadas.

Com a Lei de Cuidados Digitais (DVG) e a Lei de Proteção de Dados do Paciente (PDSG), duas leis centrais na área da lei de proteção de dados de saúde foram aprovadas nos últimos anos,[94] a fim de promover a digitalização do sistema de saúde[95] e, ao mesmo tempo, fortalecer especificamente a soberania dos dados do indivíduo.[96] Os regulamentos foram controversos desde o início e o DVG também foi objeto de processos provisórios de proteção judicial sem sucesso perante o BVerfG.[97] O DVG fez grandes alterações aos regulamentos sobre transparência de dados (§§303a – 303f SGB V),[98] embora estes regulamentos tenham sido, por sua vez, parcialmente modificados com o GDNG.[99] O PDSG reestrutura exaustivamente os regulamentos sobre infraestrutura telemática (§§306 e seguintes SGB V).[100]

94 Cf., quanto a isso, já BRETTHAUER, Sebastian; APPENZELLER, Arno; BIRNSTILL, Pascal. Datensouveränität für Patienten im Gesundheitswesen: Eine Chance für die medizinische Forschung und den Datenschutz. *Datenschutz und Datensicherheit (DuD)*, v. 45, n. 3, p. 173-179, 2021. p. 173.

95 DEUTSCHER BUNDESTAG. *Entwurf eines Gesetzes für eine bessere Versorgung durch Digitalisierung und Innovation (Digitale-Versorgung-Gesetz – DVG) 19/1e3438*. [Publicações do Parlamento Federal] n. 19/13438. 2015. p. 2; DEUTSCHER BUNDESTAG. *Entwurf eines Gesetzes für eine bessere Versorgung durch Digitalisierung und Innovation (Digitale-Versorgung-Gesetz – DVG) 19/18793*. [Publicações do Parlamento Federal] n. 19/18793. 2020. p. 2.

96 DEUTSCHER BUNDESTAG. *Entwurf eines Gesetzes für eine bessere Versorgung durch Digitalisierung und Innovation (Digitale-Versorgung-Gesetz – DVG) 19/13438*. [Publicações do Parlamento Federal] n. 19/13438. 2015. p. 97; DEUTSCHER BUNDESTAG. *Entwurf eines Gesetzes für eine bessere Versorgung durch Digitalisierung und Innovation (Digitale-Versorgung-Gesetz – DVG) 19/18793*. [Publicações do Parlamento Federal] n. 19/18793. 2020. p. 130.

97 BVerfG, Beschl. v. 19.3.2020 – 1 BvQ 1/20; Bretthauer/Spiecker gen. Döhmann, JZ 2020, 990.

98 DEUTSCHER BUNDESTAG. *Entwurf eines Gesetzes für eine bessere Versorgung durch Digitalisierung und Innovation (Digitale-Versorgung-Gesetz – DVG) 19/13438*. [Publicações do Parlamento Federal] n. 19/13438. 2015. p. 71 ss.

99 DEUTSCHER BUNDESTAG. *Entwurf eines Gesetzes zur verbesserten Nutzung von Gesundheitsdaten (Gesundheitsdatennutzungsgesetz – GDNG) 20/9046*. [Publicações do Parlamento Federal] n. 20/9046. 2023. p. 26 ss.

100 DEUTSCHER BUNDESTAG. *Entwurf eines Gesetzes für eine bessere Versorgung durch Digitalisierung und Innovation (Digitale-Versorgung-Gesetz – DVG) 19/18793*. [Publicações do Parlamento Federal] n. 19/18793. 2020. p. 98 ss.

I A transparência dos dados como prerrequisito para um sistema de saúde digitalizado

1 Transparência de dados para melhorar a investigação em saúde digital

Com os regulamentos sobre transparência de dados nos §§303a – 303f SGB V, o legislador concedeu ao Instituto Federal de Medicamentos e Dispositivos Médicos – uma autoridade federal superior – permissão para armazenar grandes quantidades de dados sobre pessoas seguradas do seguro de saúde legal, mantendo ao mesmo tempo altos padrões de segurança e enviá-lo para determinados locais para pesquisa e melhoria do atendimento.[101] Os padrões são especificados com mais detalhes pelo chamado regulamento de transparência de dados (DaTraV).[102] O objetivo dos regulamentos de transparência de dados é aumentar a usabilidade dos dados num sistema de saúde digitalizado, especialmente para fins de investigação, e assim proteger o direito dos segurados à autodeterminação informativa (Art. 2 Par. 1 em conjunto com o Art. 1 Parágrafo 1 GG, Art. 8 GRCh).[103]

Portanto, num sistema de saúde digitalizado, nem todos os dados do segurado podem ser disponibilizados a terceiros, mesmo que os dados fornecidos sejam muito extensos. O §303b, parágrafo 1 do SGB V, portanto, padroniza os dados que as companhias de seguros de saúde e os fundos de cuidados de enfermagem só podem transmitir à associação guarda-chuva da Federação dos Fundos de Seguros de Saúde (SpiBuKK) como um ponto de coleta de dados, embora isso já envolva uma grande quantidade de dados, bem como dados particularmente sensíveis. Além das informações gerais sobre idade, sexo e local de residência (Seção 303b Parágrafo 1 No. 1 SGB V), os dados de custo e desempenho em particular também estão de acordo com as Seções 295, 295a, 300, 301, 301a e 302 SGB V, bem como a Seção 105 SGB XI (Seção 303b Parágrafo 1 No. 3 SGB V). Isto aplica-se em particular aos dados de faturação e aos dados fornecidos para ajuste da estrutura de risco, bem como aos dados utilizados exclusivamente para transparência de dados.[104] Os dados do ajuste da estrutura de risco são, nomeadamente, dados-mestre e informações

[101] KÜHLING, Jürgen; SCHILDBACH, Roman. Die Reform der Datentransparenzvorschriften im SGB V. *Neue Zeitschrift für Sozialrecht*, n. 41, 2020.

[102] Veja, quanto a isso, BUNDESMINISTERIUM DER JUSTIZ. *Verordnung zur Umsetzung der Vorschriften über die Datentransparenz (Datentransparenzverordnung – DaTraV)*. Disponível em: https://www.gesetze-im-internet.de/datrav_2020/BJNR137110020.html. Acesso em: 11 jul. 2024.

[103] KÜHLING, Jürgen; SCHILDBACH, Roman. Die Reform der Datentransparenzvorschriften im SGB V. *Neue Zeitschrift für Sozialrecht*, n. 41, 2020. p. 42.

[104] ROLFS, Christianl GIESEN, Richard; KREIKEBOHM, Ralf; MESSLING, Miriam; UDSCHING, Peter. *BeckOK Sozialrecht*. 61 Ed. München: C.H. Beck, [2012]. SGB V §303b Rn. 5.

sobre tratamentos ambulatoriais e hospitalares, bem como informações sobre os medicamentos prescritos.[105] Para os segurados individuais, são registrados o ano de nascimento, o sexo, o tempo de tratamento e os códigos do CID[106] para que se possam tirar conclusões sobre os diagnósticos realizados.[107] Para os medicamentos são transmitidos o número da central farmacêutica,[108] a data da prescrição e o número de receitas.[109] No entanto, dados não estruturados, como cartas médicas, não são registrados.[110] Esta visão geral deixa claro que um sistema de saúde digitalizado gera uma grande quantidade de dados particularmente sensíveis, que podem agora ser sistematicamente processados e avaliados no futuro. Ao mesmo tempo, são, portanto, necessárias medidas de proteção especiais para proteger de forma abrangente a autodeterminação informativa do segurado, de acordo com o artigo 2º, nº 1, em conjugação com o artigo 1º, nº 1 GG.

Portanto, as seguradoras de saúde apenas transmitem à SpiBuKK as informações que armazenam sobre os segurados e prestadores de serviços de forma pseudonimizada.[111] O nome do segurado não será transmitido. O SpiBuKK reúne então os dados que lhe são transmitidos e verifica-os quanto à integralidade, plausibilidade e consistência (Secção 303b Parágrafo 2 SGB V). Os dados processados são então transmitidos ao centro de dados de pesquisa (ver Seção 303d SGB V) e ao escritório fiduciário (ver Seção 303c SGB V), por outro. O Instituto Federal de Medicamentos e Dispositivos Médicos[112] desempenha as tarefas do centro de dados de pesquisa (Seção 2 Parágrafo 2 DaTraV) e o Instituto Robert Koch assume as tarefas do órgão de confiança (Seção 2 Parágrafo 1 DaTraV).

O centro de dados de investigação, como ponto de contato central para todas as questões relativas ao (posterior) processamento de dados (ver Secção 303e SGB V), desempenha um papel central no sistema de saúde digitalizado. A sua área de responsabilidade é muito ampla e vai desde a garantia da qualidade dos

[105] KÜHLING, Jürgen; SCHILDBACH, Roman. Die Reform der Datentransparenzvorschriften im SGB V. *Neue Zeitschrift für Sozialrecht*, n. 41, 2020. p. 42.
[106] KÜHLING, Jürgen; SCHILDBACH, Roman. Die Reform der Datentransparenzvorschriften im SGB V. *Neue Zeitschrift für Sozialrecht*, n. 41, 2020. p. 42.
[107] KÜHLING, Jürgen; SCHILDBACH, Roman. Die Reform der Datentransparenzvorschriften im SGB V. *Neue Zeitschrift für Sozialrecht*, n. 41, 2020. p. 42.
[108] KÜHLING, Jürgen; SCHILDBACH, Roman. Die Reform der Datentransparenzvorschriften im SGB V. *Neue Zeitschrift für Sozialrecht*, n. 41, 2020. p. 42.
[109] KÜHLING, Jürgen; SCHILDBACH, Roman. Die Reform der Datentransparenzvorschriften im SGB V. *Neue Zeitschrift für Sozialrecht*, n. 41, 2020. p. 42.
[110] KÜHLING, Jürgen; SCHILDBACH, Roman. Die Reform der Datentransparenzvorschriften im SGB V. *Neue Zeitschrift für Sozialrecht*, n. 41, 2020. p. 42.
[111] ROLFS, Christianl GIESEN, Richard; KREIKEBOHM, Ralf; MESSLING, Miriam; UDSCHING, Peter. *BeckOK Sozialrecht*. 61 Ed. München: C.H. Beck, [2012]. SGB V §303b Rn. 3a.
[112] ROLFS, Christianl GIESEN, Richard; KREIKEBOHM, Ralf; MESSLING, Miriam; UDSCHING, Peter. *BeckOK Sozialrecht*. 61 Ed. München: C.H. Beck, [2012].

dados que lhe são transmitidos (artigo 303d, nº 1, nº 2 do SGB V) até a avaliação e desenvolvimento de procedimentos de transparência de dados (artigo 303d, nº 1, nº 7 do SGB V), e oferecer oportunidades de treinamento para aqueles autorizados a usar a infraestrutura de dados (Seção 303d Parágrafo 1 nº 9 SGB V). Para posterior investigação com os dados existentes, o tratamento dos dados transmitidos (artigo 303d nº 1 nº 1 SGB V), tornando os dados solicitados acessíveis às pessoas autorizadas a utilizá-los (artigo 303d nº 1 nº 4 SGB V), a avaliação do risco de reidentificação dos dados solicitados (Seção 303d Parágrafo 1 nº 5 SGB V), bem como a promoção do desenvolvimento científico dos dados (Seção 303d Parágrafo 1 nº 10 SGB V) são de particular importância. A fim de minimizar o risco específico de reidentificação, o centro de dados de investigação deve tomar medidas adequadas, preservando simultaneamente de forma adequada o benefício científico.[113] O que isto significa especificamente em casos individuais e quais os critérios que estas medidas devem ser utilizadas para ponderar e avaliar permanecem obscuros neste momento. Portanto, especificações claras são necessárias aqui. Estas poderiam consistir em referir-se a um estado da arte específico, a regras de tecnologia geralmente reconhecidas ou mesmo ao estado da ciência e da tecnologia.[114]

Finalmente, a Seção 303e do SGB V especifica quais atores (Seção 303e, Parágrafo 1 do SGB V) estão autorizados a usar o conjunto de dados do centro de dados de pesquisa para quais fins (Seção 303e, Parágrafo 2 do SGB V). Todas as pessoas singulares e coletivas abrangidas pelo âmbito de aplicação do RGPD têm, portanto, direito à utilização dos dados, desde que estejam autorizadas a tratar os dados. Do ponto de vista da minimização de dados (Art. 5 Par. 1 lit. c GDPR), a crítica apropriada é sobre se um grupo tão amplo e indefinido de usuários autorizados é absolutamente necessário. A minimização dos dados significa principalmente reduzir o nível de interferência com o direito fundamental à proteção de dados dos titulares dos dados.[115] No entanto, a minimização também se refere à extensão do processamento de dados, de modo que o número e a extensão das utilizações também devem ser reduzidos ao necessário,[116] e o círculo de utilizadores autorizados deve ser mantido pequeno e gerível. A fim de mitigar este aspecto e reduzir ao mínimo

[113] DEUTSCHER BUNDESTAG. *Entwurf eines Gesetzes für eine bessere Versorgung durch Digitalisierung und Innovation (Digitale-Versorgung-Gesetz – DVG) 19/13438*. [Publicações do Parlamento Federal] n. 19/13438. 2015. p. 73.

[114] Cf., quanto a isso, basicamente SEIBEL, Mark. Abgrenzung der "allgemein anerkannten Regeln der Technik" vom "Stand der Technik". *Neue Juristische Wochenschrift*, n. 41, p. 3000, 2013.

[115] SIMITIS, Spiros; HORNUNG, Gerrit; DÖHMANN, Indra Spiecker gennant (Orgs.). *Datenschutzrecht*: DS-GVO mit BDSG. Baden-Baden: Nomos, 2019. Art. 5, nota de rodapé 116.

[116] SIMITIS, Spiros; HORNUNG, Gerrit; DÖHMANN, Indra Spiecker gennant (Orgs.). *Datenschutzrecht*: DS-GVO mit BDSG. Baden-Baden: Nomos, 2019. Art. 5, nota de rodapé 30.

as ameaças à autodeterminação informacional, o legislador estipula pelo menos uma limitação estrita da finalidade na Seção 303e Parágrafo 2 do SGB com uma lista final de finalidades de uso,[117] de modo que o círculo inicialmente amplo de usuários autorizados é restringido por uma limitação estrita de propósito.

Do ponto de vista da pesquisa, a Seção 303e Parágrafo 2 nº 4 SGB V é de particular importância. Os usuários autorizados – como universidades ou instituições de pesquisa – estão autorizados a processar dados para pesquisas científicas sobre questões nas áreas de saúde e cuidados. Este catálogo de finalidades de tratamento de dados para investigação não é exaustivo, pelo que outras formas e métodos de investigação médica também podem ser considerados.[118] O centro de dados de pesquisa deve então transmitir os dados selecionados ao usuário autorizado solicitante. Os dados devem ser geralmente fornecidos de forma anonimizada e agregada (Seção 303e Parágrafo 3 Sentença 4 SGB V). Os detalhes disso estão padronizados na Seção 10 DaTraV. Em casos especiais, o centro de dados de pesquisa também pode transmitir dados anonimizados e agregados com referência a um pequeno número de casos (Seção 303e Parágrafo 3 Sentença 5 SGB V). Ao mesmo tempo, porém, existe um risco crescente de que dados anteriormente anônimos se tornem dados pessoais. Quanto menor for o número de casos, maior será a probabilidade de reidentificação, especialmente quando se trata de investigação de doenças particularmente raras.[119] Finalmente, em casos excepcionais estritamente definidos, existe também a possibilidade de fornecer conjuntos de dados pseudonimizados (Secção 303e Parágrafo 4 Sentença 1 SGB V). No entanto, também devem ser tomadas medidas técnicas e organizacionais para garantir que o tratamento do utilizador autorizado seja limitado na medida necessária e, em particular, que a cópia dos dados possa ser evitada (Secção 303e Parágrafo 4 Sentença 2 nº 2 SGB V). Em última análise, no tratamento dos dados disponibilizados, os utilizadores autorizados devem garantir que não estabelecem qualquer referência a pessoas ou prestadores de serviços (artigo 303e, nº 5, frase 2 do SGB V). Caso contrário, isso deverá ser comunicado imediatamente ao Centro de Dados de Pesquisa (Seção 303e Parágrafo 5 Sentença 3 SGB V).

[117] ROLFS, Christianl GIESEN, Richard; KREIKEBOHM, Ralf; MESSLING, Miriam; UDSCHING, Peter. *BeckOK Sozialrecht*. 61 ed., München: C.H. Beck, [2012]. SGB V §303e Rn. 4.

[118] BECKER, Ulrich; KINGREEN, Thorsten. *SGB V*: Gesetzliche Krankenversicherung. München: C.H. Beck, 2022. SGB V §303e nota de rodapé 3.

[119] Cf., quanto ao problema da reidentificação, também KÜHLING, Jürgen; SCHILDBACH, Roman. Die Reform der Datentransparenzvorschriften im SGB V. *Neue Zeitschrift für Sozialrecht*, n. 41, 2020. p. 43 ss.

2 Potencial de melhoria nas regulamentações de transparência de dados

O sistema diferenciado de regulamentações de transparência de dados não é fácil de penetrar. Com os seus vários atores – SpiBuKK, centro de dados de investigação e confiança – que estão eles próprios integrados em complicadas estruturas de saúde alemãs, o legislador deu, no entanto, um primeiro passo importante e correto para reforçar a importância da transparência dos dados num sistema de saúde digitalizado. No entanto, os regulamentos sobre transparência de dados representam apenas um primeiro passo na direção certa. Para além dos requisitos estabelecidos, são absolutamente necessárias mais melhorias.[120]

Não existem direitos específicos das pessoas afetadas, como o direito das pessoas afetadas de se oporem à utilização de dados para fins de investigação ou o direito das pessoas afetadas à informação sobre os conjuntos de dados individuais armazenados sob pseudônimo sobre eles no centro de dados de investigação.[121] Não há recurso aos regulamentos gerais (artigo 21º do RGPD, artigo 15º do RGPD). Com o artigo 89º, nº 2, do RGPD e o artigo 27º, nº 2, do BDSG, existem regulamentos excecionais na área da investigação científica que restringem o direito do titular dos dados à oposição e à informação. No entanto, uma disposição específica nos regulamentos sobre transparência de dados seria juridicamente necessária neste momento, no sentido de um direito genuíno de transparência para as pessoas afetadas, que está associado a um direito de oposição específico do projeto.[122] Em qualquer caso, isto permitiria uma implementação significativamente mais diferenciada do direito à autodeterminação informacional no contexto da investigação.[123] De qualquer forma, isto deve aplicar-se ao direito à informação devido à sua garantia constitucional (cf. Art. 8 Parágrafo 2 Sentença 2 GRCh).[124] O legislador deve, portanto, fazer ajustes aqui e integrar regulamentos apropriados.

Deverão também ser consideradas outras utilizações especiais dos dados e a sua normalização. Muitas vezes, a investigação no setor da saúde só é possível com conjuntos de dados pessoais individuais, por exemplo, se o foco for a investigação

[120] WEICHERT, Thilo. "Datentransparenz" und Datenschutz. *Medizinrecht*, v. 38, p. 539-546, 2020. p. 539-542 ss.

[121] WEICHERT, Thilo. "Datentransparenz" und Datenschutz. *Medizinrecht*, v. 38, p. 539-546, 2020. p. 543 ss.

[122] WEICHERT, Thilo. "Datentransparenz" und Datenschutz. *Medizinrecht*, v. 38, p. 539-546, 2020. p. 543 ss.

[123] Posição semelhante se encontra em WEICHERT, Thilo. "Datentransparenz" und Datenschutz. *Medizinrecht*, v. 38, p. 539-546, 2020. p. 543.

[124] Cf., quanto a isso, também JARASS, Hans D. *Charta der Grundrechte der Europäischen Union*. 4 Ed. Frankfurt: C. H. Beck, 2021. Art. 8, nota de rodapé 20, bem como SIMITIS, Spiros; HORNUNG, Gerrit; DÖHMANN, Indra Spiecker gennant (Orgs.). *Datenschutzrecht*: DS-GVO mit BDSG. Baden-Baden: Nomos, 2019. Art. 15, nota de rodapé 1.

de doenças específicas.[125] Embora conjuntos de dados individuais pseudonimizados já possam ser disponibilizados em casos especiais (ver Seção 303e, parágrafos 4 e 5 do SGB V), os requisitos legais padronizados não são suficientemente precisos para permitir o tratamento de dados legalmente compatível. Porque os requisitos para uso posterior mencionados são baixos. É suficiente, entre outras coisas, que os destinatários dos dados estejam sujeitos ao sigilo profissional e que medidas técnicas e organizacionais adequadas garantam a minimização dos dados. O que também seria necessário é uma separação espacial, organizacional e de pessoal entre o cumprimento das tarefas operacionais de um escritório e o processamento pseudônimo de dados de transparência. Também são necessárias disposições que tomem precauções suficientemente precisas contra a reidentificação de dados.[126] Também aqui, o estado da arte ou o estado da ciência e da tecnologia poderiam ser tidos em conta a fim de integrar procedimentos modernos – como procedimentos específicos de cifragem, como chave pública e chave privada ou assinaturas digitais – no sentido de processamento avançado de dados que esteja em conformidade com os regulamentos de proteção de dados em nível legal. Além disso, devem ser tomadas precauções de utilização, que incluem uma marcação particularmente rigorosa.[127] Finalmente, a relação entre os regulamentos de transparência de dados e os regulamentos especiais de investigação no SGB X (§67c seção 2 n. 2, seção. 5 e §75 seção 1, 2 e 4a S. 1 SGB X) é totalmente obscura e exige por isso uma solução.[128]

Do ponto de vista organizacional, é o centro de dados de investigação em particular que, juntamente com o SpiBuKK, está a tornar-se fundamentalmente mais importante. Isto ocorre porque uma recolha central de dados de saúde altamente sensíveis de todas as pessoas com seguro de saúde legal na Alemanha está a ser estabelecida ou expandida.[129] Devido à sua gama abrangente de tarefas, é um elemento essencial e um motor para o desenvolvimento de um sistema de saúde digitalizado. No entanto, também pode contribuir para prevenir a digitalização progressiva se não conseguir realizar as tarefas que lhe são atribuídas com os recursos necessários (pessoal, equipamento, conhecimentos especializados). Para uma investigação bem-sucedida com dados, é, portanto, essencial que os regulamentos recentemente inseridos ajudem a permitir uma investigação moderna e progressiva.

[125] WEICHERT, Thilo. "Datentransparenz" und Datenschutz. *Medizinrecht*, v. 38, p. 539-546, 2020. p. 543.
[126] WEICHERT, Thilo. "Datentransparenz" und Datenschutz. *Medizinrecht*, v. 38, p. 539-546, 2020. p. 543.
[127] Veja, quanto isso, exposição extensa em WEICHERT, Thilo. Die Forschungsprivilegierung in der DS-GVO. *Zeitschrift für Datenschutz*, v. 18, p. 21 ss., 2020.
[128] WEICHERT, Thilo. "Datentransparenz" und Datenschutz. *Medizinrecht*, v. 38, p. 539-546, 2020. p. 544.
[129] Essa posição já se encontra em WEICHERT, Thilo. "Datentransparenz" und Datenschutz. *Medizinrecht*, v. 38, p. 539-546, 2020. p. 542.

O centro de dados de investigação desempenhará, portanto, um papel fundamental na decisão de se e como a investigação bem-sucedida será implementada num sistema de saúde digitalizado na Alemanha.

II A infraestrutura telemática e a pesquisa com dados do prontuário eletrônico do paciente

Além da necessária transparência dos dados, outro motor fundamental para a digitalização do sistema de saúde é a expansão da infraestrutura telemática (§306 e seguintes do SGB V). A infraestrutura telemática (TI) é a infraestrutura de informação, comunicação e segurança interoperável e compatível que serve para prestadores de serviços de rede, pagadores, segurados e outros atores no sistema de saúde, bem como reabilitação e cuidados (Secção 306 Parágrafo 1 Sentença 2 SGB V). Em princípio, pretende-se colocar em rede todos os atores no sistema de saúde – como médicos, hospitais, seguradoras de saúde, farmácias e doentes. Os regulamentos sobre TI no SGB V são, portanto, padronizados em um capítulo separado (11º capítulo) e incluem nada menos que 77 regulamentos (§§306 – 383 SGB V). Numa primeira secção (§§306 – 309 SGB V), os requisitos gerais para o TI são padronizados e as responsabilidades em matéria de proteção de dados são definidas (§307 SGB V).[130] A segunda, terceira e quarta seções (§§310 – 333 SGB V) contêm regulamentos sobre as tarefas da Sociedade Telemática, o funcionamento da infraestrutura telemática e a monitorização da funcionalidade e segurança do TI. Central para as funcionalidades do TI é a quinta seção sobre as aplicações do TI (§§334 – 363 SGB V), que contém os regulamentos relevantes para o arquivo eletrônico do paciente (§§341 – 355 SGB V), bem como a disponibilidade de dados provenientes de aplicações do TI para fins de investigação (§363 SGB V). A sexta, sétima e oitava seções (§§364 – 383 SGB V) contêm regulamentos adicionais sobre procedimentos telemédicos, requisitos para interfaces de sistemas de tecnologia da informação, bem como disposições sobre financiamento e reembolso de custos.

1 Processamento de dados de prontuários eletrônicos de pacientes para fins de pesquisa

Com a introdução do processo eletrônico do paciente, os segurados podem agora também disponibilizar os dados nele armazenados para fins de investigação

[130] DOCHOW, Carsten. Das Patienten-Datenschutz-Gesetz (Teil 1): Die elektronische Gesundheitskarte und Telematikinfrastruktur. *Medizinrecht*, n. 38, p. 979-993, 2020. p. 979-983 ss.

(artigo 341º, nº 2, nº 6 do SGB V). Isto significa que a digitalização do sistema de saúde está mais uma vez a registar um enorme impulso. Embora anteriormente os dados dos pacientes pudessem ser disponibilizados para investigação, a digitalização permite agora que os dados sejam disponibilizados em todo o mundo de forma muito mais rápida, fácil e descomplicada. A Seção 363 SGB V cria, portanto, a base jurídica correspondente, que padroniza amplamente os requisitos para o processamento de dados do prontuário eletrônico do paciente para fins de pesquisa. O objetivo da norma é estabelecer uma base de dados sólida para pesquisa, garantia de qualidade e melhoria dos cuidados de saúde. Nesta base, as ligações médicas podem ser examinadas e podem ser encontradas abordagens de tratamento inovadoras que beneficiam os cuidados médicos gerais do segurado.[131] Este é, portanto, um uso secundário dos dados do paciente.[132] O novo regulamento abre basicamente duas formas de disponibilizar dados médicos para fins de investigação.[133] Por um lado, os dados do arquivo eletrônico do paciente são disponibilizados para fins de acordo com a Seção 303e Parágrafo 2 SGB V, desde que os segurados não tenham se oposto à transferência de dados e, por outro lado, de acordo com a Seção 363 Parágrafo 8 SGB V, eles também podem utilizar os dados para um projeto de pesquisa específico ou determinadas áreas da pesquisa científica no sentido de consentimento informado. Resta saber qual destes dois caminhos se estabelecerá na prática no futuro.

As finalidades para as quais os segurados podem divulgar os dados do arquivo eletrônico do paciente são descritas com precisão na Seção 363 Parágrafo 1 SGB V com referência à Seção 303e Parágrafo 2 SGB V. Os dados só podem ser divulgados para melhorar a qualidade dos cuidados e melhorar os padrões de segurança de prevenção, cuidados e enfermagem, para investigação científica, para apoiar processos de tomada de decisão política para o desenvolvimento do seguro de saúde legal e para realizar tarefas de notificação de saúde. Outros fins são, portanto, excluídos à partida. Se as duas primeiras finalidades mencionadas são aquelas que estão intimamente relacionadas com os pacientes, as duas últimas finalidades baseiam-se nos interesses do público em geral, que, na melhor das hipóteses, têm um benefício indireto para o segurado.[134] Parece questionável se

[131] DEUTSCHER BUNDESTAG. *Entwurf eines Gesetzes für eine bessere Versorgung durch Digitalisierung und Innovation (Digitale-Versorgung-Gesetz – DVG) 19/18793*. [Publicações do Parlamento Federal] n. 19/18793. 2020. p. 130.

[132] Veja, quanto a isso, também SCHNEIDER, Uwe K. *Sekundärnutzung klinischer Daten*: Rechtliche Rahmenbedingungen. Berlin: MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, 2015.

[133] DOCHOW, Carsten. Das Patienten-Datenschutz-Gesetz (Teil 3): Die Datenspende. *Medizinrecht*, p. 115 ss., 2021. p. 118.

[134] DOCHOW, Carsten. Das Patienten-Datenschutz-Gesetz (Teil 3): Die Datenspende. *Medizinrecht*, p. 115 ss., 2021. p. 118.

estes objetivos amplos irão realmente ajudar as pessoas seguradas a disponibilizar os seus dados mais livremente no futuro. A aprovação de processos de tomada de decisão política provavelmente exigirá inicialmente um esforço não insignificante por parte do médico para explicar aos pacientes e, portanto, aos segurados, algo a que os médicos geralmente não podem dedicar muito tempo. Os dados divulgados são então transmitidos ao centro de dados de pesquisa (Seção 363 Parágrafo 2 SGB V). Além dos dados já recebidos das seguradoras de saúde e da SpiBuKK provenientes do processo de transparência de dados, o centro de dados de investigação receberá mais dados específicos dos pacientes, demonstrando mais uma vez a sua especial importância no contexto da investigação em saúde, uma vez que terá um impacto significativo em grande quantidade de dados de saúde. Os dados são pseudonimizados, criptografados e transmitidos ao centro de dados de pesquisa com um número comercial previamente atribuído. O centro de dados de pesquisa pode então disponibilizar esses dados para usuários legítimos autorizados, como instituições de pesquisa em saúde ou universidades (ver Seção 363, Parágrafo 4 do SGB V). Os segurados podem opor-se à transmissão de dados a qualquer momento (artigo 363, Parágrafo 5 SGB V). Em caso de revogação, o centro de dados de investigação deve eliminar os dados transmitidos, embora os dados transmitidos até a revogação e já utilizados para projetos de investigação específicos possam continuar a ser processados para esses projetos de investigação (Seção 363 Parágrafo 6 SGB V). Finalmente, o Ministério Federal da Saúde está autorizado a padronizar em regulamento legal as medidas adequadas e específicas para proteger os interesses do titular dos dados, bem como os detalhes técnicos e organizacionais da divulgação e transmissão de dados, bem como a pseudonimização (Seção 363 Parágrafo 7 SGB V). Ainda não está claro por que estes requisitos, que abordam a proteção dos pacientes e segurados, não foram imediatamente incorporados na lei. Medidas de proteção como a proibição e restrições à mudança de finalidade, obrigações de transparência, pseudonimização e procedimentos de encriptação, bem como outras precauções técnicas organizacionais devem ser regulamentadas em nível jurídico, uma vez que dizem respeito a questões essenciais do exercício dos direitos fundamentais e, portanto, não podem apenas ser padronizado em norma legal.[135]

Independentemente da possibilidade de disponibilizar os dados do prontuário eletrônico do paciente para fins de pesquisa por meio do processo de transparência de dados, os segurados também podem disponibilizar os dados do prontuário eletrônico do paciente com base exclusiva no consentimento informado (Seção 363 Parágrafo

[135] Posição igualmente crítica se encontra em DOCHOW, Carsten. Das Patienten-Datenschutz-Gesetz (Teil 3): Die Datenspende. *Medizinrecht*, p. 115 ss., 2021. p. 119.

8 SGB V).[136] O regulamento não representa um padrão independente de autoridade para a transferência de dados, de modo que os requisitos para o consentimento informado decorrem diretamente do Artigo 9, Parágrafo 2, Carta a do RGPD, em conjunto com o Artigo 7 do RGPD.[137] No entanto, a finalidade é restringida e os dados só podem ser disponibilizados para um projeto de investigação específico ou para determinadas áreas de investigação científica.[138] Um projeto de pesquisa específico requer, portanto, um projeto de pesquisa especificamente descrito e claramente definido, com objetivos e propósitos específicos.[139] Na prática, isto pode basear-se em projetos de investigação específicos que são frequentemente financiados no setor da saúde pelo Ministério Federal da Educação e Investigação ou pelo Ministério Federal da Saúde. Um projeto de pesquisa específico pode envolver pesquisas sobre opções de tratamento para uma doença metabólica rara. Em contrapartida, o termo "certas áreas de investigação científica" deve ser interpretado de forma mais ampla. É concebível aqui que o consentimento seja concedido para certas áreas de investigação científica, como a investigação médica ou a investigação sobre o cancro.[140] Nestes casos, também devem ser tidos em conta os padrões éticos reconhecidos da investigação científica.[141] Estas podem resultar de recomendações e orientações para garantir boas práticas científicas, de um código de ética ou de regulamentos profissionais.[142] Em qualquer caso, um consentimento tão amplo na acepção do artigo 363º, nº 8 do SGB V, no contexto

[136] DEUTSCHER BUNDESTAG. *Entwurf eines Gesetzes für eine bessere Versorgung durch Digitalisierung und Innovation (Digitale-Versorgung-Gesetz – DVG) 19/18793*. [Publicações do Parlamento Federal] n. 19/18793. 2020. p. 132; cf., quanto a isso, ja BRETTHAUER, Sebastian; APPENZELLER, Arno; BIRNSTILL, Pascal. Datensouveränität für Patienten im Gesundheitswesen: Eine Chance für die medizinische Forschung und den Datenschutz. *Datenschutz und Datensicherheit (DuD)*, v. 45, n. 3, p. 173-179, 2021. p. 173-177 ss.

[137] BRETTHAUER, Sebastian; APPENZELLER, Arno; BIRNSTILL, Pascal. Datensouveränität für Patienten im Gesundheitswesen: Eine Chance für die medizinische Forschung und den Datenschutz. *Datenschutz und Datensicherheit (DuD)*, v. 45, n. 3, p. 173-179, 2021. p. 132; DOCHOW, Carsten. Das Patienten-Datenschutz-Gesetz (Teil 3): Die Datenspende. *Medizinrecht*, p. 115 ss., 2021. p. 122; quanto a isso, também SIMITIS, Spiros; HORNUNG, Gerrit; DÖHMANN, Indra Spiecker gennant (Orgs.). *Datenschutzrecht*: DS-GVO mit BDSG. Baden-Baden: Nomos, 2019. Art. 9, nota de rodapé 32 ss.

[138] DATENSCHUTZKONFERENZ. *Beschluss der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zu Auslegung des Begriffs "bestimmte Bereiche wissenschaftlicher Forschung" im Erwägungsgrund 33 der DS-GVO, 3. April 2019.* Disponível em: https://www.datenschutzkonferenz-online.de/media/dskb/20190405_auslegung_bestimmte_bereiche_wiss_forschung.pdf. Acesso em: 11 jul. 2024.

[139] BRETTHAUER, Sebastian; APPENZELLER, Arno; BIRNSTILL, Pascal. Datensouveränität für Patienten im Gesundheitswesen: Eine Chance für die medizinische Forschung und den Datenschutz. *Datenschutz und Datensicherheit (DuD)*, v. 45, n. 3, p. 173-179, 2021. p. 173-177.

[140] DEUTSCHER BUNDESTAG. *Entwurf eines Gesetzes für eine bessere Versorgung durch Digitalisierung und Innovation (Digitale-Versorgung-Gesetz – DVG) 19/18793*. [Publicações do Parlamento Federal] n. 19/18793. 2020. p. 132.

[141] EG 33 DSGVO. Disponível em: https://dsgvo-gesetz.de/erwaegungsgruende/nr-33/. Acesso em: 12 jul. 2024.

[142] DOCHOW, Carsten. Das Patienten-Datenschutz-Gesetz (Teil 3): Die Datenspende. *Medizinrecht*, p. 115 ss., 2021. p. 122.

da investigação científica, pode definitivamente fazer sentido para a otimização do atendimento ao paciente, a utilização de medicina personalizada ou a utilização de inteligência artificial.[143] No entanto, a forma como os dados serão divulgados na prática de acordo com o §368, parágrafo 8 do SGB V é uma questão em aberto e requer mais esclarecimentos.[144] Isto diz respeito, por exemplo, aos requisitos de prova de consentimento, bem como aos requisitos técnicos e de segurança aquando da transferência de dados do TI para uma possível futura infraestrutura de dados de investigação em rede.[145]

2 Potencial de melhoria do padrão

Com o §363 SGB V, o legislador criou uma norma que, além dos regulamentos de transparência de dados, é dedicada ao processamento de dados do prontuário eletrônico do paciente para fins de pesquisa, regulamenta isso de forma abrangente e explora as vantagens da digitalização na forma de fornecimento e transmissão eletrônica. No entanto, a norma na sua forma atual não é totalmente convincente.

As finalidades para as quais os dados podem ser processados de acordo com a Seção 363 Parágrafo 1 SGB V – as finalidades de acordo com a Seção 303e Parágrafo 2 SGB V são levadas em consideração – são muito amplas. A ligação entre a divulgação de dados para fins de investigação – este é o título da norma para a Secção 363 SGB V – e o apoio associado aos processos de tomada de decisão política para o desenvolvimento do seguro de saúde legal (Secção 303e Parágrafo 2 nº 5 SGB V), bem como o desempenho das tarefas de relatórios de saúde (Seção 303e Parágrafo 2 nº 7 SGB V) não são claros. O legislador aparentemente queria garantir o direito de participar do tesouro de dados e informações armazenados no arquivo eletrônico do paciente.

Também é fundamental avaliar se o segurado não tem influência sobre para quais usuários autorizados os dados divulgados são repassados. A seleção de qual usuário autorizado em qual área de avaliação de dados de acordo com a Seção 303e Parágrafo 2 SGB V recebe os dados e com que finalidade não é feita pelo segurado, mas pelo centro de dados de pesquisa. No entanto, a ideia de soberania

[143] DOCHOW, Carsten. Das Patienten-Datenschutz-Gesetz (Teil 3): Die Datenspende. *Medizinrecht*, p. 115 ss., 2021. p. 122.

[144] A mesma posição se encontra em DOCHOW, Carsten. Das Patienten-Datenschutz-Gesetz (Teil 3): Die Datenspende. *Medizinrecht*, p. 115 ss., 2021. p. 123.

[145] Cf., quanto a isso, BRETTHAUER, Sebastian; APPENZELLER, Arno; BIRNSTILL, Pascal. Datensouveränität für Patienten im Gesundheitswesen: Eine Chance für die medizinische Forschung und den Datenschutz. *Datenschutz und Datensicherheit (DuD)*, v. 45, n. 3, p. 173-179, 2021. p. 173.

dos dados é negada porque o segurado não pode mais influenciar a utilização posterior dos seus dados.[146]

Em última análise, a posição do centro de dados de investigação como um todo será significativamente reforçada. Além de seu papel já central nas regulamentações de transparência de dados, também atua como intermediário no processamento de dados de prontuários eletrônicos de pacientes para fins de pesquisa. Está se transformando em um "supercoletor de dados". Portanto, isto requer salvaguardas especiais, que dizem respeito particularmente aos requisitos de segurança para proteger a sua infraestrutura de TI.[147]

D Inteligência artificial na saúde

A utilização da inteligência artificial (IA) nos cuidados de saúde e na investigação médica é, em última análise, uma das grandes esperanças do século XXI.[148] Em geral, espera-se que a utilização da IA no setor da saúde traga uma melhoria significativa na prevenção e nos cuidados de saúde. Por exemplo, a sua utilização na avaliação de imagens médicas já está bem desenvolvida e difundida.[149] Ao analisar e avaliar numerosos registros médicos, o curso da doença e da terapia pode ser previsto individualmente e, assim, planejado e controlado de forma mais eficaz. Na sala de cirurgia, as informações processadas podem aparecer na ocular do microscópio cirúrgico ou ser preparadas para óculos de realidade aumentada. A IA também é usada em sistemas de assistência inteligentes – como robôs de atendimento. Um alicerce básico essencial para a implantação e utilização da IA no setor da saúde é a extensa recolha, processamento, análise e avaliação de dados

[146] Cf., quanto a isso, também DEUTSCHER ETHIKRAT. *Big Data und Gesundheit*: Datensouveränität als informationelle Freiheitsgestaltung. 2018. Disponível em: https://www.ethikrat.org/fileadmin/Publikationen/Stellungnahmen/deutsch/stellungnahme-big-data-und-gesundheit.pdf. Acesso em: 07 jul. 2024.

[147] Cf., quanto a isso, LASSAHN, Philipp; POSCHER, Ralf. §7. *In*: HORNUNG, Gerrit; SCHALLBRUCH, Martin (Orgs.). *IT-Sicherheitsrecht*: Praxishandbuch. Baden-Baden: Nomos, 2021. §13, nota de rodapé 1 ss.

[148] Cf., quanto a isso, *BUNDESMINISTERIUM FÜR BILDUNG UND FORSCHUNG. Bundesbericht Forschung und Innovation für die Menschen – Die Hightech-Strategie 2015*. 2018. p. 11 ss., 16 ss.; DETTLING, Heinz-Uwe; KRÜGER, Stefan. Digitalisierung, Algorithmisierung und Künstliche Intelligenz im Pharmarecht. *PharmR*, p. 513, 2018. p. 513; KATZENMEIER, Christian. Big Data, E-Health, M-Health, KI und Robotik in der Medizin. *Medizinrecht*, v. 37, p. 259-271, 2019. p. 268; JÖRG, Johannes. *Digitalisierung in der Medizin*: Wie Gesundheits-Apps, Telemedizin, künstliche Intelligenz und Robotik das Gesundheitswesen revolutionieren. Heidelberg: Springer, 2018; HUSS, Ralf. *Künstliche Intelligenz, Robotik und Big Data in der Medizin*. Heidelberg: Springer, 2019; KERSTING, Kristian; LAMPERT, Christoph; ROTHKOPF, Constantin (Orgs.). *Wie Maschinen lernen*: Künstliche Intelligenz verständlich erklärt. Heidelberg: Springer, 2019.

[149] Veja, quanto a isso, BUNDESMINISTERIUM FÜR BILDUNG UND FORSCHUNG. *Digitalisierung und Künstliche Intelligenz*. Disponível em: https://www.gesundheitsforschung-bmbf.de/de/digitalisierung-und-kunstliche-intelligenz-9461.php. Acesso em: 11 jul. 2024.

e informações. Regulamentos para a regulamentação da IA – seja de natureza geral ou específica, seja em nível nacional ou europeu – no entanto, ainda não existem.

I Projeto de regulamento da Comissão Europeia sobre Inteligência Artificial (KIVO-E)

No início de 2021, a Comissão Europeia publicou um projeto de regulamento (KIVO-E) intitulado "Lei da Inteligência Artificial",[150] que visa criar o quadro jurídico para uma inteligência artificial confiável a nível europeu.[151] Pretende-se com isso criar, pela primeira vez no contexto europeu, um quadro que padronize os requisitos gerais para a regulamentação da inteligência artificial. Os regulamentos devem, portanto, também ser aplicados num sistema de saúde digitalizado que queira utilizar ainda mais a IA no futuro do que antes. É necessário garantir que os riscos de segurança que os sistemas de IA representam no setor da saúde sejam adequadamente evitados e mitigados. Portanto, robôs autônomos na assistência e cuidados pessoais, por exemplo, devem ser capazes de trabalhar com segurança e cumprir suas funções mesmo em ambientes complexos. Da mesma forma, os sistemas de diagnóstico cada vez mais sofisticados e os sistemas de apoio às decisões humanas no setor da saúde, onde os riscos para a vida e a integridade física são particularmente elevados, devem ser fiáveis e precisos.[152] Além disso, ao desenvolver determinados sistemas de IA, os atores, como os fornecedores, os organismos notificadores e outros organismos relevantes, como os centros de inovação digital, as instalações de ensaio e experimentais e os investigadores, devem poder aceder e utilizar conjuntos de dados de elevada qualidade nas respetivas áreas de atividade. A ligação com os regulamentos de transparência de dados e com o reforço da interoperabilidade e da cibersegurança é óbvia. No setor da saúde, o Espaço Europeu de Dados de Saúde[153] também se destina a facilitar o acesso não discriminatório aos dados de saúde e a formação de algoritmos de IA utilizando estes conjuntos de dados.[154] O KIVO-E estabelecerá, portanto, também padrões completamente novos para a utilização da IA no setor da saúde e fornecerá

[150] UNIÃO EUROPEIA. *Vorschlag für eine Verordnung des europäischen parlaments und des rates zur festlegung harmonisierter vorschriften für künstliche intelligenz (gesetz über künstliche intelligenz) und zur änderung bestimmter rechtsakte der union*. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52021PC0206. Acesso em: 30 jun. 2024.

[151] Vgl. *Begründung KIVO-E*, S. 1.

[152] *EG 28 KIVO-E.*

[153] Cf. mais detalhes em EUROPEAN COMISSION. *European Health Data Space*. Disponível em: https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en. Acesso em: 10 jul. 2024.

[154] *EG 45 KIVO-E.*

um quadro jurídico uniforme que os fornecedores e utilizadores de sistemas de IA devem aderir (ver artigo 2º do KIVO-E).

Após mais de dois anos de negociações no âmbito das negociações do trílogo, a Comissão, o Conselho Europeu e o Parlamento Europeu chegaram a acordo sobre uma proposta legislativa conjunta no final de 2023, que ainda terá de ser adotada pelo Parlamento.[155] Houve algumas mudanças significativas em comparação com o projeto original da Comissão de 2021.[156]

II A utilização da IA no setor da saúde

Com o artigo 3º, nº 1, do KIVO-E, uma definição de inteligência artificial está agora ancorada na lei pela primeira vez. Um "sistema de inteligência artificial" – como o KIVO-E ainda prevê – é um *software* que foi desenvolvido utilizando uma ou mais das técnicas e conceitos listados no Anexo I[157] e tendo em vista uma série de objetivos definidos pelos humanos, pode produzir resultados como conteúdos, previsões, recomendações ou decisões que influenciam o ambiente com o qual interagem. Tais técnicas e conceitos incluem conceitos de aprendizado de máquina, incluindo aprendizado profundo – o chamado aprendizado profundo –, conceitos lógicos e baseados em conhecimento, bem como abordagens estatísticas e métodos bayesianos de estimativa, pesquisa e otimização. A definição torna-se, portanto, o ponto de partida central que decide se um sistema técnico deve ser avaliado como um sistema de IA.

No entanto, a definição foi inicialmente muito ampla na sua concepção, uma vez que abrangeu também sistemas determinísticos até sistemas especialistas normais, uma vez que os elementos característicos da inteligência artificial, como a imprevisibilidade do seu comportamento e o efeito de caixa negra, não foram mencionados de todo no texto padrão.[158] Os algoritmos convencionais ou os métodos estatísticos foram, portanto, rapidamente suspeitos de se enquadrarem no âmbito

[155] Veja EUROPEAN COMISSION. *Commission welcomes political agreement on Artificial Intelligence Act*. Disponível em: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6473. Acesso em: 11 jul. 2024.

[156] Veja EUROPEAN COUNCIL. *Artificial intelligence act: Council and Parliament strike a deal on the first rules for AI in the world*. Disponível em: https://www.consilium.europa.eu/en/press/press-releases/2023/12/09/artificial-intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide-rules-for-ai/. Acesso em: 11 jul. 2024.

[157] Cf., quanto a isso, UNIÃO EUROPEIA. *Vorschlag für eine Verordnung des europäischen parlaments und des rates zur festlegung harmonisierter vorschriften für künstliche intelligenz (gesetz über künstliche intelligenz) und zur änderung bestimmter rechtsakte der union*. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52021PC0206. Acesso em: 30 jun. 2024.

[158] SPINDLER, Gerald. Der Vorschlag der EU-Kommission für eine Verordnung zur Regulierung der Künstlichen Intelligenz (KI-VO-E). *Computer und Recht*, n. 12, p. 361-374, 2021. p. 363.

do KIVO-E, conduzindo assim a uma regulamentação excessiva. A utilização de *softwares* clássicos para analisar o curso da doença, otimizar medidas terapêuticas ou avaliações gerais de prontuários, dados de pacientes e segurados já atenderia, portanto, às características da inteligência artificial no sentido do KIVO-E. Isto se aplicaria especialmente aos robôs de cuidado e assistência, que, por exemplo, tomam a decisão com base em parâmetros previamente programados entre servir comida a um paciente no hospital ou tocar uma melodia para animá-lo. No entanto, foi avaliado criticamente se os algoritmos convencionais que já são utilizados em aplicações de *software* médico clássico também deveriam ser sujeitos ao KIVO-E. Caso contrário, um grande número de sistemas técnicos no setor da saúde estaria sujeito ao KIVO-E. Isto levaria a uma regulamentação excessiva e, assim, impediria o necessário impulso à inovação.

Esta crítica foi claramente retomada no processo do trílogo. A fim de garantir que a definição de um sistema de IA contém critérios suficientemente claros para distinguir entre IA e sistemas de *software* mais simples, o compromisso agora negociado basear-se-á na abordagem proposta pela OCDE.[159] Assim, um sistema de IA é um sistema baseado em máquina que persegue objetivos explícitos ou implícitos e infere a partir das entradas que recebe como gerar resultados, como previsões, conteúdos, recomendações ou decisões que podem influenciar ambientes físicos ou virtuais. Diferentes sistemas de IA variam no seu grau de autonomia e adaptabilidade dependendo da sua implantação.[160] Em comparação com a proposta do KIVO-E, a definição agora utilizada é mais restrita, pelo que os sistemas especialistas simples já não são abrangidos pela regulamentação. No entanto, a adequação desta abordagem ainda tem de ser comprovada na prática até que ponto a utilização de sistemas automatizados no setor da saúde ainda cumpre os requisitos da IA ou já não os cumpre.

III Sistemas de IA no setor da saúde e seu estatuto jurídico

O KIVO-E adota uma abordagem baseada no risco que contém requisitos obrigatórios para sistemas de IA de alto risco.[161] Os sistemas de IA que representam

[159] Veja EUROPEAN COUNCIL. *Artificial intelligence act: Council and Parliament strike a deal on the first rules for AI in the world*. Disponível em: https://www.consilium.europa.eu/en/press/press-releases/2023/12/09/artificial-intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide-rules-for-ai/. Acesso em: 11 jul. 2024.

[160] Veja OECD. *Updates to the OECD's definition of an AI system explained*. Disponível em: https://oecd.ai/en/wonk/ai-system-definition-update. Acesso em: 11 jul. 2024.

[161] SPINDLER, Gerald. Der Vorschlag der EU-Kommission für eine Verordnung zur Regulierung der Künstlichen Intelligenz (KI-VO-E). *Computer und Recht*, n. 12, p. 361-374, 2021. p. 362.

um risco inaceitável são geralmente proibidos (ver artigo 5º KIVO-E). Isto aplica-se, em particular, aos procedimentos de influência sobre o comportamento, à pontuação social e ao reconhecimento biométrico através da IA, embora a identificação biométrica remota possa ser utilizada para a aplicação da lei em espaços públicos, desde que sejam observadas determinadas medidas de proteção.[162] No entanto, esses sistemas de IA geralmente não desempenham um papel no setor da saúde, uma vez que a IA é utilizada principalmente para melhorar a prevenção e os cuidados de saúde. No entanto, no futuro, será necessário examinar se os sistemas de IA no setor da saúde devem ser classificados como sistemas de IA de alto risco, para que tenham de cumprir os extensos requisitos do artigo 8º e seguintes do KIVO-E. Em qualquer caso, não são abrangidos os sistemas que não sejam suscetíveis de causar violações graves dos direitos fundamentais ou outros riscos significativos.[163] Apenas obrigações de transparência muito baixas seriam aplicáveis aos sistemas de IA com riscos tão limitados. No setor da saúde, haverá, portanto, uma discussão sobre se estes são sistemas de IA de alto risco que estão sujeitos a obrigações mais extensas.

Para definir sistemas de IA de alto risco, o KIVO-E utiliza uma abordagem dupla.[164] Por um lado, o KIVO-E centra-se na utilização de sistemas de IA como elementos relevantes para a segurança em produtos que estão sujeitos à legislação em matéria de segurança dos produtos e a uma avaliação de conformidade por terceiros e, por outro lado, para os sistemas de IA, existe um anexo III abrangente, que compreende determinados sistemas de IA *per se* classificados como de alto risco (cf. Art. 6 KIVO-E.). O primeiro grupo inclui todos os sistemas de IA utilizados na área de dispositivos médicos.[165] Isto afeta um grande número de sistemas correspondentes. As áreas típicas de aplicação incluem radiologia, cardiologia, endocrinologia e oncologia, que dependem cada vez mais do uso de IA. No futuro, tais aplicações deverão ser avaliadas em relação ao KIVO-E. O segundo grupo mencionado inclui sistemas de IA que impactam principalmente os direitos fundamentais. Os sistemas de IA no setor da saúde não desempenham obviamente aqui qualquer papel, uma vez que não são mencionados no anexo III. Ou porque o

[162] Veja EUROPEAN COUNCIL. *Artificial intelligence act: Council and Parliament strike a deal on the first rules for AI in the world*. Disponível em: https://www.consilium.europa.eu/en/press/press-releases/2023/12/09/artificial-intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide-rules-for-ai/. Acesso em: 11 jul. 2024.

[163] Veja EUROPEAN COUNCIL. *Artificial intelligence act: Council and Parliament strike a deal on the first rules for AI in the world*. Disponível em: https://www.consilium.europa.eu/en/press/press-releases/2023/12/09/artificial-intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide-rules-for-ai/. Acesso em: 11 jul. 2024.

[164] SPINDLER, Gerald. Der Vorschlag der EU-Kommission für eine Verordnung zur Regulierung der Künstlichen Intelligenz (KI-VO-E). *Computer und Recht*, n. 12, p. 361-374, 2021. p. 365.

[165] *Art. 6 Abs. 1 KIVO-E iVm Anhang II, Abschnitt A Nr. 11 zu KIVO-E*.

organismo de normalização considera que o setor da saúde já está abrangido pelo setor dos dispositivos médicos ou porque não está suficientemente consciente do risco específico da utilização da IA neste domínio. Uma melhoria subsequente é, portanto, indicada. Caso contrário, continua a ser verdade que apenas a utilização de sistemas de IA no setor dos dispositivos médicos está sujeita aos extensos requisitos do KIVO-E (ver artigo 8º e seguintes do KIVO-E).

IV Requisitos legais para sistemas de IA no setor da saúde

Para sistemas de IA de alto risco no setor da saúde, deve então ser estabelecido um sistema de gestão de riscos (Art. 9 KIVO-E), que deve ser atualizado regularmente ao longo de todo o ciclo de vida do sistema de IA. Isto é visto como um processo iterativo contínuo ao longo de todo o ciclo de vida de um sistema de IA e inclui, por exemplo, identificação, análise e avaliação de riscos, bem como a implementação associada de medidas de gestão de riscos (ver Artigo 9, Parágrafo 2 KIVO-E). No futuro, os fornecedores e utilizadores de sistemas de IA no setor da saúde terão de estar preparados para o fato de que esta tarefa só pode ser realizada com recursos humanos e financeiros significativos e que, por conseguinte, devem ser criadas estruturas adequadas.

Outro aspecto importante na regulamentação da IA diz respeito à qualidade dos dados. Isto é particularmente importante na pesquisa médica. Os algoritmos subjacentes à inteligência artificial baseiam-se frequentemente na análise de grandes quantidades de dados, razão pela qual a regulação destes dados utilizados é de considerável importância. Garantir a qualidade dos dados é, portanto, um prerrequisito essencial para sistemas de IA fiáveis. Isto deve aplicar-se especialmente aos sistemas nos setores da saúde e médico. O artigo 10º KIVO-E também retoma esta abordagem. Assim, os sistemas de IA de alto risco que utilizam técnicas nas quais os modelos são desenvolvidos com conjuntos de dados de treinamento, validação e teste devem atender a critérios de qualidade específicos. Os conjuntos de dados utilizados para treinar a IA devem cumprir práticas adequadas de gestão de dados. Isto aplica-se, por exemplo, à preparação e avaliação de dados e também às investigações relativas a possíveis distorções. Além disso, devem ser relevantes, representativos, isentos de erros e completos (Art. 10 Parágrafo 3 KIVO-E). No entanto, surge sempre a questão de saber se é mesmo possível, do ponto de vista técnico, garantir esta qualidade muito elevada. Deve ser esclarecido se os elevados requisitos para que os dados de treinamento sejam representativos e livres de erros podem ser atendidos. O mesmo se aplica à integridade dos dados. O KIVO-E não aborda de modo algum a forma como a utilização de dados

sintéticos[166] em diferentes contextos pode substituir o processamento de dados reais e até que ponto os dados sintéticos se baseiam nas propriedades dos dados reais. Esses conjuntos de dados podem ser utilizados de forma particularmente lucrativa no setor da saúde se forem utilizados como conjuntos de dados gêmeos para permitir estudos em que os requisitos particularmente elevados de proteção de dados tornem difícil trabalhar com dados reais.[167] É, portanto, necessário aprofundar estas considerações e uniformizá-las num regulamento final.[168]

Finalmente, os sistemas de IA são frequentemente caracterizados pelo chamado problema da caixa preta, em que a rastreabilidade dos resultados gerados pela IA permanece obscura. Tendo em conta esta complexidade específica, a procura de transparência, explicabilidade e rastreabilidade na prática é confrontada com o fato de que muitas vezes é dificilmente possível, mesmo para especialistas, compreender e compreender plenamente todos os componentes individuais de um sistema e a sua interação. Isto é particularmente verdadeiro para métodos individuais de aprendizagem automática utilizados no setor da saúde. Pela primeira vez, o KIVO-E contém agora dois regulamentos (artigo 12º e artigo 13º KIVO-E) (registro e transparência) que se destinam a ter em conta este problema.

Os sistemas de IA de alto risco devem ser concebidos e desenvolvidos com funcionalidades funcionais que permitam o registro automático de processos e eventos – ou seja, o registro – durante o funcionamento dos sistemas de IA de alto risco. O registro deve garantir que o funcionamento do sistema de IA seja rastreável ao longo de todo o seu ciclo de vida, numa medida adequada à finalidade do sistema (artigo 12º KIVO-E).

Do mesmo modo, os sistemas de IA de alto risco devem ser concebidos e desenvolvidos de modo que o seu funcionamento seja suficientemente transparente para que os utilizadores possam interpretar e utilizar adequadamente os resultados do sistema (artigo 13º KIVO-E). No entanto, os requisitos técnicos específicos que devem existir para cumprir os requisitos legais permanecem pouco claros, e o projeto de regulamento perde-se numa infinidade de termos jurídicos vagos. Ainda não está claro qual ator ou atores precisam ser rastreáveis. É suficiente que o médico assistente consiga compreender o resultado ou o paciente também tenha que ser capaz de compreender a decisão da IA? Neste ponto, são necessários critérios precisos e suficientemente específicos. Dependendo do contexto, as

[166] *Art. 6 Abs. 1 KIVO-E iVm Anhang II, Abschnitt A Nr. 11 zu KIVO-E.*

[167] Cf. MECKEL, Miriam. *Realität auf Abruf: Synthetische Daten sind die Zukunft der KI.* Disponível em: https://www.handelsblatt.com/meinung/kolumnen/kolumne-kreative-zerstoerung-realitaet-auf-abruf-synthetische-daten-sind-die-zukunft-der-ki/27286854.html. Acesso em: 11 jul. 2024.

[168] Cf., quanto a isso, já DATENETHIKKOMMISSION. *Gutachten der Datenethikkommission.* Disponível em: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?__blob=publicationFile&v=6. Acesso em: 07 jul. 2024. p. 132.

decisões não precisam ser compreensíveis para todas as pessoas. Em vez disso, uma distinção deve ser feita com base no contexto de uso. Os critérios podem basear-se no nível de compreensão das pessoas afetadas. Existe também a opção de regulamentação específica do setor, que exige requisitos diferentes dependendo do contexto. Por exemplo, se no setor da mobilidade for oferecida ao utilizador a rota errada devido a uma decisão incorreta da IA, isso não terá consequências tão abrangentes como se um paciente sofresse uma desvantagem de saúde no setor da saúde como resultado de uma decisão incorreta da IA. Estas considerações devem ser levadas em conta ao projetar a rastreabilidade. Em última análise, os sistemas de IA no setor da saúde requerem supervisão humana e, em particular, devem ser protegidos contra ataques cibernéticos.[169]

E Conclusão e perspectivas

A digitalização do sistema de saúde alemão está a progredir rapidamente e é enquadrada por inúmeras leis. Com o DigiG, a legislatura aborda a melhoria da interoperabilidade e o aumento da segurança cibernética como dois blocos centrais para um sistema de saúde moderno e preparado para o futuro. A interoperabilidade dos numerosos sistemas informáticos utilizados é necessária para permitir, de um modo geral, o intercâmbio de dados e informações entre os atores envolvidos. Além disso, a cibersegurança deve ser tida em conta e aumentada porque o setor da saúde está cada vez mais exposto a ataques cibernéticos. Com os regulamentos de transparência de dados, bem como os regulamentos sobre TI e pesquisa com dados do prontuário eletrônico do paciente no DVG e PDSG, o legislador deu mais um passo importante em direção a um sistema de saúde moderno e digitalizado. O centro de dados de investigação, em particular, tem um papel central a desempenhar, que determinará se a investigação que utiliza dados de pacientes e segurados pode ser mais direcionada e eficaz no futuro. Em última análise, a utilização da IA nos cuidados de saúde está associada ao desejo de conduzir a prevenção e os cuidados de saúde para uma nova era. Os desafios resultantes devem ser enfrentados, apoiados legalmente, contidos e controlados por um regulamento europeu para a regulamentação da inteligência artificial. No entanto, ainda é necessário fazer ajustamentos nesta altura e também é necessário estabelecer regulamentações nacionais.[170] No entanto, isto está longe de ser o fim

[169] Cf., quanto aos detalhes, Art. 14 e Art. 15 *KIVO-E*.

[170] Cf., quanto a isso, já DATENETHIKKOMMISSION. *Gutachten der Datenethikkommission*. Disponível em: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?__blob=publicationFile&v=6. Acesso em: 07 jul. 2024.

e são necessários mais esforços para entusiasmar todos os envolvidos com um sistema de saúde digitalizado e, ao mesmo tempo, levá-los consigo.

Referências

BECKER, Ulrich; KINGREEN, Thorsten. *SGB V*: Gesetzliche Krankenversicherung. München: C.H. Beck, 2022.

BITKOM. *Stellungnahme zum Referentenentwurf eines Gesetzes zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz)*. Berlin, 2023. Disponível em: https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/Gesetze_und_Verordnungen/Stellungnahmen_WP20/DigiG/stellungnahme_bitkom.pdf. Acesso em: 10 jul. 2024.

BRETTHAUER, Sebastian; APPENZELLER, Arno; BIRNSTILL, Pascal. Datensouveränität für Patienten im Gesundheitswesen: Eine Chance für die medizinische Forschung und den Datenschutz. *Datenschutz und Datensicherheit (DuD)*, v. 45, n. 3, p. 173-179, 2021.

BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK. *Die Lage der IT-Sicherheit in Deutschland 2023*. Disponível em: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.pdf?__blob=publicationFile&v=7. Acesso em: 07 jul. 2024.

BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK. *Lagebild Gesundheit*: Cyber-Sicherheit im Gesundheitswesen 2022. Disponível em: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Lagebild_Gesundheit_2022.pdf?__blob=publicationFile&v=6. Acesso em: 10 jul. 2024.

BUNDESGESETZBLATT. *Bundesgesetzblatt Teil I* [= Diário Oficial Federal]. Disponível em: https://www.recht.bund.de/de/bundesgesetzblatt/bgbl-1/bgbl-1_node.html. Acesso em: 10 jul. 2024.

BUNDESKRIMINALAMT. *Cybercrime*: Bundeslagebild 2021. Disponível em: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2021.pdf?__blob=publicationFile&v=6. Acesso em: 10 jul. 2024.

BUNDESMINISTERIUM DER JUSTIZ. *Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG)*. Disponível em: https://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html. Acesso em: 07 jul. 2024.

BUNDESMINISTERIUM DER JUSTIZ. *Verordnung zur Umsetzung der Vorschriften über die Datentransparenz (Datentransparenzverordnung – DaTraV)*. Disponível em: https://www.gesetze-im-internet.de/datrav_2020/BJNR137110020.html. Acesso em: 11 jul. 2024.

BUNDESMINISTERIUM FÜR BILDUNG UND FORSCHUNG. *Bundesbericht Forschung und Innovation für die Menschen – Die Hightech-Strategie 2015*. 2018.

BUNDESMINISTERIUM FÜR BILDUNG UND FORSCHUNG. *Digitalisierung und Künstliche Intelligenz*. Disponível em: https://www.gesundheitsforschung-bmbf.de/de/digitalisierung-und-kunstliche-intelligenz-9461.php. Acesso em: 11 jul. 2024.

BUNDESMINISTERIUM FÜR GESUNDHEIT. *Stellungnahme der Gesellschaft für Qualitätsmanagement in der Gesundheitsversorgung e.V. (GQMG) zum Referentenentwurf des Bundesministeriums für Gesundheit über das Gesetz zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG)*.

Disponível em: https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/Gesetze_und_Verordnungen/Stellungnahmen_WP20/DigiG/stellungnahme_gqmg.pdf. Acesso em: 07 jul. 2024.

BUNDESVERFASSUNGSGERICHT. *BVerfGE, 65, 1 (43)*. Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1983/12/rs19831215_1bvr020983.html. Acesso em: 12 jul. 2024.

BUNDESVERFASSUNGSGERICHT. *BVerfGE*: Entscheidungen des Bundesverfassungsgerichts. [Decisões do Tribunal Constitucional Federal], 120, 274-350. Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227_1bvr037007.html. Acesso em: 07 jul. 2024.

BverwGE. *Entscheidungen des Bundesverwaltungsgerichts* [= Decisões do Tribunal Administrativo Federal], 42, 26 (28).

BverwGE. *Entscheidungen des Bundesverwaltungsgerichts* [= Decisões do Tribunal Administrativo Federal], 49, 16 (23)

DARMS, Martin; HAβFELD, Stefan; FEDTKE, Stephen. *IT-Sicherheit und Datenschutz im Gesundheitswesen*: Leitfaden für Ärzte, Apotheker, Informatiker und Geschäftsführer in Klinik und Praxis. Wiesbaden: Springer Vieweg, 2019.

DATENETHIKKOMMISSION. *Gutachten der Datenethikkommission*. Disponível em: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?__blob=publicationFile&v=6. Acesso em: 07 jul. 2024.

DATENSCHUTZKONFERENZ. *Beschluss der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zu Auslegung des Begriffs "bestimmte Bereiche wissenschaftlicher Forschung" im Erwägungsgrund 33 der DS-GVO, 3. April 2019.* Disponível em: https://www.datenschutzkonferenz-online.de/media/dskb/20190405_auslegung_bestimmte_bereiche_wiss_forschung.pdf. Acesso em: 11 jul. 2024.

DEHMEL, Susanne; HULLEN, Nils. Auf dem Weg zu einem zukunftsfähigen Datenschutz in Europa? Konkrete Auswirkungen der DS-GVO auf Wirtschaft, Unternehmen und Verbraucher. *Zeitschrift für Datenschutz*, ano 3, n. 4, p. 147-153, 2013.

DETTLING, Heinz-Uwe; KRÜGER, Stefan. Digitalisierung, Algorithmisierung und Künstliche Intelligenz im Pharmarecht. *PharmR*, p. 513, 2018.

DEUTSCHE KRANKENHAUSGESELLSCHAFT. *Branchenspezifischer Sicherheitsstandard "Medizinische Versorgung".* Version 1.2, 2022. Disponível em: https://www.dkgev.de/fileadmin/default/Mediapool/2_Themen/2.1_Digitalisierung_Daten/2.1.4._IT-Sicherheit_und_technischer_Datenschutz/2.1.4.1._IT-Sicherheit_im_Krankenhaus/Branchenspezifischer_Sicherheitsstandard_Medizinische_Versorgung_v1.2_Stand_2022-12-08.pdf. Acesso em: 07 jul. 2024.

DEUTSCHE KRANKENHAUSGESELLSCHAFT. *Stellungnahme der Deutschen Krankenhausgesellschaft zum Referentenentwurf eines Gesetzes zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz)*. 2023. Disponível em: https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/Gesetze_und_Verordnungen/Stellungnahmen_WP20/DigiG/stellungnahme_dkg.pdf. Acesso em: 07 jul. 2024.

DEUTSCHER BUNDESRAT. *Entwurf eines Gesetzes zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG) 435/23*. [Publicações do Parlamento Federal] n. 435/23. 2023.

DEUTSCHER BUNDESRAT. *Entwurf eines Gesetzes zur verbesserten Nutzung von Gesundheitsdaten (Gesundheitsdatennutzungsgesetz – GDNG) 434/23*. [Publicações do Parlamento Federal] n. 434/23. 2023.

DEUTSCHER BUNDESTAG. *Entwurf eines Gesetzes für ein Zukunftsprogramm Krankenhäuser (Krankenhauszukunftsgesetz – KHZG) 19/22126*. [Publicações do Parlamento Federal] n. 19/22126. 2020.

DEUTSCHER BUNDESTAG. *Entwurf eines Gesetzes für eine bessere Versorgung durch Digitalisierung und Innovation (Digitale-Versorgung-Gesetz – DVG) 19/13438*. [Publicações do Parlamento Federal] n. 19/13438. 2015.

DEUTSCHER BUNDESTAG. *Entwurf eines Gesetzes für eine bessere Versorgung durch Digitalisierung und Innovation (Digitale-Versorgung-Gesetz – DVG) 19/18793*. [Publicações do Parlamento Federal] n. 19/18793. 2020.

DEUTSCHER BUNDESTAG. *Entwurf eines Gesetzes für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen 18/5293*. [Publicações do Parlamento Federal] n. 18/5293. 2015.

DEUTSCHER BUNDESTAG. *Entwurf eines Gesetzes zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG) 20/9048*. [Publicações do Parlamento Federal] n. 20/9048. 2023.

DEUTSCHER BUNDESTAG. *Entwurf eines Gesetzes zur digitalen Modernisierung von Versorgung und Pflege (Digitale-Versorgung-und-Pflege-Modernisierungs-Gesetz – DVPMG) 19/27652*. [Publicações do Parlamento Federal] n. 19/27652. 2021.

DEUTSCHER BUNDESTAG. *Entwurf eines Gesetzes zur verbesserten Nutzung von Gesundheitsdaten (Gesundheitsdatennutzungsgesetz – GDNG) 20/9046*. [Publicações do Parlamento Federal] n. 20/9046. 2023.

DEUTSCHER ETHIKRAT. *Big Data und Gesundheit*: Datensouveränität als informationelle Freiheitsgestaltung. 2018. Disponível em: https://www.ethikrat.org/fileadmin/Publikationen/Stellungnahmen/deutsch/stellungnahme-big-data-und-gesundheit.pdf. Acesso em: 07 jul. 2024.

DITTRICH, Tilmann; IPPACH, Jan. IT-Sicherheit betrifft nicht nur Großkrankenhäuser – die Regulierung der IT-Sicherheit im ambulanten und stationären Bereich. *GesundhaeitsRecht*, n. 5, p. 285 ss., 2021.

DOCHOW, Carsten. Das Patienten-Datenschutz-Gesetz (Teil 1): Die elektronische Gesundheitskarte und Telematikinfrastruktur. *Medizinrecht*, n. 38, p. 979-993, 2020.

DOCHOW, Carsten. Das Patienten-Datenschutz-Gesetz (Teil 3): Die Datenspende. *Medizinrecht*, p. 115 ss., 2021.

DÖHMANN, Indra Spiecker gen.; BRETTHAUER, Sebastian. Das Digitale-Versorgung-Gesetz als Einfallstor für eine Neujustierung von einstweiligem Rechtsschutz vor dem BVerfG und der Eingriffsqualität bei Datenverwendungen. *Juristen Zeitung (JZ)*, Ano 75, n. 20, p. 990-996, 2020. Disponível em: https://www.mohrsiebeck.com/artikel/das-digitale-versorgung-gesetz-als-einfallstor-fuer-eine-neujustierung-von-einstweiligem-rechtsschutz-vor-dem-bverfg-und-der-eingriffsqualitaet-bei-datenverwendungen-101628jz-2020-0326/?no_cache=1. Acesso em: 10 jul. 2024.

EG 33 DSGVO. Disponível em: https://dsgvo-gesetz.de/erwaegungsgruende/nr-33/. Acesso em: 12 jul. 2024.

EUROPEAN COMISSION. *Commission welcomes political agreement on Artificial Intelligence Act*. Disponível em: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6473. Acesso em: 11 jul. 2024.

EUROPEAN COMISSION. *European Health Data Space*. Disponível em: https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en. Acesso em: 10 jul. 2024.

EUROPEAN COUNCIL. *Artificial intelligence act: Council and Parliament strike a deal on the first rules for AI in the world*. Disponível em: https://www.consilium.europa.eu/en/press/press-releases/2023/12/09/artificial-intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide-rules-for-ai/. Acesso em: 11 jul. 2024.

EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA). *ENISA threat landscape*: Health Sector. 2023. Disponível em: https://www.enisa.europa.eu/publications/health-threat-landscape/@@download/fullReport. Acesso em: 07 jul. 2024.

FIX, Alexander Daniel. *Das Recht auf Datenportabilität*: Art. 20 DSGVO als Schnittstelle zwischen Wettbewerbsförderung und Datenschutz. Berlim: Peter Lang, 2022.

GEMATIK. *Stellungnahme der gematik zum Referentenentwurf eines Gesetzes zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG)*. Disponível em: https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/Gesetze_und_Verordnungen/Stellungnahmen_WP20/DigiG/stellungnahme_gematik.pdf. Acesso em: 07 jul. 2024.

HÄNLEIN, Andreas; SCHULER, Rolf. (Orgs.) *Sozialgesetzbuch V*: Gesetzliche Krankenversicherung. 6. ed. Baden-Baden: Nomos, 2022.

HEINICKEL, Caroline; FEILER, Lukas. Der Entwurf für ein IT-Sicherheitsgesetz – europarechtlicher Kontext und die (eigentlichen) Bedürfnisse der Praxis. *Computer und Recht*, n. 11, p. 708-714, 2014.

HEISE ONLINE. *Cyberangriff auf Kliniken in Ostwestfalen*. Disponível em: https://www.heise.de/news/Cyberangriff-auf-Kliniken-in-Ostwestfalen-9582719.html. Acesso em: 10 jul. 2024.

HELISCH, Michael; POKOYSKI, Dietmar (Orgs.). *Security Awareness*: Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung. Wiesbaden: Vieweg & Teubner, 2009.

HUSS, Ralf. *Künstliche Intelligenz, Robotik und Big Data in der Medizin*. Heidelberg: Springer, 2019.

INFORMATION SECURITY MANAGEMENT. *ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements*. Disponível em: https://pecb.com/whitepaper/iso-27001-information-technology–security-techniques-information-security–management-systems–requirements. Acesso em: 07 jul. 2024.

JARASS, Hans D. *Charta der Grundrechte der Europäischen Union*. 4 Ed. Frankfurt: C. H. Beck, 2021.

JÖRG, Johannes. *Digitalisierung in der Medizin*: Wie Gesundheits-Apps, Telemedizin, künstliche Intelligenz und Robotik das Gesundheitswesen revolutionieren. Heidelberg: Springer, 2018.

JÜLICHER, Tim; RÖTTGEN, Charlotte; VON SCHÖNFELD, M*ax*. Das Recht auf Datenübertragbarkeit – Ein datenschutzrechtliches Novum. *Zeitschrift für Datenschutz*, p. 358-362, 2016.

KAHL, Wolfgang; LUDWIGS, Markus. *Handbuch des Verwaltungsrechts*. Heidelberg: C.F. Müller, 2023.

KASSENÄRTZLICHE BUNDESVEREINIGUNG. *Entwurf eines gesetzes zur beschleunigung der digitalisierung des gesundheitswesens (Digital-Gesetz – DIGIG)*. Disponível em: https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/Gesetze_und_Verordnungen/Stellungnahmen_WP20/DigiG/stellungnahme_kbv.pdf. Acesso em: 10 jul. 2024.

KASSENÄRTZLICHE BUNDESVEREINIGUNG. *Richtlinie nach §75b SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit*. 2020. Disponível em: https://www.kbv.de/media/sp/RiLi___75b_SGB_V_Anforderungen_Gewaehrleistung_IT-Sicherheit.pdf. Acesso em: 10 jul. 2024.

KATZENMEIER, Christian. Big Data, E-Health, M-Health, KI und Robotik in der Medizin. *Medizinrecht*, v. 37, p. 259-271, 2019.

KELBER, Ulrich. Datensouveränität und Digitalisierung. *Soziale Sicherheit*, n. 3, 2022.

KERKMANN, Christof; NAGEL, Lars-Marten. *Todesfall nach Hackerangriff auf Uni-Klinik Düsseldorf*. Disponível em: https://www.handelsblatt.com/technik/cycberkriminalitaet-todesfall-nach-hackerangriff-auf-uni-klinik-duesseldorf/26198688.html. Acesso em: 10 jul. 2024.

KERSTING, Kristian; LAMPERT, Christoph; ROTHKOPF, Constantin (Orgs.). *Wie Maschinen lernen*: Künstliche Intelligenz verständlich erklärt. Heidelberg: Springer, 2019.

KÜHLING, Jürgen; SCHILDBACH, Roman. Die Reform der Datentransparenzvorschriften im SGB V. *Neue Zeitschrift für Sozialrecht*, n. 41, 2020.

KÜHLING, Martini. Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?. *Europäische Zeitschrift für Wirtschaftsrecht*, número 12, p. 448, 2016.

LASSAHN, Philipp; POSCHER, Ralf. §7. *In*: HORNUNG, Gerrit; SCHALLBRUCH, Martin (Orgs.). *IT-Sicherheitsrecht*: Praxishandbuch. Baden-Baden: Nomos, 2021.

MACHO, Andreas. *"Hacker-Angriffe auf Kliniken nehmen zu"* – obwohl sie Leben kosten. Disponível em: https://www.welt.de/wirtschaft/article246400880/Krankenhaeuser-Hacker-Angriffe-nehmen-zu-obwohl-sie-Leben-kosten.html. Acesso em: 12 jul. 2024.

MARKUS, Heike; MEUCHE, Thomas. *Auf dem Weg zur digitalen Verwaltung*: Ein ganzheitliches Konzept für eine gelingende Digitalisierung in der öffentlichen Verwaltung. Wiesbaden: Springer Gabler, 2022.

MAYER, Peter; BALLREICH, Fabian; DÜZGÜN; SCHWARTZ, Christian; VOLKAMER, Melanie. Erstellung von effektiven Sensibilisierungsmaterialien zur Passwortsicherheit. *Datenschcutz und Datensicherheit – DuD*, v. 44, p. 522-527, 2020.

MECKEL, Miriam. *Realität auf Abruf: Synthetische Daten sind die Zukunft der KI*. Disponível em: https://www.handelsblatt.com/meinung/kolumnen/kolumne-kreative-zerstoerung-realitaet-auf-abruf-synthetische-daten-sind-die-zukunft-der-ki/27286854.html. Acesso em: 11 jul. 2024.

MÜLLMANN, Dirk; VEIT, Maxime; VOLKAMER, Melanie. Weiterleitungs-URLs in e-mails. *Datenschcutz und Datensicherheit – DuD*, n. 5, p. 275 ss., 2023.

OECD. *Updates to the OECD's definition of an AI system explained*. Disponível em: https://oecd.ai/en/wonk/ai-system-definition-update. Acesso em: 11 jul. 2024.

ROLFS, Christianl GIESEN, Richard; KREIKEBOHM, Ralf; MESSLING, Miriam; UDSCHING, Peter. *BeckOK Sozialrecht*. 61. Edition, München: C.H. Beck, [2012].

SCHNEIDER, Uwe K. *Sekundärnutzung klinischer Daten*: Rechtliche Rahmenbedingungen. Berlin: MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, 2015.

SCHOCH, Friedrich; SCHNEIDER, Jens-Peter. *Verwaltungsrecht VwVfG*: 3. Ergänzungslieferung. München: C.H. Beck, 2022.

SEIBEL, Mark. Abgrenzung der "allgemein anerkannten Regeln der Technik" vom "Stand der Technik". *Neue Juristische Wochenschrift*, n. 41, p. 3000, 2013.

SIMITIS, Spiros; HORNUNG, Gerrit; DÖHMANN, Indra Spiecker gennant (Orgs.). *Datenschutzrecht*: DS-GVO mit BDSG. Baden-Baden: Nomos, 2019.

SPINDLER, Gerald. Der Vorschlag der EU-Kommission für eine Verordnung zur Regulierung der Künstlichen Intelligenz (KI-VO-E). *Computer und Recht*, n. 12, p. 361-374, 2021.

STELKENS, Paul; BONK, Heiz Joachim; SACHS, Michael. *VwVfG*: Verwaltungsverfahrengesetz. 10 ed. München: C.H. Beck, 2023.

THÜSING, Gregor; ROMBEY, Sebastian. Forschung im Gesundheitswesen: Anforderungen an einen passgenauen Datenschutz. *Neue Zeitschrift für Sozialrecht*, p. 201-205, 2019.

UNIÃO EUROPEIA. *Directiva 2001/95/CE do Parlamento Europeu e do Conselho, de 3 de dezembro de 2001, relativa à segurança geral dos produtos (Texto relevante para efeitos do EEE)*. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32001L0095. Acesso em: 07 jul. 2024.

UNIÃO EUROPEIA. *Regulamento Geral sobre a Proteção de Dados (RGP)*. Disponível em: https://eur-lex.europa.eu/PT/legal-content/summary/general-data-protection-regulation-gdpr.html. Acesso em: 30 jun. 2024.

UNIÃO EUROPEIA. *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 (Text with EEA relevance.)*. Disponível em: https://eur-lex.europa.eu/eli/reg/2017/745/oj. Acesso em: 30 jun. 2024.

UNIÃO EUROPEIA. *Vorschlag für eine Verordnung des europäischen parlaments und des rates zur festlegung harmonisierter vorschriften für künstliche intelligenz (gesetz über künstliche intelligenz) und zur änderung bestimmter rechtsakte der union*. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52021PC0206. Acesso em: 30 jun. 2024.

UP KRITIS. *Branchenspezifischer Sicherheitsstandard für gesetzliche Kranken- und Pflegeversicherer B3S-GKV/PV*. 2023. Disponível em: https://www.vdek.com/Service/brachenspezifischer-sicherheitsstandard-b3s-gkv-pv/_jcr_content/par/download/file.res/B3S_GKV-PV_V.1.3.28_final.pdf. Acesso em: 12 jul. 2024.

VOLKAMER, Melanie; SASSE, Martina A.; BOEHM, Franziska. Phishing: Kampagnen zur Steigerung der Mitarbeiter-Awareness. *Datenschcutz und Datensicherheit – DuD*, v. 44, p. 518-521, 2020.

WEBER, Kristin; SCHÜTZ, Andreas E.; FERTIG, Tobias. *Grundlagen und Anwendung von Information Security Awareness*: Mitarbeiter zielgerichtet für Informationssicherheit sensibiliesieren. Wiesbaden: Springer Vieweg, 2019.

WEICHERT, Thilo. "Datentransparenz" und Datenschutz. *Medizinrecht*, v. 38, p. 539-546, 2020.

WEICHERT, Thilo. Die Forschungsprivilegierung in der DS-GVO. *Zeitschrift für Datenschutz*, v. 18, p. 21 ss., 2020.

Informação bibliográfica deste texto, conforme a NBR 6023:2018 da Associação Brasileira de Normas Técnicas (ABNT):

BRETTHAUER, Sebastian. Um sistema de saúde digital na Alemanha – Cibersegurança, proteção de dados e inteligência artificial. *Direitos Fundamentais & Justiça*, Belo Horizonte, ano 18, n. 50, p. 19-65, jan./jun. 2024.

Submissão: 13.03.2024
Aceite: 28.06.2024
Cota convite