环球首发

《欧盟人工智能法案》的背景、主要内容与评价

——兼论该法案对劳动法的影响*

[德]沃尔夫冈·多伊普勒

内容提要:为了应对人工智能系统带来的各种挑战,《欧盟人工智能法案》采用基于风险分类的监管路径。法案首先明确禁止了某些存在不可接受风险的人工智能系统,然后重点规制高风险人工智能系统,任何在欧盟市场上提供此类系统的企业都必须满足法案规定的从风险管理、数据治理到全面的记录义务等诸多要求。但是,法案的监管要求可能造成小微企业负担过重,模糊的规定也可能导致实施方面的困难。在劳动关系领域,对雇员进行社会评分、预测雇员犯罪风险、分析雇员情绪等人工智能系统可能因为存在不可接受的风险而被禁止。对岗位申请者和雇员使用人工智能系统的,则根据是否属于高风险系统而负担不同的义务。除了要让雇主向雇员提供相关人工智能技能培训以外,工作中使用 ChatGPT 的问题也值得关注。

关键词:欧盟　人工智能法案　风险分类　劳动法　ChatGPT

沃尔夫冈·多伊普勒(Wolfgang Däubler),德国不来梅大学法学院教授。

一　引　言

(一)当下人工智能的发展

在德国和欧盟,人工智能正在不断征服新的应用领域。无论是医疗诊断、自动驾驶还是生产过程控制,人工智能的应用无处不在,其往往可以加快甚至改善流程。〔1〕企业和

* 本文为作者在全世界范围内首发。本文由上海政法学院教授王倩译,上海交通大学凯原法学院副教授朱军校,特此致谢。

〔1〕 Vgl. U. Meyer, Künstliche Intelligenz im Personalmanagement und Arbeitsrecht, NJW 2023, 1841, 1841 f; Holthausen, Einsatz künstlicher Intelligenz im HR-Bereich und Anforderungen an die „schöne neue Arbeitswelt X.0", RdA 2023, 361, 361 ff.

公共机构的人力资源部门的工作也离不开人工智能的支持,比如系统会对应聘材料进行分类,还会剔除某些不符合形式要求的文件。人工智能系统还可以用来判断某人是否适合特定职位,也可用于裁员或其他的人员精简过程。德国劳工部长海尔(Hubertus Heil)预测,最迟到 2035 年,世界上将没有与人工智能应用无关的工作。[2]

所有这些表现背后隐含着统一的效应。在机器时代,各种机器为劳动人民分担了一些繁重的体力劳动,后来相当多的脑力劳动由计算机来完成,尤其类似计算大量数字或纠正拼写错误等常规任务。现在,人工智能正在将更大比例的脑力劳动从人类转移给机器,ChatGPT 在欧洲的风靡是最好的例子。其不仅威胁到了“演讲稿撰写人”这一收入不错的职业,而且可以预见今后可能有人会非法使用 ChatGPT 来解答各种考试题。又比如,DeepL 可以在多种语言之间完成质量很不错的翻译工作,同样使得翻译的职业前景黯淡。

此类现象引发了德国及世界范围内关于人工智能的广泛讨论。人工智能会在不久的将来超越人类智能吗?人类将只能从事小部分智力劳动吗?除这些忧虑外,在可预见的未来还存在着更为具体的风险和不利因素。相关系统的决策过程对于受影响的人来说不再透明,甚至专家也往往无法破解。如果人工智能所依据的训练材料存在缺陷,比如它只承认人的某些积极特征,就可能导致对不具备这些特征或仅较少具备这些特征的人的无端歧视。这种歧视可能在招聘过程中或发放贷款时显现出来,现有的不平等还可能会加剧。此外,还存在各种滥用的风险:在竞选期间,社交媒体上会出现一个伪造的“人”。此“人”被塑造得像某个候选人,然后在社交媒体上表现得像是一个自相矛盾的人或诽谤者。这些所谓的深度伪造已经成为现实。[3]

(二)立法者的应对

1. 存在哪些规制需求?

新技术并不一定需要新法律。民法中的许多规定非常抽象,完全可以适用于新现象。不管出售的是牲畜、房屋还是软件,《德国民法典》设定的规则适用起来并无本质区别——除了在几年前《德国民法典》第 327 条到 327t 条对与消费者签订的数字产品合同作出了特殊规定。此外,互联网时代的到来对合同法的改变微乎其微,只是规定了某些明确的信息义务,核心内容一仍其旧。

然而,这种灵活性并不遍及于法律制度的全部,问题主要体现在以下两方面。一方面,某些现行法律创设于技术创新之前,其适用可能会对技术发展造成本可避免的障碍。这在人工智能领域尤为明显:训练人工智能所需的材料可能包含个人数据,从而受到数据保护法的限制;还有许多文本和图像受到著作权保护,原则上禁止获取;类似的问题也可能出现在诸如车辆耗电量等事实数据上,因为发掘和分析属于他人的物体的属性并非理

〔2〕 Vgl. Günther/Gerigk/Berger, Von Algorithmen und Arbeitnehmern: Die europarechtliche Regulierung von KI im arbeitsrechtlichen Kontext, NZA 2024, 234, 234.

〔3〕 德国联邦信息安全办公室汇编的网络安全宣传材料对其进行了专门介绍,还提到了相关应对措施,值得一读。Vgl. BSI, Deepfakes - Gefahren und Gegenmaßnahmen, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/Deepfakes/deepfakes_node.html (16.3.2024).

所当然。另一方面,新技术可能带来未知的风险。早先德国公众较为关注的是自动驾驶的汽车造成事故由谁来担责,[4]现在这个问题逐渐淡出人们的视线,取而代之的是其他可识别的风险。如果人工智能系统可以肆无忌惮地收集某个人的任何信息,比如利用人脸识别来判断他是否违反了交通规则,那么个人不就成了无助的被监视对象?此做法很容易转用于人力资源管理,试想由人工智能自动生成人事决定引发的问题:假设人工智能的"训练材料"主要考虑身高等特征,那么女性的职场机会将大大降低,被拒绝的求职者该怎么办?此外,还有一个远未被重视的问题,如果法律创设的框架条件对谷歌和微软等大公司更为有利,而不给初创公司等中小企业真正的发展机会,难道不是在阻碍创新吗?

2. 计划和建议的初步尝试

人工智能的出现并没有引起立法者的自发反应。相反,欧盟委员会和各国政府最初发布的是不具有法律约束力的各种"计划"。值得一提的有欧盟委员会于2018年4月25日公布的关于"欧洲人工智能"的"通报",[5]和德国2018年11月的"联邦政府人工智能战略"。该战略在2020年更新并于2023年由"人工智能行动计划"进一步具体化。[6] 其重点在于促进人工智能发展,因为德国希望取得"领先地位"。

美国如今仍然青睐这种规制方式。2022年10月白宫发布了一份"人工智能权利法案蓝图",[7]也引起了德国的关注。[8] 文件强调了五项原则:安全有效的系统、防止算法歧视、数据保护、系统的透明度、保留由人类而非人工智能作出决策的选项。原本这是一项立法草案,但目前尚无实现的可能。拜登总统在2023年10月30日发布的行政命令[9]再次描述了相关风险,但同时也为更好的人工智能提出了相当高的标准,比如强调负责任地开发和使用人工智能意味着应当改善美国工人的地位。由于人工智能创造了新的工作岗位和行业,所有工人都必须在集体谈判桌上占有一席之地。考虑到美国劳动法的发展,这是一个了不起的愿望,当然也可能是考虑到2024年11月的总统选举才被提出的。迄今为止,美国只有少数几个州就人工智能出台了具有约束力的法规。[10]

许多国际组织也在关注人工智能并为负责任地使用相关技术提出了"建议"。[11] 它们的实际意义低于主要经济体的相应文件,当然也不具有约束力。众多不具约束力的宣

---

〔4〕 Vgl. Spindler, Neue Haftungsregelungen für autonome Systeme? JZ 2022, 793, 793.

〔5〕 Europäische Kommission, Künstliche Intelligenz für Europa COM(2018) 237 final, https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/? uri=CELEX:52018DC0237(16.3.2024).

〔6〕 相关文件可以参考 Die Bundesregierug, Künstliche Intelligenz (KI) ist ein Schlüssel zur Welt von morgen, www.ki-strategie-deutschland.de,最近访问时间[2024-03-16]。

〔7〕 Vgl. https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf (17.3.2024).

〔8〕 Vgl. Blanke-Roeser, Der US-amerikanische „Blueprint for an AI Bill of Rights", JZ 2023, 509, 509.

〔9〕 Vgl. https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ (17.3.2024).

〔10〕 Vgl. Hutson, Wie Staaten weltweit KI in Schach halten wollen, Spektrum der Wissenschaft v. 24.8.2023, S. 12, https://www.spektrum.de/news/wie-nationen-vorhaben-kuenstliche-intelligenz-in-schach-zu-halten/2171376 (17.3.2024).

〔11〕 相应介绍详见 Waas, Künstliche Intelligenz und Arbeitsrecht, 2023, S. 40-59, https://www.hugo-sinzheimer-institut.de/faust-detail.htm? sync_id=HBS-008472, 最近访问时间[2024-03-17]。

言的优势在于,它们指出了一些决策者以前可能没有认识到的问题。各种不同的利益诉求也可以进入宣言的视野而得到公开的讨论,因为这些只是各方的“愿望表达”,而不是对每个人都有拘束力的法律。此类建议的缺点则是其所倡导的解决方案有时自相矛盾,比如有文件要求同等支持大公司和初创企业,但现实是不可能为两者都提供充裕的资金。还有的建议一边提出应无条件推广人工智能,一边要求对训练材料进行严格的质量控制,而后者会使人工智能的发展变得复杂和缓慢。〔12〕

3.《欧盟人工智能法案》的立法过程

2021 年 4 月 21 日,欧盟委员会向公众发布“欧洲议会和理事会关于制定人工智能统一规则(人工智能法案)并修改某些欧盟法律的条例”草案。〔13〕 但其并未进一步解释为何要首次制定一项具有约束力的条例。〔14〕 立法理由只是提到了人工智能的益处和风险,并强调应保持两者之间的“平衡”关系。这符合欧盟的利益,即“加强欧盟的技术领导力,确保欧洲人能够受益于根据欧盟的价值观、基本权利和原则开发和运作的新技术”。该法案草案在随后的三年完成了立法程序。欧洲议会〔15〕和部长理事会〔16〕的意见与欧盟委员会的提案存有很大分歧。所以按照惯例,2023 年下半年进行了所谓的“三方会议”:委员会、议会和理事会代表努力通过非公开谈判达成妥协,终于在 2023 年 12 月就草案达成一致,之后发布了欧盟所有 22 种语言的版本。〔17〕

经三方会议达成一致的妥协草案于 2024 年 3 月 13 日得到欧洲议会的批准。〔18〕2024 年 5 月 21 日,部长理事会也正式批准了该法案。〔19〕 然而,以这种方式组织的立法程序使得嗣后对所通过的法律进行解释面临重重困难,因为公众无法了解在三方讨论中规则变迁的原因和论据,对立法史的回溯将面临阻碍。此外,欧盟的法律规范有 22 种不同的语言版本,所有版本在效力上具有同等地位。如果它们之间存在差异,也难以通过文义

〔12〕 比如 UNESCO, Recommendation on the Ethics of Artificial Intelligence, Adopted on 23 November 2021, p. 5:“应对风险和伦理问题不应阻碍创新和发展,而应提供新的机遇,激励人们以符合伦理的方式开展研究和创新,使人工智能技术立足于人权和基本自由、价值观和原则、对道德和伦理反思。” https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence, 最近访问时间[2024-03-17]。

〔13〕 EUR-Lex COM(2021) 206 final, https://eur-lex.europa.eu/legal-content/DE/TXT/? uri=CELEX:52021PC0206 (17.3.2024).

〔14〕 译者注:《欧盟人工智能法案》官方英文亦称 Artificial Intelligence Act,本文遵循目前主流译法,译为“法案”,但其性质在欧盟法上属于条例(regulation)。

〔15〕 European Parliament 2021/0106 (COD), https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2021/0106(COD)&l=en (17.3.2024).

〔16〕 Council of the EU, Artificial Intelligence Act: Council Calls for Promoting Safe AI that Respects Fundamental Rights, https://www.consilium.europa.eu/en/press/press-releases/2022/12/06/artificial-intelligence-act-council-calls-for-promoting-safe-ai-that-respects-fundamental-rights/ (17.2.2024).

〔17〕 EUR-Lex, COM/2021/206 final, https://eur-lex.europa.eu/legal-content/EN/TXT/? uri=CELEX:52021PC0206 (17.2.2024).

〔18〕 Vgl. Artificial Intelligence Act: MEPs Adopt Landmark Law, https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law (16.3.2024).

〔19〕 Vgl. Artificial Intelligence (AI) Act: Council Gives Final Green Light to the First Worldwide Rules on AI, https://www.consilium.europa.eu/en/press/press-releases/2024/05/21/artificial-intelligence-ai-act-council-gives-final-green-light-to-the-first-worldwide-rules-on-ai/pdf/ (21.5.2024). 译者注:本文的写作系基于 2024 年 3 月 13 日欧洲议会批准的版本。

解释得出可靠的结论。所以,将来只能求助规范体系和对标立法目的,这就给解释者,尤其是欧洲法院留下了相对较大的解释空间。

二 《欧盟人工智能法案》的主要内容

(一)适用范围

根据《欧盟运作条约》第288条第2款,欧盟条例具有全面约束力,适用于成员国的所有公民。条例因此有时也被称为"欧盟法律",尽管这与欧盟法上的术语不一致。《欧盟人工智能法案》第2条从多个维度界定了适用范围。

1. 适用对象

首先,《欧盟人工智能法案》针对不同群体规定了不同的义务。该法案区分了人工智能系统的提供者(第2条第1款a项)、人工智能系统的运营者(第2条第1款b项)、人工智能系统的进口者和分销者(第2条第1款d项)、将人工智能系统与其他产品一起投放市场或投入使用的制造者(第2条第1款e项)、未在欧盟境内设立场所的提供者的授权代表(第2条第1款f项)以及位于欧盟境内的受影响主体(第2条第1款g项)。

显然,为实现人工智能系统市场化所进行的活动都不包括在内。根据法案第2条第8款,该法案不适用于人工智能系统或人工智能模型在投放市场或投入使用前的研究、测试和开发活动,仅在例外情况下适用于真实条件下的测试。这意味着新的人工智能的研发活动不直接受到该法案要求的影响或阻碍,尽管人工智能系统提供者应满足的要求自然会对制造过程产生影响。从形式上看,仅须遵守其他欧盟法律。

2. 适用地域

希望在欧盟市场上销售人工智能系统的提供者如果在欧盟设立了场所,属于"当然"的适用主体。设立在第三国却希望在欧盟市场上销售其人工智能系统的提供者也受到法案管辖,但必须根据法案第22条指定在欧盟境内设立的授权代表。甚至当这些提供者和运营者希望在欧盟使用系统生成的"结果"时,该法案也适用。如此确保了所有在欧盟经营的市场参与者必须遵守相同的条件。这也与欧盟《通用数据保护条例》(GDPR)第3条的规定相呼应。[20]

3. 适用事项

《欧盟人工智能法案》适用于"人工智能系统"。法案第3条第1款对其使用的67个术语进行了界定,其中也包括对人工智能系统的定义。所谓人工智能系统必须是一个"以机器为基础的系统",其设计可实现不同程度的自主操作,这里的"自主"是指其结果不能预测或不能完全预测,与袖珍计算器不同。[21] 我们可以说它是一个非确定性系统,[22]它必须从接收到的输入中得出"预测、内容、建议或决定",而这些输入可能会影响

〔20〕 Vgl. Däubler, Das Kollisionsrecht des neuen Datenschutzes, RIW 2018, 405, 405 ff.

〔21〕 法案草案的立法理由第12条也提到,法案不应涵盖仅基于自然人所定义的规则自动执行操作的系统。

〔22〕 Vgl. Zweig, Die KI war's! Von absurd bis tödlich: Die Tücken der künstlichen Intelligenz, 3. Aufl. 2023, S. 29 ff.

物理或虚拟环境。该定义表述并不十分清晰,所以对人工智能系统的具体界定可能将由欧洲法院的司法实践决定。

4. 排除适用的情形

根据《欧盟人工智能法案》第 2 条第 6 款,该法案不适用于仅为科学研究和开发目的而设计和使用的人工智能系统和人工智能模型。可见,整个科研领域被排除在外,也排除了不寻求“市场成熟度”的开发情形。就此而言,科学研究也确实不应受到影响,而这本可以通过专门的“除外”条款来明确规定。如果某人开发人工智能既非为了科学研究,也不打算将其商业化,即其行为完全是出于个人的、非职业目的,那么依据法案第 2 条第 10 款也同样被排除在适用范围之外。法案第 2 条第 3 款亦将专门用于军事目的或服务于国家安全的人工智能系统排除在适用范围之外。《欧盟条约》第 4 条第 2 款第 3 句已清楚地表明,维护国家安全完全是成员国的责任。

5. 与其他法律的关系

《欧盟人工智能法案》第 2 条第 7 款明确有关数据保护的法律适用不受影响,也就是说,除了明确规定的两个例外情形,法案本身不包含数据处理的法律依据。如果个人数据被用作人工智能的训练材料,那么必须具有符合《通用数据保护条例》或其他数据保护法规的法律依据。此外,根据法案第 2 条第 9 款,欧盟有关消费者保护和产品安全的法规的适用也不受限制。这对责任问题尤为重要。[23] 在对雇员使用人工智能的情形下,法案第 2 条第 11 款明确规定,欧盟和成员国制定的对雇员更有利的规定适用不受影响,包括集体合同,无论这些规定在法案生效时已存在还是在法案之后制定。[24] 这一开放性条款远远超出了《通用数据保护条例》第 88 条的规定。

(二)风险等级的划分

1. 原则

《欧盟人工智能法案》原则上区分了三种形式的人工智能系统。法案第 5 条列出了具有不可接受风险的人工智能系统并加以禁止。法案第 6 条和第 7 条调整所谓的高风险人工智能系统。这些系统在法案附件三中被明确列出,须满足法案第 8 条至第 15 条详细说明的要求。法案第 16 条至第 22 条规定了人工智能系统提供者的义务,法案第 23 条和第 24 条则分别规定了进口者和分销者的义务。满足特定条件时,法案第 25 条将提供者的义务拓展至价值链上的所有公司。法案第 26 条规定了经营者的义务,其范围要小得多。在高风险系统投入运行之前,必须根据法案第 27 条规定先进行基本权利影响的评估。法案第 28 条至第 39 条规范所谓通知机构的组建和任务,法案第 40 条至第 49 条则涉及合规性评估。对于低风险或最小风险的人工智能系统,法案只设定了少量义务,其中最重要的是法案第 50 条规定的透明度义务。

2. 哪些系统具有不可接受的风险?

《欧盟人工智能法案》第 5 条列举了“人工智能领域禁止的实践”,指向会引发不可接受的后果的人工智能系统。它们的实际意义各不相同,但目前还无法明确预见。

---

〔23〕 Vgl. Wagner, Die Richtlinie über KI-Haftung: Viel Rauch, wenig Feuer, JZ 2023, 123, 123 ff.

〔24〕 译者注:本文使用的“雇员”和“雇主”仅指劳动关系的劳资双方。

(1)潜意识的影响。法案第5条第1款a项禁止了“让人无法觉察的利用人的潜意识”或者使用“故意操纵或者欺诈技术”的人工智能系统。[25] 这些技术的目的必须是明显损害当事人知情决定的能力,即该系统可以使得当事人作出他们本来不会作出的决定,而且必须造成或能够造成“重大损害”。与《德国民法典》第123条规定的传统欺诈相比,区别在于德国司法实践至今未考虑潜意识的影响,[26]而且重大损害并非该条规定的先决条件。与之不同的还有,根据法案第99条第3款的规定,侵权行为可能会导致最高罚款额达3500万欧元或全球年营业总额的7%的行政处罚[详见本部分第(七)1点]。该条款最有可能在广告领域产生实际影响。

(2)利用人的弱点。与操纵行为有关的还有法案第5条第1款b项中提到的情况,即人工智能系统利用一个人的弱点或因其年龄、残疾或特殊的社会或经济状况而需要保护的情况,使其从事对该人造成重大损害的行为。原本在德国法中一般借助《德国民法典》第138条来处理这些情况,而该条并不要求“重大损害”。

(3)基于社会行为和个人特征对人进行评估。法案第5条第1款c项禁止使用人工智能系统根据自然人或自然人群体的社会行为对其在一定时期内的表现进行评价(“社会评分”)。这同样适用于根据已知、推导或预测的个人特征和属性进行评估,比如根据画像。然而,评估本身并不违法。只有当它被用于与收集数据的情况无关的领域而导致相关主体处于更为不利地位时,它才是非法的。例如,由于某雇员在私人生活中犯下的交通违规行为被获悉,导致他无法获取圣诞奖金。此外,如果出现与社会行为及其影响范围“不合理或者不成比例”的不利对待,评估也是违法的。相反,如果该行为评估导致了优待,比如当事人因其特别强烈的助人意愿而获得公共褒奖,则不违法。

(4)调查某人犯罪的可能性。法案第5条第1款d项禁止人工智能系统仅根据画像或对个人特征和属性的评估来调查某人实施犯罪行为的可能性。不过也有例外,如果已经存在与犯罪活动直接相关的客观的、可核实的事实,那么在补充调查时适用人工智能系统就没有问题。

(5)创设人脸识别数据库。根据法案第5条第1款e项,如果人工智能系统的目的是通过从互联网或监控录像中无目标地读取面部图像来创建或扩展人脸识别数据库,则该系统是被禁止的。这尤其也适用于此类私人活动。

(6)分析人的情绪。法案第5条第1款f项禁止在工作场所或教育机构使用人工智能系统记录人的情绪。出于医疗原因而规定的例外情形没有问题,但以“安全原因”为理由的例外则并非如此:这可能意味着,如果根据法案第2条第11款优先适用的国内法律不禁止这种对人格领域的侵犯,那么警察或安保人员很可能需要接受情绪检测。

(7)根据生物信息对人进行分类。法案第5条第1款g项的禁止性规定并不容易理解。根据该条规定,不得根据人们的生物识别数据对其进行分类,以推断其种族、政治观点、工会会员身份、宗教或哲学信仰、性生活或性取向。就种族而言这种做法或许还可以

〔25〕 法案对投放市场和投入使用同样对待,这也适用于下述情况。

〔26〕 相关例证参见 Ellenberger, in: Grüneberg Kommentar zum BGB, 83. Aufl. 2024, § 123 Rn. 3 bis 9。

理解,但就其他特征而言情况并非如此。通过个头大小和眼睛颜色怎么能对某人的政治观点下结论呢?立法者所意图规制的可能是这样一种情况,即生物识别信息加上所谓的附加信息就可以对上述特征得出结论。比如某人参加了一个工会或宗教组织的会议,并有相关视频记录,然后人工智能系统使用人脸识别来确定哪些人参与了会议,该人是否在其中。此时就满足禁止性规定的要件。

(8)实时远程识别系统。当人工智能系统被用于刑事追诉的目的时,将人工智能支持的生物特征实时远程识别系统用于公众可进入区域受到非常详细的规制。根据法案第 5 条第 1 款 h 项,此种系统原则上是违法的,但也有一些重要的例外情况,不过法案第 5 条第 2 款和第 3 款又对例外情况作出了限制。而且根据法案第 5 条第 4 款至第 6 款,市场监督机构和国家数据保护机构也必须参与其中。

3. 高风险人工智能系统

(1)一般情形下的界定

《欧盟人工智能法案》第 6 条第 1 款对于高风险人工智能系统的分类参照了欧盟有关产品安全的指令和条例,这些指令和条例也覆盖了机器、玩具、运动船、电梯和缆车等产品。如果人工智能系统是作为这些产品的安全组件安装或使用的,则自动构成高风险系统。此外,根据法案第 6 条第 2 款,附件三所指的人工智能系统也应被视为高风险系统,比如那些不在法案第 5 条列举的禁止清单上的生物识别系统[见上文第 2(7)点]。至于其他系统的界定,就要根据生活领域加以区分了。

(i)关键基础设施。人工智能系统作为安全组件被用于道路交通、供水、供气、供热和供电以及更广泛的关键数字基础设施的管理和运行体系之中。法案规定的领域比德国《关键设施条例》(*BSI-Kritisverordnung*)所涵盖的范围要广泛得多。[27] (ii)教育领域。当人工智能系统录取一个人进入某教育课程或将其分配到某特定机构时;当人工智能系统用于评估学习成果时;当人工智能系统用于评估一个机构提供的教育水平时;当人工智能系统旨在学习考试中的违禁行为时。(iii)就业领域。当人工智能系统用于招聘程序时,特别是发布有针对性的招聘广告、筛选简历和评估申请人时;当人工智能系统影响有关工作条件、员工晋升和解雇决策时;当人工智能系统根据个人行为或个人特点和特征分配任务时;当人工智能系统监控和评估员工的表现和行为时。人工智能系统可能引发劳动世界的重大变化,下文将详细地解析这些规定(下文第四部分)。(iv)基本福利的享受。当国家机关使用人工智能系统评估一个人是否有权享受医疗保健等基本的公共福利时,这也适用于评估是否应该给予、限制、取消或收回这些福利的情形。基本福利也包括发放信贷,因此检查信用度的人工智能系统也被归类为高风险系统,但用于检测金融欺诈的系统除外。基本福利还包括健康和人寿保险,因此评估相关风险的人工智能系统也属于高风险系统。最后,人工智能系统用于鉴定紧急呼叫和确定紧急救援服务的优先级时,也属于高风险系统,比如警务和消防。(v)刑事追诉。如果在根据欧盟和成员国法律合法的犯

〔27〕 详见[德]沃尔夫冈·多伊普勒著:《数字化与劳动法》,王建斌、娄宇等译,中国政法大学出版社 2022 年版,第 264 页。

罪侦查措施中使用人工智能系统，则德国法明确提及可使用的测谎仪恐怕属于违法。[28]（vi）移民、庇护和边境管制。当人工智能系统用于评估安全风险、非正常移民风险或移民造成的健康风险时；当人工智能系统支持主管当局审查签证和庇护申请时，包括用于审验证据的可靠性。（vii）司法。人工智能系统被用于支持司法机关查明和解释事实和法律规定以及适用法律时；这也包括在现有法律框架内影响选举的行为。

如果人工智能系统的提供者认为不存在高风险，但市场监督机构不认可，那么应该根据法案第 80 条来处理。如果无法消除意见分歧，当局可以采取行政管理措施，在个案中当局甚至可以要求提供者将人工智能系统撤出市场。

（2）例外情形

《欧盟人工智能法案》第 6 条第 3 款针对附件三目录规定了例外情况，不过满足法案第 6 条第 1 款规定的情况时总是属于高风险系统。法案第 6 条第 3 款第 2 句所列的四种情况在立法者看来风险较小，具体包括以下几种情况：人工智能系统旨在执行“狭窄定义的程序任务”，例如检查申请文件的完整性；人工智能系统旨在改进先前完成的人类活动的结果，例如医生根据已有症状得出了可能的诊断结果，人工智能系统告诉他是否还有其他可能；人工智能系统被用于识别与先前决策模式的偏差，但不能在未经人类适当审核的情况下取代或改变先前的决策；人工智能系统只是为附件三中的评估做“准备工作”。

然而，依据法案第 6 条第 3 款第 3 句，如果人工智能系统在前述过程中对具体个人进行画像，那么这些例外情况就不适用了。根据法案第 6 条第 4 款的规定，提供者须将其对人工智能系统属于同条第 3 款列举情形之一的评估记录在案。应国家主管机关要求，提供者有义务提交该记录文件。例外情况的存在一方面是可以理解的，但另一方面却导致了相当大的法律不确定性。什么情况下程序性任务属于“狭窄定义的”？什么时候一项活动仅仅是“准备性的”？法院将来会面临诸多有待裁决的疑问。法案第 6 条第 5 款也试图解决这个问题，欧盟委员会被要求在法案生效后 18 个月内发布关于第 6 条的具体实施指南，通过一份全面的实例清单来说明如何区分高风险和非高风险系统。这是一个有益的补充，但并不必然能够防止相关法律纠纷产生。

（3）后续的修订

某个人工智能系统是否属于高风险系统，主要取决于技术的发展，立法者可能需要很长时间才能跟上。因此《欧盟人工智能法案》第 7 条针对附件三目录和第 6 条第 6 款规定的例外情况设置了简化的修正方案。具体做法是授权欧盟委员会根据《欧盟运作条约》第 290 条的规定，以授权法案的形式根据某些标准对相关条款进行修改或增加新的适用情况。与制定国内法类似，此过程无需其他欧盟机构参与。

4. 其他人工智能系统

不符合高风险系统定义的人工智能系统通常被称为低风险或最小风险的人工智能系统。《欧盟人工智能法案》中只有少数条款对其适用，后文还将详述［下文第（四）点］。另外，法案第 51 条及以下条款是针对“通用目的”人工智能模型特殊规定。这些都将在

〔28〕 Vgl. BGH 30. 11. 2020 - 1 StR 509/10 - Rn. 6 (Strafverfahren); BVerwG 31. 7. 2014 - 2 B 20/14 - Rn. 9 ff. (Disziplinarverfahren); LAG Düsseldorf 19. 1. 2022 - 12 Sa 705/21 - NZA-RR 2022, 460 (arbeitsgerichtliches Verfahren).

下文讨论[下文第(五)点]。

(三)对高风险人工智能系统的要求

高风险人工智能系统必须满足《欧盟人工智能法案》第 9 条及以下条款规定的特定要求。此外,法案第 26 条及以下条款规定的提供者义务以及其他人的义务对这些要求进行了补充。

1. 风险管理系统

《欧盟人工智能法案》第 9 条第 1 款在未指明适用对象的情况下规定,对高风险人工智能系统应"建立、实施、记录和维护"相应的风险管理体系,也就是说此要求伴随人工智能系统的始终。按照法案第 9 条第 2 款的设想,风险管理是一个持续的过程。它涉及识别、分析和评估系统对他人的健康、安全和基本权利造成的可合理预见的风险,其中也包括"可合理预见的系统滥用"。相关责任人必须采取适当措施管理已识别的风险,而"管理"意味着只保留可接受的剩余风险。按照法案第 9 条第 6 款至第 8 款的要求,高风险人工智能系统在投放市场或投入使用前必须进行首次检测。随后的检测必须在任何适当的时刻进行,特别是在存在相关事由的情况下。检测也可以在真实的条件下进行。检测旨在探明最恰当的措施以最大限度地降低风险,确保人工智能系统按预期运行。

2. 数据管理

人工智能系统通常必须使用个人或非个人数据进行训练。这些数据的质量决定了人工智能是否能很好地工作。《欧盟人工智能法案》第 10 条针对这一问题提出了训练、验证和测试数据集所须满足的要求。值得一提的是,法案第 10 条第 2 款 f 项规定必须对可能导致欧盟法律所禁止的歧视的"偏见"进行审查,而且必须采取适当措施以识别、防止和减轻这种扭曲的风险。根据法案第 10 条第 3 款,就人工智能系统预期实现的目的而言,数据集必须具有充分的代表性,并且尽可能无误和完整。比较难以实现的是法案第 10 条第 4 款的要求,考虑到高风险系统预期在"特定地理、背景、行为或功能的框架性条件"下被使用,数据集必须是符合上述条件的典型特征或元素。[29] 鉴于这些表述的宽泛性(比如"具备足够的代表性""尽可能地无误")及其处理的难度,在发生争议时将难以确定人工智能系统是否符合规定,特别难以确定其并未造成歧视。就此,反歧视法中至今有效的基本原则仍予适用。[30]

3. 透明度

《欧盟人工智能法案》第 11 条对高风险人工智能系统的技术文件提出了要求,其详细内容规定在法案的附件四中。技术文件应当体现系统已经达到了法案第 8 条至第 15 条的要求。由于这是一项非常艰巨的任务,欧盟委员会将根据小微企业和初创企业的需要制定简化表格。虽然技术文件在一定程度上包含了设计计划,但法案第 12 条要求在系统的整个生命周期内自动记录相关事件。法案第 12 条第 2 款和第 3 款详细规定了日志记录事件的内容,从而也确保了后续的监督控制。最后,法案第 13 条确立了一般原则,即

〔29〕 就此,立法理由第 67 条的相关陈述没有太多意义,因为它们只是重复了条款的措辞,在许多其他情况下也是如此。

〔30〕 参见[德]沃尔夫冈·多伊普勒著:《数字化与劳动法》,王建斌、娄宇等译,中国政法大学出版社 2022 年版,第 147 页。

高风险人工智能系统的设计必须透明,使得运营者可以适当地解释和使用系统产出的结果,尤其是提供者和运营者应当能够履行法案第 16 条及以下条款规定的义务。根据法案第 13 条第 2 款,高风险人工智能系统必须附有“使用说明”,该说明必须包含“准确、完整、正确和明确的信息且对运营者而言具有相关性、便于获取和易于理解”。除了载明提供者的联系方式以外,法案第 13 条第 3 款 b 项还细致要求使用说明须介绍高风险人工智能系统的特点、功能和性能限制。

4. 人类的监督

人工智能不应独立运作。因此,《欧盟人工智能法案》第 14 条第 1 款规定高风险系统的设计必须能被自然人有效监督,以排除或至少减少人工智能对健康、安全和基本权利的威胁。预防措施应在系统投入使用前就安排到位。这些措施应尽可能在技术可行的情况下内置于系统中,或者在设计时使运营者能够实施这些措施。

根据法案第 14 条第 4 款,受托进行监督的人员必须充分了解系统的能力和局限性,还必须能够识别异常、故障和意外性能并消除其诱因。值得注意的是,必须防止人类对人工智能系统结果的过度信任,负责监督的人员必须能够忽略这些结果或暂时关闭系统。法案第 14 条第 5 款还对生物特征远程识别系统作了特别规定,只有在两个具有必要能力、培训和授权的自然人确认系统的识别结果后,才能将其作为措施或决定的依据。

5. 准确性、稳健性和网络安全

《欧盟人工智能法案》第 15 条第 1 款要求人工智能高风险系统具备“适当水平”的准确性、稳健性和网络安全。什么是“适当的”可能会引起疑问,这正是第 15 条第 2 款规定欧盟委员会有义务与相关利益方合作制定基准和测量方法的动因。立法者显然意识到了这样一个事实,即应该追求更清晰和更具体的标准。根据法案第 15 条第 3 款,人工智能系统的“使用说明”必须明确规定准确度的等级。稳健性可以通过技术冗余解决方案辅以其他的技术和组织措施来实现。为确保网络安全,防御攻击必须特别注重对训练数据集或预训练组件的干预。

6. 提供者的义务

《欧盟人工智能法案》第 16 条列出了相关方的 12 项义务,特别规定了人工智能系统提供者的义务,但不仅限于此群体。其中最重要的是遵守法案第 9 条至第 15 条规定的义务,上文第 1-5 点已阐释过。此外,提供者还有义务在高风险人工智能系统上注明提供者的名称、注册商标和联系地址,或于必要时在其包装或附件上注明。提供者还负有引入质量管理体系的义务。法案第 16 条还指向了其他条款规定的一些义务,比如完成合格性评估程序,或履行第 49 条第 1 款所规定的注册义务。当国家监管机构提出合理要求时,提供者还有义务提交证据证明系统符合法案第 9 条至第 15 条的各项要求。该系统还必须满足欧盟法律对残疾人的无障碍要求。

值得强调的是,法案第 17 条规定了设立质量管理体系的义务,以确保法案的所有要求得到遵守。该体系应该“系统而适当地”以书面形式将规则、程序和指令记录在案。之后,法案还进一步以目录形式列出了至少 13 点需要记录的事项,比如“用于系统的开发、质量控制和质量安全的技术、程序和系统措施”和“在开发高风险人工智能系统之前、期间和之后要进行的检查、测试和验证”。目录的稍后部分还提到了“所有相关文件和信息

的记录保存系统和程序”。目录列举范围之广,几乎没有事项无需被记录。如此繁重的记录义务恐怕会阻碍小微企业的发展,法案第 17 条第 2 款也间接体现了此顾虑,其规定前款义务的落实“应当与提供者的组织规模成比例”,但该规定又话锋一转,指出“在任何情况下提供者都应遵守为确保其人工智能系统符合本法案所要求的严格程度和保护水平”。由此可见,法案第 17 条第 2 款带来的减负效应可能收效甚微。不过,法案第 63 条对小微企业减负作出了特别规定。

按照法案第 18 条,特定文件必须保存 10 年,其中包含法案第 11 条规定的技术文件和第 17 条规定的质量管理体系文件。不过对于自动生成的日志,第 19 条规定的保存期限要短得多。法案第 21 条则重申了与主管当局合作的义务。

7. 进口者、分销者和价值链上其他参与者的义务

在第三国制造的高风险系统进入欧盟市场之前,进口者必须根据《欧盟人工智能法案》第 23 条检查该系统是否符合法案要求。进口者必须澄清是否按照法案第 43 条进行了所谓的合格评估程序,是否按照法案第 11 条制作了技术文件,系统是否附有提供者准备的合格声明和使用说明,以及提供者是否按照法案第 22 条在欧盟境内指定了授权代表,以便监管部门和商业伙伴有一个负责的联系人。此外,如果存在假冒系统或附有假冒文件的任何嫌疑,进口者有义务排除之,并须通知监管部门。

法案第 24 条也规定了分销者的义务。首先,分销者必须检查提供者以及进口者是否履行了相关义务。其次,如果分销者根据其所掌握的信息有理由相信该人工智能系统未满足法案第 9 条至第 15 条的要求,则不得在市场上销售该系统。假设这种嫌疑是之后才出现的,那么分销者必须及时采取修正措施或召回该系统。

法案第 25 条使用的“价值链”一词有些难以理解。其第 1 款规定了三种情形,在这些情形下进口者、分销者、运营者或其他第三方都应承担原本应由提供者承担的义务:(1)在“产品”即高风险人工智能系统上标注其名称或商标的人;(2)对已投放市场的系统进行“重大改变”而不改变其特性的人;(3)将已投放市场的非高风险系统改造为高风险系统的人。此时,最初的提供者将不再承担作为提供者的义务,而是必须在法案第 25 条第 2 款规定的范围内,为现在被视为提供者的第三方提供支持。

如果人工智能系统是某些产品的安全组件,那么根据法案第 25 条第 3 款,产品制造者被视为提供者。法案第 25 条第 4 款将那些在高风险人工智能系统制造过程中提供“工具、服务、组件或程序”的人也纳入了规制。虽然这些人未被视为提供者,但他们有义务根据公认的技术水平在书面协议中具体说明必要的信息、能力、技术访问和其他支持措施,以便提供者能够完全履行法案规定的义务。

8. 运营者的义务

尽管运营者对高风险系统有实际的“控制”,但是根据《欧盟人工智能法案》第 26 条,其必须履行的义务要少得多。不过,此规则只适用于欧盟法律,若成员国国内法规定了无过错的损害赔偿责任,则法案规定不影响其适用。

运营者最重要的义务是按照提供者制定的使用说明行事,且必须根据法案第 14 条指定一名合格人员对系统进行监督。此外,根据法案第 4 条的规定,所有参与使用人工智能

系统的人员都应具备必要知识和经验(见上文第4点)。法案第26条第7款还规定,在启用高风险人工智能系统之前,运营者还必须告知受影响的雇员和雇员代表,他们将成为高风险人工智能系统的使用"对象"。可想见的适例是他们将与人工智能系统一起工作,或者将受到该系统监控。法案第26条第11款还规定运营者必须告知有关主体,针对他们的决定将由人工智能系统作出或在其支持下作出。此外,运营者有义务将新出现的风险和"严重事故"通知提供者和其他机构。

在运营者将高风险人工智能系统投入使用之前,必须根据法案第27条进行基本权利影响评估。这与《通用数据保护条例》第35条规定的数据保护影响评估类似,但需要分析的问题更为详细。基本权利影响还包括禁止歧视。运营者有义务通知市场监督机构评估结果,以便其在必要时采取适当措施。

9. 行政管理规定

《欧盟人工智能法案》第28条至第49条规定了如何从行政管理上确保适用于高风险人工智能系统的标准得到遵守。根据法案第28条第1款,各成员国有义务至少建立一个"通知机构",或授予现有机构相应的权力,其任务是确保建立和监督法案第19条第3款规定的合格性评估机构,而这些机构必须满足法案第31条规定的要求,特别是必须具有一定程度的独立性。只有在向欧盟委员会递交通知申请,[31]且欧盟委员会(及其他成员国)在一定期限内未提出反对意见的情况下,合格性评估机构才能开展活动。就合格性评估机构的工作内容而言,主要涉及检测高风险人工智能系统是否符合法案的要求。法案对要遵循的程序有详细的特殊规定,如果人工智能与某产品相关联,而对该产品也有相应的程序要求,那么生产企业也须适用该规定。值得注意的是,法案明确要求国家的通知机构和合格性评估机构都必须拥有必要的人员和其他资源,以便全面完成任务。

(四)对其他人工智能系统的要求

对于不属于《欧盟人工智能法案》第6条意义上的人工智能系统,即与高风险无关的人工智能系统,法案中虽无相关的系列规定,但针对所有人工智能系统的一些通行规则须得到遵守。比如,法案第4条规定人工智能系统的提供者和运营者的雇员应当具备特定能力,这也适用于其他代表提供者或运营者参与人工智能系统操作和使用的人员,他们必须具备足够水平的人工智能专业知识。不过,何为"足够水平"仍不明确。法规只要求考虑他们的技术知识、经验、教育和培训,以及人工智能系统的使用环境和使用对象。如果使用人工智能系统的雇员因不知情而对第三方造成损害,将由提供者或运营者承担责任。

值得一提的还有法案第50条第1款规定的透明度义务,其要求旨在与人类直接互动的人工智能系统须具有相应设计,使得人们知道自己正在与人工智能系统而非人类打交道。如果由聊天机器人接听电话,则必须使来电者知晓该事实,只有人工智能的使用对于"一个知情、善于观察和谨慎的人"来说显而易见时,才构成例外。根据法案第50条第2

〔31〕 在德语中其实很少使用"通知"(Notifizierung)这个词,它意味着正式转发或传递,特别是向其他国家或超国家机构转发或传递。

款和第 4 款,生成合成音频、图像、视频或文本内容的人工智能系统必须能够被识别为“人工生成”或“被操纵”;这尤其适用于深度伪造。不过更合适的其实是直接规定明确的贴标签义务。对于人工智能生成的文本,如果其经过人类审核且自然人或法人对内容发布负有编辑责任,也可以省略标签。因此,记者可以通过使用 ChatGPT 来简化工作,前提是他们随后要审查文本并纠正错误。根据法案第 50 条第 3 款,如果在特殊情况下允许使用情感识别系统或生物识别分类系统,则必须告知有关主体使用人工智能的情况。

(五)通用目的人工智能模型

直到“三方会议”的谈判,《欧盟人工智能法案》才新增了现在的第 51 条至第 56 条。这些规定是为通用目的人工智能模型而设,即可用于不同任务的人工智能技术的表现形式。ChatGPT 是人们最常提到的例子。

法案区分了两种形式的通用目的人工智能模型。与基础形式的通用目的人工智能模型相区别的是“具有系统性风险”的通用目的人工智能模型,后者受到立法者的特别关注。法案第 51 条第 1 款 a 项将此类模型描述为具有“使用适当的技术工具和方法(包括指标和基准)评估”的高影响能力;法案第 51 条第 2 款则从“如果用于训练的累计计算量(以 FLOPs〔32〕计)大于 10^25”推定系统满足此条件。这是一个极高的计算能力,OpenAI 公司的 GPT-4 或 Inflection AI 公司的 Inflection-2 可能达到或超过了此计算能力,但德国的 Aleph Alpha 就没有达到。〔33〕 法案的附件十三就此规定了其他认定标准。因此,较小的竞争者只须满足较低的要求,但问题是他们能在多大程度上跟上大公司的步伐。如果属于法案第 51 条第 1 款 a 项意义上的具有系统性风险的模型,那么提供者有义务将此告知欧盟委员会。法案第 52 条第 2 款赋予人工智能模型提供者提出反证的机会,即该模型由于其特殊性并不会带来任何系统性风险,随后由欧盟委员会判定是否如此。

法案第 53 条针对普通的通用目的人工智能模型规定了提供者的义务,包括提供模型的技术文件,以及向意图将该模型纳入其人工智能系统的其他人工智能企业提供相应信息和文件。此外,提供者还必须记录其遵守欧盟著作权法规的策略。最后,提供者必须在(未来会设置的)人工智能办公室准备的模板基础上对用于训练人工智能模型的内容进行足够详细的总结。就来自第三国的通用目的人工智能模型提供者,法案第 54 条作了特别规定,即应根据法案第 22 条委托授权代表。

法案第 55 条还针对具有系统风险的通用目的人工智能模型提供者规定了额外义务,要求对其进行“模型评估”,确保模型应符合先进技术水平并考虑到可能发生的对系统的攻击。提供者必须对由此产生的系统风险进行评估并尽量减少风险。提供者须将“严重事故”和可能的补救措施的信息记录在案,之后须立即告知人工智能办公室和国家主管机关。最后,必须确保适当的网络安全水平。鉴于尚未就有关的所有问题点形成统一规则,此类人工智能模型的提供者可将法案第 56 条制定的行为准则作为指导。

〔32〕 FLOPs 是 Floating Point Operations Per Second 的缩写,代表每秒浮点运算次数,用于衡量计算机的性能。

〔33〕 Vgl. Jacob Steinschaden, Der AI Act hat nun einen sprichwörtlichen FLOP, https://www.trendingtopics.eu/der-ai-act-hat-nun-einen-sprichwoertlichen-flop/ (20.3.2024).

（六）促进创新的措施

1. 人工智能监管沙盒

人工智能监管沙盒是促进技术创新的设施，同时也是后续发展国家监管的设施。[34]《欧盟人工智能法案》采纳了这一概念并在第 57 条第 1 款规定，原则上每个成员国应至少建立一个监管沙盒。第 57 条第 5 款描述了立法者设想的功能：监管沙盒可以提供一个受控的环境来“促进创新并推动人工智能系统的开发、培训、测试和验证”。相应的开发、培训、测试和验证应该在人工智能系统投放市场之前的一段时间内进行并以真实世界的实验条件为基础。第 57 条第 9 款指明了创新之所在；稍显惊讶的是，改善法律的确定性被置于首位，但之后明确提到了“促进创新”、为中小企业进入欧盟市场提供便利以及“促进以数据为基础的监管学习”。由于创新方法会增加责任风险，第 57 条第 12 款作出了法案规定之罚款的豁免规定，前提是参与监管沙盒符合具体计划和其他协议。另外，法案第 58 条授权委员会通过详细规定确保监管沙盒的建立和正常运行。其中也提到了小微企业和初创企业的免费使用，但在成本高昂的情形下，它们可能需要承担“公平和合比例”的部分费用。法案第 62 条进一步规定了小微企业和初创企业的优惠措施。法案第 59 条例外地包含了一则数据保护法的规定，即在满足特定的、精确界定的条件时，为其他目的合法收集的个人数据可在监管沙盒中被用于开发、训练和测试特定人工智能系统。

2. 促进创新的其他措施

法案第 60 条针对在“真实条件下”进行的、于监管沙盒之外以高风险系统为对象的测试作出了详细规定。根据法案第 61 条，进行这些试验还须征得所涉及主体的知情同意。

（七）其他规定及法案的生效

1. 其他规定

在“治理”的章节标题下，《欧盟人工智能法案》第 65 条至第 70 条规定了应在欧盟层面（人工智能办公室、欧洲人工智能委员会、咨询论坛和独立科学专家小组）和国家层面（通知机构、市场监督机构）设立主管部门和机构。针对高风险人工智能系统，欧盟将建立一个数据库，这些系统投入市场的使用将根据法案第 72 条的规定受到监控。如果发生法案第 3 条第 49 项意义上的“严重事故”，提供者有义务进行通报和信息交流。法案第 74 条至第 77 条进一步规定了对欧盟市场上人工智能系统的监督和控制机制。法案第 78 条对信息的保密进行了规定，只要有关机构或个人在适用法案时掌握了相关信息，就必须严格保密。这尤其适用于知识产权和商业秘密。此外，公共和私人安全利益也应受到维护。如果某人工智能系统符合法案的规定，但市场监督管理机构仍然发现该系统对人的健康、安全和基本权利存在风险，其有权依据法案第 82 条第 1 款要求相关主体在其确定的期限内消除这种风险。

根据法案第 85 条，任何人如果有理由认为存在违反法案的行为，都可以向市场监督机构投诉，不以本人受到具体影响为前提。法案第 86 条第 1 款则规定，如果任何人因某

〔34〕 Dazu eingehend Spindler/Büning, Einsatz von Reallaboren (Regulatory Sandboxes) - insbesondere im Recht der Künstlichen Intelligenz und der Finanzmärkte, JZ 2023, 799, 799.

一高风险人工智能系统基于数据作出的决策受到影响,都有权从运营者处获得“关于人工智能系统在决策过程中所起作用的清晰且充分的解释”。解释还应包含决策所涉及的重要因素。通用目的人工智能模型的提供者还必须遵守法案第 86 条至第 94 条的特殊监管规定。根据法案第 96 条,欧盟委员会负责制定法案的具体实施指南。鉴于法案规定往往存在广泛的解释需求,所以委员会享有的具体化权限具有重大实操意义。

特别值得一提的是法案第 99 条规定的制裁措施。其制裁力度相当大,根据所违反的规定而具体有别:如果违反了第 5 条的禁止性规定(人工智能系统具有不可接受的风险),可处以最高 3500 万欧元或上一财政年度全球年营业额 7%的罚款,根据比例原则此惩罚仅适用于最严重的情况,而且估计不会在法规生效后立即被使用;如果违反了法案第 99 条第 4 款,特别是与高风险人工智能系统有关的规定,罚款最高可达 1500 万欧元或上一财政年度全球年营业额的 3%,根据法案第 101 条这也适用于违反通用目的人工智能模型相关规定的提供者;如果违反了某些信息披露义务,罚款最高可达 750 万欧元或上一财政年度全球年营业额的 1%。对于普通公司而言可能适用较高的罚款金额,而就小微企业和初创企业而言,则会适用较低的罚款金额上限,这一点在营业额相对较低的情况下尤为重要。不同寻常的是,法案第 100 条还规定了对欧盟机构和团体的惩罚,尽管这些罚款的金额远远低于对企业的制裁。

2. 法案的生效

《欧盟人工智能法案》将在欧盟官方公报上公布后的第 20 天生效。为便于相关企业逐步适应新的法律框架,该法案将在此时刻的两年后才具有法律约束力。不过,法案的第一章和第二章(尤其是第 5 条中对特定人工智能系统的禁止性规定)在生效的六个月后即具有法律约束力。

三 《欧盟人工智能法案》的整体评价

(一)牺牲小微企业利益的产品安全法?

《欧盟人工智能法案》就其内容重心而言应该属于产品安全法范畴,其目的是将使用人工智能系统对第三方造成的不利和风险降至最低,这也有利于提高公众对人工智能新技术的接受程度。至于以后能否真正实现此目标,目前难以分析和判断。不过,针对高风险人工智能系统规定的复杂而昂贵的预防措施可能会产生意想不到的效果,即减缓人工智能的发展。不可忽视的风险还有,谷歌和微软等大型国际公司将最有能力满足该法规的要求,从而将进一步扩大它们对小微企业的领先优势。尤其是创新型初创公司将面临巨大挑战,比如人工智能监管沙盒等要求可能导致它们经济负担过重。[35]

(二)实施中的问题

《欧盟人工智能法案》在实施过程中还会面临一个问题,即实践中通常难以判断一家企业是否在使用人工智能,尤其是人工智能与“普通”软件之间的区别并不十分明确。所

〔35〕 Dazu Kögel, Fünf Fragen, fünf Antworten – Interview mit Daniel Kögel zum AI Act, ZdiW 2023, 210, 210; Bedenken auch bei Spindler/Büning, JZ 2023, 799, 808.

以,将来有可能会出现相当大的执法缺陷。[36] 法案规定的极其高额的罚款力度[详见上文第二部分第(七)1点]是否足以作为解药,恐怕值得怀疑,因为许多条款的表述比较模糊,以至于故意违反法案的行为很少能够得到证实。

(三)未被考虑的问题:训练材料的获取

《欧盟人工智能法案》中并未提及人工智能的训练材料应该如何获取,只是在法案第10条中提出使用的训练材料应该符合一定的质量标准[见第二部分第(三)2点]。然而,法案之外的其他法律存在一些限制性规定,可能不利于人工智能的开发。

1. 数据保护法上的前提条件

与很多其他合同一样,劳动合同也不以创造和改进人工智能的材料为目的。就此,雇主不能援引《通用数据保护条例》第6条第1款第1句b项来使用雇员数据作为训练材料。雇员的同意通常也难以作为数据处理的基础,因为该条例第4条第11项的同意以自愿为前提,而雇员因担心拒绝雇主招致不利后果,往往并非出于自愿。[37] 此外,根据该条例第7条第3款,同意可随时撤销并向将来生效,由此导致人工智能训练材料的获取部分丧失数据法上的正当性。对此有两条出路:其一,援引该条例第6条第1款第1句f项。据此,人工智能的开发者可主张就获取与人工智能开发有关的数据存在合法利益,而数据主体要求不处理其数据的利益须退居其次。[38] 其二,放弃个人相关性数据而使用匿名数据或汇总数据。[39] 这两种方法也可以结合使用,但这并不排除如此安排可能效果欠佳。

2. 著作权法上的前提条件

如果人工智能的训练材料涉及文本、图像或其他受版权保护的作品,那么其使用需要特殊的法律依据。《单一数字市场版权指令》(*Directive on Copyright and Related Rights in the Digital Single Market*)[40]第4条解决了这一问题,出于"文本和数据挖掘"的目的可以"复制和提取"可合法获取的作品(如互联网上的作品),但存在两个重要限制:第一,只能保留复制件到"文本和数据挖掘"所必需的时间;第二,更为重要的是,作者和其他权利人可以作出所谓的使用保留,该保留必须是机器可读的,可防止相关数据被用作训练材料。就此人工智能系统的提供者需要获得相应的许可。不过,根据《数字单一市场指令》第3条,这些限制不适用于科学研究。德国立法者已经通过《著作权法》第44b条和第60d条转化了该指令的要求。当然,非法存储的内容即使能被自由访问,也不在被许可使用的范围内。[41] 由此可见,著作权法的相关规定可能阻碍类似ChatGPT的人工智能系统的改

〔36〕 See Troge, Does AI Enhance the Risk of Dark Patterns and How Does EU Law Regulate Them? ZdiW 2023, 207, 209.

〔37〕 就知情同意的问题详见 Däubler, in: Däubler/Wedde/Weichert/Sommer, EU-DSGVO und BDSG. Kompaktkommentar, 3. Aufl. 2024, Art. 7 DSGVO Rn. 33 ff.。

〔38〕 Dazu eingehend Ashkar, Wesentliche Anforderungen der DS-GVO bei Einführung und Betrieb von KI-Abwendungen, ZD 2023, 523, 525 ff.

〔39〕 Dazu Klebe, Künstliche Intelligenz – eine Herausforderung für die Mitbestimmung, SR 2019, 128 ff.

〔40〕 欧洲议会和理事会2019年4月17日"关于数字内部市场的版权及邻接权以及对指令96/9/EC和2001/29/EC的修订"的2019/790号指令,公布于ABl v. 17. 5. 2019 L 130/92。

〔41〕 Weitere Einzelheiten bei Köhler/Vogel, Das Training künstlicher Intelligenzen mit urheberrechtlich geschützten Werken, ZdiW 2023, 238 ff.

进,而该系统在工作中经常被使用。

3. 机器相关数据的使用

当信息涉及物体的属性时,并不存在个人数据,而了解这些属性对于训练人工智能可能是至关重要的。至于有关物体(如机器或汽车发动机的一个部件)的所有权是否延伸到与之相关的事实数据,是一个学界还在争议的主题,至今尚无定论。[42] 可消除不确定性的合理建议是,人工智能系统提供者可以考虑与相关所有权人签订一种数据许可协议。这也是发展人工智能的一个不容忽视的障碍。

(四)未被考虑的问题:对就业市场的影响

如果人工智能的发展导致例如记者或者翻译等职业萎缩到仅有少量人员,那么将会如何,在《欧盟人工智能法案》的立法理由中几乎没体现这方面的考量。即使是剩下的从业者能够从事的工作也很有限,比如限于检查 ChatGTP 或类似人工智能系统的产品是否有错误,而且这种错误的发生几率会越来越低。此外还有很多其他职业也可能受到影响,比如出租车司机等,但法案似乎不认为存在这样的问题,甚至没有提及。三方会议是否曾提及这个话题不得而知,因为谈判是非公开进行的,目前也没有任何会议记录可考。因此,没有明显迹象表明此种后果曾成为商议的话题。

法案的立法理由(属于该法案正式文本的一部分)第 4 条和第 6 条强调了人工智能将带来的"经济、环境和社会的多重效益",并认为人工智能将"按照欧盟的价值观"为人们服务。值得注意的是,第 8 条立法理由指出要保护基本权利,包括"民主、法治和环境保护"。此外,第 9 条立法理由声明,该法案无意以任何方式改变欧盟的社会政策规定或成员国的劳动法,这也适用于集体自治和罢工权。

四 《欧盟人工智能法案》对劳动法的影响

尽管规制的侧重点不同,但是《欧盟人工智能法案》也对从属劳动领域产生了影响,就此已有一些德国劳动法学家展开了讨论,[43] 讨论中以下几点受到较多关注。

(一)具有不可接受风险的人工智能系统

《欧盟人工智能法案》第 5 条普遍禁止某些做法,此禁令不区分作为行为人的提供者、运营者或第三方在法律关系中的角色,因此使用人工智能系统的雇主无疑也受其约束。

1. 影响雇员潜意识和利用人性弱点

如果人工智能系统设置的激励制度"无意中"诱导员工更加努力地工作,[44] 那么很有可能违反禁止影响潜意识的规定[见上文第二部分第(二)2(1)点]。然而,由于《欧盟

〔42〕 Näher vgl. Baum/Appt/Schenk, Die vernetzte Fabrik: Rechtliche Herausforderungen in der Industrie 4.0, DB 2017, 1824, 1826 f.

〔43〕 Vgl. Frank/Heine, KI-Einsatz im Betrieb unter der KI-Verordnung, NZA 2023, 1281-1284; Günther/Gerigk/Berger, Von Algorithmen und Arbeitnehmern: Die europarechtliche Regulierung von KI im arbeitsrechtlichen Kontext, NZA 2024, 234-240.

〔44〕 相关案例参见 BAG 1. 12. 2020-9 AZR 102/20-NZA 2021, 552 = NJW 2021, 1551。

人工智能法案》明确要求这种情况发生在“人的意识之外”并且已经造成“重大损害”,因此很难想象在劳动关系中出现这种情况。[45] 此情形更多可能发生在为集团内另一家企业的产品做广告时。在职场生活中,也很少出现人工智能系统压榨利用某雇员的弱点或因年龄、残疾或某种社会和经济弱势地位的情况。

2. 对雇员进行社会评分

相反,利用人工智能系统对雇员进行社会评分的现象会变得较为普遍[见上文第二部分第(二)2(3)点]。有文献提到了一家美国银行收集员工行为数据的做法,包括电话、电子邮件、是否参加合规课程以及对银行的个人评论,然后银行利用人工智能系统来预测员工未来做出不当行为的可能性,而如此确定的“有风险人员”可能被调到更差的工作岗位或成为下一次裁员的牺牲品。[46] 人工智能系统还可能被用于全面记录和分析雇员(或大或小的)违反合同义务的行为,从而确定何时应向雇员发出警告,何时考虑基于不当行为的解雇。前述两种情况下,雇主都使用了人工智能系统对雇员的社会行为进行评估,但是此举只有在随后实施的制裁“不合法或者不合理”时才属于非法。这是一个个案判断问题。假设使用人工智能的时间记录系统显示雇员迟到了一刻钟,就因此扣减了10%的工资,那么显然逾越合理限度。雇主为给予企业奖励而记录雇员值得称赞的行为,则是毫无问题的,不过必须确保这些的数据不能用于其他目的。仅凭目的限制原则难以实现这一点,还须采取进一步措施,比如数据区分存储。[47]

3. 预测雇员犯罪的风险

不仅警方和检察机关,雇主也可能对雇员是否可能实施刑事犯罪行为感兴趣。因此,《欧盟人工智能法案》第5条第1款d项的禁止规定也适用于劳动关系中。该条规定的例外情况也可转用于劳动法,即如果已经存在与犯罪活动直接相关的客观且可核验的事实,那么雇主可借助人工智能系统进行相应调查。

4. 建立雇员人脸识别数据库

《欧盟人工智能法案》第5条第1款e项还禁止雇主通过“无目的地读取”互联网或监控录像中的面部图像来创建人脸数据库。然而,如果雇员进出公司场所被拍摄下来,[48]并在此基础上使用人脸识别软件,则不存在前述“无目的地读取”,而且此时与条款规定的两种情况不同,并不能获取极其大量的信息。

5. 雇员情绪分析

《欧盟人工智能法案》第5条第1款f项有关禁止使用人工智能系统识别情绪的规定在劳动关系中具有重要的现实意义。这意味着呼叫中心经常使用的以下技术不再合法,即可从声音中推测出对话的情绪,进而经常导致呼叫中心的工作人员被要求克制自己的情绪并对来电者采用更加友好的语气。[49] 如果人工智能系统被用于分析求职者的面试

〔45〕 持同样意见的有 Frank/Heine NZA 2023, 1281, 1282。

〔46〕 Im Einzelnen beschrieben bei L. Schröder, Die digitale Treppe, Wie die Digitalisierung unsere Arbeit verändert und wie wir damit umgehen, 2016, S. 132.

〔47〕 就分开存储等数据保护措施详见 Däubler, Gläserne Belegschaften, 9. Aufl. 2021, Rn. 408 ff. 。

〔48〕 类似案情详见 BAG 29. 6. 2023-2 AZR 296/22, NZA 2023, 1105。

〔49〕 就德国呼叫中心对雇员的监控行为详见 Däubler, Gläserne Belegschaften, 9. Aufl. 2021, Rn. 378h-378m。

谈话,并从中识别相应情绪,[50]则此种做法也将被禁止。虽然法案认可出于安全原因的例外情况,即可以对警察候选人或警官的情绪进行分析,但该例外规定与德国劳动法冲突,因为根据法案第 2 条第 11 款,对雇员更有利而应优先适用的德国劳动法禁止对雇员的人格领域进行如此深入的调查。

6. 对雇员进行生物信息分类

劳动关系中也可能出现使用人工智能系统对雇员进行生物信息分类的情形,具体分析可参考前面部分的论述[见上文第二部分第(二)2(7)点]。

7. 实时远程识别系统

根据《欧盟人工智能法案》第 5 条第 1 款 h 项的措辞,其禁止性规定仅限于公共场所以刑事追诉为目的的行动。至于国家或企业是否可以将人工智能系统用于刑事追诉以外的目的,在法案的立法理由和正文部分均未涉及。但可以推断的是,既然出于刑事追诉目的也只允许在有限范围内使用,那么在为实现较小利益而进行追查的情形下,就应禁止使用该系统。这对作业区域较大的企业具有重大的实践意义,比如海港[51]或机场等。不过,恐怕只有在欧洲法院作出澄清后,才有可能对法案的解释有明确结论。德国劳动法仅允许在如下情形下采取此种形式的监视,即监视出于业务目的绝对必要,因为不使用该系统将对工作流程造成巨大干扰,且没有其他办法能够在不确定相关人员身份的情况下实现顺畅的工作。

(二)招聘中人工智能的运用

如果将人工智能系统用于招聘程序,需要考虑其是否构成《欧盟人工智能法案》附件三第 4 条所指的高风险系统。根据法案附件三第 4 条 a 项,如果人工智能系统被用于“招聘或甄选”应聘者,包括发布有针对性的招聘广告、筛选和过滤简历以及评估应聘者,则应得出肯定结论。若满足这些前提条件,雇主通常就是人工智能系统的“运营者”,必须履行与这一角色相关的义务。然而[见上文第二部分第(三)8 点],如果某企业集团根据自己掌握的数据开发了人工智能系统并投入使用,则应将把该系统用于运营的企业视为提供者,从而必须遵循法案第 8 条及以下条款规定的要求和义务。

法案第 6 条第 3 款规定的例外情形在实践中相当重要。首先,如果人工智能系统只是为了完成“狭窄定义的程序任务”,就不会被认定为高风险人工智能系统。比如系统只是对以数字形式提交的简历进行所需文件的完整性检查,就属于这种情况。其次,如果传统的遴选程序完全由人类决策者参与,只是之后由人工智能系统对结果进行复核,同样也不属于高风险系统。最后,仅完成对应聘者进行评估的“准备工作”也不属于高风险系统,因为在这种情况下人工智能系统要么只准备事实依据,要么虽然进行评估但评估结果都必须由人工决策者进行全面审视,否则就不属于“准备工作”了。

人工智能系统不属于高风险系统的,雇主也必须根据法案第 50 条向申请人说明人工智能的使用情况[详见上文第二部分第(四)点]。例如,使用聊天机器人回答申请人或新雇员的问题时,就属于这种情况。雇主使用人工智能系统对申请人进行语音分析但不进

〔50〕 就相关实践详见 Betz, Automatisierte Sprachanalyse zum Profiling von Stellenbewerbern, ZD 2019, 148, 148 ff.。

〔51〕 德国吕贝克港曾有过类似案情,详见 LAG Schleswig-Holstein 29. 8. 2013-5 TaBV 6/13-NZA-RR 2013, 577。

行情绪记录的,[52]也应当告知。

按照法案第2条第11款,成员国的劳动法对求职者更有利的,则予优先适用。[53] 在德国,企业职工委员会的共同决定权尤为重要。[54] 根据法案第2条第7款,数据保护法的一般规定的适用同样不受影响。其中需特别强调的是《通用数据保护条例》第22条,该条禁止应聘者成为仅由自动化系统作出决策的对象。[55]

(三)针对雇员的人工智能运用

如果人力资源部门对雇员使用人工智能系统,原则上会出现与招聘程序中相同的问题。如果人工智能被用于法案附件三第3款b项所列的特定目的,则是被认定为高风险人工智能系统的典型情况。这些目的包括人工智能系统"影响"雇主作出有关工作条件、晋升和解雇的决定,当然也包括由人工智能自己作出决定的情形。使用人工智能系统按照《解雇保护法》(*Kündigungsschutzgesetz*)第1条第3款在不同雇员之间进行社会性挑选时,也属于高风险人工智能系统。此外,人工智能系统基于个人行为或个人特征进行任务分配,也属于这种情形。但若工作指令在人工智能帮助下生成,且指令发出不是基于个人而只是出于经营需要,[56]则不属于这种情形。还有一种可能的目的是使用人工智能系统观察和评估员工的表现和行为,但此时也适用前面提到的例外情况。

与在招聘程序中一样,即使人工智能系统不属于高风险系统,雇主也必须根据法案第50条向雇员说明人工智能的使用情况。成员国的劳动法规定对雇员更有利的,其适用不受影响。在德国这一点尤为重要,因为根据《企业组织法》(*Betriebsverfassungsgesetz*)第87条第1款第6项,企业职工委员会就雇主通过技术设备监控雇员的绩效和行为享有共同决定权。此外,还须始终考虑是否逾越《通用数据保护条例》第22条之界限的问题。

(四)在工作中使用人工智能

1. 继续培训

《欧盟人工智能法案》第4条是在三方会议过程中才被引入的条款,前文业已介绍并阐释[见上文第二部分第(四)点]。让雇主负有确保雇员掌握适当人工智能技能的义务,此规定具有真正的劳动法性质。雇主必须履行此义务,这意味着根据《透明度指令》(*Transparenzrichtlinie*)[57]第13条,雇主必须向雇员提供免费培训措施,而且培训应当计

〔52〕 就语音分析的使用和其他的数字化调查方法详见 Däubler, in: Däubler/Wedde/Weichert/Sommer, a. a. O. (2024), § 26 BDSG Rn. 53 a bis 53r。

〔53〕 Aktuelle Darstellung bei Däubler, in: Däubler/Wedde/Weichert/Sommer, a. a. O. (2024), § 26 BDSG Rn. 18-77a.

〔54〕 Dazu Klebe, SR 2019, 128 ff.; Witteler/Moll, Künstliche Intelligenz und Arbeitsplatz - Datenschutz und Rechte des Betriebsrats, NZA 2023, 327 ff.; Lang/Rheinbach, Künstliche Intelligenz im Arbeitsrecht, NZA 2023, 1273, 1276 ff.

〔55〕 详见关于《通用数据保护条例》的法律评注:Däubler/Wedde/Weichert/Sommer, EU-DSGVO und BDSG, 3. Aufl. 2024, Art. 22 Rn. 1 ff.; Gola/Heckmann (Hrsg.), Datenschutz-Grundverordnung Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 22 Rn. 1 ff.; Simitis/Hornung/Spiecker (Hrsg.), Datenschutzrecht. DSGVO mit BDSG, 1. Aufl. 2019, Art. 22 Rn. 1 ff.; Paal/Pauly, Datenschutz-Grundverordnung Bundesdatenschutzgesetz, 3. Aufl. 2021, Art. 22 Rn. 1 ff.。

〔56〕 就此类指令的效力详见[德]沃尔夫冈·多伊普勒著:《数字化与劳动法》,王建斌、娄宇等译,中国政法大学出版社2022年版,第155页;分析深入的还有 Philipp Knitter, Digitale Weisungen. Arbeitgeberentscheidungen auf Grundlage algorithmischer Berechnungen, 2022, S. 35 ff.。

〔57〕 欧洲议会和理事会2019年6月20日"关于欧盟透明和可预测工作条件的2019/1152号指令",公布于 ABl L 186/105, Deinert/Treber, Europäische Arbeits- und Sozialordnung, Frankfurt/Main 2021, unter Nr. 50 中也有收录全文。

入工作时间并尽可能在工作时间内实施。在德国法上,这一要求在德国《工商业条例》(*Gewerbeordnung*)第 111 条中得到转化。

2. **使用 ChatGPT 工作**

使用 ChatGPT 的相关问题最近在德国引发了热议。[58] ChatGPT 制作文本和技术说明的强大能力引发了受雇记者或程序员是否可以主动使用该技术的问题。根据《德国民法典》第 613 条第 1 句,负劳务给付义务之人"有疑义时应亲自"提供劳务。劳动合同双方可以明示或默示地偏离这一规定,因此雇主可以允许雇员使用 ChatGPT 工作,但同时坚持要求对以该方式创建的文本内容进行审查。如果双方未就此达成一致,则雇员擅自使用 ChatGPT 将违反劳动合同义务。[59] 选择这样做完全值得肯定,因为由 ChatGPT 创建的产品并不享有版权保护,按照现行法作者只能是人类,而不是人工智能系统。如果第三方伪造出版物或宣称自己是作者,雇主可能会遇到困难,因为雇主并无寻求法律救济的依据。《欧盟人工智能法案》第 50 条也可确认此结论,该条规定人工智能的使用必须透明。

ChatGPT 在多大程度上可用于法官或律师工作的问题尤其引人关注。两位大学教授在 ChatGPT 系统中输入了 200 个民法和劳动法案例,这些案例的解决方案在互联网上无法找到,其难度大致相当于法科生在大学课程第三学期时必须掌握的任务,ChatGPT 大概就其中一半的案例给出了实际可用的解决方案。[60] 但对于更复杂的任务,情况就有所不同了。人们对此做了个实验,即向系统询问联邦宪法法院关于气候保护的判决时(该判决非常著名和重要),ChatGPT 就判决本身内容给出的信息是正确无误的,关于法律文献中是否有赞成和反对意见的问题也得到了正确回答。ChatGPT 还给出了回答此问题的论据和两个看似可信的参考文献,然而,事实证明这两个文献纯属捏造,所引用的期刊根本没有这两篇文章,甚至连作者姓名都是虚构的。就这一点,该系统表示了歉意。[61] 至少从目前来看,人类的自然智慧还是不可或缺的。

五 结 语

法律应该是为实践提供方向的路标,但它不应预先规划和控制每一个小步骤,如果非要这样做,就会使创新陷于瘫痪。一方面,人工智能领域的技术发展必须与劳动力市场的形势相协调,但这可能延缓发展潜力的实现。另一方面,我们也不应人为制造那些阻碍与放缓技术发展的无谓障碍。《欧盟人工智能法案》将促进还是阻碍欧盟在全球经济中的地位,尚未可知。目前来看,后者的可能性似乎更大。

---

〔58〕 ChatGPT 属于通用目的人工智能模型[前文第二部分第(五)点]。

〔59〕 Dazu Heine, ChatGPT im Arbeitsverhältnis - Meilen- oder Stolperstein für Arbeitgeber? ZdiW 2023, 221 ff.; Mohn, Dürfen Arbeitnehmer ChatGPT zur Erledigung ihrer Aufgaben einsetzen? NZA 2023, 538 ff.; R. Schaub, Nutzung von Künstlicher Intelligenz als Pflichtverletzung? NJW 2023, 2145 ff.

〔60〕 Einzelheiten bei Conrads/Schweitzer, Einsatz Künstlicher Intelligenz im Vertrags-, Wirtschafts- und Arbeitsrecht, NJW 2023, 2809 ff.

〔61〕 Berichtet nach Schirmer, ChatGPT: (K)eine Zukunft für Kommentare? JZ 2023, 144, 144 ff.

Background, Main Contents, and Evaluation of the EU Artificial Intelligence Act – Also on Its Implications for Labor Law

[**Abstract**] The Parliament of the EU adopted the Artificial Intelligence Act in March 2024, which takes a risk-based approach. The Act establishes obligations for providers and users depending on the level of risk from artificial intelligence. It prohibits certain AI systems associated with an unacceptable risk. AI systems that negatively affect safety or fundamental rights will be considered high risk. All high-risk AI systems will be assessed before being put on the market and throughout their lifecycle. Anyone offering such systems on the market must comply with numerous requirements, ranging from risk management and data governance to comprehensive documentation obligations. The "operator" of a high-risk AI system is first and foremost obliged to comply with the mandatory instructions for use provided by the provider. Special rules exist for systems with a "wide scope of application" such as ChatGPT. When using systems that do not entail high risk, only a few provisions that apply to all AI systems need to be observed. In the event of violations, high penalties of up to 7% of global turnover are envisaged. The AI Act does not address the question of which training material the developer of AI can use without violating data protection or copyright law. In this respect, the GDPR and the relevant copyright regulations apply. The handling of machine-related data has also not been regulated. These problems could significantly hinder the further development of AI. Additionally, there is no consideration of what will happen if entire professions such as journalists or translators are reduced to just a few people. The current labor laws of the EU member states also do not have any effective means of cushioning a slump in employment in the event of widespread use of AI. A responsible legislator should have faced up to the problems in the labor market. The regulatory requirements of the AI Act may create an undue burden on MSMEs. Vague statements in the Regulation may also lead to difficulties in implementation. In the field of labor relations, the application of AI systems such as social scoring of employees, predicting the risk of employees committing crimes, and analyzing employees' emotions may be prohibited due to unacceptable risks. When AI systems are used in the recruitment procedure or human resource management, employers must fulfill different obligations, depending on whether the AI systems are considered high-risk systems. Since employers are obliged to ensure that employees have adequate AI skills, they must offer free training at their own expense. Issues related to the use of ChatGPT in work deserve further study. Unauthorized use of ChatGPT by employees would constitute a violation of labor contract obligations. It seems unwise, at least for the time being, to use ChatGPT in legal advice work, as the system is prone to error.

(责任编辑:余佳楠)