人工智能时代数据与个人信息保护制度研究

王涛

中国移动通信集团河北有限公司，河北石家庄，061299

摘要：人工智能时代，数据与个人信息保护至关重要。探讨保护制度能保障个人权益、维护社会秩序。分析现有制度存在的不足，如法律覆盖不全、监管力度弱等。提出完善法律体系、加强监管、提升技术防护等措施，以构建全面有效的数据与个人信息保护制度。

关键词：人工智能时代；数据保护；个人信息保护；保护制度

作者简介：王涛（1986－），男，满族，河北易县，硕士，中级经济师，研究方向：数据安全与个人信息保护。

课题名称及编号：人工智能时代数据与个人信息保护制度研究

引言：人工智能时代，数据与个人信息的价值日益凸显。然而，信息泄露、滥用等问题频发，对个人和社会造成严重威胁。研究数据与个人信息保护制度，能填补法律空白、规范行业行为，对保障信息安全和推动人工智能健康发展意义重大。

1. 人工智能时代数据与个人信息保护概述

1.1 人工智能时代数据与个人信息的特点

在人工智能时代，数据与个人信息呈现出诸多新的特点。首先，数据量呈爆炸式增长。随着人工智能技术在各个领域的广泛应用，如智能家居、智能医疗、智能交通等，大量的个人信息和各类数据被持续收集。这些数据不仅包括传统的姓名、年龄、联系方式等基本信息，还涵盖了行为习惯、消费偏好、健康状况等深层次的信息。其次，数据的多样性和复杂性增加。不同来源的数据格式各异，有结构化数据，如数据库中的表格数据，也有大量非结构化数据，如文本、图像、音频等。

1.2 数据与个人信息面临的主要风险

在人工智能时代，数据与个人信息面临着诸多主要风险。一方面，技术漏洞带来的风险。人工智能系统本身可能存在技术缺陷，例如算法中的漏洞可能会被黑客利用来获取数据。随着数据挖掘和分析技术的发展，恶意攻击者可以通过复杂的技术手段从看似杂乱无章的数据中提取有价值的个人信息。另一方面，数据收集与使用环节存在风险。许多企业在收集用户数据时，往往存在过度收集的情况，收集的信息远超提供服务所需的范围。而且，在数据使用过程中，缺乏明确的授权机制，数据可能被用于未经用户同意的目的。

2. 国内外数据与个人信息保护制度现状

2.1 国外典型保护制度分析

国外在数据与个人信息保护方面有许多典型的制度值得分析。以欧盟的《通用数据保护条例》（GDPR）为例，它具有广泛的适用性，涵盖了欧盟境内外的企业处理欧盟公民个人数据的情况。GDPR 强调了用户的同意权，企业在收集和处理用户个人数据之前，必须获得用户明确的同意，并且用户有权随时撤回同意。它还规定了数据主体的诸多权利，如访问权、更正权、删除权等。这使得用户能够更好地控制自己的个人信息。在数据泄露通知方面，GDPR 要求企业在发现数据泄露后的 72 小时内通知相关监管机构和数据主体。美国则采取了分散式的立法模式，不同的州和行业有不同的法律法规。例如，加利福尼亚州的《消费者隐私法案》（CCPA），它赋予了消费者更多对自己个人信息的控制权，如有权要求企业披露收集的个人信息类别、用途等。

2.2 国内现有保护制度梳理

在国内，数据与个人信息保护制度也在不断发展完善。我国已经出台了一系列法律法规来保护数据和个人信息。例如，《网络安全法》对网络运营者收集、使用个人信息等方面做出了规定，要求网络运营者遵循合法、正当、必要的原则收集个人信息，并且要对用户信息进行严格的保密。《民法典》将人格权独立成编，其中明确规定了对个人信息的保护，将个人信息纳入人格权的范畴，强调了对个人信息的人格尊严和人格自由的保护。此外，在一些特定领域，如电信、金融等行业，也有专门的规章制度来保护用户的个人信息。

2.3 国内外制度对比与借鉴

通过对比国内外数据与个人信息保护制度，可以发现各有优劣，有许多值得相互借鉴之处。从保护范围来看，欧盟的GDPR保护范围广泛，涵盖了多种类型的数据主体和处理行为，而我国在特定领域有更细致的规定。我国可以借鉴欧盟在扩大保护范围上的经验，进一步整合不同领域的规定，形成更全面的保护体系。在用户权利方面，国外制度赋予用户较多的控制权，如数据主体的删除权等，我国在这方面可以进一步强化用户的权利保障，让用户能够更好地掌控自己的个人信息。而国外可以借鉴我国在特定行业监管方面的经验，加强对特定行业中数据和个人信息保护的针对性。在监管执行方面，我国有较强的行政监管力量，国外可以借鉴我国的监管模式，提高监管的有效性。同时，我国也可以借鉴国外在法律执行过程中的一些监督机制，确保法律法规的严格执行。

3. 现有数据与个人信息保护制度存在的问题

3.1 法律体系不完善之处

现有的数据与个人信息保护法律体系存在着一些不完善的地方。首先，法律规定的协调性不足。不同法律法规之间对于数据和个人信息的定义、保护标准等存在差异，这导致在实际执行过程中容易出现法律适用的混乱。例如，在一些新兴领域，如人工智能生成数据的归属和保护问题，目前的法律并没有明确的规定。其次，法律的前瞻性不够。随着技术的飞速发展，新的数据类型和数据处理方式不断涌现，但现有的法律往往滞后于这些技术发展。例如，对于量子计算技术可能对数据加密带来的挑战，目前的法律尚未有相应的应对措施。再者，法律对于新兴主体的规范不足。在人工智能时代，除了传统的企业之外，还有许多新兴的主体参与到数据处理中来，如小型的数据创业公司、开源社区等，现有的法律并没有很好地对这些新兴主体在数据和个人信息保护方面进行规范。

3.2 监管机制的缺陷

当前的数据与个人信息保护监管机制存在缺陷。一方面，监管部门之间的协调困难。由于数据和个人信息保护涉及到多个部门，如网信部门、工信部门、公安部门等，各个部门的职责存在一定的交叉，在实际监管过程中，容易出现相互推诿或者重复监管的现象。另一方面，监管技术手段相对滞后。面对日益复杂的技术环境，监管部门的技术手段往往跟不上数据和个人信息处理技术的发展速度。例如，对于一些采用先进加密技术隐藏的数据违规行为，监管部门可能难以发现。此外，监管的力度和威慑力不足。对于一些数据和个人信息保护方面的违规行为，处罚力度相对较轻，这使得一些企业和个人在权衡违规成本和收益之后，仍然选择冒险违规操作。

3.3 企业责任落实问题

在数据与个人信息保护方面，企业责任的落实存在诸多问题。部分企业缺乏足够的保护意识，只注重数据带来的商业价值，而忽视了对数据和个人信息的保护。一些企业在内部管理方面没有建立完善的数据保护制度，数据的收集、存储、使用等环节缺乏规范的流程和标准。例如，在员工对数据的访问权限管理上，没有严格的限制，容易导致内部人员的数据泄露风险。而且，企业在数据共享和交易过程中，往往为了追求利益最大化，没有对合作方进行严格的背景审查，导致数据可能被合作方滥用。此外，企业在面对数据和个人信息保护方面的投诉时，响应不及时，处理不积极，没有真正承担起应有的社会责任。

4. 完善数据与个人信息保护制度的策略

4.1 健全法律法规体系

为了完善数据与个人信息保护制度，健全法律法规体系是首要任务。首先，要加强法律法规之间的协调性。通过立法解释或者修订法律等方式，统一不同法律法规中关于数据和个人信息的定义、保护标准等内容。例如，可以制定专门的统一的数据与个人信息保护法，将分散在各个法律法规中的相关规定进行整合。其次，提高法律的前瞻性。立法机构需要密切关注技术发展趋势，在法律中设置一些前瞻性的条款，以应对未来可能出现的技术挑战。比如，对于新兴的数据技术如区块链技术在数据保护中的应用，要提前在法律中有所涉及。再者，完善对新兴主体的规范。针对新兴的主体，如数据创业公司、开源社区等，制定专门的规范条款，明确他们在数据和个人信息保护方面的权利和义务。

4.2 强化监管执行力度

强化监管执行力度是保障数据与个人信息保护制度有效实施的关键。一是要加强监管部门之间的协作。建立跨部门的协调机制，明确各个部门的职责分工，避免职责交叉和推诿现象。例如，可以设立专门的数据与个人信息保护监管协调委员会，由各相关部门派人组成，共同制定监管政策和处理监管事务。二是提升监管技术手段。监管部门要加大在技术研发方面的

投入，采用先进的技术手段来监测和监管数据和个人信息的处理行为。如利用大数据分析技术来发现数据异常流动情况，采用人工智能技术来识别数据违规处理模式。三是加大处罚力度。对于违反数据和个人信息保护规定的企业和个人，要给予严厉的处罚，提高其违规成本。例如，对于故意泄露大量用户数据的企业，可以处以高额罚款，并限制其在相关领域的业务开展。

4.3 推动行业自律规范

推动行业自律规范是完善数据与个人信息保护制度的重要补充。行业协会等组织应该发挥积极作用，制定行业自律规则。这些规则可以针对本行业的特点，对数据和个人信息的收集、使用、共享等方面制定更为细致的规范。例如，互联网行业可以制定专门的用户数据保护自律规范，规定企业在收集用户数据时的最小化原则，即只收集提供服务所必需的数据。同时，行业协会要加强对企业的监督和管理，建立行业内部的监督机制。对于违反行业自律规则的企业，可以给予警告、行业内通报批评等处罚措施，促使企业自觉遵守规则。此外，行业组织还可以通过开展培训、宣传等活动，提高行业内企业和从业人员的数据与个人信息保护意识。

5. 数据与个人信息保护制度的未来发展趋势

5.1 技术创新对制度的影响

技术创新将对数据与个人信息保护制度产生深远的影响。随着区块链技术的发展，其分布式账本、加密算法等特性为数据保护提供了新的思路。区块链可以实现数据的不可篡改和可追溯性，这有助于在数据存储和共享过程中确保数据的真实性和安全性。例如，在医疗数据共享方面，区块链技术可以让患者更好地掌控自己的医疗数据，只有经过患者授权的数据才能被访问和使用。人工智能技术的持续进步也对制度有影响。一方面，人工智能可以用于数据保护的监测和预警，通过机器学习算法来识别数据的异常行为。另一方面，人工智能本身的算法和模型需要大量的数据进行训练，这就需要在制度上平衡数据获取与个人信息保护之间的关系。此外，量子计算技术的兴起可能会对现有的数据加密制度带来挑战，促使制度需要不断创新以适应新的加密需求。

5.2 国际合作与协调方向

在数据与个人信息保护方面，国际合作与协调将成为未来的重要方向。随着全球化的发展，数据的跨境流动日益频繁。不同国家和地区之间的数据保护制度存在差异，这可能会导致数据跨境流动的障碍。因此，各国需要加强国际合作，制定统一的国际标准或者建立双边、多边的协调机制。例如，在国际贸易中，涉及到数据跨境传输的企业需要遵循不同国家的规定，这增加了企业的合规成本。通过国际合作，可以减少这种不必要的成本，促进数据的合理流动。同时，国际组织如联合国、世界贸易组织等也可以在数据与个人信息保护的国际合作中发挥积极作用，推动各国之间的交流与协调，共同应对全球性的数据保护挑战。

5.3 制度发展的挑战与机遇

数据与个人信息保护制度在发展过程中面临着诸多挑战与机遇。挑战方面，技术的快速发展是最大的挑战之一。新的数据处理技术不断涌现，如边缘计算、5G 等，这些技术在带来便利的同时，也给数据和个人信息保护带来了新的风险，制度需要不断适应这些技术变化。另外，公众意识的提高也对制度提出了更高的要求。随着公众对个人信息保护意识的增强，他们对制度的期望也更高，制度需要更好地满足公众的需求。机遇方面，技术创新也为制度发展提供了机遇。如前所述，区块链、人工智能等技术可以为数据和个人信息保护提供新的手段和方法。而且，随着全球对数据和个人信息保护的重视，各国都在积极探索和完善相关制度，这为国际间的交流与借鉴提供了良好的机会，有助于推动本国制度的发展和完善。

结束语：人工智能时代，数据与个人信息保护制度建设刻不容缓。虽面临诸多挑战，但通过完善法律、加强监管等措施，能不断优化保护制度。未来需紧跟技术发展，加强国际合作，为数据与个人信息安全筑牢防线，推动人工智能良性发展。

参考文献

[1] 宋平. 人工智能应用中个人信息保护研究 [D]. 河北大学 ,2019.

[2] 奉海玲. 人工智能时代个人信息的保护研究 [J]. 山东青年政治学院学报 ,2020,36(01):83-89.

[3] 赖时伍. 互联网时代人工智能算法及其在个人信息保护中的应用研究 [J]. 中国高新科技 ,2022,(14):89-91.

[4] 韩婷雯. 人工智能时代下个人信息法律保护研究 [D]. 青海师范大学 ,2023.

[5] 刘晓旭. 人工智能时代个人信息保护研究 [D]. 山东政法学院 ,2020.