利用人工智能实施犯罪的刑法应对策略研究

◆余　振

（中国政法大学，北京 100091）

【摘要】随着人工智能技术的快速发展，刑法对人工智能犯罪的规定需与技术发展保持同步，不断跟进技术的演变和犯罪手段的变化，及时修订和完善刑法对人工智能犯罪的规定。通过制定明确的罪名界定人工智能犯罪行为，利用人工智能检测网络攻击、欺诈、数据篡改等行为，动态掌握各环节的进展情况，并获取详细的信息数据，能够让司法机关准确地认定犯罪行为，并落实相关法律法规，加大刑事追究力度，重点维护各方合法权益，从而促进社会经济健康发展。

【关键词】人工智能；犯罪；刑法

刑法领域中人工智能犯罪是一个相对新的领域，因现有刑法对此类犯罪行为的规定不够全面和详细，还需采取相关措施及法律法规对不法行为严肃处理，反映犯罪行为的社会危害和严重性。再加上职能部门对人工智能技术的监督管理，制定相关法规和机制，防止其被滥用于犯罪活动，需符合法律和道德标准。在此基础上，加强国际合作，追踪、调查、打击此类犯罪，在各领域相互合作的情况下，制定共同的对策和行动计划，从而推动社会秩序发展。

一、刑法领域人工智能的类型划分

（一）预测与预防犯罪

预测与预防犯罪是犯罪学和社会学领域的重要课题之一。在预测犯罪方面，利用数据分析和统计模型来发现犯罪的模式和趋势，预测可能发生的犯罪活动。一些常用的预测方法包括时空分析、热点分析和社会网络分析。

（二）证据分析与识别

证据分析与识别是犯罪调查和司法领域中的重要工作，是确定和评估犯罪案件相关证据的有效手段。遵循科学、客观、公正的法律规定的原则和方法，确保证据的真实性、完整性、可靠性，为犯罪调查和司法审判提供有效支持。

（三）法律研究与辅助

法律研究与辅助通过各种方法和工具帮助法律研究和法律实践，运用科学的方法进行分析和推理，包括文献研究、案例分析、比较法研究、实证研究等，帮助研究人员更全面、准确地了解和解释法律问题，在提高法律领域的学术水平和实践能力方面发挥着重要作用。

（四）智能监狱管理

智能监狱管理是利用人工智能技术和物联网技术提升监狱管理效率和智能化水平，提高监狱管理的智能化程度，提高监狱安全和人员管理的效率和科学性。通过利用人工智能技术和物联网技术，更好地应对监狱管理中的各种挑战，促进监狱安全和犯人康复的双重目标实现。

二、利用人工智能实施犯罪的基本情况及特征分析

（一）基本情况

人工智能具有强大的计算、存储和处理数据的能力，与传统技术有明显区别。传统工具和技术往往是由人类根据自身能力及需求所创造，而人工智能是通过计算机程序和机器学习等技术模拟人类智能的能力，具备自主学习、决策和行动能力，使人工智能在许多领域具有更高的效率和精度，能处理更复杂的问题和数据，并为人类社会带来许多新的机会和挑战。然而，人工智能的发展也需关注其伦理、隐私、安全等方面的问题，确保其应用的合理性。

从刑法层面上打击利用人工智能实施犯罪行为势在必行，通过立法和司法实践，完善刑法规定，使其能适应人工智能技术的发展和应用。同时，加大技术监督管理和刑事打击力度，确保人工智能的应用不会给社会带来安全风险。另外，还需加强法律与技术的融合，培养专业人才，提升司法机关对人工智能犯罪的识别和打击能力，保护社会安全。

例如，部分地区基础设施不完善，成为制约“智慧社会”发展的主要原因之一。人工智能的应用，需良好的网络基础设施和信息技术支持，管理者需要重视对基础设施建设的投入，人工智能技术的普及和应用，大量的个人和敏感信息被收集和使用，信息安全和隐私保护面临新的挑战。再加上相关政策和措施的落实，能够保护个人和社会的信息安全和隐私权益，同时注重社会参与，关注大众的知情权和参与权，从而促进“智慧社会”持续健康发展。

（二）基本特征

第一，形式更新快。人工智能技术的快速发展和广泛应用为犯罪分子提供了新的工具和手段，使得犯罪分子更加隐蔽和高效地进行犯罪活动。例如，网络攻击和数据盗窃处理，因犯罪分子利用机器学习算法和自动化工具，对网络

扫描和漏洞进行攻击，获取敏感信息或控制目标系统。 此外，人工智能技术的发展也使社交攻击更具有针对性和迷惑性，犯罪分子利用人工智能生成的虚假信息和假身份进行欺骗和诈骗。 面对此种情况，需要司法机关和执法部门密切关注人工智能技术的发展趋势，本着与时俱进发展理念更新技术和工具，提高对人工智能犯罪的识别和打击能力。 同时，还需加强国际合作，共同应对跨境人工智能犯罪行为，共同维护网络安全和社会秩序。

第二，影响范围广。 人工智能的强大计算和处理能力使犯罪分子能够高效地进行犯罪活动，并且应用在各个领域中。 例如，在网络安全领域，人工智能被用于进行网络攻击、恶意软件开发、数据盗窃等犯罪行为，利用机器学习和自动化工具，犯罪分子发起钓鱼攻击、破解密码等，从而实现犯罪目的。 或者是在金融领域中，人工智能被用于进行金融欺诈、洗钱和交易操纵等犯罪活动中，犯罪分子预测市场走势、操纵交易或者伪造交易记录，从中获取非法利益。面对此种情况，保护社会安全和打击人工智能犯罪需全球合作和共同努力，各国主管部门、执法机关和技术公司应加强合作，共享情报和技术，提高对人工智能犯罪的预防和打击能力。 同时，加强用户教育和安全意识培养也比较重要，让人们能够识别和防范人工智能犯罪的威胁。

第三，活动更隐蔽。 人工智能被用于加密和隐藏通信，使犯罪分子在网络上进行秘密交流，并组织犯罪活动，难以被发现和干扰。 同时，犯罪分子对人工智能技术的应用，能更精确地选择目标和执行犯罪行为，通过分析大量数据和利用机器学习算法，犯罪分子了解目标的行为模式、喜好和弱点，从而更有针对性地进行攻击或诈骗。 对此问题的处理与防控，打击利用人工智能实施犯罪活动需要加强技术监督管理和执法能力，需要相关部门不断更新技术手段，提高对人工智能犯罪的识别和打击能力。

第四，深度融合。 人工智能技术的发展使犯罪分子将传统犯罪行为与人工智能技术相结合，提高了犯罪活动的效率和隐蔽性。 例如，在网络犯罪领域，犯罪分子利用人工智能技术分析网络攻击、钓鱼诈骗等行为，犯罪分子利用机器学习算法分析目标，恶意攻击社交工程或制定非法软件，使传统网络犯罪行为更具效率。 这引起更多领域的高度重视，尤其是职能部门发挥着较强的职责作用，承担着重点打击和预防犯罪的工作。 例如，执法机关和技术公司深度合作，共同研发和应用人工智能技术，提高对人工智能犯罪的识别和打击能力。

三、利用人工智能实施犯罪的刑法应对策略

(一)完善相关司法解释

第一，制定相关法律法规，明确对利用人工智能实施犯罪行为的定性和处罚。 通过对不同类型的人工智能犯罪行为进行界定，加大刑事责任追究力度，在系统化监督管理过程中，培养执法机构人员的科技素养，提升技术能力，及时识别和应对利用人工智能实施的犯罪行为。 同时，执法机构与科技公司和专业机构建立密切的合作关系，共同研究和开发技术工具和方法，用于犯罪行为的侦查和取证。

第二，在国际合作方面加大投入力度。 因人工智能犯罪往往涉及跨国界的活动，开展国际合作工作极其重要，执法机构与各国共享信息、相互合作，共同应对利用人工智能实施犯罪的挑战，通过签署双边和多边协议，建立跨国合作机制，共同打击跨国犯罪行为。

第三，完善司法解释，在具体案件中的应用非常重要。相关司法机关根据实际案例和技术发展情况，及时发布、修订相关司法解释和判例法，明确对利用人工智能实施犯罪行为的认定标准和处罚措施，维护社会安全和秩序。

(二)调整相关犯罪的构成要件

第一，增加或修改相关罪名，更准确地界定利用人工智能实施的犯罪行为。 例如，设立或修改关于盗取、滥用或篡改人工智能系统的罪名，以及关于利用人工智能系统进行网络攻击、欺诈等犯罪行为的罪名。 在利用人工智能实施犯罪的过程中，扩大犯罪责任的适用范围，涵盖利用人工智能系统进行犯罪活动的教唆者、共谋者等，加重刑罚的惩罚幅度，更好地反映犯罪的严重性和社会危害性。

第二，引入新的构成要件，更准确地描述犯罪行为的特点和特征。 例如，引入与人工智能技术相关的构成要件，如未经授权访问、操纵或干扰人工智能系统等，调整相关犯罪的构成要件，避免过度扩大犯罪责任范围，保障法律的适用性和公正性。

(三)明确利用人工智能实施犯罪的刑法主体界定

在刑法中，犯罪主体是指能够承担刑事责任的人。 当前，人工智能(AI)并不具备独立的法律主体地位，因 AI 本身不具备自主的行为能力和刑事责任能力。 然而，随着技术的发展，AI 在犯罪活动中扮演不同角色，在当前的刑法框架下，利用人工智能实施犯罪的主体界定，通常会将责任归咎于实际操控或控制 AI 的人，因 AI 系统具备更高的自主性和决策能力，使其能在没有人类干预的情况下做出独立决策和行为。 例如，对 AI 系统的行为，追究开发者、制造商、运营者在设计、制造及运营过程中的一定的责任，刑法主体界定考虑到 AI 系统的行为是否符合刑法中对于犯罪的主观要素的要求，如是否具备故意、过失等，使用或操纵人工智能系统、利用人工智能算法进行犯罪活动等，明确犯罪行为的主体和对象，为司法机关提供明确的判定依据。

(四)构建公民个人信息数据保护系统

第一，海量数据的集聚本身就面临着安全风险。 大数据系统需确保数据的完整性、保密性、可用性，防止数据泄

露、篡改、滥用等问题的出现。同时，随着人工智能技术的发展，对海量数据的需求持续增加，需收集、存储更多数据，使安全风险进一步增加。

第二，人工智能技术的不断更新和普及，为侵犯信息安全的犯罪活动提供了便利条件。犯罪分子利用人工智能技术进行网络攻击、钓鱼诈骗等行为，从而获取他人的个人信息和敏感数据，但并不意味着所有人都具备足够的安全意识和知识，给信息安全带来了更多挑战。

第三，对侵犯公民个人信息的犯罪行为，相应的保护方式需及时改善。随着人工智能的广泛应用，个人信息的保护尤为重要，相关部门应加强对个人信息的监督管理和保护，制定相关法律法规和政策，加大对个人信息的收集、存储、传输、处理等过程的监控力度，确保个人信息的安全和隐私得到有效保护。

(五)构建人工智能犯罪风险防范系统

第一，设立技术准入制度。对人工智能技术的引入和应用，在技术尚未成熟和安全性有待验证的情况下，设立准入门槛和适用范围的限制极其重要。在保障安全的前提下，需权衡各方利益，制定合理的政策和规定，促进人工智能技术的发展。同时，人工智能技术的强大辅助能力和潜力不可否认，有着广泛的应用前景和发展空间。然而，由于人工智能技术的特殊性，一旦出现故障或错误，会对人民的生命和财产安全造成严重影响。因此，在引入人工智能技术时，需设立准入门槛和适用范围的限制，确保其安全可控。

例如，涉及人民生命财产安全的领域，同样需要设立严格的准入制度，在医疗领域应对人工智能技术的应用进行严格审查，确保其准确性和安全性。在金融领域，对于自动化交易系统等应设立合理的监督和控制机制，以防止不可预测的风险和风险滥用。

第二，设置人工智能命令“禁区”。在允许人工智能涉及的领域内，设定人工智能的工作原则，包括对数据隐私和信息安全的保护、对决策透明性和解释性的要求、对公平性和道德价值的考虑等，确保人工智能在工作过程中遵循一定的准则和规范，保障使用人工智能时的安全性和合法性。对人工智能涉及的领域进行规定，不同领域的特点和需求不同，需明确规定人工智能在各个领域中的应用范围和限制。

例如，在医疗领域，设定人工智能在诊断、治疗等方面的应用原则，确保其准确性和安全性；金融领域，设立相应的监督和控制机制，防止人工智能在交易和投资决策中的滥用。为实现对人工智能行为的规制和预测，还需加强相关法律法规的建设和政策制定，从法律法规和政策方面创新技术、加强隐私保护等，确保人工智能的应用符合社会的期望和价值观。

第三，严控人工智能技术发展。为保障人类的生存和发展，在控制人工智能时限制其进化速度，加强对人工智能技术的监督管理和控制，划定特定领域和行业，对研发者和使用者严格审查，也属于一种有效的方式，确保人工智能技术的发展符合社会期望和价值观，避免出现潜在的风险和危害。

此外，有关部门和行业制定严格的国家标准和行业标准，对相关领域和行业的配套设施、资格准入政策等规范管控，通过制定相关标准和规范，提高人工智能技术的安全性和可靠性，使其在特定领域和行业的应用符合相关要求，并规范相关行为，对人工智能技术有效把控和限制，权衡各方利益和技术发展需求。在制定政策和规定时，充分考虑技术创新和发展需求，避免过度限制和阻碍科技的进步。

四、结束语

综上所述，了解刑法领域人工智能的类型，分析人工智能实施犯罪的基本情况及特征，能够深层次探析各种问题发生的具体原因。因此，职能部门需引起高度重视，在多个领域中加大监督管理力度，完善相关司法解释，构建个人信息保护相关的法律法规体系，明确个人信息的定义、范围和权利，确定数据主体和数据处理方的责任、义务，加强对个人信息的监督管理和惩处力度，保证法律法规实施的有效性。与此同时，随着人工智能的普及及宣传力度的持续加大，人工智能技术及法律法规的应用范畴将会扩大，因此需要应用现代化技术手段构建人工智能犯罪风险防范系统，重点打击违法行为，从而推动社会经济健康发展。

参考文献：

[1]姜莹.人工智能的刑事风险及刑法应对[J].法制博览,2022(27):43-45.

[2]王立博.《刑法》视阈下涉人工智能犯罪应对措施研究[J].法制博览,2022(24):61-63.

[3]陶宏硕.论人工智能时代,犯罪的危险性与刑法对策[J].秦智,2022(04):18-20.

[4]孙道萃.人工智能刑法研究的反思与理论迭进[J].学术界,2021(12):64-76.

[5]张国妮,刘军.人工智能的犯罪主体及其刑法规制[J].宜宾学院学报,2021,21(03):68-76.

[6]齐思雨.我国人工智能犯罪的刑法困境与立法构建策略[J].法制博览,2021(07):131-132.

作者简介：

余振(1989－),男,汉族,浙江杭州人,本科,研究方向:刑法学。