网络犯罪的刑法适用问题研究

●胡建东

[摘要] 本文旨在探讨网络犯罪行为的特殊性，及其对传统刑法理论与实践提出的挑战。随着互联网技术的迅猛发展，网络犯罪呈现出跨国性、匿名性、高技术性等特点，这对现行刑法的立法、执法及司法适用均提出了新的要求。本文阐述了研究网络犯罪的刑法适用问题意义，分析了网络犯罪的基本特征与类型，论述了网络犯罪的刑法适用难点。同时，笔者对现有刑法体系在应对网络犯罪时存在的不足之处进行研究，并提出利用先进技术预防与侦查网络犯罪的刑法应对策略，以供参考。

[关键词] 网络犯罪；刑法适用；跨国性；匿名性；技术侦查

研究网络犯罪刑法适用问题的意义

研究网络犯罪的刑法适用问题具有重大的理论与实践意义，具体体现在以下方面。

(1)适应时代发展需求：随着信息技术的快速发展，网络犯罪形式不断创新，手段日益隐蔽，跨越地理界限，对传统的刑法理论与司法实践提出了挑战。研究网络犯罪的刑法适用问题，有助于刑法体系及时解决技术变革带来的新问题，确保法律的有效性和适应性。

(2)填补法律空白：网络空间的特殊性导致一些传统犯罪在网络环境中呈现出新的特点，可能不在现有刑法条款的直接规制范围内。研究其适用问题，可以明确如何合理延伸或解释现行法律，或提出立法建议，填补法律空白，确保所有网络违法行为都能得到有效制裁。

(3)保护公民权益：网络犯罪往往涉及对个人隐私、财产安全等基本权利的侵犯。深入研究刑法如何有效打击此类犯罪，对于维护公民的隐私权、财产权等合法权益至关重要，有助于提升公众对网络环境的信任感和安全感。

(4)促进网络文明与秩序：网络空间作为现代社会不可或缺的一部分，其秩序直接影响到公众的个人隐私、财产等方面的安全。研究网络犯罪的刑法适用，旨在整顿网络秩序，促进网络文明，创造一个健康、安全的网络环境，支持数字经济和社会信息化的可持续发展。

(5)国际合作与交流：网络犯罪的跨国性质要求国家之间进行法律合作。研究刑法适用问题，可以为国际司法协助、引渡协议等提供法律基础，加强全球范围内的网络犯罪防治合作。

(6)提升司法效率与司法公正性：明确网络犯罪的定性、量刑标准及证据规则，能够指导司法机关更加准确、高效地处理网络犯罪案件，保障刑事司法的公正性和权威性。

网络犯罪的基本特征与类型

网络犯罪是指行为人运用计算机技术，借助于网络平台对其系统或信息进行攻击、破坏，或利用网络进行其他类型犯罪活动的总称。网络犯罪的特点：隐蔽性高与风险小、预谋性强、犯罪主体年轻化、法律与监管滞后性、成本低、传播快、范围广、取证与司法执行难度大、严重的社会危害性、双重性质。网络犯罪的主要类型涵盖了从直接针对计算机信息系统的技术攻击，到利用网络作为工具的各种经济、社会性犯罪，主要体现在以下几个方面。

(一)直接针对计算机信息系统的犯罪

(1)非法侵入计算机信息系统罪：未经许可擅自进入他人计算机系统，如黑客攻击。(2)破坏计算机信息系统罪：故意制作、传播计算机病毒，对系统进行攻击导致功能失常或数据丢失。(3)非法获取计算机信息系统数据、非法控制计算机信息系统罪：未经授权获取系统数据或控制权，如盗取个人信息、商业秘密。(4)提供侵入、非法控制计算机信息系统程序、工具罪：制造、销售用于非法侵入或控制计算机系统的工具。

(二)利用计算机网络实施的经济犯罪

(1)金融诈骗罪：通过网络实施的各类金融诈骗，如网络钓鱼、假冒网站、投资诈骗。(2)盗窃罪：利用技术手段窃取电子资金、虚拟财产等。(3)贪污、挪用公款罪：利用职务之便，在网络环境中进行的贪污或挪用行为。(4)网上走私、非法交易：利用网络平台进行走私物品交易或进行非

法商品买卖。(5)网上洗钱：利用网络金融系统掩饰非法所得的资金来源和性质。

(三)侵犯个人和社会秩序的犯罪

侵犯个人和社会秩序的犯罪类型包括但不限于以下方面：(1)侵犯个人隐私，非法获取、泄露个人数据或监视个人网络活动。(2)虚假广告，在网络上发布虚假信息误导消费者。(3)网上毁损商誉，通过网络散布谣言、恶意评价损害企业或个人名誉。(4)在线侮辱、毁谤，利用网络平台对他人进行言语攻击和诽谤。(5)网上侵犯商业秘密，非法获取并泄露或使用他人的商秘业密。(6)在线间谍活动，利用网络刺探、窃取国家秘密。(7)网上刺探、提供国家机密，非法获取并通过网络泄露国家秘密。这些类型的网络犯罪展示了网络空间中犯罪行为的多样性和复杂性，对于网络犯罪的打击和预防需要实施法律、技术、教育等多方面的综合措施。

Q 网络犯罪的刑法适用难点

证据收集与保全在法律实践中具有特殊性，特别是在处理复杂的或技术密集型案件时，如网络犯罪、知识产权侵权、国际商事仲裁等领域的案件时，其特殊性体现在以下方面。

(1)公权力介入与法定程序：证据保全通常涉及法院或其他具有公权力的机构根据法律规定采取措施，以确保重要证据不会被破坏、篡改或遗失。这与一般由当事人自行收集证据的方式形成对比，体现了法律对特定证据的重视及对程序正义的保障。

(2)技术性要求：特别是在处理电子证据时，由于电子数据的易变性、易篡改性和技术依赖性，收集和保全电子证据时需采用专门的技术手段和程序，如数据镜像、加密传输、时间戳记录等，以确保证据的完整性和真实性。

(3)紧急性与即时性：某些情况下，证据可能迅速消失或改变，如网络数据的自动覆盖、服务器关闭等。因此，对证据的即时收集与保全至关重要，这可能需要紧急申请法院命令进行干预。

(4)专业人员的参与：专业技术人员，如 IT 专家、法医鉴定人员等，在特定类型证据的收集与保全中扮演关键角色，他们提供的专业知识和技术支持是确保证据合法性和有效性的重要因素。

(5)跨国合作：在跨国案件中，证据可能存储在不同国家，这就需要国际法律协助和合作，通过引渡请求、司法互助条约等方式实现证据的收集与交换，增加了过程的复杂性和挑战性。

(6)知识产权案件的特殊考量：在知识产权诉讼中，证据的特殊性在于可能涉及商业秘密、技术细节等敏感信息。因此，在保全过程中需特别注意保密性，避免将敏感信息泄露给竞争对手，影响企业的市场竞争力。

总之，证据收集与保全的特殊性要求法律从业者、技术人员及相关机构具备高度的专业知识、敏锐的应急反应能力以及良好的国际合作能力，以确保法律程序的顺利进行和司法公正的实现。

Q 利用先进技术预防与侦查网络犯罪的刑法应对策略

大数据和人工智能在犯罪预防与侦查中发挥着日益重要的作用，有助于提升公共安全管理和犯罪响应的效率与效果。

(一)数据分析与预测

相关部门利用大数据技术对海量历史犯罪数据进行分析，揭示犯罪模式、热点区域和时间分布，帮助执法部门预测犯罪趋势和高风险区域，实现犯罪的前瞻性预防。人工智能算法能够通过机器学习模型，识别犯罪行为的早期迹象，预测潜在的犯罪活动，为警方部署资源提供科学依据。

(二)智能监控与识别

智能视频监控系统集成人脸识别、行为分析技术，能够实时监测异常行为，及时发现并预警犯罪行为，尤其在公共场所的安全管理中效果显著。相关部门利用大数据整合各类监控资源，如社交媒体信息、通讯记录等，有助于追踪犯罪分子行踪，为案件侦查提供线索。

(三)案件关联分析

通过人工智能对不同案件的数据进行深度挖掘和关联分析，发现案件之间的隐含联系，支持串并案侦查，提高破案效率。建立预警机制，基于数据分析结果，对可能发生的犯罪活动进行预警，为预防措施提供决策支持。

(四)智能情报研判

人工智能技术能够快速处理和分析海量情报信息，辅助侦查人员识别关键信息，提升情报分析的准确性和速度。自动化筛选和分类海量数据，帮助侦查人员识别嫌疑人、受害者的关联信息，以及犯罪网络结构，为制定侦查策略提供依据。

(五)数据处理自动化与效率提升

大数据和人工智能技术的自动化处理能力，减少了人工处理数据的负担，提高了工作效率，使侦查人员能够聚焦于更为复杂的案件分析和决策制定。此外，还可以提升证据收集与保全的效率，尤其是在电子证据的处理上，自动化工具可以确保数据的完整性和链路的可追溯性。

(六)司法公正与透明度

虽然大数据和 AI 技术增强了犯罪预防与侦查的能力，但也对算法的公正性、透明度产生了一些影响。因此，相关部门建立相应的监督机制，确保算法决策的可解释性和公

平性。

总之，大数据和人工智能技术正逐步改变犯罪预防与侦查的传统模式。大数据和人工智能使侦查人员对案件的处理更加精准、高效，为构建安全社会环境贡献了力量。然而，相关部门在应用先进技术处理网络犯罪案件的同时，也需重视伦理、隐私保护以及司法公正等方面的问题。

网络犯罪的刑法适用应注意的关键问题及相关建议

（一）网络犯罪的刑法适用应注意的关键问题

（1）管辖权确定：由于网络犯罪的跨地域性，确定案件的管辖权是一大挑战。相关部门需要明确国内法与国际法的适用范围，以及如何协调不同国家间的司法管辖权，确保犯罪行为得到有效追究。

（2）犯罪行为的界定：网络犯罪手段新颖多变，传统刑法可能难以直接适用。相关部门需不断更新和完善法律条文，明确界定如黑客攻击、网络诈骗、侵犯个人隐私、制作与传播恶意软件等网络犯罪行为的构成要件。

（3）证据收集与保全：网络犯罪证据易被篡改、删除且分布广泛，如何合法有效地收集、固定电子证据，确保其完整性和真实性，是司法实践中的一大难题。

（4）技术理解与应用：司法人员需要具备一定的技术知识，以便理解复杂的网络犯罪手法，正确解读技术证据，这对培训和教育提出了更高要求。

（5）国际合作：网络犯罪往往涉及跨国界，加强国际的法律互助、信息共享和引渡合作是打击此类犯罪的关键，但这也面临着法律差异等挑战。

（6）法律滞后性：技术的快速发展使得法律往往滞后于现实需求，需要不断修订法律，确保刑法的有效性和适应性。

（7）隐私权与国家安全的平衡：在打击网络犯罪的同时，必须注意保护公民的隐私权和数据安全，避免过度监控和侵犯个人权利。

（8）量刑标准：如何合理设定网络犯罪的刑罚，确保罪责刑相适应，既能有效威慑犯罪，又不至于过度惩罚，是刑法适用中的重要考量。

（9）预防与预警机制：构建有效的预防网络犯罪机制，包括预警系统、风险评估和公众教育，也是刑法适用之外的重要补充。

针对这些关键问题，各国政府和国际组织正不断探索和改进相关法律制度与国际合作机制，以适应网络空间安全的新形势。

（二）针对网络犯罪的刑法适用相关问题的建议

（1）立法修订：随着网络犯罪形态的不断演变，立法机关需要定期审查和更新相关法律法规，确保其能够覆盖新的犯罪形式，明确网络犯罪的定义、罪状描述和量刑标准。同时，强化数据保护和隐私权法律保护，为有效维护网络空间的良好秩序提供坚实的法律基础。

（2）强化国际合作：网络犯罪的跨国性质要求国际社会加强合作。通过签订双边或多边协议，建立快速有效的法律互助机制，促进情报共享、证据互认和犯罪嫌疑人的引渡。国际组织如联合国、欧盟、国际刑事警察组织等在推动国际标准、指导原则和合作框架方面扮演着关键角色。

（3）技术工具开发与应用：利用先进的技术手段，如大数据分析、人工智能、区块链追踪等，开发专门针对网络犯罪侦查和预防的工具。这些技术可以帮助执法机构更高效地识别犯罪模式、追踪资金流动、保护关键基础设施安全，并增强网络防御能力。

（4）加强公众教育，增强公众安全防范意识：普及网络安全知识，提升公众对网络犯罪的认识和防范能力，是预防网络犯罪的第一道防线。通过学校教育、媒体宣传、社区活动等多种渠道，教育公众如何识别网络诈骗、保护个人信息、安全使用网络服务，营造全社会共同维护网络空间安全的良好氛围。

以上这一系列措施相互支撑，形成了一套多维度、多层次的网络犯罪防控体系，旨在构建更加安全、可信的网络环境。

参考文献

[1]王文华，姚图，孟庆松，等.网络犯罪案件适用法律问题研究[J].人民检察，2019(04)：69-72.

[2]卓翔.网络犯罪综合治理刑事政策刍议[J].福建政法管理干部学院学报，2002(04)：18-22.

[3]于冲.网络犯罪罪名体系的立法完善与发展思路——从97年刑法到《刑法修正案(九)草案》[J].中国政法大学学报，2015(04)：39-54，159.

[4]杜文辉.网络犯罪的刑法规制研究[D].哈尔滨：黑龙江大学，2020.

[5]喻海松.网络犯罪的立法扩张与司法适用[J].法律适用，2016(09)：2-10.

作者简介：

胡建东(1988－)，男，汉族，福建龙岩人，硕士研究生，中国政法大学法学院，研究方向：经济法。