Open Journal of Legal Science 法学, 2024, 12(5), 2970-2975
Published Online May 2024 in Hans. https://www.hanspub.org/journal/ojls
https://doi.org/10.12677/ojls.2024.125423

Hans汉斯

网络犯罪在刑法中的定性与处罚机制研究

杨依琳

汉口学院文法学院，湖北 武汉

收稿日期：2024年3月25日；录用日期：2024年4月7日；发布日期：2024年5月17日

摘 要

随着互联网技术的飞速发展，网络犯罪以其匿名性、跨国性、技术性的特点，日益成为全球性的挑战。这类犯罪不仅对个人的财产和隐私权造成了严重影响，同时也对国家安全和社会稳定构成了威胁。因此，如何在刑法框架内准确定性网络犯罪，并建立有效的处罚机制，成为了法学研究的重要议题。本研究揭示了当前网络犯罪刑法定性与处罚机制面临的主要问题，包括法律条文的滞后性、跨国执法的复杂性等，并提出了相应的改进建议。这旨在为法律实践者和政策制定者提供参考，以更有效地应对网络犯罪，保护公民权益，维护社会秩序。

关键词

网络犯罪，刑法，定性，处罚机制，信息安全

Study on the Characterization and Punishment Mechanism of Cybercrime in Criminal Law

Yilin Yang

School of Arts and Law, Hankou University, Wuhan Hubei

Received: Mar. 25th, 2024; accepted: Apr. 7th, 2024; published: May 17th, 2024

Abstract

With the rapid development of Internet technology, cybercrime, with its anonymity, transnationality and technological nature, has increasingly become a global challenge. Such crimes not only have a serious impact on the property and privacy of individuals, but also pose a threat to national security and social stability. Therefore, how to accurately characterize cybercrime within the framework of criminal law and establish effective punishment mechanisms has become an important

文章引用: 杨依琳. 网络犯罪在刑法中的定性与处罚机制研究[J]. 法学, 2024, 12(5): 2970-2975.
DOI: 10.12677/ojls.2024.125423

topic of legal research. This study reveals the main problems faced by the current criminal law characterization and punishment mechanism of cybercrime, including the lag of legal provisions and the complexity of transnational law enforcement, and puts forward corresponding suggestions for improvement. This aims to provide reference for legal practitioners and policy makers to more effectively respond to cybercrime, protect citizens' rights and interests, and maintain social order.

Keywords

Cybercrime, Criminal Law, Characterization, Punishment Mechanisms, Information Security

1. 引言

网络技术的进步为社会发展带来了诸多便利，但同时也孕育了新型的犯罪形式——网络犯罪。尽管各国在立法和执法方面做出了努力，网络犯罪的高发态势仍未得到有效遏制。特别是网络犯罪的刑法定性和处罚机制，成为法律实务和学术研究中的难题。传统的刑法原则和规定往往难以适应网络空间的特殊性，如何精准定性网络行为，制定合理有效的处罚措施，既要考虑到技术的发展变化，又要兼顾法律的稳定性和公正性，成为摆在我们面前的紧迫问题。

2. 网络犯罪的概念与特点

网络犯罪，作为信息时代的产物，随着互联网技术的普及和发展迅速崛起。它涉及利用电脑网络进行的非法活动，包括对信息系统的侵害、网络诈骗、侵犯个人隐私等多种形式。网络犯罪的定义虽然在不同国家和地区有所差异，但普遍认为，任何利用计算机网络技术实施的、侵犯他人权益、违反社会管理秩序的行为，都可以归类为网络犯罪。

2.1. 网络犯罪的定义

网络犯罪的核心在于其利用了网络技术，作为犯罪的手段或目标。这包括通过网络对计算机系统造成破坏、非法侵入和控制网络系统、通过网络传播有害信息或进行网络诈骗等。它的本质是对网络空间的非法控制和利用，目的是获取非法利益或造成他人损失[1]。

2.2. 网络犯罪的主要特点

网络犯罪区别于传统犯罪的显著特征，主要体现在以下几个方面：一是跨国性，网络空间没有国界，网络犯罪往往涉及跨国行为，犯罪分子和受害者可能分布在世界的不同角落，这给犯罪的侦查和司法管辖带来了巨大的挑战。二是匿名性，网络为犯罪分子提供了前所未有的匿名性。通过技术手段，犯罪分子可以隐藏自己的真实身份，使追踪和定责变得异常困难。三是技术性，网络犯罪的实施通常需要一定的技术知识和能力，从利用软件漏洞、编写恶意代码到利用社会工程学手段，技术性是网络犯罪的重要特点之一。四是侵害性，网络犯罪对个人和社会的危害极大，不仅对个人的财产、隐私权造成侵害，还可能对国家安全、社会公共利益造成威胁。例如，网络攻击可能导致重要基础设施瘫痪，数据泄露可能导致公民个人信息被滥用。

3. 网络犯罪的类型及其刑法定性问题

3.1. 网络犯罪的分类

网络犯罪主要有以下几种类型，一是网络诈骗，这是一种利用电子通信技术进行的诈骗行为，通过虚构事实或隐瞒真相，诱使受害者转移资产。网络诈骗的手法多样，包括但不限于网络购物诈骗、网络投资理财诈骗、网络赌博诈骗等。二是网络盗窃，指利用网络技术非法侵入他人计算机系统，窃取财产的行为。这包括盗取网络银行账户信息、信用卡信息等。三是网络侵权，主要指侵犯他人知识产权或个人隐私权的行为[2]。例如，未经授权下载和传播受版权保护的音乐、电影，或者非法搜集和使用他人个人信息。此外，网络犯罪还包括如网络色情、网络暴力、网络恐怖主义等其他通过网络实施的犯罪行为。

3.2. 网络犯罪的刑法定性

网络犯罪的刑法定性是将这类犯罪有效纳入司法体系的关键一环，它要求法律实践者不仅识别出网络环境中的非法行为，还需要依据现有的法律框架对其进行恰当的法律评价和处理。这一过程中，法律的基本原则，如罪刑法定原则和比例原则，成为了进行刑法定性的基石。罪刑法定原则要求任何刑事处罚都必须有明确的法律依据，这意味着只有当法律条文明确规定了某种网络行为构成犯罪时，才能对行为人追究刑事责任。这一原则确保了法律的透明度和公正性，同时也给法律制定者提出了挑战，即如何在迅速变化的网络环境中及时更新和完善相关法律规定。比例原则则要求处罚必须与犯罪行为的严重程度相匹配。在网络犯罪的背景下，这一原则的应用尤为复杂，因为网络犯罪的影响和危害往往跨越国界，涉及多方面的利益冲突。法律制定和实践过程中，如何恰当评估网络犯罪的危害程度，并据此制定相应的处罚标准，是对法律专业人士的重大考验。

在对网络犯罪进行定性的过程中，存在新颖性和复杂性两大难点，一方面，网络技术的快速发展使得新型犯罪形式层出不穷，现有的法律条文可能难以涵盖所有新出现的犯罪行为；另一方面，网络犯罪的技术性特征使得判断犯罪行为的界限变得更加困难，如何界定正当的网络行为和犯罪行为之间的边界，成为法律实务中的一个难题。

4. 现行刑法对网络犯罪的处罚机制

对于网络犯罪的处罚，不同国家和地区根据其法律体系和实际情况，制定了相应的法律条文和政策指导。这些处罚机制主要包括刑事处罚、行政处罚和民事赔偿等，旨在通过法律手段对犯罪分子进行惩戒，同时对受害者给予一定的补偿。

4.1. 处罚原则和法律依据

在全球范围内，对网络犯罪的处罚不仅是法律行为的一个重要组成部分，也是确保数字空间安全和公正的关键机制。为实现这一目标，各国法律体系普遍采用了罪刑相适应和法定刑罚的原则。这意味着任何形式的刑罚都必须与犯罪的性质和严重程度相匹配，并且犯罪及其相应的刑罚必须有法律明文规定，确保法律的明确性和可预测性。

罪刑相适应原则要求刑罚必须与犯罪行为的危害程度和犯罪人的过错程度相符合，这一点在网络犯罪的处罚中尤为重要[3]。因为网络犯罪的影响范围广泛，涉及到的利益关系复杂，其危害性有时不易直观评估。因此，法律在设定处罚时必须综合考虑犯罪行为对社会、个人及国家安全的实际影响，以制定合理的处罚标准。

法定刑罚原则则确保了刑罚的实施不会受到任意性的影响，每一项刑罚都必须依据法律条文执行。

这对于网络犯罪尤为关键，因为网络环境的复杂性和新颖性要求法律必须具备足够的灵活性和前瞻性，以适应不断变化的技术环境。为了应对网络犯罪的复杂性和新颖性，多个国家都制定或修订了《网络安全法》、《数据保护法》等特别法律和条款，这些法律和条款不仅定义了网络犯罪的法律框架，也为处罚提供了明确的法律依据。这些法律的制定和实施，构建了一个更加安全、公平的网络空间，再保障公民的数字权利的同时，也能对网络犯罪行为施以有效的法律制裁。

4.2. 具体处罚措施

在应对网络犯罪的过程中，具体处罚措施的制定和实施对于维护网络空间的法律秩序，保护公民的合法权益具有至关重要的作用。根据犯罪的性质和严重程度，可以采取包括刑事处罚、行政处罚和民事赔偿在内的多种处罚方式。

刑事处罚在打击网络犯罪方面起到了核心作用，特别是针对那些严重危害社会秩序和公民权益的行为，如网络诈骗、网络盗窃等。刑事处罚通过罚金、监禁等手段，不仅对犯罪分子进行直接的惩戒，更重要的是发挥了威慑作用，防止相似犯罪行为的发生。例如，对于盗取他人财物或资金的网络盗窃行为，严厉的刑事处罚能够显著提升法律的震慑力，保护网络交易的安全性。

行政处罚则更多地应用于较轻微的网络犯罪或犯罪初期的行为，通过罚款、警告、吊销营业执照等措施，旨在纠正非法行为，恢复被破坏的社会秩序。行政处罚的优势在于其操作的灵活性和及时性，能够迅速对犯罪行为做出反应，减少社会损失。比如，对于非法搜集和使用个人数据的行为，行政机关可以通过罚款等方式，及时制止违法行为，保护公民个人信息安全[4]。

民事赔偿机制的设立，则主要考虑到保护受害者的权益，使其能够通过法律途径获得损失的补偿。这不仅有助于缓解受害者的经济和情感损失，也强化了对犯罪行为的法律制裁。在网络犯罪中，犯罪行为通常会导致个人或企业遭受财产损失，在这个过程中，民事赔偿成为了受害者追求正义的重要手段。受害者通过法院提起民事诉讼，要求犯罪分子赔偿因网络犯罪造成的经济损失，不仅体现了法律对受害者权益的保护，也增强了社会公众对法律的信任。

5. 网络犯罪处罚机制的问题与挑战

尽管现行的刑法对网络犯罪设立了一定的处罚机制，但在实践中仍然面临许多问题和挑战。这些问题不仅涉及法律条文的适应性和先进性，还包括跨国执法的协作难题、技术发展带来的新型犯罪形式，以及预防和教育措施的不足。

5.1. 法律适用的困难

随着互联网的普及和技术的不断进步，网络犯罪呈现出前所未有的复杂性和多样性。现行法律体系在设计之初往往未能充分预见到这些技术的发展，导致对新出现的网络犯罪类型缺乏明确的法律规定和适应性。例如，云计算、物联网、人工智能等新兴技术领域的快速发展，带来了新型的犯罪方式，而这些往往在传统的刑法体系中找不到对应的法律条文进行准确定性。加之网络犯罪的匿名性和跨国性特征，使得追踪犯罪分子、收集证据以及确定法律管辖权变得更加困难。

5.2. 跨国执法的挑战

网络犯罪的跨国性质不仅扩大了其犯罪影响的范围，也为国际执法合作带来了前所未有的挑战。由于不同国家和地区在法律体系构建、执法机构能力、以及技术基础设施等方面的差异显著，这些差异成为了加强国际间协作、有效打击网络犯罪的主要障碍[5]。例如，一国的网络犯罪可能在另一国造成损害，

但两国之间若缺乏快速反应和信息共享的机制，则难以形成有效的打击力度。同时，国际间缺乏统一的法律标准和协调机制，使得即便是意识到跨国犯罪行为，各国之间在法律适用和证据交换上的冲突和障碍也会大幅度降低追责的效率和效果。

5.3. 技术发展与法律滞后

技术的快速发展带来了新型犯罪手段和模式，而法律的更新往往滞后于技术发展。这种滞后不仅体现在新型犯罪形式难以及时纳入刑法框架，也表现在执法机关缺乏应对新技术的知识和工具。这种差距使得法律对网络犯罪的威慑和处罚效果大打折扣。

5.4. 预防与教育的不足

除了对犯罪行为的处罚外，预防网络犯罪的发生同样重要。然而，目前在网络犯罪预防和公众教育方面的投入和效果仍然不足。公众缺乏有效的网络安全意识、网络道德教育和技术防护措施，是导致网络犯罪高发的重要原因之一。

6. 完善网络犯罪的刑法定性与处罚机制的建议

6.1. 加强国际合作，共同打击网络犯罪

鉴于网络犯罪的跨国性特征，国际合作是打击网络犯罪的关键。建议各国加强法律和技术层面的交流与合作，建立统一或兼容的网络犯罪定义和处罚标准。通过签订国际条约、建立国际执法机制，提高跨国网络犯罪案件的侦破和司法效率。

6.2. 更新和完善刑法条款，适应技术发展

为应对技术进步带来的新型犯罪形式，相关部门需定期审视和更新刑法中有关网络犯罪的条款，明确新型网络犯罪行为的法律界定和处罚规定。同时，增设针对网络犯罪的专门章节或条款，加强对网络犯罪的法律规制。

6.3. 强化网络犯罪的预防和教育

预防网络犯罪的发生同样重要。建议在全社会范围内加强网络安全教育和网络道德教育，提高公民的网络安全意识和自我保护能力。对于青少年，应在学校教育中加入网络安全和法制教育的内容，培养健康的网络行为习惯。

6.4. 提高执法效率和法律的适用性

针对网络犯罪定性难、证据收集难等问题，建议加强执法机关的技术装备和专业培训，提升对网络犯罪的侦查和证据收集能力。同时，探索和发展适用于网络环境的法律程序和技术手段，如利用数字证据、网络追踪技术等，增强法律适用的实效性和精准度。

7. 结语

在应对网络犯罪这一全球性挑战时，法律体系的适应性、国际合作的深度与广度、社会公众的安全意识，以及技术与教育的支持，共同构成了一个综合性的防控网络。有效地打击和预防网络犯罪，不仅要求法律不断进步以匹配技术的发展，还需要全球范围内的协同努力和广泛的社会参与。通过不断完善法律制度、加强国际协作、提升公众意识和执法能力，可以为网络空间的安全、稳定和繁荣提供坚实的基础。这一过程中，每个个体的责任感与参与度，都是守护网络空间安全的重要一环。

参考文献

[1] 张硕. 网络数据安全的刑法保护分析[J]. 法制博览, 2024(6): 46-48.

[2] 路军, 杨子衿. 帮助信息网络犯罪活动罪定性之探讨[J]. 辽宁师范大学学报(社会科学版), 2024, 47(1): 67-74.

[3] 夏伟. 网络有组织犯罪的组织进化与治理转型[J]. 法学论坛, 2024, 39(1): 63-73.

[4] 梅正崇. 我国网络犯罪刑法规制问题研究[J]. 法制博览, 2023(36): 115-117.

[5] 赵雅琪. 网络平台淫秽直播的刑法定性[J]. 西部学刊, 2023(24): 58-61+79.