

# 网络犯罪的治理困境与应对举措

袁 婷

南京邮电大学马克思主义学院, 江苏 南京

收稿日期: 2024年3月20日; 录用日期: 2024年4月12日; 发布日期: 2024年5月24日

## 摘 要

作为一种新型犯罪形式, 网络犯罪对国家安全和社会治理造成了巨大威胁。当前, 网络犯罪治理主要面对三个方面的“实然”困境: 人民群众防范意识薄弱, 网络犯罪立法存在缺陷, 科技发展现状难以满足治理要求。在积极借鉴境外网络犯罪规制经验的基础上, 采取应对措施, 可以从法律、技术和道德三个维度破解这一难题。

## 关键词

网络犯罪, 困境, 举措

# Governance Dilemmas and Countermeasures to Cybercrime

Ting Yuan

School of Marxism, Nanjing University of Posts and Telecommunications, Nanjing Jiangsu

Received: Mar. 20<sup>th</sup>, 2024; accepted: Apr. 12<sup>th</sup>, 2024; published: May 24<sup>th</sup>, 2024

## Abstract

As a new form of crime, cybercrime poses a great threat to national security and social governance. At present, the governance of cybercrime is faced with three main “real” dilemmas: the people’s weak sense of prevention, deficiencies in cybercrime legislation, and the current state of scientific and technological development, which makes it difficult to meet the requirements of governance. On the basis of actively learning from overseas experience in cybercrime regulation, countermeasures can be taken to solve this dilemma from the three dimensions of law, technology and morality.

## Keywords

### Cybercrime, Dilemma, Countermeasures

Copyright © 2024 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

## 1. 引言

2023年8月28日,中国互联网络信息中心(CNNIC)发布的第52次《中国互联网络发展状况统计报告》显示,截至2023年6月,我国网民规模达10.79亿人,较2022年12月增长1109万人;互联网普及率达76.4%,较2022年12月提升0.8个百分点[1]。网络化信息化是当今世界发展的趋势,计算机网络尤其是互联网已经成为社会生活中必不可少的重要部分,并渗透在政治、经济、文化等社会生活的各个方面。置身于互联网时代,随着网络信息技术的日臻成熟,我们在充分认识到网络的快捷、便利、无时空障碍等优点的同时,也不得不面对其对国家和社会治理带来的巨大挑战。网络犯罪便是典型现象。马克思、恩格斯曾指出:“蔑视社会秩序的最明显极端的表现就是犯罪”[2]。因此,如何在归纳清楚网络犯罪基本类型的基础上,正视我国网络犯罪治理困境,并采取积极措施进行应对,维护社会秩序,亟需深思和探讨。

## 2. 网络犯罪类型

自1986年第一起网络犯罪案件发生后,我国的网络犯罪案件逐年飙升。截至2023年6月,全国各级网络举报部门共受理举报9652.1万件,较2022年同期上升12.2% [1]。我国网络犯罪的严峻形势可见一斑。网络犯罪作为现实犯罪的一面镜子,既有现实犯罪的普遍性特征,又有其特殊性。具体来说,网络犯罪可以分为以下四种主要类型:

### 2.1. 侵犯知识产权

知识产权是人的智力劳动的结晶,是人通过智力劳动获得的成果。网络信息技术的发展使传统的知识产权制度遭到了前所未有的挑战。在开放流动的互联网世界,人们自由地分享、使用、创造着信息,但这并不是百利而无一害,其潜在的对知识产权的威胁会随着网络技术的不断发展而浮出水面。知识产权主要包括商标权、著作权、专利权、域名权等,在网络世界中,商标权和著作权最容易受到侵犯。在商标权方面,主要包括非法使用商标,即未经商标权人授权,在网络上使用他人的商标,以及在商品或服务上使用与他人商标相同或近似的标志,造成混淆视听的表象,从而从中牟利。还包括侵权链接,也就是说利用他人的商标在网络上进行搜索,从而引导消费者访问与该商标无关的网站并从中获利。此外还包括恶意注册,别有用心者未经商标权人授权,恶意将他人的商标注册为域名,或者注册含有他人商标的关键词,以此为根据进行牟利活动。网络犯罪对著作权的侵犯更是屡见不鲜。比如非法复制和传播,这种行为主要指未经著作权人同意,将他人的作品复制、上传、下载或通过网络传播的行为。还有侵权衍生,一些人恶意对他人的著作进行修改、改编、翻译、制作衍生作品等,未经著作权人同意而据为己有。还有版权盗版:以盈利为目的,未经著作权人同意,复制、发行他人的著作。以上种种行为均对知识产权者造成了严重的困扰。

## 2.2. 网络色情

网络色情犯罪是指利用网络平台传播、出售或制作色情内容，或者从事其他与色情内容有关的违法犯罪活动。因此，利用网络平台宣传、招揽、引诱他人卖淫或介绍他人卖淫的行为和利用网络视频等形式进行色情表演的行为也都属于网络色情内容。网络色情之所以能够如此有恃无恐猖狂发展，主要在于相比于传统色情行业，它具有得天独厚的优势。具体体现在：第一，隐秘性极强，难以查出。网络色情犯罪往往以匿名或虚假身份进行，加剧了其暗藏性。而且网络色情犯罪者往往会使用 VPN、加密软件等技术手段，以隐藏自己的 IP 地址和真实身份。这就给警方对其身份的认定造成困难。再者，色情证据难以保存。因为网络色情犯罪往往以计算机数据的形式存在，证据保存和收集相对比较困难。第二，传播形式和传播渠道多样化。色情网站是网络色情犯罪的主要传播渠道之一，通过访问色情网站，人们可以观看、下载色情内容。而且，社交媒体平台上有大量的色情群组 and 账号，网络色情犯罪者通过发布色情图片、视频、链接等信息，吸引人们前往色情网站或下载色情内容。此外，点对点软件可以在不通过服务器的情况下，直接在用户之间进行文件的传输，这类软件被越来越多的用于网络色情犯罪。

## 2.3. 电信网络诈骗

自 2000 年起，电信网络诈骗从东南沿海向内陆地区不断蔓延，成为主要的网络犯罪类型，受害者的范围不计男女老少。据报道，2023 年，公安机关破获电信诈骗案件 43.7 万件[3]。电信网络诈骗是指诈骗分子利用电信网络，通过各种电子通讯工具，如电子邮件、网站、聊天室，实施网络刷单诈骗、冒充公检法诈骗等诈骗行为。电信网络诈骗的特点主要有以下几个方面：高智能性。诈骗分子可以利用各种网络技术，在不同的网络平台上进行诈骗。且诈骗分子普遍具有极强的组织性，分工明确，采取智能设备进行诈骗活动；高隐蔽性。诈骗分子可以在网络上匿名或伪装身份，让被害人难以识别。一些诈骗分子利用高科技设备伪装成受害者的亲人家属，使其防不胜防；高涉及性。电信网络诈骗涉及的金额巨大，且被害人的范围十分广泛，不仅限于个人，还包括企业和政府等。且在选择受害者时，具有极强的随机性，具有“广撒网”的特点；高危害性。电信网络诈骗不仅仅是经济损失，还可能造成个人信息泄露，身份盗用等严重后果。更有甚者，还会发生受害者经受不住打击而选择自杀的事件，严重危害社会治安。

## 2.4. 网络赌博犯罪

犯罪学领域的先驱之一埃德温 H. 萨瑟兰在分析和预测才智和现代技术工具的结合产生犯罪的可能性之后，早在数十年前就提醒人们，要把视野从传统犯罪转向现代犯罪[4]。果不其然，随着科技的飞速发展和互联网的普及，越来越多的犯罪行为开始转向网络空间。网络赌博就是一个典型的特征。虚拟飘渺的互联网世界让每一个沉迷其中的网络赌徒享受到现实世界难以提供的自由和乐趣，无法自拔地投身网络赌场。网络赌场在人为操控下，往往能够抓住赌徒们的特殊心理，设置好一步步陷阱，“守株待兔”。一般来说，在赌徒刚进入网络赌场中后，为了使其卸下防备心理，挑起赌徒的好奇和上瘾心理，往往会在前几局中使赌徒赢利，然后在赌徒没有意识到的情况下诱使其不断加大砝码，越玩越大，最后陷入无法收场的境地。区别于传统的赌博形式，网络赌博既不需要固定的赌博场所、管理人员，也不需要特点的赌博工具，只需要简单的网络技术设备就可以针对不同的赌博群体的需要对其投送合适的赌博游戏即可。且在用户注册上的门槛极低，仅需要信用卡即可。但与付出相比，网络赌博这一黑色产业链的受益是巨大的，这就使非法犯罪分子即使冒着坐牢的风险也要运营下去。

## 3. 网络犯罪治理困境

“每一种技术或科学的馈赠都有其黑暗面”[5]。计算机网络作为一把双刃剑，在造福人民的同时也

对国家安全和社会治理造成威胁。当前，我国网络犯罪治理面临着严峻的现实困境。

### 3.1. 人民群众防范意识薄弱

网络犯罪治理面临的现实困境中，人民群众防范意识较差是一个重要的方面。这是因为许多人对网络犯罪的危害还缺乏足够的认识，没有建立起强大的安全防范意识。主要表现在以下几个方面：第一，不注重网络安全。许多人在使用网络过程中，往往忽视网络安全的重要性，不注重密码的保护和网络交易的安全性，让网络犯罪得以借机。第二，缺乏防范知识。许多人对网络犯罪的防范知识了解不够，不清楚如何防止网络诈骗、网络非法入侵等犯罪行为的发生。第三，不注重举报。许多人在遇到网络犯罪时，不愿意举报或者不知道如何举报，这给网络犯罪治理带来了一些障碍。

### 3.2. 网络犯罪立法存在缺陷

现实社会中的人的行为总是要受到法律规范的约束。但在网络世界中，现实社会中的行为规范便失去了原有的效力，一些觉悟较差的人们便不再自觉地遵守责任与义务。在崇尚自由的网络空间中，相关法律法规的制定并非一件简单的事情。而现有的法律法规又往往难以支撑网络犯罪案件的审理。从而造成立法与实际脱节。这是由网络犯罪的特殊性所决定的。这就使网络犯罪看到了可以钻的漏洞。网络犯罪立法存在缺陷还体现在立法滞后这一点上。网络技术发展迅速，网络犯罪手段和方式越来越多样，但现有的法律法规往往跟不上这种发展，无法有效地应对新型犯罪。此外，由于网络跨国界的特点，各国的网络犯罪立法存在差异，缺乏统一的法律法规。这就使得一些重大国际网络犯罪案件的追捕和审查受到层层桎梏，运行不畅。

### 3.3. 科技发展现状难以满足治理要求

当前，科技的发展现状还难以满足网络犯罪治理的需求。技术手段是应对网络犯罪的必备基础要素，但是目前存在着许多不足，需要解决。主要表现在以下几个方面。资金不足：购置先进的网络技术侦查装备需要大量的资金，而一般的公安机关资金有限，无法满足购置的需要。装备更新换代快：网络技术发展迅速，购置的装备很快就会被淘汰，从而让网络犯罪侦查和网络信息侦控装备一直落后于网络技术的发展。装备使用范围有限：由于这些专门的技术装备的发挥作用范围有限，无法满足公安机关侦查网络犯罪者的需要。此外，囿于互联网的无时空限制性，各国缺乏统一的互联网技术标准这一现实也会给网络犯罪治理造成阻碍。

## 4. 域外网络犯罪治理经验借鉴

网络犯罪是伴随着互联网的产生和发展而诞生的。西方国家互联网发展早、技术水平高，相应的网络犯罪问题也更加突出。习总书记曾指出：“世界范围内侵害个人隐私、侵犯知识产权、网络犯罪等时有发生，网络监听、网络攻击、网络恐怖主义活动等成为全球公害” [6]。积极借鉴域外网络犯罪治理经验，有助于为解决中国网络犯罪治理问题提供启示。

### 4.1. 制定严格的法律法规，建立专门管理机构

世界各国在应对网络犯罪方面的法律法规各具特点，但总体上趋向于强化法律法规，加强打击网络犯罪。美国已通过包括《计算机欺诈和虐待防止法案》、《电子通讯隐私法案》和《数字暂存法案》等的多项法律法规。欧盟出台了《数据保护指令》、《网络中立性法规》等法规。日本制定了《不正当访问禁止法》、《计算机网络监视法》等法规。此外，各个国家普遍建立专门的执法机构处理网络犯罪问题：如美国网络犯罪调查局、英国国家网络犯罪调查局、德国联邦网络犯罪调查局、日本警察厅网络犯



罪监察中心、新加坡警方网络犯罪分析中心。

## 4.2. 加强公众教育, 提高公众预防网络犯罪意识

世界各国逐渐意识到网络犯罪的严重性, 纷纷采取措施加强公众教育和预防工作。美国政府通过多种渠道(如网站、社交媒体和社区活动)向公众提供安全知识和资源, 举办各种网络安全意识月活动。英国政府建立了“国家网络安全中心”(National Cyber Security Centre), 提供专业指导和资源, 增强公众和企业的网络安全意识。德国政府启动了“安全在线”(Sicher online)计划, 旨在加强公众和企业的网络安全知识和技能。日本政府建立了“网络空间基本法”(Basic Act on Cybersecurity), 强调网络安全的重要性, 并推进网络犯罪预防教育。通过教育和预防措施, 这些国家努力提高公众的网络安全意识, 从而减少网络犯罪的发生率和危害。

## 5. 网络犯罪治理举措

从目前网络技术的发展速度和全球范围内网络犯罪发展的表现形态与特征可以预测, 今后网络犯罪的内涵和外延都会呈现出持续扩大的趋势[7]。但事实上, 科学技术是一个中性的东西, 它所带给人类的影响完全取决于人类自身的选择和导向。因此, 为了最大化发挥网络技术的优势, 促进社会经济、政治、文化等方面的发展, 必须采取有力措施, 坚决有效治理网络犯罪, 维护网络空间风清气正的良好氛围。具体措施可以从以下三个方面展开:

### 5.1. 法律维度

不管是在现实世界, 还是在网络世界, 法律都发挥着调节器的作用, 对于维护秩序具有重大意义。因此, 推动网络犯罪治理, 必须把法律工作摆在核心地位。一方面, 要完善网络犯罪立法。及时修订和完善网络犯罪的立法, 使之能够跟上网络技术的发展, 填补现有法律的漏洞, 从而为打击网络犯罪提供法律基础。在完善立法期间, 考虑到网络犯罪具有跨国界的特点, 因此应该有意识地展开加强国际合作, 共同研究和制定网络犯罪的立法, 以便能够更好地应对网络犯罪。在立法的同时, 还需要加强对法律的执行, 打击网络犯罪的同时, 保护网络的安全和稳定。加强网络空间的管理: 通过立法的方式, 对网络空间进行管理, 包括对网络服务提供商、网站进行监管, 以及对网络用户的行为进行约束, 从而降低网络犯罪的发生。

具体到普法对象, 应加强网络安全教育, 提高公众的法律意识。我国《公民道德建设实施纲要》指出“要引导网络机构和广大网民增强网络道德意识, 共同建设网络文明。”因此, 要通过各种途径, 采取人民群众喜闻乐见的宣传形式, 提高公众的法律意识, 让公众知道网络犯罪的危害, 认识到个人信息的重要性, 增强自我防范意识。

### 5.2. 技术维度

技术进步所带来的挑战最终必须由技术本身来解决[8]。也就是说, 网络空间的本质是一个技术世界。想要解决由于技术的进步引发的社会问题, 必须反过来求助于技术本身。对于技术的发展, 主要有“防”、“改”、“监”、“研”四个关键词组成。

首先, 应大力开发防御软件, 以防止网络攻击和病毒感染, 提高网络安全的水平。许多网络犯罪事件的源头都是网络病毒的侵入。为了筑起安全的高墙, 必须注重防御软件的开发, 发展防病毒技术、防火墙技术。其次, 应改进安全技术。安全系数的高低往往直接影响网络的正常使用。通过不断完善加密技术、安全认证技术、漏洞检测技术等, 防止网络信息被盗用和篡改。然后, 应建立监控系统。只有建立完善的网络监控系统, 对网络信息进行实时监控, 才有助于及时发现和解决网络安全问题。最后, 研

发安全设备。唯有抢占技术的制高点，研发如网络安全设备、反病毒设备等，以提高网络的安全性和稳定性，才有可能在同网络犯罪分子的博弈中取得上风。

### 5.3. 道德维度

网络犯罪归根到底还是人的问题。作为新型犯罪形式的网络犯罪同传统犯罪相比，显然存在一定的技术门槛。而拥有先进技术的人如果存在道德上的缺陷，则必然受价值观影响而误入歧途，成为危害社会的犯罪分子。囿于网络犯罪巨大的利益诱惑，法律和技术双管齐下也往往难以彻底根除网络犯罪。想要解决网络犯罪，道德防范十分重要。尽管网络世界具有很多法律和技术无法触碰到的空白，但如果网络用户能够建立建好的网络价值观念，形成坚实的网络伦理道德，就会促使人们在无人监督的网络空间中自觉地遵守秩序。因此，最好的犯罪预防方式还是帮助网络用户培养网络伦理道德情操，接受中华优秀传统文化滋养，加强社会主义精神文明建设。

因地制宜弘扬网络道德势在必行。作为一种新的道德形态，网络道德与现实道德既有区别又相互联系。现实社会道德规范是网络道德的根据和基础，网络道德是社会道德的延伸和扩展，也就是说网络道德是在现实道德的基础上针对网络空间的特殊性而设定的。网络道德不仅是一种价值观念，还应当是行为准则。具体来说，以公正正直、尊重他人、守法自律、爱护网络为核心。

## 6. 结语

网络犯罪治理面临着一系列的现实困境，道阻且长。但笔者相信，随着科学技术的不断发展、法律规范的不完善、网民道德素质的不断提高，网络犯罪治理的困境将被科学系统的应对措施所打破，实现网络世界向着科学文明的方向有效发展的光明前景。

## 参考文献

- [1] 中国互联网络信息中心. 第 52 次中国互联网络发展状况统计报告[EB/OL]. <https://cnnic.cn/n4/2023/0828/c199-10830.html>, 2023-08-28.
- [2] 马克思恩格斯全集(第二卷) [M]. 北京: 人民出版社, 1965: 46.
- [3] 公安部: 2023 年共破获电信网络诈骗案件 43.7 万起[EB/OL]. <https://baijiahao.baidu.com/s?id=1787588990522314174&wfr=spider&for=pc>, 2024-01-09.
- [4] 奥古斯特·比库尔. 利用计算机犯罪[J]. 法学译丛, 1985(1): 42.
- [5] N·尼葛洛庞帝. 数字化生存[M]. 海口: 海南出版社, 1996: 26.
- [6] 习近平在第二届世界互联网大会开幕式上的讲话(全文) [EB/OL]. [https://www.gov.cn/xinwen/2015-12/16/content\\_5024712.htm?eqid=950c902f0003daf100000003646f7fe8](https://www.gov.cn/xinwen/2015-12/16/content_5024712.htm?eqid=950c902f0003daf100000003646f7fe8), 2015-12-16.
- [7] Vertes-Olteanu, A. (2014) Evolution of the Criminal Legal Frameworks for Preventing and Combating Cybercrime. *Journal of Eastern-European Criminal Law*, **1**, 84-96.
- [8] Clark, C. (1996) The Answer to the Machine Is in the Machine. *The Future of Copyright in a Digital Environment*, **10**, 139-146.