论帮助信息网络犯罪活动罪的法律适用

◆邱玉宇

(江西开放大学，江西 南昌 330046)

【摘要】信息网络犯罪活动日益成为全球性问题，对国家、个人、组织都造成了很大的威胁。然而，信息网络犯罪的形式变化多样，往往涉及多个参与者，除了直接执行网络犯罪的主要犯罪分子外，协助信息网络犯罪的行为者也扮演着关键的角色。基于此，本文阐述了帮助信息网络犯罪的定义、类型以及其法律适用，分析了当前帮助信息网络犯罪活动罪司法实践中的挑战，并提出了相应预防措施，以打击信息网络犯罪活动，保护网络安全。

【关键词】帮助信息网络犯罪；法律适用；挑战；措施

随着信息技术的快速发展，信息网络已经融入人们生活的各个领域。然而，随之而来的是信息网络犯罪活动的激增，如网络诈骗、数据泄露、恶意软件传播等。这些犯罪活动不仅威胁到个人和组织的隐私和财产安全，还可能对国家安全产生重大影响。因此，打击信息网络犯罪活动已成为国际社会的共同目标。

一、帮助信息网络犯罪的定义和类型

在法律上，帮助信息网络犯罪的行为通常被称为“协助和教唆信息网络犯罪”。这包括为犯罪分子提供技术支持、帮助策划犯罪活动、传播恶意软件或帮助隐瞒犯罪证据等行为。

(一)提供黑客工具

帮助信息网络犯罪的行为类型之一是为潜在的黑客提供工具、软件或技术，使他们能够攻击计算机系统、网络或个人设备，例如漏洞利用程序(窃取敏感信息、破坏系统或进行其他犯罪活动)、密码破解工具(入侵电子邮件、社交媒体或银行账户等)、端口扫描软件(发现易受攻击的系统)。这种行为是信息网络犯罪生态系统中的关键组成部分，它为那些不具备技术能力的犯罪分子提供了便捷的途径来实施犯罪活动。这些工具的提供者通常是技术精通的个人或团体，他们以赚取金钱或满足犯罪动机为目的，增加了信息网络犯罪的威胁，为潜在的攻击者提供了便利和资源。因此，法律体系通常将协助提供这些工具的行为列为犯罪，并追究相关人员的刑事责任。

(二)协助网络诈骗

帮助策划和执行网络诈骗行为也是常见的协助信息网络犯罪类型，这也是当下我国严厉打击的犯罪行为之一，如虚假投资、假冒网站、钓鱼攻击等欺诈活动。这些活动旨在欺骗受害者，获取他们的财产或敏感信息，而帮助信息网络犯罪的行为者在这些活动中发挥了关键作用。行为者可能提供虚假的投资机会、赚钱方案或商品信息，吸引受害者投资或购买。或者，行为者帮助创建看似合法的虚假网站、模仿知名品牌或公司，以欺骗受害者提供个人信息或支付款项。另外，行为者可能协助发起钓鱼攻击，通过虚假电子邮件、网站或消息，诱使受害者揭示密码、银行信息或其他敏感数据，这些协助行为使网络诈骗活动变得更加复杂和隐秘。

(三)协助恶意软件传播

帮助分发恶意软件也是常见的信息网络犯罪危险行为，如协助传播勒索软件、间谍软件、广告软件等恶意程序。这些恶意软件可能对受害者的计算机系统、个人数据和隐私造成严重损害。这种协助行为对网络安全构成严重威胁，因为它有助于传播恶意软件，导致大规模的网络感染和数据泄漏。

(四)盗窃和泄露数据

协助窃取敏感数据或泄露数据也是常见的信息网络犯罪类型。这种行为可能导致严重的隐私侵犯和数据泄露，给受害者带来巨大的损失。协助窃取敏感数据或泄露数据的行为者可能采用多种手段，如提供访问数据库的方法、窃取身份信息、在黑市上出售数据。这种类型的协助行为对个人和组织的数据安全构成了严重威胁，可能导致金融损失和个人信息泄漏。

二、帮助信息网络犯罪活动罪的法律适用

(一)共谋犯罪

帮助信息网络犯罪活动可能构成共谋犯罪，即与主要犯罪分子合谋策划和实施犯罪行为。共谋者可能会被追究刑事责任，与主要犯罪分子一同受审判。

例如，一名计算机安全专家 A 与一名黑客 B 合谋进行一次大规模网络攻击，旨在入侵银行的计算机系统，窃取客户的敏感金融信息。A 拥有计算机安全知识和技能，她协助 B 规划攻击策略、寻找潜在漏洞，并提供了一种专门工具，可以绕过银行的安全防护系统。在攻击进行期间，A

继续为B提供技术支持，帮助他在攻击过程中解决技术难题，最后成功入侵了银行的系统，窃取了大量客户信息，造成了严重的数据泄漏和财务损失。在此案例中，A的行为构成了共谋犯罪，尽管她没有亲自执行入侵，但她协助策划、提供技术支持以及提供攻击工具，是与B合谋实施了犯罪行为。因此，A会受到法律制裁，包括刑事起诉和审判，并依法追究她的刑事责任。

（二）计算机犯罪法律

如今，许多国家都已颁布了计算机犯罪法律，明确规定了各种与信息网络犯罪相关的罪行，旨在维护网络安全、打击犯罪活动以及保护个人和机构的信息资产。这些法律对于协助信息网络犯罪的行为者提供了明确的法律框架，如果涉及非法活动，协助者将受到法律追究。例如，非法访问计算机系统的行为，未经授权侵入计算机系统、窃取登录凭据、入侵网络资源、篡改数据等行为，未经授权窃取、复制或传播数据的行为，窃取敏感信息、财务数据或个人身份信息的行为等。计算机犯罪法律也涵盖了各种网络攻击，包括分布式拒绝服务攻击（DDoS）、恶意软件攻击、端口扫描等。以上任何一种行为，如有协助者，不论其实施方式如何，也将受到法律追究，都可能会面临刑事起诉、刑罚和法律制裁。该法律有助于打击信息网络犯罪，维护网络安全和法律秩序。

（三）数据保护和隐私法律

如果协助信息网络犯罪导致个人数据的泄露或侵犯个人隐私，可能涉及国家数据保护和隐私法律的规定，来确保个人数据的安全和隐私权的保护，这些规定对于非法获取、使用或泄露个人数据的行为提供了明确的法律框架。协助者如果牵涉到窃取、泄漏或滥用他人的个人数据，可能会受到数据保护法制裁。因为许多国家明确规定了个人数据的收集、处理和存储方式，以及对数据泄漏的处罚，如果参与非法数据获取或泄漏行为，可能会受到这些法律的约束，并面临刑事起诉和罚款。隐私法律旨在保护个人通信隐私和在线隐私，如果监视通信或非法访问私人通信，会违反这些法律，面临法律责任。此外，一些国家还制定了专门的信息泄漏法律，规定了如何处理数据泄露事件，如果协助者涉及个人数据的泄露，可能需要按照这些法律要求进行通报和处理，否则将受到法律追究。

（四）合谋和犯罪团伙法律

一些国家的法律体系明确规定了合谋和犯罪团伙的罪行，这也适用于协助信息网络犯罪的行为者。合谋通常指与主要犯罪分子共谋策划和实施犯罪行为，如果协助者被认定为合谋犯，将面临相应的刑事处罚和罚款。犯罪团伙是一组人共同参与犯罪活动的组织，如果被认定为参与了犯罪团伙，其法律责任可能更加严重。一些国家制定了特殊法律规定，以应对犯罪团伙的组织和活动，对涉及团伙犯罪的人员进行刑事追究。如美国的《有组织犯罪控制法》（RICO法案），旨在打击有组织犯罪团伙，其中包括勒索、贩毒、洗钱、非法赌博等一系列罪行。该法案不仅仅追究个别犯罪行为，还着重打击犯罪团伙的组织和活动，其中洗钱为试图掩盖犯罪所得，通常被视为严重犯罪，会受到刑事起诉。

三、帮助信息网络犯罪活动罪司法实践中的挑战

（一）技术难题

许多协助信息网络犯罪的行为发生在虚拟环境中，这增加了打击犯罪的难度。这些行为可能涉及高度技术化的手法，使用加密工具和匿名网络，使得追踪和识别犯罪行为的参与者变得复杂且困难。为了有效打击这些罪行，需要不断提升执法机构的技术能力，加强网络安全监测，以及改进国际合作机制，以更好地追踪和揭示协助信息网络犯罪的行为者，确保他们受到法律制裁。

（二）国际性质

信息网络犯罪的特点之一是跨国性质，犯罪分子可能位于不同的国家，而犯罪行为又常常涉及多个司法管辖区。因此，国际合作和信息共享变得至关重要。各国法律执法机构如国际刑警组织需要积极合作，分享情报和证据，以便追踪和打击跨国犯罪网络，打击信息网络犯罪，更有效地应对跨国信息网络犯罪带来的挑战。

（三）证据保全

与传统纸质证据不同，电子证据因为存在于数字媒体中，可以在不留下明显痕迹的情况下被修改，所以面临受到篡改和破坏的威胁。例如，电子邮件是常见的电子证据形式之一，恶意行为者可以轻松地伪造电子邮件，修改邮件内容或伪造发件人的身份；照片和视频也可以通过各种工具进行编辑和篡改，以伪造事件的发生或者误导观众。有效保全和使用电子证据对于打击信息网络犯罪和维护法治至关重要，因此需要采取一系列措施确保电子证据的完整性和真实性。

四、有效制止协助信息网络犯罪的措施

（一）强化执法和司法合作

信息网络犯罪常常具有跨国性质，犯罪行为可能从一个国家发起，但危害可以跨越多个国家。因此，国际合作和引渡协议在打击这类犯罪活动中至关重要。国际法律适用和合作可以帮助将协助信息网络犯罪的行为者引渡至涉案国家受审判，推动国际社会共同打击信息网络犯罪。例如，信息网络犯罪可能在一个国家进行攻击，而在另一个国家隐藏，国际合作可以协助追捕这些犯罪分子，将其绳之以法。另外，由于关键证据可能存储在不同国家的服务器上，通过国际合作，可以促成涉案国家之间的数据共享和取证协助，以确保证据的合法获取。国际机构如国际刑警组织和联合

国犯罪和司法研究所也为各案提供了国际合作和打击信息网络犯罪的平台和资源，共同应对这一威胁，确保网络安全和法律秩序。例如，国际刑警组织协助各国执法机构打击国际范围内的网络诈骗活动，他们提供了一个平台使不同国家的警察部门能够共享有关网络诈骗团伙的信息，协调行动，追踪并逮捕犯罪分子。通过这种方式已经成功打击了一些跨国网络诈骗犯罪团伙。

此外，建立有效的引渡协议和法律机制也是必要的。这些协议和法律机制允许国家之间引渡涉嫌犯罪的个体，确保犯罪分子无法逃避法律责任。同时，国际社区还应加强合作，共同制定和实施国际法规，以适应不断发展的信息网络犯罪形式，更有效地维护网络安全和法治。

（二）加强网络监督

有关部门和网络服务提供商在确保网络空间的合法和安全方面发挥着关键作用。首先，有关部门应当采取措施打击虚假信息和谣言的传播，如制定法律法规、设立举报渠道、与社交媒体平台合作等，以保护大众免受错误和误导性信息的影响。其次，通过执法行动、教育宣传和提供举报机制，积极打击各种形式的网络诈骗，如虚假投资、钓鱼攻击和假冒网站等。再次，有关部门和网络服务提供商应采取措施加强网络安全监测，防范和打击恶意软件的传播，及时发现并隔离恶意软件，以及提供安全更新和工具来减少感染风险。如建立网络监测系统检测到恶意软件的活动，并及时采取隔离措施，防止其传播；当发现感染时，可以隔离受感染的计算机或设备，以阻止其与其他设备通信，从而减少传播风险；提供免费的反恶意软件工具，帮助用户检测和清除计算机中的恶意软件。例如，Windows Defender 是一款由微软提供的反恶意软件工具，用于检测和清除计算机中的病毒和恶意软件，以建立更安全、更可信赖的网络环境。

（三）进行技术创新和研发

科技领域的不断创新是防范信息网络犯罪的重要手段之一，可有效提高网络安全水平。例如，利用人工智能可以监测网络流量、识别异常活动，并自动响应潜在威胁，其中，机器学习算法可以分析网络流量、系统日志和文件以识别潜在的威胁行为。这些算法可以自动学习新的威胁模式，而无需手动更新规则。如果出现新型的勒索软件变种，即使没有先前的签名信息，机器学习也可以检测到其异常行为，提高检测准确性。另外，区块链技术在金融、医疗和供应链等领域都有广泛的应用，其提供了安全的数据存储和传输方式，可以用于保护敏感信息和防止数据篡改。在保护信息方面，可以使用多因素身份验证方法，如指纹识别、虹膜扫描和生物识别技术，增加访问控制的安全性，减少未经授权的访问，保障信息安全和隐私。

当下，随着物联网设备的普及，创新的安全技术可以帮助确保这些设备不受到黑客的入侵，其中，加密通信和远程漏洞管理是其中的关键技术。加密是保护物联网设备通信的关键，设备之间的通信可以使用强加密协议进行保护，以确保数据在传输过程中不被黑客窃取或篡改。例如，Z-Wave 和 Thread 等通信协议在物联网设备之间使用加密通信以确保数据的机密性。物联网设备可能会存在漏洞，黑客可以利用这些漏洞进行攻击，而远程漏洞管理技术可以帮助设备制造商及时识别并修复这些漏洞，确保设备的安全性。

这些创新和技术的应用可以帮助组织更好地应对信息网络犯罪的挑战。然而，创新也伴随着新的安全风险，因此需要不断改进和升级安全措施，以适应不断演变的威胁。相关部门、企业和个人都需要积极参与，共同努力建立更加安全的网络环境。

（四）加强国际合作

国际社会迫切需要共同应对信息网络犯罪这一全球性挑战。为了维护网络空间的安全和稳定，国际合作至关重要。首先，各国应加强国际法律合作，签署双边和多边法律协议，明确规定信息网络犯罪的罪行和惩罚。其次，引渡协议应得到加强，以确保犯罪嫌疑人无法通过国际边界逃避法律制裁。此外，国际组织如联合国、国际刑警组织等应加强协作，共享情报和实践经验，帮助各国打击信息网络犯罪。只有通过国际社会的共同努力，才能有效地应对信息网络犯罪，维护全球网络空间的安全和稳定。

五、结束语

综上所述，打击信息网络犯罪需要法律体系的支持，以确保那些帮助犯罪分子的人也会受到法律追究，进而对信息网络犯罪形成威慑。经济在发展，技术也在变化，打击信息网络犯罪始终面临挑战，需要增强跨国合作和不断更新法律法规来应对不断变化的网络犯罪形式。

参考文献：

[1]黎文华.帮助信息网络犯罪活动罪司法适用问题研究[D].桂林：广西师范大学，2023.

[2]戴建军，李星亿.刍议帮助信息网络犯罪活动罪的法律性质[J].天津法学，2022，38(04)：56-65.

[3]刘梦.帮助信息网络犯罪活动罪的限缩适用研究[D].南京：东南大学，2022.

[4]王凤.正犯视角下帮助信息网络犯罪活动罪的法律适用研究[J].辽宁公安司法管理干部学院学报，2021(02)：13-18.

[5]常玉凤.帮助信息网络犯罪活动罪的司法适用问题研究[D].南昌：华东交通大学，2021.

作者简介：

邱玉宇(1977－)，女，汉族，江西上饶人，本科，讲师，研究方向：法律。