Dispute Settlement 争议解决, 2026, 12(4), 137-144
Published Online April 2026 in Hans. https://www.hanspub.org/journal/ds
https://doi.org/10.12677/ds.2026.124110

Hans汉斯

“盒威胁”下个人数据法权益的保护及责任认定

王田露，秦　蓉

上海政法学院刑事司法学院，上海

收稿日期：2026年3月2日；录用日期：2026年3月26日；发布日期：2026年4月7日

摘　要

随着个人信息黑灰产与网络暴力相互勾连，“开盒”已由一般“人肉搜索”异化为以非法获取、整合加工、公开扩散公民个人信息为核心，并诱发侮辱、诽谤、线下骚扰等后果的链条化、产业化、跨平台乃至跨境违法犯罪形态。围绕“开盒”产业链的刑事责任认定，司法实践中仍面临行为类型交叉、罪名适用边界模糊、共同犯罪层级复杂、电子证据固定困难以及跨境溯源追责不畅等问题。本文以“开盒”产业链的刑事责任认定困境与破解为研究中心，在梳理上游非法获取、中游整合交易、下游扩散煽动等行为结构的基础上，提出通过细化构成要件判断规则、强化分层分类追责、完善电子证据规范并推动跨部门与跨境协同治理，提升对“开盒”行为的精准规制与个人信息法益保护水平。

关键词

网络开盒，个人信息保护，刑事责任认定，数据安全，网络治理

Protection of Legal Interests in Personal Data and Liability Attribution under “Doxxing Threats”

Tianlu Wang, Rong Qin

School of Criminal Justice, Shanghai University of Political Science and Law, Shanghai

Received: March 2, 2026; accepted: March 26, 2026; published: April 7, 2026

Abstract

With the convergence of the black market for personal information and cyber violence, “doxxing”

文章引用: 王田露, 秦蓉. “盒威胁”下个人数据法权益的保护及责任认定[J]. 争议解决, 2026, 12(4): 137-144.
DOI: 10.12677/ds.2026.124110

has evolved from ordinary “human flesh search” into a chain-based, industrialized, cross-platform, and even transnational form of unlawful and criminal conduct centered on the illegal acquisition, aggregation, processing, and public dissemination of citizens’ personal information, often triggering insults, defamation, and offline harassment. In judicial practice, the criminal liability of the doxxing supply chain still faces a number of difficulties, including the overlap of behavioral types, blurred boundaries in the application of criminal charges, the complexity of accomplice liability, difficulties in the preservation of electronic evidence, and obstacles to cross-border tracing and accountability. Focusing on the dilemmas and solutions in identifying criminal liability within the doxxing supply chain, this paper analyzes the behavioral structure of upstream illegal acquisition, midstream integration and trading, and downstream dissemination and incitement, and proposes to improve the precision of legal regulation and the protection of personal information rights and interests by refining the rules for determining constituent elements, strengthening tiered and categorized accountability, improving the rules on electronic evidence, and promoting interdepartmental and cross-border collaborative governance.

Keywords

Online Doxxing, Personal Information Protection, Determination of Criminal Liability, Data Security, Cyber Governance

1. 引言

随着互联网平台、即时通信工具与数据处理技术深度嵌入社会生活，个人信息的收集、聚合与再传播成本显著下降，“开盒”也由早期“人肉搜索”的异化形态，演变为集非法获取、整合加工、公开扩散与网络暴力于一体的复合型侵害行为。已有研究指出，“开盒”已形成“上游数据窃取–中游信息整合–下游扩散危害”的黑灰产业链，并呈现出链条化、产业化、跨平台、跨境化等特征；在司法实践中，其不仅侵害公民隐私权、个人信息权益和人格尊严，还可能诱发侮辱、诽谤、敲诈勒索乃至线下滋扰等多重后果。自 2023 年以来，监管整治、司法打击与案例发布持续加码，“开盒”已被纳入重点治理议题，2026 年“两高”工作报告又同时点名相关案件，表明其已成为网络空间治理和个人信息司法保护中的突出问题。

但总体而言，既有研究仍存在若干不足：首先，“开盒”与“人肉搜索”“网络暴力”“侵犯公民个人信息”等概念之间的边界尚未完全厘清，致使其法律定性在不同语境下仍显模糊；其次，现有讨论较多停留于风险描述、政策倡议或综合治理层面，对于“开盒”所侵害的个人数据法权益类型、权利层级，以及其与隐私权、个人信息权益、人格权之间的规范关系，尚缺乏更为细致的法教义学分析；再次，在责任认定方面，如何在民事、行政与刑事责任之间实现准确分层，如何界定平台、数据提供者、传播者与技术服务者等多元主体的注意义务与责任边界，尤其在跨境“社工库”、人工智能深度合成、电子证据固定困难等情形下，仍有待进一步研究。正因如此，本文拟从个人数据法保护与责任认定的双重视角出发，对“开盒”行为的概念界分、侵害法益、责任结构及治理路径展开系统分析，以期为相关司法适用和制度完善提供更具针对性的解释方案。

(一) 绪论

1) 研究背景

伴随互联网的快速发展，信息技术持续演进并不断向社会生活各领域深度渗透。当前我们处于互联

网发展的时代，互联网与我们的生活紧密联系。“网络开盒”“人肉搜索”现象的频发，对个人隐私和数据安全都造成了严重的威胁。近年来不断的泛滥升级，公民个人信息的侵犯已经严重影响到公民的正常生活，侵犯公民的人身财产安全。“网络开盒”也会引发相应的网络暴力的产生，目前对于新型违法犯罪手段的防护措施并没有全面的规定，通过对开盒行为的分析，来更好地面对生活中的隐私侵犯，从而做到真正的数据保护。但目前我国针对个人信息隐私权的保护仍旧不充分，关于相关的规定也甚少。实践中，网络用户如果想要寻求救济的途径很有限并且较为困难。“开盒”现象正是在这一背景下迅速扩张的一种新型网络侵权行为。其通常表现为行为人借助非法技术手段、社工库查询、平台漏洞利用、熟人信息拼接、黑灰产业购买等方式，获取他人的姓名、住址、联系方式、身份证号、社交账号、工作单位乃至家庭成员信息，并通过社交媒体、群组传播、评论区扩散等方式进行公开披露，从而引导舆论围攻、现实骚扰与人格羞辱。与传统“人肉搜索”相比，“开盒”行为的组织化程度更高、技术门槛更低、传播链条更完整、现实危害更显著，其已经不再是单纯的网络失范现象，而是具有明确法益侵害性质和秩序破坏效应的复合型违法行为。

2) 研究意义

a) 理论意义

对于公民的信息隐私权的保护是对人权的尊重，是法律事业发展进步的重要体现，也有利于我国网络发展更加安全化。开盒行为常常涉及侵犯公民的个人信息，利用非法技术手段进行窃听窃照，由于开盒行为涉及罪名相对较广，并且较为融合和复杂，由开盒行为所引起的网络暴力是更为严重的人身侵害。目前我国法律对于网络空间隐私权的保护相对薄弱。开盒行为涉及不同部门的分工协作，通过对其研究有益于对于公民个人信息数据的保护，从而促进社会的稳定。我国法律应根据社会发展的现实情况完善和修改相关法律，以适应我国社会的发展变化。从法学角度探讨“开盒”“人肉搜索”行为的法律边界，为完善相关法律法规提供理论支持。

b) 现实意义

当今社会已经进入数字时代，每个人的信息数据都沉迷在网络当中。注重对公民隐私权的保护，一方面要重视对互联网公民用户个人隐私权的保护，又要注重对于互联网发展的促进。随着法律社会的发展和普及，人们对于信息数据的保护的维权意识越来越增强，只有不断完善法律，增强信息数据的保护，使公民感受到人格权利正在被切实的尊重，才会由心地产生安全感，增强生活的幸福感。从而使公民能够在清朗有序的网络环境中更高效地处理生活与工作事务。反之，若任由“开盒”等网络乱象蔓延，不仅会破坏网络空间秩序，还将对公众的正常生活、人格权益乃至人身安全造成更多现实困扰与损害。

(二)“盒威胁”的内涵与表现形式

1)“盒威胁”的内涵

“开盒”是一种网络用语，主要指通过非法手段获取并公开他人隐私信息的行为，通常还伴随着对被曝光者的网络暴力。“开盒”最初来源于网络贴吧、论坛等匿名平台，每个人的网络社交账号被视为一个“盲盒”，“开盒”就是打开这个盒子，揭露其中的隐私。“开盒”与“人肉搜索”其实是相伴而生，都是对公民信息隐私的侵犯，通过非法手段，窃取窃听窃照他人的隐私，通过网络进行快速传播，进而侵犯他人的人身财产的权利。“人肉”“开盒”一词多运用与网络热词，由于网络的快速传播，网友通过列举所常识的人物信，通过更多人的参与，搜寻出有效的资料和个人信息。而“盒威胁”是指在互联网中他人通过非法手段获取公民个人信息进行非法传播，从而对“开盒”者造成人身财产方面的威胁。公开隐私信息后，引导网民对被“开盒”者进行攻击、谩骂、造谣、诋毁等，甚至可能延伸到现实生活中的骚扰和威胁[1]。

2) “盒威胁”的表现形式和发展历程

由于大数据技术的广泛应用，数据收集也变的轻而易举。各种应用程序的使用导致公民的各项隐私已经被收集。相关的技术人员又通过非法手段获得海量数据，为“网络开盒”提供了丰富的信息源。“开盒”这一行为涉及到三个方面：数据的收集、整合与分析等环节。因此，只有拥有相关的技术人员才能获取他人信息数据。2025 年百度副总裁女儿对素人“开盒”事件并进行网络暴力，利用百度数据库非法获取信息，并进行网络传播。早期的“盒威胁”表现为未成年利用网络技术，进行跨地域式的攻击他人，并且形成了相关的“开盒技巧”进行大量传播，使得开盒行为迅速传播[2]。如今是数字化时代，“开盒行为”造成大量受害者，在网络空间中面临骚扰，例如：骚扰电话、社交软件上的谩骂和攻击等。随着数字时代的发展，目前社会已经形成了相关的黑色产业，其中最为出名的为“某工库”“爬虫”。其信息来源广泛，长期存在于黑市中的数据平台。因此应明确“开盒”行为的法律界定，加大对相关行为的惩处力度[3]。

2. “盒威胁”视角下行为的法律风险

“开盒”行为之所以值得法律重点关注，在于其并非单一的网络失德现象，而是同时触及民事侵权、行政违法乃至刑事犯罪的复合型行为。从行为结构看，“开盒”通常包含非法获取信息、整合识别信息、公开传播信息以及诱发进一步侵害后果等多个环节；从法益侵害看，其既侵害个人信息权益和隐私权，也可能侵害名誉权、人格尊严、人身安全乃至社会管理秩序。因此，对“开盒”行为的法律风险分析，应当从多重责任体系展开，而不能将其简单视为一般性的网络言论失范[4]。目前我国对于公民的个人信息、隐私权加大了保护力度。“开盒”行为所触及的不仅是公民的隐私权，由“开盒”行为所导致的网络暴力，从而衍生更加危害的后果。对于“开盒”行为所面临的法律风险是不同的，因为此行为不仅仅触犯民事责任，也会触及行政、严重的话更会触及刑事犯罪。因此“开盒”行为所造成的危害不容小觑。

“开盒”行为主要的法律风险有以下三种：其一、“开盒”行为违反我国民法典对于公民隐私权的保护，由于“开盒”行为是通过非法手段获取的公民的个人信息，进行肆意的传播，导致他人受到攻击，严重侵犯了公民的个人信息。其二、第二百五十三条之一：违反国家有关规定，向他人出售或者提供公民个人信息，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金[1]。目前，“开盒”行为已逐渐形成较为隐蔽的黑灰产业链，一些行为人通过地下黑市非法获取他人个人信息，并进一步实施售卖、传播等违法活动[5]。“开盒”行为已经触犯了我国刑法规定的犯罪。“开盒”行为也可能造成网络暴力等后果的发生，通过获取他人信息，在网络上进行传播，侮辱、诽谤他人，造成他人自杀的行为，依法应当承担相应的刑事责任。前文所讲述的百度副总裁的女儿，通过“开盒”行为，任意传播他人的信息，使其遭受他人恶意攻击和谩骂。如果行为人通过网络平台对被害人进行侮辱、诽谤，造成被害人自杀，且情节严重，可能构成侮辱罪或诽谤罪。例如，在德阳女医生遭受网暴自杀一案中，行为人通过网络平台发布侮辱性言论，导致被害人自杀，最终被认定为侮辱罪。并且也可触及其他犯罪，例如：寻衅滋事罪、敲诈勒索罪、诽谤罪等[2]。其三：对于“开盒”行为背后侮辱、恐吓、非法散布他人的个人信息等行为，尚未构成犯罪的，面临着治安处罚中的如罚款、拘留等处罚。因此“开盒”的违法性需要引起我们的重视[6]。

[1]《中华人民共和国刑法》第二百五十三条之一：“违反国家有关规定，向他人出售或者提供公民个人信息，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。”
[2]最高人民法院：《依法惩治网络暴力违法犯罪典型案例》案例二：常某一等侮辱案。

3. 针对“盒威胁”的数据保护的责任认定与建议

(一) 数据保护与个人隐私侵犯现状

我国已经初步建立比较完善的个人信息数据保护的法律框架，其中《网络安全法》《数据安全法》《个人信息保护法》构成了我国数据保护的核心法律体系，为保护个人隐私以及数据的安全保护提供了基本的遵循。《网络安全法》是我国于 2017 年颁布并实施，明确规定了网络运营者在大量的数据收集、存储、传输等负有安全保护的义务，法律要求运营管理者通过信息网络技术或者其他的必要措施，来保证网络数据的安全使用与运行 [3]。《数据安全法》主要是对数据处理活动的保障，将数据进行层层分级保护、评估，加强对数据的保护以及监测等，将数据安全上升到国家安全的高度。《个人信息保护法》主要针对于个人信息保护权益的保护，明确了公民对于个人信息中的权利，如知情权、决定权、查询权等。法律体系的初步建立并不意味着实践困境已经得到有效解决。面对“开盒”“人肉搜索”“社工库传播”等新型网络侵害形态，现行制度仍表现出一定的滞后性与适用局限 [4]。首先，从概念界定上看，“开盒”并非法定术语，其行为外延较广，既可能包括单纯的隐私披露，也可能包括信息非法获取、批量传播、侮辱诽谤、现实骚扰等多重行为[7]。这种复合性导致司法实践中在行为定性时容易出现标准不统一、责任评价不充分的问题。其次，从证据认定看，“开盒”行为往往依托匿名账号、境外平台、临时群组或跨平台传播链条完成，电子证据易灭失、责任主体难锁定、传播范围难统计，客观上增加了维权和追责难度。再次，从治理效果看，现行法律虽对个人信息保护作出较为原则性的规定，但对“开盒”这一典型场景的回应仍然较为间接，导致法律规范与实践需要之间存在一定落差[8]。

如今数字化时代的发展，现有法律对“开盒”“人肉搜索”等新型的网络侵权行为仍有不足之处。首先，由于“开盒”行为为新型犯罪，法律存在相关的漏洞，未对其进行规定具体的构成犯罪构成要件，因此在司法实践中难以准确界定该行为的违法性。其次，“开盒”行为往往又会涉及跨境数据流动，我国目前对此方面的监管还存在一些漏洞，对于境外的犯罪打击力度较小，难以进行有效的打击，所造成被害人的增多[9]。一些“开盒者”通过海外设备及账号隐匿身份，追踪难度大幅增加。根据我国现有法律的规定，对“人肉搜索”的行为惩处力度也相对较轻，难以对其违法行为形成一定的威慑力。例如，根据《刑法》第二百五十三条之一的规定，侵犯公民个人信息罪的立案有数量要求，导致很多“人肉搜索”案件难以达到刑事立案标准。最后，随着信息网络技术的发展，技术的不断提高以及应用场景的不断出现，现有法律存在一定的滞后性 [5]。

(二) 网络平台的责任与治理

据《网络安全法》第二十四条相关规定可知，网络运营商与用户签订协议或确认为用户提供线上服务时，应当要求用户提供真实身份信息 [6]。因此，在用户拒绝提供其个人真实身份信息情形下，网络运营者也不得为其提供相应的服务。“开盒”行为正日益成为一种新型的网络暴力，严重侵犯了个人隐私和数据安全，给社会的秩序和网络的生态环境带来了巨大威胁。随着科学技术的不断发展，人与人之间的交流日益频繁，各类网络平台和软件也随之迅速发展。网络平台作为信息传播的重要载体，在应对“开

[3]《中华人民共和国网络安全法》第四十条规定：“网络运营者应当对其收集的用户信息严格保密，并建立健全用户信息保护制度。”
[4]《中华人民共和国个人信息保护法》第四十四条规定：“个人对其个人信息的处理享有知情权、决定权，有权限制或者拒绝他人对其个人信息进行处理”；第四十五条规定，个人有权查阅、复制其个人信息；第四十六条规定，个人有权请求更正、补充个人信息；第四十七条规定，在法定情形下个人有权请求删除个人信息。
[5]《中华人民共和国刑法》第二百五十三条之一规定：“违反国家有关规定，向他人出售或者提供公民个人信息，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。”
[6]《中华人民共和国网络安全法》第二十六条规定：“网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通讯等服务，在与用户签订协议或者确认提供服务时，应当要求用户提供真实身份信息。用户不提供真实身份信息的，网络运营者不得为其提供相关服务。”

盒”行为过程中负有不可推卸的治理责任。我国《网络安全法》《个人信息保护法》等法律规范，均对网络服务提供者和管理者的信息内容管理义务及合法性审查责任作出了明确要求。对于平台内可能出现的违法行为或者违法信息，网络平台应当依法及时采取屏蔽、删除、拦截、断链等必要措施，以防止侵害后果的进一步扩大。对于其他公民用户所提出的举报投诉应当快速做出反应，以最大化的效率去保护公民的个人信息，消除侵犯公民个人信息的行为。本文将从以下几个方面讲述网络平台的责任与治理。

1) 网络平台的责任

网络平台作为人与人交往的纽带，在信息传播和用户管理中具有关键的作用。根据《网络安全法》《数据安全法》和《个人信息保护法》等法律法规，网络平台应当承担信息审核责任，面对用户发布的违法信息，应当及时地审核与撤销，防止信息进一步扩散。提高相关的技术，识别“开盒”行为。平台应当严加保护公民的个人信息数据，防止被非法传播[10]。平台应当建立实名制，对于“开盒”者应当进行作出封号等处理。应加强对未成年人的保护，“开盒”行为多为青少年为满足自己的好奇心，利用非法手段去窃取他人的信息，完善青少年模式，防止青少年接触和传播不良信息。

2) 网络平台的治理措施

网络服务的提供者应及时的更新相关的技术，对用户个人信息数据进行加密，确保数据的安全性。通过智能化进行监测系统，对于违规的行为进行精准识别。应完善审核机制，对于可能会造成公民个人信息的传播的应该重点审查，防止其传播。平台应加强对用户进行法制教育，“开盒”行为的违法性，增强其法律意识。

3) 网络平台应对措施

当前，“开盒”行为的技术手段的不断更新，如“社工库”“人肉搜索引擎”等工具的出现，使得相关管理部门的难以管控。平台需不断更新技术手段，提升对“开盒”行为的监测和识别能力。部分“开盒”行为存在跨境流动，平台需加强与国际组织和其他国家的司法合作，共同打击跨境“开盒”行为。“开盒”行为作为目前新型的网络违法行为，侵犯公民的个人信息和隐私权。网络平台的提供者应当承担相应的责任，有效地遏制“开盒”行为的发生。监管部门也应当加强为网络服务的提供者的监督，保障切实履行自身的责任。只有平台、监管部门以及用户的各方努力，才能抵制“开盒”行为的衍生[11]。

(三) 数据保护与个人隐私保护的完善建议

目前“开盒”行为已经形成了黑色产业链，遍布领域较广，其中涉及未成年人的违法行为，因此应加强相关法律的完善，填补缺失的漏洞，遏制和打击“开盒”行为的存在。“开盒”行为的遏制需要各部门机构进行联合打击，明确各方责任，有效地打击违法行为。

1) 以“全链条规制”为导向细化“开盒”行为的法律适用规则

当前“开盒”已不再是单一的信息泄露行为，而是呈现出“非法获取–整合加工–公开扩散–煽动网暴–引流牟利”的链条化、产业化特征，部分案件还伴随跨境数据来源、加密群组传播和线下骚扰等情形。基于此，相关法律完善不宜停留于原则性宣示，而应转向对具体行为模式的类型化规制。可考虑围绕《刑法》第二百五十三条之一及相关司法解释、规范性文件，明确将运营“社工库”、批量整合并出售敏感信息、明知系非法获取数据仍提供查询服务、公开披露他人住址和联系方式并诱导线下骚扰、利用人工智能合成侮辱性内容实施二次扩散等行为，纳入“情节严重”或者从重处罚的考量因素；对于同时触犯侵犯公民个人信息罪、非法利用信息网络罪、侮辱罪、诽谤罪等情形，还应进一步明确竞合处理规则，避免对严重“开盒”行为仅作轻微行政处理。与此同时，应结合信息敏感程度、传播范围、是否牟利、是否针对未成年人、是否造成现实侵害后果等因素，构建分层次的责任评价体系，并细化电子证据的固定、提取与认定标准，提升此类案件的可诉性与可罚性。

2) 完善跨境数据保护的法律创制

“开盒”行为往往涉及跨境数据流动，但我国对于此方面的问题还存在漏洞。例如外籍人员通过网络技术手段，将我国公民的个人信息进行“开盒”，导致我国公民的信息隐私权遭到侵犯，但由于相关技术完备，无法锁定具体的外籍人员，导致办案困难。应加强与他国的法律合作，打击有关非法行为，提高相关的技术手段进行侦查、拦截个人信息的泄露[12]。通过加强对先进的加密技术对跨境数据流动进行加密处理，以确保数据在流动传输或者储存过程中的安全性。积极参与国际对于数据保护规则的制定，与其他国家进行共同交流，签订双边或多边数据保护协议，实现跨境数据流动的互认机制。由于我国的跨境数据流动还存在一定的问题，应该参考欧盟 GDPR 等国际上对于数据保护先进的法规，引入对于数据保护的充分性认定，对企业的规则进行约束性等机制。此外，对于数据库中的敏感数据进行脱敏处理，在不影响数据流动的情况下降低隐私风险。最后，可以通过大数据、云计算等先进的技术手段，对大量的跨境数据进行实时的监控和检测，以便及时地发现问题和处理安全问题。通过完善跨境数据保护的法律创制，进一步保护数据流动的安全性[13]。

3) 压实平台的数据安全责任与内容治理责任

对“开盒”的治理不能仅依赖事后追责，更应将平台责任嵌入事前预防和事中阻断环节。一方面，平台应将 API 漏洞扫描、服务器安全加固、核心数据加密存储与隔离、入侵检测、强密码策略、多因子认证以及异常登录监测纳入常态化安全管理，从源头减少“拖库”“撞库”造成的大规模信息泄露[14]。另一方面，应建立针对“开盒”行为的专门识别与处置机制，围绕“姓名 + 身份证号 + 家庭住址 + 电话号码”等敏感信息组合、侮辱性煽动语句、证件图片等高风险内容进行实时监测和智能识别，对高危内容自动拦截或转入人工复核；同时结合账号登录 IP、设备指纹、社交关系图谱、群组规模、文件传输频率等行为数据，识别协同作恶账号和传播群组。对于涉及未成年人参与或者受害的事件，平台还应启动特别处理程序，及时采取限流、禁言、封号、线索上报等措施，防止“开盒”进一步演化为持续性网络暴力[15]。

4) 完善被害人救济机制与未成年人预防机制

在权利保护层面，应推动形成“刑事惩治–民事救济–公益保护–事前禁令”相衔接的综合救济体系。除依法追究行为人的刑事责任外，还应进一步完善个人信息侵权案件中的责任认定、损害赔偿和举证分配规则，充分发挥民事公益诉讼在个人信息保护中的制度功能；对于侵害仍在持续、受害人已面临现实危险的案件，人民法院可根据申请及时发出人格权侵害禁令，责令行为人立即停止传播、删除内容并中止侵害，实现由“事后追责”向“事前、事中止暴”延伸。与此同时，考虑到未成年人既可能成为“开盒”的主要受害者，也容易因认知不足、从众心理和圈层文化影响而成为实施者，教育部门应将网络伦理、数字公民责任、个人信息保护与反网络暴力教育系统纳入中小学课程，家庭和学校则应加强对未成年人网络行为的引导与监督，并配套设置专门举报入口、心理支持通道和受害援助机制，降低未成年人卷入“开盒”行为的风险[16]。

4. 结语

在当今社会的背景下，互联网侵权日益严重化，尊重互联网网络用户的隐私权侵权问题，对于侵犯公民个人信息保护的问题是大势所趋。目前我国对于“开盒”行为的法律界定不够完善，以及互联网隐私权的保护范围的规定也不够明确，导致司法实践中存在适用难、打击难等问题。对于“开盒”行为也多存在于未成年人当中，青少年由于好奇心而进行的“开盒”行为，导致公民的个人信息被侵犯，进而引起网络暴力的发生。本文基于“盒威胁”下数据保护与责任认定的研究得出了一些启示，第一，需要明确“开盒”行为的具体的犯罪构成，与其他犯罪具有明确的界定，因“开盒”行为是利用非法手段获

取他人的信息，并通过互联网进行大肆传播，为他人造成难以想象的后果，应当对“开盒”行为有相应的入罪出罪的规定；第二，加强对互联网隐私权的立法保护，从“人肉搜索”到“开盒”行为，都是对于公民个人信息隐私权的侵犯，应以民法为主，其他特别法保护为辅助的救济方式，对于无法构成刑事责任的案件，应具有相应的民事责任或者行政处罚；第三，应加强相关技术的完善，随着科技社会的不断发展，科学技术的落后，是无法精准实施打击犯罪的原因。为了能够有效地进行打击违法犯罪行为，应完善相关信息管理技术；第四，加强宣传“开盒”行为的违法性，“开盒”一词也是近几年流行起来的词语，大多数不明白“开盒”的含义，并且部门公民由于不明白、不清楚而进行了“开盒”行为，因此，应扩大宣传，“开盒”行为的违法性与弊端，减少相关违法行为的出现。最后，只有公民的个人信息隐私权得到重视，相关权利才能够真正得到保护。另一方面，我国经济发展离不开互联网的发展，绿色网络的发展有助于和谐社会的发展。因此，抵制“开盒”行为需要各方主体部门的共同努力，才能做到真正地保护公民的个人信息和隐私权不受侵犯。

参考文献

[1] 肖潇, 王峰. 最高检法律政策研究室主任杨剑波: 依法打击“网络开盒”等网络犯罪, 坚决摧毁利益链条[N]. 21世纪经济报道, 2026-03-06(005).

[2] 孙梓翔. 从“人肉搜索”到“网络开盒”: 侵犯公民个人信息犯罪的现状分析及治理路径研究[J]. 中国防伪报道, 2026(1): 72-79.

[3] 李光杰, 李小波. 网络“开盒”的多维风险及治理研究——基于行动者网络理论的透视[J/OL]. 北京警察学院学报: 1-19. https://doi.org/10.16478/j.cnki.jbjpc.20260203.001, 2026-03-09.

[4] 胡宁. 个人信息在境外软件“裸奔”检察公益诉讼追责网络“开盒” [N]. 中国青年报, 2026-02-05(007).

[5] 李想. 新型网暴“开盒”: 警惕“数字时代的游街” [N]. 中国青年报, 2025-10-27(004).

[6] 刘艳红. 数字时代“网络开盒”的系统性治理[J]. 人民论坛, 2025(19): 83-87.

[7] 霍旻含. 严惩“开盒”, 给隐私“上锁” [N]. 人民日报海外版, 2025-07-07(008).

[8] 本刊采编中心. 加强未成年人网络保护构建多元协同治理格局[J]. 中国信息安全, 2025(6): 12.

[9] 李沅恒. “开盒”乱象中的未成年人个人信息权益危机与协同治理[J]. 中国信息安全, 2025(6): 44-47.

[10] 高艳东, 李华勇. 斩断“开盒”黑产链条, 重塑清朗网络[N]. 环球时报, 2025-05-30(015).

[11] 陈曦, 秦亦姝, 张小简. “开盒”污染网络生态, 网暴之门该咋关闭? [N]. 工人日报, 2025-05-28(004).

[12] 朱婧薇. 网络开盒: 数字时代的安全困局[J]. 光明少年, 2025(5): 12-13.

[13] 李娜. 侵犯公民人格权, “开盒”已成网络新毒瘤[N]. 宁夏法治报, 2025-04-16(006).

[14] 林碧涓. “开盒”事件敲响警钟数据应用需上好“安全锁” [N]. 通信信息报, 2025-04-09(003).

[15] 银昕. “开盒”事件追踪: 揭开数据交易“灰链” [N]. 中国工业报, 2025-04-07(005).

[16] 孟文静. 大数据时代下公民隐私权法律保护研究[J]. 公关世界, 2025(7): 118-120.