Open Journal of Legal Science 法学, 2025, 13(4), 723-732
Published Online April 2025 in Hans. https://www.hanspub.org/journal/ojls
https://doi.org/10.12677/ojls.2025.134105

Hans汉斯

# 电子证据合法性与排除规则的优化路径

## ——基于数字权利视角

**程炜琪**

中山大学法学院，广东 广州

收稿日期：2025年3月7日；录用日期：2025年3月27日；发布日期：2025年4月29日

## 摘　要

**由于电子证据的无形性、易篡改性及其收集过程中的技术复杂性，现行的非法证据排除规则在适用电子数据时常常面临挑战，难以实现预期的法律效果。随着公民数字权利的日益发展，数字人权等理念逐渐兴起，电子数据不仅关系到有效追诉犯罪，也涉及被追诉人的人身、财产等重要权益。因此，如何在这一过程中平衡电子证据的合法性与真实性尤为重要。文章对我国现行电子证据合法性审查与排除规则进行制度分析，探讨相关规则在立法和司法实践中的不足，随后通过对比国外司法实践，提出将电子证据纳入非法证据排除规则，并从取证主体和取证程序两个角度提出完善电子证据审查标准的建议，以期为我国电子证据制度的法治化建设提供参考。**

## 关键词

**电子证据，合法性审查，非法证据排除规则，程序正义，数字权利**

# Optimization Path of Legality and Exclusion Rules for Electronic Evidence

## —From the Perspective of Digital Rights

**Weiqi Cheng**

School of Law, Sun Yat-sen University, Guangzhou Guangdong

Received: Mar. 7th, 2025; accepted: Mar. 27th, 2025; published: Apr. 29th, 2025

## Abstract

**The intangible nature, susceptibility to tampering, and technological dependence of electronic evidence have led to a lack of systematic standards for reviewing its legality in current legislation, making**

文章引用: 程炜琪. 电子证据合法性与排除规则的优化路径[J]. 法学, 2025, 13(4): 723-732.
DOI: 10.12677/ojls.2025.134105

**the exclusionary rule for illegal evidence difficult to effectively apply to electronic data. With the growing development of digital rights and the emergence of concepts like digital human rights, electronic data not only pertains to the effective prosecution of crimes but also involves important rights and interests of the accused, such as personal and property rights. Therefore, balancing the legality and authenticity of electronic evidence in this process is crucial. Based on an institutional analysis of the current legality review and exclusionary rules for electronic evidence in China, this paper explores their shortcomings in legislation and judicial practice. By comparing international judicial practices, it suggests incorporating electronic evidence into the exclusionary rule for illegal evidence and improving the standards for reviewing electronic evidence from the perspectives of the evidence collector and the collection procedure, with the aim of providing a reference for the rule of law in China's electronic evidence system.**

## Keywords

**Electronic Evidence, Legality Review, Exclusionary Rule for Illegal Evidence, Procedural Justice, Digital Rights**



## 1. 引言

近年来，随着信息技术的飞速发展，与互联网有关的犯罪类型在我国刑事犯罪中所占比重越来愈高，相应的电子证据在刑事诉讼中的地位愈发重要[1]。电子邮件、短信记录、社交媒体信息、网络交易记录等多种电子数据形式，逐渐成为刑事案件，尤其是金融犯罪、网络犯罪等领域的重要证据[2]。在认定犯罪事实和量刑过程中，电子证据常常发挥核心作用。

自 1979 年《刑事诉讼法》首次颁布以来，我国的刑事证据制度经历了多次修订，其中 2012 年的修订将电子数据明确纳入证据体系，成为独立的法定证据类型。这一举措是对信息化时代法律需求的积极回应，满足了司法实践中对电子证据的迫切需求。电子证据的收集与使用不仅关系到有效追诉犯罪，还涉及保障被追诉人的合法权益。如何平衡其合法性与真实性，成为了电子证据合法性审查与非法电子证据排除规则亟待解决的重要问题。

基于对现行电子证据合法性审查与排除规则的制度分析，本文探讨了目前在立法与司法实践中的不足，并通过对比国际经验，结合电子证据的特点，从取证主体和取证程序两个方面提出未来刑诉法修订应将电子证据纳入非法证据排除规则，并完善电子证据审查标准，以推进我国电子证据制度的法治化建设。

## 2. 电子证据合法性审查及排除规则的法律框架

(一) 我国电子证据合法性审查的法律基础

我国现行的电子证据合法性审查制度建立在 2012 年修订的《刑事诉讼法》基础上。随后，相关司法解释和规范性文件进一步对电子证据的收集、提取、保管及审查作出明确规定，尤其是在保障电子数据

[1] 参见 2024 年《最高人民检察院工作报告》：根据 2024 年两会最高检工作报告统计，2023 年检察机关起诉利用网络实施的犯罪 32.3 万人、起诉电信网络诈骗犯罪 5.1 万人、帮助信息网络犯罪 14.7 万人、网络赌博犯罪 1.9 万人。
https://www.spp.gov.cn/spp/2024qglh/zgjgzbg/index.shtml

[2] 例如，在某些金融犯罪案件中，电子邮件和网络交易记录被用作关键证据，帮助执法机关追踪资金流向；在网络犯罪中，社交媒体信息和网络交易记录则用于确认犯罪行为的发生和参与者身份。

真实性及适用排除和效力补正规则等方面进行了详尽规定。

从现有法律及其司法解释的规定来看[3]，电子证据的合法性主要集中在以下三个方面：首先是主体适格性，2016 年发布的《关于办理刑事案件收集提取和审查判断电子数据若干问题的规定》(以下简称“两院一部《电子证据规定》”)第 7 条和第 24 条第一款规定，收集和提取电子证据的人员应具备侦查人员的法定资格，并对人数作出明确规定。其次是程序合法性，两院一部《电子证据规定》第 2 条宏观上规定了收集、提取电子证据的程序合法性标准，第 13~17 条具体规定了取证方法、证据收集过程中的见证人见证、笔录记录等程序合法要求。此外，第 24 条审查标准中也明确规定了以上程序合法的审查要求。最后是证据保管链条的合法性，两院一部《电子证据规定》第 5 条和第 8~12 条规定，电子数据从收集、提取到审查的全过程应保证其完整性，确保没有被增加、删除或修改，并在必要时采取冻结等保全措施。

(二) 电子证据采用的补正机制与排除规则

两院一部《电子数据规定》第 27 条列举了电子数据收集提取过程中的四类瑕疵情形，包括未以封存状态移送、缺乏相关签名或盖章、标注信息不明确及其他瑕疵问题。当电子数据存在上述问题时，经补正或合理解释后可以采用，无法补正或合理解释的，则不得作为定案依据。第 28 条进一步明确了篡改、伪造、增加、删除或修改等情况，导致无法保证真实性的电子数据不得作为定案依据。2019 年的《公安机关办理刑事案件电子数据取证规则》(以下简称“《电子数据取证规则》”)从技术角度对电子数据收集、提取程序作出了合法性要求，但未对违反程序的后果进行明确规定。《公安机关办理刑事案件程序规定(2020 修正)》(以下简称“2020 年《公安部规定》”)第 66 条第 3 款明确了电子数据真伪存疑时“不能作为证据使用”，第 71 条第 2 款则进一步规定“收集物证、书证、视听资料、电子数据违反法定程序，可能严重影响司法公正的，应当予以补正或合理解释；无法补正或合理解释的，对该证据应予以排除”，由此确立了电子数据参照书证、物证的相对排除规则。《最高人民法院关于适用〈中华人民共和国刑事诉讼法〉的解释(2021)》(以下简称“最高法《解释》”)细化了电子数据收集提取的合法性要求，但对排除情形的规定并未超出前述规范的范围。2022 年《最高人民法院、最高人民检察院、公安部关于办理信息网络犯罪案件适用刑事诉讼程序若干问题的意见》(以下简称“2022 年《网络犯罪若干意见》”)对电子数据的审查判断作出了具体规定，如数据真实性、完整性和关联性的评估标准。然而，该意见未对在取证过程中存在的非法行为或程序瑕疵导致的电子数据排除问题进行详细说明，未能全面覆盖非法电子数据排除的需求。结合以上内容不难看出，上述规定主要强调电子数据的真实性，旨在规范其证明力，而非合法性问题。

综上所述，我国电子证据的法律框架主要聚焦于确保电子数据的真实性和证明力，通过明确主体适格性、程序合法性以及保管链条完整性等方面的规定，力图提高电子证据在刑事诉讼中的合法性。同时，通过补正机制与排除规则，对存在瑕疵的电子数据进行审查，确保取证程序的规范性，以此来保障司法的公正性和案件定案的可靠性。

## 3. 现行电子证据制度的缺陷与比较分析

(一) 我国现有立法上缺乏非法电子证据的排除规则

目前，我国立法中对于非法电子数据的排除尚缺乏明确可适用的规范指引。虽然已有一些电子证据排除的相关规定，但这些规定主要关注证据的证明力问题，而非证据的能力。具体而言，证据具有两个基本属性：证据能力与证明力。

首先，证据能力(也称为证据资格)决定了材料或事实能否作为证据进行调查与采纳，只有具备证据能

[3]最高人民法院、最高人民检察院、公安部印发《关于办理刑事案件收集提取和审查判断电子数据若干问题的规定》的通知，法发〔2016〕22 号。

力的材料才能作为证据使用。而证明力则是证据本身的固有属性，表征证据对案件事实的证明作用及其证明程度[1]。这两者之间存在本质区别。非法证据排除规则主要涉及证据的证据能力判断，即是否具备作为证据的资格；而证明力规则则是判断证据对于案件事实的证明作用，其适用更为灵活，是法官综合全案证据作出的裁量判断。

然而，在现行的《刑事诉讼法》及相关司法解释中，非法证据排除的相关规定对于电子数据的适用存在不足。具体来说，《刑事诉讼法》第 52、56 条以及相关规定在证据种类上具有封闭性，导致电子数据虽然属于法定证据种类，但未能纳入非法证据排除的适用范围[2]。根据《刑事诉讼法》、最高法《解释》[4]、两院三部《办理死刑案件证据规定》、两院三部《非法证据排除规定》[5]以及两院一部《电子证据规定》等规范性文件，现有的证据排除规则可分为四类：非法言词证据排除规则，排除通过非法手段获取的口供和证人证言；非法实物证据排除规则，排除未经合法程序收集的物证；不得作为定案根据的规则，排除无法作为定案依据的证据，即使其存在也不能影响案件的最终判决；其他不得作为证据使用的材料，排除一些特定类型的证据，如推断证据或补充性证据等，尽管不能作为直接证据使用，但可以作为案件参考。

其中，两院一部《电子证据规定》第 27、28 条明确规定，针对电子证据的排除适用于“不得作为定案根据规则”，这一规则从用语上来看属于规范证明力的问题，与非法证据排除规则的证据能力判断规则存在本质区别。尽管两者都涉及证据的排除，但它们的立法基点与适用条件不同：非法证据排除规则是为了制裁取证程序严重违法、侵犯公民基本权利的行为，导致证据能力丧失，因此适用该规则时，证据无论真伪，只要符合《刑事诉讼法》第 56 条的情形，就应当绝对、当然地排除，因为非法证据排除规则的目的是通过严格的程序制裁，防止侦查机关的权力滥用，确保司法公正。因此，当证据获取过程中存在严重违法行为时，法律要求无论证据是否真实，都必须绝对排除，避免任何主观判断或自由裁量，确保规则的严肃性和统一适用。而证明力规则则由法官根据全案证据综合判断，适用时具有相对性与裁量性。

尽管现有的一些规范性文件对电子数据的排除作出了规定，但这些规定主要针对取证程序瑕疵导致电子数据真实性存疑的情形，并未从保障人权的角度规范非法取证行为。举例而言，2020 年《公安部规定》第 71 条虽明确规定非法电子数据应参照物证、书证进行相对排除，但作为部门规章，其效力层级较低，仅规范侦查取证行为，未对审查起诉与审判程序产生规制作用，因此尚不能作为非法电子数据排除的适用依据[2]。

(二) 现实中电子证据合法性与排除规则的适用情况

在目前的司法实践中，对电子数据的审查主要围绕着“查证属实”这一核心目标展开。控辩双方在法庭上提交的证据，必须经过法庭调查确认是否具有证据资格，并同时满足合法性、真实性、关联性等要求，才能作为“定案依据”。由于电子数据可以独立于其存储介质而存在，在网络环境下极易面临被篡改的风险，因此，证据的完整性成为审查过程中的一个关键环节[3]。辩方往往会对证据的完整性提出异议。因此，从制度设计的角度看，电子数据的审查应当涵盖合法性、真实性、关联性和完整性这四个方面。然而，目前在举证、质证和认证环节，仍然存在着以下两种问题：

1) 合法性审查的标准有被真实性标准取代或掩盖的趋势

针对电子数据，司法实践中辩方一般会在案件中提出多种异议，主要集中在取证程序违法、程序瑕疵、电子数据真实性存疑等问题上。有学者根据实证分析发现，取证程序违法是最常见的异议理由，占 46.4%；其次是电子数据的真实性存疑，占 16.8%。其他异议还包括鉴定意见违法、不符合技术要求、未

[4]参见最高法《解释》第 88、135 条的规定。

[5]最高人民法院、最高人民检察院、公安部、国家安全部、司法部《关于办理死刑案件审查判断证据若干问题的规定》和《关于办理刑事案件排除非法证据若干问题的规定》。

扣押原始储存介质等。然而，尽管辩方在不少案件中提出了这些异议，但法院在大多数情况下并不采纳。此外在裁判过程中，法院主要通过四种方式处理辩方的异议：直接采信电子数据、补正后采信、未作针对性回应、排除电子数据。其中超过 90%的案件中，法院通过直接采信或要求侦查机关补正相关程序瑕疵来驳回辩方的排除申请，只有 3.2%的案件最终成功排除了非法电子数据[2]。值得注意的是，即使在成功排除的案件中，法院并未依据“非法证据排除规则”，而是依据“不能作为定案根据”的原则，认为取证程序存在无法补正或合理解释的重大瑕疵，影响了证据的真实性。

这揭示了一个重要的司法现象：在电子数据的排除问题上，法院更倾向于重视证据的真实性，而对取证过程中的程序合法性审查较为宽松。这一现象背后可能存在多重原因，包括现行法律规定对于电子数据的程序合法性审查不够具体，司法人员在处理电子证据时缺乏系统的培训和实践经验，以及现行排除规则在适用电子数据时的局限性等。虽然辩方提出的异议往往指向取证程序的不规范，但法院更关注的是电子数据是否能够通过补正程序保持其真实性，导致证据真实性成为了补正程序违法性的实质因素[6]。

2) 实践中电子证据的举证载体存在混淆

在司法实践中，电子数据的举证方式出现了通过实物形式，如打印件、截图、视频等，来替代电子数据本身进行举证，这些形式原本是用于在无法获取原始储存介质时的补充性手段。然而，实践中这些补充手段却逐渐演变为常规的举证方式，取代了对电子数据本体的展示和审核。这种实物证据化的举证方式，模糊了前端证据收集与后端证据呈现的界限，导致取证过程不够严谨，可能出现电子数据本体未被妥善收集或展示的情况。事实上，电子数据是否需要严格遵循“原件”制度一直存在分歧，部分学者认为电子数据具备“无损再生性”，因此原件与复制件内容完全一致时，没有必要坚持原件制度[4]。而另一些学者则主张，电子数据的举证应当坚持“原始性优先原则”，确保其真实性和完整性[5]。由于立法和规范没有对电子数据的外部载体和展示形式作出明确的统一规定，实践中的举证方式混乱且不一致。

根据两院一部《电子数据规定》第 21 条、第 19 条第二款[7]，电子数据的举证可以通过多媒体设备展示，也可以通过专门知识人员的说明，无法展示的应当通过对电子数据属性、功能等情况的说明进行展示。两院三部《办理死刑案件证据规定》第 29 条第 2 款和两院一部《电子数据规定》第 17 条指出[8]，电子数据还可以通过鉴定意见和检验报告等方式进行举证。此外，《电子数据取证规则》第 8 条也规定了打印、拍照、录像等手段可以作为与扣押和提取并行的固定证据形式[9]。然而，这些规定对电子数据的举证缺乏具体要求，未明确举证内容和顺序安排，也未清晰界定“无法展示”的具体情况，导致实践中办案人员会选择通过打印材料、照片或录像等方式来完成举证，忽略了这些手段是否能充分展示电子数据的合法性和完整性。

实际上，按照《人民检察院公诉人出庭举证质证工作指引》的规定[10]，举证方在出示电子数据时需要

[6]参见王某刚、王某荣组织、领导传销活动案，山东省烟台市芝罘区人民法院(2018)鲁 0602 刑初 320 号刑事判决书以及颜理尧、周维东等侵犯商业秘密案，江苏省扬州市中级人民法院(2017)苏 10 刑终 199 号刑事裁定书。

[7]两院一部《电子数据规定》第 21 条：“控辩双方向法庭提交的电子数据需要展示的，可以根据电子数据的具体类型，借助多媒体设备出示、播放或者演示。必要时，可以聘请具有专门知识的人进行操作，并就相关技术问题作出说明”。两院一部《电子数据规定》第 19 条第二款：“对数据统计量、数据同一性等问题，侦查机关应当出具说明。”

[8]两院三部《办理死刑案件证据规定》第 29 条第 2 款：“对电子数据有疑问的，应当进行鉴定”。两院一部《电子数据规定》第 17 条：“对电子数据涉及的专门性问题难以确定的，由司法鉴定机构出具鉴定意见，或者由公安部指定的机构出具报告。对于人民检察院直接受理的案件，也可以由最高人民检察院指定的机构出具报告。”

[9]《电子数据取证规则》第 8 条：“具有下列情形之一的，可以采取打印、拍照或者录像等方式固定相关证据：(一) 无法扣押原始存储介质并且无法提取电子数据的；(二) 存在电子数据自毁功能或装置，需要及时固定相关证据的；(三) 需现场展示、查看相关电子数据的。根据前款第二、三项的规定采取打印、拍照或者录像等方式固定相关证据后，能够扣押原始存储介质的，应当扣押原始存储介质；不能扣押原始存储介质但能够提取电子数据的，应当提取电子数据。”

[10]最高人民检察院《人民检察院公诉人出庭举证质证工作指引》第 39 条：“出示以数字化形式存储、处理、传输的电子数据证据，应当对该证据的原始存储介质、收集提取过程等予以简要说明，围绕电子数据的真实性、完整性、合法性，以及被告人的网络身份与现实身份的同一性出示证据。”

提供有关原始储存介质及其提取过程的信息，确保证据的真实性、完整性和合法性。同时，如果控方仅提交书面材料，而未能提供原始介质或完整备份，辩方将难以对电子数据进行有效质证，削弱了庭审实质化的效果。

(三) 完善电子证据合法性与排除规则的必要性与可行性分析

在刑事诉讼中将电子证据纳入非法证据排除规则的必要性，首先源于电子数据的特有属性，如虚拟性和易篡改性。这些特性使得电子数据的合法性审查成为刑事司法中一个亟待解决的关键问题。尽管《刑事诉讼法》自 2012 年修改后已将电子数据列为法定证据种类，但其适用的排除规则仍主要沿用传统实物证据的标准，这导致电子证据合法性审查未得到足够重视。例如，在司法实践中，通常更关注电子数据的真实性，而忽视了侦查过程中可能存在的程序违法行为，从而导致合法性存在瑕疵的电子数据未能被排除。这不仅影响了证据规则的一致性，也可能侵害被告的隐私权及正当程序的保障权[6]。

进一步而言，电子数据作为信息化社会中的重要证据形式，其在网络犯罪中的广泛应用凸显了取证过程的复杂性，特别是在数据的收集、提取和鉴定方面。任何不当的取证行为都可能严重影响数据的完整性和真实性，例如，未经授权的远程访问、数据篡改、缺乏适当的取证程序等不当取证行为，都可能导致电子数据的完整性和真实性受到严重影响，从而削弱其在司法程序中的证明力。因此，对电子数据合法性的审查，不仅是确保证据真实可靠的必要步骤，更是维护程序正义和保障人权的重要一环[7]。如果不将电子数据纳入非法证据排除规则，可能导致侦查活动失控，无法充分发挥合法性审查的作用，进而使被告难以质疑证据来源及取证程序的合法性。

然而，现行的电子数据合法性审查规则仍存在滞后性和片面性。例如，两院一部《电子数据规定》要求审查电子数据的真实性、合法性和关联性，但在司法实践中，合法性审查往往被视为辅助内容，而非独立审查项。这种做法在一定程度上削弱了非法证据排除规则的核心价值——通过程序制裁防止侦查权力的滥用[8]。

从国际经验来看，美国通过宪法和判例赋予了公民隐私权较高的保护。例如，美国宪法第四修正案规定，人民有权保护其个人信息免受无理搜查和扣押，未经合法程序的搜查和取证行为会导致获得的证据不能作为法庭证据使用 [11]。这一规则通过“毒树之果”原则延伸，任何源自非法证据的后续证据也应被排除 [12]。随着数字时代的发展，美国法院在处理电子证据时也逐步加大保护力度，尤其是在涉及手机信息和电子邮件的案件中，法院要求执法机关必须先获得搜查令，否则其获得的证据会被视为非法 [13]。

相比之下，我国目前在电子证据排除方面的立法仍显不足。尽管随着犯罪活动日益网络化，电子证据在刑事案件中的重要性不断提升，但我国对电子证据的合法性审查及隐私权保护尚未形成完善的法律体系。这一差距在一定程度上反映出我国在面对数字信息时代带来的挑战时，仍未充分关注电子证据的特殊性和对个人隐私的保护。

## 4. 电子证据合法性与排除规则制度法治化的构建

(一) 将电子数据纳入非法证据排除规则的适用范围

为确保电子证据在刑事诉讼中符合程序正义原则，有必要将电子数据纳入非法证据排除规则的适用范围。这不仅有助于防止侦查机关的程序违法行为，还能保障公民的隐私权、财产权等基本权利，同时也是对侦查机关电子数据违法取证侵犯公民基本权利行为的程序性制裁。在刑事诉讼中，程序性制裁是

[11] 参见美国国家档案馆(https://www.archives.gov/founding-docs/bill-of-rights)。

[12] 这一规则源自美国的“毒树之果”原则，根据《美国宪法》第四修正案和相关判例，如《麦卡洛诉伊利诺伊州案》，任何源自非法证据的后续证据也应被排除，以防止非法取证行为的蔓延。

[13] 参见 Riley v. California, 573 U.S. 373 (2014), Carpenter v. U.S. 138 S. Ct. 2206 (2018), USA v. Steven Warshak, No. 08-4085 (6th Cir. 2010)。

实现对国家专门机关程序违法制裁和个人权利救济的重要方式，它是通过宣告违法收集的证据、实施的诉讼行为、作出的裁判结果丧失法律效力来实现对程序违法的制裁。非法证据排除规则是程序性制裁的重要方式之一，它主要是通过排除侦查机关违法收集的证据从而对其违法行为予以制裁[9]。

我国《刑事诉讼法》已初步确立非法证据排除规则，尤其是对非法言词证据与非法实物证据的区分[14]。然而，该法在非法实物证据的界定上，仅明列物证和书证，而未明确涵盖电子数据和视听资料。这一立法上的局限，导致非法证据排除规则在实物证据层面仅适用于传统的物证和书证，电子数据的非法取证排除尚未得到有效保障。尽管最高人民法院与最高人民检察院发布的相关司法解释，以及《人民检察院刑事诉讼规则》对非法证据排除规则进行了一定程度的细化[15]，但电子数据仍未被纳入排除适用的实践范围中，侦查机关违法收集电子数据的现象仍然存在，侵犯公民基本权利的案例屡见不鲜。

例如，在侦查环节，取证人员认识偏差导致取证不全，“片面取证”等现象时有发生。由于欠缺针对电子证据的非法证据排除规则，导致即使取证程序欠规范，侦查机关存在电子数据收集主体不合格、程序有瑕疵的情况，也可以通过事后采取相应的补正措施获得证据能力；另有部分司法人员将电子数据依附于其原始存储介质，视为非法物证以适用排除规则[10]。前者的做法纵容了非法取证行为，无法对违法行为进行程序性制裁，也未能为受害者提供程序性救济；后者虽提供一定的救济，但随着云存储和远程取证的普及，电子数据往往与物理介质分离，传统的物证排除规则难以有效应对。国际经验表明，域外国家和地区的非法证据排除规则通常适用于严重侵害公民隐私权和财产权的取证行为，不局限于物证和书证，亦涵盖电子数据和视听资料。例如，美国第四修正案不仅适用于传统的物证和书证，还明确涵盖电子数据和视听资料；欧盟《数据保护条例》(GDPR)在取证过程中对个人数据的保护提出了严格要求，确保电子数据在收集和使用过程中不侵犯个人隐私权。随着信息社会和数据经济的发展，电子数据作为“证据之王”，承载着公民的多项基本权利。因此，为更好地保护公民的数字权利，并对非法获取电子数据的行为实施程序性制裁，亟需通过修改《刑事诉讼法》将电子数据明确纳入非法证据排除规则的适用范围。

(二) 完善电子证据取证主体的合法性

如前文所述，我国现行规定主要强调了取证主体的适格性，但在以下几个方面仍有待完善。

首先，对于取证人员，应构建专业化培训和认证制度。根据《电子数据取证规则》第六条，电子数据收集应由两名以上侦查人员进行，必要时可以聘请专业技术人员协助。但现行规定对取证人员的技术资质和专业能力并未作详细要求，缺乏针对电子数据取证的系统化培训和认证机制。因此，建议设立统一的电子数据取证人员培训和资格认证制度，以确保取证人员具备足够的技术能力和法律知识，适应信息化取证日益复杂的需求，例如，可以设立由司法部或相关专业机构主导的电子数据取证人员培训项目，涵盖电子取证技术、数据安全、法律法规及职业道德等内容，并通过考试和认证程序，确保取证人员具备必要的专业知识和技能。其次，需明确第三方技术人员的责任和权利。《电子数据取证规则》提到，在必要时可以聘请专业技术人员协助收集电子数据。然而，对于这些技术人员在取证过程中的法律责任和权利，现行规定并未详细说明。例如，当第三方在数据提取过程中出现失误或违规操作时，法律责任的承担机制尚不清晰。因此，建议明确第三方技术人员在取证过程中的法律地位、职责范围及相应法律责任，以规范其行为并确保取证质量。此外，对于取证主体的授权程序，应增强其透明性和可追溯性，例如，可以通过建立电子化的取证授权系统，记录每一次取证授权的申请、审批和执行过程，并定期公开审计报告，以确保取证行为的透明和可追溯。两院一部《电子证据规定》第十三条规定，调取电子数据，

[14] 参见《刑事诉讼法》第 56 条第一款：“采用刑讯逼供等非法方法收集的犯罪嫌疑人、被告人供述和采用暴力、威胁等非法方法收集的证人证言、被害人陈述，应当予以排除。收集物证、书证不符合法定程序，可能严重影响司法公正的，应当予以补正或者作出合理解释；不能补正或者作出合理解释的，对该证据应当予以排除。”

[15] 参见最高法《解释》第 74 条、《人民检察院刑事诉讼规则(2019)》第 70 条。

应当制作调取证据通知书，注明需要调取电子数据的相关信息，通知电子数据持有人、网络服务提供者或者有关部门执行。由此可知，电子数据的收集和提取应遵守法定程序，确保证据的真实性、合法性和关联性。从现行规定来看，虽然要求取证行为必须经过相应授权，例如制作调取证据通知书，但对于授权的具体程序和审查标准缺乏细化说明，可能导致授权程序不透明或审批随意性问题。因此，建议完善取证授权程序的标准化，明确授权申请、审批以及记录的细节，并建立可追溯的取证授权记录，以增强取证主体行为的透明性和可监督性。

最后，应对“见证人”制度进行进一步细化。《电子数据取证规则》第九条要求取证过程中的见证人签名或盖章，以确保取证过程的公正性和合法性。然而，见证人的选择和职责目前并未有详细规定。例如，见证人应具备什么样的资质？见证人是否需要具备相关的法律或技术背景？这些问题仍不明确。因此，建议对见证人制度进行进一步细化，明确见证人的选择标准、权利与义务，以提高见证过程的可信度。

(三) 完善取证程序的合法性

在完善取证程序合法性的同时，需要回应电子数据侦查取证中的权利保障需求，对现有搜查、扣押等侦查措施进行改进和完善。电子数据不仅是信息网络和数字经济时代承载公民财产权和隐私权的重要载体，而且其取证过程可能会对这些基本权利产生干预。因此，有必要将电子数据取证行为纳入法定程序控制之中，确保取证行为既高效又合法，维护公民的合法权益。

1) 对传统侦查手段的数字化措施

首先，现行《刑事诉讼法》虽未明确规定电子数据作为搜查对象，但已有相关条款隐含电子数据应属于搜查适用范围的意图。例如，《刑事诉讼法》第 136 条中规定，搜查的目的是“收集犯罪证据”和“查获犯罪人”，而电子数据作为法定的证据类型之一，自然应纳入搜查的适用对象[16]。此外，第 137 条也规定：“任何单位和个人，有义务按照人民检察院和公安机关的要求，交出可以证明犯罪嫌疑人有罪或者无罪的物证、书证、视听资料等证据”。根据“等证据”的立法表述，电子证据作为与物证、书证、视听资料并列的八种证据之一，也应当属于任何单位和个人按照义务交出的证据种类。然而，司法实践中公安司法人员通常只将电子数据的存储介质(如硬盘、手机)作为搜查对象，而未将电子数据本身纳入搜查范围，导致承载公民隐私权、财产权的电子数据未能获得充分的程序保障。因此，未来在《刑事诉讼法》的修改中，应明确电子数据本身作为搜查和扣押的对象，以此应对信息社会中的取证需求。例如，欧盟《网络犯罪公约》第 19 条[17]中明确将电子数据纳入搜查和扣押的适用对象，这一规定不仅包括存储介质(如计算机、硬盘)，还包括数据本身，这种突破传统有形物的搜查制度的方式，为打击网络犯罪提供了更为有力的法律依据，为我国法律在这方面的完善提供了参考和借鉴。

其次，新兴的侦查取证措施，如网络远程勘验和电子数据冻结已经被用于司法实践，以适应电子数据取证的需求。网络远程勘验是对传统现场勘验的延伸，通过远程连接勘验数据，可以解决电子数据存储在物理位置上难以接触的问题，例如，可以在《刑事诉讼法》中明确网络远程勘验的法律程序和技术标准，如取证设备的安全性、数据传输的加密要求，以及远程勘验过程的监控和记录，以确保证据收集的合法性和数据的完整性。电子数据冻结则适用于无法通过扣押和封存措施有效保全的数据，例如存储于云空间或远程服务器上的数据。这些新兴的侦查取证措施虽然在某些方面与传统取证措施类似，并已经规定于《电子数据取证规则》以及两院一部《电子证据规定》中，但由于这两部规范效力位阶较低以及电子证据本身的特殊性，需要在《刑事诉讼法》的框架内给予明确和规范的程序保障。

[16]《刑事诉讼法》136 条：“为了收集犯罪证据、查获犯罪人，侦查人员可以对犯罪嫌疑人以及可能隐藏罪犯或者犯罪证据的人的身体、物品、住处和其他有关的地方进行搜查。”

[17]参见《欧洲条约集》第 185 号——《网络犯罪公约》，2001 年 11 月 23 日，第 19 条搜查和扣押存储的计算机数据。

2) 取证程序的差异化

电子数据的特殊性在于其广泛承载着公民财产权、隐私权、通信自由等不同权利，因此，必须根据数据类型和所涉及的法益来制定针对性的取证措施。现行《刑事诉讼法》、两院一部《电子数据规定》《电子数据取证规则》等法律文件中已有一些差异化取证的具体做法，但仍存在改进空间。

首先，针对电子数据承载的不同类型基本权利，取证程序应体现出不同的控制强度。例如，《刑事诉讼法》在侦查措施的设置中，针对承载公民财产权、隐私权的房屋适用搜查程序，而对于通信自由、通信秘密的邮件则适用检交扣押程序，而案件现场中的勘验则适用于公开环境中的证据调查。这反映了对不同权利类型的差异化保护。在电子数据侦查取证中，也应基于数据的分类分级，设置相应的程序控制，以确保对不同权利的有效保护。例如，《数据安全法》中规定电子数据存储于第三方平台(如网络服务提供者)中的数据，通常通过调取程序来获取[18]。然而，该调取过程中的程序控制强度较弱，未充分考虑不同类型数据的敏感性，这可能会影响公民的数据基本权利。为实现取证过程的差异化和合法性，需要根据数据类型设置具体的取证措施。例如，对于网络服务提供者掌握的数据，涉及公民财产权、隐私权的电子数据(如交易记录、电子邮件等)，应采取更为严格的程序进行调取，将其视为对第三方的搜查。相比直接搜查犯罪嫌疑人，第三方搜查的适用条件应更加严格，例如，必须经过县级以上公安机关负责人的审批才能进行。这种规定可以确保在涉及个人隐私和财产权时，取证行为经过更加严格的司法审查，从而减少对公民基本权利的过度干预。

此外，对于涉及通信秘密的数据(如电子邮件、即时通信记录等)，现行规定中并未完全纳入邮件检查和扣押的适用范围，而是通过较为宽松的调取程序进行。这在实践中可能会导致公民通信秘密受到侵害。因此，建议将此类通信数据的调取严格纳入检交扣押程序中，确保在获取此类数据时必须经过法定的审批程序，并明确相关主体的权利和义务，以维护公民的通信自由和秘密。对于承载公民个人信息的电子数据，如用户注册信息、网络访问日志等，调取这些数据同样可能对公民个人信息自决权造成影响，因此应将其界定为强制性侦查措施，并设置相应的审批程序。这是由于个人信息的收集和使用需在法律框架内进行，未经合法授权的取证行为可能侵犯公民的个人信息安全和自决权。为了与《数据安全法》等相关法律保持一致，应将涉及公民个人信息的数据调取程序进一步规范化，确保在进行数据调取时依法保护公民的个人信息权利[19]。

另一方面，网络空间中公开发布的信息数据(如社交媒体上公开的帖子、博客等)，由于其公开性，涉及的隐私和财产权较少，这类数据通常可纳入任意性侦查措施，调取时无需设置严格审批程序，但侦查机关应出具相应证明文件，以保证取证行为的正当性和合法性。这有助于提高取证效率，满足司法机关对公共信息快速取证的需求。

## 5. 结论

将电子数据纳入非法证据排除规则，不仅有助于提高证据审查标准，防止侦查过程中程序违法行为的发生，还能更好地保障公民的隐私权、财产权等基本权利。这一举措充分体现了程序正义原则，也是对非法取证行为的有效制裁。完善电子证据合法性审查标准，是确保电子证据在司法程序中有效适用的关键。通过严格规定取证主体合法性、程序合法性、证据保管链完整性、数据真实性以及合法授权等要

[18] 参见《数据安全法》第三十八条：“国家机关为履行法定职责的需要收集、使用数据，应当在其履行法定职责的范围内依照法律、行政法规规定的条件和程序进行；对在履行职责中知悉的个人隐私、个人信息、商业秘密、保密商务信息等数据应当依法予以保密，不得泄露或者非法向他人提供。”

[19] 参见《数据安全法》第三十二条：“任何组织、个人收集数据，应当采取合法、正当的方式，不得窃取或者以其他非法方式获取数据。法律、行政法规对收集、使用数据的目的、范围有规定的，应当在法律、行政法规规定的目的和范围内收集、使用数据。”第三十五条：“公安机关、国家安全机关因依法维护国家安全或者侦查犯罪的需要调取数据，应当按照国家有关规定，经过严格的批准手续，依法进行，有关组织、个人应当予以配合。”

求，能够有效防止电子证据在收集和运用过程中出现瑕疵，保障刑事诉讼的公正性和证据的可靠性。

未来，应通过立法和司法实践的双重努力，进一步推动电子证据制度的法治化建设。在信息技术飞速发展的背景下，司法机关应不断更新对电子证据的审查标准，以应对数字化犯罪的新挑战，确保在追求司法公正的同时，充分保障被追诉人的合法权益。这不仅是对信息时代司法公正性的要求，更是现代法治国家对公民权利保护的应有之义。

## 参考文献

[1] 陈光中. 证据法学[M]. 第 5 版. 北京: 法律出版社, 2021.

[2] 韩旭, 陈玥茜. 非法电子数据排除规则的实证分析与完善路径[J]. 证据科学, 2024, 32(4): 468-483.

[3] 李祥雨, 张小玲. 电子数据鉴真规则的构建——以形式关联性为中心[J]. 证据科学, 2024, 32(1): 83-92.

[4] 奚玮. 我国电子数据证据制度的若干反思[J]. 中国刑事法杂志, 2020(6): 135-154.

[5] 龙宗智, 等. 刑事庭审证据调查规则研究[M]. 北京: 中国政法大学出版社, 2021.

[6] 胡铭, 王林. 刑事案件中的电子取证: 规则、实践及其完善——基于裁判文书的实证分析[J]. 政法学刊, 2017, 34(1): 79-89.

[7] 赵航. 电子数据合法性审查规则的反思与完善[J]. 大连理工大学学报(社会科学版), 2022, 43(1): 87-94.

[8] 刘译矾. 论电子数据的双重鉴真[J]. 当代法学, 2018, 32(3): 88-98.

[9] 谢登科. 电子数据侦查取证措施法治化与《刑事诉讼法》再修改[J]. 法治研究, 2024(5): 90-105.

[10] 谢登科. 非法电子数据排除的理论基点与制度建构: 以数字权利的程序性救济为视角[J]. 上海政法学院学报(法治论丛), 2023, 38(3): 62-80.