刑事司法科学与治理
*Criminal Justice Science & Governance*
2022 年 第 3 卷 第 2 期

# 电子侦查取证中的公民通信秘密权利保护 *

叶翔宇

西南政法大学，重庆

**摘　要** | 当前技术手段的应用对案件侦查发挥着重要作用，随之而来的公民基本权利保护问题也愈发显现，电子侦查取证过程中公民通信秘密的宪法权利保护问题尤为突出。细究问题之症结，侦查机关在电子数据取证过程中未能结合时代特征准确把握通信秘密的内含，在平衡惩罚犯罪与保障公民通信秘密宪法权利方面难以实现困境突破。通过揭露电子侦查取证过程中侵犯公民通信秘密权的现实情况，在比例原则指导下，以通信秘密层级的区分为基础，对案件进行类型化划分，从而为电子侦查取证活动中的公民通信秘密宪法权利保护问题提供有益探索。

**关键词** | 电子侦查；通信秘密权利；宪法规制；比例原则



## 一、问题的提出

时代的变革会赋予事物新的变化，公民的通信秘密权利随着时代的发展也有了新的内涵。最高人民法院、最高人民检察院和公安部 2016 年 9 月颁布的《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《电子数据证据规定》）和公安部 2019 年 1 月颁布的《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》）对电子数据收集、提取做了较详细的规定，但这些规定侧重于从取证技术层面来保障电子数据的真实性与可靠性，对电子数据收集中的权利保护关注不足[1]。

在网络信息时代，公民的通信秘密权利的内涵得到扩张，与之带来的是公民通信秘密权利也更加容易受到侵犯。在电子侦查取证过程中，哪些行为侵犯了公民的通信秘密权利，对于侵犯公民通信权利的电子数据应当如何处理，如何在案件侦破与公民通信秘密权利保护两者之间做出平衡，都是当前电子数据发展完善过程中亟待解决的重要问题。这些问题的解决，不仅有利于电子数据侦查取证制度的完善，更有利于刑事诉讼中“惩罚犯罪与保障人权”目的的实现。

从公民的基本权利角度出发，探究电子数据取

*本文系2021年度西南政法大学校级学生科研创新项目（编号：2021XZXS-135）。

［1］谢登科．论电子数据收集中的权利保障［J］．兰州学刊，2020，12：33-45.

证规制问题，已经成为当前研究的前沿阵地。潘金贵教授在文章中明确了电子数据收集措施对居住自由权、隐私权、财产权等公民基本权利存在干预，但是并未提及对于公民通信自由权的干预[1]。梁坤教授在其文章中提到了电子数据收集措施有侵犯公民通信自由权利之嫌，但是并没有展开详细论述[2]。谢登科教授基于经典案例，对刑事电子数据取证中侦查机关对公民通信权利干预的行为进行了分析。但遗憾的是，其在文章中并未将通信秘密权和通信自由权进行有效区分[3]。由此可见，通信自由权和通信秘密权往往因其具有抽象性、模糊性等特点而在研究过程中被学界所忽视。

本文以宪法对于公民通信自由和通信秘密的权利保护为依据，从通信秘密权利角度出发，结合电子侦查取证的相关法律规定和实践，阐述在当前电子数据收集过程中对公民通信秘密权利保护存在的挑战，并进一步探究如何在电子侦查取证过程中最大程度地保护公民的通信秘密权，最终实现惩罚犯罪与保障公民通信秘密权相平衡的目的。

## 二、电子侦查取证中公民通信秘密宪法权利之解说

科技的快速发展推动着侦查技术水平的提高。与此同时，侦查活动的开展与公民基本权利的保护之间的对抗也愈发激烈。对以电子数据取证为代表的侦查活动进行科学规制，需要明确公民通信秘密权利保障在侦查活动中的定位并进一步揭示通信秘密权的时代内涵、阐述保障公民通信秘密权利的必要性。

### （一）侦查活动中保障公民通信秘密宪法权利的一般表现

《中华人民共和国宪法》（以下简称《宪法》）第 40 条规定：“除因国家安全或者追查刑事犯罪的需要，由公安机关或者检察机关依照法律规定的程序对通信进行检查外，任何组织或者个人不得以任何理由侵犯公民的通信自由和通信秘密。”《中华人民共和国刑事诉讼法》（以下简称《刑事诉讼法》）第 143 条规定：“侦查人员认为需要扣押被告人的邮件、电报的时候，经公安机关或者人民检察院批准，即可通知邮电机关将有关邮件电报扣押，不需要扣押的时候，应即通知邮电机关。”可见在规范层面并不缺乏对公民通信相关权利的保护性规定。

立法背后的深层次原因主要有两点：其一，侦查的保障功能所要求。侦查的保障功能要求侦查人员在侦查活动中要保护国家、集体和个人的合法权益，而公民的通信秘密权利作为公民的基本权利，在侦查活动中应当受到保护。诚然在某些情况下限制公民的通信秘密权利是打击犯罪、维护社会稳定的有效手段，但是此种权利限制应当是有条件的、有限度的，并且权利的限制并不意味着权利能够被任意侵犯；其二，通信秘密权自身的特点所决定。通信秘密权利本身具有抽象性和模糊性的特点，又在某种程度上与隐私权相竞合，在侦查实践中极易被侦查人员所忽视。侦查人员为了实现快速打击犯罪的目的，极有可能在电子侦查活动中逾越《宪法》《刑事诉讼法》等对公民通信秘密权利保障的规定。因此，对公民通信秘密权利的保护应当持更加审慎的态度，将公民通信秘密权利保障置于更加重要的地位必然是未来电子侦查活动发展的趋势。

### （二）电子侦查取证中公民通信秘密宪法权利的全新内涵

通信是公民参与社会生活，进行交流的必要手段[4]。宪法学界传统的观点认为通信秘密是指公民通过书信、电话、电报、传真、邮件、电子邮件等现代通讯方式表达其意愿，不得被非法扣押、隐匿、拆阅、录音、窃听或采取其他方式获取其内容。然而日益庞大的通信需求远远超过了传统通信可及的速度和承载量[5]。

---

［1］潘金贵，李国华．我国电子数据收集提取措施对基本权利的干预与立法完善［J］．湖南社会科学，2019，5：71–78.

［2］梁坤．论初查中收集电子数据的法律规制：兼与龙宗智、谢登科商榷［J］．中国刑事法志，2020，1：39–57.

［3］谢登科．刑事电子数据取证的基本权利干预：基于六个典型案例的分析［J］．人权，2021，1：72–88.

［4］《宪法学》编写组．宪法学［M］．北京：北京法律出版社，2011：224–225.

［5］帅奕男．基本权利“新样态”的宪法保障：以互联网时代公民通信自由权为例［J］．法学评论，2018，6：116.

因此，无论是通信秘密的载体、通信秘密的相关资料还是通信秘密表现形式都需要在电子侦查中进一步完善。首先，通信秘密载体的内涵需要完善。传统的通信秘密载体主要包括纸张、电话、传呼机、汇款单等，而当前通信秘密载体呈现出多样化的特点。智能手机、电脑、平板电脑等电子设备作为现代通信载体，为公民搭建了一个私人通信空间，通过电子设备进行表达交流已经成为公民生活的重要部分。其次，通信秘密相关资料的内涵需要完善。随着通信技术的变革，通信秘密的相关资料范围更加广泛，传统的相关资料已经不能完整反映通信秘密的相关情况。传统的通信秘密相关资料包括邮编、收件人、发件人、通信地址、邮戳时间、主叫号码、被叫号码、联系时间、地点、次数、电子邮件网址、IP 地址等[1]。而现在通信秘密相关资料还包括通信工具的固件版本型号、通信工具存储器、MAC 码、短信储存位置号等。再次，通信秘密表现形式的内涵需要完善。传统的通信秘密大多以文字或语言呈现，侦查机关非经法定程序不得对这些内容进行检查、获取。而在当今社会，通信秘密的表现形式已经从传统的纸张文字演变为数据形式，通信工具也不仅只有通信功能，混杂的海量数据使得侦查机关是否侵犯了公民的通信秘密权利变得难以辨别。

综上，无论是传统侦查活动中对公民通信秘密权利保护方式，还是针对电子数据取证的特殊性构建的新型保护形式，都需要基于现实状况不断修正完善，在这种多重变化的促使下，公民的通信秘密权利势必得到全新保护。

## 三、电子侦查取证对公民通信秘密宪法权利的突出挑战

通过分析《电子数据规定》《电子数据取证规则》等现有的规范性法律文件可知，当前电子侦查取证常用的方式主要包括三种：电子数据与储存介质的一体化收集、网络远程勘验以及第三方协助取证。这些取证方式能够为侦查机关快速有效地收集电子数据提供便利，也极易侵犯公民的通信秘密权利，以下便分别从这三个方面展开论述。

### （一）“一体化收集”模式中的挑战

《公安机关办理刑事案件电子数据取证规则》第 7 条明确规定电子数据与储存介质的收集方法主要有五种。扣押封存原始储存介质和现场提取电子数据是实践中比较常用的收集方法。有学者基于电子数据的特性，从取证主体的视角出发，将电子数据收集方法总结为两种，即“一体收集”模式和“单独提取”模式[2]。从现实情况来看，“一体化收集模式”具有不可替代的优越性。一方面，这种取证模式符合最佳证据规则的基本精神[3]，能最大限度地保证电子数据的真实性。另一方面，该模式符合当前电子侦查取证活动的实际情况。目前大部分侦查人员缺乏相关专业技能，“一体收集模式”能够降低载体中的原始证据毁损灭失的风险，弥补侦查人员的技能缺失。当前电子数据取证的相关规范性文件，均要求以扣押、封存原始储存介质为原则，如表 1 所示。

表 1　规范性文件中对于扣押、封存原始存储介质的规定

| | |
|---|---|
| 2016 年“两高一部”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》 | 第 8 条：“收集、提取电子数据，能够扣押电子数据原始存储介质的，应当扣押、封存原始存储介质，并制作笔录，记录原始存储介质的封存状态。” |
| 2019 年公安部发布的《公安机关办理刑事案件电子数据取证规则》 | 第 10 条：“在侦查活动中发现的可以证明犯罪嫌疑人有罪或者无罪、罪轻或者罪重的电子数据，能够扣押原始存储介质的，应当扣押、封存原始存储介质，并制作笔录，记录原始存储介质的封存状态。” |
| 2020 年公安部发布的《公安机关办理刑事案件程序规定》（修正版） | 第 66 条：“收集、调取电子数据，能够扣押电子数据原始存储介质的，应当扣押原始存储介质，并制作笔录、予以封存。” |

但是，一体化收集模式的应用也滋生了侦查机关侵犯公民的通信秘密权利的现象。在“北京比特时代科技有限公司申请湖南省长沙市望城区公安局刑事违法扣押国家赔偿案”[4]中，为了快速有效地获取证据，侦查人员将载体全部予以扣押，忽视了载体与案件之间的关联性。具体而言，一体化收

[1] 周伟．通信自由与通信秘密的保护问题［J］．法学，2006，6：59.

[2] 谢登科．电子数据的取证主体：合法性与合技术性之间［J］．环球法律评论，2018，1：85.

[3] 谢登科．电子数据的鉴真问题［J］．国家检察官学院学报，2017，5：57.

[4] 详见最高人民法院网站，http://www.court.gov.cn/zixun-xiangqing-211061.html.

集可能对于公民通信秘密权利的侵犯主要体现在以下两个方面。

其一，一体化收集模式的使用使公民丧失了通信秘密的阵地。当前手机、电脑等通信工具已成为公民自由表达意志和接收信息的重要途径，其所发挥的作用和带来的意义已不是传统邮件、电报所能比拟的。根据刘品信教授的电子数据“场”理论，公民的电子通信工具实质上是由电子数据所构成的私密空间。手机、电脑等通信工具除了“物”的财产价值外，还承载着诸多公民基本权利，公民的个人情感信息、个人行动轨迹等敏感信息亦寓存其中。侦查机关“一刀切”扣押电子数据载体的行为，为后续窥测公民私人空间提供了便利，不仅犯罪嫌疑人的私人通信空间遭到践踏，其他不特定公民的私人空间也有受到侵犯的可能。因此，侦查机关在采取对手机刑事扣押措施时，应更加严格地遵循比例原则。

其二，一体化收集模式的法律规定忽视公民通信秘密权利。一体化收集模式未设定明确的审批程序，在某种程度上体现出电子数据取证规范独立于《刑事诉讼法》的立法意图[1]。以扣押原始储存介质为例，基于通信秘密权利的保障，《刑事诉讼法》第 134 条规定，侦查人员扣押犯罪嫌疑人的邮件、电报，需经公安机关或者人民检察院批准。而扣押以电子通信工具为代表的原始储存介质则没有法定的审批程序。但是随着通信技术的快速发展，公民的通信工具也发生了翻天覆地的变化。邮件、电报、传呼机、汇款单等传统的通讯方式已经被智能手机、平板电脑等电子设备所取代，通过手机、平板移动智能终端进行移动通信表已经成为公民日常通信活动的必然选择。由此可见，侦查中扣押犯罪嫌疑人的电子通信工具设备与扣押邮件、电报，两者之间并无实质性区别。据此，侦查中扣押移动电子通信工具也应当受到审批程序的制约。当前相关规范未明确一体化收集模式中的程序规制，实质上是对公民通信秘密权利保护的忽视。

综上，一体收集模式确实是当前电子侦查中收集电子数据的最直接、有效的方式。但是在一体收集的过程中，是否对于所有类型的电子数据载体的扣押都采取同等程度的程序规制，值得进一步商榷。当前侦查中的扣押活动的启动，多以发现案件的事实真相、提高刑事诉讼的效率为基点，很大程度上脱离了宪法对于侦查行为的控制。笔者认为未来电子数据扣押活动应当更多考虑宪法中公民基本权利的相关规定，侦查活动应当受到宪法的规制。

### （二）网络远程勘验中的挑战

犯罪分子的犯罪手段在升级，部分传统的侦查措施已经不能适应当前打击犯罪的需要，以网络和信息技术为依托的远程侦查措施应运而生。网络远程勘验作为一种新型的远程侦查措施，已经成为侦查机关侦破案件的有力武器。其不仅在很大程度上提高了侦查机关收集证据的能力，而且对当前电子侦查实践中犯罪空间虚拟化、远程储存介质难以提取电子数据等问题作出了有效回应。

但与此同时，网络远程勘验也是一把双刃剑，极易侵犯公民的通信秘密权利。在“张某、陈某等侵犯公民个人信息罪”[2]一案中，侦查机关对陈某的 QQ 邮箱进行网络远程勘验后，发现公民个人信息共 10566 条。此时，侦查机关的行为可能会对公民的通信秘密权利构成威胁。为此，笔者主要从两个方面进行分析。

其一，以网络远程勘验替代远程搜查使公民通信秘密权利失去程序保护。虽然当前远程搜查措施并未纳入电子数据规范体系之中，但是从本案例中可以看出，远程搜查措施在电子侦查过程中仍被使用。从当前刑事诉讼法律规范来看，远程搜查与远程勘验有着不同的程序规制。远程搜查措施作为传统搜查措施在虚拟空间的延伸，被普遍认为是一种强制性侦查措施，应适用刑事诉讼法中有关搜查的程序。在现有的电子数据规范体系之下，网络远程勘验有两种实施方式。一种是常规方式的网络远程勘验，另一种是技术侦查方式的网络远程勘验[3]。就常规方式的网络远程勘验而言，其实践中的程序适用与现场勘验一致。而网

---

［1］龙宗智．寻求有效取证与保证权利的平衡：评“两高一部”电子数据证据规定［J］．法学，2016，11：12.

［2］广东省茂名市中级人民法院（2019）粤09刑终82号刑事判决书，案例检索自中国裁判文书网。

［3］《公安机关办理刑事案件取证规则》第33条规定：网络在线提取或者网络远程勘验时，应当使用电子数据持有人、网络服务提供者提供的用户名、密码等远程计算机信息系统访问权限。采用技术侦查措施收集电子数据的，应当严格依照有关规定办理批准手续。收集的电子数据在诉讼中作为证据使用时，应当依照刑事诉讼法第145条规定执行。

络远程勘验作为一种涉及网络攻防的侦查措施，其法律性质不应以传统的任意侦查理论为依据进行简单划分，应结合比例原则对其法律性质进行重新认定。实践中侦查人员以网络远程勘验替代远程搜查，此时的网络远程勘验并非技术侦查方式的网络远程勘验，仅仅是简单的网络攻防行为。此时侦查人员实际上通过任意性侦查措施的程序，实施了强制性侦查措施，公民的基本权利就此失去了程序保护屏障。就本案而言，侦查人员对陈某的 QQ 邮箱进行网络远程勘验，实质上是一种远程搜查的行为，尤其是 QQ 邮箱作为公民常用的通信工具，涵盖了大量的公民通信秘密信息。

其二，网络远程勘验与技术侦查界限模糊使公民通信秘密权利失去程序保护。在上述案例中，侦查人员在对犯罪嫌疑人 QQ 邮箱进行远程勘验时，并未获得相应的授权，此时侦查人员的行为应当属于技术侦查方式的网络远程勘验，需要经过严格的审批手续。但是，技术侦查方式的网络远程勘验与技术侦查有何区别？技术侦查方式的远程勘验与常规方式的远程勘验界限何在？这些问题无论从法条还是实践来看，没有明确的规定。这种概括式表述的技术指引规范就导致查人员在实践中避重就轻，为了减少程序的限制，以常规网络远程勘验的名义，大量运用技术侦查的方式实施网络远程勘验。此时，侦查机关的行为虽然名义上实施的是网络远程勘验行为，但实质上很有可能实施的是技术侦查行为。相关法规为保障公民基本权利而设置的程序性保护屏障在这一过程中遭到忽视，电子侦查取证中的公民通信秘密权利也同样失去了程序保护。

综上，侦查人员滥用网络远程勘验的行为有侵犯公民通信秘密权利之嫌，无论是以网络远程勘验替代远程搜查，还是以普通方式的网络远程勘验代替技术侦查方式的网络远程勘验，侦查人员都可能对公民的通信秘密权利构成侵犯。因此，相关法律规范应进一步确定网络远程勘验的法律性质，明确网络远程勘验与技术侦查措施之间的界限，以防实践中出现侦查机关错误使用网络远程勘验的侦查行为。

### （三）第三方协助取证中的挑战

当前电子数据已成为人工智能和网络信息时代的“证据之王”，大量传统实物证据通过信息技术而转化为电子数据[1]。这些数据不仅数量多、类型复杂，而且难以进行有效地识别与筛选，这就对侦查人员提出了更高的技术要求。而第三方具有数据与技术的双重优势，能够最大程度地弥补当前侦查机关在电子侦查取证活动中所面临的短板。通过第三方协助的方式进行取证，能够使侦查机关避开与侦查相对人的直接冲突[2]。

然而，实践中侦查机关委托第三方取证实质上逾越了第三方协助取证的限度，可能会侵犯公民的通信秘密权。囿于侦查机关本身技术力量相对薄弱等因素的影响，部分侦查机关在电子侦查取证活动中选择将一些取证活动交由鉴定人或者第三方科技公司进行，这种行为严重违反了《刑事诉讼法》的规定和行使侦查权的相关原则。在“周灵苹组织、领导传销活动罪”[3]一案中，上诉人周灵苹及其辩护人提出：“鉴定检材系由公安机关委托鉴定人员提取，而非由侦查机关依法提取，电子证据的取证程序违法。”虽然法院最终认定电子证据取证程序合法，但侦查机关的行为仍对公民通信秘密权利的保障产生了消极影响，主要有以下两个原因。

其一，委托第三方取证忽视了侦查权不可让渡的原则。首先，从取证主体角度而言，第三方鉴定人和科技公司不具备取证主体资格。刑事诉讼法明确规定了行使侦查权的主体，其中并无鉴定人员和科技公司。侦查人员与鉴定人、科技公司是三个独立的身份，侦查人员取证与委托鉴定人进行鉴定、委托科技公司代为取证，也应该是三个独立的行为。其次，从功能定位而言，第三方鉴定人和科技公司不具备独立取证的资质。结合《刑事诉讼法》第 128 条和第 308 条规定也可以看出，第三方鉴定人和科技公司在被侦查机关委托鉴定或者指派、聘请勘验检查的过程中，并不具备单独进行电子数据证资质。最后，从职责权限而言，第三方鉴定人和科技公司不具备单独取证的权限。侦查权是一种特殊的权力。侦查人员在实施侦查权的过程中，不仅不得委托、

---

［1］胡铭．电子数据在刑事证据体系中的定位与审查判断规则：基于网络假货犯罪案件裁判文书的分析［J］．法学研究，2019，2：174.

［2］裴炜．论个人信息的刑事调取：以网络信息业者协助刑事侦查为视角［J］．法律科学（西北政法大学学报），2021，3：80.

［3］详见四川省雅安市中级人民法院（2019）川18刑终39号刑事判决书，案例检索自中国裁判文书网。

转让和放弃，同时还要保证侦查权的实施受到内部制约和外部制约[1]。超越限度委托第三方鉴定人取证，使得侦查权力的制约出现了现实的缺口。而第三方鉴定人在电子侦查取证中又难以受到法规的制约，长此以往现实缺口将会越来越大，这为证据的保全和公民通信秘密权利的保护埋下了隐患。

其二，第三方协助取证难以实现合法性与技术性相契合。在案例三中，侦查机关将相关检材的提取交予第三方鉴定人执行，难以实现取证的合法性和合技术性相契合。从合法性角度来看，鉴定人和科技公司虽然在取证技术方面拥有巨大优势，但是其获取检材来源的合法性，必然会受到质疑；从技术性的角度来看，由于鉴定人和科技公司的取证行为很难受到相关法律的规制，鉴定人和科技公司为了快速获取鉴定检材和相关证据材料，极有可能最大程度地发挥自己的技术优势。这种情况下，公民的通信秘密信息非常容易被第三方鉴定人或科技公司获取，公民的通信秘密权利难以在这一过程中获得有效保护。

综上，虽然宪法规定在刑事案件办理的过程当中可以对公民的通信秘密权利进行限制，但是限制的主体仅有公安机关和检察机关，并没有被委托的第三方。第三方协助取证的核心在于“协助”二字，侦查机关委托第三方单独取证的行为使得公民的通信内容、通信时间、通信方式等完全暴露于第三方取证人员的视野之下，这显然已远远超过了法律和公民内心期待的必要限度，违反了宪法的核心理念。据此，相关法律规范应当明确第三方在侦查活动中的法律地位。具体而言，根据打击犯罪与保护人权的双重需要，应赋予在侦查人员主持下，第三方协助取证行为的合法性。

## 四、比例原则下的公民通信秘密宪法权利保护之展望

判断一项限制或侵犯此类基本权利的公权行为是否具有正当性，核心在于衡平赋权与限权背后的社会价值，而这正是比例原则介入并发挥功能的领域[2]。比例原则也同样应当在电子侦查取证活动中发挥作用。据此，有学者提出在电子取证过程中，应区分“重要数据与非重要数据，对数据进行分类、分层级保护”[3]。笔者认为这一理念虽在数据安全保护方面具有重要的指导意义，但对于电子侦查实践中公民通信秘密宪法权利的保护很难发挥实质性作用。为此，笔者以比例原则为内核，以数据秘密性为区分标准，在将不同种类的通信数据进行层级区分的基础之上，再以此为依据针对不同性质的案件选择适当的侦查手段，尝试构建“数据层级区分 + 案件层级区分”的取证模式，以期成为电子侦查取证中保护公民通信秘密宪法权利的有效方法。

### （一）数据层级区分：不同种类通信秘密数据的分类分级

明确电子侦查取证中通信秘密的界限是保护公民通信秘密宪法权利的前提条件。2021 年最高人民检察院发布的《人民检察院办理网络犯罪案件规定》第 27 条第 1 款较为全面地列举了电子数据的表现形式，其中不乏与通信秘密相关的电子数据表现形式。本文以此为依据，对涉及通信秘密权利的电子数据表现形式，进行了简单的层级区分，如表 2 所示。

表 2　对涉及通信秘密电子数据表现形式的层级区分

| 保护标准 / 表现形式 | 低度保护标准 | 中等保护标准 | 严格保护标准 |
|---|---|---|---|
| 手机短信、电子邮件 | 发件人姓名、收件姓名、地址等 | 联系方式 | 短信、邮件内容 |
| 电子通信记录 | 开户资料，如姓名、电话号码等 | 通话时间、通话频次等 | 通话内容 |
| 即时通信 | QQ、微信号码、各 APP 登录信息等 | 好友、朋友圈内容等 | 交流记录 |
| 通讯组群 | 群组基本信息、设立目的等 | 群组成员信息等 | 通讯记录 |

［1］内部制约包括通过侦查机关内部上级对侦查权主体的领导关系和通过同级侦查主体优化侦查权配置两方面来对于侦查权主体运用侦查权实施的侦查活动进行制约。外部制约一方面，通过外界权力进行制约，如检察院规范侦查权主体的义务和义务来制约侦查权。另一方面，通过权力进行制约。如通过广泛分配权力。优化权力机构和优化救济途径的方式来对于侦查主体实施侦查权进行制约。

［2］裴炜．比例原则视域下电子侦查取证程序性规则构建［J］．环球法律评论，2017，1：81–82.

［3］梁坤．以分级分类为指引落实数据调取程序［N］．检察日报，2021–07–14（3）.

涉及通信秘密的电子数据表现形式层级区分，主要根据以下三个标准。

（1）首要标准——是否公开。通信秘密权利是公民期望在进行自由的通信交流的过程中不被第三方知晓、刺探的权利，“秘密性”是其最本质的特点[1]。如果侦查人员在侦查过程中发现相关的通信信息是公开的，便可以确定这部分的信息不属于通信秘密权利的保护范围，如网页、社交平台、论坛等网络平台发布的信息，即使这些信息对于案件的侦破有着重要意义，也不能将其划归到通信秘密当中。

（2）重要标准——敏感程度。所有通信秘密都具有一定的敏感性，应当根据不同敏感程度区别对待。对于敏感度的区分主要参考以下几点：第一，通信秘密的量级。信息量越大，通信秘密内容就越广泛，敏感程度也会随之提升。例如，电子邮件的具体内容的敏感程度要高于发件人姓名；第二，信息披露的自愿程度[2]。这主要用以区分低度保护标准和中度保护标准。例如，在电子通信记录信息中，相较于通话时间和通话批次，公民更愿意披露电话号码和通信对象；第三，社会共识。除朋友圈内容等有争议的通信秘密外[3]，其他通信秘密以社会共识作为敏感度划分标准，符合公民的普遍认知。例如，当前社会普遍认为相较于通话次数、时间，通话内容的敏感程度更高。

（3）附属标准——与案件的关联程度。通信秘密在电子侦查取证过程中，大多以海量数据的形式出现，在部分通信秘密的敏感程度难以判断的情况下，将其与案件的关联程度作为通信秘密层级划分的附属标准具有重要意义。与案件关联程度高的通信秘密信息，往往会受到侦查人员的重视，得到更好的保护，反之，与案件关联程度低的通信秘密信息，则易受到侦查人员的忽视。因此，对于与案件关联程度较低的通信秘密信息，侦查人员应当保持更加审慎的态度，其保护标准就应当越高。

根据以上标准，对于通信过程中的通信秘密可进一步划分，如表3所示。

表3　通信秘密表现形式的层级区分

| 通信秘密保护标准 | 表现形式 | 是否公开 | 敏感程度 | 相关性 |
|---|---|---|---|---|
| 低度保护标准 | 发件人姓名、收件姓名、地址、开户资料、QQ、微信号码、各APP登录信息、群组基本信息、设立目的等 | 否 | 低敏感程度 | 根据具体案件判断 |
| 中度保护标准 | 联系方式、通话对象、通话时间、通话频次、好友、朋友圈内容群组成员信息等 | 否 | 中度敏感程度 | 根据具体案件判断 |
| 高度保护标准 | 短信、邮件内容、通话内容、交流记录、通讯记录等 | 否 | 高度敏感程度 | 根据具体案件判断 |

综上，在电子侦查取证实践中，侦查机关忽视载体的关联性进行扣押、随意启动网络远程勘验、以技术性侦查措施代替网络远程勘验、委托第三方代为取证等行为，可能使低度、中度和高度保护标准的通信秘密存在被侵犯的风险。因此，侦查机关需要对通信秘密进行区分处理，再根据办案需要对不同保护标准的通信秘密进行不同程度的干预。这既符合《宪法》和《刑事诉讼法》赋予侦查机关合理干预通信秘密的法律规定，同时又能给予公民通信秘密宪法权利最大程度地保护。

### （二）案件层级区分：通信秘密分层保护下案件类型化区分

通过前文可知，无论何种性质的案件，对于最低度保护的通信秘密都可以进行适当干预。但是，是否任何刑事案件都可以对中度保护标准和高度保护标准的通信秘密进行干预？是否所有的案件干预的标准都是一致的？答案显然是否定的。笔者基于通信秘密分层保护标准，以保障电子侦查取证实践中的公民通信秘密权利为目的，对刑事案件做了进一步的类型化区分，主要依据以下三个标准进行划分。

（1）基本标准——参考传统刑事案件分类。新技术的发展并未推动刑事案件的种类并发生根本性的变化，“国、恐、黑、毒”仍然是当前刑事司法治理领域的重点案件。根据2018年《中国法

［1］张新宝．个人信息收集：告知同意原则适用的限制［J］．比较法研究，2019，6：4.

［2］王仲羊．科技定位侦查与隐私权的层级保护：以美国Carpenter案为视［J］．河北法学，2021，3：178.

［3］朋友圈内容是否属于通信秘密目前仍属于争议问题。笔者认为公民朋友圈内容的公开的对象仅是公民的好友，是特定人群的公开，而这部分特定人群不应包括案件办理中的侦查机关的侦查人员。因此，在电子取证过程中，公民朋友圈的内容也应当认定为公民的通信秘密。

律年鉴》，“杀人、抢劫、走私、绑架、盗窃、拐卖妇女儿童、强奸、伤害”等传统刑事犯罪仍占比66.62%，打击传统犯罪的形势依然严峻。因此，将传统刑事案件作为分类的基本标准，结合新型案件的犯罪情况进行类型化区分具备一定的合理性。

（2）现实标准——刑事案件治理现状。受新冠疫情的影响，以电信网络诈骗、网络赌博为代表的严重网络犯罪在疯狂蔓延，已经严重影响到了正常的社会秩序。《人民检察院办理网络犯罪案件规定》第 2 条规定，当前网络犯罪主要有三类，包括针对信息网络实施的犯罪、利用信息网络实施的犯罪以及其他上下游关联犯罪。以网络电信诈骗案件为例，2020 年，全国公安机关共破获电信网络诈骗案件 32.2 万起，抓获犯罪嫌疑人 36.1 万名，打掉涉“两卡”违法犯罪团伙 1.1 万个，封堵涉诈域名网址 160 万个[1]。因此，在严重的网络犯罪案件侦破过程中，应结合刑事案件治理现状和刑事政策，赋予侦查机关更高强度的通信秘密干预权利。

（3）辅助标准——刑事案件实际情况。电子侦查取证过程不可能处于理想化环境，侦查人员的能力水平、电子数据的取证环境、案件的社会影响力等因素决定了案件的类型化区分不能僵化，必须要结合案件具体情况作出判断，这样才能增加案件类型化区分在实践中应用的灵活度。但若将做出判断的权力交由侦查机关，极有可能会使案件类型化区分在侦查实践中产生异化；若由检察机关就侦查机关是否能干预某一程度的通信秘密进行审查决定，能够在一定程度上避免侦查机关“既当运动员又当裁判员”的情况出现。当然，检察院在进行审查决定时，同样需要将刑事案件的实际情况作为案件类型化区分的辅助标准。

根据以上标准，可将刑事案件类型进一步划分，如表 4 所示。

表 4　通信秘密分层区分标准下的刑事案件类型化区分

| 通信秘密标准案件类型 | 低度保护标准通信秘密 | 中等保护标准通信秘密 | 严格保护标准通信秘密 |
| --- | --- | --- | --- |
| 危害国家安全犯罪、恐怖活动犯罪、黑社会性质组织犯罪、重大毒品犯罪、严重网络犯罪或者其他严重危害社会的案件 | 可干预 | 可干预 | 可干预 |
| 八类主要刑事案件（故意杀人、故意伤害致人重伤或者死亡、强奸、抢劫、贩卖毒品、放火、爆炸、投放危险物质罪）以及刑事案件治理热点问题 | 可干预 | 可干预 | 结合案件实际情况 |
| 以盗窃、走私等传统犯罪为代表的其他案件 | 可干预 | 结合案件实际情况 | 结合案件实际情况 |

需要注意的是，上述所构建的电子侦查取证中通信秘密宪法权利保护模型并非严格适用的模型。除了通信数据分级、案件类型化区分以外，还需考虑到相对人的主观意愿。根据刑事诉讼“同意”理论，如果相对人自愿配合侦查，同意将秘密性较高的通信数据进行披露，那么对于此类通信数据的保护程度和干预程度侦查机关也可以做出相应的调整。相对人自愿披露的情况应当记录在相关笔录之中，或者有见证人在场，抑或者进行录音录像。

## 五、结语

犯罪分子利用新技术更新犯罪手段，侦查机关运用新技术打击新型犯罪，在这场博弈中最大的权益损失者无疑是普通公民，如果不为侦查机关设置一定的限度，公民的通信秘密权利必然受到践踏。当然，在当前的犯罪形势下，一味地呼吁保护权利并不是最佳选择。习近平总书记对打击治理电信网络诈骗犯罪工作作出了重要指示，“要坚持以人民为中心，全面落实打防管措施，坚决遏制电信网络诈骗犯罪的多高发态势。宪法的外部限制也表明根据公共利益的需要可以对权利加以限制”[2]。因此，侦查机关在电子侦查取证活动中划分对公民的基本权利干预的限度边界时，应当力求在发挥最大社会效益的基础上进行价值选择。总之，信息化时代的到来加剧了公权力与私权利之间的冲突，惩罚犯罪与保障人权之间的平衡问题更需要深层次的探索与研究。

（责任编辑：彭　曦）

［1］中国防伪报道编辑部．严防狠打电诈犯罪，切实保障人民利益，公安部部署深入推进打击防范电信网络诈骗犯罪工作［J］．中国防伪报道，2021，3：9.

［2］习近平对打击治理电信网络诈骗犯罪工作作出重要指示强调 坚持以人民为中心 全面落实打防管控措施 坚决遏制电信网络诈骗犯罪多发高发态势 李克强作出批示［J］．中国刑事警察，2021，2：2.

# Challenges and Prospects: Constitutional Protection of Citizens' Communication Secrets in Electronic Investigation Evidence Collection

Ye Xiangyu

*Southwest University of Political Science and Law, Chongqing*

**Abstract:** The application of current technical means plays an important role in case investigation, and the ensuing problem of protecting the basic rights of citizens has become more and more apparent. It is urgent to solve the constitutional rights protection of citizens' communication secrets in the process of electronic investigation and evidence collection.The crux of the problem lies in the fact that although the application of new technology has a positive impact on the investigation of the case of the investigating organs, the investigation organs have failed to grasp the connotation of communication secrets accurately in the course of electronic data forensics, which makes it difficult for the investigating organs to achieve a difficult breakthrough in the balance between punishing crime and the guarantee of the secret constitutional rights of citizens' communications. By exposing the reality of violating the secret of citizens' communication in the process of electronic investigation and evidence collection, and under the guidance of the principle of proportionality, the case is typed according to the distinction between the levels of communication secrets, with a view to providing an effective solution to the problem of the protection of citizens' communication secret rights in the electronic investigation and evidence-gathering activities of the investigation organs.

**Key words:** Electronic investigation; Communication secrets; Constitutional regulation; Principle of proportionality