主题研讨

论电子通讯数据搜查、扣押的制度建构

陈永生

内容提要：由于电子通讯数据包含的内容非常丰富，因而为防止侦查机关滥用权力侵犯公民个人隐私权，域外国家、地区普遍对电子通讯数据的搜查、扣押作出了特别规定。搜查、扣押电子通讯数据的条件通常高于搜查、扣押普通信件，必须遵循比例原则的要求。侦查人员在搜查、扣押电子通讯数据过程中有权要求相关人员提供协助，应当尽可能将电子通讯数据转换为书面或其他可以直接识别的形式，必须将原始存储介质予以封存，与案件无关的以及诉讼不再需要的信息必须及时删除、销毁。辩护律师有权在侦查机关搜查、扣押电子通讯数据时在场，搜查、扣押电子通讯数据完毕应当及时告知犯罪嫌疑人及相关人员，犯罪嫌疑人及其辩护人有权了解、查阅被搜查、扣押的电子通讯数据的内容，采用非法手段收集的电子通讯数据必须予以排除。

关键词：电子通讯数据　原始存储介质　搜查　扣押　非法证据排除

陈永生，北京大学法学院院聘教授。

电子数据与传统实物证据在物质载体方面存在重大差别。传统实物证据以物品、文书等实物为载体，侦查人员通常可以通过感官直接感知，并且传统实物证据承载的信息量非常有限，因而搜查、扣押的内容是否与案件有关一般不难判断，也因此，搜查、扣押的范围一般不难确定。电子数据以电子介质作为信息载体，侦查人员很难直接获知电子数据的具体内容；同时，随着信息技术的发展，电脑、手机等电子设备的功能及存储容量越来越强大，侦查人员在对电脑、手机等电子数据进行搜查、扣押时，能够接触的信息非常广泛，不仅可能接触到与案件有关的信息，而且可能接触到与案件无关的信息；不仅可能接触到与犯罪嫌疑人有关的信息，而且可能接触到与犯罪嫌疑人的家人、亲友有关的信息，如果不对搜查、扣押的范围作出严格限定，极易导致侵犯公民个人隐私权的情况发生。因此，自上世纪末以来，许多国家、地区，尤其是法治发达的国家、地区普遍对刑事诉讼法进行了修改，对搜查、扣押电子数据，尤其是搜查、扣押电子通讯数据作出了特别规定。

然而，我国《刑事诉讼法》对搜查、扣押电子数据的规定一直滞后于时代的发展。我

国 1979 年以及 1996 年《刑事诉讼法》都没有对电子数据作出任何规定。2012 年修正的《刑事诉讼法》虽然将电子数据增列为法定证据的一种,但是对电子数据的搜查、扣押没有作出任何特别规定。2018 年修订的《刑事诉讼法》对电子数据的搜查、扣押也没有作出任何特别规定。法学理论界对电子数据,尤其是电子通讯数据搜查、扣押的研究也严重滞后,因此本文试图对电子通讯数据搜查、扣押的制度建构进行深入研究。

一 电子通讯数据搜查、扣押立法的必要性

由于对电子数据,尤其是对电子通讯数据进行搜查、扣押可能严重侵犯公民权利,尤其是隐私权,因而域外国家和地区,特别是法治发达的国家和地区普遍通过立法或判例对搜查、扣押电子数据,尤其是电子通讯数据作出特别规定。

英国最早对搜查、扣押电子数据作出规定。英国 1984 年通过的《警察与刑事证据法》就对搜查、扣押电子数据作出了规定。该法第 19 条第 4 款规定,对于存储于计算机之中且在该场所里即可获取的任何信息,警察如果有合理的理由相信,该信息是与其正在侦查的某一犯罪或其他任何犯罪有关的证据,或者是因为实施某一犯罪而取得的证据,并且对于防止该证据被藏匿、遗失、损坏或者毁灭确有必要,可以要求将其制作成有形且可读的、能被带走的形式,予以扣押。〔1〕

美国早在 20 世纪末就开始探索电子数据搜查、扣押的法律规制问题,提出了电子数据搜查、扣押的“二阶段搜索模式”(two-stage searching approach)规则。〔2〕 根据该规则,传统的搜查、扣押属“一阶段搜索模式”(one-stage searching approach):侦查人员在犯罪现场发现可能与案件有关的证据后,通常当场就能依靠自己的感官,判断该证据能否证明案件事实、能够证明哪些案件事实。而对电子数据的搜查、扣押通常无法在犯罪现场一次完成。由于查阅电子存储介质中的电子信息往往必须借助一定的电子设备,而犯罪现场不一定有相应的设备;并且电子设备中包含的信息量可能非常大,搜索、检查需要的时间可能很长,因而现场通常只能对电子存储介质进行扣押,并对电子存储介质的外部特征进行检查;将电子存储介质运回侦查机关办案场所以后,才能对电子存储介质中电子信息的具体内容进行搜索、检查。早在 1995 年,美国法院判例就要求,在扣押电子存储介质以后,如果需要对电子存储介质中的电子数据进行搜查,那么在向法官申请搜查令时必须说明意图搜查的电子数据内容和具体特征。在执行搜查时,只能对可能与案件有关的信息进行搜查;对显然与案件无关的信息不得进行搜查。如果在搜查过程中发现了涉嫌新的罪行的证据,必须重新就新的罪行向法官申请签发搜查令;反之,如果没有向法官重新申请签发令状,那么收集的证据必须被排除。〔3〕

德国国会于 2013 年 6 月 20 日对《电信通讯法》以及相关法律,包括《刑事诉讼法》进

〔1〕 参见英国《1984 年警察与刑事证据法》,陈瑞华等译,载中国政法大学刑事法律研究中心编译:《英国刑事诉讼法(选编)》,中国政法大学出版社 2001 年版,第 266 页。

〔2〕 参见李荣耕:《电磁数据的搜索及扣押》,《台大法学论丛》2012 年第 3 期,第 1060 – 1064 页。

〔3〕 参见陈永生:《电子数据搜查、扣押的法律规制》,《现代法学》2014 年第 5 期,第 117 页。

行了修改,对执法机关获取电信通讯数据作出了规定。根据修正以后的《刑事诉讼法》第100条j的规定,只有对查清案情或者犯罪嫌疑人确有必要,经检察机关申请,法院批准,侦查人员才可以要求提供或参与提供电讯服务的人员,依照《电信通讯法》第95条、第111条的规定,提供所保存的与犯罪有关的基本通讯信息,包括姓名、出生日期、住址、账户信息、IP地址、社交网络服务的密码、邮箱密码、电子书的打开密码,等等。[4]

意大利于2008年3月18日通过第48号法律对其《刑事诉讼法典》第256条、第260条、第352条、第354条等条款进行修改,并增加第254条-2,对搜查、扣押电子数据,尤其是电子通讯数据作出了全面规定。该法第254条-2规定,只有司法机关有权决定在信息、电信或电讯服务商处扣押由上述服务商持有的数据材料,包括送达的或者定位数据材料。考虑到正常提供上述服务的需要,可以决定将有关的数据材料复制在适当载体上以实现对该材料的提取,为此所采用的程序应确保被提取的数据与原始数据的一致性和不可变更性。在此情况下,命令服务商妥善保存和保护原始数据。[5]

韩国于2011年7月18日对其《刑事诉讼法典》进行修改,在第106条中增加了一款,作为第3款。该款规定,如果扣押的对象为电脑磁盘或者其他类似存储介质,法院应当指定范围,要求将该范围内的信息打印或者复制后提交,如果无法指定打印或者复制的范围,或者明显难以实现扣押的目的,可以扣押信息存储介质。[6]

俄罗斯于2010年7月1日对其《刑事诉讼法典》进行修改,增加了一条(第186-1条),对侦查人员获取电子通讯数据的适用条件、申请与审批程序、期限等作出了详细的规定。[7]

不仅发达国家普遍对搜查、扣押电子通讯数据的法律程序作出了明确规定,许多发展中国家也对搜查、扣押电子通讯数据作出了明确规定。如乌克兰早在2001年6月21日就对其《刑事诉讼法典》第187条进行了修改,并增加第187-1条,对搜查、扣押电子通讯信息作出规定。[8] 保加利亚于2010年5月28日颁布生效的《国家公报》对其《刑事诉讼法典》第159条进行了修改,对搜查、扣押计算机信息、计算机用户资料作出了规定。[9] 土库曼斯坦于2012年12月22日对其《刑事诉讼法典》第282条进行修改,对搜查、扣押电子计算机信息以及电子邮件信息作出了规定。[10]

近年来,我国智能手机发展迅猛,无论是在智能手机的普及率、人们对智能手机的依

〔4〕 参见德国《刑事诉讼法典》,宗玉琨译注,知识产权出版社2013年版,第76页。

〔5〕 参见意大利《刑事诉讼法典》,黄风译,载《世界各国刑事诉讼法》编辑委员会编译:《世界各国刑事诉讼法·欧洲卷(下)》,检察出版社2016年版,第1664页。

〔6〕 参见[韩]韩尚勋:《韩国刑事诉讼法上扣押搜查的令状主义和电子证据的证据能力》,金玫译,《私法》2016年第1期,第72页。

〔7〕 参见俄罗斯《刑事诉讼法典》第186-1条,赵路译,载《世界各国刑事诉讼法》编辑委员会编译:《世界各国刑事诉讼法·欧洲卷(上)》,检察出版社2016年版,第447页。

〔8〕 参见乌克兰《刑事诉讼法典》第187条、第187-1条,张璐译,载《世界各国刑事诉讼法》编辑委员会编译:《世界各国刑事诉讼法·欧洲卷(中)》,检察出版社2016年版,第1496-1497页。

〔9〕 参见保加利亚《刑事诉讼法典》第159条,栗峥等译,载《世界各国刑事诉讼法》编辑委员会编译:《世界各国刑事诉讼法·欧洲卷(上)》,检察出版社2016年版,第103页。

〔10〕 参见土库曼斯坦《刑事诉讼法典》第282条,赵路译,载《世界各国刑事诉讼法》编辑委员会编译:《世界各国刑事诉讼法·亚洲卷》,检察出版社2016年版,第520页。

赖程度,还是在智能手机所牵涉的隐私权的广度和深度方面,我国都与美国等发达国家不相上下,有些方面甚至超过了美国等发达国家。随着电脑、手机、网络应用的普遍化,犯罪证据也越来越多地以电子数据,尤其是电子通讯数据的形式存在。与此相应,实践中,公安司法机关也越来越广泛地通过搜查、扣押手机、电脑等电子设备来收集犯罪证据,查获犯罪事实。在许多地方,尤其是城市地区,在绝大多数案件中,侦查人员在拘留、逮捕犯罪嫌疑人以后都会通过搜查、扣押手机来查找犯罪证据。由于搜查、扣押电子数据,尤其是电子通讯数据极易导致侵犯公民隐私权以及财产权,因而我国立法部门亟需对搜查、扣押电子数据,尤其是电子通讯数据的法律程序作出严格规定,从而实现控制犯罪与保障人权的有效平衡。

如本文开头部分所述,我国 1979 年以及 1996 年《刑事诉讼法》都没有对搜查、扣押电子数据作出规定,2012 年《刑事诉讼法》虽然将电子数据增列为一种法定的证据种类,但是对搜查、扣押电子数据的条件、程序等没有作出任何特别规定。值得注意的是,有司法解释对电子数据的收集和审查判断作出了规定。最高人民法院、最高人民检察院、公安部于 2016 年 9 月 9 日联合发布的《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》(以下简称三机关《电子数据规定》)对电子数据收集与提取、移送与展示、审查与判断的程序作出了比较全面的规定。最高人民法院、最高人民检察院、公安部于 2014 年 5 月 4 日发布的《关于办理网络犯罪案件适用刑事诉讼程序若干问题的意见》(以下简称三机关《网络犯罪意见》)第四、五、六部分也对电子数据的收集与审查程序作出了规定。最高人民法院、最高人民检察院、公安部、国家安全部、司法部于 2010 年 6 月 13 日联合发布的《关于办理死刑案件审查判断证据若干问题的规定》第 29 条也对电子数据的审查判断作出了规定。最高人民法院于 2012 年 12 月 20 日发布的《关于适用〈中华人民共和国刑事诉讼法〉的解释》第 4 章第 7 节也对电子数据的审查认定作出了规定。此外,还有一些部门发布的规范性文件也对电子数据的收集与审查判断作出了规定。譬如,公安部于 2005 年发布的《计算机犯罪现场勘验与电子证据检查规则》(公信安[2005]161 号)、同年公安部发布的《公安机关电子数据鉴定规则》(公信安[2005]281 号),最高人民检察院于 2009 年发布的《电子证据鉴定程序规则(试行)》,等等。

但是,所有这些司法解释和规范性文件都有一个共同特点:都只对收集和审查电子数据的技术性规则作出规定,目的仅在于保障收集的电子数据的真实性和同一性;相反,对收集电子数据的法律程序则几乎没有规定,完全无视保护相对人的合法权利、防止公安司法人员滥用权力等问题。譬如,三机关《电子数据规定》第 2 条规定:侦查机关应当遵守法定程序,遵循有关技术标准,全面、客观、及时地收集、提取电子数据。虽然从措辞来看,该条要求侦查机关收集证据时既要遵守相关技术标准,也要遵守法定的程序,但是从该条规定的立法宗旨来看,其目的只是为了保障收集电子数据的“全面、客观、及时”,也即确保真实性,因而实质上只是强调必须遵守相关的技术性标准。并且,如前所述,由于我国《刑事诉讼法》对电子数据的收集并没有规定特别的适用条件和程序规则,这也导致该条所规定的“应当遵守法定程序”只具有形式意义,没有实质约束功能。不仅如此,三机关《电子数据规定》第 7 条规定得更加直白,只要求:“取证方法应当符合相关技术标准”,而没有要求必须遵守法定的条件和程序,这一条更直接反映出我国现行电子数据收集的法律规则

的价值取向，仅在于保障所收集的电子数据内容的真实性，而忽视程序的正当性。而搜查、扣押电子数据，尤其是电子通讯数据严重侵犯公民的隐私权、财产权，我国未来在修改刑事诉讼法时，有必要借鉴域外的成功经验，对搜查、扣押电子数据，尤其是电子通讯数据的适用条件、程序以及救济机制等作出规定，从而有效保障公民的隐私、财产等合法权利。

二　电子通讯数据搜查、扣押的适用条件

由于搜查、扣押电子数据，尤其是电子通讯数据可能直接侵犯公民个人隐私；同时，电脑、手机等电子设备包含的信息非常丰富，一旦搜查、扣押不当，将对公民个人隐私造成巨大损害，因而域外国家、地区普遍对搜查、扣押电子数据，尤其是电子通讯数据设置了严格的适用条件。

（一）域外电子通讯数据搜查、扣押适用条件的共同特点

1. 搜查、扣押电子通讯数据的条件通常高于搜查、扣押普通信件

搜查、扣押电子通讯数据对公民隐私权以及财产权的侵害通常高于搜查、扣押普通信件。

一方面，搜查、扣押电子通讯数据对公民隐私权的侵害通常高于搜查、扣押普通信件。其一，普通信件承载的信息量非常有限，搜查、扣押普通信件通常只会导致信件记载的有限内容被他人获悉，不会导致其他隐私被泄露。而电脑、手机等电子设备存储容量非常大，如果侦查人员对这些电子设备进行搜查，那么，不仅犯罪嫌疑人与他人的通讯信息会被侦查人员获知，其他与通讯无关的信息，如电脑、手机中存储的与案件无关的文档、照片、视频、日记，甚至上网记录、交易信息都可能被侦查人员所了解，因而搜查、扣押电子通讯数据对公民隐私权的侵犯是全方位的。其二，搜查、扣押普通信件通常只会导致搜查、扣押令确定时限内的信件被搜查、扣押，搜查、扣押令确定时限外的信件不会被搜查、扣押；一般只会导致犯罪嫌疑人与同案犯或其他与案件有关的人员的信件被搜查、扣押，显然与犯罪无关的信件，譬如，犯罪嫌疑人与其子女的通信一般不会被搜查、扣押。而搜查、扣押电子通讯数据则不存在这些客观限制，一旦侦查人员进入犯罪嫌疑人的电脑、手机等电子设备，打开其邮箱、QQ、微信等通讯终端进行查看，就会导致不仅犯罪嫌疑人涉嫌犯罪时段内的通讯被搜查、扣押，此前的通讯也能够被侦查人员查看；不仅犯罪嫌疑人与同案犯以及其他相关人员之间的通讯被搜查、扣押，犯罪嫌疑人完全与案件无关的通讯也可能被侦查人员查看。

另一方面，搜查、扣押电子通讯数据对公民财产权的侵害通常也高于搜查、扣押普通信件。传统信件的经济成本很低：一个信封、一张邮票、几张纸，可能只有区区数元；而搜查、扣押电子通讯数据则完全不同，由于大多数国家、地区为了保障搜查、扣押电子通讯数据内容的客观性、同一性和完整性，都要求侦查人员必须扣押手机、电脑等保存电子通讯数据的设备，而手机、电脑少则数千元，多则上万多元，经济价值是普通信件的数千倍。正因为搜查、扣押电子通讯数据对公民隐私权以及财产权的侵害程度高，所以较之于搜查、扣押普通信件，大多数国家、地区都对搜查、扣押电子通讯数据的条件规定得更加严格。

譬如,德国《刑事诉讼法典》第 94 条规定了对普通物品进行扣押的条件,根据该条的规定,所有对侦查有意义的、可以作为证据材料使用的物品,如果财物持有人拒绝交出的,侦查机关都可以进行扣押。该法第 99 条规定了对普通邮件、电报进行扣押的条件,根据这一规定,无论是向被指控人发送的普通邮件、电报,还是被指控人自己发送的普通邮件、电报,只要其内容对侦查具有意义,都可以扣押。由此可见,在德国,搜查、扣押普通物品,包括普通邮件、电报的条件相对较低,只要对查清案件事实有意义,都可以扣押。而根据该法第 100 条 g、第 100 条 i、第 100 条 j 的规定,搜查、扣押电子通讯数据则必须符合非常严格的条件。第 100 条 j 规定的是搜查、扣押电子通讯的非内容信息的条件和程序,由于非内容信息,如姓名、出生日期、账户信息等涉及公民隐私的程度较低,因而对所有犯罪都可以适用。该法第 100 条 g 规定的是搜查、扣押电子通讯的内容信息的条件和程序,由于电子通讯的内容信息,如通话、邮件、短信的具体内容隐私程度非常高,因而只能适用于重大犯罪,并且必须遵守比例原则的要求。第 100 条 i 规定的是搜查、扣押移动通讯的非内容信息的条件和程序,由于移动通讯的非内容信息,如手机串号(IMEI)、手机卡号一旦被获知,就能对犯罪嫌疑人进行实时跟踪、定位,获取大量重要的个人信息,涉及隐私的程度也非常高,因而也只能适用于重罪,并且必须遵循比例原则的要求。[11]

2. 搜查、扣押电子通讯数据普遍要求必须遵循比例原则

比例原则是现代法治国家划分国家权力与公民个人权利界限的一项基本原则,其内容包括三个方面,也即三项子原则。一是适合性原则,是指国家机关所采取的每一手段都必须用于实现法定的职能目标;二是必要性原则,是指如果为实现某一职能目标,存在两种以上的手段,那么必须采用对公民个人权利损害最小的手段;三是相称性原则,是指只能采用对公民个人权利损害较小的手段来保护较大的国家、社会公共利益;不得采用对公民个人权利损害较大的手段来保护较小的国家、社会公共利益,不得杀鸡用牛刀,大炮打蚊子。[12] 由于搜查、扣押电子数据,尤其是电子通讯数据可能严重侵犯公民隐私、财产等重要权利,因而域外国家、地区普遍要求搜查、扣押这些证据必须符合比例原则。如丹麦《司法行政法》第 782 条第 1 款明确规定:“如果侵犯某人通信秘密的侦查行为之目的、方法以及案件严重程度与该侵犯通讯秘密措施不成比例,则此种侦查行为不得实施。”[13] 比利时《重罪审理法典》第 46(2)条第 §1 款第 2 项明确规定,搜查、扣押电子通讯数据必须“体现尊重私生活的比例性特点,并将上述活动作为其他所有调查职责的辅助性措施”。[14]

〔11〕 参见德国《刑事诉讼法典》,宗玉琨译注,知识产权出版社 2013 年版,第 50、55、73 - 77 页。

〔12〕 参见[德]哈特穆特·毛雷尔著:《行政法学总论》,高家伟译,法律出版社 2000 年版,第 238 - 239 页。

〔13〕 丹麦刑事诉讼法被规定在《司法行政法》当中。丹麦《司法行政法》由五卷组成:第一卷是法院,第二卷是民事和刑事诉讼共同规则,第三卷是民事诉讼法,第四卷是刑事诉讼法,第五卷是过渡性规定。参见丹麦《司法行政法》,杨宇冠、杨依译,载《世界各国刑事诉讼法》编辑委员会编译:《世界各国刑事诉讼法·欧洲卷(上)》,检察出版社 2016 年版,第 223、229 页。

〔14〕 比利时《重罪审理法典》,宋泫沙译,载《世界各国刑事诉讼法》编辑委员会编译:《世界各国刑事诉讼法·欧洲卷(上)》,检察出版社 2016 年版,第 156 页。

(二)域外电子通讯数据搜查、扣押的基本条件

1. 只能适用于比较严重的罪行

如前所述,域外国家、地区普遍要求搜查、扣押电子通讯数据必须符合比例原则的要求。比例原则的第三项子原则是相称性原则,也即只能采用对公民权利损害较小的手段保护较大的国家、社会公共利益,而搜查、扣押电子数据,尤其是电子通讯数据对公民权利损害较大,如果适用于侦查轻微犯罪,会导致侦查手段对公民权利造成的损害大于其所保护的国家、社会公共利益,不符合比例原则的要求,因而域外国家、地区普遍要求搜查、扣押电子通讯数据只能适用于比较严重的犯罪。譬如,德国《刑事诉讼法典》第 100 条 g 明确规定,只有在"1. 实施了在个案中亦属重大的犯罪行为,特别是第一百条 a 第二款所称犯罪行为,[15]或者他在未遂可罚的情形中行为未遂,或者他通过犯罪行为进行预备,或者,2. 借助电信通讯实施犯罪行为",才可以对电子通讯数据进行搜查、扣押。[16] 再如,新加坡《刑事诉讼法典》第 39 条、第 40 条明确规定,搜查、扣押电子通讯数据只能适用于可捕罪,也即比较严重的犯罪。[17]

我国《刑事诉讼法》以及司法解释对搜查、扣押电子通讯数据适用于哪些犯罪没有作出特别规定,这实际上意味着搜查、扣押电子通讯数据可以适用于所有犯罪。譬如,最高人民检察院于 2012 年 1 月 22 日发布的《人民检察院刑事诉讼规则(试行)》第九章第五节将电子数据作为搜查的对象(第 228 条),第六节将电子数据作为调取、查封、扣押的重要对象(第 38 条),但都没有对搜查、扣押电子数据规定特别的适用条件,不要求搜查、扣押电子数据只能适用于比较严重的犯罪。笔者认为,这不符合比例原则的精神,不利于保障公民个人权利。我国在未来修改刑事诉讼法时,应当借鉴域外成功经验,完善搜查、扣押电子通讯数据的适用条件,将搜查、扣押电子通讯数据的适用条件现定为比较严重的犯罪。不仅如此,由于电子通讯数据的内容信息与非内容信息涉及公民个人隐私的程度不同,因而应当设置不同的适用条件。电子通讯数据的非内容信息,如手机号码、邮箱号码、QQ 号、微信号码、IP 地址,等等,虽然涉及公民个人隐私,但程度较低,因而可以将其适用范围限定为可能判处徒刑以上刑罚的犯罪。电子通讯数据的内容信息,如电话、邮件、短信、微信的具体内容,涉及公民个人隐私的程度非常高,应当将其适用范围限定为可能判处 3 年有期徒刑以上刑罚的犯罪。3 年是我国重罪与轻罪的分界线,也是不少其他国家、地区划分重罪与轻罪的分界线,以可能判处 3 年有期徒刑以上刑罚作为对电子通讯数据的内容信息实施搜查、扣押的条件,是合适的。

2. 只有采用传统侦查措施难以查清案件事实才能搜查、扣押电子通讯数据

如前所述,域外国家、地区普遍要求搜查、扣押电子通讯数据必须符合比例原则的要

---

〔15〕 德国《刑事诉讼法》第 100 条 a 规定的是监听和记录电信通讯的适用条件,第 2 款规定的是可以监听和记录电信通讯的案件范围,都只能适用于重罪。参见德国《刑事诉讼法典》,宗玉琨译注,知识产权出版社 2013 年版,第 58 页。

〔16〕 参见德国《刑事诉讼法典》,宗玉琨译注,知识产权出版社 2013 年版,第 73 页。

〔17〕 参见新加坡《刑事诉讼法典》,裴炜等译,载《世界各国刑事诉讼法》编辑委员会编译:《世界各国刑事诉讼法·亚洲卷》,检察出版社 2016 年版,第 582 页。

求。比例原则的第二项子原则为必要性原则,是指如果为实现某一目标,存在两种以上的手段,那么必须采用对公民权利损害最小的手段。正因为如此,法治发达国家要求,如果采用非强制性侦查手段就能够查清案件事实,就不得采用强制性侦查手段(这被称作任意侦查原则);如果采用传统侦查手段就能够查清案件事实,就不得采用特殊侦查手段。如前所述,搜查、扣押电子通讯数据是一种对公民权利损害较大的手段,因而域外国家、地区普遍规定,只有采用传统侦查手段难以查清案件事实,才能采用对电子通讯数据进行搜查、扣押的手段。譬如,德国《刑事诉讼法》第 110 条 g 第 1 款明确规定,对利用电信通讯手段实施的犯罪,只有在"查清案情或者侦查被指控人所在地采用其他方式可能无望,且提取数据与案件的重大性成适当比例时",才能搜查、扣押电子通讯数据。[18] 再如,土耳其《刑事诉讼法典》第 134 条第 1 款明确规定:"在犯罪侦查过程中,如果无法通过其他方式获得证据,根据检察官的申请,法官应当作出搜查犯罪嫌疑人使用的电脑、电脑程序和电脑记录,以及对这些记录进行拷贝、分析和文本化的决定。"[19]

我国《刑事诉讼法》并未将比例原则确立为刑事诉讼的基本原则,因而实践中并不要求如果采用非强制性侦查手段能够查清案件事实,就不能采取强制性侦查手段;不要求如果采用传统侦查手段就能够查清案件事实,就不能采用特殊侦查手段。同理,我国也不要求如果采用传统侦查手段就能够查清案件事实就不能搜查、扣押电子通讯数据。这对保护公民的隐私、财产等权利非常不利,建议我国在未来修改刑事诉讼法时借鉴域外的成功经验,规定只有采用传统侦查措施无法查清案件事实,才能搜查、扣押电子通讯数据。

3. 必须申请法官许可

在刑事诉讼中,法官、法院不承担侦查、控诉职责,要求侦查机关在采用强制性诉讼手段之前必须申请法院许可,对于防止侦查机关滥用强制性诉讼手段,保护相对人权利具有重要意义。搜查、扣押电子通讯数据也是一种强制性诉讼手段,而且是一种强制力度较大的诉讼手段,因而域外国家、地区普遍要求必须经过法官许可才能实施。按照德国《刑事诉讼法典》第 100 条 g 第 2 款以及第 100 条 b 第 1 款的规定,搜查、扣押电子通讯数据,必须由检察院提出申请,由法院签发命令,迟延有危险时才可以由检察院签发命令。检察院的命令只要未在三个工作日内取得法院确认,即失去效力。[20] 在俄罗斯,根据其《刑事诉讼法典》第 29 条的规定,对电子通讯数据进行搜查、扣押,必须向法院申请签发许可令。[21]

在美国,联邦最高法院于 2014 年 6 月 25 日,在赖利诉加利福尼亚州案(Riley v. California)和美利坚合众国诉沃瑞案(United States v. Wurie)的合并判决(以下简称赖利案判决)中作出裁断:警察在逮捕犯罪嫌疑人时无权搜查其手机中的数据信息,警察要想搜查手机中的数据信息,必须单独获得令状。[22] 根据赖利案确立的规则,警方搜查、扣押手机

〔18〕 参见德国《刑事诉讼法典》,宗玉琨译注,知识产权出版社 2013 年版,第 73 - 74 页。

〔19〕 土耳其《刑事诉讼法典》,王贞会等译,载《世界各国刑事诉讼法》编辑委员会编译:《世界各国刑事诉讼法·欧洲卷(中)》,检察出版社 2016 年版,第 1425 页。

〔20〕 参见德国《刑事诉讼法典》,宗玉琨译注,知识产权出版社 2013 年版,第 64、73 页。

〔21〕 参见俄罗斯《刑事诉讼法典》,赵路译,载《世界各国刑事诉讼法》编辑委员会编译:《世界各国刑事诉讼法·欧洲卷(上)》,检察出版社 2016 年版,第 388 条。

〔22〕 参见 Charlie Savage, Between the Lines of the Cellphone Privacy Ruling, *the New York Times*, June 25, 2014。

数据信息必须受到双重司法审查:一是,搜查、扣押手机通常是在拘留、逮捕犯罪嫌疑人时附带进行的,而美国拘留、逮捕的实施以有证拘留、逮捕为原则,无证拘留、逮捕为例外,这意味着,警方在拘留、逮捕犯罪嫌疑人以前通常必须向法官申请签发令状。二是,按照赖利案确立的规则,在拘留、逮捕犯罪嫌疑人时,搜查、扣押其手机只能针对手机机体,如手机的型号、颜色、新旧程度等,不能针对手机中的数据信息,如果需要对手机中的数据信息进行搜查、扣押,必须再次向法官申请签发令状。之所以如此,是因为联邦最高法院认为,如果授权警方拘留、逮捕犯罪嫌疑人后可以无证搜查手机数据,将给予警方"随心所欲地翻查一个人私生活的不受约束的自由裁量权"。[23]

在我国,强制性诉讼手段除逮捕必须报请检察院批准,其他都由侦查机关自行决定、实施。如前所述,搜查、扣押电子通讯数据是一种强制力度非常大的诉讼手段,由侦查机关自行决定实施对防止侦查人员滥用权力和保护公民个人权利都非常不利,因而建议我国在将来修改刑事诉讼法时,建立搜查、扣押电子通讯数据的司法审查机制。由于内容信息与非内容信息涉及隐私的程度不同,因而可以考虑,在制度建构初期,搜查、扣押电子通讯数据的非内容信息,由县级以上公安机关负责人决定;搜查、扣押电子通讯数据的内容信息,必须报请检察机关批准。将来,在我国真正建立审前程序的司法(法院)审查机制以后,再进一步提高要求:搜查、扣押电子通讯数据的非内容信息由检察机关批准;搜查、扣押电子通讯数据的内容信息必须报请法院批准。

三 电子通讯数据搜查、扣押的适用程序

由于搜查、扣押电子数据,尤其是电子通讯数据涉及复杂的信息、通讯技术,侦查人员可能不具备相关专业知识;有些侦查人员即使曾经学习过相关专业知识,但是由于信息、通讯技术的日新月异,知识更新的速度非常快,因而其对新一代信息、通讯技术可能也并不熟悉。此外,由于电子数据,尤其是电子通讯数据涉及公民个人隐私,因而很多电子设备、程序设置了复杂的加密程序,没有相对人的配合以及相关专业人士的协助,可能很难启动、破解,因而域外国家、地区普遍对搜查、扣押电子数据,尤其是电子通讯数据设置了不同于搜查、扣押一般场所、物品的特殊程序。

(一)有权要求电信运营商、犯罪嫌疑人以及其他专业人员提供协助

由于电子通讯信息很多被电信运营商掌握,甚至有些电讯通讯信息只有电信运营商掌握,因而域外国家、地区立法都特别强调电信运营商对侦查人员的配合义务。比利时《重罪审理法典》第46(2)之§2明确规定:"被要求提供§1中规定的数据的电讯网络操作人员及电讯服务运营商,向国王检察官或司法警察警官提供相关数据,期限由国王根据司法部长及负责管理电讯业务的部长的建议确定。"[24]其他许多国家刑事诉讼法典也对

〔23〕 Riley v. California, 134 S. Ct. 2473, 2491 – 2495 (2014).

〔24〕 比利时《重罪审理法典》,宋汶沙译,载《世界各国刑事诉讼法》编辑委员会编译:《世界各国刑事诉讼法·欧洲卷(上)》,检察出版社2016年版,第156页。

电信运营商的配合义务作出了规定，如俄罗斯《刑事诉讼法典》第 186 - 1 条、丹麦《司法行政法》第 786 条、奥地利《刑事诉讼法典》第 76a 条、保加利亚《刑事诉讼法典》第 59 条第 1 款、拉脱维亚《刑事诉讼法典》第 219 条，等等。

由于许多电子设备都设置了密码，如果没有获知密码很难打开该设备，因而不少国家、地区都规定，电子设备的使用人，通常即犯罪嫌疑人，也有义务配合侦查人员搜查、扣押电子通讯数据。如克罗地亚《刑事诉讼法典》第 257 条第 1 款明确规定："在搜查执行机关的要求下，使用计算机或能访问计算机、数据载体的人或电信服务提供商应当提供访问计算机、设备或数据载体的方式并且提供无干扰地使用及实现搜查目的的必要信息。"〔25〕但是，在有些国家，就搜查、扣押电子数据而言，犯罪嫌疑人也受不得被迫自证其罪特权以及亲属、职业、职务作证豁免权的保护，因而立法规定，不得强迫犯罪嫌疑人及其近亲属提供协助。如荷兰《刑事诉讼法典》第 125K 条第 3 款规定，不得强制要求犯罪嫌疑人配合警方搜查、扣押电子数据，嫌疑人有权以近亲属、身份、职业保密为由拒绝协助警方搜查、扣押电子数据。〔26〕

如前所述，搜查、扣押电子通讯数据涉及专业的，甚至精深、前沿的信息、网络技术，侦查人员可能不了解相关专业知识；同时，在有些国家和地区，搜查、扣押电子数据也被认为受到不得被迫自证其罪的约束，因而不能强迫犯罪嫌疑人本人提供协助，因此，有些国家规定，在搜查、扣押电子数据时，侦查人员有权命令其他知晓相关专业知识的人提供协助。譬如，新西兰于 2012 年颁布实施的《搜查与监控法》第 130 条明确规定，对储存在电脑系统或其他数据存储装置中的数据行使搜查权的人员，可以要求一名指定的人员来提供登录信息和其他信息，或者提供合理的、必要的帮助，以便搜查人员顺利行使搜查权来获取数据。〔27〕

如前所述，我国现行《刑事诉讼法》只是将电子数据增列为一种法定的证据种类，而没有对搜查、扣押电子数据的程序作出特别规定，因而当然没有对搜查、扣押电子数据过程中相关人员的配合义务作出规定，这对实践中公安司法人员调查、收集电子数据非常不利。据报道，在 2018 年 8 月引起广泛关注的滴滴女乘客被奸杀案件中，滴滴客服曾两度拒绝向警方提供司机信息，〔28〕与这一状况有一定关系。对于相关人员的配合义务，立法在作出规定时应当明确以下几点：首先，电信公司、网络运营商、电子商务平台等有义务配合公安司法机关搜查、扣押电子通讯数据，这是毋容置疑的。如果拒不配合，公安机关及相关主管部门有权对其进行处罚。其次，侦查机关如果在搜查、扣押过程中遇到专业性问题，公安机关网监部门专家无法解决，可以聘请科研机构、商业网络、电讯公司等机构的专业人员提供协助，相关专业人员应当提供协助。最后，侦查机关还应当有权要求犯罪嫌疑人提供协助。如前所述，许多电子设备、移动终端、应用程序、软件等，在开机或启动时

〔25〕 克罗地亚《刑事诉讼法典》，罗海敏译，载《世界各国刑事诉讼法》编辑委员会编译：《世界各国刑事诉讼法·欧洲卷（中）》，检察出版社 2016 年版，第 984 页。

〔26〕 参见荷兰《刑事诉讼法典》，魏武译，载《世界各国刑事诉讼法》编辑委员会编译：《世界各国刑事诉讼法·欧洲卷（中）》，检察出版社 2016 年版，第 846、850、876 页。

〔27〕 参见《2012 年新西兰搜查与监控法》，李玉华、田力男、安贝译，中国政法大学出版社 2013 年版，第 213 页。

〔28〕 参见《滴滴女乘客遭奸杀，警方：客服两度拒绝提供司机信息》，资料来源：http://news.163.com/18/0826/01/DQ3MESRS0001875P.html，最近访问时间［2018 - 11 - 09］。

都必须有密码，并且有些密码很难破解，因而如果确有必要，侦查机关应当有权要求犯罪嫌疑人提供协助。但需要注意的是，电子信息很容易被删除、修改，因而为防止犯罪嫌疑人利用协助公安司法人员搜查、扣押电子通讯数据的机会毁灭、篡改证据，立法对侦查人员要求犯罪嫌疑人协助办案人员搜查、扣押电子通讯数据的程序应当进行严格规制。

（二）应当尽可能转换为书面或其他可以直接识别的形式

电子通讯数据以电子介质为载体，通常无法直接通过感官感知，而必须借助于电脑、手机或其他播放设备、软件等进行播放、显示。办案人员在诉讼过程中可能随时需要对电子通讯数据进行审查，但并非在任何场所都能获得对所有电子通讯数据进行播放、显示的设备、软件，因而为方便办案，许多国家、地区都规定，侦查人员应当尽可能将电子通讯数据转化为书面或其他可以直接识别的形式。如奥地利《刑事诉讼法典》第138条第4款规定，在搜查、扣押电子通讯数据以后，“检察机关应当对侦查结果进行审查，并要求将对诉讼具有意义的、可以作为证据使用的部分转换为图像或书面形式”。〔29〕

在我国，司法解释以及相关法律文件都不要求将电子通讯数据转化为书面或其他可以直接识别的形式。三机关《电子数据规定》第18条第2款甚至明确规定：对网页、文档、图片等可以直接展示的电子数据，可以不随案移送打印件。实践中，大多数地方侦查机关都不将电子通讯数据转化为书面或其他可以直接识别的形式，而只是在搜查、扣押笔录中或者以“情况说明”简单表述电子通讯数据的基本内容。笔者认为，这种做法非常不合理。其一，这不利于检察机关、法院以及辩护方全面了解电子通讯数据的内容。电子通讯数据包含的内容非常丰富，经常既包含不利于犯罪嫌疑人、被告人的信息，也包含有利于犯罪嫌疑人、被告人的信息，侦查机关如果不将电子通讯数据转换为书面或其他可以直接识别的形式，而只表述基本内容，其作为追诉方的诉讼立场，极易导致其在表述电子数据的基本内容时只注意证明犯罪嫌疑人、被告人有罪、罪重的信息，而忽视证明犯罪嫌疑人、被告人无罪、罪轻的信息。而由于电子通讯数据包含的信息非常丰富，甚至包含海量信息，检察机关、法院审判人员受时间、精力的限制，在办案时很难亲自审查电子通讯数据的原始载体，通常只会查阅侦查机关所做的书面记录，这必然导致他们对电子数据内容的了解不全面。辩护律师虽然有充分的时间、精力查阅电子数据原始载体，但实践中办案机关普遍只允许辩护律师查阅书面卷宗材料，而不允许辩护律师查阅电子存储介质，这导致辩护方对电子通讯数据的了解也非常不全面。其二，这不利于检察机关、法院以及辩护方审查电子通讯数据的真伪。要审查电子通讯数据的真伪，一方面要审查电子通讯数据收集、运输、保管、鉴定的程序是否符合技术规范以及法定的程序；另一方面要审查电子通讯数据的内容是否符合逻辑、常理，是否存在内部矛盾，是否与其他证据存在矛盾，等等。要审查电子通讯数据内容的真伪，首先必须对电子通讯数据的内容有全面的了解。但如前所述，在我国实践中，侦查机关通常只表述电子通讯数据的基本内容，而不将电子通讯数据的全部内容转换为书面形式或其他易于识别的形式，而检察机关、法院审判人员因为时间、精力限制，往往难以对电子

〔29〕 奥地利《刑事诉讼法典》，池颖、蒋毅译，载《世界各国刑事诉讼法》编辑委员会编译：《世界各国刑事诉讼法·欧洲卷（上）》，检察出版社2016年版，第31页。

数据的原始信息进行全面审查;辩护律师虽然有充分的时间、精力,往往又不被允许查阅电子存储介质,这导致检察机关、法院以及辩护方都很难通过全面审查电子通讯数据的内容来判断其真伪。为解决这一问题,建议我国在未来立法时,借鉴其他国家、地区的成功经验,规定侦查机关必须尽量将电子通讯数据转换为书面或其他能够直接识别的形式。

(三)必须将原始存储介质予以封存

虽然为便于其他办案人员以及诉讼参与人查阅,许多国家、地区立法要求将电子通讯数据转换为书面或其他便于识别的形式,但是由于电子通讯数据转换为书面或其他易于识别的形式以后,通常只能反映电子文档的内容信息,与该文档相关的附属信息、关联痕迹、系统环境信息等通常无法得到反映,而这些信息对查清案件事实、审查判断电子文档内容的真伪经常也具有重要价值,因而域外许多国家、地区都要求,在搜查、扣押电子通讯数据时,应当尽量将原始存储介质也予以扣押。同时,由于电子设备一旦开机,其中存储的电子数据很容易被删除、篡改,尤其是具有无线联网功能的电子设备,机主及相关人员甚至可以对其中的数据信息进行远程擦除,并且电子数据一旦被删除、修改,很难被发现,因而许多国家、地区立法都要求,在搜查、扣押电子通讯数据时,通常应对原始存储介质进行封存。譬如,俄罗斯《刑事诉讼法典》第 186 - 1 条第 6 款明确规定,搜查、扣押的电子通讯信息"应密封保存在排除其他人员可能了解的条件下,同时还应保障其完整性"。[30]

对电子数据原始存储介质必须予以封存,我国司法解释以及相关法律文件作出了比较全面的规定。三机关《电子数据规定》第 8 条第 1 款明确规定: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。该条第 2 款进一步规定:封存电子数据原始存储介质,应当保证在不解除封存状态的情况下,无法增加、删除、修改电子数据。封存前后应当拍摄被封存原始存储介质的照片,清晰反映封口或者张贴封条处的状况。第 3 款还针对手机等具有无线通讯功能的电子设备规定,封存手机等具有无线通信功能的存储介质,应当采取信号屏蔽、信号阻断或者切断电源等措施。第 18 条进一步要求电子存储介质在随案移送时必须保持封存状态:收集、提取的原始存储介质或者电子数据,应当以封存状态随案移送,并制作电子数据的备份一并移送。三机关《网络犯罪意见》第 14 条、第 17 条对电子数据原始存储介质的封存作出了与三机关《电子数据规定》基本相同的规定。应当肯定,司法解释以及相关法律文件对电子存储介质封存的规定比较严格,公安司法机关应当确保以上规定在实践中得到严格执行。

(四)与案件无关的以及诉讼不再需要的信息必须及时删除、销毁

由于电子通讯信息与公民隐私联系非常紧密,一旦泄露将严重损害相关人员的人格、名誉等重要权利,因而为降低泄露的风险,许多国家、地区立法都规定,如果经审查,发现此前搜查、扣押的电子通讯数据与案件无关,或者诉讼不再需要,应当立即删除或销毁。

〔30〕 俄罗斯《刑事诉讼法典》第 186 - 1 条,赵路译,载《世界各国刑事诉讼法》编辑委员会编译:《世界各国刑事诉讼法·欧洲卷(上)》,检察出版社 2016 年版,第 447 页。

如德国《刑事诉讼法典》第101条第8款规定，如果搜查、扣押的电子数据“不再为刑事追诉和法院可能进行的措施审查所必要时，应当不迟延地删除。删除应当记入案卷。如果仅为法院可能进行的措施审查而迟延删除，未经所涉及人员同意时，数据只能为此目的使用；数据应当相应封锁”。〔31〕

在我国，司法解释以及相关法律文件都没有规定与案件无关以及诉讼不再需要的电子数据必须予以删除或销毁，这对保护犯罪嫌疑人以及相关人员的隐私权极为不利，建议我国在未来修改刑事诉讼法或相关司法解释时借鉴域外国家、地区的经验，规定对于与案件无关以及诉讼不再需要的电子数据，尤其是电子通讯数据必须予以删除或销毁。

四　电子通讯数据搜查、扣押的权利保障

如前所述，由于搜查、扣押电子数据，尤其是电子通讯数据直接涉及公民隐私，因而为防止侦查人员滥用权力，侵犯公民个人隐私，域外国家、地区在设计搜查、扣押电子通讯数据的程序制度时都非常关注对相关人员，尤其是犯罪嫌疑人的权利保障。同时，由于侦查机关搜查、扣押的电子通讯数据中也可能包含对犯罪嫌疑人有利的信息，因而域外国家、地区都充分保障犯罪嫌疑人及其辩护人有机会充分参与搜查、扣押程序，能够全面了解电子通讯数据包含的信息。

（一）辩护律师有权在侦查机关搜查、扣押电子通讯数据时在场

由于电子设备中储存的信息非常丰富，可能既有大量与案件有关的信息，也有大量与案件无关的信息，因而为防止侦查人员随意扩大搜查、扣押的范围，侵犯犯罪嫌疑人以及相关人员的隐私权，域外许多国家、地区立法都规定，在搜查、扣押电子数据，尤其是电子通讯数据过程中，辩护人有权在场。如意大利《刑事诉讼法典》第356条规定：“被调查人的辩护人有权出席第352条和第354条规定的活动”，而第352条第1－2款、第354条第2款规定的就是对电子数据，包括电子通讯数据的搜查、扣押，〔32〕因而，这意味着，在侦查机关对电子数据，包括电子通讯数据进行搜查、扣押时，辩护人有权在场。荷兰《刑事诉讼法典》第99a条、第125i条规定，在搜查电子数据时，“犯罪嫌疑人有权获得辩护人的帮助，但不得拖延搜查的进行”。〔33〕

我国《刑事诉讼法》第239条仅规定，在搜查的时候，应当有被搜查人或者他的家属、邻居或者其他见证人在场，而没有规定辩护律师有权在场。司法解释以及相关法律文件也都没有规定在搜查、扣押电子数据，包括电子通讯数据时辩护律师有权在场。如前所述，电脑、手机等电子设备包含的内容非常丰富，可能既包含大量与案件有关的信息，也包含大量与案件无关的信息，如果缺乏有效的监督，极可能导致侦查人员随意扩大搜查、扣

〔31〕 德国《刑事诉讼法典》，宗玉琨译注，知识产权出版社2013年版，第79页。

〔32〕 参见意大利《刑事诉讼法典》，黄风译，载《世界各国刑事诉讼法》编辑委员会编译：《世界各国刑事诉讼法·欧洲卷（下）》，检察出版社2016年版，第1686－1687页。

〔33〕 荷兰《刑事诉讼法典》，魏武译，载《世界各国刑事诉讼法》编辑委员会编译：《世界各国刑事诉讼法·欧洲卷（中）》，检察出版社2016年版，第847、849、950页。

押的范围,侵犯公民隐私权。为强化对公民隐私权的保护,建议我国在未来修改《刑事诉讼法》以及相关司法解释时,借鉴域外国家、地区的成功经验,规定在侦查人员搜查、扣押电子数据,尤其是电子通讯数据时,辩护律师有权在场进行监督。

(二)搜查、扣押电子通讯数据完毕应当及时告知犯罪嫌疑人及相关人员

由于电子数据,尤其是电子通讯数据一旦被搜查、扣押,犯罪嫌疑人、被告人及相关人员的隐私就在办案人员的掌控之下,因而为防止办案人员滥用权力,侵犯公民个人隐私,域外许多国家、地区都规定,侦查机关在搜查、扣押电子通讯数据完毕后,应当及时告知犯罪嫌疑人及相关人员,通过犯罪嫌疑人及相关人员的监督,确保办案机关严格依法行使权力。如德国《刑事诉讼法典》第 101 条第 4 款、第 5 款规定,在搜查、扣押电子数据后,一旦不危及侦查目的、他人的生命、身体之不受侵犯权与人身自由,以及重要的财产价值,应当立即通知被指控人及相关人员。[34] 韩国《刑事诉讼法典》第 106 条第 4 款规定:"法院依据第 3 款的规定扣押信息后,必须向《个人信息保护法》第 2 条第 3 项规定中的信息主体,通知其扣押的事实。"[35]

在我国,《刑事诉讼法》第 143 条规定,侦查人员认为需要扣押犯罪嫌疑人的邮件、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的邮件、电报检交扣押,而没有要求在扣押邮件、电报后告知犯罪嫌疑人及相关人员。司法解释以及相关法律文件同样没有规定在搜查、扣押电子通讯数据以后,必须告知犯罪嫌疑人及相关人员。笔者认为,这对防止侦查机关滥用权力,保护公民隐私权极为不利,建议我国在未来修改《刑事诉讼法》以及相关司法解释时,规定侦查机关在搜查、扣押电子通讯数据时如果没有通知犯罪嫌疑人或者其近亲属、辩护人在场见证,在搜查、扣押结束后,必须及时通知犯罪嫌疑人及相关人员。

(三)犯罪嫌疑人及其辩护人有权了解、查阅被搜查、扣押的电子通讯数据的内容

如前所述,电子通讯数据包含的信息非常丰富,既可能包含对犯罪嫌疑人不利的信息,也可能包含对犯罪嫌疑人有利的信息,而侦查机关受诉讼立场的限制,往往更重视对犯罪嫌疑人不利的信息,而不太重视对犯罪嫌疑人有利的信息,因而为确保对犯罪嫌疑人有利的信息也能够被纳入诉讼轨道,从而使法官兼听则明,有效查清案件事实,域外许多国家、地区立法都规定,在搜查、扣押电子数据,包括电子通讯数据以后,犯罪嫌疑人及其辩护人有权了解、查阅被搜查、扣押的电子通讯数据的具体内容。如丹麦《司法行政法》第 784 条第 1 款规定,搜查、扣押电子通讯数据时,法庭应当为相对人指派律师。第 785 条第 1 款规定,搜查、扣押电子通讯数据过程中,被指定的律师"应当被通知并且有权参加所有涉及本案的法庭会议,除此之外应当知悉警方所掌握的各种材料"。[36] 沙特阿拉伯《刑事诉讼法典》第 59

〔34〕 参见德国《刑事诉讼法典》,宗玉琨译注,知识产权出版社 2013 年版,第 78 页。

〔35〕 韩国《刑事诉讼法典》,金玄卿译,载《世界各国刑事诉讼法》编辑委员会编译:《世界各国刑事诉讼法·亚洲卷》,检察出版社 2016 年版,第 239 页。

〔36〕 丹麦《司法行政法》,杨宇冠、杨依译,载《世界各国刑事诉讼法》编辑委员会编译:《世界各国刑事诉讼法·欧洲卷(上)》,检察出版社 2016 年版,第 229 - 230 页。

条规定，在搜查、扣押结束后，“文件、邮政信件、电子邮件的内容应当告知犯罪嫌疑人或所有权人，或尽快将物品照片传送给上述人员，上述行为可能影响侦查时除外。”〔37〕

根据我国《刑事诉讼法》以及司法解释的规定，侦查机关在搜查、扣押电子通讯数据以后，无须通知犯罪嫌疑人及其辩护人了解、查阅电子通讯数据的内容。虽然按照《刑事诉讼法》第40条的规定，辩护律师自人民检察院对案件审查起诉之日起，可以查阅、摘抄、复制本案的案卷材料，但实践中，办案机关通常只允许辩护律师查阅书面材料，而不允许辩护律师查阅电子数据；而如前所述，按照我国立法以及司法解释的规定，侦查机关在搜查、扣押电子数据以后无须将电子数据转化为书面或其他能够直接识别的形式，实践中也很少转化为书面或其他能够直接识别的形式，这必然导致即使电子数据中存在对犯罪嫌疑人有利的信息，被告方也无法知悉，法官也很难知晓，这对保护被告方的辩护权、保障法官查清案件事实都非常不利。为解决这一问题，建议我国在未来修改《刑事诉讼法》或相关司法解释时，借鉴域外的经验，规定侦查机关在搜查、扣押电子数据，包括电子通讯数据以后，应当告知犯罪嫌疑人及其辩护人有权了解、查阅电子数据的内容。

（四）采用非法手段收集的电子通讯数据必须予以排除

如前所述，电子数据，尤其是电子通讯数据直接涉及公民个人隐私，搜查、扣押电子数据的权力一旦被滥用，将对公民个人隐私造成重大损害，因而为防止侦查机关滥用权力，域外许多国家、地区立法都规定，采用非法手段收集的电子数据，尤其是电子通讯数据必须予以排除。如奥地利《刑事诉讼法典》第140条第1款规定，搜查、扣押电子通讯数据必须符合法定的条件和程序，否则，搜查、扣押所得的证据不得用作认定案件事实的根据。〔38〕拉脱维亚《刑事诉讼法典》第214条以及第229条规定，如果特殊侦查行为，包括对电子数据的搜查、扣押违反了法定的条件、程序，那么收集的证据不得在证明程序中使用。〔39〕

在我国，虽然最高人民法院、最高人民检察院、公安部、国家安全部、司法部于2010年6月13日联合发布的《关于办理刑事案件排除非法证据若干问题的规定》系统确立了非法证据排除规则，2012年修正的《刑事诉讼法》又进一步完善了非法证据排除规则，但是非法证据排除规则并不适用于电子数据。《刑事诉讼法》第56条规定：“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。”由此可见，按照《刑事诉讼法》的规定，非法证据排除规则只适用于犯罪嫌疑人、被告人供述、证人证言、被害人陈述、物证、书证五种证据。而按照《刑事诉讼法》第50条的规定，视听资料、电子数据是与这五种证据并列的证据种类，既不属于物证、书证，也不属于

〔37〕 沙特阿拉伯《刑事诉讼法典》，侯宇翔等译，载《世界各国刑事诉讼法》编辑委员会编译：《世界各国刑事诉讼法·亚洲卷》，检察出版社2016年版，第415页。

〔38〕 参见奥地利《刑事诉讼法典》，池颖、蒋毅译，载《世界各国刑事诉讼法》编辑委员会编译：《世界各国刑事诉讼法·欧洲卷（上）》，检察出版社2016年版，第31页。

〔39〕 参见拉脱维亚《刑事诉讼法典》，倪润译，载《世界各国刑事诉讼法》编辑委员会编译：《世界各国刑事诉讼法·欧洲卷（中）》，检察出版社2016年版，第1057、1059页。

犯罪嫌疑人、被告人供述、证人证言、被害人陈述,因而不适用非法证据排除规则。然而,笔者认为,非法证据排除规则适用于物证、书证,却不适用于电子数据并不合理,因为非法搜查、扣押电子数据,尤其是电子通讯数据对公民隐私权的侵害比非法搜查、扣押一般物证、书证的侵害更严重,因为电子数据,尤其是电子通讯数据包含的公民个人隐私的数量远远超过一般物证、书证。对此,美国联邦最高法院在赖利案的判决中进行了深刻论证:"美国政府声称,对于手机中储存的所有数据的搜查与对各种实物证据的搜查是'没有实质区别的'。那相当于说骑马走一程与飞往月球没有本质区别……现代手机,作为一个类别,其所牵涉的隐私权问题远比一个香烟盒、一个钱包所牵涉的隐私权问题广泛得多。那种认为对被捕者口袋内容的检查并不构成除逮捕本身之外的对隐私权进一步实质侵犯的观点就实物证据而言是有道理的,但是,任何将这一推理扩张适用于数据的主张都必须有自己的基础。"[40] 因此,我国在未来修改《刑事诉讼法》以及相关司法解释时,应当扩大非法证据排除规则的适用范围,对于采用非法手段收集的电子数据,尤其是电子通讯数据,必须予以排除,不得用作认定案件事实的根据。

[本文为作者主持的 2015 年度教育部人文社会科学研究一般项目"刑事诉讼法实施问题与对策研究"(15YJA820003)的研究成果。]

[**Abstract**] Since electronic communication data is very rich in content, foreign countries and regions have generally adopted special provisions on the search and seizure of electronic communication data to prevent investigative organs from abusing their power to infringe upon citizens' right of privacy. The search and seizure of electronic communication data usually have to meet higher conditions than those for the search and seizure of ordinary letters, and must follow the principle of proportionality. Investigators have the authority to request assistance from relevant persons in the process of searching and seizing electronic communication data; electronic communication data should be converted into written or other forms that can be directly identified as much as possible; the original storage medium must be sealed; information that is unrelated to the case or no longer needed must be deleted or destroyed in time. The defense lawyer has the right to be present when the investigators search and detain electronic communication data; the suspect and relevant persons shall be informed in time after the completion of the search and seizure; the suspect and his/her defender have the right to be informed of and to inspect the electronic communication data searched and seized; and data of electronic communication collected by illegal means must be excl uded from evidence.

(责任编辑:郑 佳)

〔40〕 Riley v. California, 134 S. Ct. 2473, 2488 – 2489.