重庆大学学报(社会科学版)　2024年第30卷第1期
JOURNAL OF CHONGQING UNIVERSITY(Social Science Edition) Vol. 30 No. 1 2024

Doi:10.11835/j.issn.1008-5831.fx.2023.04.003

欢迎按以下格式引用:周伟.电子监控证据开示制度研究[J].重庆大学学报(社会科学版),2024(1):206-219. Doi:10.11835/j.issn.1008-5831.fx.2023.04.003

Citation Format: ZHOU Wei. Research on the discovery of the electronic surveillance evidence[J]. Journal of Chongqing University (Social Science Edition),2024(1):206-219. Doi:10.11835/ j.issn.1008-5831.fx.2023.04.003

电子监控证据开示制度研究

周　伟

(西南政法大学 法学院,重庆　401120)

摘要:电子监控证据的开示既触及社会公共利益,又涉及被告人获得公正审判的权利,探究电子监控证据开示制度对于平衡公共利益和个人基本权利具有重要意义。通过规范分析和比较研究,揭示出电子监控证据的生成机制具有封闭性,公诉机关和审判机关可能会以"公共利益豁免"为由拒绝开示电子监控证据;同时,因遵循最后使用原则,电子监控证据对被告人定罪量刑具有决定性作用,拒绝开示必然会影响公民的基本权利。从"目的"或"动机"看,以维护公共利益为名,限制公民的基本权利并非不可,但在同等实效下,应当选择不限制基本权利或者限制程度更小的其他手段。直接以保护公共利益为由,拒绝开示电子监控证据违背了必要性原则的要求,因此,有必要探索适当的电子监控证据开示方式。在我国刑事诉讼中,电子监控证据开示的是纳入监控卷宗,准备作为指控依据的卷宗材料和关联电子数据,开示的方式均为查阅、摘抄和复制。此种制度安排的缺陷在于:一方面,对于纳入监控卷宗的电子监控证据,刑事诉讼法没有区分卷宗材料和电子数据,缺乏精细化规定,进而导致电子监控证据开示局限于开示与不开示的二元模式;另一方面,对控诉机关不准备作为证据使用,没有纳入案卷的材料,辩方难以获得查阅、摘抄和复制的机会,因而对其无从知悉,即便知悉后申请司法机关调取,也难以获得支持。事实上,监控卷宗和电子数据承载的内容不同,监控卷宗和电子数据的开示方式应当有所区别。而电子监控获取的海量电子数据可能包含对被告人定罪量刑有决定性意义的材料,故未入卷材料具有开示的必要。有鉴于此,需按照入卷证据和未入卷证据的二元框架,建构差异化的电子监控证据开示制度。对于入卷证据的开示,可以要求辩方签署保密协议,准许其查阅、摘抄、复制监控卷宗,以及查阅、摘抄监控电子数据。然而,基于保护技术侦查方法的目的,对辩方复制监控电子数据的申请可不予准许。对于未入卷材料的开示,控方应当向辩方提供数据清单和数据选择的标准,同时辩方享有提出异议、申请调取关联数据的权利。

关键词:电子监控证据;证据开示;阅卷;数据访问权;必要性原则

中图分类号:D925.2　　**文献标志码**:A　　**文章编号**:1008-5831(2024)01-0206-14

基金项目:国家社会科学基金一般项目"监控类技术侦查证据运用研究"(19BFX090);西南政法大学2019年度学生科研创新项目博士生资助项目"刑事初查电子数据取证程序研究"(2019XZXS-020)

作者简介:周伟,西南政法大学诉讼法博士研究生,西南政法大学检察研究中心助理研究员,Email:15223404506@163.com。

电子监控证据是指通过记录监控、行踪监控、通信监控、场所监控等监控类技术侦查措施获得的可以用于证明案件事实的材料。电子监控证据的开示不仅触及社会公共利益，而且涉及被告人的基本权利：一方面记录监控、行踪监控、通信监控、场所监控等监控类技术属于国家秘密，开示电子监控证据可能泄露监控技术，危及国家安全、妨害公共利益、损害公民的合法权益；另一方面电子监控证据的开示有助于发现对被告人有利的证据材料，通过辩方的审查可以保证电子监控证据的客观性和真实性，减少被告人被错误定罪的几率。

电子监控证据开示①制度的理论和实践均需进行深入研析。首先，关于电子监控证据能否开示，有观点认为，凡是涉及国家秘密，可能对侦查活动造成不利影响的材料都应不予开示[1]；而有观点认为，在司法信息化的背景下，应当赋予刑事被告人数据访问的权利[2]。其次，关于纳入案卷材料的电子监控证据（以下简称入卷证据）的开示，有学者提出，“应当允许辩护方对被搜查、扣押的电子数据进行查看、审查和复制”[3]。但是，另有学者基于监控技术泄露的担忧，对入卷证据的开示方式提出了不同的意见。最后，关于未纳入案卷材料的电子监控证据（以下简称未入卷材料）能否开示，有观点认为，为了保护辩方的合法权益，控方有义务向辩方提供所有的证据复制件[4]。然而部分司法机关认为，电子监控证据的开示仅限于纳入案卷的证据，而未纳入案卷的材料不属于证据开示的范围。理论和实践认识的不一致，导致案件在处理上存在专断和差异，亟需完善的制度加以规制。因此，电子监控证据开示制度的研究成为理论和实践都无法回避的议题。

研究发现，电子监控证据能否开示，重点需要考虑其生成机制和对被告人定罪量刑的作用，入卷证据的开示会因证据载体的不同而略有差异，而未入卷材料既有开示的必要，也应有其特殊的开示方式。有鉴于此，本文围绕电子监控证据开示的必要性、入卷证据的开示和未入卷材料的开示三个问题展开剖析，并对理论观点进行回应，以期对完善我国的电子监控证据开示制度，丰富其理论研究有所助益。

一、电子监控证据开示的必要性

检视电子监控证据开示的必要性，是证成电子监控证据开示制度的逻辑基点，对该问题的分析，需要从电子监控证据的生成机制和对被告人定罪量刑的作用两个维度，评估拒绝开示的目的和手段是否相称。

（一）电子监控证据的生成具有封闭性

电子监控证据有其特殊的生成机制。需要采取监控措施的，办案部门会提出建议，经过县级以上公安机关负责人审批之后，交技术侦查部门实施。在实施的过程中，技术侦查部门会将监控的情况通报给办案部门。之后，办案部门将获得的关联监控电子数据作为证据线索尝试转化为被告人供述、证人证言等公开证据。最后，办案部门根据证据转化的情况，综合评断证明案件事实的证据，决定是否向技术侦查部门调取电子监控证据。确有必要调取的，技术侦查部门会根据办案部门的

①在我国法学论著中，证据开示（discovery，或者 disclose）又被译作“证据开示”“证据展示”“证据公开”或者“证据发现”，涉及电子数据等证据的，多使用“证据展示”，但不同于法庭审理阶段的“证据展示”。关于证据开示的表述可参见陈瑞华《比较刑事诉讼法（第二版）》（北京大学出版社，2021 版第 279 页）。本文为避免与法庭审理阶段的“证据展示”产生歧义，统一使用“证据开示”，特此说明。

要求,提取监控数据,制作监控卷宗,然后交给办案部门作为证据使用②。

根据前述生成机制,技术侦查部门获得的电子监控证据可以分为入卷证据和未入卷材料。其中,入卷证据包含两个方面的材料:一是采取监控措施的法律文书、证据清单、翻音材料、监听译文以及有关说明等;二是关联电子数据,即纳入证据体系用以证明案件事实的电子数据。文书形式的证据被纳入监控卷宗,关联电子数据被存入特定存储介质,作为监控卷宗的附件。未入卷材料则是以电子数据的形式,保存在技术侦查部门特定的存储介质当中。

电子监控证据的生成具有如下特点:首先,不论是入卷证据还是未入卷材料,其原始数据都记录和保存在技术侦查部门。根据我国公安机关的组织体系,技术侦查部门负责监控的实施,而办案部门负责刑事案件的侦查,二者之间是协作关系。与英国等域外国家的刑事侦查组织体系不同,我国公安机关的办案部门并不掌握电子监控证据。电子监控证据由技术侦查部门记录和保存,办案部门需要电子监控证据时,需向技术侦查部门申请调取。其次,开示的电子监控证据经过了四次筛选,第一次是技术侦查部门选择将监控的情况通报给办案部门;第二次是办案部门根据证据转化的情况,选择向技术侦查部门申请调取相关证据;第三次是技术侦查部门选择监控电子数据,制作监控卷宗交给办案部门;第四次是办案部门根据案件的情况,决定是否向公诉机关移送其获得的监控卷宗和电子数据。最后,开示的电子监控证据仅限于入卷证据。在我国,技术侦查部门和办案部门都没有义务向辩方开示证据,在审查起诉之后,公诉机关和审判机关才有义务向辩方开示相关证据材料。而公诉机关和审判机关开示的材料仅限于办案部门向其移送的监控卷宗和电子数据。

从电子监控证据的生成机制看,容易引发两个方面的问题:一是监控会产生海量的电子数据,增加了有效提取数据的难度[5],可能湮没一些有价值的数据。诚如欧洲人权法院所言,在证据开示的背景下,开示电子数据会引发复杂的问题(数据湮没),因为控方掌握了大量的数据信息③。二是监控的实施和使用均在公安机关控制之下,存在风险。制度的控制完全依赖办案人员的职业伦理,而让办案人员放弃追诉便利,追求角色的客观性,存在角色上的冲突[6]。

不仅如此,基于电子监控证据生成机制的特殊性,即使其已经被移送,公诉机关和审判机关还会以“公共利益豁免(public interest immunity)”[7]为由拒绝开示。在我国,证据开示是通过阅卷制度来实现的。按照传统的观点,基于诉讼结构的非对抗性,法院依职权推进诉讼程序,加之检察官具有客观义务,辩护人查阅案卷在制度上不会产生特别的困难[8]。但这种观点在电子监控证据的开示中遭遇到“公共利益豁免”原则的阻击。辩护人申请查阅、摘抄和复制电子监控证据,公诉机关和审判机关会以涉及公共利益为由,驳回辩护人的阅卷申请。我国《人民检察院刑事诉讼规则》(以下简称《刑诉规则》)第48条规定,律师以外的辩护人申请查阅、摘抄、复制案卷材料,涉及国家秘密的,人民检察院可以不予许可。《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》(以下简称《刑诉解释》)第53条规定,合议庭、审判委员会的讨论记录以及其他依法不公开的材料不得查阅、摘抄、复制。

(二)电子监控证据对被告人的定罪量刑具有决定性

由于技术侦查措施对公民基本权利的侵入程度大,同时,基于权力的扩张性,技术侦查措施存

---

②关于电子监控证据的生成机制和司法实践的使用机制,可参见2012年12月26日,北京市公安局、北京市高级人民法院、北京市人民检察院联合印发的《关于刑事诉讼中适用技术侦查措施有关问题的解答》(京公法字〔2012〕1588号)。

③相关内容可参见欧洲人权法院案例ECHR,Sigurdur Einarsson and Others v. Iceland,no. 39757/15,4 June 2019.

在被滥用的风险，世界各国在使用技术侦查证据时都恪守最后使用原则[9]。在实践中，确实没有其他公开证据证明犯罪事实时，办案部门才会向技术侦查部门调取技术侦查证据。作为一种技术侦查证据，电子监控证据亦遵循最后使用原则，即以公开证据为主，电子监控证据为辅。

基于最后使用原则，电子监控证据成为对被告人定罪量刑具有决定性作用的证据。对于不需要采取监控措施的案件，侦查机关利用公开证据完成对案件事实的证明。对有必要采取监控措施的案件，则存在两种情况：一是办案部门根据技术侦查部门通报的情况，将关联监控电子数据转化为被告人供述、证人证言等公开证据；二是办案部门根据技术侦查部门通报的情况，未能完成将关联监控电子数据转化为被告人供述、证人证言等公开证据。只有第二种情况下，电子监控证据才会被调取使用。这就意味着调取使用的电子监控证据成为证明被告人犯罪事实的唯一证据，即“不提供技侦证据则不足以对被告人定罪量刑”[10]。

电子监控证据在被告人定罪量刑中发挥了决定性作用，直接影响程序的公正性。在传统的证据开示理论中，证据开示是维系对抗式诉讼模式公正高效运转的关键因素：一方面，证据开示有助于实现公诉机关和被告人之间诉讼资源的平衡，确保控辩双方能够尽量实现平等武装；另一方面，证据开示为控辩双方提供了证据信息交换的渠道，能够确保诉讼高效便捷地运转，减少诉讼资源的浪费[11]。根据之前的论述，公诉机关、审判机关和辩方均不掌握电子监控证据。虽然，没有经过证据开示的诉讼程序消耗的诉讼资源更少，诉讼运行的效率更高。但是，由于电子监控证据均为“不利于被告人的证据，甚至是关键性的定罪证据”[12]，这就会导致控辩双方对电子监控证据的质辩流于形式，被告人定罪的安全性存在的风险更高，对程序公正的影响也更大，诚如欧洲人权法院所言，辩方知悉该证据对定罪安全的影响是评估程序是否公正必须考虑的重要因素④。

（三）电子监控证据开示需要遵循必要性原则

开示电子监控证据旨在保护被告人的基本权利。一方面，证据开示关乎被告人能否获得公正的审判。获得公正审判的权利是国际人权法律的一项基本准则，要求辩方能够获得控方所掌握的所有对被告人不利或者有利的证据材料，而控方有义务为辩方接触、查阅这些材料提供便利。另一方面，电子监控证据是决定被告人定罪量刑的关键证据，被告人一旦被错误定罪，其人身自由和人格尊严权都将被剥夺。电子监控证据开示必要性考察流程如图 1 所示。

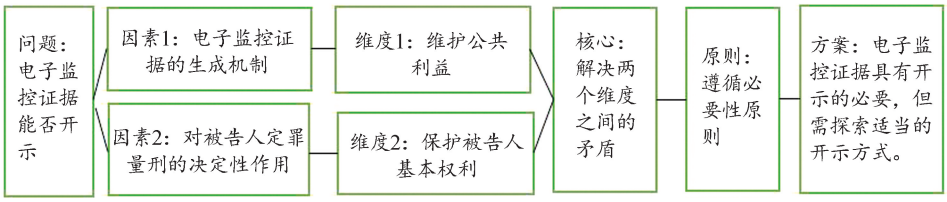

图 1　电子监控证据开示必要性考察流程

拒绝开示电子监控证据是为了保护公共利益。从功利的角度来说，在刑事诉讼程序中存在与被告人权益相冲突的利益，如国家安全、保护证人或者保守侦查秘密等。根据《德国刑事诉讼法》第 147 条第 2 款规定，案件尚未侦查终结的，如果查阅案卷有危及侦查目的之虞的，当局可以拒绝辩护

④相关内容可参见欧洲人权法院案例 ECHR，Rowe and Davis v. United Kingdom［GC］，no. 28901/95，16 February 2000.

人查阅案卷、个别文件或者查看官方保管的证据⑤。《冰岛刑事诉讼法》第37条第2款规定,如果警方认为查阅证据可能损害案件调查的,那么可以拒绝辩护律师获取案件文件副本的请求。如果当事人利益受到影响,或者国家利益、公共利益或者第三人利益处于危险当中,警方也可以拒绝辩护律师获取案件文件副本的请求⑥。《比利时刑事诉讼法》第28条、第57条、第61条规定,如果涉及未成年人,并且可能存在剥夺其获取证据复印件情形或者存在无法保护其人格的危险时,国家检察官可以拒绝向其提供证据副本。如果查阅案卷可能对他人造成危险,或者严重危害他人私生活,抑或申请人未提出查阅案卷的合法理由,预审法官可以限制其查阅或者复制案卷及相关材料的权利⑦。我国《刑诉规则》第48条规定,涉及国家秘密或者商业秘密的,同案犯罪嫌疑人在逃的;案件事实不清,证据不足,或者遗漏罪行、遗漏同案犯罪嫌疑人需要补充侦查的;有事实表明存在串供、毁灭、伪造证据或者危害证人人身安全可能的,律师以外的辩护人申请查阅、摘抄、复制案卷材料,人民检察院可以不予许可。

如何平衡被告人基本权利和公共利益之间的矛盾呢?从“目的”或“动机”来看,以维护公共利益为名,限制公民的基本权利并非不可。欧洲人权法院曾在判决中提出,在某些案件中,有必要限制辩方获得某些证据,以保护更重要的社会利益⑧。但限制被告人的基本权利应遵循必要性原则的要求,即在同等实效的情况下,“选择不限制基本权利或者限制程度明显更小的其他手段”[13]。然而,直接以保护公共利益为由,拒绝开示电子监控证据的观点违背了必要性原则的要求。因为公共利益只能表明有限制被告人基本权利的必要,而拒绝开示直接剥夺了被告人的基本权利,手段明显缺乏必要性。事实上,涉及公共利益的证据并非绝对不能开示。我国《刑诉解释》第55条规定,“案卷材料,涉及国家秘密、商业秘密、个人隐私的,应当保密;对不公开审理案件的信息、材料,或者在办案过程中获悉的案件重要信息、证据材料,不得违反规定泄露、披露,不得用于办案以外的用途”。域外法也有类似规定,如《奥地利刑事诉讼法》第52条规定,涉及其他参加人或者第三人隐私利益的,嫌疑人行使阅卷权时应当就此类信息的获取承担保密义务⑨。即使在“公共利益豁免”原则的起源地——英国,检察官基于公共利益申请免除己方证据开示的义务时,仍需要提交法庭审查,由法庭作出是否开示的决定⑩。按照上述规定的精神,电子监控证据是可以开示的,只是需要掌控好电子监控证据开示的方式。因此,制度研究的对象是适当的电子监控证据开示方式,包括入卷证据的开示方式和未入卷材料的开示方式。

二、入卷证据的开示

入卷证据包含书面卷宗材料和电子数据两个方面的材料,卷宗材料和电子数据开示方式应当

---

⑤《德国刑事诉讼法》第147条第2款的内容可参见《世界各国刑事诉讼法》编辑委员会《世界各国刑事诉讼法(欧洲卷)》(中国检察出版社,2016年版第283页)。

⑥《冰岛刑事诉讼法》第37条第2款的内容可以参见欧洲人权法院判例 ECHR, Sigurdur Einarsson and Others v. Iceland, no. 39757/15, 4 June, 2019.

⑦《比利时刑事诉讼法》第28条、第57条、第61条的内容可参见《世界各国刑事诉讼法(欧洲卷)》(中国检察出版社,2016年版第151页、第163页、第164页)。

⑧相关内容可参见欧洲人权法院案例 ECHR, Rook v. Germany, no. 1586/15, 25 July, 2019.

⑨《奥地利刑事诉讼法》第52条的内容可参见陈卫东主编《刑事辩护与代理制度:外国刑事诉讼法有关规定》(中国检察出版社,2017年版第66页)。

⑩上述内容可参见陈瑞华《比较刑事诉讼法(第二版)》(北京大学出版社,2021版第284-285页)。

有所区别。

（一）入卷证据开示的探索及分歧

我国实行阅卷制度，证据开示可以通过阅卷的方式实现。我国刑事诉讼法及司法解释将证据开示的范围限定为案卷材料，包括诉讼文书和证据材料[11]。这种开示相当于英美国家的控方履行预先提供信息义务（duty to provide advance information），即控方告知辩方将在法庭上使用的指控材料[12]。因此，我国电子监控证据开示的是纳入监控卷宗，准备作为指控依据的卷宗材料和电子数据。

就入卷证据的开示，目前实践中的探索性做法是司法机关要求辩方签署保密协议，然后向辩方开示电子监控证据，但在具体方式上存在分歧：一是关于监控卷宗的开示，一些司法机关允许辩方查阅、摘抄和复制监控卷宗，而少数司法机关认为，电子监控证据涉及公共利益，只能查阅，不能摘抄和复制；二是关于监控电子数据的开示，部分司法机关允许辩方查阅、摘抄和复制监控电子数据，而个别司法机关则认为，复制监控电子数据可能泄露技术方法，开示应仅限于查阅、摘抄，不能复制。

（二）入卷证据开示存在的问题及理论分析

入卷证据开示的分歧源于阅卷方式缺乏层次性。我国刑事诉讼法笼统规定，凡属案卷材料，辩方均可查阅、摘抄和复制[13]。同时，对于涉及国家秘密或者有碍侦查的，司法机关对辩方查阅、摘抄和复制的申请，可以不予准许[14]。由此可见，刑事诉讼法没有区分证据的表现形式，立法较为概括，缺乏精细化的规定，进而导致电子监控证据开示局限于开示与不开示的二元框架。由于入卷证据涉及国家秘密，开示该证据可能妨碍侦查，故司法机关通常会以此为由拒绝辩方的开示申请。事实上，涉及公共利益与基本权利之间的矛盾，禁止保护不足和禁止过度侵害互为“镜像”，让权力机关承担保护被告人基本权利的义务，目的在于禁止对被告人基本权利造成过度的侵害[15]。域外法治国家通过个案的平衡来实现公共利益与基本权利之间的平衡，在其刑事诉讼法典中既有不予开示的规定，也有准予开示的措施。基于我国刑事证据规范体系，应当细化电子监控证据开示的规定，从而有效保护被告人的基本权利。

建构有层次的入卷证据开示制度，其现实基础是监控卷宗和电子数据承载的内容不同。监控卷宗包括诉讼文书和证据材料，用以证明监控措施的合法性和电子监控证据的内容。一旦泄密，可以通过回溯知悉卷宗内容的人员，锁定泄密者。通过签署保密协议，能够控制监控卷宗开示的风险。而监控电子数据除了前述内容外，还涉及监控技术。在监控措施的实施中，侦查人员在犯罪嫌疑人没有感知的情况下，利用技术手段截获大量犯罪信息。如果监控技术被暴露，监控措施将面临手段失效的问题。为了确保监控技术的有效运用，监控卷宗和电子数据的开示方式应当有所区别。同时，如果技术手段泄密，难以建立泄密者与被泄露技术之间的关联性，而签署保密协议不足以防

---

⑪参见：2018年《中华人民共和国刑事诉讼法》（第40条、《刑诉解释》第53条、《刑诉规则》第47条、第48条。

⑫关于预先提供信息义务，可参见陈瑞华《比较刑事诉讼法（第二版）》（北京大学出版社，2021版第278页）。

⑬参见：《刑诉法》第40条规定，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。其他辩护人经人民法院、人民检察院许可，也可以查阅、摘抄、复制前述材料。

⑭参见：《刑诉规则》第48条规定，律师以外的辩护人申请查阅、摘抄、复制案卷材料，涉及国家秘密的；同案犯罪嫌疑人在逃的；案件事实不清，证据不足，或者遗漏罪行、遗漏同案犯罪嫌疑人需要补充侦查的；有事实表明存在串供、毁灭、伪造证据或者危害证人人身安全可能的，律师以外的辩护人申请查阅、摘抄、复制案卷材料，人民检察院可以不予许可。

⑮参见：小山刚《基本权利保护的法理》（吴东镐，崔冬日译，中国政法大学出版社，2021年版第88-90页）。

控监控技术泄密的风险。

(三)监控卷宗开示的有效路径

准许向辩方开示监控卷宗是综合考虑卷宗开示的重要性和弊害程度的结果。查阅、摘抄和复制监控卷宗可能产生泄露技术侦查方法的风险,但签署保密协议能够控制这种风险,同时查阅、摘抄和复制监控卷宗可以充分保障被告人的基本权利。

首先,自审查起诉之日起,辩方可以到人民检察院、人民法院查阅监控卷宗。欧洲人权法院在马坦诺维奇诉克罗地亚案中提出,必要时间内不受限制地查阅案卷档案,是获得公正审判的重要保障[16]。具体而言,查阅监控卷宗可以保证辩方充分了解电子监控证据的来源和内容:一方面查阅采取监控措施的程序性材料,便于辩方对证据的合法性进行检验,避免非法电子监控证据成为定案的依据;另一方面查阅监控译文等内容信息,能够与监控电子数据进行比对,确保电子监控证据内容的可靠性和准确性。

其次,辩方可以根据查阅的内容,摘抄监控卷宗。域外刑事诉讼法普遍赋予辩方摘抄卷宗材料的权利,如《保加利亚刑事诉讼法》第55条规定,被告人享有知晓案情的权利,包括利用特殊情报设备获取的信息以及进行必要的摘录[17]。《俄罗斯刑事诉讼法》第47条、53条、217条规定,刑事被告人、辩护人在预先审查结束后有权了解案件的全部材料,并从中摘录信息[18]。《奥地利刑事诉讼法》第52条规定,犯罪嫌疑人可以在技术允许的范围内自行制作副本[19],自行制作方式包括摘抄。

最后,辩方可以复制监控卷宗。通过复制,辩方就能获取与控方掌握的图文相同的案卷材料,不仅可以查看案卷的内容,而且能够审查其表现形式。由于监控卷宗的内容和表现形式均与监控技术无关,因此可以复制。目前有两种复制卷宗的模式:一种是有偿方式,如《奥地利刑事诉讼法》第52条规定,嫌疑人可以申请有偿获得卷宗影印件或者其他重现卷宗内容文本的副本[20];另一种是无偿方式,如《德国刑事诉讼法》第147条规定,无辩护人的嫌疑人可以在辩护所需的范围内,依申请获取案卷信息或者影印件[21]。我国采取的是无偿复制方式,我国《刑诉规则》第49条规定,辩护人复制案卷材料,不收取费用。

(四)监控电子数据开示的完善路径

监控电子数据是指通过监控技术获取,记录和保存在特定介质中,与犯罪有关的电子数据。《中华人民共和国刑事诉讼法》(以下简称《刑事诉讼法》)及其司法解释规定,辩护人可以查阅、摘抄、复制的案卷材料包括诉讼文书和证据材料。但是,证据材料是否包涵监控电子数据,缺乏明确的法律规定。我国《刑诉规则》第49条规定,应当设置电子案卷阅卷终端设备,为辩护人阅卷提供

---

⑯参见:欧洲人权法院案例 ECHR, Matanovic v. Croatia, no. 2742/12, 4 April, 2017.

⑰《保加利亚刑事诉讼法》第55条的内容可参见陈卫东主编《刑事辩护与代理制度:外国刑事诉讼法有关规定》(中国检察出版社,2017年版第76页)。

⑱《俄罗斯刑事诉讼法》第47条、53条、217条的内容可参见陈卫东主编《刑事辩护与代理制度:外国刑事诉讼法有关规定》(中国检察出版社,2017年版第118页、第122页、第126页)。

⑲《奥地利刑事诉讼法》第52条的前述内容可参见陈卫东主编《刑事辩护与代理制度:外国刑事诉讼法有关规定》(中国检察出版社,2017年版第66页)。

⑳《奥地利刑事诉讼法》第52条的前述内容可参见陈卫东主编《刑事辩护与代理制度:外国刑事诉讼法有关规定》(中国检察出版社,2017年版第66页)。

㉑关于《德国刑事诉讼法》第147条的内容可参见陈卫东主编《刑事辩护与代理制度:外国刑事诉讼法有关规定》(中国检察出版社,2017年版第95页)。

便利,同时准许辩护人采取复印、拍照、扫描、刻录的方式查阅、摘抄、复制案卷材料。有观点认为,《刑诉规则》第49条已经准许辩方查阅、摘抄、复制电子数据。事实上,该规定针对的是案卷材料,复制刻录的是数字化的诉讼文书和证据材料。

2013年9月22日,最高人民法院刑事审判第二庭就辩护律师能否复制侦查机关讯问录像的问题作出批复。该批复认为,侦查机关对被告人的讯问录音录像已经作为证据材料向人民法院移送并已在庭审中播放,不属于依法不能公开的材料,在辩护律师提出要求复制有关录音录像的情况下,应当准许[22]。于是有观点提出,虽然同步录音录像以电子数据的形式出现,但其已经作为结果证据,可以成为查阅、摘抄、复制的对象[14]。然而,准许查阅、摘抄、复制同步录音录像,并不能推导出可以查阅、摘抄、复制监控电子数据的结论。由于监控电子数据的载体承载着监控的技术方法,所以监控电子数据的开示不仅涉及数据的内容,还涉及数据的载体。而同步录音录像虽然以数据化形式呈现,但其载体承载的技术方法与案件不存在关联性。同步录音录像属于以数据赋能智慧案件管理建设的范畴,与证据开示并不相同[15]。

基于监控电子数据的特性,监控电子数据的开示应当遵循区分原则,采取差异化的开示方式,寻求保障被告人基本权利和维护公共利益之间的平衡。具体而言,应当允许辩方查阅、摘抄监控电子数据,基于保护技术侦查方法的目的,对辩方提出复制监控电子数据的请求可不予准许。从域外刑事诉讼法的规定看,准许辩方查阅电子数据,限制辩方获取电子数据副本是通行的做法,如《奥地利刑事诉讼法》第52条规定,犯罪嫌疑人不能获得普遍禁止的或者内容涉及可以推断出个人身份或者生活情况的录音录像的副本[23]。欧洲人权法院亦认为,如果将涉及他人隐私或者国家秘密的材料全部向辩方开示,并不恰当。在签署保密协议的情况下,查阅、摘抄监控电子数据,与查阅、摘抄监控卷宗无异,不会泄露监控措施使用的技术设备和方法,有利于保护技术侦查方法,而查阅、摘抄监控电子数据可与已经获取的监控卷宗进行比对,达成证据开示的目的。但就复制而言,签署保密协议不足以防控监控技术设备和方法泄露的风险,在能够实现证据开示功能的情况下,没有必要进行复制。

三、未入卷材料的开示

电子监控证据的开示不仅包括入卷证据的开示,还包括未入卷材料的开示,但未入卷材料的开示应当有别于入卷证据。

(一)未入卷材料开示制度的缺失

我国刑事诉讼法及其司法解释确立的证据开示系入卷证据的开示。对控诉机关不准备作为证据使用,没有纳入案卷的材料,辩方难以获得查阅、摘抄和复制的机会,因而对其无从知悉,即便知悉后申请司法机关调取,也难以获得支持[24]。而在英美法系国家,对于检察官不准备在法庭上使用的材料,检察官都有向辩方开示的义务,只要这些材料能削弱控方的指控或者增强被告人辩护,这

---

[22]参见:2012年9月22日,最高人民法院刑事审判第二庭《关于辩护律师能否复制侦查机关讯问录像问题的批复》[(2013)刑他字第239号]。

[23]关于《奥地利刑事诉讼法》第52条的前述内容可参见陈卫东主编《刑事辩护与代理制度:外国刑事诉讼法有关规定》(中国检察出版社,2017年版第66页)。

[24]关于辩方难以获得查阅、摘抄和复制的机会可参见陈瑞华《刑事诉讼法》(北京大学出版社,2021版第257页)。

种义务被称为展示的义务(duty of disclosure)㉕。由于监控获取的海量电子数据可能包含对被告人定罪量刑有决定性意义的材料,因此,未入卷材料具有开示的必要。

现阶段,关于未入卷监控电子数据的开示,学者提出了两种方案:一是赋予辩方数据访问的权利,控方需要向辩方提供一个完整的"比特流备份";二是赋予辩方接触数据的权利,当被告人被采取强制措施之后,辩方可接触到全部的监控电子数据。这两种方案是否符合证据理论和司法实践的需求,有待进一步考察。

(二)未入卷材料开示的两种方案评析

1. 向辩方提供完整数据复制件

2017年,在欧洲人权法院审理的马坦诺维奇诉克罗地亚案中,辩护人提出,控方没有向辩方提供完整的数据复制件,损害了被告人获得公正审判的机会㉖。这一观点得到了我国学者的认同,他们提出在司法信息化的背景下,应当赋予刑事被告人数据访问权,具体到操作层面,控方应当制作一个完整的"比特流备份"交给辩方㉗。但这一观点存在两个问题:一是违背了比例原则的均衡性要求。根据比例原则的均衡性要求,国家机关采取的手段给当事人造成的利益损失,应当与所追求的目的成比例。入卷筛选是按照与案件事实的关联程度进行的,入卷电子数据与案件事实的关联性更大,对案件的证明价值更高,不开示将对被告人的基本权利造成更大的损害;而未入卷电子数据与案件事实的关联性更小,对案件的证明价值更低,相较于入卷证据,不开示对被告人的基本权利造成的损害更小。根据前面的讨论,出于保护技术侦查方法的目的,辩方不能复制入卷电子数据。假设准许复制关联性弱的未入卷电子数据,而关联性更强的入卷电子数据却不能复制,那么手段和目的缺乏均衡性。此外,未入卷电子数据也承载了监控技术方法,一旦准许复制未入卷电子数据,将架空不允许辩方复制入卷电子数据的制度设计。二是误读数据访问权的内容。《刑事司法的欧盟2016/680号指令》第14、15条规定,"查阅访问数据的权利对于信息主体,特别是被追诉人而言'生死攸关',只有当辩方有权查询访问相关个人数据时,方能对公权力机关所掌握的信息和证据有充分了解,辩护才能有的放矢"[16]。由此可见,赋予辩方数据访问权的目的是让辩方充分了解控方证据,以实现平等武装,保证双方在平等条件下进行诉讼竞技与对抗。数据访问权更接近访问或者接触数据的权利。至于欧盟《通用数据保护条例》㉘规定的数据主体都可以获得个人数据复制件,则是数据访问权的延伸。因此,赋予辩方数据访问权并不等同于准许辩方复制未入卷监控电子数据,控方尊重和保障辩方数据访问的权利也不意味着控方有向辩方提供完整数据复制件的义务。在这个问题上,欧洲人权法院的观点颇具启发意义。在洛克诉德国案中,欧洲人权法院明确表示,没有必要让申请人的律师听阅所有监控电子数据。原则上,控方只要为辩护律师提供一个可以有效分析的机会,以便其可以识别并听阅相关的数据即可㉙。质言之,开示监控电子数据没有必要向辩方提供所有的监控电子数据,而只需要给辩方提供一个能够接触数据的机会即可。

㉕关于展示的义务的内容可参见陈瑞华《比较刑事诉讼法(第二版)》(北京大学出版社,2021版第278页)。

㉖关于马坦诺维奇诉克罗地亚案的案情及裁判理由可参见欧洲人权法院案例ECHR,Matanovic v. Croatia,no. 2742/12,4 April,2017.

㉗关于控方应当制作一个完整的"比特流备份"交给辩方可参见陈永生《电子数据搜查、扣押的法律规制》(《现代法学》,2014年第5期第124页)。

㉘GDPR(General Data Protection Regulation),全称《通用数据保护条例》,为欧洲联盟的条例,前身是欧盟在1995年制定的《计算机数据保护法》,2018年5月25日出台。

㉙关于洛克诉德国案的案情及裁判理由可参见欧洲人权法院案例ECHR,Rook v. Germany,no. 1586/15,25 July,2019.

2. 赋予辩方接触数据的权利

准许辩方接触到全部的监控电子数据是德国等欧洲国家的惯常做法。如在洛克诉德国案中，德国法院在洛克被采取强制措施之后，准许辩护人在工作时间到检察官办公室，通过一台特殊的电脑，查阅所有的监控电子数据。那么，我国可否赋予辩方接触数据的权利呢？答案是否定的，具体理由如下。

其一，赋予辩方接触数据的权利可能造成程序的冗余。虽然欧洲人权法院认为，不开示任何证据都会影响辩方的权利，不仅应当开示控方认为与案件相关的证据，而且控方在指控中没有考虑或者认为并不相关的材料也应当开示。但欧洲人权法院又提出，在考察辩方是否获得公正审判时，需要评估诉讼的性质、阶段和案件的复杂程度。由此可见，欧洲人权法院主张根据证据对案件诉讼的必要性，决定是否开示证据，同时认为没有必要让申请人的律师接触到所有监控电子数据。

其二，控方没有必要为辩方提供接触所有数据的渠道，赋予辩方接触数据权利的作用十分有限。以洛克诉德国案为例，虽然德国国内法院为辩护人提供了可以查阅所有监控电子数据的渠道，但是辩方没有通过该渠道，逐一筛查未入卷电子数据，因为辩方，尤其是被告人清楚数据的内容，能够迅速确定需要开示的未入卷电子数据。

其三，基于我国司法实践，让辩方接触未入卷电子数据存在现实困境。根据职能分工，技术侦查部门负责监控的实施，按照办案部门、公诉机关、审判机关的要求，调取、提供、调查核实电子监控证据，而技术侦查部门没有向辩方提供电子监控证据的义务。不仅如此，办案部门、检察机关、法院也不能接触到所有的电子数据，如果他们对入卷的监控电子数据有疑问，需要向技术侦查门申请查阅，其查阅到的仍是经过技术侦查部门筛选的部分电子数据，既然办案部门、公诉机关、审判机关都接触不到所有的未入卷电子数据，又遑论准许辩方接触到全部的监控电子数据？

综上所述，在未入卷材料的开示中，向辩方提供完整的数据复制件或者赋予辩方接触数据的权利的方案皆不可行。

（三）未入卷电子监控证据开示制度的构建

考察和评析向辩方提供完整的数据复制件和赋予辩方接触数据的权利两种方案，目的是对两种方案进行比较和扬弃，从而提出一种更加妥适的方案。结合我国刑事司法实践，应当采取有限开示的方式，向辩方提供数据清单和入卷数据选择的标准，同时辩方享有提出异议、申请调取关联数据的权利。

1. 向辩方提供数据清单

首先，对未入卷电子监控证据而言，向辩方提供数据清单是最佳的选择。数据清单为辩方提供了获取监控数据信息的渠道，有助于解决未入卷电子监控证据开示必要性的问题。数据清单承载的信息均为非内容信息[17]，限缩了开示证据的范围，能够避免完全开示证据造成的程序冗余。同时，数据清单提供了充足的非内容信息，以便快速确定未入卷电子监控证据中具有关联性的数据，确保证据开示的有效性。

其次，数据清单应满足数据完整性和适当性的要求。一方面，数据清单中载明的数据应当囊括技术侦查部门通过监控措施获取的全部数据；另一方面，数据清单只提供通信主体的身份信息，例如手机号码、身份证号码、IP 地址等，通信的时间（包括通信开始和结束的时间）及通信的时长，监控电子数据的技术识别码和检索链接等有限的非内容信息。

再次,向辩方提供数据清单具备可行性。从数据清单的内容看,其与司法实践中普遍使用的通话记录类似。既然调取通话记录在技术上是可行的,生成数据清单也应当是可行的。就数据清单的使用而言,如前所述,辩方,尤其是被告人十分清楚数据的内容和生成时间,通过特定通信号码、IP地址等非内容信息,可以缩小检索的范围,找到对被告人有利的数据,而数据清单中的技术识别码和检索链接,有助于快速检索到与案件相关的数据。

最后,域外法治国家已采取向辩方提供数据清单的方式。在洛克诉德国案中,欧洲人权法院作为欧洲最重要的人权保障机构,其在判决中已经认可控方向辩方提供数据清单的做法,欧洲人权法院判定德国国内法院不违反《欧洲人权公约》的规定,控方向辩方提供数据清单是重要考量因素之一。

2. 向辩方提供数据选择的标准

提供数据清单是为了便于辩方检验技术侦查部门通过监控手段获取的全部电子数据。数据选择的标准,不仅可以将数据清单中的数据区分为入卷数据和未入卷数据,而且可以为辩方提供查验数据是否准确的机会,正如欧洲人权法院所说,提供数据选择的标准等同于向辩方提供检索数据的参数。数据选择的标准通常是以说明的形式呈现,包含以下内容:一是通信的主体,通信的时间和通信的时长,数据的技术识别码和检索链接等,通过这些信息建立数据与数据清单之间的联系;二是与案件的关联性,按照美国《联邦证据规则》第401条规定,关联性是指证据对案件事实更有可能或更无可能的证明趋势。关联性须同时满足实质性和证明性两个条件,利用对案件事实证明趋势的有无建立数据与案件之间的联系。

向辩方提供数据选择的标准,可以达到两个目的:一是筛查遗漏数据,辩方可以结合数据清单和数据选择的标准,利用被告人熟悉通信内容的有利条件,通过通信主体和通信的时间,筛查出其他可能与案件关联的数据,检视控方选择纳入案卷数据的全面性;二是为辩方提出异议、申请调取关联数据提供线索和依据。辩方通过查阅数据选择的标准,可以找出数据开示存在的问题,从而为其提出异议找到恰当的理由和必要的线索。

需要说明的是,提供数据选择的标准不同于辩方参与制定数据选择的标准。欧洲人权法院曾在判决中提出,辩方参与制定入卷数据选择的标准是被告人获得公正审判的重要保障。为此,应当赋予辩方参与制定数据选择标准的权利。该权利不仅包括获得数据选择标准的权利,还包括辩方参与修正数据选择标准的权利。与欧洲国家相比,我国辩护律师调取证据的权限较小,辩护律师不能通过自行调查取证来修正控方选择数据的标准,而是需要借助公诉机关、审判机关的权力来调取证据,才能实现修正数据选择标准的目的。因此,结合我国司法实践,目前尚不具备让辩方制定数据选择标准的条件,而赋予辩方获得选择数据标准的权利更为实际。

3. 赋予辩方提出异议、申请调取关联数据的权利

赋予辩方提出异议、申请调取关联数据的权利是提供数据清单和数据选择标准的必然延伸。辩方通过查阅数据清单,发现未入卷数据中遗漏了对被告人有利的部分,然后通过审查数据选择标准,找到数据选择标准存在的问题、线索和材料。为了维护自己的诉讼权益,辩方必然会就此提出异议。因此,域外法治国家通过立法,赋予辩方提出异议、申请调取关联数据的权利。如《日本刑事诉讼法》第316条之20规定,辩方可以请求证据(等同于我国的入卷证据)之外证据的开示,但需要明确足以识别与开示请求相关的证据、与开示请求相关的证据的关联性、开示对被告人辩护必要性

的理由。又如《荷兰刑事诉讼法》第 34 条规定，犯罪嫌疑人可以请求检察官将其认为与案件评估有关的特定材料纳入诉讼材料。对荷兰的犯罪嫌疑人来说，如果认为未入卷的监控数据中存在与案件评估有关的特定数据，那么犯罪嫌疑人可以请求检察官将其纳入诉讼材料。

然而，由于监控电子数据存储在我国技术侦查部门特定介质当中，并不由公诉机关和审判机关掌握，辩方只能申请人民检察院、人民法院调取相关数据。根据我国《刑事诉讼法》第 41 条规定，辩护人认为在侦查、审查起诉期间，公安机关、人民检察院收集的证明犯罪嫌疑人、被告人无罪或者罪轻的证据材料未提交的，有权申请人民检察院、人民法院调取。但实践中对存在疑问的监控电子数据，审判人员通常采用的是庭外核实的方式进行审查，这种方式值得商榷。结合《刑诉解释》第 120 条的规定，审查核实技术侦查措施收集的证据材料有三种方式：一是常规方式，对于采取技术调查、侦查措施收集的证据材料，经过当庭出示、辨认、质证等法庭调查程序进行查证；二是保护性方式，如果当庭调查技术调查、侦查证据材料可能危及有关人员的人身安全，或者可能产生其他严重后果的，应当采取不暴露有关人员身份和技术调查、侦查措施使用的技术设备、技术方法等保护措施；三是必要时，审判人员可以在庭外对证据进行核实。这三种方式之间呈递进关系，只有前一种方式不足以保护人员和技术的安全时，才能考虑适用下一个层次的核实方式。直接采取庭外核实的方式审查监控电子数据有悖于《刑诉解释》第 120 条的规定。

基于此，有必要赋予辩方提出异议、申请调取关联数据的权利。具体而言，辩方申请调取数据之后，人民检察院、人民法院要对其请求进行审查，区分情况进行处理：如果认为辩方的异议成立，申请调取的数据与案件事实有联系，那么依法向技术侦查部门调取辩方认为有关联的电子数据，并按照入卷电子监控证据开示的方式进行开示。如果认为辩方的异议不成立，则决定不予调取，并向辩方说明理由。这样才能实现制度整体的逻辑自洽。电子监控证据开示流程如图 2 所示。

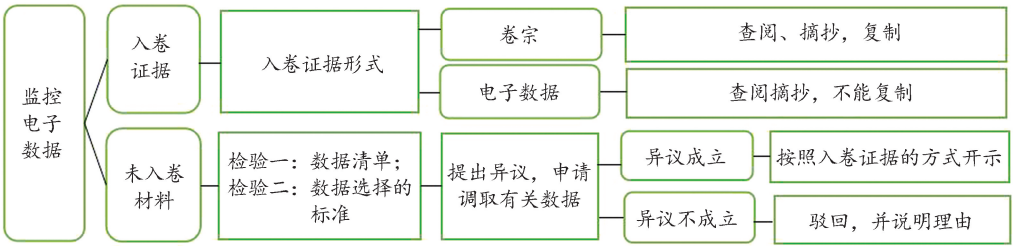

图 2　电子监控证据开示流程

四、结语

电子监控证据对被告人定罪量刑具有决定性作用，司法机关直接以保护公共利益为由拒绝开示电子监控证据违背了必要性原则的要求。通过比较研究发现，域外法治国家采用个案平衡决定是否开示电子监控证据的方法，不利于我国电子监控证据开示制度的完善。基于我国的法律规定和司法实践，应当按照入卷证据和未入卷证据的二元框架，建构差异化的电子监控证据开示制度。具体而言，细化入卷证据开示的规定，准许辩方查阅、摘抄、复制电子监控卷宗，查阅、摘抄监控电子数据，但不能复制监控电子数据。同时，对于未入卷证据的开示，域外法规定的向辩方提供完整的数据复制件和赋予辩方接触数据的权利的方案均不符合我国司法实际，未入卷证据的开示应当采取有限开示的方式，即控方向辩方提供数据清单和数据选择的标准，同时辩方享有提出异议、申请

调取关联数据的权利。

参考文献:

[1]龙宗智.刑事程序论[M].北京:法律出版社,2021:266.

[2]郑曦.超越阅卷:司法信息化背景下的刑事被告人数据访问权研究[J].河南大学学报(社会科学版),2020(2):59-65.

[3]陈永生.电子数据搜查、扣押的法律规制[J].现代法学,2014(5):111-127.

[4]陈瑞华.刑事诉讼法[M].北京:北京大学出版社,2021:256.

[5]柳永.大数据背景下电子数据行刑衔接机制研究[J].行政法学研究,2018(5):127-135.

[6]龙宗智.中国法语境中的检察官客观义务[J].法学研究,2009(4):137-156.

[7]约翰·斯普莱克.英国刑事诉讼程序[M].徐美君,杨立涛,译.北京:中国人民大学出版社,2006:187-192.

[8]龙宗智.刑事诉讼中的证据开示制度研究(上)[J].政法论坛,1998(1):3-10,14.

[9]喻海松.刑事诉讼法修改与司法适用疑难解析[M].北京:北京大学出版社,2021:169.

[10]李晓林,赵丹.毒品犯罪案件中技术侦查证据的审查和运用[J].人民司法(案例),2016(17):17-19.

[11]陈瑞华.比较刑事诉讼法[M].2版.北京:北京大学出版社,2021:277.

[12]程龙.论大数据证据质证的形式化及其实质化路径[J].政治与法律,2022(5):96-114.

[13]小山刚.基本权利保护的法理[M].吴东镐,崔冬日,译.北京:中国政法大学出版社,2021:86-87.

[14]谢小剑.讯问录音录像的功能发展:从过程证据到结果证据[J].政治与法律,2021(8):149-161.

[15]李云.以数据赋能智慧案管建设[J].人民检察,2022(15):76.

[16]郑曦.刑事诉讼个人信息保护论纲[J].当代法学,2021(2):115-124.

[17]刘梅湘.侦查机关实施网络监控措施的程序法规制:以域外法的相关规定为参照[J].法商研究,2017(1):174-182.

Research on the discovery of the electronic surveillance evidence

ZHOU Wei

(*Law School, Southwest University of Political Science and Law, Chongqing 401120, P. R. China*)

Abstract: The discovery of electronic surveillance evidence not only touches public interests, but also involves the defendant's right to a fair trial. It is of great significance to explore an appropriate discovery system of electronic surveillance evidence for balancing public interests and individual fundamental rights. Through normative analysis and comparative research, it is revealed that the generation mechanism of electronic surveillance evidence is not transparent, and public prosecution and judicial organs may refuse to discovery electronic surveillance evidence on the grounds of public interest immunity. At the same time, due to the principle of last used, electronic surveillance evidence is decisive for the defendant's conviction and sentencing, refusal to discovery it will inevitably affect the individual fundamental rights of citizens. From the perspective of purpose or motivation, individual fundamental rights of citizens can be restricted in the name of safeguarding public interests, but under the same effect, other means should be chosen that do not restrict the individual fundamental rights of citizens or that are significantly less restrictive. Refusal to discovery electronic surveillance evidence directly on the grounds of protecting public interests violates the requirements of the principle of necessity. Therefore, it is necessary to explore appropriate methods of electronic surveillance evidence discovery. In China's criminal proceedings, the electronic surveillance evidence to discovery is dossier materials and associated electronic data, which are incorporated into the surveillance dossier and ready

to be served as the basis for charges. The methods of discovery are to view, extract and copy. The disadvantage of this institutional arrangement is that, on the one hand, for the electronic surveillance evidence incorporated into the surveillance dossier, the Criminal Procedure Law does not distinguish between dossier materials and electronic data, and lacks refined regulations, which leads to the discovery of electronic surveillance evidence being limited to the dual model of discovery and non-discovery. On the other hand, it is difficult for the defense to obtain opportunities to view, extract and copy materials that the prosecution agency is not prepared to use as evidence, and is not incorporated into the surveillance dossier, so they have no way of knowing about it. In fact, the secrets carried by dossier materials and electronic data are different, and the discovery methods of them should be differentiated. The massive electronic data obtained by electronic surveillance may contain materials that are decisive for the defendant's conviction and sentencing, it is necessary to discovery the materials that are not incorporated into the surveillance dossier. In view of this, it is necessary to construct a differentiated electronic surveillance evidence discovery system according to the dual framework of electronic surveillance evidence incorporated into the surveillance dossier and not incorporated into the surveillance dossier. For the discovery of electronic surveillance evidence incorporated into the surveillance dossier, the defense may be required to sign a confidentiality agreement, allowing to view, extract, and copy the dossier materials, and to view and extract the associated electronic data. However, due to the protection of the technology of electronic surveillance, the defense's application for a copy of the associated electronic data may not be allowed. For the discovery of electronic surveillance evidence not incorporated into the surveillance dossier, the prosecution is obliged to provide the defense with a list of data and criteria for the selection of associated electronic data, and the defense has the right to raise objections and apply for access to linked data.

Key words: electronic surveillance evidence; the discovery of evidence; to review case files; the right to access data; the principle of necessity

（责任编辑　胡志平）