主题研讨:数字法学前沿问题

通信记录数据调取的合比例性

郭旨龙

内容提要:通信记录数据调取是打击犯罪、治理社会的重要制度。现行的通信隐私分析框架构建于简单、静态、二元的通信数据结构之上,但其理论假设,即第三人规则,在现代日益复杂的信息技术环境中愈发难以成立。基于内容与非内容数据的法律保护的传统区分,与现代通信技术运作中用户数据和流量数据生成、交换和存储的方式日益不兼容,与现代通信中个人隐私和个人信息保护的正当期待愈发背离,是对通信数据形式和类型的不合理区别对待。未来需要一个统一的标准化法律框架,匹配阶层化的调取措施以落实实质法治。复杂动态多元的通信数据分类分级结构为隐私分析提供了一个实用的替代方案,即权利干预程度的多阶层对应权利干预必要性的多阶层。该方案足够灵活,可以适应迅速发展的通信技术。

关键词:通信秘密　第三人规则　镶嵌理论　数据分级

郭旨龙,中国政法大学刑事司法学院网络法学研究所副教授。

一　引　言

在日常生活中,动态性数据伴随着人们随身携带设备的使用在持续地发生流动和存储活动,这些电子通信数据日益成为打击犯罪、治理社会,进而满足公民安全期待的重要辅助。这些数据虽部分为行为人占有和保存,但大部分由电信和网络运营商、服务商、移动设备系统商等第三方存储,其在数据的读取、查看、接触和控制上具有技术便利和制度便利。公安机关、国家安全机关等有权机关开始常态化地向具有配合义务法律外观的第三方调取通信记录数据。

《网络安全法》《数据安全法》有关数据调取条款的出台、解释与适用,存在着与《民事诉讼法》《行政诉讼法》《刑事诉讼法》《监察法》等法律以及相关司法解释〔1〕、部门

〔1〕 如2016年《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》、2019年《人民检察院刑事诉讼规则》。

规章〔2〕进行衔接和协调的问题。这些问题首先体现在法律保留与比例原则上:法律保留要求有相关法规范,且公开、明确,符合形式法治的原则;比例原则要求相关法规范的条件与所欲达成之目标合乎正当比例,满足实质法治的精神。

针对通信记录〔3〕法律保留问题,宪法学界的主流观点是通信数据二元结构论。〔4〕有研究区分了通信的内容信息和非内容信息,认为我国宪法第 40 条两款的通信秘密都只保护通信的内容信息,通信的非内容信息则属于隐私权和个人信息相关权益的保护内容。〔5〕也有研究认为,第 40 条的通信秘密保护存储在服务商处的通信内容信息和非内容信息,但区分了通信的内容信息和非内容信息,认为第 2 款的宪法保留只适用于内容信息,非内容信息适用简单的法律保留。〔6〕还有研究认为,第 40 条的通信秘密保护所有的通信内容信息和非内容信息,但也认为第 2 款的宪法保留只适用于内容信息。〔7〕三者的共同之处是都认为宪法保留只适用于内容信息,不适用于非内容信息。只有内容层面的通信秘密隐私利益才值得特别的宪法保留,对其减损需满足宪法规定的条件;而非内容层面的通信秘密隐私利益则只需简单的法律保留,对其减损不与宪法冲突即可。早期并未将流量数据与通信内容的获取置于同一层面,因为从隐私利益和数据保护角度,通信内容的获取会产生更多不利影响;但现在,这种观点的争议越来越大,欧盟早已从只处理通信内容的机密性转变为平等对待内容数据和流量数据(在此包括位置数据),要求会员国确保其保密待遇。〔8〕

更重要的是,通信记录二元结构论的适用和判断过程也并不简单明了。宪法学者已经意识到了这种判断过程可能存在的复杂性,认为要考虑技术上能否准确区分以及实践中的部门程序规范和技术是否区分了两类信息对应的数据及其调取等问题;甚至还提出,如果无法区分,或公权力机关无法论证是不是内容信息的数据,则推定为需要严格保护的揭示内容信息的数据。〔9〕

二 简单静态二元的通信数据结构

判断结论上的简单二元结构容易导致判断过程中的静态简单二元结构。简单二元说

〔2〕 如公安部 2020 年修正的《公安机关办理刑事案件程序规定》(下称“《刑事案件程序规定》”)、公安部 2019 年《公安机关办理刑事案件电子数据取证规则》(下称“《电子数据取证规则》”)、国家网络信息办公室 2017 年《互联网信息内容管理行政执法程序规定》。

〔3〕 承载通信秘密的通信数据包括通话记录和通讯记录,本文将二者统称为通信记录。

〔4〕 通信记录数据调取形式合法性的首要要求是,不得与宪法上的明确规范产生冲突;即使经过解释,认为不适用特别的宪法保留,也要适用一般性的简单的法律保留,在法律上有所依据。参见郭旨龙:《通信记录数据调取的形式合法性》,《国家检察官学院学报》2021 年第 6 期,第 19 页。

〔5〕 参见杜强强:《法院调取通话记录不属于宪法上的通信检查》,《法学》2019 年第 12 期,第 78 页。

〔6〕 参见王锴:《调取查阅通话(讯)记录中的基本权利保护》,《政治与法律》2020 年第 8 期,第 107 页。

〔7〕 参见张翔:《通信权的宪法释义与审查框架——兼与杜强强、王锴、秦小建教授商榷》,《比较法研究》2021 年第 1 期,第 33 页。

〔8〕 See Ian Walden, Communications Privacy, in Ian Walden ed., *Telecommunications Law and Regulation*, Oxford University Press, 2018, pp. 652-653.

〔9〕 参见张翔:《通信权的宪法释义与审查框架——兼与杜强强、王锴、秦小建教授商榷》,《比较法研究》2021 年第 1 期,第 46 页。

把通信数据简单区分为内容数据和非内容数据,静态是指某一通信数据从生成那刻起就确定归属于内容数据或非内容数据。

(一)通信数据二元类型结构保护程度的区分

2001 年欧洲理事会《网络犯罪公约》(*Convention on Cybercrime*,下称"《公约》")区分了内容数据,流量数据和用户信息。《公约》第 1 条第 4 款规定了流量数据,第 18 条第 3 款规定了用户数据,但内容数据并未被《公约》所明确定义。[10] 虽然《公约》将通信数据分为以上三大类,但其规则设定的思路其实是基于二元类型结构。

区分内容数据和非内容数据的数据类型结构在保护程度判断上的主要影响在于其静态地划分各类数据的保护程度,出现了双层布置的通信隐私权保护体系。因为元数据被宣称为只是被请求的总共的、原初的数据,而不是精确的数据,即使很多时候它更有价值,但却被当作没有价值来对待,有的行为主体甚至公开地低估或否认其价值,借此营造元数据价值和重要性较低的错觉。[11] 将位置数据和流量数据作为元数据进行标注会对各机构的权力产生影响,元数据是关于数据的数据,是技术性信息,这种话语使得有权机关可以经由更低的法律限制而调取保留的相关数据。公约相关专家组认为,各国刑事调查实践中最需要的数据类型是用户数据,其次是流量数据,最后是内容数据;与获取流量数据、特别是内容数据相比,获取用户数据对个人权利的干扰较小,各国应通过区分流量数据和用户数据,充分执行公约第 18 条,以便依据国内立法规定获取用户数据。[12] 这种静态地确定内容数据的保护程度高于非内容数据的思路也出现在欧洲刑警组织的调研报告中。[13]

国内有研究认为,在初查过程中应对通信内容数据和非内容数据予以区分,内容数据不可调取,而用户数据和流量数据允许调取。[14] 亦有研究认为,电子通信的内容数据涉及公民个人隐私的程度非常高,而非内容数据涉及公民个人隐私的程度较低,二者应当适用不同的获取条件。[15] 还有研究认为,内容数据,不管是通信结束之后已经存储好的,还是通信过程中实时监听的,侵犯隐私权的程度都高于用户数据和流量数据这些非内容数据。[16] 这相当于是一种通信数据的简单、静态分类结构决定了通信数据的分级保护的思路,非内容数据无疑处于比内容数据更低的保护层级。

(二)通信数据二元类型结构理论假设条件存在的疑问

内容数据和非内容数据的二元划分基于一个隐私期待的理论假设。非内容数据中的

---

〔10〕《公约》的解释性报告认为,内容数据指的是特定各方之间直接输入或录入通讯终端的沟通内容,即通讯的意义或主旨,或通讯所传达的讯息或信息(流量数据除外),以用户可识别的自然语言(与机器语言相对)为外部表征。See Council of Europe, Explanatory Report of the Budapest Convention (Budapest, 23. XI. 2001), para. 209.

〔11〕See Council of Europe, Explanatory Report of the Budapest Convention (Budapest, 23. XI. 2001), p. 211.

〔12〕See T-CY (2016), Criminal Justice Access to Electronic Evidence in the Cloud - Informal Summary of Issues and Options under Consideration by the Cloud Evidence Group.

〔13〕See Europol, Sirius: European Union Digital Evidence Situation Report 2019 (20 December 2019).

〔14〕参见梁坤:《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》,《中国刑事法杂志》2020 年第 1 期,第 52-53 页。

〔15〕参见陈永生:《论电子通讯数据搜查、扣押的制度建构》,《环球法律评论》2019 年第 1 期,第 11 页。

〔16〕参见裴炜:《犯罪侦查中网络服务提供商的信息披露义务——以比例原则为指导》,《比较法研究》2016 年第 4 期,第 95-98 页。

用户数据是用户主动提供的,流量数据是通信过程结束后留存在第三方处的,处于半公开状态;而内容数据则直接触及通信秘密的内容,但却往往保存在用户自己的终端上。[17] 第三人规则主要考虑两个要素,首先是用户将相关信息提供甚至公开给了第三方,其保密性在客观上已被降低,其次是此种提供、公开是用户自愿做出的,其主观上的保密意愿也被降低。美国在 1877 年的判例中确认,密封的邮件中是行为人不想透露给第三方的内容信息,而报纸、杂志等印刷品是本就对外公开的非内容信息;[18] 1952 年认定个人交谈中行为人主动告知的内容可被交谈方(线人、举报人)公开或用于作证;[19] 1976 年和 1979 年认可拨打的电话号码和银行交易的记录都是行为人在常规商业沟通中提供的对话记录,政府可直接获取。[20] 延伸到电信与网络时代,可以得出一个推论,即内容数据不是行为人主动告知服务商的,而流量数据和用户数据是行为人为实现交易与通信服务而提供给服务商的信息,所以内容数据和非内容数据的隐私期待与法律保护是不同的。然而,这种理论假设越来越难以应用于当前的信息技术环境下的个人通信数据。[21]

1. 信息保存的地点发生变化

传统的内容信息和非内容信息的二元划分,是基于单个财产性物理空间内外有别、泾渭分明的技术水平与商业实践。典型如信件,信封里面的内容客观上没有向第三方服务商公开,而信封外部的信息向第三方公开了。但是,这种传统物理场域规则设计中的简单二元划分在电子通信场域越来越难成立。第一,新的信息技术导致内容数据也会像非内容数据那样提供给第三方。内容数据不仅一般性地存储在用户自己的设备上,而且越来越多地存储在通信服务商和其他服务商提供的云存储空间上。籍此,通信记录,包括最敏感的数据,不再局限于受保护的空间和个人秘密,而是分布在存储、处理和传输信息均自动化计算的第三方云网络中,用户不知道,甚至也不需要知道向他们提供的可利用计算资源中单个资源的数量、身份、位置或功能。第二,传统邮件通过物理性的信封实现了内外有别,而电子邮件的地址和内容显示在同一页面,服务商必然会把内容数据和非内容数据一并存储。许多主要的电子邮件服务提供商依赖于云服务进行设计,并为消费者提供无缝衔接的刻意模糊本地和远程资源的体验。第三,电子通信中的内容数据和非内容数据的类型区分并不能借助传统物理场域中的内外有别经验而泾渭分明。网络通信内容数据中可能同时含有 URLs 链接这种纯数据构成的流量数据,它有时是元数据,有时是内容,最常见的是部分元数据加部分内容,它可以揭示关于某人的大量信息。

2. 隐私保护的主观意愿性发生变化

对于通信记录数据保护的主观意愿发生变化,用户并非实质性地自愿暴露、真正共享其通信数据给第三方。第一,虽然传统的物理性通信对于用户来说比较重要,但其重要性

〔17〕 参见裴炜:《犯罪侦查中网络服务提供商的信息披露义务——以比例原则为指导》,《比较法研究》2016 年第 4 期,第 98 页。

〔18〕 See Ex parte Jackson, 96 U. S. 727, 733 (1877).

〔19〕 See On Lee v. United States, 343 U. S. 747 (1952).

〔20〕 See Smith v. Maryland, 442 U. S. 735 (1976); United States v. Miller, 425 U. S. 435 (1979).

〔21〕 参见朱嘉珺:《数字时代刑事侦查与隐私权保护的界限——以美国卡平特案大讨论为切入口》,《环球法律评论》2020 年第 3 期,第 49 页。

不如现代信息环节中的电子通信对于个人生存和发展的重要性。在电信和网络时代,用户数据看似是用户主动提供,实际上是通信完成的必要条件,是不得已的牺牲和交换,但其使用目的仅限于通信场景,而非被调取和用于其他社会场景。第二,传统的物理性通信经由信封的技术设计而天然地内外有别,即使法律要求用户提供内部的内容,在技术上,其业务操作也会因为成本高而难以长久地大规模推行。如今这在技术上是相对以往简便可行的。但是,流量数据中的大部分数据,和用户数据中的一部分数据如位置数据,是法律强行要求留存以便备查,它们原本并非用户谋求通信利益而必然放弃的利益。第三,新技术也带来了新的业务模式,使得提供信息变得必要,如通信计费等。但这并不代表用户同意公权力机关将向第三方服务商公开的数据用于其他情形。即使用户明知服务商会记录通信位置数据等细节,商业记录中也蕴含着委托与信任关系,其意义不可忽视。[22] 如果信息可以归类为信息主体与第三方之间的对话,则第三方属于参与者,享有信息披露的权利;如果该信息不是主体希望向第三方传输的内容,第三方仅是承载该信息的中转站,不属于因此发生关系的一部分,无助于收件人和发送者之间建立的亲密关系的真实性,第三方就不享有对该信息的任何处置权,包括披露权。[23] 用户对数据的控制能力被通信技术和业务的架构削弱了,这并非自愿的风险承担。

3. 原有第三人规则下的信息传播规则不再成立

第三人规则客观上推定向第三人提供、公开的信息的保密性降低,是因为在传统通信场景下可以假定提供给第三方的信息一般不会和其他信息产生联系继而被挖掘出新的信息,即使会产生联系,这种频率也是较低的;在主观上推定用户的保密性意愿降低,也是因为用户和第三方乃至整个社会都默认了这种技术水平局限下(信息)的相对安全。但是,在电信和网络通信时代,通信记录所蕴含的信息量和信息敏感度都发生了关键变化。主要包括:第一,元数据留存几乎不受限制,普遍深入地创建了详细的历史记录和全面的档案,此时无需深入了解通信内容,从元数据中就可以推断和揭示几乎无限数量的信息。第二,复杂性数据汇聚起来足以揭示敏感性信息。美国联邦最高法院在2012 年的判决中确认,28 天的持续性个人位置定位信息叠加的整体信息量足以勾画出具体个人的生活模式和生活细节。[24] 在 2018 年的判决中确认,手机基站定位信息记录了个人移动轨迹,包括敏感信息在内,五年的数据保留期“给予了警察接触此前未知信息的机会”。[25]

由上可见,基于第三人规则的通信数据二元区分并不能为通信数据的调取法治提供有力的指导。这背后的原因在于混淆了数据分类、分级的功能与关系。研究表明,数据分类保护具有内容归类和要件类型化的作用,但无实体规则构建的关键指引作用。而独立

〔22〕 See Carpenter v. United States, 138 S. Ct. 2206; 585 U. S. (2018), Gorsuch J., dissenting, at 14.

〔23〕 See Richard M. Thompson II, The Fourth Amendment Third-Party Doctrine 13, Congressional Research Service Report No. 7-5700, 2014; Monu Bedi, Social Networks, Government Surveillance, and the Fourth Amendment Mosaic Theory, 94 *Boston University Law Review* 1809, 1873-1874 (2014).

〔24〕 See United States v. Jones, 132 S. Ct. 945 (2012); Riley v. California, 134 S. Ct. 2473 (2014) at 2491.

〔25〕 See Carpenter v. United States, 138 S. Ct. 2206; 585 U. S. (2018) at 12-13.

于数据分类保护的分级划分标准,能够在分类保护基础上实现数据实体规则构建的最终目的。分类决定分级保护的思路将分级保护概念置于形式化地位,并不可取。刑事法应当塑造分类保护和分级保护的独立关系理论,明确数据分类保护的特定内容属性和分级保护的危害后果属性的划分标准。[26] 通信数据各个类别的特定内容属性已经在上述部分明确,在此基础上,通信数据分级保护的危害后果属性将在下一部分进一步明确。

三 复杂动态多元的通信数据结构

通信数据的获取和相关权利的被干扰、被危害的程度,很大程度上决定了法律保留和合比例性考量的过程和结论。

(一)通信数据的分级标准

对通信服务商而言,其受到的数据相关权利对经营自由的干扰,与调取数据的种类和数量关系不大,因为法律已经在先规定了数据种类和数量的留存期限,调取的种类和数量再多,服务商也早有准备,可高效、准确地确定相关数据的类型和体量,通过技术进行筛选和反馈意味着增加的成本是边际递减的。[27]

但是,对法律关系当事人而言,通信数据具体分类基础上的分级与其权利受干扰程度密切相关,以隐私权或敏感个人信息是否受干扰为基本标准。首先,《民法典》第 1032 条保护自然人不愿为他人知晓的私密空间、私密活动、私密信息,规定任何组织或者个人不得以刺探、侵扰、泄露、公开等方式侵害他人的隐私权。《宪法》特别保护的通信秘密首先指向了公民不愿为他人知晓的私密信息的重要内容。内容数据涉及宪法明文保护的通信隐私,这和人格尊严和基本自由密切相关,所有组织和个人负有尽力尊重的义务。其次,《民法典》《个人信息保护法》《信息技术安全 个人信息安全技术规范》等法律法规保护自然人的个人信息,《宪法》特别保护的通信秘密也指向了公民的个人信息,其获知和使用应当限定在特定的通信场景。最后,个人信息分为普通个人信息和敏感个人信息。《个人信息保护法》第 28 条规定,敏感个人信息是一旦泄露或者非法使用,容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息,包括特定身份、行踪轨迹等信息。连续性的流量数据可能在具体案件中揭示行踪轨迹信息,用户信息也可能揭示特定身份信息。这也是 2017 年最高人民法院、最高人民检察院《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》第 5 条将流量数据、用户信息等通信记录的敏感性界定为通信内容之下而在其他个人信息之上的原因,该条认为它们“可能影响人身、财产安全”。

所以,通信数据的分级标准可以设定为:不揭示通信人隐私内容或仅揭示一般个人信息内容的一般通信数据(对这些通信数据的获取是对其权利的一般干扰);能够揭示通信

〔26〕 参见熊波:《数据分类分级的刑法保护》,《政法论坛》2023 年第 3 期,第 155 页;郑曦:《刑事司法数据分类分级问题研究》,《国家检察官学院学报》2021 年第 6 期,第 5-6 页。

〔27〕 如果没有较为明确的数据类型、范围、期限的限定,而要求进行搜索式的动作,则为搜查行为,其法治要求另当别论。参见孙长永主编:《中国刑事诉讼法制四十年:回顾、反思与展望》,中国政法大学出版社 2021 年版,第 538 页。

人的隐私权内容或者个人敏感信息的重要通信数据(对这些通信数据的获取是对其权利的严重干扰);在极少数特殊情形下关系极度重要个人利益、重大公共利益乃至国家安全的核心通信数据(对这些通信数据的获取是对相关权利、利益的极度干扰)。第三层级中对极度重要个人利益的干扰是指通过揭示隐私信息或敏感个人信息,从而对个人隐私权、个人信息的显著加重干扰。这里揭示与否的判断存在着单一论(homogeneousness theory)和镶嵌论(mosaic theory)的区别,下面将用单一论和镶嵌论两种视角分别分析具体的通信数据类别涉及的数据级别,最后总结出可用的通信数据分级框架。

(二)通信秘密干扰程序的判断

1. 单一论下的通信秘密干扰程度判断

单一论是指单一种类的一个或一组通信数据能够直接揭示通信人通信秘密的内容,也即其特殊隐私权的内容;或者其敏感个人信息,也即其特别受保护的个人信息权利。内容数据在此是典型的明证。

此外,对一组流量或位置数据的存取,确实容易就被保留数据者的私人生活得出精准的结论,例如日常生活习惯、永久或临时居住地点、日常或其他活动、正在进行的活动,这些人的社会关系和他们经常出现的社会环境。[28] 这一结论的补强理由是,流量和地点数据可能揭示有关人员私人生活许多方面的信息,包括敏感个人信息,如性取向、政治观点、宗教、哲学、社会、其他信仰和健康状况,而这些数据还受到欧盟法律的特殊保护。[29] 欧盟法院认为,从一组流量或位置数据提供的有关其使用者通讯或其使用的终端设备位置的数据中容易得出有关个人或其私人生活的准确结论。有学者认为,收集位置信息的行为本身就是侵入性的,访问和使用位置信息并不一定比收集通信内容的侵入性更小,位置信息是开启与有权机构的功能和目的相关的询问、调查和执法活动的钥匙。[30]

2. 镶嵌论下的通信秘密干扰程度判断

镶嵌论是指获取的所有通信数据整合、镶嵌在一起,能够合理地推断出其特殊隐私权内容或者个人敏感信息。该理论描述了计算机网络和人工智能时代情报收集的一个基本原则,即也许零散的信息单独存在对其拥有者来说用处有限或没有用处,但当其与其他信息结合起来时,就会产生额外的意义,因为将这些条目组合在一起,可以阐明它们之间的相互关系,并产生分析上的协同效应,从而产生价值超过其各部分之和的信息组合体。[31] 有学者指出,电信和网络服务提供商会保留用户、位置和流量数据,其目标是将持有的用户有关数据镶嵌到一个单一的数据库中,这样就可以利用人工智能实施高级分析,并

---

〔28〕 See Judgment of 2 March 2021, H. K., C-746/18, EU:C:2021:152, para. 36.

〔29〕 See Judgment of 6 October 2020, La Quadrature du Net and Others, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, para. 117.

〔30〕 See Stanley Shanapinda, *Advance Metadata Fair: The Retention and Disclosure of 4G, 5G and Social Media Location Information, for Law Enforcement and National Security, and the Impact on Privacy in Australia*, Springer Nature Switzerland AG, 2020, pp. 181-182.

〔31〕 See David E. Pozen, The Mosaic Theory, National Security, and the Freedom of Information Act, 115 *The Yale Law Journal* 628, 630 (2005); United States v Maynard, 615 F3d 544, at 558, 562 and 563 (DC Cir. 2010); United States v Jones, 132 SCt at 964 (Alito, J, concurring); Riley v California, 134 *SCt* 2473 (2014) at 2489.

有能力了解更多关于用户的信息,以研究新产品和服务以及查看现有服务的质量和附加值。〔32〕

电子通信服务提供者必须保留的数据使其能够追踪和识别通信的来源及目的地,识别通信的日期、时间点、持续时间和类型,识别用户通信设备,并确定移动通信设备的位置。当用户数据和流量数据被大数据算法软件处理并与其他数据合并时,可以显示个人的敏感信息,即使是匿名数据也会揭示出个人的身份、习惯、特征、活动和隐藏的秘密。〔33〕通过这些数据,可以确定用户或注册用户与谁进行了通信以及通过何种方式进行了通信,也可以确定通信的时间以及通信发生的地点。此外,还可以知道订阅者或注册用户在给定时期内与某些人的通信频率。〔34〕这些数据作为一个整体,很容易从中得到有关个体的私人生活信息。〔35〕特别是,这些数据收集者提供了建立个人档案的途径,其敏感性不亚于通讯的实际内容。〔36〕

(三)通信数据具体分类基础上的类型化分级判断

至此,可以对三类通信数据类型化地做出一般性的判断。进行事先的类型化抽象判断是因为最终可获得数据的数量以及由这些数据得出的有关人士私人生活的具体数据,只有在查阅数据后才能加以评估。然而,在查阅由此产生的数据和信息之前,必须先获得具有管辖权的法院或其他主管机构的查阅授权。因此,对权利干扰严重性的评估,并不在于所获数据在实际情况中是否敏感,而是要对数据对应的类别有关的通常风险进行评估。〔37〕当然,这种评估往往是微妙的,倾向于光谱性描述,而非确定性地分明界限,这样有助于在比例原则框架下追求具体衡量后的动态平衡。它提供的是相对可预测的、可操作的经验规则。

第一,用户信息一般只揭示特定人的身份等非隐私权内容和非个人敏感信息,而且一般单一的信息就能够直接揭示。这些数据本身并不能提供除电子通信方式使用者的联络人数据(例如他们的地址)以外的,任何有关通信及使用者私人生活的数据。〔38〕但是用户信息不限于与使用通信服务直接相关的信息,还指除流量数据和内容数据之外的其他任何信息,可通过这些信息确定用户的身份、邮政或地理地址、电话号码和其他接入号码,

〔32〕 See Stanley Shanapinda, *Advance Metadata Fair: The Retention and Disclosure of 4G, 5G and Social Media Location Information, for Law Enforcement and National Security, and the Impact on Privacy in Australia*, Springer Nature Switzerland AG, 2020, p. 211.

〔33〕 See Stanley Shanapinda, *Advance Metadata Fair: The Retention and Disclosure of 4G, 5G and Social Media Location Information, for Law Enforcement and National Security, and the Impact on Privacy in Australia*, Springer Nature Switzerland AG, 2020, p. 212.

〔34〕 See Judgment of 8 April 2014, Digital Rights Ireland and Seitlinger and Others, C-293/12 and C-594/12, EU:C:2014:238, para. 26; Judgment of 21 December 2016, Tele 2, C-203/15 and C-698/15, EU:C:2016:970, para. 98.

〔35〕 See Judgment of 8 April 2014, Digital Rights Ireland and Seitlinger and Others, C-293/12 and C-594/12, EU:C:2014:238, para. 27.

〔36〕 See Judgment of 21 December 2016, Tele 2 Sverige, C-203/15 and C-698/15, EU:C:2016:970, para. 99.

〔37〕 See Judgment of 2 March 2021, H. K., C-746/18, EU:C:2021:152, paras. 39-40. 我国刑事诉讼法对搜查、技术侦查等强制性侦查,主要并不是基于司法审查而取得授权或令状,而是基于侦查机关内部的行政化审批而取得授权。这种内部的审批机构是“其他主管机构”之一种。

〔38〕 See Judgment of 2 March 2021, H. K., C-746/18, EU:C:2021:152, para. 34.

以及计费和支付信息,其他有关通信设备安装地点或位置的信息。用户信息中的位置数据可能直接揭示隐私权内容或个人敏感信息,这种揭示可能通过单一信息,也可能通过镶嵌的大量位置数据。相比于其他基本的用户数据,(动态)IP 地址对公民基本权利的干预程度更强。[39]

第二,流量数据通过单一信息一般不能直接揭示隐私权内容或个人敏感信息,但是通过镶嵌信息一般可以揭示。即便不查看邮件的具体内容,很多情况下内容信息也可以通过调查接收方、发件方近期网络活动、双方通信时间等加以了解。[40]

第三,内容数据一般可以通过单一信息直接揭示隐私权内容或个人敏感信息,应当受到最为严格的保护。通信内容直接将个人最私密的思想自由外化于社会交往关系中,是隐私信息的核心部分。刑事实体法对通信内容和位置数据(行踪轨迹信息)采取最严格的保护(50 条以上的即可入罪),对其他可能影响人身、财产安全的通信记录,适用较为严格的保护(500 条以上的即可入罪)。[41] 可见,根据能否揭示内容信息以及揭示内容信息的敏感程度采取不同程度的法律保护,已经为刑事实体法所接受和实践。但是,就什么在实质上构成内容数据而言,仍存在争议。镶嵌论强调了信息碎片的累加价值,这意味着难以用内容数据作为单一标准判断权利侵犯程度的高低。

综上所述,通信数据调取的法治框架应当从通信数据的静态二元分类结构过渡到以结合数据类型细节性、数据内容敏感性、数据时间长短性、数据范围广阔性为标准的动态多元向度结构,以层次化地划分权利干预的程度。通信数据的分级可以在通信数据具体分类的基础上,被总结为透明的、一致的三阶层框架:第一层级是一般的通信数据,是指位置数据之外的更有针对性(更少侵入性)的单一类型的、短期的用户数据;第二层级是重要的通信数据,是指位置数据之外的全面类型的、长期的用户数据,或者单一且短期的位置数据或流量数据;第三层级是核心的通信数据,是指全面的或长期的位置数据或流量数据,或者内容数据。在此,长期与短期的区别是一个没有固定标准的问题,需要各个法域根据自身的法律实践和保护理念不断探索和调试。例如美国学者认为,“长期”可以界定为一个确定的时间,即七个累计的日子,这样利大于弊。[42]

四 通信数据调取的合比例性框架

对于通信数据调取的合比例性原则及其适用的问题,已经有许多的讨论。此处简要

---

〔39〕 See Benedik v. Slovenia, App. no. 62357/14 (ECtHR 24 April 2018); EuroISPA's Comments on the Provisional Text of the 2nd Additional Protocol to the Budapest Convention on Cybercrime, https://rm. coe. int/euroispa-2929-comments-to-5th-round-draft-provisions-2nd-add-protocol/1680a16180,最近访问时间[2023-04-25]。

〔40〕 参见裴炜:《犯罪侦查中网络服务提供商的信息披露义务——以比例原则为指导》,《比较法研究》2016 年第 4 期,第 98 页。

〔41〕 参见 2017 年最高人民法院、最高人民检察院《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》第 5 条。

〔42〕 See Gabriel R. Schlabach, Privacy in the Cloud: The Mosaic Theory and the Stored Communications Act, 67 *Stanford Law Review* 677, 706-709 (2015). 美国联邦最高法院认为,访问七天的手机定位数据就构成了宪法第四修正案的搜查。See Carpenter v. United States, 138 S. Ct. 2206; 585 U. S. (2018) at 11.

重述组成这一原则性框架的系列要素,然后重点对通信数据调取场景下的狭义均衡要素进行充分阐述。

(一)通信数据调取的合比例性框架要素

第一是目的正当。那些能够为损害电子通信保密原则的国家立法提供理由的目标清单(保护公共安全、国防、国家安全和刑法的执行)是详尽无遗的,对保留数据的访问必须真正和严格地符合其中任何一个目标。〔43〕 并非所有通信数据的执法获取都是平等的,比如情报机构在保护国家安全方面负有独特的责任,相应地享有更高的权限。何为国家安全,可以由国家安全机关根据《国家安全法》等法律来认定,但何为追查刑事犯罪,则存在复杂的界定问题。《警察法》概况性地授权预防、制止和侦查违法犯罪活动,如果事发后,难以确定是构成违法还是犯罪,例如盗窃和殴打行为,就必须等确定达到入罪门槛之后,方可检查通信内容。刑事犯罪的追查可以扩张解释为除了侦查已经结束的犯罪外,还包括制止正在发生的犯罪,因为这也是为侦查正在发生的犯罪所必需的。但如继续解释为还包括事先的预防则需慎重,必须是犯罪行为已经开始发生,或者根据其他证据证明犯罪已经开始预备,〔44〕而不可仅仅根据过往经验或大数据推断某个人(群)具有犯罪倾向,为了预防其犯罪开始就检查其通信内容。〔45〕 这种犯罪预防和情报资料信息收集领域内调取行为的合宪性问题也与手段合适、手段必要以及狭义均衡相关。

第二是手段适合,即采取的手段必须对于达成目的有促进作用,具有相关性。警察实践由犯罪侦查中的嫌疑标准开始向一般性社会治理中的风险标准转化,这意味着难以事先合理地划定取证的范围,因为警方难以确定、容易混淆数据载体的相关性和具体数据的相关性。〔46〕 所以,对某个人(群)预备行为的预防不应当被认定为《宪法》上的追查刑事犯罪需要而证成通信秘密检查。

第三是手段必要,必须是没有其他伤害性更小、成本更低的手段能够达成目的。例如,为了预防他人实行犯罪,完全可以调取非内容数据和采取其他手段。如果能向通信主体直接调取通信数据,比如已获得通信主体同意,此时就不存在对信息主体权利的强制,反而有利于通信主体知情、监督和获得救济;有权机关不应直接向电信、网络通信服务商调取,因为会造成运营成本的增加。然而,对于这种最后手段性的强调,在整体上,不管是在程序法上对侵害手段的司法审查,还是刑事实体法上对犯罪化的审查,英美法系和欧洲大陆的权威司法机关,都罕有详细叙说。原因可能是里面涉及大量复杂的法社会学乃至

〔43〕 See Judgment of 21 December 2016, Tele 2, C-203/15 and C-698/15, EU:C:2016:970, para. 115.

〔44〕 如果是公开的现场提取或网络远程勘验措施,属于搜查措施,需要向数据持有人或服务者公开宣示;秘密勘验则属于技术侦查措施,但二者都属于刑事立案以后的侦查措施。参见孙长永主编:《中国刑事诉讼法制四十年:回顾、反思与展望》,中国政法大学出版社 2021 年版,第 550-551 页。

〔45〕 使用储存和分析的数据库来创建个人档案,以及将该数据库用于推测性数据匹配,可能适用于当一个人没有涉及一个罪行,但该人却仍与国家安全有关时的情况。

〔46〕 参见裴炜:《数据侦查的程序法规制——基于侦查行为相关性的考察》,《法律科学》2019 年第 6 期,第 46-48 页。关于通信信息取证中的相关性问题,参见贾志强:《微信通信信息取证问题实证探究——以相关裁判文书为样本》,《出版发行研究》2018 年第 2 期,第 84 页;陈厚楠:《通信记录证据审查要点及运用方法》,《检察日报》2018 年 11 月 25 日第 3 版。

法经济学的知识运用与考量过程。[47] 我国学者认为,基于消极目的的规制对于维持国民的生命与健康而言乃是不可或缺的,理应容许施加强力的规制,若将此种规制限定于必要的最小限度之内,其妥当性不无疑问。无论是从宪法文本自身的规范结构来看,还是就社会发展的现状而言,传统意义上的自由法治理念似乎都不宜成为指引合宪性判断的唯一方针。[48]

第四是狭义均衡,即手段的侵害和成本必须小于所达成的目的收益。如果是制止已经开始的犯罪,其损害减免和犯罪侦破都是必然存在的收益;而在事先预防他人犯罪的情形中,他人是否真的会着手犯罪是不确定的,其损害减免和犯罪侦破都并非必然存在的收益,狭义均衡的判断也就存疑。狭义均衡是英美法系和欧洲大陆法系国家的权威司法机关在司法审查中反复强调的流程和标准。这为理论上如何构建一套审查标准提供了有益经验。

(二)通信数据多元结构下的狭义均衡

司法审查的模式主要是认定对侵害性手段的一般性授权不符合狭义比例原则,但却没有充分说明何种具体授权符合狭义比例原则,这是由司法审查的本质所决定的。然而,理论研究必须追求从消极审查转向积极构建,才能全面地反哺实践。下面将在通信数据多元结构下,根据权利干预程度进行通信数据调取行为的分类,探究符合狭义比例原则的具体授权方式。

1. 严重干涉对应严重犯罪/严重威胁

通信数据的保留和调取无论是一般性的、无差别的针对所有人员和犯罪类型,还是有针对性的,都可能对有关基本权利造成严重干涉。[49] 一种是例如流量和位置数据的保留和调取所引起的严重干扰,可提供有关电子通信手段使用者通信的数据,或有关所使用终端设备的位置,并能就有关人士的私人生活作出准确结论的数据。另一种是这些电子通信服务提供者提供的数据作为一个整体,允许对数据涉及者的私人生活得出精确的结论。欧盟法院认为,只有以打击严重犯罪或防止对公共安全的严重威胁为目标,才有资格通过国家立法查阅电子通信服务提供者所保留的通信数据。[50] 例如,为打击恐怖主义犯罪和严重跨国犯罪这一符合欧洲联盟普遍利益的目标,即使是严重干涉《欧盟基本权利宪章》(*Charter of Fundamental Rights of European Union*)第7条(尊重私人与家庭生活)和第8条(保护个人数据)所载的基本权利也是有理由的。此外,对公共安全的保护也有助于保护他人的权利和自由。例如仅为防止恐怖主义的目的,授权实时收集先前被确定与恐怖主义威胁有关联的人的有关信息;又如在授权所规定的参数范围内,在其网络上应用自动数

〔47〕 参见戴昕、张永健:《比例原则还是成本收益分析——法学方法的批判性重构》,《中外法学》2018年第6期,第1519页。

〔48〕 参见陈鹏:《公法上警察概念的变迁》,《法学研究》2017年第2期,第39页。

〔49〕 See Judgment of 2 March 2021, H. K., C-746/18, EU:C:2021:152, para. 33.

〔50〕 See Judgment of 21 December 2016, Tele 2 Sverige, C-203/15 and C-698/15, EU:C:2016:970, para. 115; Judgment of 2 October 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, para. 56; Home Office, Investigatory Powers Act 2016: Consultation on the Government's Proposed Response to the Ruling of the Court of Justice of the European Union on 21 December 2016 Regarding the Retention of Communications Data (November 2017).

据处理方法,以检测可能构成恐怖主义威胁的链路,这种方法并不涉及一般性地和不加区分地数据保留问题,其目的是在一个有限的时期内收集可能与恐怖主义性质罪行有关的所有通信数据。防止、调查、发现和起诉一般刑事罪行的目标不能够证明某一组流量或位置数据的调取是正当的。[51] 因为期间再短,该组数据也可能对有关基本权利造成严重干涉。

相比之下,这种接触如果对基本权利造成的干扰不严重,就能够以防止、调查、发现和起诉一般刑事罪行的目标为理由。[52] 在刑事调查过程中,主要在两种特定情况下需要用户数据。第一,需要用户数据确定哪些服务和相关技术措施已经或正在被用户使用,如电话服务类型(例如移动的),其他相关的服务类型(例如电话转接、语音信箱等)、电话号码或其他技术地址(例如电子邮件地址)。第二,当技术地址已知时,就需要用户通信数据,以协助确定有关人员的身份。其他用户数据,例如关于用户的账单和付款记录的商业信息也可能与刑事调查有关,特别是在调查的犯罪涉及计算机欺诈或其他经济犯罪的情况下。[53]

当内容数据、流量数据和位置数据能够单一地或者整体地揭示通信内容或通信人的私人生活、敏感信息时,查阅、复制等调取行为构成对基本权利的严重干涉,只有严重犯罪才能与之相匹配。而调取位置数据之外的用户信息,则难以从数据类型上直接认定有此种严重干扰,只能在个案中认定;而在立法上,调查一般犯罪等行为背后的一般利益,也能证成这种对基本权利的一般干扰。对此,欧盟法院认为,国家主管部门应当确保在每个案例中,所涵盖的资料类别及要求查阅该等资料的期间,是根据案件的情况,仅限于对有关一般犯罪调查的目的所严格必要的。[54] 可见,当追求只是作为一般利益的目标时,必须适当平衡一般利益的目标和所涉权利,使之与措施所影响的基本权利相协调。[55]

我国法律体系已经有将重大调查措施的适用情形限定为“严重犯罪”的动向。《数据安全法》第 35 条要求调取数据需经过严格的批准手续,这与《刑事诉讼法》第 150 条规定的技术侦查措施在表述是类似的,即要求适用于重大刑事案件、报地级市以上公安机关负责人批准,属于超强制性侦查措施。[56] “严格的批准程序”是在 1993 年《国家安全法》第 10 条和 1995 年《人民警察法》第 16 条中规定的对技术侦察的一贯要求。《刑事诉讼法》第 150 条的技术侦查适用罪行范围的相关表述强调的是“严重危害社会”“严重侵害公民人身权利”,这和前述欧盟法院强调的严重犯罪、公共安全的严重威胁具有相当性。[57]

---

〔51〕 See Judgment of 2 March 2021, H. K., C-746/18, EU:C:2021:152, para. 35.

〔52〕 See Judgment of 2 October 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, para. 57.

〔53〕 See Council of Europe, Explanatory Report of the Budapest Convention (Budapest, 23. XI. 2001), para. 178.

〔54〕 See Judgment of 2 March 2021, H. K., C-746/18, EU:C:2021:152, paras. 37-38.

〔55〕 See Judgment of 6 October 2020, La Quadrature du Net and Others, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, para. 130.

〔56〕 参见谢登科:《论侦查机关电子数据调取权及其程序——以〈数据安全法(草案)〉第 32 条为视角》,《环球法律评论》2021 年第 1 期,第 56-57 页。

〔57〕 2020 年修正的《公安机关办理刑事案件程序规定》第 263 条更是明文要求技术侦查适用的对象应当是“严重危害社会的犯罪案件”,并列举了四种重大犯罪案件和依法可能判处七年以上有期徒刑的“其它严重危害社会的犯罪案件”。

2. 严重犯罪/严重威胁的认定

如何认定严重犯罪是各个法域普遍面临的理论与实践难题。欧盟关于留存电子通信数据的《2006/24 号指令》在第 1(1)条中只是一般地提及严重罪行,具体内涵由每个会员国在其国内法中定义。[58] 所以,每一个法域都必须专门定义其所看重的严重犯罪。

在刑法哲学上,可能的危害性越严重,国家就越有理由采取强制性措施。[59] 而这种可能的危害性大小的判断首先依赖于形式上的法定刑判断。参考《刑法》第 7 条(属人管辖权)、第 72 条(缓刑适用条件),可以将法定最低刑为三年以上有期徒刑的犯罪称之为重罪。[60] 这个重罪与非重罪的界限,符合刑事实体法与程序法贯通和衔接的一般理论,[61]也与我国刑事诉讼中逮捕这一强制措施的适用条件一致。但现有法定刑的设置存在形式上不能完全反映多人多次侵害的情形,实质上存在规定不平衡等问题。所以,如果一味依赖现有的不合理法定刑设置确定可能的危害性大小,大前提错误就将导致结论错误。

可能的危害性大小的判断应当转向实质标准,即生活质量。刑罚严厉性取决于(可归责于行为人的事实范围内的)法益受到损害的程度。[62] 法益是服务于人的生存和生活的利益,所以危害性大的实质标准应当是生活质量标准。刑事危害的生活质量标准在英国、德国被提倡用于均衡量刑,实现对行为严重性的阶层性判断。[63] 该理论以一般人的生活质量为基准使刑事危害的评估标准化,[64]也可以用于刑事实体法上犯罪化的论证,[65]以及刑事程序上具有强制性质、权利干扰性质的措施的论证。所以应构建适用生活质量标准的规则,确定可能的危害性是否大到不可接受。一是面向性质重大的单一法益侵害时,必须是威胁生命,身体重大完整、重大健康(参考《刑法》第 95 条的重伤标准),重大财产(参考侵犯财产罪中的"数额巨大"标准),走私等涉及重大经济秩序,毒品等涉及重大社会管理秩序的情形。二是面向单一性质的、多人次的法益侵害时,必须是人次数量和侵害层次的复合评价呈现严重性的情形,比如三人次以上并且法定刑在有期徒刑以上。如果单人次的行为就符合犯罪构成,鉴于我国刑事犯罪和行政违法的二元界分立法

〔58〕 See Judgment of 8 April 2014, Digital Rights Ireland and Seitlinger and Others, C-293/12 and C-594/12, EU:C:2014:238, para. 60.

〔59〕 See Joel Feinberg, *The Moral Limits of the Criminal Law*, *vol. 1*: *Harm to Others*, Oxford University Press, 1984, p. 216.

〔60〕 参见张明楷著:《刑法学》(第六版),法律出版社 2021 年版,第 120 页。

〔61〕 See David Keenan & Tina M. Thomas, An Offense-Severity Modal for Stop-and-Frisks, 123 *Yale Law Journal* 1118, 1448 (2014).

〔62〕 参见李山河:《裁量活动与量刑规范:论确定刑罚的基础》,《政法论坛》2015 年第 6 期,第 75 页。

〔63〕 See Andrew von Hirsch, Andrew Ashworth & Nils Jareborg, Gauging Crime Seriousness: A "Living Standard" Conception of Criminal Harm, in Andrew von Hirsch & Andrew Ashworth, *Proportionate Sentencing*: *Exploring the Principles*, Oxford University Press, 2005, pp. 186-219. 另见赵书鸿:《论犯罪行为严重性的阶层性判断——中德刑法规范的比较性分析》,《比较法研究》2015 年第 3 期,第 111-122 页。

〔64〕 See Andrew von Hirsch & Nils Jareborg, Gauging Criminal Harm: A "Living Standard" Analysis, 11 *Oxford Journal of Legal Studies* 1, 4, 5, 21 (1991).

〔65〕 See Nina Peršak, Using "Quality of Life" to Legitimate Criminal Law Intervention: Gauging Gravity, Defining Disorder, in Antje du Bois-Pedain & Ulfrid Neumann eds., *Liberal Criminal Theory*: *Essays for Andreas von Hirsch*, Hart Publishing, 2014, pp. 225-246; Kelley Burton, Criminalisation: Applying A Living-Standard Analysis to Non-consensual Photography and Distribution, 7 *Queensland University Technology Law and Justice Journal* 464, 476 (2007).

格局已经进行了危害性筛选,可以认为十人次的行为,不管刑法上的侵害层次(法定刑)为何,都可认定为严重侵害。刑期的可能性判断标准不需要是合理预期,可以是能被如此判处的可能性。三是面向多种法益侵害类别,此时的法益种类是否够“多”的确定,参照上述“多人次”的认定规则。例如嫌疑人实施三种以上违法犯罪,并且侵害层次最低为有期徒刑以上的法定刑。这种发展的复合标准,能够动态地涵摄集团性的和系列性的重大犯罪案件。在《反有组织犯罪法》颁行的背景下,应对多次实施违法犯罪的恶势力组织团伙成员也采取通信信息调取手段,职业性、常业性的系列性犯罪,也能够认定为重大危害。

在重大危害之外,对公共安全的严重威胁也可证成通信数据调取制度的正当性。损害的可能性越大,作为强制调取手段理由损害的严重性就可以越小。〔66〕在可能的危害性一般,但满足我国刑法上的犯罪构成时,经由风险的其他要素的升级,也可认定风险重大,从而证成通信数据调取之必要。如果调取通信数据后找到犯罪证据、犯罪人的可能性越大,那就意味着不调取会造成公共安全威胁的可能性越大。这种可能性大小主要取决于调取的启动标准是主观上认为有犯罪嫌疑、为了查明犯罪行为的标准,还是存在一定客观事实依据的、表明可以找到犯罪证据和犯罪嫌疑人的标准,抑或是更高层次的具有充足事实基础的合理怀疑标准。〔67〕证明标准的阶层式划分对应了程序的渐进式设定。立案前的初查阶段对应的是很低的证明标准,也即很低的可能性,难以证成对通信记录的调取,一般不可为了获取犯罪线索本身而进行调取,除非是极为严重的危害性。

危险的紧迫性动态地影响可能性要素和严重性要素的适用。危险越紧迫,要求的可能性越低;同样,紧迫性越高,要求的罪行严重性也越低。因罪查人时,如不调取数据,这可疑之人和可疑之信息将立刻消失,且再难发现,此时调取信息的紧急性尤为凸显。例如流量数据可能维持的时间短暂,因此有必要下令快速保存它。因此,为了在通讯被删除之前收集进一步的证据或查明犯罪嫌疑人,可能有必要迅速披露通讯数据。〔68〕因人防罪时,针对或利用电信、计算机网络技术实施诈骗等犯罪的犯罪形态结构意味着,不仅其严重性经由(多)人次标准而得到重视,而且犯罪时所处的信息技术环境也决定了其紧急性的存在,因为如不调取,难以及时阻止犯罪后果的发生。通信数据的跨域性、动态化、碎片化意味着通信数据的脆弱性,此时需要平衡恐怖主义犯罪、有组织犯罪、电信网络犯罪制止和侦办情况的紧急性,以及诸类犯罪与通信工具的高度关联性,因应复杂犯罪类型的信息化、组织化趋向。

综上所述,有原则的实用主义充分考虑了可能的危害性、危害的可能性和危害的紧急性,根据权利的干预程度和干预必要性,构建通信数据调取的阶梯式启动结构,既能约束恣意发动通信数据调取的行为,有利于保障人权,也能指引公权机关选择合适的数据调取

〔66〕 See Joel Feinberg, *The Moral Limits of the Criminal Law*, *vol. 1*: *Harm to Others*, Oxford University Press, 1984, p. 216.

〔67〕 关于证明标准的更多探讨,参见陈瑞华著:《刑事证据法》(第三版),北京大学出版社 2018 年版,第 458-482 页。关于此方面的层次理论,参见艾明:《论刑事侦查中对手机通信记录的调取及法律规制》,《中国刑事法杂志》2011 年第 1 期,第 81 页。

〔68〕 See Council of Europe, Explanatory Report of the Budapest Convention (Budapest, 23. XI. 2001), para. 29.

行为,及时查明事实。2022 年 11 月联合国公布了关于订立反对将信息和通信技术用于犯罪目的的国际公约的综合谈判文件,其第三章第二小节关于用户数据、流量数据、内容数据的保存、调取乃至实时截取的草案,开始考虑罪行的严重性,遗憾的是,仍未考虑侦查和证据保存的紧急性、相关性。〔69〕

行文至此,权利干预必要性可被论述为三阶层。第一层是一般的危害和威胁,是指应当受到刑罚处罚以外的危害和威胁,或受到有期徒刑以下刑罚惩罚的轻微犯罪;第二层是应当受到刑罚处罚的严重的危害和威胁,是指受到有期徒刑以上刑罚惩罚的犯罪,涉及三人次或三种以上违法犯罪行为的犯罪,以及存在一定的客观事实依据或一定程度紧急性的犯罪;第三层是极度的社会危害和威胁,是指受到三年以上有期徒刑惩罚的犯罪,受到有期徒刑以上刑罚惩罚且涉及三人次或三种以上违法犯罪行为的犯罪,涉及十人次或十种以上违法犯罪的犯罪,以及存在充足的客观事实依据或很高程度紧急性的犯罪。

3. 通信数据分类基础上的分级三阶层对应通信权利干预必要性的三阶层

根据本文对通信数据具体分类基础上的分级三阶层,通信秘密权利的干预程度可以被论述为透明的、一致的三阶层框架。第一层是一般的侵害,是指仅调取一般的通信数据;第二层是严重的侵害,是指调取重要的通信数据;第三层是极度的侵害,是指调取核心的通信数据。

由此,权利干预程度的三阶层对应权利干预必要性的三阶层。〔70〕我们能得出诸多有意义的结论。对行政违法行为,主要是治安违法行为、互联网信息内容违法行为的查处以及公职人员职务违法行为的查处,(互联网)法院对民事案件的审理,不能采取对公民隐私权利侵害甚大的通信数据调取手段,只能调取位置信息以外单一种类的、短期的用户信息;只有在国家安全维护、刑事犯罪侦查中,才能考虑通信信息中位置信息、流量信息和内容信息的调取,和用户信息综合的、长期的调取。在刑事犯罪中,只有较为严重的犯罪才能适用通信信息调取,可以根据电子通信数据中内容数据、流量数据与用户数据的多个具体种类涉及公民个人隐私程度的层次不同,而设置多样的适用条件。相比在权利干预程度中只区分内容信息和非内容信息,在权利干预必要性中只区分徒刑和三年以上徒刑的双层简单二元结构,〔71〕条件的多样化能够适应更加动态和复杂的通信数据调取的法律实践体系。

不可忽视的是,在权利干预程度第三层次和权利干预必要性第三层次的对应过程中,还有更为复杂和动态的情形需要具体分析和处理。权利干预的第三层是极度的侵害,是指调取全面的或长期的位置数据或流量数据,或者调取内容数据,在单一论或镶嵌论视角下,这种调取完全可能对私人生活信息的内容进行揭示,此时揭示的信息可能包括个人敏

〔69〕 See General Assembly, Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (A/AC. 291/16).

〔70〕 阶层式上升的整体思路已经在刑事实体法上的六个(立案)追诉标准和约二十个计算机网络犯罪的司法解释所共同体现:情节、后果不严重,情节、后果严重,与情节、后果特别严重的三阶层框架已很常见。参见郭旨龙:《信息时代犯罪定量评价的体系化转变》,《东方法学》2015 年第 6 期,第 114-125 页。

〔71〕 参见陈永生:《论电子通讯数据搜查、扣押的制度建构》,《环球法律评论》2019 年第 1 期,第 11 页。

感信息,此时法律要求的不仅仅是简单的必要性,而是严格的或充分的必要性。如果第三层次的通信数据调取能被合理地认为包括某种敏感个人信息,则必须符合充分的必要性。这可以借鉴域外严格的必要性进行理解。

《英国数据保护法》(*Data Protection Act* 2018)第 35(5)(a)条规定,当数据控制者在未经数据当事人同意的情况下对敏感数据进行处理时,该处理必须为执法目的所严格必要。该声明承认了针对唯一识别一个人的生物特征数据可以处理;这对个人权利构成了更高的风险;因此,处理过程需要更高水平的保护和保障。〔72〕 严格的必要性并非指向或仅仅指向通过建立适当的安全保障政策达至数据的保密和可控安全。"严格必要性"可理解为在处理特殊类别的数据时需要特别注意必要性原则,并预见处理这类数据的准确和特别可靠的理由。〔73〕 当涉及到严格的必要性和相称性时,有效性是一个关键考虑因素。这意味着,在通信数据调取的权利干预必要性第三层次里,受到三年以上有期徒刑惩罚的犯罪或涉及十人次或十种以上违法犯罪的犯罪两种情况都必须具备存在一定程度的客观事实依据或一定程度紧急性的条件,甚至是存在充足的客观事实依据或很高程度紧急性,才能得以补足必要性要求。

五 结论

随着技术的进步,法律必须做出调整。在执法部门的利益驱使下,使用易于获得的超感官大数据算法分析软件,利用机器学习,可以轻松地、系统地获取和分析用户数据和流量数据,以准确、可靠地透露有关个人的重要隐私和敏感个人信息。基于内容与非内容数据的法律保护的传统区分,与现代通信技术运作中用户数据和流量数据生成、交换和存储的方式日益不兼容,与个人对现代通信中的个人隐私和个人信息保护的正当期待愈发背离,是对通信数据形式和类型不合理的区别对待。

我们需要一个统一的标准化法律框架,即根据数据分类多层次框架,以明确特定数据所属具体类型的数据分级,匹配阶层化的调取措施,并通过相应的批准程序和救济程序予以承接。基于尊重和保障人权的国家基本义务,公民享有不被犯罪化的权利,这一实体权利要通过通信数据调取的数字正当程序得到维护。通信秘密数据调取领域真诚、细致入微的努力是一个合理的法治测试,处于网络数据执法和司法调取理论与实践的前沿。它必须反映现代公民对隐私权和个人信息保护的合理期望,帮助重建政府和人民之间的信任,推进一个更加紧密联系的人类社会未来。

[本文为作者参与的 2021 年度国家社会科学基金重大项目"数字经济的刑事安全风险防范体系建构研究"(21&ZD209)的研究成果。]

〔72〕 See Information Commissioner's Opinion, The Use of Live Facial Recognition Technology by Law Enforcement in Public Places (31 October 2019), pp. 11-12.

〔73〕 See The Article 29 Working Party, Opinion on the Law Enforcement Directive (November 2017).

The Proportionality of the Acquisition of Communication Record Data

[**Abstract**] The acquisition of communication record data is an important system for fighting crimes and governing society. Relevant legal regulatory frameworks have been continuously introduced and updated in various jurisdictions. At the current stage, the system of acquisition communication record data should develop from the formal rule of law to the substantive rule of law. The current framework of communication privacy analysis is built on the simple, static and binary communication data structure, but its theoretical assumption of the third-party rule - the user data in the non-content data is actively provided by the user and the traffic data is retained in the third party after the termination of the communication process and is in a semi-public state while the content data, on the other hand, touches directly on the secret content of communications, but is often stored on the user's own terminal - is increasingly difficult to establish in the increasingly complex modern information technology environment. The traditional distinction between legal protections based on content data and those based on non-content data is increasingly incompatible with the generation, exchange and storage of user data and traffic data in the operation of modern communication technology, and increasingly deviates from the legitimate expectation of personal privacy and personal information protection in modern communication, constituting an unreasonable distinction between the forms and types of communication data. In the future, a unified and standardized legal framework needs to be established to match the hierarchical data-acquisition measures for the implementation of the substantive rule of law. The complex dynamic and multivariate classification and hierarchical structure of communication data provide a practical alternative to the traditional privacy analysis, that is, the multi-hierarchy of the degree of rights intervention corresponds to the multi-hierarchy of the necessity of rights intervention. The scheme is flexible enough to adapt to rapidly evolving communication technologies. The classification of communication data can be summarized as a transparent and consistent three-level framework based on the specific classification of communication data. At the first level is general communication data; at the second level is important communication data; and at the third level is core communication data. Principled pragmatism takes into full consideration the gravity of possible harm, the possibility of harm and the urgency of harm. At the first layer are general harm and threat; at the second layer are serious harm and threat that should be punished by criminal law; and at the third level are extreme social harm and threat. Through the three levels of the degree of rights intervention corresponding to the three levels of the necessity of rights intervention, we can draw many meaningful conclusions. The acquisition of communications data must reflect the legitimate expectations of modern citizens of the right to privacy and the protection of personal information, help rebuild trust between the government and the people, and create a more connected future for human society.

(责任编辑:贾　元)