法商研究 Studies in Law and Business
Vol. 39 No. 4(2022)

个人信息保护中的第三方当事人规则之反思

李 延 舜*

摘 要:网络服务提供者在提供便捷的网络服务时,也收集和存储了大量的个人信息,其中不乏能提供刑事案件侦破线索、甚至本身就能作为证据的信息。当公民主动披露个人信息给网络服务提供者时,公民是否对其信息被侦查人员获悉的可能性"自担风险"?第三方当事人规则秉持"是"的立场,规定公民对其主动披露的个人信息不享有合理隐私期待。对第三方当事人规则的"前身"和理论预设分析后发现,该规则在表面上与网络时代相契合,但在实质上却背离了个人信息保护的真正规范。该规则不仅强化了大数据侦查中"控辩双方"的不对等,而且有可能侵入公民私人领域,危及公民人权。破除第三方当事人规则的惯常思维,解决相关情境难题,需要遵循比例原则之指导,构建令状制度,重新审视隐私权理论,以及确立个人权利优先原则。

关键词:第三方当事人规则 合理隐私期待 数据共享 隐私权

一、问题的提出

(一)第三方当事人规则释义

第三方当事人规则是《美国联邦宪法第四修正案》(简称《第四修正案》)衍生理论之一,用于规范刑事侦查中警察向第三方当事人收集证据的过程。① 其内容很简单,即如果公民自愿将信息披露给第三方当事人,那么该公民就不再享有《第四修正案》有关保障其信息隐私方面的权利,亦即公民对于自愿泄露的隐秘信息不再享有合理隐私期待。第三方当事人规则最初用于"卧底"案件,通过打入敌人内部获得线索,如"昂立诉美国案"②、"洛佩兹诉美国案"③、"美国诉霍法

* 河南大学法学院副教授
基金项目:国家社会科学基金一般项目(21BFX094)、河南省哲学社会科学规划项目(2020BFX005)

① See Daniel J. Solove, A Taxonomy of Privacy, 154 University of Pennsylvania Law Review, 528－529 (2006).

② See On Lee v. United States, 343 U. S. 747 (1952).

③ See Lopez v. United States, 373 U. S. 427 (1963).

案”[①]等;第三方当事人规则的第二波浪潮指向各种商业纪录,典型案件如“美国诉怀特案”[②]、“美国诉米勒案”[③]、“史密斯诉马里兰州案”[④]等;在网络时代,第三方当事人规则的第三波浪潮指向无所不包的个人信息。在网络世界中,公民虽然不会自愿将自己的信息披露给别人,但是不得不主动将自己的信息提供给网络服务提供者。自此,不管是注册人信息、交互信息,抑或内容信息,第三方当事人规则都将其排除在合理隐私期待范围之外。

第三方当事人规则之所以广为法院接受,是因为该规则的三大理论预设。(1)较少的隐私合理期待理论。隐私合理期待是美国大法官哈兰在“凯茨诉美国案”[⑤]中提出的一项隐私确权公式:“第一,他人必须表现出实际的(且主观的)隐私期待;第二,社会公众认可他人的隐私期待是‘合理的’。”当公民自愿、主动将某一隐私信息告知他人,第三方当事人规则便将这一“自愿告知”视为自愿放弃保持信息“隐秘性”的举动,是一种排除隐私期待合理性的行为。(2)风险自担原则。信任是个高尚的词汇,但信任也从来都伴随着风险。电信公司明确知道我们的通讯记录、通讯位置及通讯时长,银行能清晰地记录客户账户信息及资金动向,网络服务提供者能够记录用户的登录身份标识号码、访问网址、电子邮件、购物信息及社交动态。即使公民在提供这些信息时曾假定该信息只会被用于特定目的,但事实上,公民提供这些信息所冒的风险并没有丝毫减少。当第三方知晓他人的隐秘信息,警察也就知晓了。(3)“隔离人”预设。所谓“隔离人”,是指“隔离于社会之外的人”。公民的日常生活离不开分享,分享产生亲密感及安全感,但同时,分享行为也带来信息被披露的风险,这就涉及公民作为一个独立个体,如何在别人的陪伴下选择自己生活方式的问题。早期的分享是“结绳记事”“口耳相传”“纸墨留香”,如今的分享则往往借助于第三方(平台)。于是,第三方因“介入分享”而成为事实上的分享对象之一,这就是第三方当事人规则背后的逻辑。无论是隐私权经典理论还是法院一般将隐私解释为私密的、独立于社会公众之外的信息,公民为了保护其隐私,最佳的方法只能隔离于社会之外、不再社交、不再分享。

(二)第三方当事人规则之于个人信息保护

应当承认,第三方当事人规则对于打击犯罪、维护公共利益具有重要作用。用美国学者科尔的话说,它维持了《第四修正案》的技术中立原则,“如果没有第三方当事人理论,投机的犯罪分子就会巧妙地利用公民与第三方当事人之间的信息隐私受到宪法保护这一点,使他们的整个犯罪活动受到《宪法第四修正案》保护。而这个结果将导致《宪法第四修正案》为平衡公民隐私和社会安全之间的利益所做出的努力付之东流,并削弱了刑法的威慑和惩罚作用”。[⑥]换言之,第三方当事人规则既有助于惩罚犯罪,又可能确保一个无罪的人不会受到错误的刑事追诉。

但仅看到第三方当事人规则之“效益”还不够,社会环境发生改变,该规则受到的质疑也越来越多。首先,在网络时代,监控是互联网的商业模式。历史已经并将继续证明,用户交出个人信息、迎接监控社会的到来是不可抗拒的,这一变化既由政府推动,也由消费者驱动。“随着消费者

① See United States v. Hoffa, 385 U. S. 296 (1966).

② See United States v. White, 401 U. S. 745 (1971).

③ See United States v. Miller, 425 U. S. 435 (1976).

④ See Smith v. Maryland, 442 U. S. 735 (1979).

⑤ See Katz v. United States, 389 U. S. 347 (1967).

⑥ [美]奥林·S.科尔:《第三方当事人理论与合理的隐私期待》,陈圆欣译,载张民安主编:《隐私合理期待分论》,中山大学出版社2015年版,第484页。

接受的不可抗拒的产品越来越多,我们交出的个人信息也就越多,那些变得更聪明的机构承担了这项业务。这是一个自我强化的循环。”①如果法官严格适用第三方当事人规则来审判涉及网络信息的案件,那么在这些案件中,公民对其网络信息所享有的权利都得不到法律的保护。其次,第三方当事人规则的前提预设已失去说服力。在网络时代,还能将现在的信息曝光情形类推为传统的信息披露情形吗?在早期的卧底案件中,被告可以自行决定隐藏哪些个人信息,选择披露还是不披露,起码拥有一定的意志自由,现在则截然不同。美国马歇尔大法官提出:“在打电话已经成为公民日常生活中必不可少的一种需求时,在公民向电话公司披露其电话号码信息的情况下,认为公民在这种情况下自担风险的观点是否具备现实性?”②为此,《中华人民共和国个人信息保护法》(以下简称《个人信息保护法》)第 16 条规定,个人信息处理者不得以个人不同意或者撤回同意为由,拒绝提供产品或服务。最后,第三方当事人规则赋予政府过大的权力,极易侵犯公民的信息隐私。在美国,具有明显隐私权传统的个人信息保护将“公开可得信息”排除在保护范围之外,③“政府对于来自第三方的私人信息的处置被划到保护范围之外,其结果是,当政府搜查或起获由第三方持有的私人信息时,政府的行为既不需要具备合理性,也不需要任何司法授权”。④在我国,基于现行网络平台数据协查机制,网络平台对来自侦查人员的数据调取毫无规范可言。其具体表现如下:(1)调取程序不统一,有些平台要求出具《调取证据通知书》,有些要求出具单位介绍信即可;(2)对调取数据的类型未予区分,尤其是对敏感数据与一般数据相同对待;⑤(3)轻罪与重罪不分;(4)调取对象不问,不管是嫌疑人、罪犯或证人。换句话说,“政府机构的数据信息共享以及第三方披露义务的规定为公权的数据采集和运用‘大开方便之门’”。⑥

二、第三方当事人规则的文本考察及类型

(一)第三方当事人规则的文本考察

实质上,第三方当事人规则是经由法官阐释并创造出来的,但是这一过程并非空穴来风,而是建立在诸多规范性的法律文本及自治文本上。

1. 法律文本中第三方当事人规则的呈现。从国内法的角度看,诸多法律规定了第三方平台向政府机关提供个人信息的义务,主要体现在以下 3 个方面:(1)涉及国家安全、网络安全方面的法律。例如,《中华人民共和国国家安全法》第 52 条规定国家安全机关、公安机关等依职责依法搜集涉及国家安全的情报信息;第 77 条第 4~5 款规定了公民和组织向前述机关提供便利条件、必要支持和协助的义务。《中华人民共和国反恐怖主义法》第 18~19 条以及《中华人民共和国网

① [美]马克·罗滕伯格、[美]茱莉亚·霍维兹、[美]杰拉米·斯科:《无处安放的互联网隐私》,苗森译,中国人民大学出版社 2017 年版,第 79 页。

② 转引自[美]莫努·贝蒂:《社交网络、政府监控与隐私的合理期待》,凌玲译,载张民安主编:《场所隐私权研究》,中山大学出版社 2016 年版,第 142 页。

③ 参见刘晓春:《已公开个人信息保护和利用的规则建构》,《环球法律评论》2022 年第 2 期。

④ Fred H. Cate, Government Data Mining: The Need for A Legal Framework, 43 Harvard Civil Rights-Civil Liberties Law Review, 485 (2008).

⑤ 参见王燃:《大数据时代侦查模式的变革及其法律问题研究》,《法制与社会发展》2018 年第 5 期。

⑥ 张可:《大数据侦查之程序控制:从行政逻辑迈向司法逻辑》,《中国刑事法杂志》2019 年第 2 期。

络安全法》(以下简称《网络安全法》)第28条也规定了网络服务提供者应当维护国家安全和为侦查犯罪活动提供技术支持和协助的义务。(2)涉及刑事侦查及诉讼方面的法律。例如,《中华人民共和国刑事诉讼法》(以下简称《刑事诉讼法》)第52条规定了相关个人及单位应当如实向公安机关提供证据的义务。《公安机关执法细则》(第3版)及公安部《公安机关办理刑事案件程序规定》第57～59条规定了侦查机关有权向相关个人或单位调取与案件有关的物证、书证及视听资料。① (3)涉及个人信息保护方面的法律。例如,《中华人民共和国民法典》(以下简称《民法典》)第1036条第2款规定,处理"自然人自行公开的或其他已经合法公开的信息"行为免责;《个人信息保护法》第13条第3、6款和第27条也与该规则息息相关,能为第三方当事人规则之适用提供广阔空间,如自然人提供给网络服务商的个人信息是否属于"自然人自行公开或已经合法公开的信息"?

2. 自治性文本中第三方当事人规则的呈现。除法律文件外,互联网企业发布的自治性文本也隐含第三方当事人规则。例如,《微信隐私保护指引》第1.32条规定了"无需用户同意,微信即可自行收集并使用个人信息"的情形,其中a款(为履行法定义务或法定职责所必需)、d款(处理用户自行公开或者其他已经合法公开的个人信息)和e款(行政法规规定的其他情形)与第三方当事人规则紧密相连。② 又如,《京东隐私政策》第(3)部分同样包含"根据法律法规、行政及司法部门强制性要求进行提供""基于符合法律规定的社会公共利益、突发公共卫生事件而使用"个人信息的内容。③ 再如,《"抖音"隐私政策》第1.10条规定了"依法豁免征得同意处理个人信息"情形,其b款为"为履行法定职责或者法定义务所必需,例如与国家安全、国防安全、与刑事侦查、起诉、审判和判决执行等直接相关的法定职责或者法定义务",其e款为"处理自行公开的个人信息,或者其他已经合法公开的个人信息"。④ 总之,无论是基于法律文件施加的"协助披露"义务,还是互联网企业"隐私政策"中的声明,其在法律层面与事实层面都为第三方当事人规则的适用大开方便之门。

(二)第三方当事人规则适用的情境类型

1. 政企共谋。第三方当事人规则的典型生态表现即政府与企业共谋个人信息收集及利用。2015年11月24日,浙江省高级人民法院与阿里巴巴集团签署战略合作框架协议。双方以审务云平台为依托,整合浙江省各级人民法院案件数据资源,结合公安、政务、金融、电商、社交、交通等周边数据,形成跨界融合、全面覆盖、移动互联、智能应用的"智慧法院"大数据生态圈。⑤ 此消息一出,欢呼者有之——终于有望解决"送达"难题,质疑及忧虑者也有之——合宪性及个人信息保护愈加扑朔迷离。该事件非常契合第三方当事人规则,用户既然自愿将个人信息提供给阿里巴巴集团,那么阿里巴巴集团自然就能提供给人民法院。"斯诺登事件"就揭露了美国国家安全

① 参见孙茂利主编:《公安机关执法细则(第三版)释义》,中国民主法制出版社2016年版,第295～296页。

② 参见《微信隐私保护指引》,http://weixin.qq.com/cgi-bin/readtemplate?lang=zh_CN&t=weixin_agreement&s=privacy,2022-06-04。

③ 参见《京东隐私政策》,https://about.jd.com/privacy/,2022-06-04。

④ 参见《"抖音"隐私政策》,https://www.douyin.com/agreements/?id=6773901168964798477,2022-06-04。

⑤ 参见《浙江高院联手阿里巴巴打造"智慧法院"》,https://www.chinacourt.org/article/detail/2015/11/id/1755976.shtml,2022-06-04。

局依靠众多企业来监控互联网的真相,美国国家安全局秘密收集了数千万美国人的通话记录,利用由美国电话电报公司、沃莱詹通信公司及贝尔南方公司提供的数据。① 美国《爱国者法案》通过后,"所有前往美国的航班甚至必须在抵达之前,就以电子形式向数十个美国执法机构,提供每位旅客的详细个人资料,包括地址、信用卡资料等等,好让美国政府得以和犯罪嫌疑人资料库交叉比对"。②事实上,政府从企业获取数据已经常态化、制度化,甚至可以说形成了"业务外包",据《华盛顿邮报》2010 年报道,有 1 931 个不同的公司在为美国境内的情报、反恐、国土安全等方面开展工作;③同样,英国政府通信总部通过代号为"TEMPORA"的计划,向英国电信公司和沃达丰电信公司付费,以取得全球各地的大容量通信数据,沃达丰提供了阿尔巴尼亚、匈牙利、埃及、爱尔兰等 19 个国家的通信数据。④

2. 企企共享。第三方当事人规则的适用还体现在"公开披露后的利用"及"数据共享"情境中。首先,一旦公民主动在某平台(尤其是类似抖音、微信以及求职或相亲等社交平台)公开发布某一信息,该信息就立刻丧失隐私信息属性而成为"合法公开发布的信息",其他平台自然能使用该信息,这一点已经得到《民法典》第 1036 条和《个人信息保护法》第 13 条第 6 款的肯定。其次,是数据共享,《淘宝隐私权政策》第三(一)部分"共享"规定无需用户同意,淘宝即可共享用户个人信息的种类,该部分第 4 款即为"与关联公司间分享"的情形。⑤ 换句话说,用户个人信息被披露的对象可能远远超出完成订单所需提供的必要范围,而消费者对此并不知情。事实上,笔者曾阅读过的互联网企业隐私政策几乎都有类似的共享条款,而合作伙伴、关联方、第三方又各自有别的合作伙伴、关联方、第三方,如此一来,个人数据将在"数据共享"的名义下失去控制。

3. 政政互通。"政政互通"指的是政府数据库之间的共享。与互联网企业相比,政府数据库中的个人数据涵盖门类更广,所涉公民信息更重要。在政务信息化建设及政府信息公开实施之前,如果说各政府机构间的数据共享还不那么频繁的话,那么当今的数字政府理念让政府机构间的数据库连接与共享常态化并制度化。2010 年中纪委、中组部、中宣部等联合发文《关于建立和完善执行联动机制若干问题的意见》,2011 年公安部牵头联合发布《关于建立实名制信息快速查询协作执法机制的实施意见》,2014 年最高法、证监会联合发布《关于加强信用信息共享及司法协助机制建设的通知》,2016 年最高法、公安部联合发布《关于建立快速查询信息共享及网络执行查控协作工作机制的意见》。从这些规范性文件可以更加清晰地看出国家权力机关间信息互通的趋势。⑥ 不仅如此,政府数据库共享还将负有公共职能的第三方采集的信息纳入其中,如国务院 2016 年发布的《政务信息资源共享管理暂行规定》第 2 条就将政府各部门间信息交流与共

---

① See Roger Wollenberg, NSA Has Massive Database of Americans' Phone Cells, USA Today, 11 May, 2006.

② [英]麦尔荀伯格:《大数据·隐私篇:数位时代,「删去」是必要的美德》,林俊宏译,台湾地区远见天下文化出版股份有限公司 2015 年版,第 206 页。

③ See Dana Priest, William M. Arkin, A Hidden World, Growing Beyond Control, Washington Post, 19 July, 2010.

④ See Jame Ball, Luke Harding, and Juliette Garside, BT and Vodafone Among Telecoms Companies Passing Details to GCHQ, Guardian, 2 August, 2013.

⑤ 参见《淘宝隐私权政策》,https://terms.alicdn.com/legal-agreement/terms/suit_bu1_taobao/suit_bu1_taobao201703241622_61002.html?spm=a2e15.8261149.1997523009.40.528429b42m529u,2022-06-04。

⑥ 参见张兆瑞:《关于公安大数据建设的战略思考》,《中国人民公安大学学报》2014 年第 4 期。

享的范围扩展至“政务部门直接或通过第三方依法采集的、依法授权管理的和因履行职责需要依托政务信息系统形成的信息资源等”。

总之,第三方当事人规则已经远远超出侦查机关自第三方获取信息的情形,政府拥有广泛的权力去收集、分析数据,“一方面它可以基于同任何公众成员一样的方式公开获取可用数据,可以以合同的方式取得数据;另一方面它还可以行使独一无二的权力,通过发出需要私人数据作为调查结果的传票、搜查令、窃听命令、国家安全密函、外国情报监视法令等方式达到目的”。①

三、第三方当事人规则对个人信息保护基本规范的背离

在“卡彭特诉美国案”②中,美国联邦最高法院裁定警方必须获得法院签发的搜查令才能追踪公民的手机位置信息,而按照惯常理论(第三方当事人规则),警方完全可以在没有搜查令的情况下获得该定位信息。借此契机,我们必须反思:第三方当事人规则究竟在哪些方面背离个人信息保护的基本规范?

(一)“合法性”存疑

“合法”是个人信息保护的首要原则。《欧盟一般数据保护条例》(以下简称《欧盟条例》)第6条规定了6种合法性基础,《个人信息保护法》第13条规定了7种合法性基础。而之所以说第三方当事人规则违反“合法”原则,是因为以下两个方面。

1. 违反“合法”原则中的“同意”规则。之所以称“同意”为规则,是因为将“同意”归为“合法”的具体情形之一。《欧盟条例》第6条规定的6种合法性基础中,第一种就是“数据主体的同意”,《个人信息保护法》亦然,《网络安全法》第41条更是将“经被收集者同意”视为网络运营者收集、使用个人信息的必备要件。而在很多学者眼中,第三方当事人规则恰恰是一种“同意或弃权”规则,③即当公民把自己的隐私透露给第三方时,公民实质上就是同意政府执法人员对自己的隐私信息进行搜查。这是一种“推定同意”。④ 这其中存在两个方面的同意:公民自愿将信息告知第三人,以及第三人自愿将信息披露给政府执法人员。然而,这两种同意都是虚假的。一方面,现代社会已经离不开第三方的参与,即使离群索居生活,也要将家庭住址等信息告知电厂和水厂,还有银行、交通部门、电信部门等;另一方面,第三方也并非完全出于“自愿”而将消费者个人信息披露给政府人员。例如,2013年雅虎首席执行官玛丽莎·梅耶尔在解释为什么雅虎没有保护用户隐私时称:“如果你不遵守,这是叛国罪”。⑤可见,第三方当事人规则蕴含的“自愿”及“视为同意”既不合逻辑也不完全合乎现实。

2. 作为第三方当事人规则的最大受益者,国家机关处理个人信息更需合法。美国《隐私法案》(1974)专门针对政府而立,规范政府机构应当如何收集个人信息、收集什么类型的个人信息、

① [美]特伦斯·克雷格、[美]玛丽·E. 卢德洛芙:《大数据与隐私——利益博弈者、监管者和利益相关者》,赵亮、武青译,东北大学出版社2016年版,第61页。

② See Carpenter v. United States, 138 S. Ct. 2206; 585 U. S. (2018).

③ See Sonia K. McNeil, Privacy and the Modern Grid, 25 Harvard Journal of Law & Technology, 216－218 (2011).

④ 参见宁园:《“个人信息已公开”作为合法处理事由的法理基础和规则适用》,《环球法律评论》2022年第2期。

⑤ Alex Dickinson, Yahoo CEO Feared Jail over NSA Scandal, New York Post, 12 September, 2013.

如何向公众开放以及信息主体的权利等。欧盟则是另外一种模式,即公主体和私主体统一适用《欧盟条例》。例如,《欧盟条例》第 4 条在对数据“控制者”“处理者”“第三方”等主体进行解释时将“自然人、法人、公共权力机关、代理机构或其他机构”囊括在内。在《欧盟条例》之外,欧洲议会和欧盟理事会在 2016 年 4 月 27 日发布了《针对警察和刑事司法机关的数据保护指令》,专门用以规范刑事司法领域的数据处理。而《网络安全法》主要的规制对象是“网络运营者”,政府机关并不是该法的适用主体。由此引发的疑问是,建有庞大数据库的政府机关如何执行“网络信息安全”的规定?《中华人民共和国数据安全法》(以下简称《数据安全法》)第 6 条虽然规定公安机关和国家安全机关是适格主体,但是条款内容却指向承担数据安全监管职责。《个人信息保护法》虽在第 2 章第 3 节专门对国家机关处理个人信息行为作出规定,但也存在问题——这里的国家机关是否包含刑事司法机关?答案不言而喻,我国当前的数据保护法与大数据时代的侦查权脱节甚远。

(二)数据主体权利易遭忽视

隐私的重要性从来不在于私法层面,而关乎一个完整、独立、自决的“人”。美国学者塞弗森谈到:“我们必须学会将个人数据视为自我的延伸,就像对待活生生的个体的人一样,给它同等尊重。否则,我们就面临损害自己隐私的风险;正是有了隐私,才让自我决定成为可能。”①这种倡导自我决定、自我统一性的隐私,与美国学者科恩所理解的隐私有异曲同工之处:“隐私保护了动态的、新兴的主体关系,使其免受商业和政府行为侵扰,不至于使个人和社群成为固定、透明和可预测的对象。它保护了边界管理中情景化的做法,自我决定的能力正是通过这种做法得以发展”。②个体的统一性是我们所有人驾轻就熟、采取各种隐私保护手段而加以维护的东西,而第三方当事人规则恰恰在破坏它。而无论是“自我统一性”还是自治的实现,都离不开知情权即关于我们的个人信息被如何处理、如何使用的知情。在多数情境中,个人会出于特定的需要将个人信息披露给第三人,个人也希望“基于交易目的而不是其他”去使用个人信息。然而,个人在政府与企业的共谋面前毫无抵抗力,甚至没有机会对信息及其潜在意义进行一番主动评估。引用美国学者乔纳森·格鲁丁的观点,在数字技术中,我们遭遇了“显然已被场景化的行动的持续侵蚀。我们正在失去对我们行动后果的控制和了解……因此,不再能够控制自己披露的任何东西”。③美国著名隐私权学者索罗韦伊曾探讨过何谓有效的隐私保护制度,他认为有效的隐私保护制度“应当是个人能够自主选择何种信息可以被收集与使用的制度,在这一制度下,个人对其隐私信息的使用享有充分而自主的选择权,在这一制度下,个人与大型机构之间由于巨大的知识、权力以及其他障碍而造成的不平等地位将被消除,在这一制度下,个人能够在被通知且自主的情况下表达其同意的意愿”。④《个人信息保护法》第 23 条紧跟时代潮流,规定个人信息处理者向第三方提供其处理的个人信息时,应向信息主体告知第三方的身份、联系方式、处理目的、处理方式和个人信息的种类,并取得个人的单独同意。显然,第三方当事人规则妨碍了信息主体“知情权”的实

① Richard W. Severson, The Principles of Information Ethics, Armonk, M.E. Sharpe, 1997, pp.67-68.

② Julie E. Cohen, What Privacy Is For, 126 Harvard Law Review, 1905 (2013).

③ 转引自[美]约翰·切尼-利波尔德:《数据失控:算法时代的个体危机》,张昌宏译,电子工业出版社 2019 年版,第 208 页。

④ [美]丹尼尔·J.索洛韦伊:《隐私权与权力:计算机数据库与信息性隐私权隐喻》,孙言译,载张民安主编:《信息性隐私权研究:信息性隐私权的产生、发展、适用范围和争议》,中山大学出版社 2014 年版,第 176 页。

现，也弱化了信息处理者的“告知义务”。

（三）人际交往及自由权易受非法干预

技术和法律共同规定了现代社会的人际交往：一方面，网络技术使得公民的交往空间、交流方式、人际关系都发生了质的改变，人们足不出户却与世界相连；另一方面，法律又给“线上”交流套上枷锁。第三方当事人规则便给“线上”交往设定了沉重枷锁——公民对在网络交往中主动披露的信息不再抱有合理隐私期待。然而，从“线上”交流的情境出发，这种设定是否合理？首先，所有社会互动的基础都始于自我介绍，并通过允许用户建立自己想要的身份来强化用户建立自己独特身份的需求。就此，每一个账户的个人档案实质上是一种受到控制的社会建构。其次，隐私权并不意味着“离群索居”，如果公民认识到与别人分享这一社会实践是公民生活的主要构成部分，不否认“即便公民与别人分享个人事务，公民仍然希望所分享的信息不被社会公众所知悉”，那么来源于社会实践的隐私权理论就必须重新审视第三方当事人规则。最后，第三方当事人规则的预设是“你将信息告诉他人，也就相当于告诉了全世界”，该规则成立的初衷是“他人在实质上参与了交流，是人际交往的一部分”。然而，第三方服务提供者仅仅是公民网络交往的中介。就此而言，公民私密信息受到政府侵害的风险产生于人际交往过程之外。对此，我们需要反思，“为什么在作为风险之源的网络服务提供者对公民的交流没有做出实质贡献的情况下，公民仍然需要承担起隐私信息受到政府侵害的额外的风险？”①不仅如此，如果将人际交往推广到自由权，那么第三方当事人规则对社会的破坏更为严重。其一，法律应当保护特定类型的、高度私人化的社会关系，因为它们是衡量政府是否不当干涉公民自由权的重要依据。“如果政府知道公民分享给第三人的所有事情，无论是私人信息、对话或网络，还是住所、所有物或其他空间，政府可能会主导公民的人际关系；如果政府真的主导了公民的人际关系，那么作为公民自由选择或者政治认同基础的自由权，则会渐渐被破坏。”②其二，自由权的实现，有赖如下保证——政府在不具备充分合理依据的情况下，无权获得公民之间自由的信息交流。从本质上讲，表达自由与交往自由不仅要求他人向其他人披露自己的信息，而且还要求通过一定的方式保证他人的信息不会为政府所知悉。而之所以说第三方当事人规则的隐藏含义是“恶”的，就是因为它一并排除了表达自由和交往自由所同时要求具备的上述两个本质要求。一方面，不受实质约束的政府数据监控使得公民的信息隐私无法得到保障；另一方面，公民为了保障信息隐私而对交往自由进行自我限制或放弃。如此，宪法所保障的自由陷入了两难对立之境地。

（四）政府权力的扩张危及公民人权

第三方当事人规则可能在两个层面加剧公民与政府间的“权利－权力”失衡：一是“泛在监控”的形成，二是大数据侦查可能使得犯罪嫌疑人正当权利受损。

首先，第三方当事人规则打通了政府数据库与企业数据库，通过交叉比对与数据挖掘，政府能够全面掌握每个人的个人信息。德国联邦法院在1983年“人口普查案”判决中指出：“在综合性资料系统下，可以将个人资料组合成部分或相当完整的人格图像，以致会对个人人格产生威

① ［美］莫努·贝迪：《Facebook与人际交往隐私权——为什么第三方当事人规则不能适用》，马志健译，载张民安主编：《隐私合理期待分论》，中山大学出版社2015年版，第474页。

② ［美］托马斯·P.克劳克：《从隐私权到自由权——Lawrence一案后的〈美国联邦宪法第四修正案〉》，敬罗晖译，载张民安主编：《隐私合理期待分论》，中山大学出版社2015年版，第375页。

胁,因此原本无关紧要的一项资料,可以在资料整合之下产生新的价值,所以在此情形下已不再有所谓不重要的资料。”[①]政府数据库的建立在本质上是一种公权力的扩张及对公民私生活的介入,从法理上讲,“国家中心数据库的建立涉及公民基本权利和自由,必须由立法机关立法,制定明确的法律依据。在立法时,关键在于严格限制该数据库的利用,只有重大社会公共利益方能构成利用的正当性理由,在立法中明确利用该数据库的具体情形和前提条件”。[②]然而,现实却是政府已将“权力之手”延伸到企业数据库,在打通“公”“私”两域的同时强化了控诉职能。[③] 诚然,第三方当事人规则确实在某些刑事案件侦查过程中扮演了重要角色,但其危险在于:一旦社会环境发生改变,这些工具将会迅速更换监控对象。

其次,第三方当事人规则使得大数据侦查中犯罪嫌疑人的正当权利受损。其理由如下:(1)“无罪推定”不再牢固。基于风险防控理念,“预测警务”在我国犯罪治理中占据越来越重要的地位,这也意味着刑事侦查启动的节点提前。2015 年,中共中央办公厅和国务院办公厅联合印发《关于加强社会治安防控体系建设的意见》,强调通过“强化信息资源深度整合应用,充分运用现代信息技术,增强主动预防和打击犯罪的能力”。而要实现该目标,数据收集与分析将先于“立案标准”进行。从表面看,该变化仅导致侦查权行使的时间前移了一点,但实际上,侦查权却得到极大的扩张,且不受刑事侦查正当程序的限制。这种不受实质限制的侦查权扩张与“无罪推定”原则有无冲突呢?答案是肯定的。“无罪推定原则的要义在于,对审前预判以及基于该预判进行的干预或限制公民基本权利的行为进行严格限制,这种限制与审前具有社会防卫性质的措施存在紧张关系。”[④](2)第三方当事人规则使得公民的程序性权利受损。自动化决策机制的形成往往被视为“黑箱效应”,大数据侦查同样如此。尽管大数据侦查缘于大数据本身的技术特征,但是仍对正当程序原则产生重大的影响。[⑤] 正当程序旨在规范和限制公权力,以保障犯罪嫌疑人在刑事诉讼中的正当权益,若有侵犯,侦查行为则变身“非法搜查”。但第三方当事人规则使得一切数据的收集、比对及挖掘行为合法化。例如,在美国,“在没有搜查许可的情况下,有权通过国家安全信函有针对性或者批量搜集各种各样的个人信息,这些基本上都是联邦调查局在没有司法监督的情况下,发出的行政传票”。[⑥] 而在我国,甚至“国家安全信函”这样的文件都不需要,侦查人员手持单位介绍信即可。如此,第三方当事人规则在事实上排除了“非法搜查”的存在空间,继而,公民陷入无由申诉、无法质证、无效辩护且只能无奈接受的不对等刑诉程序中。

---

① 转引自《“一九八三年人口普查案”判决》,萧文生译,载台湾地区“司法院”秘书处编:《西德联邦宪法法院裁判选集》(一),台湾地区“司法院”1991 年版,第 288 页。

② 陈新民:《德国公法学基础理论》(下册),山东人民出版社 2001 年版,第 358 页。

③ 参见郑曦:《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》,《河南大学学报》(社会科学版)2020 年第 2 期。

④ 裴炜:《个人信息大数据与刑事正当程序的冲突及其调和》,《法学研究》2018 年第 2 期。

⑤ See Crawford. Kate, Schultz. Jason, Big Data and Due Process: Toward A Framework to Redress Predictive Privacy Harms, 55 Boston College Law Review, 109 (2014).

⑥ [美]布鲁斯·施奈尔:《数据与监控——信息安全的隐形之战》,李先奇、黎秋玲译,金城出版社 2018 年版,第 95 页。

四、个人信息保护中第三方当事人规则的解决方案

在司法实践中已有反思第三方当事人规则适用的案例，主要集中在通信领域，如严格区分地址信息和内容信息、对加密信息予以特殊保护等。但新情况产生新的法律问题，人民法院不能比附旧的案例解决所有的问题。摒弃第三方当事人规则之惯性思维，使得政府在“多重规制”之下对个人信息实施搜查，是一件很重要的事。

（一）来自令状制度的新思路

事实上，在国外这一思路已相对成熟并付诸实施。以美国为例，《第四修正案》反对“非法搜查与扣押”的规定是保护公民信息性隐私权的最主要依据，通过“搜查令”制度来对抗警察的滥权行为。除此之外，美国国会还颁布了一系列成文法来规制警察不受限制地要求第三方披露用户特定信息的行为：1970 年《公平信用报告法案》规定，消费者的信用报告只有在响应法庭指令或应报告当事人书面请求时，方能提供给第三方；1986 年《电子通信隐私法》规定，政府需要取得搜查证才能强制要求网络服务提供者披露某些特定信息，并且只能通过传票才能获取其他信息；2006 年《财务隐私法》[①]、《健康保险携带和责任法》[②]、限制政府执法人员查看公民电子邮箱的《存储通信保护法》[③]等都有相关规定。在德国，《德国刑事诉讼法典》中的“计算机排查侦缉”与我们平时讲的数据比对、数据挖掘并无二致，也规定了严格的法律程序，并比照电话监听对大数据侦查实施法官令状制度。在数据比对过程中，比对的数据库来源不同，所设程序的严格性也有不同——刑事司法部门自身所属数据库间的比对相比司法机关之外的其他部门或单位所属数据库的比对要稍微宽松一点，毕竟后者对公民的个人信息自决权造成的干涉更多。[④]

至于我国可否实施法官令状制度，是值得商榷的。有学者认为，我国尚不具备实施该制度的条件和可能性。[⑤] 但在无其他更优设计之前，对法官令状制度进行改造是可行的。具体而言，可以在以下 4 个方面做出努力：（1）由检察机关对申请进行审查，并在认为条件符合时发布令状，由侦查机关向占有或控制犯罪嫌疑人个人信息的第三方主体进行取证。（2）检察机关判断发布令状的条件不宜过于宽松，且针对不同的搜查对象其严格程度也有不同。一般来说，侦查机关需向检察机关提供材料证明两项基本事实：一是该数据由特定第三方主体控制或占有；二是该数据与侦查案件具有关联性，但仅此还不足以对抗第三方对所收集/存储信息的保护义务。美国针对此种情形，于 1994 年引入了更加严格的令状条件，即“具体而明确之事实”要求。获取此种新令状的难度介于取得传票与取得搜查证之间，政府必须提供“具体而明确的依据来使法院相信：其所要求获得的记录信息关乎某个正在进行的刑事调查活动，并且具有重大作用”。[⑥]并且，警方申请获取的证据越是靠近“私密领域”就越要提交充分材料来证明其重要性和必要性。在美国，警方调取私密程度不同的数据时，需要履行传票、法庭调查令、搜查令等不同程度的程序就是基于此

① See 12 U. S. C. § 3401－3422 (2006).

② See 45 C. F. R. § 164. 512 (f) (l) (ii) (A) (2007).

③ See 18 U. S. C. § 2703 (c) (2005).

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 29～31 页。

⑤ 参见程雷：《大数据侦查的法律控制》，《中国社会科学》2018 年第 11 期。

⑥ United States v. Kennedy, 81 F. Supp. N. 2d 1103, 1109 n.8 (D. Kan. 2000).

道理。(3)检察机关签发令状后,仍要保持对侦查机关数据侦查行为的检察监督。这又分为两个方面:一是可以考虑建立大数据侦查的备案机制,实现办案数字系统互联互通,侦查机关要将数据排查的开展过程、相应结果在线提交,以接受检察机关的备案审查和法律监督;二是检察机关在后续的批捕、审查起诉阶段对侦查机关提交的数据证据进行合法性审查,对非法搜查所得证据限制适用。(4)基于坚持"控辩平等"原则及保障当事人诉讼权利的考量,有必要将辩方的程序性介入相应提前。① 侦查机关对数据收集及数据挖掘的能力远超个人,同时,侦查机关也更倾向于收集对己方有利的证据,而对利于当事人的证据视而不见,这将直接影响当事人的质证能力。

(二)来自比例原则的制约

比例原则在个人信息保护领域占有重要的地位,一方面跟隐私领域理论有关,另一方面跟个人信息保护向公法扩展有关。在大数据侦查规制理念中,比例原则化身"愈……愈……"公式:"若资料愈是涉及当事人的私密领域或一个特别的信赖关系时,则对于比例原则的检验要求就应愈严格……若资料愈能回溯推论出创作者身份或是产生羞辱效应时,则应更加清楚与严格地说明其目的拘束。此外,若资料的匿名程度愈高且愈接近单纯的统计时,则国家愈能够自由地调查与利用"。②这个看似简单的公式能否单纯依靠个人信息敏感性来适用比例原则呢?恐怕不是如此简单,其原因在于,保护个人正当权益仅是比例原则的核心任务之一。兼顾公共利益与个人正当利益,需要依照比例原则的构成要件在个案中进行具体的分析。

关于比例原则的构成要件,我国行政法学界一般划分为适当性、必要性和平衡性,③下面结合三要件依次阐述。(1)适当性原则,是指在"目的-手段"的关系上必须是适当的,存在一个正当目的导向的要求。至于执法手段在多大程度上达成目的,在所不问。这也由此受到诸多诘责,因为无论什么手段,总会多多少少跟"目的"有关。第三方当事人规则的适用更是如此,不管是警方初查还是立案侦查,总会与公共利益有所关联。所以,适当性原则不能严格地遵循"结果导向",而要兼具"过程导向",要与案件本身的性质、严重程度、涉及公民个人信息种类等关联起来。即目的必须是合法、特定的:合法是指政府信息获取行为发生在法定职权范围内,特定是指结合传票、搜查令等的申请,将欲通过执法行为实现何种目的予以明示,从而形成实质上的"目的拘束力"。(2)必要性原则,指通过网络服务商获取公民信息既是"最后"手段也是对公民基本权利干预最少的手段。唯有那些性质严重、涉及公民数据众多、所获取信息敏感程度高的案件,执法人员才能对犯罪嫌疑人及相关人员实施全面的数据监控及数据挖掘行为。(3)平衡性原则,是指所采取行为要与目的达成之间符合比例,要在维护社会公益与个人利益之间维持均衡,"愈……愈……"公式严格来说应放置在这里。例如,《数据安全法》第 21 条初步规定了数据的分级分类保护,《欧盟条例》与《个人信息安全规范》分别规定了"个人敏感信息"的概念及范围等;《网络犯罪公约》将个人信息分为注册人信息、交互信息和内容信息;2014 年网络犯罪公约委员会在 30 个成员方中进行的调查显示,披露注册人信息的基本要求是至少怀疑某人实施了某项犯罪行为。

① 参见裴炜:《个人信息大数据与刑事正当程序的冲突及其调和》,《法学研究》2018 年第 2 期。

② 陈戈、柳建龙等:《德国联邦宪法法院典型判例研究——基本权利篇》,法律出版社 2015 年版,第 120 页。

③ 参见杨登峰:《从合理原则走向统一的比例原则》,《中国法学》2016 年第 3 期。

而披露注册人信息对于隐私权的影响最低，对于交互信息和内容信息的披露条件更高。①

（三）来自隐私权理论的再审视

事实上，当前个人信息权利救济主要还是依赖隐私权，面对第三方当事人规则的“隐私失权”预设，当代隐私权理论需要作出两个方面的转变。

首先，依“语境”而非“一刀切”地判断隐私期待之合理性。“合理隐私期待”概念的精妙之处在于它将论证过程分为两个部分——主观的、实际的隐私期待及客观的社会认同，而不论是主观期待还是客观认同，都存在一个“程度”的问题。而“程度”的判断取决于具体的语境。美国学者尼森鲍姆认为：“人们并不因此认为，在隐私场所之外，人们的隐私权就不再受隐私权规范的保护。换言之，人们不会认为，如果人们离开某些特定的场所，人们的信息就与其原本的语境相剥离，从而变成了人们口中所说的‘人人有份’的信息。”②第三方当事人规则显然无视语境的特殊性，对所有用户提供给网络服务提供者的情形一视同仁。换言之，人们在不同的语境中原本含有程度不同的隐私期待，但第三方当事人规则抹杀了这种差异。支持第三方当事人规则的法官显然把隐私想象成了“要么全开、要么全关”的开关，这种理念虽然简单明了，但是它背离了社会实践的真相。美国马歇尔大法官认为：“隐私不是一件独立的商品，不能简单地认为公民完全拥有或者完全不拥有它。为了某个特定的商业目的把自己的信息披露给一家银行或者一家电话公司，公民不需要承担其信息因为别的目的而被第三方当事人向别人披露的风险。”③

其次，法官常将隐私权解释为独立于公众之外的私人信息，且在论证该信息的“私密性”时，往往需要权利主体有“维持其私密性”的努力，这一努力表现为使该信息不为任何人所知。这种解释正好迎合了第三方当事人规则，公民自愿披露其信息给第三方的行为使得维持信息私密性的努力失效。在该规则中“披露给第三方就等于披露给全世界”的判断背后，隐含的正是“第三方”等于“社会公众”的理念，更进一步，该规则传达了一种隐私信息向公共信息、私人事务向公共事务的转变。那么，这种判断是否正当？不可否认，数据库的出现使得许多个人信息同时具备了公共信息属性，如私人消费行为变成了公共记录的一部分，但两种信息界限的模糊并不等于两种信息的划分失去价值。“在公共事务领域内，政府有权设置标准和规则，该标准和规则适用于社会中的每一个人，而不论社会环境如何，或者公民的意愿如何。只有当公民对私人事务作出决定时会增加社会成本或者损害公共利益时，该行为才会转变为公共事务。”④在此理念下，面对兼具两种属性的个人信息时，要坚持一个原则——没有经过充分论证，不得随意牺牲个人的正当利益。⑤ 以这个思路反思第三方当事人规则，显然，告知第三方等于向全社会公开、用第三方替代社会的理念不符合个人信息保护的应然方向。

---

① 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。

② ［美］海伦·尼森鲍姆：《信息时代的公共场所隐私权》，凌玲译，载张民安主编：《公共场所隐私权研究》，中山大学出版社2016年版，第78页。

③ 转引自［美］奥林·S.科尔：《第三方当事人理论与合理的隐私期待》，陈圆欣译，载张民安主编：《隐私合理期待分论》，中山大学出版社2015年版，第491页。

④ ［美］托马斯·P.克劳克：《从隐私权到自由权——Lawrence一案后的〈美国联邦宪法第四修正案〉》，敬罗晖译，载张民安主编：《隐私合理期待分论》，中山大学出版社2015年版，第383页。

⑤ 参见张新宝：《从隐私到个人信息：利益再衡量的理论与制度安排》，《中国法学》2015年第3期。

(四)来自个人权利与公共利益的再衡量

在个人信息保护规范中有许多“同意之例外”条款,即无须数据主体同意即可处理个人信息的情形,如《欧盟条例》第 6 条、《个人信息保护法》第 13 条、《民法典》第 1036 条之规定。之所以如此,是因为个人信息背后的多元利益往往处于冲突之中。在第三方当事人规则中,从表面看公民因其主动披露行为而丧失合理隐私期待,而在实质上,这是个人信息为政府获取背后的公共利益对个人利益的胜利。换句话说,国家在社会治理中承担的事务越多,就越容易以“公共利益”之名驱逐“个人权利”。因为就数量计算而言,个人利益很难胜过公共利益。但也因此,个人信息利用及共享行为的规制理念决不能单纯地考虑“效用”,纯粹的功利主义计算会使得公民的信息权利毫无意义。

个人信息权利与社会公共利益的衡量,需要注意以下几点:(1)利益与权利不可通约,权利优于利益,且权利可以对社会公共利益施加限制。因为“权利不是以功利或社会效果为基础,而是以其正当性的演化与利益无关的道德原则为基础”。① 就此而言,权利是个人对抗社会政策的一张王牌。美国法学家德沃金也认为:“为了普遍的利益社会有权做任何事情,或者有权保护多数人希望在其中生活的任何一种环境……那么我们就是消灭了人们反对政府的权利。” ②(2)个人利益并非与公共利益截然对立。在个体与整体的关系上,“抽象地肯定人类权利却具体否定个人权利,颇有架空人类的意味。……所以,除非特指,我们所说的自由、平等、权利等都必须落实到个人才有意义”。③(3)公共利益优先的法定事由应具体,论证应充分。基于法律的一般性及抽象性,个别条款泛泛而谈出于保护公共利益的需要,无须告知数据主体就能处理公民信息,这并非最佳方案。第一,应采取“详列+兜底”的方法,尽可能将涉及公共利益的情形明示,如《刑事诉讼法》第 184 条将技术侦查限定在几种严重犯罪等情形。第二,政府申请搜查公民个人信息时,在提供材料中需有明确的指向,而不能模糊地表述为“保护公共利益”“打击恐怖主义犯罪”“维护国家安全”,甚至以“以防万一”为目的。第三,应在个案中决定个人权利与公共利益的取舍,同时予以充分论证。例如,在 2008 年欧洲人权法院审理的一个案件中,被告虚构并在网络上传播未成年受害人的性交易广告,但网络服务商拒绝提供被告之注册信息。对此,欧洲人权法院的法官认为,对服务商来说,基于隐私权保护所产生的保密义务不足以阻却侦查机关获取相关信息的要求。总之,公共利益不能成为一个口号,更不能打着公益的旗帜,恣意侵入公民的私人领域。④

五、结 语

第三方当事人规则貌似合情合理,在实质上却经不起逻辑的推敲与公民隐私生活的检验。在第三方当事人规则创设早期,政府信息获取难度较大,需要增强政府信息获取能力以维护公共

① [美]皮文睿:《论权利与利益及中国权利之旨趣》,载夏勇主编:《公法》(第 1 卷),法律出版社 1999 年版,第 107 页。

② [美]德沃金:《认真对待权利》,信春鹰、吴玉章译,中国大百科全书出版社 1998 年版,第 256 页。

③ 钱满素:《个人、社群、公正》,载刘军宁、王焱编:《自由与社群》,生活·读书·新知三联书店 1998 年版,第 2 页。

④ 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。

利益。然今时不同往日，当前努力的方向是限制政府超强的信息获取能力，从而减少政府恣意收集和利用个人信息的情形。《欧洲人权公约》有个很有意思的表述：相较于对名誉、声誉的保护仅限于非法攻击，《欧洲人权公约》对隐私的保护除禁止非法攻击外，还包括禁止任意干预。而“任意的干预包含了不正义、不可预测性和不合理性的因素。再者，‘任意的’这一表达就提示着国家机关的侵犯”。[①]就此而言，在公民隐私意识觉醒、数据权利彰显、个人信息保护迈入新阶段的今天，即便是基于犯罪侦查的需要从网络服务提供者手中调取用户信息，也应受到一定的限制，以实现国家利益、公共利益与个人正当权益平衡的目标。

Abstract: Nowadays, the Internet has become another “home”. When providing convenient network services, ISP also collect and store a large amount of personal information, many of which can provide clues to the detection of criminal cases, or even information that can itself be used as evidence. So, when citizens voluntarily disclose personal information to ISP, do citizens “risk at their own risk” for the possibility of their information being obtained by investigators? The third-party doctrine stands in a “yes” position and believes that citizens do not enjoy reasonable privacy expectations. However, after analyzing the “predecessor” and theoretical presuppositions, it's found that the rules are ostensibly consistent with the Internet age, but actually violate the true norms of personal information protection. This doctrine not only strengthens the big data investigation, but also probably invade the private domain of citizens and endanger the human rights. To break the habitual thinking of the third-party doctrine and solve relevant situational difficulties, it is necessary to follow the guidance of the principle of proportionality, innovate the writ system, re-examine the theory of privacy, and establish the principle of priority of individual rights.

Key Words: third-party doctrine, reasonable privacy expectations, data sharing, the right of privacy

责任编辑　　张家勇

① ［奥］曼弗雷德·诺瓦克：《民权公约评注》（上册），毕小青、孙世彦等译，生活·读书·新知三联书店 2003 年版，第 291 页。