欧盟大规模数据监控的赋权、制衡与挑战*

廖　丽　师亚楠

内容提要:2020年的新冠肺炎危机迫使国家采取大规模的监控手段维护安全,再次引起公民对隐私的担忧。不同于生命健康权等其他人权,隐私权本就具备可被减损的特性。处于隐私保护"道德高地"的欧盟,在确认以安全为目的进行大规模监控合法的情况下,要求监控机关的监控合法、合目的,在数据的审查、使用、保留和销毁环节尽足够的注意义务;要求监督机关能够获取所有的相关信息;要求救济机关为任何怀疑自己受到监控的个人提供有效救济途径。这样的隐私保护程序性规定成效斐然,为成员国监控权力的约束提供了范式。欧洲人权法院若能处理好欧盟法与成员国的裁量权关系问题,欧洲法院如进一步明确数据保护的标准,则可将隐私保护水平提升至全新的高度。

关键词:欧盟　大规模监控　数据安全　个人隐私　赋权

自新冠疫情暴发以来,为了有效抑制病毒传播,多个国家政府借助公民手机定位系统实现轨迹追踪,要求公民上报出行信息、身体状况,这样大范围收集个人信息的行为引起公民对隐私权的担心。在欧盟境内,欧盟委员会于2020年4月8日出台了一份委员会建议,为与抗击疫情相关的手机软件和数据的使用设定了基本的原则。① 在大数据时代,个人隐私应当为国家安全、卫生安全和公共安全等公共利益的保护做出何种程度的让步,如何保证国家在通过监控手段保护国家安全、公共安全等利益时的权力不被滥用,都是当今国际社会亟待解决的问题。联合国于2020年4月25日指

* 感谢匿名审稿人的建议,文章仅代表作者本人观点,文责自负。

① European Commission, "Coronavirus: Commission Adopts Recommendation to Support Exit Strategies Through Mobile Data and Apps," https://ec.europa.eu/commission/presscorner/detail/en/IP_20_626, last accessed on 2 December 2020.

出,本次突发疫情的事态已经演变成为一场人权的危机。①

大规模数据监控早期仅指对于通信传输过程中的参与者、持续时间、频率、使用设备或防卫等与通信内容本身无关的元数据②的监控行为。但随着各国对于打击恐怖主义、维护国家安全和公共利益的需求日益增加,被监控的数据范围逐渐扩大,通信内容也逐渐被囊括其中。③ 本文将聚焦"如何平衡安全与隐私"关系的问题,对欧洲人权法院与欧洲法院围绕大规模数据监控(既包含元数据也包括内容数据)的相关案例进行考察,总结欧盟的经验和不足,以此为中国提供借鉴。

一 赋权:基于国家安全目的确认大规模跨境监控的合法性

欧盟数据处理的规定包括欧盟指令 95/46、欧盟指令 2002/58、欧盟指令 2006/24 以及 2016 年的《一般数据保护条例》(GDPR)等,但大多数规定都将涉及成员国国家安全的行为排除在规范范围之外。如欧盟指令 2002/58 第 1 条第 3 款规定:"本指令不适用于……涉及公共安全、自卫、国家安全和国家刑法领域的行为。"④到目前为止,欧洲法院讨论大规模跨境监控案件安全与隐私关系的主要是欧洲人权法院和欧洲法院。欧洲人权法院的裁判依据为《欧洲人权公约》第 8 条第 2 款,欧洲法院的裁判依据为《欧洲基本权利宪章》第 52 条第 1 款,都将隐私权干涉的合法性判断分为两步:"依法"(in accordance with the law)以及"合目的"(公民隐私的限制对于民主社会中国家安全、公共安全等利益是必要的)。欧洲人权法院对于监控行为本身和规模大小的合法性做出解释,而欧洲法院侧重审查监控数据向欧盟境外流动方面的规则。

(一)监控行为本身的合法性

最早讨论公权力机关监控的是欧洲人权法院,它首先将合法性中的"依法"进一步分为三个要素:有国内法依据、可获得性和可预见性。2008 年的"韦伯与萨拉维亚案"中,欧洲人权法院首先指出监控行为本身应当依法。在确认了监控在德国有国内法依据——《德国监控法案》(以下简称"G10")后,欧洲人权法院对于可预见性做出

① 《联合国秘书长古特雷斯:将人与人权置于抗疫行动的中心》, https://news.un.org/zh/story/2020/04/1055752,2020 年 4 月 23 日访问。

② 吴常青、薛大政、吴轩:《欧盟法视野下的情报部门元数据监控——以欧洲法院数字权利案为视角》,载《情报杂志》,2016 年第 11 期,第 14-15 页。

③ Big Brother Watch and Others v. the United Kingdom, ECtHR Judgment of 13 September 2018, para. 336.

④ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, https://eur-lex.europa.eu/legal-content/EN/ALL/? uri=CELEX%3A32002L0058, last accessed on 30 April 2020.

进一步解释,认为在官方机构的秘密监控的特殊情况下,法的可预见性并不意味着个人能够预见具体的截取时间。但为了防止监控的滥用,法的可预见性要求国内法具备足够的透明度,即应当对公民在何种情形和条件下会被监控做出明确的规定。①

1978 年"克拉斯案"中,欧洲人权法院解释了合法性中的合目的性。欧洲人权法院在该案中首先确认公权力对公民的监控构成对隐私的侵犯。在进一步确认此种侵犯是否属于《欧洲人权公约》第 8 条第 2 款中的例外情况时,②欧洲人权法院重点考察了《德国监控法案》的合目的性。G10 中规定监控实施的目的——"避免对自由民主的宪法秩序、联邦或土地的存在或安全和驻扎在该国的(盟军)武装部队的安全构成的紧急危险"——被认定与《欧洲人权公约》第 8 条第 2 款中规定的维护国家安全或阻止混乱的目的一致。主权国家在平衡通过秘密监视保卫国家安全和尊重个人隐私生活的利益时有较大的裁量权,而仅就"克拉斯案"中被诉监控的目的来看,对德国公民隐私的干涉不含不合法成分。③

(二)"大规模"监控的合法性

确认了监控本身的合法性后,第二个问题便是监控方式的合法性。监控方式的范畴由两个变量控制:被监控对象的范围和监控的目的。这两个变量其实属于实施监控的有权机关的裁量权范畴及其行使方式。

在"韦伯与萨拉维亚案"之前,监控的对象基本特定并受到严格的限制,限于已有充分证据证明其为可能实施了某些严重犯罪的人及其近亲属,这种监控手段又被称为"个人监控"。④ 在"韦伯与萨拉维亚案"中,德国政府采取的是战略监控,目的是识别和避免针对联邦德国的严重威胁,因此其特点在于对信息的收集和存储规模为批量而非个别。在确认战略监控在德国有国内法依据并且可获得后,欧洲人权法院重点考察了 G10 是否具有可预测性。G10 规定监控的对象是通过无线电或卫星进行国际电话通信的人,如果目的是为阻止针对德国的武装冲突,监控对象可以扩大到使用固定电话通话的人。而且被监控对象必须在对话中使用了有关关键词的个人,此类关键词足以引发针对 G10 法案中第 3 节(1)1-6 条中列出的罪行的调查。欧洲人权法院认为,这满足了可预测性的最低要求。⑤ 然而在 2016 年的"萨博和维西案"中,匈牙利依据本国 CCVII 法案(又称警察法案)成立的反恐怖主义工作组(TEK)可以拦截的对象范

① Weber and Saravia v. Germany, ECtHR Decision of 29 June 2006, para. 93.
② European Convention on Human Rights, Article 8(2).
③ Klass and Others v. Germany, ECtHR Judgment of 6 September 1978, para. 49.
④ Roman Zakharov v. Russia, ECtHR Judgment of 4 Decemeber 2015, para. 171.
⑤ Weber and Saravia v. Germany, para. 96.

围较为模糊,除具体的特定对象之外还包括“一系列人员”。欧洲人权法院认为,匈牙利缺乏在实践中对“一系列人员”概念的解释,也缺乏对该“一系列人员”与防止任何恐怖主义威胁之间的实际或假定关系的证明,因此,匈牙利政府的行政裁量权太过宽泛,无法对公民在何时可能会被监控给予明确的指示。①

在考察大规模监控是否合目的时,欧洲法院要求所针对的犯罪必须是严重犯罪,但何为严重犯罪由成员国国内法加以规定。② 欧洲人权法院沿用了“克拉斯案”中的标准,即国家对于平衡国家安全和个人隐私享有广泛的裁量权,前提是不能以保卫民主社会的名义损害民主的根基。在“韦伯与萨拉维亚案”中,欧洲人权法院发现,继“克拉斯案”后,德国重新修订了 G10 法案,其中涉及可被监控的罪行从仅阻止“针对德国的武装冲突”扩展到了一些其他的严重罪行,但是,为阻止这些罪行的监控仍然受到严格的条件限制——必须是 G10 第 3 节(1)1-6 条明确列出的、会对社会造成威胁的严重罪行。因此,欧洲人权法院认为此种监控并未超出主权国家的裁量权。在 2015 年的“罗曼·扎哈罗夫案”中,欧洲人权法院再次指出,一国法律不必详细列出具体的罪名,充分说明犯罪的性质满足了一国法律的可预测性。③ 在 2018 年的“老大哥案”中,考虑到当前许多欧盟成员国面临的威胁(包括全球恐怖主义和其他严重罪行,如毒品运输、人口贩卖、儿童性剥削和网络犯罪),网络技术的发达让恐怖主义分子和犯罪分子更容易逃脱侦查,欧洲人权法院承认国家有权实施大规模监控以识别这些迄今为止对国家安全构成威胁的犯罪。④

(三)“跨境”监控的合法性

最早涉及监控跨境性质的案件是“韦伯与萨拉维亚案”。欧洲人权法院在此案中否定了通过卫星或广播的通信信息的跨境性质,指出如果截取信号的站点坐落在实施监控的国家领土内,即使通信本身是一通国际电话,截取通信信息也不构成对别国主权的侵犯。⑤ 跨越欧盟境内外的案例则来自 2015 年的“施雷姆斯 I 案”。在该案中,欧盟法对于请求数据的第三方主体应当承担的义务态度坚决,明确了为安全目的的传输请求也不能免责:根据欧盟《第 95/46/EC 号保护个人在数据处理和自动移动中权

① Szabó and Vissy v. Hungary, ECtHR Judgment of 12 January 2016, para. 38.
② Joined Cases C-293/12 and C-594/12 Digital Rights Ireland Ltd., E.C.J. Judgment of 8 April 2014, para. 16.
③ Roman Zakharov v. Russia, para. 244.
④ Big Brother Watch and Others v. the United Kingdom, para. 314.
⑤ Weber and Saravia v. Germany, para. 88.

利的指令》,请求数据的第三方主体[①]必须为数据提供与欧盟相同水平的保护。[②] 2000 年,欧委会根据上述指令通过了决定 2000/520,确认了美国提供的安全港保护框架。在本案的审查中发现安全港规则仅对自愿加入的美国企业有约束力,而美国政府以“国家安全、公共利益和执法要求”为由提出的数据传输请求不受该规则约束。因此,欧洲法院认定美国未对欧盟的数据提供相同水平保护,而做出确认安全港原则的决定 2000/520 也被宣布无效。[③]

在 2018 年的“老大哥案”中,欧洲人权法院第一次处理监控数据的跨境分享系统,并确立了以“控制”为条件的合法性检验原则。本案中的数据分享发生在英国的情报部门(IPA)和美国的国家安全局(NSA)之间。欧洲人权法院将分享的数据分为 IPA 请求 NSA 拦截的数据和 IPA 要求 NSA 传输的已拦截数据。欧洲人权法院指出,这些数据的拦截主体都是 NSA,拦截行为都在美国的全面控制之下,而英国对于拦截行为没有控制,也没有帮助,因此英国不对拦截行为承担责任。[④] 这意味着欧盟默认了跨境数据分享系统原则上并不违法。

综上,从欧洲两法院的案例中可以看出,在跨境的大规模数据监控中,只要大规模监控的行为、进行的方式和数据的跨境传输拥有国内法依据,具有可获得性和可预见性,并且对于保护国家安全、公共安全等目的来说是必要的,其本身就不构成违法。

二 制衡:为保护隐私约束监控机关的裁量权

(一)内部:监控机关应遵循的数据处理标准

在确认大规模数据监控不违法后,欧盟对所得数据的处理提出了更高的要求。GDPR 第 6 条第 4 款指出:“在不需要数据主体同意的数据处理中,数据处理应当是对于第 23 条(1)的目的而言必要且成比例。”[⑤]第 23 条(1)中所列目的包含但不限于国家安全,两法院也遵循此逻辑,在判例中进一步诠释了何为“必要且成比例”。欧洲人权法院在早期有关刑事监控的判例法中制定了四项最低的保障标准:监控时长的限制;审查、使用和保留所获数据应遵循的程序;与第三方交流数据时应采取的预防措

① 此处的第三方是针对数据的所有者和持有者以外的第三方。如公安机关向储存了用户信息的互联网公司请求调取数据,此时公安机关就是第三方。

② Case C-362/14 Schrems, E.C.J. Judgment of 6 October 2015, para. 4.

③ Ibid., paras. 84-86.

④ Big Brother Watch and Others v. the United Kingdom, paras. 416-421.

⑤ General Data Peotection Regulation, https://gdpr-info.eu/, last accessed on 30 April 2020.

施;在何种情况下可能或必须删除或销毁已拦截数据。① 随后,欧洲人权法院和欧洲法院分别在 2015 年的“罗曼·扎哈罗夫案”②和“爱尔兰数字权利有限公司案”③中确认了上述标准也适用于以国家安全为由而进行的监控。

(1)监控时长。监控时长指的是监控行为实际进行的时长。两法院都未对监控时长的绝对值做限制。2010 年的“肯尼迪案”中,欧洲人权法院认为对监控时长的限制包含两方面内容:监控初次启动的时长和申请延续的条件,而成员国可以自主决定上述两项内容。只要规定足够明确,延续理由和程序足够清晰,就满足了法的可预见性。④ 这意味着在符合一定条件的情况下,监控可以无限期延续。而欧洲法院未讨论过这一问题。

(2)监控数据的审查、使用和保留。数据的审查是指对监控得来的所有数据以某种标准进行筛选,审查和使用的步骤往往紧密相连。欧洲人权法院在“韦伯与萨拉维亚案”中认可了关键词审查法,条件是这些关键词必须与国家想要通过监控实现的目的紧密相关,且国家仅使用筛选后的数据。⑤ 在“老大哥案”中,欧洲人权法院指出,关键词的具体内容不必公开,否则将破坏原本的活动,使监控失去意义。另外,欧洲人权法院对本案中英国当局所使用的电脑自动过滤系统提出了更高的要求。筛选后留下的数据将形成索引,经英国外交部国务大臣证明必要性后交由独立的数据分析师处理。由于索引表中列出的词汇类别用语过于笼统,包括但不限于“恐怖组织、恐怖分子和攻击计划”等,该筛选系统最终被认定具有相当大的滥用风险。⑥

数据保留中的两个关键标准为保留的绝对时长和数据的区分原则。欧盟指令 2006/24 要求成员国保留数据的时长要限制在 6 个月到两年之内。⑦ 而在 2008 年的“S.和马珀案”中,欧洲人权法院直接判定三十年的数据保留过长,“任何声称在新技术开发中起先锋作用的国家都应为实现适当的平衡负有特殊责任”,过长时间的保留体现了公共利益和私人利益的不平衡。⑧ 体现区分原则的标志性案件是爱尔兰数字

① Weber and Saravia v. Germany, para. 95.
② Roman Zakharov v. Russia, paras. 227-238.
③ Joined Cases C-293/12 and C-594/12 Digital Rights Ireland Ltd, paras. 46-55.
④ Kennedy v. the United Kingdom, para. 161.
⑤ Weber and Saravia v. Germany, para. 32.
⑥ Big Brother Watch and Others v. the United Kingdom, paras. 328-347.
⑦ Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC, https://eur-lex.europa.eu/legal-content/EN/TXT/? uri=celex%3A32006L0024, last accessed on 30 April 2020.
⑧ S. and Marper v. United Kingdom, paras. 105-125.

权利有限公司一案。在该案中,爱尔兰数字权利有限公司也采用了电脑自动筛选系统,保留了与固定电话、移动电话、互联网访问、电子邮件和网络电话有关的所有流量数据。这种处理覆盖了所有电子通信方式以及所有订阅用户和注册用户。与欧洲人权法院相同,欧洲法院指出,在电脑自动筛选系统下,对于基本权利的保障更应当加强,因为数据被非法访问的风险更大。事实上仅仅是涉及通信的元数据,如指令2006/24 第 5 条中罗列的可识别通信源头的必要数据、可识别通信进行的地点的必要数据等才可以得到保留,凡是会暴露通信内容的数据一概不允许保留,而爱尔兰数字权利有限公司恰恰相反的做法构成对隐私的严重侵犯。① 争议指令——欧盟 2006/24 指令以笼统的方式要求对所有的数据统一保留 6 个月,未做任何区分;亦没有说明保留期限的确定必须基于客观标准,最终被判决超越了比例要求的限制。②

(3)与第三方交流数据时应采取的预防措施。这里的第三方指的是监控机关与本国其他机关进一步分享其所收集的数据。这一过程中的预防措施的审查集中在欧洲人权法院的案例中。从“罗曼·扎哈罗夫案”可看出,虽然对预防措施没有进一步的指导标准,但越详细则越容易得到欧洲人权法院的肯定。俄罗斯的《行动搜索活动法》《刑事诉讼法》和《国家秘密法》共同体现出,官员访问数据存在不同阶段的限制:数据只能向具有相应安全许可级别、真正需要数据履行职责的国家官员披露;明确列出披露数据的必要的数量和步骤以及不具有权限的官员;对于将包含刑事犯罪信息的数据传送给检察机关的条件和程序必须满足安全存储以及在刑事诉讼中用作证据的条件等。③ 在“老大哥案”中,英国要求访问数据仅限于“授权用途”所必要的最低限度:材料或数据被披露或提供的人数、披露或提供该材料或数据的程度、资料或数据被复制的程度和复印的次数都应该符合比例原则。该案对于授权的情况也进行了较为详细的列举:上述数据对于授权目的有必要或有可能继续的,协助执行外交大臣的任何拦截职能,协助执行截取通信事务专员或调查权力法庭(IPT)的任何职能,确保进行刑事诉讼的需要或为履行根据公共档案立法加诸任何人的任何职责。④ 欧洲人权法院对于授权目的中“可能成为必要”表示了一定程度的担忧。“如果某数据‘可能成为必要’,则可能被视为‘必要’。英国的立法对于何种情况下数据对于授权的目的‘可能成为必要’缺乏解释,实践中有关当局访问数据的裁量权可能过于广泛。”⑤即便

① Joined Cases C-293/12 and C-594/12 Digital Rights Ireland Ltd, para. 55.
② Ibid., paras. 63-65.
③ Roman Zakharov v. Russia, paras. 54-64.
④ Big Brother Watch and Others v. the United Kingdom, paras. 365-369.
⑤ Ibid.

如此,欧洲人权法院仍认为这符合最低保障限度,未将“可能成为必要”视为对隐私的不合法侵犯。

(4)数据的销毁。欧洲人权法院和欧洲法院一致认为,一旦数据没有保留的必要,就应当立即删除。在“罗曼·扎哈罗夫案”中,欧洲人权法院认为,明确销毁被截取数据的程序可以最大限度地减少未经授权的访问或披露的风险。无关数据应当立即销毁,而俄罗斯的国内法要求所有的数据都自动存储 6 个月是不合理的。① 在“老大哥案”中,英国的《调查权力法案》(RIPA)中规定的通信内容保留的时长从 30 天到 1 年不等,通信数据保留时长从 6 个月到 1 年不等,虽然各个机构对“何为合理的数据保留”的规定不同,但都说明了原因,且有 IPT 定期审查有关数据是否严格根据国内法和 GDPR 第 8 条及时得到删除。② 欧洲法院在“沃森案”中对于和政府合作的电子通信服务商也提出了类似的要求。基于用户通信数据包括实时的交通和位置信息,考虑到这类数据的敏感性以及非法访问该数据的风险,电子通信服务商必须确保特别高水平的保护,以确保该数据的完整性和机密性,欧洲法院要求此类数据只能保留在欧盟内部,并在数据保留期结束时对其予以不可逆转地立即销毁。③

(二)外部:确保有效的司法监督或救济

(1)有效的司法监督

目前存在的三种监督模式分别是一般司法监督、专门法院监督和专门人员监督。欧洲人权法院在“罗曼·扎哈罗夫案”中将一般司法监督中法院的职权分为三个关键步骤:事前授权、实施中监督和事后监督。④ 相比事前授权,实施中监督和事后监督更为重要。如在 2016 年的“萨博和维西案”中,匈牙利未要求监控的实施需要获得事前的司法授权,也没有明确规定续签监视令的频率,因此,欧洲人权法院要求未经司法事前授权的监视措施必须接受事后的司法审查。⑤ 专门法院监督存在于“肯尼迪案”中英国当局设立的独立于立法和行政机构的调查权力法庭,任何怀疑自己被监控的人都可以向 IPT 提出申请,IPT 可以撤销监控中任何的监听命令,要求销毁被监听的材料。⑥ 专门人员的监督较为特殊,最为典型的是“肯尼迪案”中英国根据 RIPA 设立的通信监听专员,必须是担任或曾担任高级司法职务的人,其地位独立于立法和行政机

① Roman Zakharov v. Russia, paras. 254-256.
② Big Brother Watch and Others v. the United Kingdom, paras. 370-374.
③ Case C-698/15 Tele2 Sverige, E.C.J. Judgment of 21 Decemebr 2016, para. 122.
④ Roman Zakharov v. Russia, paras. 272-285.
⑤ Szabó and Vissy v. Hungary, paras. 85-89.
⑥ Kennedy v. the United Kingdom, ECtHR Judgment of 18 May 2010, paras. 166-170.

构,每年向首相提交报告,报告内容包括详细审查立法运作中发生的任何错误,如授权和处理截取令的程序以及信息截取的处理、销毁程序等存在的问题,并对外公开(除了不公开的附件以外)。除了监控机构和外交大臣对于监听令和材料的定期审核,专员负责监督监控制度的总体运作和特殊案件中的监听授权问题。①

无论监督的具体模式如何,监督的有效性要求其具备独立性、公开性和职权相当性。在"克拉斯案"中,欧洲人权法院就曾指出,监督不一定非要司法机关行使,也可由与监控机关相独立的非司法机构行使,前提是该机构不违背公约,并被授予了足够的权力,具备足够的能力进行有效且持续的控制。② 独立性要求监督的机构与监控的机构来自不同的权力机关。"罗曼·扎哈罗夫案"中俄罗斯国内法规定监控的监督由检察官进行。由于监督监控与授权监控的检察官都来自同一个检察官办公室,欧洲人权法院认为这种监督机制缺乏独立性。③ "萨博和维西案"中授权监控的司法部长是由警力系统下的一个战略部门反恐怖主义工作组的行政长官任命,该部门对内政事务大臣负责,主要职权是使用武力打击恐怖主义。欧洲人权法院认为,这样的监督属于行政性质,而不足以确保监控中的裁量权受到严格合理的限制。④ 公开性要求监督机构的资料向社会公开并接受公众的监督。"罗曼·扎哈罗夫案"中的检察官虽然每两年向检察长办公室提交一次详细的检查报告,但报告文件都是不公布的机密文件,公众无从知晓。⑤ "萨博和维西案"中的监督也是基于相同的原因被宣布无效。⑥ 职权相当性要求监督机构被授予的职权要使其足以实施完整的监督,这包括监督机构可以获得所有与监控有关的文件,并且可以在发现监控不合法后采取相应的措施。这些措施应当包括删除通信数据、有权做出要求当局赔偿和任何其他适当的命令、有权要求当局撤销或取消任何监听令和销毁任何记录等。"罗曼·扎哈罗夫案"中俄罗斯国内法不允许检察官访问安全部门卧底人员和他们使用的方法和手段的信息,欧洲人权法院因此认定其监督存在漏洞。同样在本案中,欧洲人权法院认定俄罗斯缺乏对检察官销毁数据权力的明确规定而宣布其监督不力。⑦

除对监督机关的要求外,有效的监督还要求监控机构保留记录,以确保监督机关能够有效获取所进行的监控活动的详细信息。在"罗曼·扎哈罗夫案"中,原本授权

① Kennedy v. the United Kingdom, paras. 166-170.
② Klass and Others v. Germany, para. 56.
③ Roman Zakharov v. Russia, para. 278.
④ Szabó and Vissy v. Hungary, para. 75.
⑤ Roman Zakharov v. Russia, No.47143/06, para. 283.
⑥ Szabó and Vissy v. Hungary, para. 82.
⑦ Roman Zakharov v. Russia, para. 284.

进行监控的机关是俄罗斯的法院,但在实践中,行政机关对于“紧急状态”享有过分宽泛的自由裁量权,司法审查的范围非常有限,俄罗斯国内法不允许法院审查包含有关卧底特工或警方线人的信息或有关作战搜寻措施的组织和策略的信息的材料。因此,欧洲人权法院要求俄罗斯对“紧急状态”进一步做出限定。①

(2)有效的司法救济

为检验司法救济的有效性,欧洲人权法院曾在“克拉斯案”中确立的唯一标准是政府的告知义务,即要求实施监控的公权力机关向被监控人告知监控的实施,以便其寻求司法救济。但是考虑到有时候告知可能会损害秘密监视的原本意图,欧洲人权法院要求告知应当在监控之后、不损害监控目的的情况下立即做出。② 在“肯尼迪案”中,欧洲人权法院发现,即使在政府不告知被监控人监控行为存在的情况下,司法救济的有效性也可以被满足——任何怀疑自己可能被监控的人都可以向专门法院 IPT 起诉。IPT 受理监控案件的条件不包括被监控人被告知受到监控实际行为的存在,且 IPT 可以为被监控人提供有关监控的信息。③ 此后,司法救济的有效性标准变为,是否告知或是否存在有效途径提供有关的监控信息。在“罗曼·扎哈罗夫案”中,原告指控俄罗斯政府的监控行为一直处于秘密进行的状态,被监控人自始至终甚至无从得知自己的隐私权被侵犯,除非政府将监控所获得的数据作为证据对被监控者提起刑事诉讼。虽然俄罗斯为监控提供了四种司法程序的救济——上诉、对于授权监控的司法决定的申诉、基于本国的《刑事程序法典》(CCrP)的司法审查和基于《司法审查法案》《民事程序法典》(CCP)的司法审查,但上述每一种司法救济都要求被监控人掌握监控通信的证据。欧洲人权法院的审查发现,与监听有关的很多证据都被俄国的司法机关视为国家机密,而不对公众披露。被监控的人所能获取的有关自己被监控情况的信息非常有限,因此这些人也无法获得司法救济。④

然而,司法救济本身的必要性却不是很明确。在 2018 年的“司法中心诉瑞典案”中,尽管瑞典法律规定了多种救济途径,包括请求根据瑞典《信号情报法案》设立的外国情报调查员调查,向情报主管机关(FRA)申诉等,但没有一种救济途径属于司法救济。然而欧洲人权法院却在判决中写道:“多种救济的集合尽管没有为申诉提供完全、公开的机会,但也为信号情报体制自身构成了抽象的压力,因此在当前情况下也应

① Roman Zakharov v. Russia, paras. 268-271.
② Klass and Others v. Germany, para. 19.
③ Kennedy v. the United Kingdom, para. 167.
④ Roman Zakharov v. Russia, paras. 293-301.

当认为已满足条件。”欧洲人权法院认为,此时应当更依赖早前阶段的监督——如外国情报法院(FIC)的司法审查和其他多个机关广泛、公开的监督。①

三 挑战:成员国监控的权力扩张和保护水平的模糊

欧洲人权法院承认,成员国“为国家安全、公共安全或国家的经济福利的利益,为防止混乱或者犯罪、为保护健康或道德、或为保护他人的权利与自由”,通过秘密监控措施干涉公民的隐私权时,对于所采取措施的选择享有一定程度的裁量权。这样的裁量权以不损害民主的本质为限,即此种情况下对于隐私的侵犯必须“为民主社会所必要”。② 而从欧洲人权法院循序渐进地为大规模跨境监控正名的过程中不难看出,欧洲国家普遍陷入一种对于打击恐怖主义、保护国家安全的焦虑中,欧洲人权法院似乎也在逐渐放宽对裁量权的审核标准。

(一)如何应对扩张解释安全概念的趋势

在最初的“克拉斯案”中,欧洲人权法院支持为“避免对自由民主的宪法秩序、联邦或土地的存在或安全和驻扎在该国的(盟军)武装部队的安全构成的紧急危险”这一目的实施监控。随着监控的目的逐渐增多,安全的定义逐渐变得广泛,监控的规模、所涉人群范围也逐渐扩大。在“肯尼迪案”中,英国 RIPA 法案未对“国家安全”一词做出定义,仅监听通信专员在年度报告中指出:“国家安全威胁”是“威胁国家的安全和存亡,用政治、工业或暴力手段削弱或推翻议会民主”。③ 事实上在几乎所有监控案件中,凡是以“国家安全、公共安全”为目的的监控,都得到了欧洲人权法院的肯定,对于合目的性的检验便在此止步,更多的只是审查后期程序性的保障是否得到满足。不仅是在监控的案件中,近年来国际社会普遍存在着泛安全化的倾向,原本与个人基本权利存在张力的“国家安全”如今被纳入强制性人权的语境中,强调对潜在受害者的保护而非对国家自身行为的限制。④ 也许通过监控手段在多大程度上实现对安全的保护,暂时无法用实证研究得出结论,但确实要警惕这种意识形态上的怀疑主义会给民主社会造成的影响。⑤

① Centrum för rättvisa v. Sweden, ECtHR Judgment of 19 June 2018, paras. 176-178.

② Big Brother Watch and Others v. the United Kingdom, para. 333.

③ Kennedy v. the United Kingdom, para. 33.

④ Elizabeth Stoycheff, et. al., “Online Surveillance's Effect on Support for Other Extraordinary Measures to Prevent Terrorism,” *Mass Communication & Society*, Vol.20, No.6, 2017, pp.784-799.

⑤ Lazarus Liora and Benjamin J. Goold, “Security and Human Rights: Finding a Language of Resilience and Inclusion,” in Lazarus Liora and Benjamin J. Goold, eds., *Security and Human Rights*, Hart Publishing, 2019, pp.1-21.

(二)是否更新程序性保障标准

法官高斯科洛(Pauliine Koskelo)和图尔科维奇(Ksenija Turković)在“老大哥案”的意见中写道:“无针对性的监控存在着巨大的滥用风险,而欧洲人权法院既往案例建立起来的标准(即对监控机关的约束和有效的监督、救济等)难以形成有力的约束……恐怖主义兴起之时,公权力以各种理由约束个人权利与自由的证据也日益增加……”在认同英国违反了《欧洲人权公约》的同时,反对意见中指出,大规模跨境监控仍使用韦伯与萨拉维亚案件建立的六个最低标准的正当性值得怀疑。韦伯与萨拉维亚案的判决迄今已逾 10 年,且该案所涉监控类型为有针对性的监控。信息技术的革新、国家对公共安全价值保护的侧重,都使得监控手段对于个人隐私的入侵不可逆转。原告曾要求欧洲人权法院更新审查标准,如要求监控的条件为掌握合理怀疑的确凿证据、要求监听令需独立的司法事先授权以及对于被监控对象的事后告知等。欧洲人权法院认为,想当然地假定大规模监控一定构成对隐私的更大侵犯是错误的,尽管增添新的标准确实将在某些情形下提高对隐私的保障,但由于证据要求和事后告知都属于成员国的自裁权范畴内的事务,而司法授权本就与大规模监控的有效运行不兼容且不足以构成制约等原因,将它们添加为最低保障是不必要的。①

欧洲人权法院的论证存在矛盾之处。首先,为什么监控可以在没有确凿证据的情况下启动,这一点有待解释。大规模监控实际上相当于在虚拟的信息世界中营造出一种“圆形监狱”的氛围——每个房间完全向外敞开,光线充足,其中每个个体的行为永远可见。该建筑模型的作用就在于使权力以永远可见而不可证实的状态存在,使所有犯人处于不变的可被监控状态。② 而将这一原本用于惩治犯罪的监狱模型扩大到全社会有些许“有罪推定”的意味,不符合法治理念。其次,司法事先授权和事后告知的重要性没有引起足够的重视。依照欧洲人权法院的检验程序,事先司法授权和事后告知都不必要,监控机制实际运行的效果是检验是否存在权力制衡、是否存在滥用的确凿证据。权力的制衡要求独立于行政机关的监督或者救济,但欧洲人权法院对于司法监督和司法救济的关系态度不明,在监督相对强一些的案件中便忽略了司法救济的重要性,反之亦然。老大哥案中的部分反对意见也指出,欧洲人权法院认为,无论是监督还是救济,都不足以保障权力不被滥用,因此这两者都不能作为最低标准。这样的推

① Big Brother Watch and Others v. the United Kingdom, paras. 316-320.

② [美]理查德·霍金斯、[美]杰弗里·P·阿尔伯特:《美国监狱制度——刑罚与正义》,孙晓雳、林遐译,中国人民公安大学出版社 1991 年版,第 38-39 页。

理是难以让人信服的。① 正是因为监督和救济可能都无法阻止权力被滥用,欧洲人权法院才应当仔细审视当前已有程序性标准存在的漏洞,承担起建立一套更完整的制衡监控机制的人权法框架的任务。

(三)是否厘清《欧洲基本权利宪章》和《欧洲人权公约》的关系

在《欧洲基本权利宪章》和《欧洲人权公约》之间,前者实际上依赖后者的判例法。欧洲法院在其处理的第一个监控案件"爱尔兰数字权利有限公司案"中指出,对隐私进行干涉的合法目的是为了打击"严重犯罪"。至于如何在公权力实施监控的过程中保证严格必要的合目的性,由于缺乏可参考的相关案例,欧洲法院在实际的论证中大量引用了欧洲人权法院的案例来说明问题。虽然该案也呼吁欧盟做出进一步清晰明确的立法,②但随后其对于公权力监控领域的立法进展并不显著,欧洲法院却要《欧洲人权公约》与《欧洲基本权利宪章》之间划清界限。如在"沃森案"中,原告曾请求欧洲法院对于《欧洲基本权利宪章》第 7 条和第 8 条的保护是否高于《欧洲人权公约》,两者有什么区别做出解释。欧洲法院指出,虽然《欧洲人权公约》是构成欧盟法的基本原则,但由于欧盟还未正式加入《欧洲人权公约》,《欧洲人权公约》不能算作欧盟法体系的一部分,二者对隐私权的保护范畴没有可比性,因此在欧洲法院的案子中仅以《欧洲基本权利宪章》为法律依据。③

与此同时,在 2020 年 7 月的"施雷姆斯 II 案"中,原审法院再次询问欧洲法院《一般数据保护条例》要求的同等水平保护是否要与欧盟法(尤其是《欧洲基本权利宪章》《欧洲人权公约》和成员国国内法)相一致时,欧洲法院承认《一般数据保护条例》框架下保护的信息权的重要价值就是隐私权,在这一点上应当将《一般数据保护条例》的保护水平根据《欧洲基本权利宪章》规定的基本权利来理解。④ 由此可见,欧洲法院认为,《一般数据保护条例》对数据传输时涉及隐私权的保护应当与《欧洲基本权利宪章》相同。欧洲法院要求请求数据的第三方提供与欧盟内部同等水平的保护,但欧洲法院审理案件参考的法律依据——无论是"施雷姆斯 I 案"及之前案件中的《欧洲基本权利宪章》和各种欧盟指令等,还是"施雷姆斯 II 案"中的《一般数据保护条例》,都未曾对"同等水平保护"这一表述做出过进一步的解释。而《一般数据保护条例》的立法说明第 41 条规定数据处理所遵循的法律基础或方法要符合欧洲法院和欧洲人权法

① Big Brother Watch and Others v. the United Kingdom, para. 25.
② Joined Cases C-293/12 and C-594/12 Digital Rights Ireland Ltd, paras. 35, 54.
③ Case C-698/15 Tele2 Sverige, paras. 126-128.
④ Case C-311/18 Schrems, E.C.J. Judgment of 16 July 2020, para. 101.

院的案例法,《一般数据保护条例》的第 46 条第 1 款中规定数据的处理要有“适当的保障,可执行的权利和有效的法律救济”。① 由此可见,《一般数据保护条例》的标准在很大程度上也都来源于《欧洲人权公约》。如果正如“沃森案”的判决中所言,“《欧洲基本权利宪章》的第 52 条第 3 款旨在确保《欧洲基本权利宪章》与《欧洲人权公约》之间必要的一致性”,②即《欧洲人权公约》的审查标准其实与欧洲法院实际参考的审查标准一致,那么欧洲法院就不该多次在判决中“澄清”,试图撇清《欧洲人权公约》对其审理的监控案件的影响,让第三方国家缺乏参照标准;而如果“《欧洲基本权利宪章》的第 52 条第 3 款并不排除欧盟法提供比《欧洲人权公约》更为广泛的保护”,③即欧洲人权法院的审查标准与欧洲法院不一致,那欧洲法院提出的“提供与欧盟内部相同水平保护”的要求就让第三方国家再一次无法可循——《欧洲基本权利宪章》和《一般数据保护条例》都不存在与“相同水平保护”的条款,而真正为欧盟内部保护水平制定了指导框架的欧洲人权法院的案例却无适用之地。

(四)是否明确个人信息权和隐私权的保护标准不同

在欧洲法院审查的涉及公权力监控的案件中(“爱尔兰数字权利有限公司案”“沃森案”“施雷姆斯 I 案”“施雷姆斯 II 案”),前三个都同时援引了《欧洲基本权利宪章》的第 7 条(隐私权)和第 8 条(个人数据权),第四个案子援引的是《一般数据保护条例》的第 46 条第 2 款,但也在判决中说明这条本质上要保护的是个人隐私权以及基本权利和自由。④ 在涉及所判断的具体权利时,欧洲法院的用词包括“隐私权和信息权”“隐私权和基本权利与自由”以及“数据处理过程中的隐私权”等等。由此引发的问题是:欧洲法院保护数据的要求⑤之所以与欧洲人权法院不同,是否出于其对个人信息权利和隐私权的双重保护?是否所有涉及公权力机关监控的案件都涉及对个人信息权和隐私权的同时侵犯?如果不是,是否有必要在监控的案件中明确隐私权和个人信息权的区别?

个人信息权与隐私权的区别与联系一直是国内外法学家热烈讨论的重点。国内大部分学者认为,个人信息关注是否能够根据信息识别特定个体,隐私强调干涉对私

① Case C-311/18 Schrems, para. 14.
② Case C-698/15 Tele2 Sverige, para. 129.
③ Ibid.
④ Case C-311/18 Schrems, para. 16.
⑤ 例如,“施雷姆斯 I 案”中要求欧盟成员国加强对第三方的审查义务,尤其是明确规定当事人如认为第三方保护力度不足时有权对监督机关提起诉讼;“施雷姆斯 II 案”中明确监督机关有权在认为第三方保护力度不足时暂停或终止数据的传输等。

人领域的影响程度。① 一方面,个人信息的重要价值之一就是隐私,但是个人信息也包括其他独立于隐私的价值,如信息安全、信息质量等,另有国外学者认为尊严也是个人信息权的独特价值之一。② 另一方面,有很多个人信息由于不具有隐私性质,因此不属于隐私权的保护范围。从欧盟将《欧洲基本权利宪章》的第 8 条——个人信息权单独作为一项基本权利来看,欧盟承认个人信息权具有独立于隐私权保护的价值。随着《一般数据保护条例》的出台,欧盟的数据保护体系已经基本成熟,但在承认个人信息权的独立价值时,欧洲法院对于个人信息权的独立性分析有些不足。到底政府的哪些行为是对隐私权的侵犯,哪些行为是对个人信息权的侵犯?欧洲法院在"爱尔兰数字权利有限公司案"中指出,本案存在对个人信息权的干涉,因为"它涉及个人信息的处理",似乎意味着所有涉及个人信息处理的行为都必然引起对个人信息权的侵犯。③在"施雷姆斯 II 案"中强调《一般数据保护条例》第 46 条第 2 款与隐私权的保护息息相关,更让隐私权和个人信息权之间的关系模糊不清。《一般数据保护条例》在个人信息保护领域的贡献主要在于风险等级差异化管理的方案,明确了信息的控制者和处理者各自的法定义务,但也缺乏详细充分的说明,④仅仅采用列举式无法勾勒出信息侵权区别于隐私侵权的基本特征。如果想要"巩固"个人信息权的独立地位,欧洲法院可能要在日后的判决中进一步明确个人信息权和隐私权的具体侵权方式分别有哪些,以及分别对应的保护标准。

四 借鉴与反思

欧盟规制大规模数据监控主要通过对监控机关进行限制、要求司法机关提供救济、监督机关独立监督等行为展开,涉及行政管理、刑事司法和情报法等各个领域法律的协调配合。本文分析得出的结论是,欧盟个人信息的隐私保护框架虽然并不尽善尽美,但就全球范围的相关规则而言已是相对前卫和成熟,⑤且可为中国进一步细化和完善国内相关立法提供借鉴。

---

① 朱悦:《大数据背景下的个人信息法律保护研究综述》,载《图书馆论坛》,2020 年第 3 期,第 5 页。

② Maria Tzanou, *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance*, Hart Publishing, 2017, p.31.

③ Ibid., p.59.

④ 苏彦、王炳智:《跨境数据时代个人信息安全的立法保护》,载《网络空间安全》,2019 年第 5 期,第 31-32 页。

⑤ 田旭:《欧盟个人数据保护法的全球影响成因与启示》,载《江西财经大学学报》,2020 年第 4 期,第 142 页。

(一)理性平衡隐私与公共安全

隐私权和个人信息权的保护近年来在国内日益受到重视,在2020年出台的两部法案中均有体现,其中一部为2020年7月3日出台的《中华人民共和国数据安全法(草案)》(以下简称《草案》)。《草案》第三条所指的数据是任何以电子或非电子形式对信息的记录,①个人的信息自然也囊括其中。其总则中的第八条规定:数据活动的开展必须遵守法律、行政法规……不得危害国家安全、公共利益,不得损害公民、组织的合法利益。② 隐私权是公民的合法权益之一,因此《草案》也对开展数据活动的主体提出了保护公民隐私的要求。而在这一条总体原则性规定的指导下,第二十九条又进一步规定:法律、行政法规对收集、使用数据的目的、范围是有规定的,应当在法律、行政法规规定的目的和范围内收集、使用数据,不得超过必要的限度。③ 而2020年10月21日公布的《个人信息保护法(草案)征求意见》(以下简称《征求意见》)更是将对个人信息的保护提升到了全新的高度。如《征求意见》第六条便规定处理个人信息应当限于事先处理目的的最小范围,不得进行与处理目的无关的个人信息处理;④第七条规定处理个人信息应当遵循公开、透明的原则,明示个人信息处理规则。⑤《草案》确立了数据分级分类管理以及风险评估、监测预警和应急处置等数据安全管理各项基本制度,明确开展数据活动的组织、个人的数据安全保护义务,全面地落实了数据安全保护责任。而《征求意见》则充分体现了处理个人信息中应当遵守的必要原则和比例原则。如德沃金所言,原则的存在不是因为它合乎需要的经济、政治或社会形式,而是因为它是公平、正义的要求。即使作为原则存在的法律存在模糊性和开放性,它依然可以弥补成文规则的不足,为司法能动性划定大致范围。⑥

另一方面要清晰地认识到,个人隐私与公共安全都是需要保护的重要法益,二者之中任何一个都不可一边倒地致使另一个完全减损,因此需要考虑的是在具体的实践中如何权衡的问题。隐私权或个人信息权并不是不可减损的绝对权利,在合法合理、满足了必要性及比例性条件的情况下,隐私或个人信息可以受到限制。通过上文对欧洲两法院的案例分析可知,即使在十分注重隐私和个人信息保护的欧洲,也要求在“为民主社会所必要”的情形下合法合理地对隐私进行干涉。可以看到,随着近年来

① 参见《中华人民共和国数据安全法(草案)》第3条。
② 参见《中华人民共和国数据安全法(草案)》第8条。
③ 参见《中华人民共和国数据安全法(草案)》第29条。
④ 参见《个人信息保护法(草案)征求意见》第6条。
⑤ 参见《个人信息保护法(草案)征求意见》第7条。
⑥ 参见周佑勇:《行政法基本原则研究》,法律出版社2019年版,第243-248页。

欧洲面临的恐怖主义和其他严重犯罪的风险日益增加,欧洲对于数据监控的管制逐渐放松,欧洲人权法院更是直接指出大规模数据的采集并不必然导致对于隐私更为严重的侵犯。正如《征求意见》第十三条所规定的,除了个人同意之外,为履行法定职责或法定义务所必需、为应对突发公共卫生事件等都可以是个人信息处理者合法处理个人信息的依据。① 因此,国家在注重保护个人隐私、尊重个人尊严的同时,也要承担起对整个社群的保护义务,个人的自由也是建立在自尊和尊重他人的基础之上,当面临恐怖主义犯罪、疫情暴发等危及国家存亡的情况时,社群内的成员都有义务促进公共利益,从而降低所有人所共同面对的风险。②

(二)完善个人信息对外传输的规则

个人信息对外传输规则在中国已具备一定的法律依据,如2018年出台的《国际刑事法院司法协助法》第十七条要求办案机关在执行外国司法协助请求的过程中维护当事人和其他相关人员的合法权益;③又如2015年的《中华人民共和国国家安全法》第四十三条和2018年修正的《中华人民共和国情报法》第十九条都规定国家工作机构及其工作人员应当严格依法办事,不得泄露个人信息;④从目前的《草案》来看,根据其第二条的规定,境外开展数据活动的组织和个人要对损害中华人民共和国国家安全、公共利益或者公民、组织合法权益的行为承担法律责任。⑤ 这是对境外的组织和个人开展数据活动的总体性规定。《草案》第三十三条特别强调了境外的执法机构要求调取存储于中华人民共和国境内的数据的,有关组织、个人应当向有关主管机关报告,获得批准后方可提供。⑥ 当涉及公民的隐私信息时,报告义务还不足以提供足够水平的保护。

除了向有关的主管机关报告之外,该被调取的数据还应当依据建立的安全审查制度进行审查。⑦ 例如面对非欧盟国家的数据传输请求,中国宜确立向外传输数据中隐私保护的最低标准,明确有关部门的审查责任以确保数据跨境传输中的合规操作。该审查部门应当具备必要的权力可以采取相应的手段,但如欧盟一样当即暂停或中止数据传输可能有些过于强硬,如有权警告并给予一定期限要求对方提高保护水平或许更

① 参见《个人信息保护法(草案)征求意见》第13条。

② 参见张燕:《埃博拉疫情爆发和防控中的"道德两难"和伦理反思》,载《伦理学研究》,2015年第1期,第129页。

③ 参见《国际刑事法院司法协助法》第17条。

④ 参见《中华人民共和国国家安全法》第43条,以及2018年修正的《中华人民共和国情报法》第19条。

⑤ 参见《中华人民共和国数据安全法(草案)》第2条。

⑥ 参见《中华人民共和国数据安全法(草案)》第33条。

⑦ 参见《中华人民共和国数据安全法(草案)》第33条以及第22条。

加合适。面对欧盟国家,中国国内的互联网市场各企业实力参差不齐,不宜全盘接受欧盟的数据保护标准。①

此外,《草案》第三十三条还指出,境外执法机构要求调取存储于中华人民共和国境内的数据的……中华人民共和国缔结或者参加的国际条约、协定对外国执法机构调取境内数据有规定的,依照其规定。② 如前文所述,欧盟内部的保护标准也存在模糊不清的边界。因此,根据此条款,更适宜的做法可能是加强与欧盟方面有关数据立法的交流,以在先的安全港和隐私盾规则为鉴,查漏补缺,促成对国内企业更具有可行性的、对于中国公权力机关也更友好的标准条款的签订。"施雷姆斯II案"后,欧美之间重新磋商形成的取代安全港的隐私盾规则也在近日被再次宣布无效,美国商务部部长表示对这个决定"非常失望,并将继续与欧盟保持密切联系,以期将损失降到最低"。③ 虽然美国目前会采取什么行动还不明朗,但这或许会让美国反思自"9·11事件"以来国内政府一直以隐私为代价过度追求安全的行为。与欧盟提出的高标准数据保护要求相比,美国的外国情报监控法中允许对不居住在美国的外国人实施监控的规定更让人不寒而栗。在吸取欧盟经验与教训时需注意的是,中国可适当加强与其他国家政府机构的交流,以求更具有影响力的顶层规则的制定,而非持续向企业施压,形成治标不治本的效果。

(三)完善内部监控的隐私保障措施

根据《草案》的第三章——数据安全制度来看,目前的数据安全制度内容包括数据安全风险评估、报告、信息共享、监测预警机制、数据安全应急处置机制、数据安全审查制度、数据出口管制和必要时对国外的歧视性的禁止、限制或者其他类似措施的相应措施。④ 其中没有涉及司法性质的监督机制的设立。根据第十二条,公安机关、国家安全机关因依法维护国家安全或者侦查犯罪的需要调取数据应当按照国家有关规定,经过严格的批准手续,依法进行,有关组织、个人应当予以配合。⑤ 国家以安全目的处理个人信息时不必以同意为前提,因此更需要公权力机关尽到足够的审慎义务。有中国学者认为,采取扫健康码、人脸识别等措施,虽然在一定程度上限制了个人的隐

① 田旭:《欧盟个人数据保护法的全球影响成因与启示》,第145页。

② 参见《中华人民共和国数据安全法(草案)》第33条。

③ U.S. Department of Commerce, "U.S. Secretary of Commerce Wilbur Ross Statement on Schrems II Ruling and the Importance of EU-U.S. Data Flows," https://www.commerce.gov/news/press-releases/2020/07/us-secretary-commerce-wilbur-ross-statement-Schrems-ii-ruling-and, last accessed on 25 August 2020.

④ 参见《中华人民共和国数据安全法(草案)》第19-24条。

⑤ 参见《中华人民共和国数据安全法(草案)》第12条。

私,但这是维护生命健康权所必须采取的合理措施,[①]然而这一措施是否符合隐私权限制的比例原则还需要进一步检验。就这一检验条件来看,欧盟内部建立的对公权力限制的保障框架——“监控机关的自我约束+外部的独立监督或救济”的模式具有重要的借鉴意义。

首先,监控机关能够进行自我约束的前提是有法可依。以安全为由进行监控的法律要足够明确、公开、可预见,具体内容可以包括但不限于(1)监控的目的、授权的机构及其程序、公民可能被监控的情形和方式;(2)监控的时限、延续监控的条件;(3)数据的筛选、使用和存储条件以及保留的时长等。要做到尽量明确具体,使监控机关可以据此规范自身行为并接受公众的监督。其次,应当以隐私保障为条件确保“监控法”的质量。对于何为“安全目的”,中国的相关立法中可以进一步缩小解释,并确保监控机关的监控行为对于该安全目的是严格必要的。如数据的获取和保留都不应当超过必要的限度,或许中国应当在立法中明确规定信息的最长保留期限。当数据的使用目的已经满足,就应立即不可逆转地销毁数据。此外,与国内第三方机关共享数据时同样尽足够的审慎义务,从而将监控行为对于公众隐私的干涉减少到最小。最后,独立的监督或者救济也必不可少。具体采取哪种方式可以根据中国的国情进一步斟酌,重要的是监督机构或救济机构的独立性和有效性。监督机构应当能够依申请为任何怀疑自己隐私权被侵犯的公民提供与监控相关的资料,而救济机构对于监视的审查权限应当进一步提高,允许法院审查涉及国家安全的信息等。

(**作者简介**:廖丽,武汉大学法学院副教授、武汉大学国际法研究所副教授;师亚楠,武汉大学法学院硕士研究生。**责任编辑**:齐天骄)

① 王利明:《民法典人格权编的亮点与创新》,载《中国法学》,2020年第4期,第14-15页。