预测性警务与欧盟数据保护法律框架:挑战、规制和局限*

魏怡然

内容提要:预测性警务是欧盟公共安全治理转型中最值得关注的趋势。基于大数据的预测性警务的兴起,意味着刑事执法正在经历从因果关系走向相关性,从合理怀疑走向概率怀疑,从针对性监控走向大规模监控,从事后回应走向主动威慑的转变。本文探讨预测性警务技术对欧盟数据保护法律框架带来的挑战,对完善解决方案提出了初步建议。文章认为,欧盟数据保护法律框架对受预测性警务技术影响的人员提供的保护存在不确定性,欧洲法院的判例可能难以应对预测性警务技术带来的挑战。因此,需要强调目的限制原则,加强技术的透明度,通过认证和追踪提高数据的准确性,以弥补数据保护法律框架的不足。

关键词:预测性警务　欧盟　数据保护　公共安全　犯罪预防

人工智能、大数据和机器学习技术的迅速发展及其在刑事执法领域的应用正在改变警察活动的固有模式。在内外安全危机的催化下,欧洲公共安全治理近年来向预防与控制倾斜,警察部门正转向以情报为主导的警务工作,结合数据驱动的决策来预防和调查犯罪。这种趋势意味着相关隐私和数据保护领域正在发生变化。本文首先分析欧洲警务的预测性转向和特征,然后分别探讨欧盟数据保护立法和欧洲法院判例法在面对基于大数据和机器学习技术的预测性警务时面临的挑战。鉴于欧盟现行数据保护框架和法院判例在保护受预测性警务影响的数据权利时存在不确定性,文章对完善解决方案提出了初步建议。

* 本文受中南财经政法大学中央高校基本科研业务费专项资金资助(项目编号:2722019JCG090)。

一 预测性警务的概念、发展和影响

近年来,欧洲的政治口号正在从“一个自由的欧洲”转向“一个有安全保障的欧洲”。建立安全联盟、打击恐怖主义和极端主义、打击有组织犯罪和非法移民等问题成为欧盟和欧洲各国的核心政治议题。在此情况下,欧盟将信息技术视为实现公共安全的关键。一方面,信息技术扩大了犯罪和恐怖主义的威胁性;另一方面,信息技术也为欧盟和成员国改善安全治理提供了重要的工具,使执法机关得以通过数据追踪甚至预测犯罪。通过监控,收集、分析、整合大量数据,对犯罪做出预判的预测性警务是当前欧洲警察部队的执法趋势之一,[①]而该技术的适用和发展正在使欧洲执法当局的行动向先发制人的方向转变。

(一)预测性警务的概念

预测性警务并没有统一的定义。威廉·布拉顿(William Bratton)等人将预测性警务界定为开发和使用信息与高级分析为前瞻性的犯罪预防提供信息的警务策略。[②]可以将其理解为一种前瞻性思维,其设计逻辑可以追溯到 19 世纪边沁提出的“道德计算”。[③] 虽然是新兴技术,但预测性警务并不是一个全新的概念,而是大数据和人工智能技术革新带来的执法能力上质的转变。就目前的发展形势而言,预测性警务的作用是提供有关犯罪活动的地点和人员的补充资料,发现在执法和调查过程中可能遗漏的联系和模式。虽然其日益受到重视,但尚未取代现有的警务技术和战略。

(二)预测性警务在欧洲的应用和发展

在欧盟层面,预测性警务技术的使用还处于起步阶段。但其预防功能在反恐中可能实现的价值受到许多欧盟机构的重视。欧盟反恐协调员[④]和欧盟执法合作局(EUROPOL)[⑤]就十分积极地推广预测性警务,期望这类技术能够对宣传极端主义思想的在线内容进行跟踪、收集、筛选和分析,在反恐和打击极端化方面发挥重要作用。

---

① Fieke Jansen, “Data Driven Policing in the Context of Europe,” *Data Justice: Understanding Datafication in Relation to Social Justice*, Cardiff University, May 7, 2018, p.2.

② Gerben Bruinsma et al., *The Encyclopedia of Criminology and Criminal Justice*, Springer Science+Business Media, 2014, p.3871.

③ Lúcia Gouveia Pais, “Predictive Policing: Is It Really an Innovation?” *European Law Enforcement Research Bulletin*, No.4, 2018, p.1.

④ Dan Williams, “EU Eyes Israeli Technologies for Spotting Militants Online,” *Reuters*, July 19, 2016, https://uk.reuters.com/article/us-europe-attacks-israel-surveillance-idUSKCN0ZZ197, last accessed on 24 September 2019.

⑤ Staffan Dahllof et al., “EU States Copy Israel's ‘Predictive Policing’,” *EUobserver*, 6 October 2017, https://euobserver.com/justice/139277, last accessed on 24 September 2019.

在欧盟成员国层面,预测性警务深受欢迎。瑞士、德国和英国等国家都开始使用预测性警务工具。一方面,欧洲各国的警察部队纷纷从科技公司购买相关分析系统。例如,丹麦从美国大数据挖掘公司帕兰提尔科技(Palantir Technologies)购买了能够结合不同来源的信息进行识别和分析的 POL-INTEL 平台;随后修改了有关个人数据保护的国内立法,为顺利使用预测性警务技术奠定了良好的基础。① 另一方面,欧洲各国的警察部队也自己投资、试验、开发或合作开发预测警务系统。荷兰阿姆斯特丹警察局(APD)就创建了刑事预判系统(Criminal Anticipation System, CAS)并在全国范围内推广。从功能上来看,这些预测性技术可以分为三类。

(1)预测映射

预测映射的运行分为三个步骤:识别过去犯罪数据中的模式和相关性,预测可能发生犯罪事件的时间和地点,并将资源部署到可能发生犯罪事件的地区。② 其代表性技术是私人公司开发设计的"PredPol",这也是现在全球范围内应用最广的预测性警务技术,已经在美国广泛适用。英国肯特的警察部队在 2018 年 3 月之前也使用了该技术。"PredPol"一般使用犯罪类型、地点和时间数据,其特点是通过历史犯罪数据来预测可能发生犯罪的时间和地点。

(2)预测评估

预测评估是预测个人犯罪的可能性或可能出现的受害者,又被称为个体风险评估。这种技术的运行也分为三个步骤:通过网络分析探究过去犯罪活动的社交网络,使用机器学习和算法来识别可能的肇事者或受害者,再由执法机构采取探访、告知等事前干预措施。③ 这类技术代表了预测性警务发展的第二个阶段,即从预测范围转向预测个人。其代表性技术是英国达勒姆警察部队和剑桥大学共同研发的系统危害评估风险工具④(The Harm Assessment Risk Tool, HART)。该系统是英国警察部队部署的首批预测算法模型之一,是通过机器学习进行危害评估的风险工具,根据犯罪历史、年龄和邮编等信息,预测被逮捕的个人再次犯罪的可能性。有数据显示,危害评估风险工具在评估中的预测准确率达到了 62.9%。⑤ 现阶段,这类技术在具体功能和精准

① Staffan Dahllof et al., "EU States Copy Israel's 'Predictive Policing'."

② James Capotosto, "Data Opportunities and Risks: The Dynamic of Public, Personal, and Commercial Interest," *Journal of Community Safety & Well- Being*, Vol. 2, No. 1, 2017, p.19.

③ Ibid., p.19.

④ Patricia Nilsson, "First UK Police Force to Try Predictive Policing Ends Contract Use of PredPol Cancelled, but Met will Try to Develop Its Own System," *Financial Times*, 26 November 2018, https://www.ft.com/content/b34b0b08-ef19-11e8-89c8-d36339d835c0, last accessed on 24 September 2019.

⑤ Isobel Thompson, "Predictive Policing and 'Pre-crime' Algorithms: The New Age of Law Enforcement," 10 May 2019, *The Face*, https://theface.com/society/the-future-of-policing, last accessed on 24 September 2019.

度方面还有待完善。

(3)预测动机

上述两种是学界和业界都广泛认可的预测性警务技术类型,其共同特点是使用犯罪数据,预测以前出现过的地区或是个人犯罪的情况。笔者认为,还有一类预测性警务技术可以称之为预测动机。这类技术已在实践中开始产生重要影响,代表了预测性警务新的发展趋势,典型的例子就是欧盟的乘客姓名记录系统(PNR System)。该系统的有效性建立在对航空乘客全面监控的基础之上。自 2018 年《乘客姓名记录指令》生效以来,在欧盟成员国起飞和降落的航班都要向目的地国家的主管当局通知每名乘客的详细信息,包括姓名、行程、如何购买机票、支付信息、预订代码和座位等。这些事无巨细的信息可以用来描述乘客的个性、生活细节、习惯和社会关系,通过全面细致地了解个人情况来分析该乘客与犯罪集团或恐怖组织是否存在联系。据此,警察部队可对有关人员进行特别检查、询问或逮捕,从而预防恐怖袭击或是避免严重犯罪的发生。在内部的乘客姓名记录系统之外,欧盟早前就与澳大利亚、加拿大和美国签订了乘客姓名记录协定,所有从欧盟前往这些国家的个人都要接受类似的检查。欧盟还有意向将这种仅限于航空乘客的预测性警务模式延展至海运和铁路运输,进一步扩大这类预测动机系统的应用范围。

之所以将乘客姓名记录系统归类为“预测动机”,主要是因为较之前两种预测性警务技术,它在逻辑和数据使用上都更进一步,意味着预测性分析的目标正在扩大,内容更加细致深入。前两种预测性警务技术的逻辑是通过研究过去的犯罪模式、地点、时间和趋势,在统计的基础上预测未来可能发生的犯罪活动信息。乘客姓名记录系统特点之一是将从私营航空公司获取的数据包括在内,通过异构数据库的连接大幅度扩大了可用数据的范围,不限于警方原本的数据库,就范围而言更类似于大规模监控;特点之二是预测的目的是找出以前未被执法当局发现的、可能具有危险性的人物,不是监控已知个人而是发现新的可疑对象,亦不是分析行为而是分析动机。笔者认为,异构数据库的整合及对没有记录的个人进行动机分析与行为预测,带来的影响是执法监控范围的大规模扩大和刑事执法对预测性警务依赖性的大幅度增加,意味着警务模式本质上正在转变。这种预测是在根据刑法不能对可疑人员采取任何行动的情况下,以避免安全风险为理由,通过监控和算法识别个人来采取预防性措施。基于风险的侵入性措施,在没有法律要求的切实证据的情况下,用于控制没有犯罪行为的人,其预测动机的逻辑存在一定的道德和法律风险。

(三)预测性警务对刑事执法的影响

预测性警务技术能够收集、分析大量数据,识别犯罪模式和预测风险。它有助于合理分配警力,节约成本,提高警察识别可疑人员的能力。该技术的适用正在改变刑事执法的结构和运行。

(1)从因果关系到相关性

传统的警察执法行为中也包括预测,但主要是根据掌握的信息按照因果关系进行分析。预测性警务技术的不同之处是从数据中挖掘可疑信息,这意味着该技术是基于相关性在运行。虽然算法分析有助于发现人工排查遗漏的信息和提高效率,但这种方法的一个关键问题在于,使用预测性警务的目标是发现因果关系,但相关性本身并不能说明因果关系。因此,预测性警务算法得出的结论可能会较为草率。

(2)从合理怀疑到概率怀疑

预测性警务技术的开发和逐渐广泛的适用,在技术层面上是因为大数据和机器学习,包括人工智能技术不断发展的必然结果;从实践层面上来看,则与自"9·11 事件"以来世界各国对安全问题的高度关注密切相关。① "9·11 事件"后出现了先发制人这种完全不同的权力运行逻辑,②各国希望能够对威胁采取提前行动。但在现实中,先发制人的逻辑针对的威胁很有可能尚未形成,具有不确定性,难以在现有信息基础上进行合理的逻辑推理和预判。在此情况下,预测性警务理论提供了一种看似科学的方法。这种方法假设可以从数据的模式中得出某些可靠的相关性,识别、锁定和跟踪那些极有可能犯下某些罪行的人,③因此可以减少政治影响和主观判断,提供更理性、公正、可靠和合法的决策方式,增加先发制人的可能性。但是,大数据并不一定是对线下现实的准确表达,而是由其创建、收集、存储和解释的方式塑造的;算法并不总是科学的,其中也可能存在错误和偏见。概率怀疑不能完全确保其真实性和准确性,也难以保证在此基础上采取警务行动的合法性和合理性。

(3)从针对性监控到普遍监控

一方面,为边境控制、移民和安全等不同目的而建立的不同执法数据库之间的相互操作性逐渐增强,这是欧盟当前安全战略的一个重要组成部分。④ 另一方面,监控越来越关注于收集日常生活中产生的个人数据。这体现了从针对性监控向大规模监

① Patrick F. Gillham, "Securitizing America: Strategic Incapacitation and the Policing of Protest since the 11 September 2001 Terrorist Attacks," *Sociology Compass*, Vol.5, Issue 7, 2011, pp.636-637.

② Brian Massumi, *Ontopower: War, Powers, and the State of Perception*, Duke University Press, 2015, p.200.

③ Andrew Guthrie Ferguson, "Policing Predictive Policing," *Washington University Law Review*, Vol.94, No.5, 2017, p.1138.

④ Valsamis Mitsilegas, "European Criminal Law and the Dangerous Citizen," *Maastricht Journal of European and Comparative Law*, Vol.25, No.6, 2018, p.747.

控发展的趋势。大规模监控提供的海量数据能够为预测性警务所用,通过包含尽可能多的信息的大型数据库产生有用和可靠的关联,以最终查明嫌疑犯和预防犯罪。然而,正如上文所言,这些技术本身也存在不确定性和缺陷,大规模监控的做法对公民的基本权利和整个社会构成许多风险。在不久的将来,随着无人机、人脸识别和具有预测能力的人工智能技术的进一步发展,监控可能会变得更具侵略性。在这种情况下,执法的重点会进一步向预防倾斜,重点从对具体犯罪行为做出反应转移到阻止那些被认为是具有危险性的人。①

(4)从事后回应到事前控制

传统上,刑事执法活动大多是被动的,执法部门在犯罪发生后进行调查。但是随着预测性警务技术的适用,刑事犯罪调查的目的和范围正在发生重大变化,更倾向于将数据分析用于预测目的,而不是回应或是解释目的,对某人是否会犯下刑事罪行的预测将越来越成为警方关注的对象。传统上,按照刑法的规定,是否受到刑事调查或逮捕都与实际行为有关。但随着执法重点从"犯罪后"转变为"犯罪前",可能重要的不是触犯刑法的实际行为,而是警察参考预测性警务技术的分析后做出的判断。技术介入下执法模式的改变,可能会产生连锁效应,改变执法机构工作的重点和执法过程中的权利义务关系,甚至会挑战刑法中既有的规定和原则。

二 预测性警务对欧盟数据保护法律框架的挑战

欧洲警察部队对预测性警务降低犯罪率的作用非常期待,但为公共安全目的收集数据,尤其是个人数据的预测性警务技术与欧洲的数据和人权保护标准之间存在紧张关系。② 随着 5G 技术的普及和人工智能技术的进步,相关风险在未来会更大。关键问题是,欧盟数据保护法律框架能否应对演进中的预测性警务技术,公私合作、数据自动化处理是否会影响对数据的充分保护。

(一)欧盟权力受限影响数据保护效果

欧盟经过 4 年的努力,在 2016 年 4 月升级了数据保护法律框架。这不但包括备受瞩目的《一般数据保护条例》,还包括《欧洲议会和理事会关于主管当局为预防、调查、侦查或起诉刑事犯罪或执行刑事处罚以及此类数据的自由流动而处理个人数据方

① Valsamis Mitsilegas, "European Criminal Law and the Dangerous Citizen," p.751.
② Dan Williams, "EU Eyes Israeli Technologies for Spotting Militants Online."

面的自然人保护问题,并废除理事会 2008/977/JHA 号框架决定的 2016/680 号指令》①(LED,简称为《执法数据保护指令》②)。该指令于 2016 年 4 月通过,2018 年 5 月生效。

《执法数据保护指令》作为特别法,是欧盟立法者考虑到刑事案件中数据保护的特殊性,专为执法部门在数字时代处理个人数据而设计,③适用于主管当局为防止、调查、侦查或起诉刑事犯罪或执行刑事处罚,包括预防和防止对公共安全的威胁④的情形。《执法数据保护指令》规定,为了预防、调查和起诉刑事犯罪,主管当局有必要将了解犯罪活动并检测不同的刑事犯罪之间的联系也包括在内。⑤ 因此,预测性警务涉及的数据处理主要是受到《执法数据保护指令》的规制。值得注意的是,《一般数据保护条例》并非对执法相关的数据处理完全不适用,而是不适用于"主管当局为预防、调查、侦查或起诉刑事犯罪或执行刑事处罚,包括防范和防止对公共安全的威胁",⑥即《执法数据保护指令》的适用范围。通过普通法与特别法结合的立法方式,欧盟改正了原有数据保护法律框架中对私营部门向执法当局传输数据没有规定的缺点,除外交政策和国家安全之外,实现了对刑事执法数据处理的全面监管。

但是,欧盟在原第二、第三支柱领域受限的权力对数据保护法律框架的实施效果产生了不利影响。其一,《一般数据保护条例》和《执法数据保护指令》的性质是存在区别的。虽然《里斯本条约》取消了支柱结构,但欧盟在自由、安全与司法领域只具备辅助性作用。这直接体现为专门规制执法数据传输与处理的立法是指令而不是条例,实际适用中给成员国留出了许多自由裁量的余地,⑦这可能不利于欧洲统一数据保护

---

① Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of such Data, and Repealing Council Framework Decision 2008/977/JHA, OJ L 119 4.5.2016, p. 89.

② 该指令简称不一,还有学者称之为《警察指令》(Police Directive)或是《警察和刑事司法当局指令》(Police and Criminal Justice Authorities Directive)。

③ Paul de Hert and Juraj Sajfert, "Police, Privacy and Data Protection from a Comparative Legal Perspective," in Monica den Boer, ed., *Comparative Policing from a Legal Perspective*, Elgar, 2018, p. 307.

④ Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of such Data, and Repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, Recital 4.

⑤ Ibid., Recital 27.

⑥ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, Article 2.2.(d).

⑦ Hielke Hijmans, "Data Protection and Surveillance: The Perspective of EU Law," Paper Presented to "the Annual Conference of the European Criminal Law Academic Network," London, May 17, 2018, p.4.

标准的形成,也会影响数据保护的具体效果。其二,《一般数据保护条例》和《执法数据保护条例》依然不适用于联盟法律之外的涉及国家安全的活动。[①]而且,国家安全是一个广泛的概念,能够将许多活动包括在内,执法机构为反恐而采取的措施也有可能被包括在内。考虑到欧洲法院近年的重要判决中对预防性反恐措施和自动分析的支持,许多预测性警务行为都有可能因其反恐功能被归类为涉及国家安全的活动,从而不适用于欧盟数据保护法律框架。这种情况对于受预测性警务技术影响的数据权利来说格外危险。因为预测性警务技术当前仍属于实验性创新,其准确性、透明度和公平性尚且存在疑问,需要在明确的法律框架内实施,而且要有足够的监督机制确保执法机构公平合法地使用技术,才能保障合理使用数据的权利,避免警察权力的滥用。因此,这种例外对于数据权利的保护是危险的,需要对"国家安全"加以限定和明确。

(二)原则性规定难以应对复杂的公私合作问题

欧盟数据保护法律框架的特点是按照数据控制者和处理数据的初始目的来确定适用的立法。例如,适用于《执法数据保护指令》的数据处理行为需要满足两个条件:处理个人数据的行为者必须是《执法数据保护指令》第 3 条第 7 款意义上的"主管当局",以及处理必须按照第 1 条第 1 款规定的"执法"目的进行。但是,主管当局并不只是传统执法机关。《执法数据保护指令》第 3 条第 7 款 b 项规定:成员国法律委托行使公共权力的其他任何机构或实体",私营公司和其他组织也被包括在内。虽然当前这种现象很少,但预测性警务技术发展的一个特点就是所用数据库不断扩大,已经逐渐通过立法或是协议将私营公司的商业数据库包括在内。前文提到的乘客姓名记录系统中,航空公司虽然是为了商业目的或是业务需要收集用户信息数据,但有义务向主管当局披露和传输乘客姓名数据,以供主管当局打击恐怖主义和严重刑事犯罪。[②] 当航空公司向主管当局传送自己收集到的乘客姓名记录数据时,主管当局会将这些数据与自己掌握的有关犯罪和恐怖分子信息的数据库进行交叉比对分析。因此,在数据保护领域,私营公司在刑事执法中地位和权力呈现上升和扩大的趋势。这种变

① Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, Article 2.2.(b); Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of such Data, and Repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, Recital 14.

② Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the Use of Passenger Name Record (PNR) Data for the Prevention, Detection, Investigation and Prosecution of Terrorist Offences and Serious Crime, OJ L 119, 4.5.2016, Recital 10, 13.

化意味着数据传输与处理和执法数据保护中的关系十分复杂。如上文所述,预测性警务技术中私营公司参与程度较高,涉及为执法目的处理数据,以及本着其他目的收集数据。随着预测性警务技术越来越多地使用非警方数据,这方面的公私合作会越来越多,需要判断合作中各方的责任和义务,落实数据保护条款。

《执法数据保护指令》第 11 项建议是欧盟数据保护法律中唯一规定机关和私营公司之间数据传输和处理方面的法律适用的条款。按照该条规定,如果此类机构或实体为了本指令以外的目的处理个人数据,则适用《一般数据保护条例》。因此,如果某个机构或实体为其他目的收集个人数据并进一步处理这些个人数据以遵守其所受的法律义务,适用《一般数据保护条例》。例如,为了调查、侦查或起诉刑事犯罪,金融机构保留由它们处理的某些个人数据,仅在特定情况下根据成员国法律向国家主管当局提供这些个人数据。相应地,警察机关等传统主管当局处理数据适用《执法数据保护指令》;私营公司代表主管当局处理数据时,也适用《执法数据保护指令》。在这种情况下,主管当局是数据控制者,私营公司是数据处理者。

应该说,欧盟的归类和解释能够对具体实践起到一定的指导作用。但是,欧盟是在立法的建议部分对法律依据做出说明,这种方式不具备法律拘束力,至多产生指导性影响,难以促成各成员国统一的实践。更大的问题在于,预测性警务技术的适用和特点决定了私营公司会在执法中起到较为重要的作用,这条规定过于简单,而且很可能与预测性警务涉及的数据处理实践不符,难以对复杂的实践进行充分指导。

其一,欧盟数据保护立法框架的判断关键是数据控制者,但实际上预测性警务技术的特点可能会让数据控制者这个概念失去原本的意义。在私营公司实际上起到执法部门作用的情形下,按照《执法数据保护指令》的规定,私营公司是数据处理者,执法机关是数据控制者。但当警方从私营公司购买预测性警务技术时,基于数据收集处理和机器学习算法的技术并不为警方所全面理解。有些私营公司甚至没有对警方进行充分的说明和讲解,一旦出了问题,警方也无法修改。如果预测性警务系统设置了供应商锁定机制,警方甚至无法自行调整软件,整个分析过程都只能依靠私营公司。① 在此情况下,警方作为数据控制者承担主要责任是否合适存在疑问。

其二,当私营公司受成员国委托,为执法目的进行数据处理,成为《执法数据保护指令》第 1 条第 1 款规定的“主管当局”时,它同时具有两个身份:当它作为私营公司进行执法目的以外的数据处理时,受《一般数据保护条例》约束;当它作为主管当局处

① Rosamunde van Brakel, “(Dis)Empowering Effects of Predictive Big Data Policing on Citizens,” in Bart van der Sloot et al., eds., *Exploring the Boundaries of Big Data*, Amsterdam University Press, 2016, p.124.

理执法数据时,受《执法数据保护指令》约束。虽然这样分类看似很清楚,但实际工作中相关活动很可能有交叉重叠之处,难以区分具体处理行为的性质,法律适用的边界存在不确定性。虽然都是为了执法目的处理数据,但欧盟的两个数据保护立法相关的规定各异,私营机构和执法机关的数据保护义务和限制也不同。《执法数据保护指令》实质限制较少,执法当局在收集和进一步处理个人数据方面的权力更具侵略性,但鉴于执法的特殊需要,它们也受到严格限制,只能在执法的公共职能范围内,根据法律规定的理由和目的按照特别程序行使。① 属于《一般数据保护条例》的数据处理受到更实质性的限制,数据处理的监督和平衡要求与《执法数据指令》存在区别。这种区别在面临私营机构双重身份的情形时,可能导致适用困难和保护标准不一致。

(三)禁止性规定实效存疑

预测性警务技术最突出的特征之一就是数据处理的剖析能力。《执法数据保护指令》第 3 条第 4 款将剖析定义为:"任何形式的个人数据自动处理,包括使用个人数据评估与自然人有关的某些个人方面,特别是分析或预测有关自然人在工作中的表现、经济状况、健康、个人偏好、兴趣、可靠性、行为、地点或动作。"《执法数据保护指令》第 11 条继而规定:"仅基于自动处理做出的决定,包括对数据主体产生不利法律效力或对其产生重大影响的描述,应该被成员国禁止。除非该自动决定的产生经过数据控制者所属的联盟或成员国法律的授权,而且联盟或成员国法律已经为数据主体的权利和自由提供适当的保障,或至少相关数据控制者有对自动处理进行人为干预的权利。" 指令第 38 项建议也强调了对自动处理的限制,认为人为干预"必须由具有改变决定的适当权力和能力的人来执行"。值得注意的是,《一般数据保护条例》第 22 条主题与指令第 11 条第 1 款相似,但措辞为"数据主体应有权不受仅基于自动处理的决定",将其定性为数据主体的权利。通过比较可以发现,《执法数据保护指令》注意到了自动处理对个人可能造成的不利影响,并要求对其进行有效的人为干预,第 11 条的规定不但对缺乏必要权利保障的自动处理明确表达了禁止态度,还清楚地列出了权利保障的标准和要求。因此,从字面上看,该指令较其前身和《一般数据保护条例》的有关规定,似乎能够为受预测性警务影响的数据提供更强大的保护。

实践中,该条规定的适用面临许多限制。其一,禁止性规定容易被规避。按照该条规定,符合欧盟或成员国法律规定的自动处理是允许的。因此,通过立法,成员国可以使执法当局依赖预测性警务系统的自动决策,不受禁止性规定的影响。其二,禁止

① Nadezhda Purtova, "Between the GDPR and the Police Directive: Navigating through the Maze of Information Sharing in Public - private Partnerships," *International Data Privacy Law*, Vol. 8, Issue 1, 2018, p.53.

性规定实施范围很窄。第 11 条指的是数据处理的完全自动化。因此,主管当局按照乘客姓名记录系统或其他预测性警务技术计算的结果开展执法活动,是否属于完全自动化处理存在疑问。关键是第 38 项建议中规定的具有适当权力和能力的人在最终决定中是否起到了判断作用,如何判断自由裁量权的行使程度并无客观标准。因此,即使主管当局只是按照预测性警务系统的分析结果决定出警,也会被认为包含了个人判断,是具有适当权力的人员的最终意见,第 11 条无法适用。① 其三,禁止性规定的实施门槛很高。适用第 11 条必须要出现自动决定对个人产生“不利法律效力”或“造成重大影响”,较之适用条件为“法律效力”或“同样显著影响”的《一般数据保护条例》标准更高。如此规定造成的结果是基于自动处理的决定如果影响不大则不足以被禁止。第 29 条工作组提供的“不利影响”典型例子是旅客因被登记在黑名单上而被拒绝进入交通系统。② 而且,在预测性警务的背景下适用可能会更加困难。一方面,正如上文所述,如果主管当局基于预测性技术的结果采取执法措施的话,即便是对个人“造成重大影响”或是产生“不利法律效力”,也可能被认定为不是自动化的预测系统的原因而是主管当局的决定,无法适用第 11 条。另一方面,第 11 条的两个定性标准太过模糊。乘客姓名记录系统得出的结果也许符合第 29 条工作组提到的例子,但基于其他预测性系统,如按照“PredPol”对犯罪趋势或地区的预测开展的执法活动是否符合标准依然无法确定。

整体而言,欧盟数据保护法律框架对受预测性警务影响的数据提供的保护存在许多不确定的地方。一是采取一般立法与专门立法并行的规制方式,但实际保护效果依然可能因为权力局限受到不利影响;二是规定了适用原则,但过于简单,而且很可能与预测性警务涉及的数据处理实践不符,难以对复杂的实践进行充分指导;三是禁止性规定有提供更强大的保护的潜力,但容易规避、狭窄的实施范围和过高的实施门槛可能限制该条款的作用。因此,欧盟数据保护法律框架对受预测性警务技术影响的人提供的保护存在不确定性。

三 欧洲法院数据保护判例对预测性警务的规制和局限

在数据保护的实体法存在局限时,欧洲法院和欧洲人权法院的判例能否提供充分

① Orla Lynskey, “Criminal Justice Profiling and EU Data Protection Law: Precarious Protection from Predictive Policing,” *International Journal of Law in Context*, Vol.15, 2019, p.174.

② Article 29 Data Protection Working Party, *Opinion on Some Key Issues of the Law Enforcement Directive* (*EU* 2016/680), WP258, 29 November, 2017, p.12.

的数据保护显得格外重要。近几年,两个法院对执法部门大量获取个人数据的相关案件做出了若干重要判决。欧洲法院在 Tele2 和 Watson 案与欧盟-加拿大乘客姓名记录协定案中对数据保护的态度,以及欧洲人权法院在扎卡洛夫诉俄罗斯和 Szabò 与 Vissy 诉匈牙利等案中的意见,虽然各有侧重,但内容有一致性:根据《欧盟基本权利宪章》(以下简称《宪章》)和《欧洲人权公约》,对不是绝对的基本权利的限制必须要有法律规定,即要有符合大众利益的合法目标,而且限制是实现上述目标所必需和适当的。也就是说,两个法院都接受了为打击包括恐怖主义在内的严重国内、跨国和国际犯罪为目的的监控实践。然后,以数据保护合法性、比例性和目的限制原则来规制大规模监控行为。结合具体实践来看,两个法院对数据保护设定的标准看似严格,但适用中存在明显的缺陷。

(一)措辞的模糊性影响合法性原则的效果

通过对相关判例的分析可以发现,欧洲法院和欧洲人权法院认定的合法性要求包括两方面的含义:其一,干预措施必须合法。国内法必须明确规定主管当局赋予的任何酌处权的范围及其行使方式,必须规定客观标准,确定可转让数据与所追求的目标之间的联系;①其二,有关干预的国家立法必须明确,公民可以轻松获取和充分理解,其适用后果是可预见的。在数据保护相关的情况下规定更为严格,要以具体的方式表明收集的数据以及从私营公司转移到执法当局的数据的性质和范围。在预测性警务范围内,只有严重的刑事犯罪才能收集和转移数据。在敏感数据问题上,还要对保护公共安全免受恐怖主义威胁和严重跨国犯罪之外的其他理由进行精确而特别严密的论证。②

合法性原则在数据的使用目的、使用方式、数据类型和保留期限方面都提出了很高的要求。其一,国家立法必须对成员国主管当局对私营公司数据的访问权限制定客观标准。例如,严格按照预先确定的数量和位置明确具有访问授权的人员,随后明确和严格限制获取的具体类型的数据只能被用于确定的目的。主管当局对数据的使用必须同样严格限制,并能够证明使用特定数据所产生的干扰是合理的,而且必须由主管当局获取和处理。其二,干涉行为必须受到有效的监督。数据使用最好由司法机构监督,或在任何情况下由具有足够权力和能力的独立机构进行监督,以实施有效和持续的控制。③ 在将数据存储在主管当局的数据库中的这段时间内,必须采取适当的组

① C-698/15 Tele2 Sverige, para. 120; Opinion 1/15, para. 202-208; Zakharov v. Russia, para. 249; Szabò and Vissy v. Hungary, para. 73.

② Opinion 1/15, para. 191; Zakharov v. Russia, para. 253.

③ C-362/14 Schrems, para. 90; C-698/15 Tele2 Sverige, para. 122; Zakharov v. Russia, para. 231.

织和技术措施,以确保数据安全。其三,必须制定规则,以便在不再需要时删除或销毁转移的个人数据。除上述情况外,两个法院还强调,在不影响使用数据目标的情况下,接受这些措施的个人应当得到相应主管当局对其数据访问和处理的通知。① 而且,任何实施此类措施的立法还必须规定个人可以寻求有效的补救措施,以获取信息及其有关数据。②

从判决的措辞和要求来看,法院对于合法性原则的要求似乎非常严格。但值得注意的是,两个法院并未要求各国制定法律列出可能需要实施预测性警务或是大规模监控的情况,这给成员国在实践中进行解释、扩大适用范围留出了余地。而且,欧洲法院所表达的态度较为宽松,"重要的国家安全、国防或公共安全利益受到恐怖主义活动威胁的特殊情况下,如果有客观证据可以推断,在具体情况下,该数据可能对打击此类活动做出有效贡献,也可以获得其他人的数据"。③ 应该说,像"重要""可能"和"有效"这样的措辞含义较为模糊,对何为"客观证据"也没有具体限定。因此,在实践中的确能让成员国在较大的范围内采取预测性警务措施。

(二)技术的侵入性影响比例性原则的功能

在为执法目的获取和使用个人数据的过程中,比例性原则要求执法当局在使用的手段和预期的目标之间取得平衡,对权利的限制必须是合理的,仅收集和处理与执法目的相关的个人数据。欧洲法院的标准是干涉程度和目标重要程度成正比。根据比例性的要求,有关保护隐私和个人数据的减损和限制必须限制在严格必要的范围内。而且需要制定最低限度的保障措施,有效保护个人权利免受滥用的风险。法院认为,除其他可能情形外,使用和转移数据应该在预防、侦查或起诉犯罪程序框架内根据这些当局的合理要求做出,还为评估以监控目的从私营公司向安全部门大量转移数据的干涉措施的比例性提供了判断标准。

按照欧洲法院的标准,实践中必然会出现的问题是安全主管部门实施预测性警务是否符合比例性原则。具体而言,就是预测性警务不能是大规模监控或是元数据监控,必须是针对性监控或是内容监控;而且针对性监控必须符合合法比例。但是,欧洲法院的标准在面对侵入性技术的发展时存在一些问题。一方面,大规模监控和针对性监控之间的区别不够清楚。虽然欧洲法院的实践对大规模监控和有针对的监控持明

① Szabo v. Hungary, para. 86.

② C-698/15 Tele2 Sverige, para. 121.

③ Hielke Hijmans, "PNR Agreement EU-Canada Scrutinized: CJEU Gives Very Precise Guidelines to Negotiators," *European Data Protection Law Review*, Vol.3, 2017, pp.410-411.

显区别的态度,但实际上,大规模监控和针对性的监控之间的区别并不总是很清楚。[①] 而且,欧洲法院最近的判例似乎改变了原有的严格限制的做法。欧洲法院在欧盟与加拿大乘客姓名记录协定案的意见中,同意将所有由欧盟飞往加拿大的旅客的资料转移。这意味着,法院认为这是有针对性的监控而不是大规模监控。虽然乘客姓名记录数据的性质、范围和数量,较之早先有关电子通信数据的范围要明显狭窄。但是,该数据的特点是全面具体,对个人是有深度揭示作用的。欧洲法院对乘客姓名记录数据未做特别限制,这个扩大解释的判决创造了为保护安全和预防恐怖主义以及允许对特定类别的数据,包括个人数据和隐私进行更强侵入性干扰的先例。另一方面,元数据监控和内容监控之间的区分可能失去意义。预测性分析技术的侵入性越来越强,基于人工智能的预测性警务已经不再是天方夜谭。这种发展正逐渐减少元数据监控和内容监控间的差异,需要规制的重点正在改变。比例性原则现有的分类规制方式,可能难以对预测性警务技术进行有效约束。

(三)技术的不确定性需要更严格的限制

通过观察欧洲两法院近几年有关数据保护和公共安全关系的判决就会发现,两个法院最近的判决虽然依然强调权利保护的标准和原则,但已体现出对大规模监控的支持态度,表现出对预防的重视以及对自动化手段的认可和对安全的追求。在欧盟与加拿大乘客姓名记录协定案的意见中,欧洲法院未反对通过自动化手段对这些数据进行预测分析,只是将其目的限制为识别可能对公共安全构成风险的个人。欧洲人权法院在 Szabò 和 Vissy 诉匈牙利案的判决中也体现出类似的倾向。整体来看,该案的判决在很大程度上与扎卡洛夫诉俄罗斯案保持了一致,遵循了扎卡洛夫案判决所设定的出于情报和国家安全目的实施大规模监控的欧洲标准。但实际上,该案判决的部分措辞与先例不同。例如,对于监控合法性的标准之一是“个人怀疑”被监控个人从事犯罪或某些活动,而不是扎卡洛夫案中的“合理怀疑”。[②] 因此,欧洲人权法院实际上明显降低了执法机关为安全目的进行监控的门槛,降低了个人数据保护标准。

欧洲法院和欧洲人权法院对预防和自动化手段的欢迎,与实践中欧洲各国在执法中预测性警务技术逐渐扩大适用的现实是一致的。为有效规制这类预测性行为,欧洲法院表示,预先制定的算法和标准应具有特定性和可靠性,而且不具有歧视性,可以针对被合理怀疑可能参与恐怖主义行为或严重的跨国犯罪的个人得出结果。为了确保

① Opinion 1/15, paras. 188-189.

② Giuseppe Rizzo, “Szabò and Vissy v. Hungary: A Step Back?” *Lexology*, 5 February 2016, https://www.lexology.com/library/detail.aspx?g=435b47eb-31a0-4240-b17a-27894e7fffd7, last accessed on 24 September 2019.

执法行为的比例性及对数据的保护,法院同时要求在自动处理数据后获得积极结果的情况下,在采取个别措施对有关航空旅客造成不利影响之前,必须通过非自动化手段对其进行重新审查。

关键的问题是,虽然欧洲各国主管当局和相关业界都对预测性警务技术帮助执法部门更有效地打击犯罪持积极支持的态度,但是该技术在现阶段存在许多不足,需要就其使用做出更严格具体的限制。一是利用预测警务技术收集的证据的价值尚未完全确定,许多学者对警察部队对预测性警务的依赖和该技术的合法性提出了质疑。① 例如,马克斯·普朗克研究所对斯图加特当地警察局使用的 PRECOBS 软件进行了调查,认为该软件能否为减少家庭入室盗窃活动做出贡献仍然"难以判断"。② 二是预测性警务技术的判断存在偏差。许多学者长期以来一直认为大数据分析和决策自动化系统存在偏见。③ 预测性警务模型主要是数据驱动。如果原始数据包含正确的数据质量和数量,那么数据分析效果更好,能提取有价值的信息。但是,当前的预测性警务技术中有下列因素会影响其结果的客观性:一是技术可能加剧偏见。在预测性警务技术使用的数据中,过去的犯罪记录发挥了很重要的作用,技术又重视相关性的连接,因此,这种方式具有延续甚至增强偏见的高风险。而且,犯罪数据中偏差不可避免,还可能存在一些错误和偏见,提供的结果可能会偏向特定的族裔或群体。也就是通常所说的,使用预测性监管模型进行分析可能形成基于算法的歧视。如果警察严重依赖于(有偏见的)预测,就会出现视野狭窄的风险;二是预测性警务技术缺乏透明度。虽然分析技术背后的算法可能是中立的,但它们的设计、开发和应用并不透明。所有这些影响可能极具破坏性,不仅危害法治和基本人权,还可能破坏对执法机构的信任,甚至可能导致对个人和群体产生偏见的结果。④ 而且,随着系统发展得更加复杂,警察无法了解技术细节的情况可能会增加。如果预测警务算法中的偏见没有得到正确纠正,就可能导致数据决定论,这意味着对个人的判断是基于暗示潜在未来犯罪行为的相关性,而不是他们实际犯下的罪行。

应该说,预测性警务中不透明的技术、算法中可能存在的不公平和适用中的歧视

---

① Andrew Guthrie Ferguson, "Policing Predictive Policing," *Washington University Law Review*, Vol.94, p.1123; Martin Degeling and Bettina Berendt, "What's Wrong about Robocops as Consultants? -A technology-centric Critique of Predictive Policing," *AI & Society*, Vol. 33, Issue 3, 2018, p.347.

② Dominik Gerstner, "Using Predictive Policing to Prevent Residential Burglary Findings from the Pilot Project P4 in Baden-Württemberg, Germany," *European Law Enforcement Research Bulletin*, No.4, 2018, p.1.

③ Rosamunde van Brakel, "(Dis)Empowering Effects of Predictive Big Data Policing on Citizens," in Bart van der Sloot et al., eds., *Exploring the Boundaries of Big Data*, Amsterdam University Press, 2016, pp.125-126.

④ Lilian Edwards and Michael Veale, "Slave to the Algorithm? Why a 'Right to an Explanation' Is probably not the Remedy you Are Looking for," *Duke Law and Technology Review*, Vol.16, No.1, 2017, p.28.

都可能引起风险,需要与之相称的执法权力问责机制和完善的数据保护法律框架。欧洲法院的规定只是简单提出非歧视的要求,没有对预防犯罪的方法做必要的限定,也没有对预防作用的自动化分析技术做限制,因此,可能难以有效约束成员国的侵入性预防措施。

总体而言,欧洲法院虽然对合法性原则做了严格的要求,但模糊的措辞扩大了合法性原则的范围,让成员国可以在较大的范围内采取预测性警务措施。比例性原则现有的分类规制方式,可能难以对预测性警务技术进行有效约束。预测性警务现阶段的技术缺陷、基础数据的不足和可能的歧视效果都需要严格的监管机制,但法院近年来对预防措施和自动决策持认可态度,对于自动决策和成员国执法行为的限制过于简单,可能对有效规制预测性警务带来不利影响。

四 展望与总结

虽然预测性警务对数据保护法律框架提出了许多挑战,但是该技术为执法部门提供了改变传统工作模式、更好地遏制犯罪和强化公共安全的可能,也因此成为世界各国执法部门改革的趋势。在可预见的未来,欧洲乃至世界各国都不太可能在执法改革方面放弃对预防的强化,预测性警务技术会不断扩大应用范围,继续开发产品。因此,现实中的关键是如何将技术缺陷带来的法律问题最小化,通过限制使用目的,加强透明度,提高数据准确性和可靠性,来促进安全目标和数据权利保护之间的平衡。从欧盟数据保护法律框架的现状考虑,可以在以下方面予以加强。

第一,针对数据保护难以落实的情况,强调目的限制原则的作用。因为目的限制原则要求只分析所需信息。通过限制与预定目的相关的收集和处理,可以保护更多数据免受未经授权的内部或外部访问,在一定程度上强化《执法数据保护指令》的保护条款。

第二,针对公私合作中的复杂局面和私营公司影响力的提高,强调透明度原则。正如前文所言,预测性警务内部技术结构复杂,而警方可能仅使用技术和参考技术得出的结果,并不知道技术如何运行或是结果按照什么样的原理产生。因此,一旦这种自动化程序出现故障则无法采取有效措施。因此,应该强调预测性警务技术和使用方式的透明度,明确算法产生具体结果的原因,让主管当局理解和掌握其运行原理,从而提高预测性警务技术的可核实性。这样有助于保护受其影响个人的权利,也能够让主管当局的相关人员更好地理解系统决策产生的原因,真正地在自动处理基础上做出有

效决策。

第三,针对现阶段预测性警务技术在准确性和成熟性方面的不足,应该解决个体数据的认证和跟踪问题。现阶段的预测性警务技术,在准确性上还存在明显的缺陷,其来源数据也存在错误的可能,但已经越来越广泛地应用于执法实践。为避免因为技术的错误和不足对执法行动的不利影响,需要明确数据的来源和轨迹,理解其编辑和分析,确认其真实性和可靠性,避免因为技术缺陷和数据的错误对个人产生不必要的影响。

本文关注的是预测性警务对欧盟数据保护法律框架的挑战。通过分析,笔者认为,欧盟现有的数据保护法律框架对预测性警务技术带来的挑战准备不足,其权力的局限、规定过于简单的适用原则和限制过多的重要保护条款会影响数据保护的充分性和确定性。欧洲法院虽然可以通过数据保护合法性、比例性和目的限制原则来进行规制,但是模糊的措辞可能导致实践中的扩大适用,分类规则可能因为技术的发展而失去原本的效果,过于原则的规定难以遏制因技术缺陷带来的不利影响。此外,预测性警务存在透明度缺乏、算法和适用歧视等风险和局限。虽然该技术在不断发展和完善,能够为公共安全治理做出一定的贡献,但至少现阶段应该更谨慎地使用,不能将其作为安全治理的主要手段。笔者认为,预测性技术的使用关键在于其设计意图和实施方式,个人、群体和社会权利受影响的原因也在于此。它可以与强制权力结合使用,发展警察的事前控制能力,导致执法前置化,公民权利面临侵入性风险;也可以转换思路,重点从强制执行层面转换到预防层面,与预防犯罪的其他更柔和、更贴近社会现实的方法结合使用,从基础上改善公共安全。归根结底,预测性警务虽然能加强执法机构的控制能力,使识别高危罪犯变得更加容易,但无助于解决犯罪产生的复杂社会原因。但是,从当前的形势来看,预测性技术的开发和适用是执法领域重要的发展趋势,欧洲乃至世界各国不会放弃强化执法的预防功能这条改革路径。因此,从欧盟个人权利保护的角度来说,需要强调目的限制原则,加强技术的透明度,通过认证和追踪提高数据的准确性,以弥补数据保护法律框架的不足。

(**作者简介:**魏怡然,中南财经政法大学教师、中南财经政法大学法治发展与司法改革研究中心青年专家;**责任编辑:**莫伟)