International Review of the Red Cross (2017), **99** (1), 179–209.
Migration and displacement
doi:10.1017/S1816383117000637

INTERNATIONAL REVIEW of the Red Cross

移民和数据保护：流离失所问题严重、监控无处不在和“大数据”的时代背景下，“不伤害”原则的坚守

本·海耶斯

本·海耶斯，驻英国研究员、顾问，在反恐、国际安全、边境控制、治安维持、人道行动以及研发框架等领域研究人权、数据保护和应用伦理。他曾为红十字国际委员会、红十字会与红新月会国际联合会、联合国难民事务高级专员公署 (难民署)、欧盟委员会和其他公共和私人部门组织开展数据保护的影响评估和设计数据保护框架。他目前为跨国学会的研究员，和平研究所 (奥斯陆) 和人类安全集体 (Human Security Collective) 的助理研究员，以及数据保护支持与管理有限公司 (Data Protection Support & Management Ltd.) 的董事。

摘 要

本文探讨了人道组织在向难民、国内流离失所者和移民提供援助的过程中，在数据保护方面面临的主要挑战。对人道组织而言，由于下列几项原因，

这些挑战尤其严峻：人道领域开始重视数据保护的时间相对较晚；人道组织正在面临需要快速创新的压力；很多这些创新所依赖的全球通信架构在本质上容易受到国家监控；各国正在部署日益先进的强制手段阻止非正常移民，并且/或者迫使人道组织接受监控，其工作受到影响。本文第一部分概述了当今数据驱动的移民控制模式给基本权利带来的诸多挑战。第二部分概述“数据驱动的人道主义”和“大规模监控”方面令人担忧的问题，显示人道组织如何可能在无意间使这些问题更加严重。第三部分评估了人道组织所面临的具体数据保护方面的挑战，介绍了它们为应对这些挑战而采取的政策和做法。文章最后简要描述了人道组织在遵守法律和履行道德义务方面的技术和政治动态，并呼吁整个领域共同努力，扩大数据保护规范的适用范围，禁止国家网络攻击行为。

关键词：移民、边境控制、入境、庇护、难民、监控、审查、大数据、人道行动、数据保护、隐私、人权。

> 当你抵达难民营时，已饥肠辘辘，内心绝望，如果要获得食物和基本必需品，你就必须同意提供生物特征数据，接受虹膜和指纹扫描。几年之后，在你生活的国家，通过了一项新法律，主张对曾帮助你的组织存储在云端的数据拥有管辖权。通过提取你的指纹，安全部门现在不仅可以知道你的种族或移民身份，还可以知道你的行踪、消费模式和财务状况。在某些情况下，数据的收集的同时，压力立即出现。“人道数据”被收集用于人道之外的用途，例如，反恐或移民流动管理 (虽然从特定角度看，可以理解也相当重要)，那么相关个人可能需要承担不利的后果，尽管这些后果可能是法律规定的结果 (例如，被捕、被拒绝入境等)。[1]

1 AnjaKaspersen and Charlotte Lindsey-Curtet, “The Digital Transformation of the Humanitarian Sector”, *Humanitarian Law & Policy Blog*, 5 December 2016, available at: blogs.icrc.org/law-and-policy/2016/12/ 05/ digital-transformation-humanitarian-sector/ (所有互联网参考资料的获取时间均为2017年8月)。

导 言

本文探讨了人道组织在向需要支持的难民、国内流离失所者和移民提供援助过程中，在数据保护方面面临的主要挑战。这些挑战很重要，原因有很多，但其中四点按照本文所讨论的框架尤为重要。第一点是简单的事实，即人道领域对数据保护关注得相对较晚。这并非指人道组织过去没有认真对待数据保护有关的问题，例如，受益人的同意、数据准确性和保密性。这些尽管有时在执行上仍有欠缺，但显然早已纳入人道组织的操作规程。问题是人道领域作为一个整体，只是刚开始采用和遵循国际数据保护规范。尽管人道组织被隐私倡导团体点名批评，[2]有些被迫采取补救措施，确实是因为没跟上隐私和数据保护法律发展的步伐，但另一方面，也是因为数据保护（包括全套法律标准以及推动变革的团体）以往一直极少提及人道行动，至少是相对于其他领域而言。[3]

数据保护领域对人道行动缺乏关注，是必须重视的问题，因为人道工作者经常需要应对的紧急情况或冲突有其自身的一些特征，人道组织在实际应用数据保护的关键原则方面因此会面临巨大挑战。虽然人道行动经常发生在无人治理或治理不善的地区，数据保护看起来可能是最不重要的事项，但这些挑战并未脱离更广泛的社会、政治或法律背景。相反，人道组织在向移民和难民提供人道支持的全球秩序大背景，现在的特点表现为对移民和边境控制的要求日益严格——在这一要求在实践中导致了数据驱动的“移民管理”技术愈发先进，进而产生了自身的一系列人权和数据保护挑战。这是构建本文框架的第二个主要问题。

人道组织必须应对这些发展的后果，主要是作为受益者的权利和最佳利益的维护者，但也越来越多地作为同一（“可互相操作的”）技术的使用者，

2 Anna Crowe, “A Paucity of Privacy: Humanitarian, Development Organisations Need Beneficiary Data Protection Policies”, *Privacy International,* 28 November 2013, available at: www.privacyinternational. org/node/240.

3 1990年联合国大会制定的“电脑个人数据文件的管理准则”在这方面是一大例外，但这些早期的数据保护准则适用于联合国电脑系统，而不是人道行动本身 (*per se*)。见联合国大会，第45/95号决议，1990年12月14日。

以及政府的合作伙伴，同时还在数据方面享有多重利益。那些正在创新和利用“数据驱动的人道主义”带来的机遇的人道组织[4]，还必须应对一个容易受到国家和非国家监控和渗透的全球通信基础设施。由于不管是友好国家还是敌对国家的情报机构，均将人道组织视为潜在目标，因此下文讨论的第三项主要挑战是人道组织可能沦为“监控的帮凶”。

这项挑战与第四项挑战有关：各类技术的应用正在形成21世纪国际人口流动和提供援助的格局，但借用马克思的说法，[5]这些应用具有内在的“双重人格”。从安全的边境到犯罪预测，再到有效确定援助目标，大数据的承诺包罗万象。入境和获取人道援助已经受到各项监控和社会分类政策，以及包容、排斥和社会控制等实践的影响，且这些影响会日益增强。

对于坚持“不伤害”原则的人道组织而言，所有这一切对其行动和声誉，以及受益人的基本权利和安全，都有着至关重要的现实后果。在发达国家，数据泄露会给受影响的人带来不便或严重经济损失；对难民及其国内家人而言，数据泄露有可能危及生命。[6]面对爱德华·斯诺登[7]所揭露的“大规模监控”，以及美国总统唐纳德·特朗普所要求的“极端审查”，[8]数据保护措施似乎显得软弱无力，尽管如此，健全的数据保护政策和做法属于唯一可行的方法，各人道组织必须负责任地进行创新，防范数据丢失或网络攻击而可能导致的名誉损害，减轻大数据和政府的强制政策所带来的巨大挑战。[9]

---

4 See, for example, Patrick Meier, “New Information Technologies and Their Impact on the Humanitarian Sector”, *International Review of the Red Cross,* Vol. 93, No. 884, 2011.

5 这一类比本身借用自：Thomas Mathiesen, *On Globalisation of Control: Towards an Integrated Surveillance System in Europe,* Statewatch, London, November 1999, p. 1.

6 A. Kaspersen and C. Lindsey-Curtet, 上文脚注1.

7 爱德华·斯诺登以举报人的身份，向英国《卫报》和美国《华盛顿邮报》的记者提供了一批情报文件。这些文件披露了美国及其澳大利亚、英国和加拿大合作伙伴的全球监控计划的运作细节，这两家报纸因为相关报道获得了普利策奖。

8 Sabrina Siddiqui, “Trump Signs ‘Extreme Vetting’ Executive Order for People Entering the US”, *The Guardian,* 27 January 2017, available at: www.theguardian.com/us-news/2017/jan/27/donald-trumpmuslim-refugee-ban-executive-action.

9 关于大数据带来的各项挑战，见Frank Pasquale, *The Black Box Society: The Secret Algorithms that Control Money and Information,* Harvard University Press, Cambridge, MA, 2015; Cathy O’Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy,* Penguin, London, 2016; GryHasselbalch and PernilleTranberg, Data Ethics – The New Competitive Advantage, Publishare, Copenhagen, 2016.关于大规模监控和国家强制政策带来的挑战，见Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World,* W. W. Norton, New York, 2015.

本文主要分为三个部分。第一部分在本导言的基础上，概述了当今国际移民控制的一些关键特征及其对基本权利构成的挑战。第二部分概述了人们对“数据驱动的人道主义”的担忧，并参考爱德华·斯诺登公布的文件，说明人道组织如何可能沦为“监控的帮凶”，在不经意间使这些问题更加严重。最后，针对对于人道创新的太多过度简单和哗众取宠的批判，第三部分试图开展更细致也相当必要的技术评估，指出为移民和难民服务的人道组织在数据保护方面遭遇的各项特别的挑战，概述了这些组织在应对挑战过程中形成的一些政策和做法。文章最后简要描述了人道组织在遵守法律和履行道德义务方面的技术和政治动态，并呼吁整个领域共同努力，扩大数据保护规范的适用范围，禁止国家网络攻击行为。

国际移民问题的安全化

在国际关系理论、批判安全学等社会科学学科中，“安全化”是将一个主题转化为“安全”问题的过程。[10]一旦以这种方式将问题政治化，原本被决策者认为过激的措施，或其他不可接受的措施，可能以一定的方式而得到采用和正常化。若不是以安全 (不管是否真的安全) 为由，便无法如此采用或正常化这些措施。尽管“安全化”理论的正当性和效用备受争议，[11]但在公共政策中，实难找到比国际移民、庇护和边境控制更为“安全化”的领域。事实上，即使是最常出入机场的旅行者，也一定难以从自己最近的记忆中，回想起一个基本上仍属于行政管理性质的移民手续，如今遍布机场检查点的人体扫描仪仍仅存在于科幻小说之中。

虽然移民长期以来与生存息息相关，但合法移民始终与特权联系在一起，并受到主流意识形态和权力结构的影响，签证制度和入境审核政策与殖

10 关于此类“安全化”理论的来源，见Barry Buzan, Ole Wæver and Jaap de Wilde, *Security: A New Framework for Analysis,* Lynne Rienner, Boulder, CO, 1998.

11 See Columba Peoples and Nick Vaughan-Williams, *Critical Security Studies: An Introduction,* Routledge, New York, 2010.

民、种族和法西斯密不可分。[12]今天，“移民”、“难民”和“非法”在政治话语中被集体客观化，前所未有地成为“国家安全”的现实问题。虽然显而易见，但还是要提醒读者注意，在如此复杂和高度政治化的领域，下文的简要概述绝然无望伸张正义，[13]因此本节只是强调指出，一个以“数据”为核心、但数据保护的关键原则无足轻重或被弃之不顾的总体政策框架，主要表现出哪些特征。这些特征是：边境控制与反恐的结合；身份管理新技术；世界范围内移民控制措施的扩散；外包和威权；加强的安全审查；以及相关人权文书的适用受限。

将移民—恐怖分子联结

这些特征中的第一个是2001年9月11日美国发生恐怖袭击后，移民控制与反恐的合并。尽管没有任何统计数据表明，“本土”产生的恐怖分子威胁大于移民带来的威胁，[14]或在美国，一个人更可能被警察或蹒跚学步的孩子杀害，而不是被恐怖分子杀害，[15]但边境现在已被广泛视为反恐的第一道也是最重要的一道防线。正如时任美国总统的乔治·W·布什在2002年所说：“我们需要知道谁将进入我们的国家，他们为何而来，是否真在自己声称的时间离开。“[16]这一主张代表一种新的正统观念，所有关于边境控制的政策辩论都可能因此且不可避免地减少。

12 See Liz Fekete, “The Emergence of Xeno-Racism”, *Race & Class*, Vol. 43, No. 2, 2001; Steve Cohen, *Standing on the Shoulders of Fascism: From Immigration Control to the Strong State,* Trentham Books, London, 2002; Liz Fekete, *A Suitable Enemy: Racism, Migration and Islamophobia in Europe,* Pluto Press, London, 2009; Marjory Harper and Stephen Constantine, Migration and Empire, Oxford University Press, 2010; LiliEskinazi, “European Immigration: A Colonial Legacy?”, *Alternatives International Journal,* 31 October 2011, available at: www.alterinter.org/spip.php?article3694.

13 本文并不寻求或声称提供一种关于监控或移民控制的理论。还应强调的是，监控可能是在该领域中引进的一系列国家和国际政策的副产品和动机。同样，本文没有提及推动这一领域中各项发展的其他因素——例如，移民模式、国内政治、技术进步和官僚提高效率的冲动，并不意味着认为这些因素不重要。最后，移民控制并非处处相同，也许会有一个明确的前进方向，但前进路线的特点是“脱节的渐进”。该术语出自政治学家查尔斯·E·林德布卢姆 (Charles E. Lindblom) 1959年发表的一篇文章：“The Science of ‘Muddling Through’”, *Public Administration Review,* Vol. 19, No. 2, 1959.

14 Alex Nowrasteh, *Terrorism and Immigration: A Risk Analysis,* Cato Institute, Policy Analysis No. 798, Washington, DC, 13 September 2016.

15 Gary Younge, “Trump Fears Terrorists, but more Americans are Shot Dead by Toddlers”, *The Guardian,* 8 February 2017, available at: www.theguardian.com/commentisfree/2017/feb/08/trump-muslim-terroristsgun-violence-america-deaths.

16 Adam Entous, “Bush to Seek New Powers in Homeland Security Plan”, *Reuters*, 15 July 2002.

这种言论绝不仅限于美国。针对911袭击，欧盟在立法方面首先做出的反应是达成一个打击恐怖的共同立场，要求成员国审查所有寻求庇护者是否与恐怖分子集团有关联，之后才能给予难民地位，[17]其本身参照了联合国安全理事会就同一主题做出的非约束性规定。[18]在随后的15年里，各行各业的旅行者都经历了越来越复杂的审查和建档程序，当局以此来评估和减轻其认为旅行者会带来的风险。这为当前美国政府要求的“极端审查”铺平了道路(详见下文)。

身份管理

第二个特征是第一个特征的必然结果。自911事件以来，各国采取了大量措施，试图控制移民。这些措施围绕着以部署生物特征识别系统为核心的身份管理技术展开。这些身份管理系统最初的重点是通过一种独特的生物特征识别信息，[19]确保旅行证件的持有者就是该证件的签发对象。现在，该系统正被纳入更广泛的执法和监控设备中。在有些国家，如英国和美国，由于公民自由的传统，强制性的公民指纹识别仍然是一个不可逾越 (但逐步后退) 的红线。除此之外，生物特征建档在世界各地广泛应用，对于“非公民”和“外国人”，已迅速成为一项标准做法，全然不顾这些传统的原则。[20]

如今，生物特征建档是全球边境控制的重要组成部分，而且随着这些系统的发展，其能力也在不断增强。所谓的“智能边境系统”可用来追踪跨地

17 Council Common Position of 27 December 2001 on Combating Terrorism, *Official Journal of the European Communities,* 2001/930/CFSP, 27 December 2001 (OJ 2001 L 344/90), Art. 16.

18 联合国安理会，第1373号决议，第3条第6款，2001年9月28日。

19 大多数用于边境和移民控制的生物特征识别系统使用数码照片、指纹或虹膜扫描，或综合利用其中两种识别信息。收集的生物特征基本信息会被输入人口数据库和/或储存在各国签发的旅行证件所附的射频识别芯片中。登记后，可根据数据库或旅行证件核对个人身份。国际民用航空组织负责制定全球航空旅行标准，该组织要求采用的唯一生物特征是数码照片。

20 事实上，欧盟早在911事件之前便决定对所有寻求庇护者和非正常移民进行生物特征建档，相关立法在1995年提出，最终于2000年获得通过。911事件后，欧盟决定对所有签证申请人、所有进入欧盟的免签第三国公民、所有合法居住的第三国公民和所有欧盟护照持有者实施强制指纹识别 (英国选择不参与该决定)。See KjetilRommetveit, “Introducing Biometrics in the European Union: Practice and Imagination”, in Ana Delgado (ed.), *Technoscience and Citizenship: Ethics and Governance in the Digital Society,* Springer, Cham, 2016.

区的个人，[21]而存储生物特征的数据库已经向国家安全和执法机构开放。[22]获得核准的旅行者似乎已经接受了生物特征建档作为通行的一个条件（当然，这并非出于其自己的选择），在更为强制情况下使用生物特征——例如在欧盟，关于庇护和驱逐政策的国家责任认定——导致出现耸人听闻的事件，有难民和移民为避免移民强制措施，不惜切断自己的指尖。[23]作为回应，各国已开始将不向移民官员提供指纹的行为定为犯罪。[24]尽管这种象征意义令人震惊，但现实情况是，为防止非正常移民进入而采取的越来越严格的措施，长期以来都是与回避这些移民的日益“极端”的企图共同发展起来的。

移民控制措施的全球扩散

这一现象也反映在移民控制技术从目的地国向原籍国和过境国的转移，这种转移是通过技术援助、移民管理协定以及援助与贸易一揽子方案进行的。这些措施采取各种形式，从实行所谓的“边境前检查”和重新接纳义务，到往往由政府间组织提供便利的政策和技术转让。

虽然随着富裕国家逐渐设法防止或控制来自贫穷国家的移民，人们可能认为，更严格的移民控制措施只是发展和现代化的必然产物，但世界上最富有的国家也在非常有意地输出这些控制技术。这样做有双重动机：首先，争取移民和难民原籍国和过境国的支持，建设其能力，阻止富裕国家不欢迎的无证移民到达这些国家，并迅速遣返那些千辛万苦来到边境的移民（欧盟-土耳其达成的难民协议是该政策执行上最显著的示例[25]）；其次，协助收集入境

21 See Ben Hayes and Mathias Vermeulen, *Borderline: The EU's New Border Surveillance Initiatives – Assessing the Costs and Fundamental Rights Implications of EUROSUR and the "Smart Borders" Proposals,* research study, Heinrich Böll Foundation, Berlin, 2012.

22 例如，在欧盟，每一个主要的移民和庇护数据库（包括申根信息系统、欧洲指纹资料库（Eurodac System）、签证信息系统和拟议的“智能边境”系统）的主要立法后来都被修改，为安全和情报机构提供访问权限。See CosticaDumbrava, "European Information Systems in the Area of Justice and Home Affairs: An Overview", *European Parliamentary Research Service,* May 2017, available at: www.europarl.europa.eu/RegData/etudes/IDAN/2017/603923/EPRS_IDA (2017) 603923_EN.pdf.

23 See, for example, Graeme Culliford, "I've Burned off Tips of My Fingers to Get to UK", *The Sun,* 14 June 2014, available at: www.thesun.co.uk/archives/news/900339/ive-burned-off-tips-of-my-fingers-to-get-touk/.

24 See EU Fundamental Rights Agency, *Fundamental Rights Implications of the Obligation to Provide Fingerprints for Eurodac,* Vienna, May 2015.

25 Council of the European Union, "EU-Turkey Statement", Press Release No. 144/16, 18 March 2016.

旅客的资料，以及收集其他有关人士的情报。欧盟及其成员国一直在这个领域最为活跃，向许多国家提供技术援助，涵盖中部和东部欧洲、西部和北部非洲、中东，在总是产生难民“危机”的剧烈武装冲突期间，甚至涵盖远离欧洲的斯里兰卡。[26]这种援助的内容也包罗万象，涵盖移民和庇护系统、边境控制基础设施、移民官员和边防部队的培训、拘留中心和反对非法移民的宣传运动。它甚至违反了联合国《人权宣言》中关于自由流动的规定，包括防止“未经核准离开”方面最为强制性的措施。[27]

美国也在该领域提供大量技术援助，包括用于移民控制系统的技术和资金，受援助国家包括阿富汗、柬埔寨、埃塞俄比亚、加纳、肯尼亚、马尔代夫、巴基斯坦、坦桑尼亚和也门。[28]面对如此慷慨的援助，受援国的一位政府部长表示，美国提供援助，就是要为“美国影响力留一扇门”，让美国能够随时掌握外国人的行踪。[29]且不论动机如何，正如下文将进一步讨论的那样，边境控制、身份管理和国家安全之间的内在关系意味着，这种技术援助经常引发在捐助国或受援国很少讨论的人权问题。

责任化、私有化和权威主义

除了富裕国家几乎毫不掩饰地试图将其对难民和寻求庇护者的责任推卸给较贫穷国家之外，当代移民控制的特点是私人部门越来越多地参与本国和国际执法。[30]例如，欧盟国家对运输公司强加了法律义务，规定运输公

26 See Ben Hayes, Steve Wright and April Humble, “From Refugee Protection to Militarised Exclusion: What Future for ‘Climate Refugees’?”, in Nick Buxton and Ben Hayes (eds), *The Secure and the Dispossessed: How the Military and Corporations Are Shaping a Climate-Changed World,* Pluto Press, London, 2015.

27 例如，欧洲国家向利比亚海岸警卫队提供了武装船只。See Maurizio Albahari, *Crimes of Peace: Mediterranean Migrations at the World’s Deadliest Border,* University of Pennsylvania Press, Philadelphia, 2015, p. 88.See also Maggie Michael, “Backed by Italy, Libya Enlists Militias to Stop Migrants”, *Associated Press*, 29 August 2017, available at: www.apnews.com/ 9e808574a4d04eb38fa8c688d110a23d.《世界人权宣言》指出，“人人有权离开任何国家，包括其本国在内”；见《世界人权宣言》第13条第2款，1948年12月10日，第217A (III) 号决议。

28 See Ben Hayes and RochTassé, “Control Freaks: ‘Homeland Security’ and ‘Interoperability’”, *DifferenTakes: A Publication of the Population and Development Programme at Hampshire College,* No. 45, Spring 2007.

29 马尔代夫国防和国家安全前国务部长伊利亚斯·侯赛因·伊卜拉欣 (IlyasHussain Ibrahim), cited in Gus Hoseinand Carly Nyst, *Aiding Surveillance,* Privacy International, London, 2013,p.55, availableat: www.privacyinternational.org/node/310.

30 See Thomas Gammeltoft, “The Migration Control Industry”, in Rita Abrahamsen and Anna Leander (eds), *Routledge Handbook of Private Security Studies,* Routledge, London, 2016.

司有责任防止无证件或证件不适当的乘客入境。从航空公司到卡车司机，未能阻止未经核准的旅行者通行，往往会导致巨额罚款，即所谓的“承运人制裁”。[31]令人震惊的是，私人参与遇险的移民船只援助同样也受到威胁和起诉的限制，因为只要救助对象没有立即被淹死的危险，救助者均可能受到起诉。[32]

更广泛而言，随着各国越来越严重地依赖大规模计算机系统和监控技术，私人部门在开发和执行移民和边境控制政策方面也不断增加投资。国防和科技部门从这些安排中获益最多，主要的国防承包商现在的收入有很大一部分来自它们进入所有“国土安全”领域的业务多样化。[33]除了提供大量加强边境和广泛地区监控的合同外，刑事司法领域的私人化使私人部门在诸如拘留移民和执行驱逐政策等领域获得越来越多的立足点。[34]边境控制和移民执法的公司化不可避免地将效率和利润置于其他价值和利益之上，例如问责机制和人权保护。

最后，最初强加给运输部门的义务一直在稳步扩展适用到公共和私人生活的其他领域，房东、雇主、银行、大学、学校和卫生服务工作者承受越来越多的法律义务，参与对其客户的执法，检查客户的移民身份，不严格履行这些义务者会受到重罚。在打击非法移民的“斗争”中，公众和私人行为体被日益工具化，虽然这一点尚未得到不加批判的接受，[35]但对致力于消除歧视和保障普遍人权的组织仍具有重要影响。

31 See Sophie Scholten, *The Privatisation of Immigration Control through Carrier Sanctions,* Brill, Leiden, 2015.

32 See Maarten den Heijer, “Frontex and the Shifting Approaches to Boat Migration in the European Union: A Legal Analysis”, in Ruben Zaiotti (ed.), *Externalizing Migration Management: Europe, North America and the Spread of “Remote Control” Practices,* Routledge, London, 2016.See also IriniPapanicolopulu, “The Duty to Rescue at Sea, in Peacetime and in War: A General Overview”, *International Review of the Red Cross,* Vol. 98, No. 902, 2016.

33 See Mark Akkerman, *Border Wars: The Arms Dealers Profiting from Europe’s Refugee Tragedy,* Transnational Institute, Amsterdam, 2016, available at: www.tni.org/en/publication/border-wars.

34 见全球拘留问题研究项目的报告和网站，网址：www.globaldetentionproject.org/.

35 其中包括医疗专业人员和大学工作人员，即使法律有要求，这些人仍抵制或拒绝开展此类检查。See, for example, Miranda Wilson, “Academics Refuse to Police Immigration”, *Institute of Race Relations News,* 13 May 2009, available at: www.irr.org.uk/news/ academics-refuse-to-police-immigration/.

极端审查

上述四项特征构成了最重要的第五个特征：集中大量个人数据，以便对旅行者和移民进行审查、建档和最终分类：是合法的还是可疑的、是应得的还是非应得的、是有权入境的还是应被阻止的，等等。如上所述，911事件在很大程度上推动了这一运动，因为首先收紧的是对难民和寻求庇护者的规定，然后是对签证申请人的规定，最后是对免签旅行者的规定。

所有这一切实现的方式包括引入生物特征签证，申请人在申请时便会被登记和审查；[36]引入旅客订座记录信息披露制度和先进的旅客信息系统，执法和安全机构在旅行开始之前便会收到详细的旅行者信息，[37]以及旅行核准电子系统，在旅行者获准登上入境航班之前，预先筛选旅行者。[38]审查主要是秘密进行，但据已知的信息包括开展检查，确保旅行者满足入境条件，没有违反移民法的记录，对照国家安全和反恐数据库进行筛查，如“禁飞”名单、“观察名单”、制裁和外交政策清单。[39]数据也定期与其他国家分享，例如通过申根、“五眼”以及其他双边和多边安全合作框架。[40]

虽然欧洲小报一直难以接受一个拥有智能手机的人还需要难民保护，[41]但欧洲各国政府抓住机会，模仿美国和以色列边境部队没收这类设备的做法，推行一些自己的“极端审查”措施。[42]在2017年初，丹麦和挪威提出了

36 例如，欧盟签证信息系统就是如此。

37 澳大利亚率先使用先进的旅客信息系统，而根据欧盟法律，安全和情报机构可以访问欧洲航空公司预订数据库中的旅客数据 (旅客订座记录)。

38 美国实行旅行核准制度，而欧盟计划引入这一制度。

39 关于这些系统应该如何运作的解释，见UK House of Commons, Committee of Public Accounts, “E-Borders and Successor Programmes”, 27th Report of Session 2015–16, London, 2016.See also JulienJeandesboz, Didier Bigo, Ben Hayes and Stephanie Simon, *The Commission's Legislative Proposals on Smart Borders: Their Feasibility and Costs,* PE 462.613, European Parliament, Brussels, 2013.

40 《申根公约》缔约国汇集了通过申根信息系统被拒绝入境或接受监控检查的人员的数据，并通过“Sirene网络”交换补充数据。“五眼”指是由澳大利亚、加拿大、新西兰、英国和美国组成的战后情报联盟。2009年，这些国家通过了一项关于生物特征的“五国会议数据共享协议”(未公开)。国际刑事警察组织 (国际刑警组织) 也为交换用于边境控制的数据提供便利。

41 See James O'Malley, “Surprised that Syrian Refugees Have Smartphones? Sorry to Break this to You, but You're an Idiot”, *The Independent,* 7 September 2015, available at: www.independent.co.uk/voices/ comment/ surprised-that-syrian-refugees-have-smartphones-well-sorry-to-break-this-to-you-but-yourean-idiot-10489719.html.

42 关于美国的情况，见Olivia Solon, “US Border Agents are Doing 'Digital Strip Searches'. Here's How to Protect Yourself”, *The Guardian,* 31 March 2017, available at: www.theguardian.com/us-news/2017/ mar/31/ us-border-phone-computer-searches-how-to-protect;关于以色列的情况，见 “Israel Approves Email Checks at the Border”, *Times of Israel,* 24 April 2013, available at: www.timesofisrael.com/israelapproves-email-checks-at-the-border/.

一份草案，提议在难民登记时没收其智能手机，并使用这些手机上的数据来评估寻求庇护者构成的安全威胁以及其庇护申请的可信度。[43]这些建议引起人们对庇护程序的重大关切，是对寻求庇护者私生活的空前侵犯。

隐私和数据保护：在边境处形同虚设

那么，原本应该约束各国肆无忌惮监控行为的隐私权和数据保护究竟发挥了怎样的作用？简而言之，由于对“必要和相称”限制的定义过于宽泛，隐私权已被证明相对无效。[44]这在很大程度上是由于一些国家的歧视性做法，认为外国人享有的隐私权应比本国公民少。[45]至于数据保护方面，按规定应该能够约束公共和私人部门对个人数据的处理，并赋予数据主体相关权利，令其有权对与自己有关的数据施加控制，以及在滥用数据时寻求补救，但由于受地域限制，安全和公共政策方面违反数据保护规定的情况更为严重。[46]虽然现在有100多个国家制定了某种形式的数据保护法律或规定，[47]但其中许多并不属于全面的数据保护机制以及/或者远低于欧洲制定的最高标准 (首先由欧洲委员会制定，之后由欧盟制定)。[48]

43 关于丹麦，见2017年2月10日关于修改《丹麦外国人法》的未公开提案，由作者存档。关于挪威，见2017年1月11日的提案 (挪威文)，网址：www.regjeringen.no/contentassets/8c99986c9bd444b6a00d56fe8afca077/visitasjon-horingsnotat-januar-2017.pdf.

44 Article 8 (2) of the European Convention for the Protection of Human Rights and Fundamental Freedoms, ETS 5, 4 November 1950 (1953年9月3日生效)，关于私人和家庭生活的权利，认为“公共当局不得干扰此项权利的行使，但在一个民主社会中，出于国家安全、公共安全或者国家的经济福利、防止混乱或犯罪、保护健康或道德、或保护他人权利和自由的需要而依法采取的行动除外。”关于哪些属于“必要和相称”的通信监控，见Necessary and Proportionate Coalition, “Necessary & Proportionate: International Principles on the Application of Human Rights to Communications Surveillance”, May 2014, available at: www. necessaryandproportionate.org/principles.关于欧洲联盟法院最近的判决中，开始限制这类允许例外的普适性，见*Tele2 and Watson,* Joined Cases Nos C-203/15, C-698/15; *Schrems v. DPC Irl,* Case No. C362/14; and *Digital Rights Ireland and Seitlinger,* Joined Cases Nos C-293/12, C-594/12.

45 See Marko Milanovic, “Foreign Surveillance and Human Rights, Part 1: Do Foreigners Deserve Privacy?”, *EJIL: Talk! Blog of the European Journal of International Law,* 2013, available at: www.ejiltalk.org/foreignsurveillance-and-human-rights-part-1-do-foreigners-deserve-privacy/.

46 虽然数据保护常被视为个人数据相关隐私权的附带要求，但它日益被确认为一项基本的宪法权利。See, for example, Charter of Fundamental Rights of the European Union, 2012/C 326/02, 26 October 2012, Art. 8.

47 See DLA Piper, “Data Protection Laws of the World”, available at: www.dlapiperdataprotection.com/.

48 See, for example, CoE, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS 108, 28 January 1981 (entered into force 1 October 1985); Regulation of the European Parliament 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, 2016/679/EU, 27 April 2016 (GDPR).

至关重要的是，即使这些高标准有朝一日得以适用，但如果是按法律处理数据，或出于国家安全的需要，则数据保护原则中关键的个人同意和选择的规定要么不适用，要么无法适用，对自身数据主张控制的权利也会受到根本性限制 (例如，关于数据访问、纠正和删除的权利)。[49]目前，人们普遍认为旅行和移民数据交给国家安全机构“理所应当”，突显出这些重大例外规定的影响。就欧盟的大量边境控制提案，欧盟数据保护监管机构在2008年做出重要回复，表示“基本假设”是“所有旅行者”均应被“事先视为潜在违法者”，并应“受到监控”的做法令人担忧，可惜这样的回复大多被置若罔闻。[50]

监控的帮凶?

如导言部分所述，国家采取的上述强制做法对人道组织有重大影响。人道组织在开展活动和创新的过程中，如不采取严密的数据保护保障措施，便有可能加剧大规模监控和数据驱动移民管理所带来的基本权利问题。倡导组织国际隐私组织 (Privacy International) 2013年一篇名为《监控的帮凶》(Aiding Surveillance) 报告中，阐明了这些担忧。该报告考察了“发展和人道援助举措在发展中国家实现监控的方式”。[51]报告集中注意发展和人道领域的四个创新领域：(1) 现金转账计划背后的信息系统；(2) 生物特征识别和投票人登记系统；(3) 使用手机及其收集和产生的数据，用于移动货币、保健服务和危机管理等目的；(4) 边境监控和安保技术。

以数十个示例为依据，这份报告发现，虽然基础技术“近年来在发达的西方民主国家已得到广泛辩论”，[52]但“对于在发展和人道行动中部署技

49 关于数据保护关键原则的综述，见European Union Agency for Fundamental Rights and Council of Europe – European Court of Human Rights, *Handbook on European Data Protection Law,* 2014, available at: www.fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_ en.pdf.

50 European Data Protection Supervisor, *Preliminary Comments of the European Data Protection Supervisor,* Brussels, 3 March 2008, p. 5, available at: https://edps.europa.eu/sites/edp/files/publication/08-03-03_comments_border_package_en.pdf.

51 G. Hosein and C. Nyst, above note 29.

52 同上，第8页。

术可能产生的不良影响，在批判性思考方面存在系统性失败，进而也未能考虑需要采取哪些法律和技术保障措施，以维护生活在发展中国家的个人的权利”。[53]联合国各机构、捐助国、国际非政府组织、发展和人道组织因此受到批评并不过分。虽然像联合国人道事务协调厅 (OCHA) 的战略性文件《网络时代的人道主义》(*Humanitarianism in a Networked Age*) [54]以及联合国2015年后发展议程高级别知名人士小组的《一种新型全球合作伙伴关系》(*A New Global Partnership*) [55]颇具开创性，但也被批评“对采用新技术和数据分析技术对个人隐私的潜在影响缺乏关注”。[56]最后，该报告警告说，援助领域所钟爱的“不伤害”方法可能将人权保护的标准定得太低。报告建议，设定的目标不应只是避免危害受益者的人权，而是应积极促进和保护人权。[57]

除了负责任地进行创新之外，人道组织也面临着因为监控做法被暴露而产生的另一项挑战。移动电话及之后智能手机数量的迅速增长[58]，不仅极大地便利了通信，也让需要人道组织支持的移民和难民获取保护和援助的机会大增。然而，正如本文导言所述，它也为政府监控提供了大量机会，人们因为自身处境容易被发现或虐待的情况下，看待和使用信息和通信技术的方式会因此受到重大影响。一些人道组织似乎无视这些顾虑，认为需要援助的人乐意把个人数据交给任何要求数据的人，或认为隐私基本上是西方的概念，在其他文化或环境下，没有什么吸引力。然而，英国开放大学 (Open University) 和法国世界媒体集团 (France Médias Monde) 对前往 (*en route*) 欧洲的移民和难民使用智能手机和社交媒体网络的深入研究表明，这种观点

53 同上，第7页。

54 OCHA, *Humanitarianism in the Network Age,* OCHA Policy and Study Series, Geneva, 2013.

55 UN, *A New Global Partnership: Eradicate Poverty and Transform Economies through Sustainable Development: The Report of the High-Level Panel of Eminent Persons on the Post-2015 Development Agenda,* 2013, New York, 2013.

56 G. Hosein and C. Nyst, 上文脚注29, 第9页.

57 同上，第56~58页。Also see Kristin BergtoraSandvik, KatjaLindskov Jacobsen and Sean Martin McDonald, “Do No Harm: A Taxonomy of the Challenges of Humanitarian Experimentation”, in this issue of the *Review.*

58 根据英国开放大学和法国世界媒体集团开展的研究，“中东和北非98%的人口使用手机、84%使用智能手机、81%可接入互联网、51%使用‘高端’设备 (即500美元以上)”。See Marie Gillespie *et al., Mapping Refugee Media Journeys: Smartphones and Social Media Networks: Research Report*, Open University and France Médias Monde, 13 May 2016, available at: www.open.ac.uk/ccig/research/projects/mapping-refugeemedia-journeys.

并不正确。[59]尤其 (*inter alia*) 是调查发现，“由于难民恐惧政府等传统机构的监控和其他团体成员的监控[原文如此]”，难民会“在社交媒体和网络上使用假身份和假名，掩饰自己的真实身份”；[60]“难民不会在线分享个人信息，而是保持匿名，因为害怕报复、监控、拘留及/或遣返”；[61]与家人和朋友沟通时，“主要使用Whatsapp，因为难民们相信Whatsapp不像推特和脸书 (Facebook) 账户那样受到监控”。[62]由于对政府和国家资助的机构和组织缺乏信任，难民们“转向非官方的、具有潜在危险的和剥削性的资源”。[63]远离“欧洲堡垒”军事化边境和不熟悉数据保护概念的受益群体也对不同行动体是否有能力以可能不符合其最佳利益的方式使用信息表示严重关切。[64]

沦为“监控帮凶”的风险还不止于此。2013年，举报人爱德华·斯诺登向记者披露了大量文件，其中一些显示，国家安全局和政府通信总部 (Government Communications Headquarters)——分别作为美国和英国重要的监控和情报机构——已将人道组织列为监控目标。通信被截获的机构包括联合国儿童基金会、联合国开发计划署和世界医生组织。[65]可以很有把握的假定，如果英国和美国这样做，其他有能力的国内外情报机构也会把人道组织

59 同上。

60 同上，第13页。该研究强调：“必须强调，在对难民的访谈中，信任和保密问题至关重要。害怕受到监控和曝光——甚至是被其他难民，而不仅仅是法国当局——是难民在回答访谈问题时以及在访谈前后进行的非正式对话中遇到的一个关键障碍。”同上，第43页。

61 同上，第17页。

62 同上，第48页。

63 同上，第13~18页。也考虑了欧盟边管局的建议。它作为欧盟的边境管理机构，建议开发一款智能手机应用程序，确保穿越地中海人员的安全。移民权利团体和隐私保护组织指出，难民显然不太可能接受一项让欧洲政府更容易对其进行跟踪和拦截的应用程序。See Diane Taylor and Emma Graham-Harrison, “EU Asks Tech Firms to Pitch Refugee-Tracking Systems”, *The Guardian,* 18 February 2016, available at: www.theguardian.com/world/2016/feb/18/eu-asks-tech-firms-to-pitchrefugee-tracking-systems.

64 作者2015年在加沙进行的一项未发表的研究 (由作者存档) 发现对数据保护的强烈关切，表现形式是人们对国际非政府组织和国际组织进行调查和收集个人信息 (包括姓名和身份证件) 感到沮丧，希望永远不再接受调查。这反过来又引起当地社区的怀疑，越来越不信任这些组织的动机。

65 See James Ball and Nick Hopkins, “GCHQ and NSA Targeted Charities, Germans, Israeli PM and EU Chief”, *The Guardian,* 20 December 2013, available at: www.theguardian.com/uk-news/2013/dec/20/ gchq-targeted-aid-agencies-german-government-eu-commissioner.See also Joan Tilouine and Simon Piel, “British Tapped UN and NGO Phones and Emails in Nigeria and Congo”, *Le Monde,* 8 December 2016, available at: www.lemonde.fr/afrique/article/2016/12/08/british-tapped-un-and-ngophones-and-emails-in-nigeria-and-congo_5045681_3212.html.

锁定为目标。这对人道组织的行动及受益人亦有重大影响。虽然被动接受大规模监控的人会认为“世道如此”，会以天真的假设自我安慰，认为这些监控很大程度上是被动的，只是为了监控而监控，但同样清楚的是，各种力量已处于准备就绪状态，能够在追求政治或军事优势的过程中，干扰人道组织的活动。这可能包括定位或收集目标或对手的情报、影响平民人口或破坏援助物资的分发等。此外，尽管人们可能意识到共享个人信息所涉及的风险，但对“元数据”收集和监视所涉及的风险却知之甚少。[66]这又提出了一些重要的问题，即人道组织在多大程度上必须承认使用新技术提供援助的内在风险，并据此向受益人提供建议，这是其保护职责的一部分。

红十字国际委员会工作人员正在与其他人士一道，呼吁采取协调一致的行动来对付这些威胁。2016年红十字国际委员会博客上的一篇文章警告恶意的国家和非国家黑客攻击的危险，其中引用了一个假想的但现在已耳熟能详的例子：人道组织建立了一个线上平台，“众包”关于人道需求和侵犯人权的证据的实时数据，要我们想象一下，如该平台遭到黑客攻击或欺骗手法袭击，创建了一个谁正在攻击谁的虚假图片，则会发生什么。[67]该文章指出：“一次成功的黑客攻击可能迅速改变人们的看法，改变冲突的进程。”[68]该文章还指出，从医疗车队到设施再到工作人员，人道组织遭受的实际攻击持续增加，同时在此背景下，“情况正在发生变化，这些机构中立的声誉不再能保证得到保护”。[69]因此，“直接攻击一个机构的声誉，攻击者越来越能得到想要的结果”，能够“散布关于人道组织职责、影响和业务宗旨或工作人员意图的错误信息”。[70]不用说，这可能对人道组织的工作人员、安全、声誉和受益人造成毁灭性的后果。

2017年2月，微软总裁布拉德·史密斯 (Brad Smith) 提出一项呼吁，应制定第五个“关于数字的日内瓦公约 (Digital Geneva Convention)”，保护互联

66 “元数据”是关于数据的数据。通信元数据包括电话、电子消息、即时消息和其他通信模式的发生时间、持续时间、来源地和目的地的数据。这些信息可用于具体刻画一个人的位置、运动和外界联系。

67 A. Kaspersen and C. Lindsey-Curtet, 上文脚注1.

68 同上。

69 同上。

70 同上。

网上的平民，解决国家支持的网络攻击、和平时期的国家黑客攻击、攻击性“网络战争”能力以及软件的“武器化”来实现国家安全目标等做法日益猖獗的问题。[71]虽然这个想法在人道圈子内得到一定支持，但针对爱德华·斯诺登揭露的大规模监控计划，再加上很多科技公司扮演的令人不安的角色，实际上为这些计划提供协助，这一呼吁除了带来零星改革之外再无其他成果，表明在这个领域内并不存在一个“立竿见影”的策略。[72]

人道行动中的数据保护

国际隐私组织名为《监控的帮凶》报告基于该组织先前关于隐私、援助和发展的工作，一改之前对各项技术的鼓吹，令当时在援助和发展领域对技术的普遍热情得以减退，[73]为关于人道行动中数据保护重要性的更广泛讨论做出基础性贡献。2013年至2016年，无国界医生组织、现金援助学习合作伙伴 (Cash Assistance Learning Partnership)、人道事务协调厅、乐施会、联合国难民事务高级专员公署、联合国世界粮食计划署、联合国全球脉动以及红十字国际委员会均通过了数据保护政策、数据共享规则或负责任的数据使用声明。[74]在2015年，数据保护和隐私专员国际会议 (ICDPPC) 通过了《关于隐私和国际人道行动的一项决议》，作为另一项率先举措，重申尽管数据处理是人道行动者执行任务必然要涉及的工作，但“整个人道圈子中，执行数据保护框架的组织仍寥寥无几”[75]数据保护和隐私专员国际会议的上述决议阐明了人道组织在寻求遵守数据保护法律和原则方面所

71 Brad Smith, “The Need for a Digital Geneva Convention”, *Microsoft Blog,* 14 February 2017, available at: blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention.

72 See Ian Brown, Mort Halperin, Ben Hayes, Ben Scott and Mathias Vermeulen, “Towards Multilateral Standards for Surveillance Reform”, in Russell Miller (ed.), *Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair,* Cambridge University Press, Cambridge, 2017.

73 See, Kristin BergtoraSandvik and Maria GabrielsenJumbert (eds), *The Good Drone,* Routledge, London, 2017.

74 See Jos Berens, Ulrich Mans and StefaanVerhulst, *Mapping and Comparing Responsible Data Approaches,* GovLab and Leiden University Centre for Innovation, June 2016, pp. 5–6.

75 37th International Conference of Data Protection and Privacy Commissioners, “Resolution on Privacy and International Humanitarian Action”, Amsterdam, 27 October 2015 (ICDPPC Resolution).

面临的一些关键挑战。其中包括“敏感数据”(欧盟《通用数据保护条例》(General Data Protection Regulation) 将其定义为“表明种族或族裔出身、政治观点、宗教或哲学信仰、工会成员身份的个人数据；有关健康或性生活及性取向的数据；遗传信息数据或生物特征数据”）的收集，因为除非符合严格的条件和要求，否则禁止收集这些数据。[76]数据保护和隐私专员国际会议还指出，监测和信息管理系统、电子数据传输、身份识别系统和生物特征系统、移动电话应用程序和无人机——基本上是整个人道的创新领域——构成了“特定的隐私和安全风险”。[77]数据保护和隐私专员国际会议的上述决议警告，“不享受特权和豁免的人道组织可能面临压力，被迫将为人道目的收集的数据提供给希望将这些数据用于其他目的的当局 (例如控制移民流动和打击恐怖)”。[78]不过，虽然该决议强调人道组织在处理数据方面会产生很多风险，并呼吁遵守国际数据保护法律，但对于如何在实务上减轻具体的挑战，包括该领域独有的挑战，却没有提供太多指引。人道组织通过的许多数据保护规定亦是如此。虽然数据保护的关键原则已转变为正式政策，但它们往往未能就如何在人道行动发生的试验环境中做到具体落实提供明确的指导。2017年7月，红十字国际委员会和布鲁塞尔隐私中心 (Brussels Privacy Hub) 出版了《人道行动中的数据保护手册》(红十字国际委员会手册) (*Handbook on Data Protection in Humanitarian Action*)，在填补这一空白方面迈出了一大步。[79]

根据红十字国际委员会《手册》中提出的主题，本文的其余部分综述了该领域在数据保护上面临的一些主要挑战。为便于说明和比较，下文的分析

76 上文脚注48，《通用数据保护条例》第9条。上文脚注75，数据保护和隐私专员国际会议的上述决议也指出，“根据数据保护法律，通常被认为不具敏感性的数据，在人道紧急情况下仍可能非常敏感”。《通用数据保护条例》是一项具有约束力的欧盟法律，而数据保护和隐私专员国际会议的上述决议是一项建议，属于“软法”措施。

77 数据保护和隐私专员国际会议的上述决议，上文脚注75。

78 同上。

79 Christopher Kuner and Massimo Marelli (eds), *Handbook on Data Protection in Humanitarian Action,* ICRC, Geneva, 2017 (ICRC Handbook).

参考了欧盟《通用数据保护条例》中规定的数据保护规则。在分析中，一般所指的“数据保护法律”是指在相关国家和国际框架中规定的共同原则。[80]

重点关注《通用数据保护条例》，有以下几个原因。首先，将数据保护的挑战与数据保护的法律规范进行比较需要一个基线：在没有任何更广泛和可比较的国际法或公约的情况下，选择欧盟法律是因为它被广泛视为“黄金标准”。而且，随着数据保护法律继续在全球稳步推广，欧盟极有可能继续制定标准。其次，《通用数据保护条例》是第一部明确提及人道行动 (尽管只是顺势提及) 的数据保护法律。[81]第三，即使人道组织在数据保护法律较薄弱的国家开展业务，那些总部设在欧盟、希望在欧盟开展业务或将数据转移到欧盟的组织也必须遵守《通用数据保护条例》。甚至是享有特权和豁免权的组织，尽管迄今为止其活动和记录一直被视为无需适用这些法律，也可能越来越需要证明其有足够的数据保护政策，否则将无法从欧盟成员国政府或人道组织接收数据。[82]第四，因为数据保护对于信息时代基本权利的保护至关重要，有人建议，人道组织作为一个致力尊重人权的团体，应致力达到人权保障方面的最高标准。

80 这包括联合国开发的框架 (联合国大会，第45/95号决议，“电脑化的个人数据文件的管理准则”，1990年12月14日)，the CoE (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS 108, 28 January 1981 (entered into force 1 October 1985; Committee of Ministers, Recommendation No. R (99) 5 for the Protection of Privacy on the Internet: Guidelines for the Protection of Individuals with Regards to the Collection and Processing of Personal Data on Information Highways, 23 February 1999; Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Regarding Supervisory Authorities and Transborder Data Flows, ETS 181, 28 November 2001; Consultative Committee of the Convention for the Protection of Individuals with Regards to Automatic Processing of Personal Data, *Guidelines on the Protection of Individuals with regard to the Processing of Personal Data in a World of Big Data,* 23 January 2017), the EU (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data), the Organisation for Economic Co-operation and Development (OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 23 September 1980), Asia-Pacific Economic Cooperation (APEC Privacy Framework, 2004), and the Economic Community of West African States (ECOWAS Supplementary Act on Personal Data Protection 2010).

81 见上文脚注48，《通用数据保护条例》叙文第46段、第73段和第112段。

82 《通用数据保护条例》规定，除非数据接收国通过“充分性认定”(意指其被视为按可比标准给予数据保护)，或需要遵守具有约束力的数据保护规则，具体形式要么是欧盟委员会制定的标准合同条款，要么是经数据保护监督当局批准的具有约束力的公司规则，否则任何人均不得将数据传输至欧盟境外。同上，第44~48条。

数据处理的合法性

数据保护法律规定了“合法依据”或允许的“处理条件”；根据定义，人道组织或任何其他数据控制者在没有该法律依据的情况下处理个人数据，即属非法。[83]这些依据中，排在第一位是同意，人道组织过去一向以同意作为收集数据的依据。然而，对许多人道组织而言，获得同意的条件是否总是符合“自愿给予”、“清楚明白”及“知情同意”的准则，仍值得怀疑。[84]这是因为人道援助计划的受益者往往(虽然并非总是)没有真正的选择，只要希望利用援助，就必需登记和提供数据。此外，应告知数据主体其数据会如何被使用，会与谁分享及作何用途，并应记录同意。但对多个经常参与向流离失所者或受围困人群发放救援物资的人道组织而言，由于所应对的紧急情况特殊或规模庞大，在实务上已面临巨大挑战，再向人们提供这些信息以获取其同意显得尤其艰巨。

因此，人道组织可能希望按其他法律依据来处理数据。那些根据国际法负有人道任务的国际组织可以选择根据其任务职能处理个人数据，但对非政府组织来说，则无法选择这样做。欧盟的《通用数据保护条例》以默示方式建议人道组织以数据主体的“切身利益”作为处理的依据，[85]但亦指出，这只应在“数据处理明显不能基于其他法律依据”的情况下才可进行。[86]此外，“敏感数据”处理虽然很可能是出于提供重要服务的需要，但只有在数据主体在身体上或法律上不能表达同意，或因公共卫生法律或紧急情况有关需要，才可未经同意处理。[87]这些不一致之处令人道组织有时左右为难，不知道何时应征求同意，何时无需征求同意，以及在不需要征求的时候，如何

83 例如，在欧盟框架内，只有以下情况下的数据处理才合乎法律：如是基于数据主体的同意，数据处理是合同要求或法律义务；出于保护数据主体或其他自然人的切身利益的需要；出于公共利益而履行任务或行使公共权力的需要；或属于控制者或第三方合法权益范围之内，除非此等权益为数据主体的基本权利和自由要求保护个人数据的权益所超越。关于数据处理的合法性，见如上所述，第6条。

84 欧盟将同意定义为一项明确的肯定行动，确立“数据主体就与其个人数据相关的处理，自由给予明确、知情且无疑的同意”。同上，叙言第32段。

85 同上，叙言第46段。

86 同上。

87 在人道背景下，数据主体可能无法表示同意的情形可能包括：无法向数据主体提供关于数据处理的必要信息，处理过程复杂，不利于数据主体做出自由决定，数据控制者与数据主体之间存在严重的力量不平衡，关于是否提供数据的问题，后者并无有意义的选择。见上文脚注79，红十字国际委员会手册第3章。

执行一个足够（及合法）健全的程序，以取得及记录有关同意。人道组织确实选择基于受益人“切身利益”处理数据的，因为根据定义是指“对生命至关重要”的利益，所以也应确保此等处理对于这一目的而言是必要和相称的(即，不过分)。[88]那些依据同意的组织还必须为儿童实施更严格的程序，以父母同意作为处理儿童数据的准则，同时为撤销同意做出可行规定，让同意的撤销与给予一样简单。此外，所有人道组织将需要协助数据主体行使相关权利，拒绝对其个人数据进行处理，并在适当情况下纠正或删除其数据。

对受益者保持透明

透明度是数据保护的根本，应成为致力于对受影响人士负责的人道组织的第二天性。不管以何作为数据处理的法律依据，数据保护法律都要求数据控制者的数据处理操作对数据主体保持透明。[89]这不仅是为了让数据主体在表达同意前获得相关信息；而且数据保护法律也授予数据主体获取该信息的权利。[90]根据《通用数据保护条例》的规定，应让数据主体“了解个人数据处理方面的风险、规则、保障措施和权利，知晓如何行使与此等处理相关的权利”，另外“个人数据处理的具体用途……应明确、合法，在收集之时便应确定”。[91]向人道行动的受益者提供这种信息的困难显而易见，在实践中，即使是遵守最低的标准，可能也难以实现。[92]虽然人道组织完全有理由指出，在某些情况下，受益者难以或不可能在收集信息时获得有关数据处理的信息，但亦不能因个别情况的紧急需要而完全忽略这些责任。相反，人道组织将需要寻求创新方法，向个人受益者和受益者群体提供信息，具体包括事先的信息宣传活动、改动个人咨询过程和宣传计划，并在其中纳入数据保护问题，使用服务台和信息通信技术向需要者提供信息。

88 欧盟将“切身利益”定义为“对数据主体或另一自然人的生命至关重要的利益”：上文脚注48，《通用数据保护条例》叙言第46段。上文脚注79，红十字国际委员会《手册》第3条第3款提供了一个更广义的解释。

89 例如，见上文脚注48，《通用数据保护条例》第12~22条，第34条。

90 同上。

91 同上，叙言第39段。

92 根据《通用数据保护条例》，“关于自然人个人数据的收集、使用、查询和其他方式处理，以及在何种程度上处理或将在何种程度上处理，均应向这些自然人披露。”

这些方法特别适用于人道组织在收集数据时，不清楚具体将如何使用或共享数据的情况，例如，在紧急响应之初，对人口及脆弱性开展评估调查过程中收集的数据。如上所述，也为了防范“职能蠕变”(技术或系统的用途逐步扩大，超出原本目的的情况)，数据保护法律通常要求数据控制者在收集数据时便明确将如何使用收集的数据。[93]对于人道组织，挑战是要尽可能具体，同时保持灵活性，以便根据人道响应的变化和发展，到时再确定数据的用途。如数据用途和/或合作伙伴有重大改变，人道组织可能需要告知受益者，并根据其同意程序，从数据主体处寻求新的或额外的同意。因此，人道组织面临着另一个艰难的判断，不知道应在哪里划线。以一次性同意给予人道组织无限制授权 (*carte blanche*)，让人道组织可视情况使用受益者的数据，无需进一步征求其意见，这样做显然违反数据保护基本原则，但针对新的数据处理作业取得额外的同意，必然会对后勤、运行和资源造成重大影响。关键的法律检验标准是看数据处理“是否与个人数据最初收集时所服务的目的相符”，[94]但如果目的被视为提供“人道援助”，则人道组织在这方面可能比其他数据控制者拥有更广泛的范围。[95]

信息安全

难民、寻求庇护者和国内流离失所者面临诸多风险，其来源包括原籍国、东道国、过境国和目的地国家 (这些国家实施压制排斥政策的情况下)，不怀好意的第三方，例如非国家武装团体，犯罪分子甚至“黑客活动分子”(那些以颠覆性的方式使用信息通信技术，促进一项政治目的或社会变革) 等。所有这些对手均有可能利用数据主体的个人数据损害其最大利益，令个别团体或个别数据主体及其家人遭受严重伤害，或严重削弱人道组织执行其任务的能力。一旦收集了受益人的数据之后，有效的信息安全政策和做法就成为人道组织和弱势群体与其潜在对手之间的唯一屏障。

93 例如，见同上第13条。
94 同上，第6条第4款。
95 见上文脚注79，红十字国际委员会手册第2条第6款第3项。

一线的安全工作已经十分具有挑战，人道领域运用信息通信技术从实物文件向数字化记录的过渡也带来了一系列新的挑战。通常，由于缺乏该领域的专门技术知识，当地的数据库、解决方案和创新，这些对于提供保护和援助而言帮助极大，但在开发或管理时并未考虑到信息安全 (委婉地说)。虽然中央数据库应该提供更强的数据安全性，但是可能需要提供的访问范围会造成其他漏洞。在这方面，与所有大型组织一样，人道组织的信息通信技术用户是其最薄弱的环节。许多人缺乏基本的信息安全培训，而且像大多数信息通信技术用户一样，经常从事破坏其个人和组织安全的行为。[96]这一点很重要，因为绝大多数成功的信息通信技术黑客不是利用技术、“后端”漏洞 (突破防火墙、进入数据库，等等)，而是依赖于某种形式的“社会工程”或心理操纵，比如欺骗用户或员工交出机密或敏感数据，具体做法是让其点击虚假链接或打开包含“恶意软件”(专门设计用于干扰、损坏计算机系统或获得对计算机系统的授权访问的软件) 的电子邮件附件。随着这些攻击的频率和先进程度增加，[97]人道组织应将信息安全作为现场安全的一个组成部分，并对其工作人员进行相应的培训。尽管对需要保护资产和声誉的企业来说，信息安全已经是第二天性，但人道领域仍需要文化上的转变。[98]

这有点老生常谈，但实现数据保护的最简单方法是直接一开始便不收集数据，或者至少只收集需要的数据。次优方案是确保数据准确和相关性，并在不再需要的时候删除。这些原则体现在“目的明确”、“必要和相称”以及“数据最小化”等概念中，[99]然而人道领域的各种迫切需要正朝着相反的

96 See Fran Howarth, “The Role of Human Error in Successful Security Attacks”, *IBM SecurityIntelligence,* 2 September 2014, available at: securityintelligence.com/the-role-of-human-error-in-successful-securityattacks/.

97 Symantec, “Extraordinary Attacks, High-Dollar Heists, Electoral Disruption”, *2017 Internet Security Threat Report,* ISTR 22, April 2017.

98 最近一份关于国际人道行动者如何管理风险的报告指出：“就员工的时间和注意力而言，安全/安保风险的管理最受重视，紧随其后的是受托人风险管理 (防止欺诈和挪用)。……研究发现，在信息安全和法律 (例如反恐法律) 遵守方面，对风险管理的整体重视和理解较少。” See Abby Stoddard, Katherine Haver and Monica Czwarno, *NGOs and Risk: How International Humanitarian Actors Manage Uncertainty,* Humanitarian Outcomes and InterAction, February 2016, available at: www.humanitarianoutcomes.org/sites/default/ files/ngo-risk_report.pdf.

99 许多数据保护法律都提及这些原则。例如，见上文脚注48，《通用数据保护条例》，第5条第1款第2项关于目的的明确，第5条第1款第3项涉及必要性、相称以及数据最小化。

方向推进。许多人道组织似乎都是从一个默认的立场开始的，即个人数据必须保留很长时间、不确定保留期间甚至无限期保留，以满足审计的要求。[100] 过度鼓吹的大数据力量 (详见下文)，也鼓励人道组织大量收集和保留个人信息，超出适当的范围，而且很多“数字卫生”做法不符要求，留下的数据轨迹放大了受益者的风险，而不是尽量减少和限制数据访问，完全以合法的存档需求为出发点。解决这些问题还需要另一种文化转变。

人道档案的维护提出了一套不同的数据保护挑战。对于一些人道组织而言，保存其活动的详细档案，有许多和令人信服的理由，其中有些包含在其任务规定中，尤其是未来很长一段时间内，这些数据对难民及其家属等数据主体可能至关重要。困难在于如何在保持“人道记忆”的重要性与数据保护法律的基本原则之间取得平衡。例如，难民署有一项长期的记录和档案政策，规定应无限期地保存个人专案文件，另外一项新的数据保护政策规定一旦不再需要，就应立即删除个人数据。[101]但是，到目前为止，所有与难民署受益人有关的个人数据都被认为是其专案文件的一部分，因此，与该组织的数据保护规定相反，工作上的假设是一切都应永远保存。保存关于难民的历史记录，相关公共和私人利益显而易见，但这是否意味着档案应该将每个人在难民营期间事无巨细全部信息均纳入其中，特别是在收集的数据越来越多的情况下？如果后来有人反对在其专案文件中保留特定的记录，并要求根据其基本权利删除这些记录，又会怎样呢?自主性是数据保护的基础，但人道领域盛行家长式作风；因此，必须找到一个合适的平衡点。

数据分享及相关责任

很多人道组织与第三方 (包括东道国政府、行动/实施伙伴及商业服务提供者) 分享个人数据，以便于或加强各项保护和援助的提供。尽管以下解释与隐私和数据保护倡导者的直觉抵触，但仍需要强调的是，对援助流离失

100 由于国家和其他捐助者可能针对其计划开展内部和外部审计，人道组织似乎害怕删除数据，而决定保留什么、丢弃什么和安全地销毁哪些数据的代价可能很高。

101 关于数据保留的规定，见UNHCR, Policy on the Protection of Personal Data of Persons of Concern to UNHCR, May 2015, Art. 4(6).

所者的人道组织数据进行汇总，不仅是应急响应的重要组成部分，而且由于大幅减少收集和储存的数据量，事实上可以降低数据保护方面的风险。另外，重复的脆弱性评估有时并无需要，需要援助者经常报告会产生“调查疲劳”，而数据的汇总也有助于减少这种现象。然而，由于缺乏整个领域共同适用的数据保护标准，这种合作带来了大量的实际问题，而人道组织之间对资金的竞争、相互重叠的任务以及数据所有权方面的政治因素，也令这些问题更加复杂。应对媒体、研究机构及私人公司对敏感信息的兴趣持续升高，人道组织作为这些信息的“守护人”，应承担更多责任。为了对关于难民的故事做出正面的解释，或促进研究，以加深对难民及其需求的了解，人道组织未必会考虑其法律责任或其行为的道德问题。[102]

数据保护法律要求，将数据主体的数据传输至其他组织，必须得到数据主体的明确同意。[103]数据控制者还必须确保，所有第三方接收者适当地保护这些数据，只将数据用于指定的目的，并只接收满足这些目的所需的数据。数据传输应受法律或合同规定的约束，并应通过安全通信渠道执行传输——人道组织过去常规的数据交换方式和这些要求大相径庭。[104]数据主体也必须能够行使其权利，并在出现问题时获得和寻求补救。虽然建成正式的数据共享安排，并能够满足数据保护基本标准的要求，需要大刀阔斧地改变实际工作做法，但这些问题并非无法克服。例如，难民署的现金援助计划经过具体

102 See European Commission, “Guidance Note – Research on Refugees, Asylum Seekers & Migrants”, Directorate-General for Research and Innovation, available at: ec.europa.eu/research/participants/data/ ref/h2020/other/hi/guide_research-refugees-migrants_en.pdf.

103 一般只有数据接收方能够控制数据的使用方式，才会适用此类规定。相关组织可将数据传输至“二级处理者”，按其指示代其执行数据处理任务，同时应采取适当的保障措施。例如，见上文脚注48，《通用数据保护条例》第6条第1款，第7条，第28条。

104 例如，见难民署委托的一项数据保护影响评估得出的结果：“应尽全力避免使用未加密的文件和容易丢失或被盗的媒介传输难民的个人可识别信息。可能的情况下，应该用安全的FTP通道或VPN替代电子邮件发送此类文件。如果要用电子邮件发送文件，在后续电子邮件中传输加密文件和这些文件的密码的做法也应停止，以便采用更安全的程序。中期目标应是执行安全的信息和通信技术解决方案，一方面使合作伙伴能够访问和使用难民署的数据 (并在必要时纠正或补充数据)，一方面难民署保留对这些数据更大的控制能力”。See UNHCR and Trilateral Research & Consulting, *Privacy Impact Assessment of UNHCR Cash Based Interventions,* Geneva, December 2015, p. 23, available at: www.globalprotectioncluster.org/_assets/files/ tools_and_guidance/cash-based-interventions/erc-privacy-impact-assessment-of-unhcr-cbi_en.pdf.

的数据保护影响评估，该组织采用创新程序确定数据共享安排，评估第三数据保护制度的充分性，尽量减少分享的数据量，并与许多合作伙伴达成数据分享协议。[105]

当然，数据共享相关的数据保护风险的性质和程度在很大程度上取决于共享的数据类型和谁是数据的接收者。因此，与已经建立了可靠的数据保护政策的业务伙伴或服务提供者共享数据的风险可能较低，而与那些对移民和难民 (或特定宗教或族裔群体) 的政策可能随时间而改变的政府合作往往被视为风险较高。[106]为妥善应付这种情况，人道组织必须评估自身及其本地合作伙伴和服务提供者遵循的法律框架，并透过这些法规是否会伤害其受益人的角度，分析这些法规。这种评估往往揭示了上文讨论的那种“积极披露”义务，这种义务目前在全世界都存在，而且经常有损害或伤害人道计划受益者基本权利的风险。其中一些风险是显而易见的，比如一些国家要求卫生服务提供者向公共当局通报诸如艾滋病、结核病甚至同性恋等“情况”。虽然人道组织可以而且往往会在遵守有关法律方面采取原则性的立场，但其本地合作伙伴未必有能力这样做。其他风险远不如这样明显，比如国际反恐和反洗钱制度带来的风险，因为这些制度要求所有金融服务提供商对金融转账和账户持有人进行“尽职调查”。[107]这包括对照数百个国家和国际制裁名单来检查个人客户，而且这项工作经常外包给“合规”服务提供商，并受到国家金融情报单位和国家安全机构的审查。虽然人们越来越认识到在现金部门中数据保护的重要性，但越来越多的人道组织开始执行现金援助计划，其是否认识到有需要与其服务供应商正面处理这个问题，则不得而知。[108]由于许多制

105 同上。See also UNHCR, *Operational Guidelines on the Protection of Personal Data of Persons of Concern,* forthcoming 2018.

106 例如，难民署很多情况下必须分享在东道国登记的难民基本生平信息，除了尽量减少实际分享的数据外，基本没有采取其他数据保护措施的余地。

107 See Gavin Sullivanand Ben Hayes, *Blacklisted: TargetedSanctions, Pre-emptive Security and Fundamental Rights,* European Centre for Constitutional and Human Rights, Berlin, 2011.Also see Ben Hayes *et al., “De-risking”: From Financial Surveillance to Financial Exclusion? Banking Problems and Solutions for the Non-Profit Sector,* Human Security Collective and Open Society Foundations, forthcoming 2018.

108 See Jessica Burniske, NazModirzadeh and Dustin Lewis, “Counter-Terrorism Laws: What Aid Agencies Need to Know”, Overseas Development Institute, Humanitarian Practice Network Briefing Paper No. 79, November 2014.

裁名单是由冲突当事国或与暴力局势有关的国家制定的，利用银行支付现金会使人道组织参与制裁的执行，可能会无意中损害人道组织的中立性。

电信注册和数据保留制度也造成了类似的问题。这些制度经常迫使服务提供者保留关于用户、通信流量甚至内容数据的信息，并向执法和安全机构提供这些信息。在移动电话出现之前，获得这类记录通常需要法官向电话公司发出逮捕令；今天，可能只需要一个手机号码。然而，尽管这种监控广泛存在、愈发难以避免，但人道组织的数据保护责任不会因此而被免除。相反，当务之急是人道组织要认识到，像短信群发一类常用的受益人通讯工具尤其容易被国家和非国家组织截获，在可能的情况下，应寻找更安全的替代工具，确保这些工具的使用不会损害人道行动的中立以及受益人的安全或安保。[109]

如上文所述，政府亦可直接向人道组织索取资料，甚至对数据主终身司法管辖权或强行占有数据，完全不顾人道组织的意愿。享有特权和豁免的组织有完善的规则，用于处理政府提出的索取要求，并可以主张各种合法利益，包括其受益人的基本权利，作为拒绝无理要求的理由。[110]而有些人道组织无权享受这样的保护，又没有就这些意外事件的预防做出相关规定，不但会使受益人的隐私面临威胁，而且也无法保障其安全和安保。2017年8月，有消息来源称，英国内政部接入无家可归者信息整合网 (Combined Homelessness and Information Network) 的数据库，从中寻找外国人并驱逐出境。该数据库由英国多家慈善组织和政府机构用于汇总数据并采取干预措施，以帮助露宿街头的人摆脱困境。[111]目前该数据库由一个关注无家可归问题的慈善组织管

109 “收集关于难民的数据，应在安保和公共安全与维护人类尊严和权利的需要之间取得平衡。各国政府和难民机构在收集难民数据时，需要赢得信任。科技公司应该承认，其平台用户既有难民也有走私者，另外应改善用户安全措施。我们应该自问，企业拥有这种带有政治色彩的数据意味着什么。” Mark Latonero, “For Refugees, a Digital Passage to Europe”, *Responsible Data Forum,* 8 February 2016, available at: responsibledata.io/for-refugees-a-digitalpassage-to-europe/.

110 See, for example, UNHCR, *Guidelines on the Sharing of Information on Individual Cases: “Confidentiality Guidelines”*, Geneva, August 2001.Also see ElsDebuf, “Tools to Do the Job: The ICRC’s Legal Status, Privileges and Immunities”, *International Review of the Red Cross,* Vol. 97, No. 897/898, 2016.

111 Mark Townsend, “Home Office Used Charity Data Map to Deport Rough Sleepers”, *The Guardian,* 19 August 2017, available at: www.theguardian.com/uk-news/2017/aug/19/home-office-secret-emails-datahomeless-eu-nationals.

理，内容包括露宿者的位置、国籍、心理健康状况和性别。[112]像这样的例子以及其他众多事例[113]，对其他排查脆弱性因素或提供“开放数据”集的行动计划应该有警示作用，表明相关数据可能被另作他用。

大数据

在2013年一份具有里程碑意义的报告中，人道事务协调厅指出：“如何让大数据为人道决策者所用，是网络时代面临的巨大挑战和机遇之一。”[114]在人道领域，开展以大数据为主导的创新，有很多极具说服力的论据，特别是明显欠缺的信息管理能力阻碍开展有效的行动，甚至有人因此付出生命的代价。虽然毫无疑问，这种创新让人道组织有机会补救一些基本的缺陷和提高效率，人道事务协调厅对关联和分析“庞大的信息，在人道组织运营的领域得出惊人的见解”过度热情，完全忽视了数据保护方面的要求。[115]

诚然，数据保护规范的要求虽然相对简单，但在这个让人充满憧憬的新天地中，至少乍看之下，找到立足的地方并不容易。数据保护要求目的明确、有限制，而大数据希望通过将数据转化为“可执行的情报”，找到数据的新用途。数据本身成为收集和处理个人数据的基本理由，“职能蠕变”成为无法根除的问题，因为大数据存在的理由 (*raison d’être*) 便是开发在收集数据时没有预见到的数据用途。因此，人道组织被鼓励采用更先进的评估方法确定援助对象及其资格条件，找出最需要援助的人群，并提供更好服务，尽管这样人道组织不可避免需要收集更多数据 (包括敏感数据)，以确定个

112 St Mungo’s, “CHAIN – Combined Homelessness and Information Network”, available at: www.mungos. org/work-with-us/chain/.

113 其他更多示例包括：公布关于非洲之角地区寻求庇护者的状况、路线和基本信息的实时数据，无意中可能帮助走私者和人贩子从中获益；绘制武装冲突期间难民的流动图，可能会成为冲突各方利用的工具；发布宗教少数群体或性暴力受害者的地理位置图，未考虑所涉及的风险，可能使这些群体或个人容易受到进一步的伤害；发表统计数字，证明向不同种族、宗教或民族团体提供援助，会引起关于厚此薄彼的指控。此处引用的第一个示例出自Joseph Guay and Lisa Rudnick, “What the Digital Geneva Convention Means for the Future of Humanitarian Action”, *UNHCR Innovation Service,* 25 June 2017, available at: www.unhcr.org/ innovation/digital-geneva-convention-mean-future-humanitarian-action/.后面的例子来自作者的工作经验，没有公开的文件。

114 人道事务协调厅，上文脚注54，第26页。

115 在人道事务协调厅112页的文件中，没有出现“数据保护”一词。

人、家庭或住户的基本情况。由于整个系统相当复杂，受益人更加难以理解自己对于大数据计划的参与情况，具体而言包括个人信息的收集、使用、存储、共享和分析方法，因此无法了解所给予的同意究竟意味着什么。至关重要的是，对脆弱性各个方面进行多级分层和建模也可能不符合受益人的“切身利益”。使用大数据分析方法确定资格条件，也可能产生歧视效应，且相关人员无法就此提出申诉。这样做不仅威胁个人权利：大数据还可能对整个受益人群体产生负面或不可预见的影响，在集体维度上造成伤害。

这些挑战绝不局限于人道组织：凡是对个人数据进行“挖掘”以深入获取信息的地方，均存在挑战，如果再加上机器学习、分析和自动化决策，挑战会更加严峻。此外，虽然数据保护方面的法律似乎一直难以跟上步伐，《通用数据保护条例》提出的要求对于开发这些工具的人道组织产生长远的影响。[116]该条例规定：“每个数据主体因此都应有权知道……任何自动处理个人数据系统的逻辑，至少是分析过程中依据的逻辑，以及这种处理的后果”；每个数据主体“在评估完成之后，有权获得人工干预和解释，并对决定提出申诉”。[117]

此外，“在可能的情况下，数据控制者应能够提供对一个安全系统的远程接入，让数据主体直接访问自己的个人数据”。[118]这些内容确定了2017年1月欧盟委员会发布的《大数据世界中个人数据处理方面的个人保护指南》(“大数据指南”) (*Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data in a World of Big Data*) 的基调。它敦促数据控制者不应局限于直接的数据保护措施，“采取预防政策和开展风险评估时”，“考虑到大数据使用的法律、社会和道德影响，包括关于获得平等待遇和不受歧视的权利”。[119]下文进一步探讨了人道组织实现这些目标的机制。

116 上文脚注48，《通用数据保护条例》叙文第63段、第71段、第4条、第13条、第14条、第15条、第22条。
117 同上，叙言第63段。
118 同上。
119 CoE, *Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data in a World of Big Data,* T-PD (2017) 01, Strasbourg, 23 January 2017 (Big Data Guidelines), p. 5.

生物特征技术

由于服务移民和难民的人道组织的受益人往往没有身份证明文件，生物特征身份识别系统越来越受欢迎。生物特征系统通过取得数码照片、虹膜扫描或指纹等独特识别信息，能够提高登记程序的效率，并通过加快资格核查和减少欺诈性要求，更快、更公平地分配援助物资。但如上所述，《通用数据保护条例》明确将生物特征定义为“敏感数据”，倡导隐私和公民自由的人士多次对生物特征身份识别系统的开发和安装启用表示担忧。这是由于一旦将个人数据与生物特征档案相联系，既会产生大量的数据保护工作，也会构成诸多安全挑战，另外，也是因为生物特征日益被用作一项警务和移民执法的工具。然而，决策者一直优先考虑的是生物特征分析明显的效率和准确性优势。现在，联合国的可持续发展目标，包括为大约24亿缺乏公认身份证件的人提供合法身份。这为各国采用生物特征技术提供了额外动力。[120]至关重要的是，尽管生物特征身份识别系统的批评者往往会本能地关注将个人纳入数据库的影响，在发展和人道背景中，生物特征登记的驱动力也可能产生社会排斥甚至无国籍的情况，因为那些被认定没有资格获得公民身份或保护的人可能被剥夺公民权。

使用生物特征技术的人道组织不能忽视这些更大范围的担忧。例如，难民署正在其行动范围内推广其全球生物特征信息管理系统 (BIMS)，为被排斥者提供持久的数字身份识别使他们获得认可。难民署还利用其收集的基本信息来核查身份和权利，以便精简粮食和现金的援助过程，并因与行动伙伴和约旦银行部门制定创新和复杂的数据分享安排而受到赞扬。但随着越来越多的利益相关者和合作伙伴实行或考虑引入或者使用生物特征技术，难民署不可避免地面临越来越大的压力来分享或提供全球生物特征信息管理系统的访问权，很多用途已超出最初的预测——例如，与东道国政府的联合注册活动、或者对成功的安置候选人的安全审查。因此，难民署的包容政策和各国的排斥政策之间开始出现冲突，产生了全球生物特征信息管理系统建立之初没有预见到的数据保护和基本权利方面的挑战。这些

120 联合国可持续发展目标，“目标16：创建公正、和平与包容的社会”，2015年9月25日通过，第9段。

挑战包括制定一项生物识别政策，以协调不同利益方相互冲突的要求，向难民解释数据流动及其给难民带来的风险，处理受益人和政府对数据提出的各项要求。[121]

人们的感知至关重要。如果人们怀疑出于人道目的收集的生物特征最终可能被用于损害其受益者的利益，则整个计划的信誉、声誉和存续都可能受到严重伤害。[122]即使是表面上看来属于“低科技”的数码照片生物特征数据库，由于面部识别技术的迅速发展，也包含一些固有的风险。[123]

风险管理

虽然人道组织在处理个人数据方面有很多风险，而且在负责任的创新方面有明显的困难，但这些挑战并非不可克服。所有数据处理都附带固有的数据保护风险；对数据控制者而言，关键是要从一开始就正确地评估这些风险，并制定适当的保障措施。[124]这种评估不单是人道组织履行“不伤害”原则的一种方式，亦已成为一项法律责任。《通用数据保护条例》要求数据控制者评估：在采用“新技术”且“自然人的权利和自由可能因此面临更大风险”的情况下，预期的数据处理会对个人数据保护产生怎样的影响。[125]

121 2017年，《经济学人》(Economist) 杂志被问到：“不享受公民身份保护的难民，对云服务器中存储的数据，是否享有隐私权？”See “Phones are Now Indispensable for Refugees”, *The Economist,* 11 February 2017, available at: www.economist.com/news/international/ 21716637-technology-has-made-migrating-europe-easier-over-time-it-will-also-make-migration.

122 2016年，*TakePart*杂志报道：“加来市的市政官员1月份宣布，将在……月清理丛林 (难民营)，作为替代，城市公布了一个新的官方难民营，位于丛林难民营的边上……但很少有人接受这个提议。手掌扫描仪吓坏了一些居民，担心如果设法前往英国，这些生物特征会被交给警方，并被用来对付他们。”See Marc Herman, “Unwelcome Refugees”, *TakePart,* 5 February 2016, available at: www. takepart.com/feature/2016/02/05/jungle-calais-france-demolition/.

123 根据欧盟基本权利机构的说法，“在大量难民抵达期间，私营机构开始提供追踪服务，特别是在奥地利、德国和匈牙利的大型火车站，过程中使用了照片，但未考虑到数据保护的风险。”See EU Fundamental Rights Agency, “Thematic Focus: Family Tracing and Family Reunification”, available at: fra.europa.eu/en/theme/asylum-migration-borders/overviews/focus-family.

124 见上文脚注1，正如Kaspersen and Lindsey-Curtet所解释的那样：“受益人需要两全其美的方案：其需求能够得到快速、高效地满足，且满足其需求的机构因为其历史而值得信任。对这些机构来说，这意味着愿意与愿意创新的人合作而进行自我颠覆——不断质疑其工作方式的价值，并认真思考技术所带来的潜在机遇，以新方式将人、物、过程和数据联系在一起。但在寻求利用技术的巨大机遇来改善人道援助的过程中，这些机构也需要意识到一些非常现实的风险。”

125 上文脚注48，《通用数据保护条例》第35条第1款。

数据保护影响评估 (DPIAs) 必须包括减低风险以及遵守数据保护法律的“措施、保障及机制”，并应征求数据主体的意见。[126]如数据控制者准备“大规模地”处理敏感数据 (例如，生物特征或健康数据)，则必须开展数据保护影响评估。如果处理是“系统的、广泛的和自动化的”，包括可能“显著影响自然人”的分析过程，则也必须开展数据保护影响评估。[127]此外，如果数据保护影响评估“表明，如果控制者没有采取措施来减轻风险，处理过程将导致高风险出现”，则数据控制者有义务事先征求其数据保护监督当局对处理过程的批准。[128]欧洲委员会最近的《大数据指南》对数据控制者提出类似要求，“需要识别和评价各项处理活动的风险”，评估其“在个人的权利和基本自由方面可能产得不到的负面结果”，[129]并进一步鼓励符合道德标准的影响评估，以防止歧视和社会排斥。

通过进行评估，人道组织可降低信息和通信技术系统设计方面的风险，并制定前瞻性的政策，为受益人提供有意义的隐私及基本权利保护。必须寄望于这些组织也将了解到，在设计阶段这样做要比对已在运行的系统重新采取数据保护保障措施容易得多。[130]这也是为什么欧盟和欧洲委员会最新的法律强制要求在设计阶段对隐私和数据进行保护。幸运的是，对这些义务进行强制的时期，正是广泛的创新和研发 (R&D) 已经将这些曾经雄心勃勃的概念转化为信息安全和数据保护的高效模式的时期。匿名化技术、[131]应用密码学、[132]“零知识”体系结构[133]以及将数据置于数据主体有意义和有效控制之

126 数据保护影响评估必须系统说明预期的处理操作及其目的；对照目的，对处理操作的必要性和相称性进行评估；对数据主体各项权利和自由所面临的风险进行评估；为应付风险而拟采取的措施，包括保障措施、安保措施、确保个人数据保护的机制以及证明数据保护法律得到遵守的机制。同上，第35条。

127 同上，第35条。

128 同上，第36条。

129 上文脚注119，大数据指南，第5页。

130 数据保护影响评估仍可非常有助于弥补现有系统和计划的数据保护缺口。

131 通过从数据集之中剥离个人可识别信息，或用代码替代个人可识别信息 (假名化)，人道组织可以大大降低数据被滥用的风险。虽然这些技术并非无懈可击——使用数据匹配或类似的技术，从多个匿名数据集中可“重新识别”相关个人，从而对包含在大型综合数据集中的个人构成潜在风险——但只要正确使用这些技术，仍可以显著降低风险。但是，如上文所述，在某些情况下，匿名化数据以产生可能发表的汇总或统计资料，或至少比个人数据更广泛地分享，可能会给受益人带来严重的保护风险：见上文脚注113。

132 应用密码学允许对静止和传输中的数据进行加密。

133 “零知识”架构涉及到存储平台，它防止平台所有者和未经授权的第三方读取数据库中存储的信息。

下的新可能性，[134]现在为人道组织提供了开发既高效又相当安全的信息和通信技术系统的机会。

结论：什么样的技术颠覆？

自国际隐私组织指出援助和发展领域“缺乏隐私”之后四年来，人道领域已经取得重大进步，[135]尽管如此，人道组织仍需做大量工作，才能满足受益人数据保护、信息安全、负责任创新方面的最低标准。这些要求目前不仅体现在数据保护法律的精神上，并且已成为这些法律的明文规定。即使是那些以身作则并采取了强有力的数据保护政策的组织，要确保这些承诺在其所有行动中得到妥善实施，仍然有很长的路要走。红十字国际委员会新推出的《人道行动中的数据保护手册》仍是人道组织唯一可用的详细指导文件。目前极其重要的任务是以这份文件为基础，继续就危机时期数据的收集、分享和存储的全球标准开展积极讨论，在可行标准的开发和实施方面，数据保护管理当局应承担更大责任。虽然人道组织像所有的组织一样，显然不愿讨论国家和非国家行为体渗透其信息系统的企图，但如果要就国际人道法要求的零容忍方法取得支持，保持人道行动所要求的中立和有效性，就必须找到一个集体处理这个问题的方法。一部“关于数字的日内瓦公约”是否能对这些问题做出切实可行的回应，仍有待观察；与此同时，人道组织必须负责妥善保障其信息系统的安全，确保其数据不会被用于损害其中立性以及受益人的各项权益。

这一根本挑战是人道领域创新和拥抱新技术的核心。这项挑战一方面具有高度技术性——要求分配相应资源来开展认真的风险评估，在研发过程中做到真正负责的创新——另一方面也具有高度政治性，在描述人道行动中的技术颠覆时，仍很大程度上以技术决定论为特点，过多地将数据保护描述或认定为一项障碍。现在，人道工作者被要求不仅要“埋头研究”，还要“深

134 例如，个人信息管理系统和数据自治及可转移性倡议。

135 G. Hosein and C. Nyst, above note 29.

入一线”，被告知如忽视新型数字化的人道主义，“会令自己处境危险”，[136]如果不能“自我颠覆”，则会有“被边缘化”的危险。[137]人道工作者还受到警告：“从完全不同的背景情况中所制定的过于规定性和死板的框架……有可能扼杀新的发现”，因此建议在拟定监管计划时，应采取“极简”的方法。[138]

当然，技术只不过是不断寻找问题的解决方案。很明显，许多技术提供者之所以被人道领域所吸引，并不仅仅是因为想做慈善，而是因为它提供了一个在现实世界中测试其解决方案的绝佳机会。如果人道领域中负责任的创新者提出目标，例如，通过寻求高度安全的通信和数据存储解决方案，则这种合作就十分有价值。但如果目标是由其他主要利益集团设定，则会出现政策不连贯、意外后果和负面外部效应的重大风险。一些科技公司显然在不遗余力地开发基于区块链的难民身份管理系统，[139]例如，向难民署这样的机构推介更稳健、功能更全面的身份识别系统，但因为本文导言部分所述的国家政策，也存在加剧排斥及公民权被剥夺问题的重大风险。捐助者在这方面也发挥了根本性的作用：数据保护内容终于出现在捐助协议之中，但在实践中，由于过分优先考虑数据密集的方案，例如现金转账计划、生物特征技术、透明度和问责机制，这项要求也可能被大打折扣。

直到人道领域的技术颠覆和数据保护构建为相辅相成的两项因素 (而非相互排斥)，在此之前，人道组织仍将不可避免要被迫仓促做出采购或部署决定，对其受益人的基本权利造成不必要的伤害。那些控制资金的人——不管是在人道组织内部还是外部——可以通过将数据保护和信息安全摆在有意义的优先地位，而发挥最大影响。如不这样做，那么业内所谓的“灾难性数据泄露”有一天就会让他们警觉起来，洗耳恭听。

136 例如，见推荐以下书籍的内容：Patrick Meier, *Digital Humanitarians: How Big Data is Changing the Face of Humanitarian Response,* Routledge, 2015, available at: www.digitalhumanitarians.com/.

137 A. Kaspersen and C. Lindsey-Curtet, above note 1.

138 J. Berens, U. Mans and S. Verhulst, above note 74, p. 8.

139 “Microsoft and Accenture’s Blockchain ID System for Refugees Highlights Data Privacy Needs”, *ITU News,* 20 June 2017, available at: news.itu.int/blockchain-refugees/.