《国际法的数字挑战》白皮书

罗旷怡* 译　黄志雄** 审校

引言①

《国际法的数字挑战》白皮书是为了迎接国际法协会（International Law Association, ILA）150周年诞辰而发布的23个不同主题白皮书的其中一份。负责本白皮书撰写工作的指导委员会于2021年7月中旬正式成立，3位主席由法国学者担任，10位委员分别来自全球不同国家。指导委员会围绕数字数据（digital data）、数字安全（digital security）和人工智能（artificial intelligence）这三个议题各组织4—5场线上专题研讨，并采访了来自学术界、政府、民间社会、私营部门等不同背景的法律和非法律专家。在指导委员会研讨内容的基础上，3位主席于2022年1—5月负责起草白皮书，并由指导委员会以协商一致方式通过。本白皮书不是一份学术性报告，而是试图强调未来的一些关键数字挑战及其对国际法的潜在影响。②理想的情况是，它有助于预测未来技术发展将引发的一些国际法问题，并使所有的利益攸关方能够理解这些问题，无论他们是否专门研究国际法或数字法。这些议题主要是从公法角度来探讨的，尽管也可能会对新兴技术的一些私人和商业用途（如数据的商业化）有所考虑。许多新兴的技术趋势（如元宇宙或数字货币的发展）可能只在涉及上述三个议题的情况下被讨论。鉴于数字技术的普遍使用及其对诸多国际法领域的影响，其中一些新发展也可能出现在其他委员会的白皮书中。

以下是本白皮书对三大议题的介绍：

---

*　武汉大学国际法研究所博士研究生。

**　武汉大学国际法研究所教授、博士生导师。

①　《国际法的数字挑战》白皮书由国际法协会于2022年8月31日发布其法文版和英文版，英文版见https://www.ilaparis2023.org/wp-content/uploads/2022/08/Numerique-VHD-EN.pdf。对本白皮书的中文翻译是为了促进学界对这一主题的关注和研讨，并不必然意味着译校者认可本白皮书的相关观点。此外，由于期刊版面限制，译校者对本白皮书进行了概况总结和摘编，但尽量保持客观中立，不改变本白皮书的原意。如需中译本完整版，可通过微信公众号“网络空间国际法前沿”留言获取。——译者注

②　因此，本白皮书将不会遵照通常的学术要求，包括在学理引注方面的要求。国际法协会150周年庆典网站将列出参考文献。

1.数字数据

数字数据无疑是网络空间以及国际数字法最重要的问题之一。首先,它构成了诸如人工智能等许多数字技术和创新不可或缺的基础。它是数字平台或社交网络等私人行为体构建其经济模式的基础。这些私人行为体的力量使数字数据成为一个政治问题,因为它被认为是一种可以被利用但也必须受到保护的资源。它已经成为一个战略问题,因为它处于私人和公共行为体之间以及每一类行为体内部权力关系的核心。数字数据的重要性,特别是对保护隐私的重要性,使其有理由成为法律、特别是国际法的客体。数字数据也可以成为一种法律工具,例如,可用于协助收集国家实践或法律意见(legal opinion)的证据。数字数据在其性质(个人数据、敏感数据、公共数据等),特别是在其用途(开放数据、商业目的、研究等)方面具有多面性。

2.数字安全

虽然信息通信技术(information and communication technologies, ICTS)的发展是为了强化国家和公民的安全,但是它已迅速导致国家和非国家行为体将其用于恶意活动——从传播被操纵的信息到发起破坏性的网络行动。的确,网络行动的普遍性与隐蔽性已被用于不同目的:间谍活动、破坏稳定、蓄意妨害、经济获利等。国家和非国家行为体之间的关系有时也难以区分。网络的互联互通以及非国家行为体在其发展和管理中的作用,使得数字安全在本质上成为一个国际问题,关系到公民、私人部门和国家的利益。因此,数字安全已成为国际安全、经济和社会发展以及人类安全的重大关切,它还构成了实现可持续发展目标的一个条件。

3.人工智能

人工智能可以理解为支撑不同技术(脸部识别、致命性自主武器等)和用途(商业或军事目的)的学习方法。人工智能的一个重要方面是机器学习,算法以此基于经验自动地自我改进。这一不断变化的因素可能会对这些算法是否符合国际法提出一些挑战。人工智能的快速发展伴随着许多挑战,有些挑战涉及国际法和国际关系。与网络空间的发展相反,人工智能本身并不被认为是一个新的领域,国际法的可适用性总体上也未受到质疑。然而,它提出了许多问题,特别是在归因、责任以及遵守国际法规则和原则方面。有趣的是,一些问题已经受到大量关注,而另一些问题则相对而言尚未被探索。例如,致命性自主武器系统(lethal autonomous weapon systems, LAWS)在文献中被大量讨论,也是多个国家间进程的主题,而关于人工智能对网络空间所发生行为的影响则讨论较少。此外,在规制人工智能的伦理和法律方法之间存在着重叠和交融。然而,在许多情况下,明确的区分是必要的。此外,人工智能技术也为促进国际法的发展和执行提供了新的途径,因此可能会对法律的实质内容产生影响。

一、现状

在过去几十年里,各国和国际组织越来越多地将其注意力和资源集中在使用新

的数字技术所带来的挑战和机遇上。在第一部分，我们将概述数字数据、数字安全和人工智能领域中最重要的国际规则和进程，对这三个主题的国际法主要适用规则和进程以及三个主题的主要特征（如地理分布、法律地位和内容、所属的法律分支等）进行简要评述。我们挑选的例子并不是一份穷尽式的法律文件清单，只是为了提供一些最突出的现有规则的样本。

鉴于当前的许多辩论和国际进程已聚焦于国际法如何适用于网络空间以及负责任国家行为规范的发展上，我们决定通过区分全球公认的概念和仍有争议的概念，概述关于国际法适用的现有争议（如关于主权、审慎、不干涉的含义的分歧），但并不试图解决这些争议。目的是让读者了解每个主题存在哪些规则（如果有的话），并注意到关于其适用的现有分歧。考虑到可适用于数字数据、数字安全和人工智能的国际法规则数量众多，此处的概述并不打算面面俱到，而是提供对当前辩论的总体认识。考虑到第二、三部分确定的挑战和问题，这部分的现状可以为评估现有规则和进程的充分性奠定基础。

现状中确定的规则和进程主要体现了地理范围、技术和法律上的碎片化。尽管对于国际法在数字领域的可适用性存在实质性共识，但在现有规则的地位、解释和适用方面仍存在重大分歧。此外，关于这三个主题的特定规则往往不具约束力、分布不均或者与国际法的具体分支相关联。

（一）数字数据

1.国际法的主要原则和规则

原则上，所有的一般国际法以及国际法的任何相关分支——如国际人道法、国际人权法（特别是隐私权、言论自由权和信息获取权）和国际贸易法——都适用于数字数据。

许多国际组织也已经完成或正在推进各种专门针对数字数据的技术和政治进程。联合国、欧盟、经济合作与发展组织（以下称“经合组织”）、非洲联盟、西非国家经济共同体（以下称“西共体”）和非洲其他次区域组织、七国集团和二十国集团、世界贸易组织（以下称“世贸组织”）都在根据各自的职责处理与数字数据有关的问题。国际组织或进程通过的文本实例包括《非洲联盟网络安全和个人数据保护公约》、东盟跨境数据流动示范合同条款、《欧盟—日本自由贸易协定》《通用数据保护条例》等。[①]

2.现行规则概述

关于数字数据的现有国际法仍处于萌芽阶段。除了欧盟法之外，很少有专门针对数字数据并具有约束力的国际法规则。事实上，大多数涉及数字数据的全球性、

① 此处文本实例作省略处理，详见中译本完整版。——译者注

区域性或双边文书都是通过解释或将数字数据归入更大的客观范畴(如人权文书中规定的隐私权)。尽管通过经合组织和欧洲委员会的工作,国际数据保护框架自20世纪70年代以来就存在了,但大多数专门针对数字数据的规则都是在有限的背景下通过的,主要是在数据保护、网络犯罪和贸易法领域(如通过《服务贸易总协定》或《与贸易有关的知识产权协定》)。

与数字安全领域相反的是,早期的非约束性文书(如经合组织的隐私指南)在逐步转向约束性文书(如《通用数据保护条例》),尽管大多数规则仍可在国内法中找到。在国际层面,专门针对数字数据的文书非常少。大多数关于数字数据的现有国际规则可以在欧盟,非洲联盟(如《马拉博公约》,尽管它尚未生效),欧洲委员会(关于数据保护的第108号公约、《网络犯罪公约》),经合组织,西共体以及非洲和亚洲的其他区域或次区域国际组织的区域法律中找到。双边行政协定和条约也是现有规则的一个重要来源。

3.共识性规则与争议性规则概述

原则上,对于一般国际法和国际法的各个相关分支(国际人权法、国际人道法、国际责任法等)在数字领域的可适用性,包括与数字数据有关的问题,存在着广泛的共识。对数据保护的主要参考因素(更正权、监管机构等)也有相对一致的意见。

然而,在个人数据的定位、隐私的概念以及现有人权法的适用方面,存在着许多文化和法律上的差异。各国和各地区的数据保护方法在不同的司法管辖区之间有很大的不同,这加剧了法律的碎片化。在网络犯罪和管辖权领域,特别是关于适当的数据保护标准(如Schrems案①)和管辖权标准对数据的跨境获取也存在许多分歧。最后,数据自由流动的观念正面临着越来越多的阻力,这从贸易法的角度提出了重大挑战。

(二)数字安全

1.国际法的主要原则和规则

原则上,所有一般国际法以及国际法的任何相关分支都适用于数字安全。

许多国际组织也已经完成或正在推进各种专门针对数字安全的技术和政治进程,其中包括联合国[联合国毒品和犯罪问题办公室主持的联合国网络犯罪全球方案,联合国信息安全开放式工作组(以下称"OEWG")和信息安全政府专家组(以下称"GGE")进程,拟订"打击为犯罪目的使用信息和通信技术"的全面国际公约的开

① 欧盟法院(Court of Justice of the European Union, CJEU)在2015年、2020年的Schrems Ⅰ和Schrems Ⅱ案(奥地利公民Maximilian Schrems与Facebook的隐私权侵害诉讼案)判决中,基于美国未能提供实质上等同于欧盟的数据保护水平的认定,分别否决了欧美数据传输《安全港协议》(Safe Harbor)和《隐私盾协议》(Privacy Shield)框架的有效性。——译者注

放式特设政府间专家委员会],国际电信联盟[国际电信联盟区域网络安全中心、电信标准化部门(ITU-T)研究组、全球网络安全指数等],经合组织(数字经济安全与隐私工作组),欧洲安全与合作组织,区域和次区域组织(美洲国家组织、非洲联盟、东盟)。在诸如打击恐怖主义、仇恨言论或加强网络安全方面,也有若干利益攸关方的倡议[科技反恐、全球互联网反恐论坛、信任与安全巴黎倡议、基督城倡议(Christchurch Call)]。

国际组织或进程通过的文本实例包括《东盟打击网络犯罪宣言》等。①

2.现行规则概述

除了网络犯罪领域和欧盟法之外,很少有专门针对数字安全的具有约束力的国际规则。然而,许多不是专门针对数字安全的有约束力的文书也是可适用的。关于数字安全的非专门性规则在全球层面(如禁止使用武力、国际人道法、国际人权法、国际空间法、国际电信法)和区域层面都可以找到。

网络犯罪和国际安全是我们发现存在有关数字安全的专门性规定的两个主要领域。在关于恐怖活动的文书中也可以找到这类规定。贸易法也可能越来越关注数字安全,特别是因为在信息和通信技术领域施加安全要求可能会对贸易造成障碍,并违反现有的贸易规则。与网络安全领域不同的是,除了在反恐宣传以及可能在人权法(特别是自由和公平选举的权利以及信息自由/获取信息的权利)和主权(破坏政治制度稳定)方面有所涉及以外,信息行动在大多数规范性倡议中还尚未得到解决。

3.共识性规则与争议性规则概述

原则上,对于一般国际法和国际法的不同分支(国际人权法、国际人道法、国际责任法等)在数字安全领域的可适用性已存在广泛的一致意见。然而,尽管对国际法的可适用性有了一定的共识,但关于其解释和适用于网络空间的许多问题仍存在争议。关于国际法的实质内容(例如,网络空间是否存在某些国际法规则或原则,如审慎和主权),关于其规则和规范在网络空间的解释(不干涉的门槛和强迫要素、数据作为国际人道法下受保护的"物体"、非物理影响与使用武力/武装攻击)以及实施(如归因)等问题,都存在尚未解决的分歧。尤其是在将国家责任法扩展到数字活动方面,特别是在归因、反措施和防卫问题上,一直存在许多分歧。总体而言,对国际法适用于数字安全的关注是不均衡的:在某些国际法规则(如禁止使用武力)上分歧的解决受到了相当程度的重视,而其他一些规则(如人权)的处理则要粗略得多。②

① 此处文本实例作省略处理,详见中译本完整版。——译者注

② 例如,在《网络行动国际法塔林手册2.0版》(剑桥大学出版社2017年版)184条规则中,只有5条专门涉及人权问题。

（三）人工智能

1.国际法的主要原则和规则

关于人工智能的国际讨论和规范性文书很大程度上聚焦于伦理问题，并往往与法律问题相重合。联合国教科文组织推出的《人工智能伦理问题建议书》是一个典型的例子，它从伦理的角度看待人工智能，同时又在实质上包含详细的法律条文。以下将概述关于人工智能的现有国际法律文书，但不深入探讨其伦理含义。

在国际层面上，专门针对人工智能并具有约束力的规则，即使有也很少。然而，有一些国际人权法标准可以直接适用于人工智能，这可能包括思想自由、隐私和非歧视等相关权利（如《公民权利和政治权利国际公约》《经济、社会和文化权利国际公约》《欧洲人权公约》《美洲人权公约》《非洲人权和民族权宪章》《打击对妇女使用暴力行为的伊斯坦布尔公约》等所载的权利），以及其他可涵盖国家使用技术的宽泛性国际规则。人工智能技术已经在敌对行动中被运用，因此关于禁止使用武力、武装冲突法以及其他相关国际法规则的问题也与此有关。

除了这些一般性文书，越来越多的国际组织正在通过专门针对人工智能的规则，其中包括欧洲委员会、经合组织（关于人工智能的理事会建议）、联合国教科文组织（关于人工智能伦理的大会建议）、国际电联（特别是通过“人工智能造福人类全球峰会”）。在联合国，关于人工智能的国际安全影响的讨论聚焦于LAWS的发展上。2013年，这一问题被列入《禁止或限制使用特定常规武器公约》缔约国会议的议程。经过几次非正式会议后，采取了与国际网络安全问题类似的讨论形式：2016年成立了政府专家组，并于2019年12月通过了关于LAWS的11项指导原则。通过这些原则，政府专家组肯定了国际法特别是国际人道法以及一系列道德和非约束性原则的可适用性。就本白皮书而言，值得强调的是，这些致命性自主武器系统原则没有提及自主网络能力。[①]国际组织或进程通过的文本实例包括《本杰里尔宣言》、联合国教科文组织《人工智能伦理问题建议书》、联合国LAWS政府专家组2019年通过的关于LAWS的11项原则；等等。[②]

2.现行规则概述

人工智能可能是大多数国家都愿意通过新文书的极少数数字主题领域之一，联合国教科文组织在2021年11月通过的《人工智能伦理问题建议书》就表明了这一点。对人工智能进行规制的尝试高度碎片化，并因对不同技术或用途的考虑而有所不同。关于人工智能的现有国际法处于非常早期的发展阶段，尽管目前有多个正在

① 第六项原则，即原则（f），只是简要提及网络安全是“在开发或获取基于致命性自主武器系统领域新兴技术的新武器系统时应考虑的适当的非物质保障措施”之一。

② 此处文本实例作省略处理，详见中译本完整版。——译者注

推进的倡议和进程，并且有时在内容上有一定程度的重叠。

关于人工智能的专门性国际规则数量有限，但这并不意味着人工智能不受国际法的规制。事实上，国际法的现有规则和原则对于规制人工智能技术及其不同用途是有关联的。然而，对于这些规则究竟如何适用于人工智能，仍然存在一定程度的不确定性。目前还没有专门针对人工智能且具有约束力的国际法规则。但是，关于人工智能的一般性或针对某些特定应用程序（例如，人工智能在健康、劳动力市场和教育方面的应用，自动驾驶汽车，人工智能在刑事司法领域的使用等）的不具有约束力的规范数量越来越多。

3.共识性规则与争议性规则概述

原则上，对于一般国际法和国际法的不同分支（国际人权法、国际人道法、国际责任法等）对人工智能的可适用性存在共识。然而，国际法上仍然没有关于人工智能的定义或概念的清晰立场，也不清楚目前的规则是否足够或有效，以及是否有必要制定新的规则（如在人权等方面）。在这种情况下，人类是否以及如何能够保持对人工智能的控制，进而是否需要对此制定新的规则，成为一个重要而备受讨论的话题。

4.人工智能对国际法的影响

前几段概述了国际法如何规制人工智能的不同层面。然而，值得注意的是，人工智能的某些应用的发展可能会影响到国际法的实质内容、与国际法有关的决策进程、造法进程以及相关规则和原则的实施和执行。例如，机器学习和计算文本分析可用于争端解决、条约谈判和国际裁决等方面，收集和处理重要数据集的能力可用于识别违反国际法规则或原则的行为。

（四）结论

从以上这些“现状”可以得出两方面结论：首先，存在以下共识，即国际法可适用于全部三个主题，且相关规范性文书有着宏大的多样性。有约束力的文书在范围上相当宽泛，没有专门涉及这三个主题中的任何一个。另一方面，在区域和全球层面，也存在着大量专门针对数字数据、数字安全或人工智能的非约束性文书。

第二点结论涉及三个主题中存在的共同挑战。我们可以看到，对于一般国际法的相关问题，以及对于国际法规则和规范在网络空间的相关性、解释和实施，都存在尚未解决的分歧。这些分歧可部分归咎于数字领域实力强大的国家和区域集团在当前谈判中有着不同的文化路径。下一部分将介绍三个关键的挑战。

二、挑战

数字数据、数字安全和人工智能领域新技术的出现，有着深刻的政治、社会和经济影响，既包括积极的影响也包括消极的影响。尽管使用数字技术所带来的挑战和

机遇中有部分是针对具体领域的，我们也找到了三个共同的挑战，它们贯穿了所考虑的全部三个主题：公共行为体与私人行为体之间的关系，国际法在数字问题上的政治工具化，以及数字不平等的普遍存在。事实上，尽管数字领域在技术、法律和地理上都呈现出碎片化（从现状部分收集的规则和程序可以看出这一点），但这些挑战是普遍存在的，并给关注全部三个主题的政策制定者、国际法律工作者和研究人员提出了难题。

尽管这里所列举的挑战并非穷尽式的，但它们可能会塑造未来若干年关于数字技术的辩论。它们也可能在数字以外的领域产生影响，如对国际法协会为迎接其150周年诞辰而正在考虑的其他一些主题而言，国际法也正在努力应对日益加剧的政治分化、持续存在的不平等和关于非国家行为体日益复杂的格局。至关重要的是，这些挑战往往是相互依存的，例如，公共行为体与私人行为体的关系会牵涉到往往不平等的数字能力的分配，而这两大挑战都被归入更广泛的有关数字问题国际法辩论的政治化之中。因此，对拟议解决方案的任何评估都必须考虑其对其他挑战和机会的外部影响，无论这一影响是积极的还是消极的。这一部分将对这三大挑战逐一加以讨论，并通过数字数据、数字安全和人工智能领域的例子加以说明，以达到理解它们所带来的困难和机遇这一目的。

（一）公私界限

就公共行为体和私人行为体之间的角色和责任应如何进行适当分配进行的辩论，是全球化进程中反复出现的特征。在数字领域，基于私人行为体对新技术的开发和使用，人们对国家是否有能力有效规制信息获取和网上言论，以及在确保数字环境安全的同时不会抑制创新，既保持乐观，也有所担忧。跨国公司，特别是大型在线服务提供商，控制和利用了大量与公共治理、经济活动和个人权利密不可分的数字数据，同时也处于人工智能技术发展的最前沿。它们的数据保护能力也是网络安全工作的一个关键组成部分，它们在预防、检测和应对恶意网络行动方面有着突出的作用。这些技术和数据是这些公司的收入来源，但也是服务公众利益的宝贵工具。相反，其他一些非国家行为体，无论是团体还是个人，也应当对发起恶意行动承担责任，而且有时应与国家密切合作。因此，国家与各种私人行为体之间、私人领域与公共领域之间关系的参考因素，是关于数字数据、人工智能和数字安全辩论的重要组成部分，下面将对未来的一些主要挑战进行概述。

1.数字数据

——私人行为体和公共行为体的数据收集、存储和分析

私营公司对通常包含个人数据的巨大数据集进行分析，并利用它们来开发新的应用程序和技术，也用于各种商业活动，如发布广告或针对特定个人和群体来开发产品或服务。各国政府也对数字数据感兴趣，无论是为了监控还是为了改善公共管

理的目的。国际组织也将数据作为一种战略资产。[①]因此，包括国家和国际组织在内的诸多行为体都对生产、控制和使用数字数据有着极大兴趣。然而，大多数数字数据都掌握在私人行为体手中，公民几乎完全依赖这些行为体来保护他们的数据和相关权利。许多私人行为体拥有比政府更多的公民数据，这导致了对通过私营部门来实现政府职能的依赖性。例如，在新冠疫情带来的危机中，来自监控和科技行业的公司向卫生部门提供服务，将其大数据分析作为应对大流行病挑战的工具。在俄乌冲突中，一家据悉在线收集了数十亿张个人照片的美国公司Clearview，所持有的数字数据被乌克兰政府用来确认死者身份和打击错误信息。[②]同样，深度造假技术的创造、使用和检测涉及私人行为体以及公共行为体。

公共行为体与私人行为体之间的角色和责任之间界限模糊的另一个方面涉及行使管辖权所需的合作。例如，在刑事调查中，国家往往需要与私营部门合作来收集数字证据。为了打击虚假信息和仇恨言论，它们也经常被迫与数字平台合作。以法国为例，2015年前后，在推特公司最初拒绝依照法国法律撤下某些内容后，法国政府不得不与该公司就此进行谈判。相反，数字平台有时也会为国家本身实施的违反国际法的行为提供便利，Meta公司（当时的Facebook）被指控没有采取足够措施来防止缅甸当局通过其平台煽动种族灭绝，也许就是这方面的一个例子。

国际组织和法院也面临着类似的挑战，联合国秘书长在《联合国数据战略》中强调了这一观点。例如，国际法院关于适用《防止及惩治灭绝种族罪公约》案（冈比亚诉缅甸）的结果，可能取决于它能否迫使Meta公司交出相关数据。[③]如果说收集数字数据的能力可能为实况调查团和国际正义的实现提供新机遇，它也对证据链和这些数据的证明价值提出了新挑战，包括由非国家行为体以及在正式调查程序之外收集数据的情况。[④]

最后，私人行为体通过参与以往专属于公共当局的活动，直接与国家开展竞争。一个很好的例子是加密货币的发展，迄今为止这在很大程度上脱离了大多数国

① See for instance, the U.N. Secretary General, Data Strategy of the Secretary-General for Action by Everyone, Everywhere with Insight, Impact and Integrity (2020) ; ITU, New UN Targets Chart Path to Universal Meaningful Connectivity (19 April 2022) ,https://www.itu.int/hub/2022/04/new-un-targets-chart-path-to-universal-meaningful-connectivity/.

② Paresh Dave, Jeffrey Dastin, Exclusive: Ukraine Has Started Using Clearview AI's Facial Recognition During War (Reuters, 14 March 2022), https://www.reuters.com/technology/exclusive-ukraine-has-started-using-clearview-ais-facial-recognition-during-war-2022-03-13/.

③ Michael A. Becker, The Gambia v. Facebook: Obtaining Evidence for Use at the International Court of Justice (Part I) (EJIL: Talk!, 5 October 2021), https://www.ejiltalk.org/the-gambia-v-facebook-obtaining-evidence-for-use-at-the-international-court-of-justice-part-i/.

④ 最近在乌克兰的冲突中，Bellingcat的开源调查就是一个很好的例子，https://www.bellingcat.com/tag/ukraine/?fwp_categories=news&fwp_tags=ukraine。

家的国内法以及国家对货币的主权权利的范围。这些发展对私人实体的角色和责任,以及对它们与国家在实现政府职能方面的关系提出了质疑。

——数据与数字经济

数据在私营部门围绕新技术发展起来的经济系统——电子货币、平台和新支付服务、数字资产等——中处于核心地位。私人行为体对数据的控制可能会产生四种类型的问题:一是在处理数据的方式上,商业逻辑和安全(包括法律安全)逻辑之间的对抗。在法律安全方面,提出了不同的问题——从涉及法律适用的具体问题到涉及国家安全的集体问题。二是数据问题规制方式的地缘政治做法与商业做法。三是经济主体与规制主体之间存在分歧和缺乏沟通及对话的风险,因为前者不一定了解后者制定新规则的考虑,这可能会影响法律的内容以及适用。四是什么需要加以规制的问题,可能没有必要将所有事项纳入法律之中。

经济部门强大的私人属性或许表明,规范性工作应主要集中在法律冲突问题上,但也需要就新文书的实质性条款开展工作,正如国际统一私法协会通过其"数字资产与私法"项目所做的那样。一些部门已经开始发生变化。受到高度监管的银行和金融部门已经接受的一点是,风险可以在不会导致其商业实践的完整性受到质疑的情况下存在。为了适应新的挑战,各国和国际组织已经采取共同的方法,来防止为犯罪目的滥用加密货币。[①]在网络安全事件报告领域,举例而言,欧盟《通用数据保护条例》是要求私人行为体承担报告义务的一个起点。

数字经济的数据不仅要求改变法律的内容,也要求改变法律的制定方式。所有这些数据都可以用来更好地了解实践,从而根据需求甚至预测需求来制定法律。私人行为体在收集和分析这些数据中的作用,使我们不禁要问,在制定标准的过程中可赋予它们什么样的角色。该部门的公私混合性质鼓励人们进一步思考"协作性国际法"(collaborative international law),[②]即改进国际法的制定、适用和解释机制,以使其更有效和高效。

总之,这里有两个主要挑战:一方面,规制需要考虑到技术中立性;另一方面,需要制定一套共同的最低标准,在保护个人和集体利益的同时促进技术发展。为了维护经济稳定,不应对法律进行彻底改变,但它必须根据现实世界的需要而发展。

——数据与规范多元性

与公私界限问题相关的另一方面挑战是私人行为体作用和重要性日益增强所带来的规范多元性。主要网络平台的服务条款和社区准则所设定的规范(如关于言

① See, FATF, Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Assets Service Providers (2021), https://www.fatf-gafi.org/publications/fatfrecommendations/docu-ments/guidance-rba-virtual-assets-2021.html.

② See Catherine Kessedjian, Le Droit International Collaboratif (Pedone 2016).

论的规制）是平台采取行动和进行内容规制的基础，它们成为适用于平台“虚拟领土”的事实上的规范，并与在一国之内适用的法律相竞争。有趣的是，服务条款中正在纳入通常属于公共立法范畴的内容。例如，Meta公司的监督委员会在自其成立以来做出的多个决定中，一直在援引国际法。[①]这就导致了私人规范和公共规范之间既竞争又互补的局面。

2.数字安全

在数字安全领域，公共和私人之间的模糊区别从威胁状况本身就可以看出。首先，国家，包括那些拥有先进能力的国家，可能会通过精心设计的方式，在不施加那些引发其自身责任的控制的情况下，允许或促进非国家行为体的活动。为了国家的利益或应国家或多或少的明确要求而进行的活动与为了威胁行为体自身的利益而进行的活动之间，界限也可能是模糊的。就能力而言，代码可以被泄露，工具可以被许多行为体再次利用，“影子经纪人”[②]的泄露以及国家和非国家行为体的再次利用就是例证。反过来说，可以通过相关工具的开发和使用来掩盖实施者的身份，并使其识别变得复杂。其次，数字威胁的影响进一步模糊了公共领域和私人领域之间的界限。正如过去许多恶意网络活动所表明的那样，恶意活动的影响可能会扩散得比最初的目标远得多。就其本质而言，信息行动也跨越了所有的界限（公共与私人、民事与军事等）。最后，为了在数字空间保护自己或他人，非国家行为体可以行使通常专属于国家的特权。然而，所有这些界限的模糊有一个好处：任何提高一个行为体安全水平的努力都可能使其他行为体受益，并使任何人都更难利用现有的漏洞进行恶意活动。

国家与非国家行为体之间的关系在确保国家安全和更广泛的国际安全方面也有其意义。确保数字领域安全的重要性，极大地增加了私营网络安全公司和计算机应急小组的力量。它们与国家的协作和关系已经成为一个重要的讨论话题，特别是在网络行动的归因、关键基础设施的安全和打击网络犯罪方面。各国越来越依赖私营公司来存储和保护敏感数据和关键基础设施，它们也经常被迫与网络安全公司合作，以防止、识别和应对网络安全威胁。国际刑警组织等国际组织也是如此。私营公司，特别是数字平台，在遏制有害信息行动的努力中也有着特别突出的作用，各国在很大程度上依赖它们。欧盟《反虚假信息行为准则》和拟议的《数字服务法》是这方面的关键倡议，还有各种国家进程（例如，目前关于英国《在线安全法案》的谈判，美国关于改革《通信净化法》第230条的讨论，各种遏制虚假信息的国内法等）。最终，国家和私营公司在内容审核和信息行动方面的关系将决定谁能控制互联网上的言论。

---

① 关于这些决定的清单，可参见https://www.oversightboard.com/decision/。

② 一个黑客组织，它在2017年4月泄露了一大批美国国家安全局开发的网络攻击工具。——译者注

私营公司、非政府组织和个人在数字安全国际谈判中的角色，已成为一个突出的讨论主题。例如，关于民间社会参与联合国GGE和OEWG进程以及网络犯罪特设委员会的规则一直是参与国之间许多分歧的根源。[①]私营公司（尤其是微软）也对参与联合国和更广泛的国际谈判非常感兴趣，尽管它们的参与程度差异很大。关于国家和民间社会/私营公司各自角色和责任的讨论，提出了有关国际立法的正当性和利益攸关方之间的权力平衡的重大问题，这一平衡可能在规范制定的不同阶段有所不同。挑战之一是设计出能够容纳所有相关行为体参与的机制性结构，同时保留国家在规范制定和决策方面的关键特权。如果多边和以国家为中心的进程不成功，其他参与者和进程也有可能填补空白。诸如关于网络空间国际法保护的牛津进程[②]或塔林手册（经常被各国引用和辩论，有时甚至出现在关于国际法适用于网络空间的国家立场中）已经表明，如果它们成功地获得足够多国家的支持，它们就会发挥作用。私营公司也在数字安全领域发起了各种进程，例如《信任宪章》（西门子）、《网络安全技术协议》（微软），以及在打击恐怖主义背景下发起的进程（尤其是全球互联网反恐论坛）。

最后，国家与非国家行为体之间的关系还在规范多元性领域得到体现。对于物理层和逻辑层，安全在很大程度上是由非国家行为体来界定的。全球性标准[如国际标准组织（ISO）的标准]塑造了技术的未来，互联网的架构也是由非国家行为体来管理的。由于安全并不总是技术要求的优先事项，或者因为国家安全问题而被降低，[③]技术要求和安全程序，例如在漏洞披露的情况下，可以直接或间接地影响安全水平。即使国家能够影响这些规范，它们在这一领域也被剥夺了很大的权力，不得不处理私人的技术规制。在虚假信息领域，存在着协同规制和自我规制的不同努力。

3.人工智能

当今，非国家行为体，特别是私营公司和研究机构，是人工智能技术和应用开发的主要行为体。即使各国正在开发自己的人工智能应用程序，它们也大多（至少部分）是基于非国家行为体开发的技术解决方案。一个人工智能应用程序可能是不同行为体（与国家相关的行为体或非国家行为体）开发的不同解决方案的结果，因此导

① 参见英国最近提出的关于多利益攸关方参与OEWG的决议，United Kingdom of Great Britain and Northern Ireland: Draft Resolution. 非政府组织、民间社会组织、学术机构、私营部门参与2021—2025年OEWG的方式（2022年4月7日A/76/L.49），或关于多利益攸关方参与网络犯罪特设委员会的辩论；联合国大会通过决议，概述网络犯罪条约谈判条件，同时担心草案的投票会损害进一步磋商（2021年5月26日GA12328）。

② Oxford Process on International Law Protections in Cyberspace, https://www.elac.ox.ac.uk/research/the-oxford-process-on-international-law-protections-in-cybers-pace/#:~:text=The%20Oxford%20Process%20on%20International%20Law%20Protections%20in%20Cyberspace%20is,2020%20in%20partnership%20with%20Microsoft.

③ 参见斯诺登曝光的加密和美国的监控。

致这些不同行为体之间的边界模糊。在这方面，与公共行为体和私人行为体之间关系和责任分配有关的问题与人工智能尤其存在关联。此外，人工智能的发展需要获取数据，而这些数据通常由私人行为体持有，这引发了与私人行为体和公共行为体在上述数据收集、存储和分析背景下已经讨论过的问题类似的担忧，本节不再赘述。

非国家行为体在国家主导的人工智能使用中的作用以及它们与国家的关系，表现形式有很大不同。为了执行某些任务，包括那些与公共权力密不可分的功能，国家机构和代表国家行事的其他实体一直在使用由私人行为体开发的人工智能应用程序。例如，人工智能解决方案越来越多地用于边境和移民控制、[①]刑事和金融调查或冲突背景。[②]所谓的“电子卫生部门”的发展也可以表明，公共和私人行为体之间的关系何以具有挑战性，因为私人开发的应用程序收集的数据可能会被公共卫生机构使用。使用人工智能技术开展某一特定活动，可能是国家和非国家行为体为开发、改造和使用某些技术而开展的不同活动的结果。非国家行为体所扮演的角色如此多样化，也对国际法把握这些关系的方式提出了挑战。

（二）网络空间法律的政治性

鉴于数字技术重大的社会和经济影响，关于其治理的国际辩论往往具有争议且充满政治色彩。制定法律规则和不具约束力的规范，已成为政治辩论和战略制定的对象，以及各国和其他利益攸关方促进其互联网治理（甚至可能是更广泛的治理）愿景的途径。

1.数字数据

目前存在几种不同的数据保护模式。举例来说，尽管有过于简单化的风险，我们可以突出强调欧洲模式（将数据视为人的属性，值得提供最有力的保护）、美国模式（将数据视为资产，并支持其自由收集和使用——特别是在商业基础上）以及新兴的中国模式（专注于维护主权和安全）。这三大模式具有共同的特征，但也有非常不同的底层逻辑，这导致其支持者对国际既定标准的解释存在分歧，并设想了不同甚至相反的数据保护和控制方法。

通过围绕规范性文书的域外效力以及国家和国际组织的行动能力等问题，这些不同模式之间的对抗得以体现。更广泛地说，我们正在见证两种相互竞争的逻辑之间的对立，一种优先考虑数据的自由流动，另一种优先考虑数据的保护。国家和区域集团根据自己的价值观来捍卫不同的规范性文书是正当的，但这些文书的域外效力可能导致规范和管辖权冲突的增加。解决办法不仅在于制定关于规范和管辖权

① See for example European Parliament, Artificial Intelligence at EU Borders. Overview of Applications and Key Issues (2021).

② 设在美国的公司 Clearview AI 提供了一个相关的例子，因为其脸部识别应用程序已被美国执法部门使用，并且最近被提供给乌克兰政府，用于识别在乌克兰遇难的俄罗斯士兵。

冲突相关规则，还在于国际公法和国际私法的实体规则的发展。

最重要的是，它还取决于在不同的规范体系之间发展适当的对话、合作甚至互补机制，无论是在法律形成阶段还是在法律实施阶段。在这个意义上，如果能够将跨境信息流动中的个人数据保护列入联合国国际法委员会长期工作方案[①]，可能会是一个有趣的前景。对法律的政治性的反思促使我们思考如何改进法律机制，以制定真正的国际法，并对本报告下文讨论的数字鸿沟予以回应。

2.数字安全

人们普遍认为，网络和信息方面的数字威胁的数量和复杂程度将继续增加。根据对几位专家的采访，从复杂的国家支持的网络活动到低级威胁，恶意活动（网络犯罪、网络恐怖主义、对关键基础设施的攻击、网络间谍活动、大规模监控、信息行动等）的性质可能会保持不变，但它们的复杂性、规模和执行速度将会增加。数字领域不断上升的不稳定性和不安全性，已经并将因此继续成为许多法律和政治辩论的主题。事实上，虽然许多行为体花费大量资源来应对这些威胁，但国家和非国家行为体也从恶意活动的实施中受益，不太可能大幅限制它们的选择。这将影响相关法律的内容以及立法进程。

今天，网络安全国际谈判的主要挑战不是法律性质的，而是地缘政治性质的。通过关于数字安全的国际谈判，各国竞相提出不同的互联网/信息通信技术治理概念：一些国家将数字领域主要视为促进经济繁荣的机会，其他国家则关注其确保人类繁荣的潜力，而另一些国家则优先考虑国家安全。这些不同的愿景在一国之内同时存在但有时相互冲突。这些愿景都会影响各国思考和讨论国际法的方式、对其解释的选择以及各国设想的国际法规则的种类。例如，优先考虑经济发展的国家寻求保护创新的国际法规则，聚焦人权的国家则强调隐私或加密，而那些主要关注国家安全的国家则寻求超越网络安全保护，以便对用户进行去匿名化和/或对数字内容实施控制。国家还可以自愿地利用国际法解释方面存在的挑战，制造新的不确定性，加大当前情势中的混乱和不稳定。在指导委员会为准备本白皮书而进行的采访中，有人提出，这种情况并不一定意味着国际法是问题或解决方案的根源，缺乏法律确定性并不是遵行法律的主要障碍。它是更大范围内的多边主义危机的一部分，国际法已成为政治竞争的工具。虽然一些国家有兴趣保持现状，但其他国家看到了提出新规则和促进自身利益的机会。

数字外交面临的地缘政治挑战也涉及网络空间本身的模式。随着网络空间的碎片化和对网络基础设施的政治控制加剧，21世纪头十年间关于国际电信联盟作用的辩论再次涌现。这加剧了关于互联网治理多利益攸关方模式的辩论，并进一步加

① International Law Commission, Report on the Work of the Fifty-eighth Session [2006]A/61/10, Annex D.

大了关于网络空间形式和实质规制的不同看法间的分歧对立。

在网络犯罪领域，当试图在负责制定联合国框架内新的网络犯罪条约的特设委员会中达成共识时，法律的政治性也会产生类似的不信任后果：网络犯罪国际规制的碎片化以及对人权的影响。事实上，我们正在见证这样一种局面：打击网络犯罪越来越多地从国家安全而非刑事司法的角度来框定，这威胁到人权和基本自由，限制了任何合作的意愿。

其后果体现在三个方面。首先，它直接影响各国在国际安全框架内达成任何有意义的协议以更好地确保网络空间安全与稳定的能力。其次，它加剧了国家之间的分歧，加强了志同道合的国家围绕共同价值聚集起来结成联盟的逻辑，从而加大了规章制度的碎片化。最后，它导致了这样一种情况，即我们看到一些安全问题被置于经济视角下来克服当前的障碍。例如，经合组织——一个专注于经济发展的国际组织，已经开始研究安全问题，如漏洞披露、信息通信技术供应链安全、私人行为体使用黑客回击。

关于数字安全国际谈判的内容有许多富有争议的讨论，而进行这些谈判的各种进程也产生了重大的政治影响。这一点在联合国谈判的背景下尤为明显，最受关注的谈判是通过联合国GGE进程（最后一届由美国及其盟友单独发起）和俄罗斯发起的OEWG进程进行的。这些进程具有重要的政治意义，各国和所有其他感兴趣的利益攸关方积极谈判和讨论了这些进程的报告。至关重要的是，国际法及其在网络空间的适用问题是这两个进程的核心。

各国一直不愿就国际法在数字安全领域的适用问题发表确切看法（从而妨碍了对有关法律——无论是基于条约的法律还是习惯法——的澄清），尽管2021年GGE最终报告（A/75/135）发布的同时，一些国家令人瞩目地发布了关于在网络空间适用国际法的国家声明（A/76/136）。这些声明的价值和政治意义将成为大量辩论的主题：它们可以被视为澄清法律和争取各国支持的工具，但也可能被视为进一步侵蚀业已脆弱的多边进程的一种单边主义形式。

最终，未来几年的关键挑战之一将是确定适当的场所来讨论敏感的数字安全问题及其与国际法的相互作用：联合国进程的重要性很可能保持不变，特别是通过OEWG和负责制定联合国框架网络犯罪条约的特设委员会最近的职责。未来几年，联合国的网络犯罪谈判将受到很大关注，因为它们可能会重新审视GGE和OEWG讨论的规范，和/或扩大关于“网络犯罪”范围的理解，将信息行动包括在内，甚至可能触及国家归因等主题。其他职责更具体的国际组织也可能发挥突出作用，特别是国际电联、经合组织[已经从经济视角开展网络安全工作，见上文第（一）部分]、区域人权和经济一体化组织（欧洲委员会、美洲国家组织、非盟、东盟等），甚至世贸组织（安全关切和技术壁垒被越来越多地援引和提出，以限制数字产品和服务贸易）。这

些进程的选择和协调(或不协调)可能取决于最强大国家的政治利益和对立情绪,而且很可能影响到谈判规则的内容。关于国际法的解释,目前没有任何传统机构,如联合国大会第六委员会、国际法委员会或国际法院,能够承担起澄清这一问题的任务。这就使得诸如国际法研究院(Institute for International Law)[①]或国际法协会等非多边机构可以发挥重要作用。与此同时,《塔林手册》和牛津进程等其他倡议也已经介入(国际法的解释)。

进行数字安全国际谈判的普遍性场所和进程,对发展中国家的积极参与也有深远影响。有一种风险是,发展中国家缺乏参与,可能导致反映大国利益的规则和原则被通过,这可能进一步侵蚀未来几十年人们所认为的数字安全国际法的正当性。由于未能整合发展中国家的观点,所通过的规则可能会对发展中国家缺乏意义或者有害,而不是帮助更多的发展中国家参与对话并减少数字不平等(见"普遍存在的数字不平等"部分)。然而,应当指出的是,在参与普遍进程的程度和影响以及次区域层面强有力的规范制定之间,存在着重要的区别。在对网络空间国际法的解释领域,区域层面也正在做出努力,美洲国家组织美洲司法委员会"提高各国对网络空间国际法看法透明度"项目的工作就是例证。[②]

3.人工智能

关于网络空间法律的政治性有两大核心挑战,它们与人工智能有关,并已经在前面的章节中讨论过。首先,法律问题和伦理问题有着很大程度的重合,这本身不是一个问题,但仍然带来一些问题。粗略一看,有关讨论和倡议似乎主要集中在伦理问题上。然而,仔细观察这些讨论就会发现,法律问题和规范是这些讨论的中心,也是理解所通过的文书的基础。因而,伦理似乎更像是推进与将国际法适用于人工智能的有关事项的切入点。因此,道德问题与法律问题之间的界限并不总是明确的。应当指出,这可能是一个值得关注的问题,因为它可能影响法律规则的价值或实质。其次,在国际安全领域,注意力主要集中在LAWS上,因此,现有讨论中往往没有涉及其他利用人工智能应用程序进行的不友好或敌对行为,这可能会加剧两极分化。例如,在多边场所中,几乎没有讨论过自主网络行动以及如何对其进行规制,尽管此类行动已客观存在。

第三个重要的挑战是:在将人工智能作为一个整体加以处理以及选择更专注于特定的人工智能技术及其使用这两种做法之间,如何寻求适当的平衡。不同的技术和应用会带来不同的法律问题。这一挑战导致了双重困难:一方面,关于人工智能的法律问题即使有也非常有限,但关于人工智能产品的具体应用和后果的问

① 2021年,国际法研究院成立了一个委员会,研究国际法对网络活动的可适用性。

② Organization of American States Inter-American Juridical Committee, International Law and State Cyber Operations [2020].

题却非常多。在某种程度上，这一挑战涉及界定何者构成人工智能，以及国际组织和进程应如何加以处理的难题。另一方面，这也有实际的后果，因为同时进行着不同的讨论和进程，每一种讨论和进程都集中于相当有限的一组问题和应用领域，目标也非常不同。最后，在某些情况下，关于人工智能的讨论是偶然的。在这些情况下，所处理的不是人工智能本身，而是根据可能影响人工智能的问题做出决定。这方面的一个例子是，在暴力极端主义和恐怖主义领域，可以在暗示使用人工智能的情况下建议采取预防措施。然而，这些对于与其他主题相关的人工智能的宽泛讨论，可能会提供非常有趣的助益，促进关于其他主题的类似讨论。因此，这些不同的讨论有的应该更多地联系起来，以促进交叉融合，同时也避免重叠和矛盾。通过对不同的人工智能相关技术采用更细致的做法，将更容易识别在不同场所开展的类似讨论。

关于国际法与人工智能的政治性的最后一点评论涉及已经采取的做法。一般而言，人们是从回应的角度来处理人工智能的，旨在防止对这些技术可能的（消极）使用。关于LAWS的讨论就是一个很好的例子，关于新的人工智能应用程序应尊重基本权利的讨论同样如此。然而，正如本白皮书不同部分所讨论的，人工智能也为制定和实施国际法、落实人权或减少数字鸿沟提供了积极的解决方案。在实况调查团与人权的背景下，这一问题几乎没有得到解决，也仍未得到充分探讨。

（三）数字鸿沟

1.数字数据

信息通信技术是发展中国家人民在数字时代获取信息和谋求更大文化多样性的重要途径。然而，国际电联在《衡量数字化发展：2021年事实与数字》报告中表示，全球63%的人口可以上网，但“仍无法上网的29亿人中，96%生活在发展中国家”。[①]数字发展不仅仅是连通性的问题。它还包括有意义的互联网接入，即无论是在城市还是在农村，不分性别，每个人都有能力从信息通信技术服务中获益。据国际电联称，存在这方面的代沟和性别差异。这就导致了“互联互通大峡谷”或“数字鸿沟”，直接影响到各国的发展和实现联合国可持续发展目标的能力。[②]尽管国际组织和许多国家正在实施互联互通领域的能力建设项目，[③]这一“数字鸿沟”远未消除，反而会加剧发展方面的不平等。这些连通性上的不平等也受到网络集中在少数处于垄断地位的行为体手中的影响。再加上出于地缘政治目的对互联网架构的损害或操纵，

① I.T.U., Measuring Digital Development Facts and Figures 2021 (2021), p.1.

② U.N. Secretary General, Roadmap for Digital Cooperation (June 2020); U.N.G.A., Resolution on Information and Communications Technologies for Sustainable Development [17 December 2021] A/RES/76/189.

③ 有关此类程序的列表，参见https://cybilportal.org/es/projects/。

这将威胁到互联网去中心化的本质及其复原力，并影响到整个互联互通。

这种“互联互通大峡谷”加剧了数字数据鸿沟，这一日益严重的问题不仅涉及发展中国家，也涉及那些没有强大公司来为经济目的收集和处理数据的国家（如欧洲国家）。“数据价值链”已成为数字经济发展的关键，需要有能力生产、存储和处理数据，以便将其货币化。它是开发和销售物联网（internet of things, IoT）产品以及AI应用程序和系统的先决条件，并将产生用于未来产品和服务的数据，增加进入数字市场的成本。正如联合国贸发会议（UNCTAD）最近的一份报告所指出的：“随着数据驱动的数字经济的发展，与数据相关的鸿沟加剧了数字鸿沟。在这种新的结构中，发展中国家可能发现自己处于从属地位，数据及其相关价值的获取集中在少数控制数据的全球数字公司和其他跨国企业手中。”①

除了经济后果外，这些技术不平等对执行数据保护机制的能力也有直接影响，因为数据是由往往位于其他司法管辖区的强大行为体存储和处理的。它们还构成了进一步分散和限制数据流动的驱动因素，因为为了确保其数据方面的法律法规的适用，各国可能会试图限制数据流动，从而影响数字产品和服务的发展。这些技术上的不平等也会产生社会和文化后果。基于数字数据的产品和服务难以反映特定人群的道德和文化价值观与信仰，进而对个人和他们所生活的社会产生不利影响。反过来说，对数据流动的限制很可能会增加“数据泡沫”，并相应地可以用来实施更强的控制和监视。

最后，由于技术还可以促进国际法的实施，包括人权和基本自由、法治和公共服务的开展，数字数据的缺乏限制了各国实现这些关键目标和责任的能力，阻碍了人类安全和民主的加强。②同样，数据的可及性有助于应对未来的重大挑战，如全球变暖、连通性和人道主义服务的提供等。促进数据的获取和有效分享将是各国和国际组织未来几年的主要挑战之一。然而，有几个因素可以解释迄今为止数据共享相对缺乏的原因，包括国家安全、保密性和隐私方面的担忧。③数据可及性不仅是一个经济问题，也是实现可持续发展目标的一个问题。

2.数字安全

社会的数字化伴随着国家和非国家行为体恶意活动的发展。随着越来越多的服务依赖于连通性，随着产品日益连接（物联网）和新技术的不断开发（量子计算机、

① U.N.C.T.A.D., Digital Economy Report 2021. Cross-border Data Flows and Development: For Whom the Data Flow (2021), xvi.

② 在预防、发现和打击腐败领域，联合国大会强调了这一点，参见U.N.G.A., Our Common Commitment to Effectively Addressing Challenges and Implementing Measures to Prevent and Combat Corruption and Strengthen International Cooperation [2 June 2021] A/RES/S-32/1.

③ O.E.C.D., Enhancing Access to and Sharing of Data. Reconciling Risks and Benefits for Data Re-use across Societies (2019).

人工智能等），可利用的漏洞数量以及利用它们的手段将随之增加。越来越多的网络攻击已成为众多行为体关注的一个关键问题。应对这些威胁需要人力、技术、组织和法律能力，而这些能力在全球分布不均，即使是最发达的国家也缺乏足够的能力。就此而言，当今在互联互通水平和安全水平之间存在着全球范围的差距。数字安全能力方面的严重不平等也加剧了数字数据获取和传输方面的不平等。这一问题关系重大，因为已经很脆弱的发展中国家很可能是受普遍存在的数字安全问题影响最大的国家。此外，由此产生的脆弱性可能加剧全球范围内的不稳定。但最发达的国家往往是连通性最紧密的国家，这也使它们极易受到数字威胁的影响。因而，各国的数字安全高度依赖于该领域所有其他国家的行动。因此，弥合数字安全鸿沟符合所有国家的共同利益，但更广泛地说，符合所有行为体的共同利益。

除了国家安全利益之外，数字安全也是确保人权得到保护的一项要求。缺乏网络安全，会对用户的数据、隐私权、言论自由或集会和结社自由构成巨大威胁。没有安全，国家保护和捍卫人权的能力就会受到限制。这可以延伸到那些旨在促进或可用于促进人权和国际法的技术的安全性。[①]信息行动也被描述为对民主的威胁。打击这些行动将有利于民主和法治。同样的逻辑也适用于企业、人权和审慎。[②]确保安全是它们预防和应对（缺乏安全）可能对人权造成的风险的一种方式。因此，数字安全有助于尊重和实施国际法。

自20世纪90年代末以来，随着增加数据访问和加速新兴经济体数字化的努力不断加强，国际社会逐步制定了网络能力建设倡议，旨在提高数字环境的安全性。[③]这些倡议涉及广泛的行为体和社区（国家、国际组织、非政府组织、网络安全公司等），关注各种主题（获取数据、网络安全等）和目标（提高认识、分享技术能力、政策、修改立法等方面的知识）。尽管它们的共同愿景是促进数字安全知识和能力的传播，但其内容和形式却大相径庭。

鉴于保护数字环境安全的集体重要性，这些倡议的协调性、有效性和正当性已成为一个突出的讨论话题。然而，在其明显的技术性质背后，能力建设倡议也提出了重要的政治问题，特别是关于发达国家和发展中国家之间的关系，但也包括发展中国家之间的关系。虽然分享知识和技能有可能加强合作并提升数字安全方面的技术、政治和法律能力，但它也可能复制甚至加剧现有的不平等和依赖性，在国际舞台上重复现有的权力等级。还有人指出，不考虑当地情况而复制现有立法，可能导

① 参见上文关于数据和人工智能在推进人权和国际法方面的作用。

② 例如联合国人权事务高级专员办公室开展的B-Tech项目，参见https://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/BTechpro-jectoverview.pdf。

③ 有关概述可参见https://www.iss.europa.eu/sites/default/files/EUISSFiles/CCB%20Report%20Final.pdf, https://www-tandfonline-com.ezp.lib.cam.ac.uk/doi/full/10.1080/23738871.2017.1294610。

致对公民的更大控制并危及人权。如果没有充分的协调和对总体原则的坚持,这些能力建设倡议有可能成为短期和自私自利的项目。

在这种情况下,网络安全能力建设工作的可持续性已成为一个重要的关注话题,并可能构成未来最重要的挑战之一。网络安全能力建设倡议将不得不鼓励采取促进数字环境安全的措施,同时又不过度限制对数据和安全工具的获取以及使用的机会(例如,通过加强对登记和记录数据的要求)。换言之,必须确保网络安全措施不会阻碍最不发达国家的数字、社会和经济发展,因为这些国家并不总能承受尽快实现数字安全的高昂成本。在网络安全和发展之间取得适当的平衡,将是今后努力缩小数字鸿沟的一个关键因素。

3.人工智能

数据是开发和使用人工智能的先决必要资产。在获得数字数据和数字安全能力方面的不平等也会转化到人工智能领域,并被放大。这一观察有两个主要后果。

首先,大多数数据是由世界上某些地区有限的行为体来收集和储存的,这使得其他行为体更难崛起并开发自己的人工智能应用程序。因此,在数据收集和存储方面已经存在的不平等,会对开发人工智能应用的能力产生影响,这不仅体现在所涉及的行为体方面,也体现在其地理分布方面。

其次,在全世界不同人口群体收集和处理的数据量方面存在着显著的不平等。这对人工智能应用程序的开发有直接影响,它们往往依赖于西方国家的数据,可能产生重大的偏见。这些偏见影响了人工智能应用的正当性,特别是当它们被用于执法目的时。

此外,正如前面所讨论的,人工智能有能力塑造国际法的造法进程、实质内容和执行。这可能会给数字鸿沟带来两个相反的后果:一方面,数字鸿沟,特别是获取数据的不平等,影响到各国和其他行为体从国际法上的人工智能解决方案中受益的能力。在这个问题上,各国可以加强能力建设方面的努力以及共享数据,以便让更多的国家能够访问这些数据并使用人工智能应用程序。这种做法通常将有利于国际法规则和原则的实施,并对以规则为基础的国际秩序有所助益。另一方面,基于人工智能的解决方案可以帮助能力较为有限的国家处理更多数据,并培养其参与立法和解释进程的能力。最后这一点将取决于各国在这方面合作与共享数据及人工智能解决方案的意愿。

人工智能还可能在弥合数字鸿沟及其国际法后果方面发挥作用。人工智能应用程序可用于收集和处理关于不同事项的大型数据集,从而帮助确定可能的解决方案,例如如何在国内层面执行特定的国际法义务。从这个角度看,人工智能可以为条约的核查和执行机制提供相关解决方案。

(四)结论

数据、数字安全和人工智能对国际法提出了三重挑战。它们涉及公共行为体与

私人行为体之间的关系，这凸显了对国际法的国家间机制进行调整、以一种新的方式看待规范性的困难；同时也涉及法律产生和实施的方式。第二个挑战涉及法律的政治性，它与国际法必须努力引入对话的文化、政治和法律模式形成对垒。最后，这些数字问题从经济以及可持续发展的角度突出了数字鸿沟。

但这些挑战也与数字技术提供的机遇相对应。数据和人工智能也是弥合国家间不平等、改善人类状况的途径。此外，如果国际法有时似乎受到技术发展的影响，这些发展也可以帮助其取得进展，甚至对其进行修改。数据收集有助于更好地了解国际关系行为体的做法，而人工智能有助于国际法的实施。

数字技术对国际法构成的挑战和机遇都突出表明了法律能力建设的重要性。法律能力建设有两个主要目标：一方面，它有助于更好地理解法律的实质内容，以及法律如何在具体情况（如本白皮书讨论的不同技术）下适用。另一方面，它有助于制定符合国际法义务的国内和区域规则与政策，并促进其实施。因此，分享良好做法是法律能力建设的一个重要内容。

因此，第二部分展示了数据、数字安全和人工智能在它们提出的挑战与带来的机会之间的相互关系，以及这些要素之间的相互关系。无独有偶，它提出了一些实质性的问题，可以为我们未来的辩论和研究提供素材。

三、问题

面对第一部分概述的法律文书和第二部分强调的主要挑战，最后一部分将确定关于数字数据、数字安全和人工智能的国际法未来发展方面一些最突出的问题。事实上，根据新技术发展的概念性和现实性影响，现有法律规则的充分性正在不断被评估。现有的学术和政策讨论经常争论当前的国际法规则是否足够清晰、准确和完整，以跟上数字化的快速步伐，尽管也有人对于数字技术会带来根本不同的法律挑战并对国际法产生比其他技术或社会发展更重大的影响持有怀疑。以下将简要而非穷尽式地概述数字数据、数字安全和人工智能领域出现的一些主要法律问题。但是，在此之前，有必要概述数字活动将给国际法带来的跨领域和共同性问题。

（一）跨领域法律问题

由于国家之间通过对话来对数字方面的需求做出法律回应并不容易，因此出现了许多非国家的倡议，这些倡议提出对国际法的解释甚至新的标准（例如《塔林手册》、全球网络空间稳定委员会等）。法律专家团体也在处理数字方面的问题（例如，国际法委员会关于跨境信息流动中个人数据保护的讨论；国际法研究院关于国际法对网络活动的可适用性的讨论）。毫无疑问，国际法协会在展望国际数字法的演变方面可以发挥作用。

在制定和适用法律的过程中应当考虑非国家行为体，这一点并不新鲜，在数字

法的背景下更是如此。从国际法的角度对私人行为体与公共行为体之间的关系能够或确实发挥哪些类型的作用加以考虑，这可能是有益的。在更理论化的层面上，这将对数字问题是否改变了国际法传统上处理非国家行为体的方式提出质疑。在更实际的层面上，它可以为更好地实施国际法提供建议。例如，我们可以区分私营公司是否：(1)作为国家履行其主权责任(代表国家保护、尊重和实现人权)的代理人；(2)对于国家履行其职能、责任和义务加以补充(Facebook的监督委员会已将国际人权法纳入其决策过程)；(3)作为各国行使主权权利的竞争者(例如，通过设计自己的数字安全标准来抵制国家对解码的要求等)；(4)取代传统上属于一国管辖范围内的职能(无论是数据方面还是防卫方面)；(5)作为既与公共行为体存在交叉又同时捍卫自身利益(例如，决定是否配合执法要求；提出、有时还强制执行自己对国际法的解释)的自主行为体。

似乎也有必要考虑信息通信技术如何改变国际法。如何对国际法进行调整，以满足技术发展所产生的需要，这是没有问题的。这些辩论必须使我们思考或重新考虑制度层面和实质层面的国际法、规范以及渊源的演进、国际法的制定进程以及这些进程的产品。但也有必要了解这些信息通信技术会给国际法带来什么。我们知道，技术解决方案可以补充法律解决方案(例如，隐私设计保护和默认保护)。但是，法律也可以在证据领域(例如在确定国家实践或法律确信方面)以及电子司法或法律技术领域运用新技术。如何对国际法与信息通信技术的相互关系加以考虑？

(二)数字数据

澄清现有法律。确定可适用于数字数据的规则并澄清其解释，这将是未来几十年的主要法律挑战之一。有必要在国际法如何适用于数字数据方面形成更大的确定性，同时对法律的发展加以塑造，以反映广泛的正当利益和目标，特别是人权和隐私、执法和国家安全等相互冲突时。根据几次专家访谈，对国际人权法中隐私权条款的解释将特别重要，因为隐私权是发展最迅速和最具可塑性的基本权利之一。欧洲人权法院和欧盟法院尤其处于国际隐私和数据保护诉讼的前沿，它们必须裁决日益复杂和有争议的案件，例如公共行为体和私人行为体大规模和有针对性的监控，为打击网络犯罪而拦截和存储个人数据，数据保护制度的域外效力，以及数据保护本身的主要参数(数据的概念、被遗忘权、更正权等)。[①]除了欧洲人权法院和欧盟法院各自做法的协调或冲突，其他区域性组织和法院能够在多大程度上提出

① ECtHR, Guide to the Case-law of the European Court of Human Rights - Data Protection (ECtHR, updated on 31 December 2021); CJEU, Factsheet on the Protection of Personal Data (updated on 11 November 2021).

自己对数据保护的理解也很重要，特别是考虑到欧盟《通用数据保护条例》的影响力日益增长。现有规则的澄清和解释也将是涉及数字数据相关问题的国际法其他领域所关注的问题。如在国际人道法中，对于武装冲突中数字数据应被归类为“物体”还是“非物体”仍存在相当大的不确定性；在国际贸易中，数据是否像其他货物一样，能够通过现有规则（也许稍作修改）加以理解？我们如何看待国际贸易产生的数据？

规制的碎片化。鉴于现有倡议相对缺乏协调，澄清法律将特别困难。国家和国际组织往往提出相互竞争的数据保护概念，这反映在它们所通过的法律文书中。欧盟侧重于基本权利和个人自主权的数据保护做法，与美国以及中国、俄罗斯等其他大国的做法存在差异，这可能会成为未来几十年重大政治对抗的根源（参见上文有关数字数据法律的政治性部分）。尽管《通用数据保护条例》已经对许多国家和地区数据保护政策产生了相当大的影响，但数字环境保护和安全规范的国内化趋势日益明显，这可能进一步分裂和破坏相关国际、区域和国内法律制度的法律互操作性。私营部门已经开始对基础设施加以设计，以应对这种碎片化（如微软开发了主权云模型）。

域外管辖。现有规范的碎片化及其国内化趋势伴随着确保国家或区域文书在域外适用的努力。鉴于数据在数字合作、证据和法律互助方面发挥着重要作用，由跨境数据流动和数据保护制度的域外效力所产生的规制冲突（如Schrems II案）可能会引发数字数据领域的一些主要法律挑战。对域外管辖权的主张不断增多可能是结构性的。由于技术上不占主导地位的国家难以迎头赶上，它们很可能诉诸单边和域外效力规制，试图以此保持对其数字数据的控制；欧盟和发展中国家就是如此。

对人权的影响。收集、共享和出售数字数据，特别是个人数据，对人权有着积极的以及消极的重大影响。定向广告、内容策划、私人和公共监控、间谍活动、为刑事调查收集数据、互联网过滤、使用生物特征数据等做法都可能危及隐私和言论自由。但数字数据和人工智能也可以帮助改善人类状况。从个人的角度来看，未来几十年的主要挑战之一将是确保能够跟踪并控制自己的数据。

关键问题

——为了确保科技公司对数字数据的有效保护，可以制定哪些不同类型的法律文书和机制？如何设计私人行为体和公共行为体之间的关系，以促进数字数据的流通和保护？

——倡导相互竞争的数据保护模式的国家之间普遍存在着政治对抗，国际社会将如何处理由此带来的法律后果（规制碎片化、域外效力等）？

——国际社会如何预防和减轻获取数字数据、特别是大数据方面的不平等所产生的不利影响？如何制定真正的国际数据法？

——数据如何弥合数字鸿沟，促进OODs[①]的实现，并改善人类状况？

（三）数字安全

规制的碎片化。世界范围内很少有协调良好的法律法规。这是缺乏普遍性文书以及对网络空间有不同愿景的结果。在网络犯罪领域，尽管在努力促进合作，但合作仍然很复杂，规制的碎片化和缺乏合作减缓了甚至阻碍了刑事调查。规制碎片化的另一个方面涉及安全要求。世界各地都在制定加强网络安全的法律和要求。除了由此产生的法律碎片化之外，还存在着出现相互矛盾的义务（如在加密领域或漏洞披露方面）或者可能为每个人制造漏洞并威胁法律安全的义务的巨大风险。规制的碎片化也对实施打击虚假信息行动、仇恨言论以及在全球范围内打击有害内容的措施构成挑战。

对人权的影响。打击数字威胁对人权既有积极影响也有消极影响。一方面，随着数字空间被越来越多地用于开展信息行动和虚假信息的扩散，参与内容删除的国家和非国家行为体正在对若干权利施加压力，包括言论自由、获得有效救济权或禁止歧视的规定。同样，监控项目的扩张（无论是否定向）以及监控行业的成功，都对许多权利和基本自由构成挑战。社会的数字化也使刑事调查中使用电子证据成为主流。在很短的时间内获取电子证据这一需要，对于国家保护人权的义务提出了挑战，特别是在向服务提供商提出有关外国公民数据的域外请求的情况下。在试图获取电子证据方面遇到的困难可能会促使各国选择大规模监控，从而削弱对公共机构、法治和基本自由的信任。随着数据量的增长速度超过法律合作的速度，上述趋势可能还会继续。另一方面，对人权的尊重和保护必然要加强数字安全。这就对数字安全在界定和评估国家、国际组织和非国家行为体义务方面的作用提出了质疑。

多边主义与国际法。数字安全对于多边主义处理新问题的能力提出了疑问，并构成了确保多边主义未来的条件。对于承诺的核查已被强调为确保在国际安全背景下遵守信息通信技术领域具有约束力的新规则的主要挑战之一，这也可以解释为什么各国不愿意就大多数问题公开达成一致。但对承诺的核查有着比核查潜在的新义务更广泛的影响。网上的恶意活动越来越多，信息来源成倍增加，信息本身被操纵，这对核查网上信息的能力提出了挑战，并加大了不信任和冲突。作为多边主义的一个对象，数字安全也不断对非国家行为体在发展有关义务中的地位和作用提出质疑。作为一项要求，数字安全将在有关信息保护的谈判方式以及在国际组织确保对其信息具有相应保护水平的能力方面发挥关键作用。

域外管辖。考虑到恶意数字活动的性质以及数字空间相对于法律属地性的特点，域外管辖一直是并仍将是未来若干年的一个关键法律挑战。鉴于威胁的数量和

① 尚不确定OODs的全称是什么，在此使用原文。——译者注

复杂性将会增加，而由于国家之间的不信任程度以及缺乏应对新威胁的能力，许多领域的合作可能仍会很紧张，这一点将尤为明显。

关键问题

——私人行为体在发起或应对恶意活动方面的作用，是否会使国际法应如何对待私人行为体的问题受到质疑？

——国际社会能否就与数字安全领域相关的现有国际法规则和概念的适用及含义达成共识，还是会制定新的规则？

——数字安全本身对于其他国际义务是否有任何作用，如果有的话，会是什么作用？

——如何优化网络能力建设和技术共享，以确保发展中国家能够实现数字安全？

（四）人工智能

前面已强调过的第一个法律挑战，是法律和伦理问题的重合，以及目前大多数进程和倡议往往主要集中于伦理而非法律这一事实。正如前文所讨论的，这本身不是一个问题，关于道德问题的工作也有利于法律讨论。然而，在某些情况下，这种做法可能会影响国际法规范的内容。

对人工智能及大部分相关概念（自主、机器、机器人、系统等）缺乏清晰和有共识的定义，带来了重大的法律挑战。这个定义上的挑战放大了另一个相关的挑战：几个平行的进程和倡议同时进行。由于这些不同的倡议和进程可能使用不同的词汇来描述类似的问题，因此更难以确定可能的重叠或分歧。

各国是否应当以及如何将传统的国际法规则适用于人工智能也存在不确定性。这一挑战与定义方面的挑战有关，原因有二：其一，很难确定讨论的对象和规制的潜在后果。其二，一些关于人工智能的讨论往往非常笼统，而出于法律目的，可能有必要对不同形式的人工智能应用程序及其对社会的影响采取更细致的做法。

关于国际法应如何规范人工智能在不友好或敌对国家行为中的应用，目前尚无普遍认识。这一观察在国际法的不同方面有着重要后果，例如相关行为的归因、确定其合法性以及援引所涉不同行为体的责任。这些困难尤其影响到国际法的两个分支：国际人权法和武装冲突法。在国际人权法方面，主要挑战包括确定脸部识别软件对人权的影响、算法中的歧视性偏见、使用人工智能造成的侵犯人权行为的归因和责任。从武装冲突法的角度来看，在规制某些作战手段和方法以及评估武器的技术演变及其法律后果方面存在着挑战。在开发和使用人工智能技术过程中，国家与非国家行为体之间可能存在的关系加剧了所有这些挑战。在决策过程中以及在自主系统中采用不同行为体开发的人工智能解决方案，可能会引发与归因和个人责任相关的问题，特别是关于指挥官责任和个人刑事责任。非国家行为体和国家所进

行的相互交织的活动，也可能引发有关其问责以及如何补救人工智能技术造成的伤害这一问题，即使有时可能不存在不法行为。最后，这种情况还提出了一个问题，即非国家行为体在开发某些人工智能技术时，应当和能够如何考虑可能的国际法义务，特别是与人权有关的义务。

人工智能对国际法提出了重要挑战，但它也为立法和解释过程以及国际法的实施提供了新的解决方案。更普遍地说，人工智能还提供了新的解决方案，可能对国际社会已经面临的挑战产生积极影响，例如帮助减少数字鸿沟。

关键问题

——如何厘清并考虑与人工智能相关的技术和应用的多样性以及它们引发的法律问题的多样性？

——如何厘清人工智能技术开发和运用中所涉行为体的多样性，特别是在责任和归责方面？未来关于人工智能的法律文书应侧重于针对特定部门的应用，还是试图全面地处理这个问题？

——各国如何将传统国际法规则适用于人工智能相关技术和解决方案，特别是人权法和人道法？

——如何弥合各国在获取人工智能技术发展的数据以及更普遍而言使用人工智能方面的分歧？

——基于人工智能的解决方案正在以及将会如何促进国际法的制定、解释和执行？

结论

除了所处理的三大主题（数据、网络安全和人工智能）以及所确定的三大挑战（公私界限、网络空间法律的政治性、数字鸿沟），还可能提出以下一些问题，为我们未来围绕已知法律主题的辩论和研究提供支持：

——法律渊源、法律的制定及解释和进一步发展、对新规则的需要；

——国家权能、域外效力；

——证明和证据；

——法律责任和归责；

——在更为理论化的方面，还包括国际法的性质和制定。

数字问题和技术既是国际法的挑战，也是国际法的机遇。不同的子主题凸显了它们各自的一些特殊性。但是，不应高估每个问题的技术性，因为许多挑战和法律问题是三个子主题所共有的。

（责任编辑：石磊）