第 3 卷第 4 期　　全球传媒学刊　　Vol. 3，No. 4：9-23
2016 年 12 月　　Global Media Journal　　December 2016

网络空间中的数据及其治理机制分析

鲁传颖

摘　要　数据是网络空间中各种流动信息的载体。从治理的角度看，它同时可以被视为权力和财富的信息、具有社会和政治意义的内容和个人在线隐私。现有的治理机制很容易将这三方面的内容混淆在一起，增加了对数据治理的认知难度，影响了治理机制的构建。本文认为，构建合理的数据治理机制应当从信息、内容和隐私三个不同的视角来看待数据的属性，在不同的领域构建有针对性的治理机制，并通过这些不同治理机制之间的松散耦合关联来共同组成网络空间的数据治理机制。

关键词　数据治理；隐私治理；内容治理

DOI　10.16602/j.gmj.20160035

一、信息、内容和隐私视角下的数据全球治理

网络空间中的数据既可以被视为权力和财富的信息（information），也可以被视为具有社会和政治意义的内容（content）和个人在线的隐私（privacy）。这三者都体现了数据在网络空间中的价值属性，因此关于数据的治理涉及各方的关键利益。政府、私营部门和市民社会作为网络空间全球治理的主要行为体，在治理机构构建的进程中，不同层面地存在着不同的利益主张，并由此导致了在治理进程中的多层次冲突。

（一）数据与网络空间全球治理

网络空间中的数据可以定义为，网络中数据或信息的生产、流通、加工、存储与使用的过程。随着网络技术的发展，现实社会中绝大多数的信息能够被转换到网络空间中，形成网络数据。从数据的产生到使用所涉及的每一个环节，都在发生颠覆性的变革。

随着网络渗透度的不断提高，网络空间中的数据的产生量呈急速的上升趋

鲁传颖：上海国际问题研究院全球治理研究所副研究员。

势，全球过去两年生产的信息占据了人类历史信息总和的 90%；[①] 同时，随着网络的普及和渗透度不断增加，信息的传播速度和深度在加快，手机等移动终端加剧了网络信息的传播；大数据技术的发展使得数据加工能力在不断的提升，在海量的数据中寻找规律提升了网络数据的信息价值；最后，云计算改变了数据存储的方式，降低了数据存储成本，提高了数据使用效率。网络数据在生产、传输、存储和应用的每一个环节都呈现出革命性的态势，这一方面提升了网络空间中信息的战略价值，另一方面也对信息治理提出了更高的要求。

数据的生产、流通、加工、存储与使用依托互联网，从某种程度上来说受到了互联网哲学和文化的深刻影响，强调数据和信息的自由流动。特别是互联网发展的早期，数据的数量和价值还未得到体现，主要是以科技信息和个人交流信息为主，所以信息的免费获取和自由流动是主要的治理理念。但随着网络空间中信息的数量和价值的上升，网络数据成为商业信息、安全信息、政治信息、文化信息的载体，并成为具有战略性意义的权力与财富（杨剑，2012，pp. 26-30），导致行为体在网络信息层面的竞争加剧。在信息的生产、传输、加工、存储和使用的这些环节中，占据主导地位的政府和行为体，无疑将会在经济上、政治上、文化上获取战略优势，而处于劣势的政府和行为体，则会在竞争中全面处于下风（基欧汉、奈，2012）。

从信息的视角来看待网络空间中的数据，更多地体现出权力与财富的意义。基欧汉与奈在《权力与相互依赖》一书中将信息分为三种不同的类别，分别是免费信息、商业信息和战略信息。他将免费信息定义为“行为体愿意获得或发送此类信息，而无须付出或获得经济报酬。接受者相信信息，则发送者获得优势，因此信息发送者有制造信息的动因，这一类的信息包括科技信息、政治家宣传用的信息等”（基欧汉、奈，2012，pp. 241-246）。一般来说这类信息的治理如果不涉及敏感内容的管理，不会有较多的治理困难；商业信息是指行为体愿意以一定的价格获得和发送信息，信息生产者从使用者那里获得补偿。这类信息的治理主要是涉及在线知识产权保护问题；战略信息体现了信息不对称的优势，只有在竞争者不拥有的情况下才会有意义，“棱镜计划”对各国领导人手机的监听即是获取战略信息的一种方法（基欧汉、奈，2012，pp. 241-246）。

(二) 内容和隐私的网络空间全球治理

为了便于区分不同的治理领域，除了从信息角度来看待数据之外，还可以从内容的视角来看待空间中的数据。这种区分对于理解网络空间全球治理中政府、私营部门和市民社会之间的冲突有一定的帮助，因为不同行为体往往对于网络空间中的数据本身存在不同的关注点，如果不对此加以澄清，往往会导致不必要的冲突。比如中国政府在第二届世界互联网大会上提倡网络主权，其

最重要的目的是针对美国政府开展大规模数据监控,这属于战略信息的竞争。但很多西方国家的政府和媒体往往将其解读为中国政府是要为自己的内容管理进行背书。同一种主张,两种不同的出发点,实际上一个是从战略信息竞争的角度,另一个是从内容管理的角度来理解。因此,将网络空间中的数据抽象地从信息和内容两个视角来区分有助于更好地对网络空间进行治理。

如果说网络数据是一种信息符号的话,从内容视角来看,网络数据还是一种价值判断,背后体现的是意识形态和伦理的冲突。从内容视角出发,数据层面的核心治理问题,即网络空间中的自由与秩序问题,同时还是价值判断和意识形态的问题。对网络空间中的各个行为体而言,数据与信息传播方式的改变,从根本上改变了很多传统社会自由与秩序的格局。网络空间中的自由与秩序体现认知和理念,背后也反映出国家战略、国家利益以及不同行为体之间的利益冲突。

究其根本,关于内容治理的分歧主要源自网络空间中伦理道德的冲突,这些冲突包括:第一,不同国家、民族、宗教在文化传统理念、价值观念、宗教信仰领域的冲突。政府、私营部门和市民社会在这一领域的冲突最大,相应的治理机制最难发挥作用。这种不同认知和观念上的差距源自于现实社会中相应的领域冲突在网络空间中的延伸。因此,各国政府普遍对数据内容采取不同程度的内容管理措施或内容审查,特别是在信仰伊斯兰教的国家普遍对不符合伊斯兰教教义的内容进行管理;反过来,这种线上的冲突也会引发现实社会的冲突。2012 年,由美籍埃及科普特基督教徒纳库拉·巴塞利制作并导演的电影《穆斯林的无知》在社交网站上引发了巨大的争议,公众认为这部电影是对穆斯林和伊斯兰教的侮辱,很多穆斯林向该社交网站提出抗议,要求网站删除这部带有侮辱和歧视穆斯林性质的影片。但社交网站以保护“言论自由”为名,拒绝将该影片从网站上删除。此后,很多穆斯林和同情穆斯林的黑客在网络上发起了一场针对美国金融企业和能源机构的大规模网络攻击;另一方面,由于听说美国驻利比亚大使馆要播放此片,利比亚境内引发了一系列大规模的骚乱,愤怒的人们冲入美国大使馆,导致驻利比亚美国大使在骚乱中被杀害。[②]这就涉及自由与秩序的核心问题,网络自由并非绝对的自由,网络空间中也不可能在无序中发展(鲁传颖,2013)。

第二,信息爆炸产生的“反理性、反传统、反道德、反主流”的内容与主流道德观念之间的冲突。网络空间的虚拟性、匿名性和跨国性助长了很多极端的言论,这些言论的制造者以“网络自由”为名,拒不接受现实社会的法律、道德的约束。法律的缺失、执法的困难和跨国合作的难度使得政府对于极端言论难以做到实时管理,很多内容管理的举措往往会引发争议,进一步助长了极端言论在网络空间中的流行。近年来不断涌现的网络恐怖主义、网络极端主义思潮就是

借道“网络自由”，利用网络空间中存在各种加密技术手段摆脱政府的监控，从而得以在网络空间中传播和动员。

第三，网络空间虚拟性产生的新的身份认同与传统现实社会中的身份认同之间冲突。网络空间中内容的生产、流通、加工、存储成本大大降低，普通的网民拥有了与现实社会中权威一样的地位。权威的缺失，或者说话语权向普通网民的扩散会引发身份认同的危机。以网络宗教为例，传统的由教会、传教士组成的权威正在发生变化，普通的教民也可以通过网络平台，建立自己的网站、微博、微信公众号等在线社群，从而让自己获得传教的权威。微博、微信中很多“公知”“大 V”现象也属于这一类问题。从治理的角度出发，这种现象出现了两个层面的问题。一是在自媒体时代，获得了权力的“新权威们”如何适应和使用手中的权力；二是政府作为传统社会中“权威”的垄断者如何适应这种新的形势变化。

此外，个人信息是网络空间数据中重要的组成部分，包括个人的身份信息和在线的活动信息。这些与个人身份特征息息相关的数据被广泛认为属于个人隐私的范畴，但是这些信息的价值确实难以估量，它不仅是巨大的商业利润来源，也是政治资源，同时还与国家安全息息相关。因此，针对个人隐私的侵犯和保护是网络空间全球治理的重要内容。

二、信息治理的机制构建

按照基欧汉与奈对信息的三分法，跨境数据流动是一个从商业信息的范畴演变为同时兼具商业信息和战略信息两种属性的过程，前者的主体是企业，后者的主体是政府。跨境数据流动是网络空间的跨国界性的直接体现，为了降低数据传输和存储的成本，很多企业会选择设立全球统一的数据中心，将分散在全球各地的数据集中到数据中心进行分析和使用。原本跨境数据流动主要是聚焦于公民隐私保护领域，并非是网络空间全球治理中的重要议题，欧美之间达成的“数据安全港”是一个较为有效的治理机制。“棱镜门事件”爆发后，一方面，欧洲普通网络用户对于美国政府侵犯用户的隐私做法普遍表示不满，另一方面，欧洲各国政府也因为美国政府开展的“大规模数据监控”对国家安全造成的危害忧心忡忡。2015 年 10 月，欧洲法院裁定“2000/520 号欧盟决定”无效，欧美于 2000 年签署的、至今已有效运营了 15 年的“数据安全港”协议被终止。跨境数据流动成为网络空间全球治理中的一项优先的重要议题，并且引发了国际社会对于“数据主权”(data sovereignty)和“数据本土化”(data localization)这两个概念的新一轮讨论。

这里的数据主要是指企业所收集和保存的用户信息。跨境数据流动的治理议题可以分为两个方面进行分析,一方面是有关用户隐私保护,另一方面是有关于国家安全。从隐私保护层面来看,私营部门既是数据收集、传输、加工和使用的主体,也是隐私保护的主体。私营部门有责任保护不滥用用户信息和用户信息安全。“棱镜门事件”之前,由于跨境数据流动并非网络空间全球治理的优先议题,除了美欧等对于隐私保护较为关注的国家之间签署了“数据安全港协议”并且对私营部门的行为有所约束之外,其他国家的政府对这一方面的要求并不高。“棱镜门事件”之后,跨境数据流动成为网络空间中国家安全的重要议题,特别是在“数据安全港协议”被终止之后,如何构建相关的治理机制是国际社会面临的一项重要任务。

因此,“数据主权”和“数据本土化”成为两个重要的治理概念。前者是指“一国独立自主地对本国数据进行占有、管理、控制、利用和保护的权力。数据主权的国内属性是指对本国境内数据的生成、传播、处理、分析、利用和交易等拥有最高权力;在国际上表现为一国有权决定以何种程序、何种方式参加相关的国际活动,有权利采取相应的措施保护本国的数据不受非法侵害。”(齐爱民、盘佳,2015,p. 67)“数据本土化”是一个更接近网络空间全球治理的概念,主要是指政府基于保护本国公民隐私和国家安全的原则要求跨国企业将本国用户的数据存储在境内。

在“数据主权”和“数据本土化”的治理机制中政府是主导的行为体,其中博弈往往是网络大国政府和本国境内的私营部门结盟之间进行博弈。市民社会的观点一方面是要保护用户隐私,另一方面是要维护网络自由,对于国家安全则不甚关注。“数据安全港协议”终止之后,国际社会尚未就此找到最佳实践或是其他解决方案。但明显的趋势是各国加大了网络安全立法进程,更加关注“数据主权”。例如,中国政府在“棱镜门事件”之后加快了网络空间的法制化进程,更加关注数据安全,要求对于数据的本地存储,并先后出台了《国家安全法》、《反恐法(草案)》、《网络安全法(草案)》。这些举措引起了美国信息通信技术企业的关切,并游说美国政府对中国施压,要求中国政府取消相关规定,如《反恐法(草案)》中规定的公开设备源代码、在境内保存数据、开放接口等法规。

从政府角度来看,这些举措有助于维护网络安全和国家安全,但在网络强国以及私营部门看来,数据的境内留存不仅将增加技术上的投入,也会大幅度增加成本。市民社会则担心这种博弈会使互联网分裂,并且侵犯网络自由等。这种趋势会让政府与私营部门、市民社会之间的博弈越来越复杂化,网络大国可以根据其庞大的市场规模和监管能力迫使私营部门在境内建立数据中心,而一般国家则处于对跨国企业的依赖和缺乏谈判筹码,无法采取强硬的措施来要求企业设立本地数据中心。关于“数据主权”和“数据本土化”的网络空间全球

治理尚未看到有明确的解决方案，虽然各国都对“数据本土化”提出了要求，但会受到网络空间本身的互联互通、跨国界性，以及降低用户成本的制约。最终的机制构建还需要国际社会寻找出一个能够平衡各方诉求的治理机制。

三、数据内容的治理

数据的符号意义也就是内容层面，反映的是不同行为体的价值观念和意识形态。从政府的角度而言，数据和信息的流通虽然是在网络空间当中，但其所依靠的物理网络与基础设施处于国家主权的管辖范围。如基欧汉与奈所言，“信息并非在真空中流动，而是在早就已有归属的政治空间中进行流动。数据跨境流动以及任何形式的交换，都是在四个世界以来国家间业已存在的政治结构中进行的。”（基欧汉、奈，2012，p. 240）因此，不同国家的政府在这个问题上存在分歧，例如美国政府认为除了儿童色情等极少数领域，政府不应当干涉网络内容的传播，德国政府反对在网络空间中宣扬纳粹的内容，信仰伊斯兰教的国家反对任何与教义相违背的内容。

但总体而言，网络发达国家与网络发展中国家在内容管理上的立场差异较大，背后所遵循的治理理念迥异，观点背后是更加复杂的文化、利益和意识形态的差异。网络发达国家倾向于认为，为了保证网络自由、互联、可操作，政府不应当对网络内容进行管理，即使需要管理也需要按照统一的标准，即西方国家的价值观，这种观点可以称为“一元论”。“一元论”的观点认为，互联网的发展得益于统一的技术标准和行为规范，如果各国都各行其是将会出现无数个互联网，从而使得现行的国际互联网分裂。虽然不同的国家有不同的文化、政治和经济背景，但必须要在网络空间采取统一的行为模式。③网络发展中国家认为多元文化是信息社会的根本属性。不同国家有不同的国情、发展阶段、文化背景，有权利采取自己适合的网络内容管理方式，依法对网络空间进行管理是一国的主权范围内之事。网络发达国家与网络发展中国家在针对网络内容管理领域的冲突影响了国际机制的构建，本文将在随后对此作进一步分析。

另一个在数据内容治理上拥有较大影响力的是市民社会。网络空间的市民社会来源广泛，既有掌握互联网关键资源的国际组织，也有在关注网络空间全球治理的各种类型的现实社会中的市民社会组织。市民社会深受网络自由主义思想的影响，支持“没有政府的治理”，特别是在网络内容领域，将网络空间中的自由表达权视为基本人权，反对政府对网络内容的管理。以互联网国际组织为代表的市民社会在互联网治理领域就以网络自由和维护互联网的完整为由与政府争夺对互联网关键资源的控制权。在网络内容管理领域，以各类人权组织为急先锋的市民社会也纷纷组织起来，成立各种形式的跨国倡议联盟对政

府进行施压,往往还会形成市民社会与网络发达国家结成价值观同盟,共同对网络发展中国家的内容管理政策进行施压的情况。以企业经营目的,大多数私营部门在对网络内容管理上没有自己的强烈立场,往往是夹在所在国政府和市民社会中间。当然,也有以网络内容为主要业务的企业,如搜索引擎企业,它们在此问题上有较强的利益和价值判断,谷歌推崇的所谓“不作恶”便是这类企业代表。当然,作为全球有影响力的从事与互联网内容相关的公司,谷歌宣扬所谓的“不作恶”理念的背后还与美国政府的“网络自由”战略存在某种联系。

网络内容有关的网络空间全球治理机制的构建与产生主要源自于网络发达国家、网络发展中国家、私营部门、市民社会等不同行为体之间的相互博弈。博弈主要在网络发展中国家与网络发达国家和市民社会的“同盟”之间展开。

政府是网络内容治理领域的主导行为体,网络空间全球治理的博弈在网络发达国家与网络发展中国家政府之间展开。市民社会因有较高的合法性和议程设置能力,也是重要的行为体,往往会和网络发达国家政府结盟,与网络发展中国家展开博弈。网络数据内容治理的博弈分别在联合国主导的平台和西方主导的伦敦进程两个不同的治理机制之间展开。在联合国层面的机制主要包括联合国信息安全政府专家组(GGE)、国际电信联盟召开的世界电信大会(WICT)、信息社会世界峰会(WSIS)及互联网治理论坛(IGF)等机制。

网络发达国家与网络发展中国家之间的博弈一直在联合国和其他国际性的论坛中展开。2011 年中国以及其他上合组织成员国集体向第 66 届联合国大会提交了《信息安全国际行为准则》,该准则强调网络主权不受侵犯,各国有权力来制定互联网发展的政策。[④]在 2012 年国际电信联盟大会上(ITU)上发达国家与发展中国家在网络主权等问题上再次发生集体性的立场对立,就国家是否有权对互联网的技术设施进行管控发生了分裂,并导致了相关的议案搁浅。[⑤]

联合国对于各国平等、一国一票的主张,使网络发达国家很难取得绝对的优势。因此,美英等国联手推进伦敦进程在网络空间全球治理中的主导作用,试图取代联合国的地位。在伦敦进程的多次会议中,都将网络自由设置为重要的讨论议题,并且放置在会议成果宣言的重要位置当中。在伦敦进程首次会议论坛峰会的主席声明中用大段的文字强调了网络自由与人权的重要性,“大会同意增加网络安全的努力不能建立在侵犯人权基础之上。大家强烈支持网络空间必须对创新和思想、信息、表达自由流通的开放。很多发言人确信对自由表达和信仰在网络空间同样有力,强调政府有必要遵守世界人权宣言的责任和义务。发言人们强调百分百地利用网络空间的福利和保护自由不仅需要政府,也需要市民社会的参与。”伦敦进程的第四次会议,《2015 全球网络空间大会(海牙)》的主席声明中专门有一个章节来表述自由与隐私,其中强调线下的自由在线上同样应当得到保护。不仅重申了《世界人权宣言》在网络空间的适用性,还

进一步指出应当落实《公民及政治权利公约》所宣布的国际人权法保护措施。

网络发达国家与网络发展中国家在网络内容管理等方面的激烈博弈使整个网络空间全球治理的进程陷入困境，对网络安全、网络恐怖主义等其他紧急议题的治理也产生负面的影响。因此，各国逐渐意识到不能因为意识形态领域的冲突影响网络空间全球治理进行，进而采取更加宽容和模糊的方式来处理在网络内容领域的分歧。2013 年 6 月，联合国发表了一份由 15 个国家的代表组成的专家组的报告，报告首次明确了“国家主权和源自主权的国际规范和原则适用于国家进行的通信技术活动，以及国家在其领土内对通信技术基础设施的管辖权。”同时，报告进一步认可了“联合国宪章在网络空间中的适用性”（鲁传颖，2014，p. 54）。“各国在努力处理通信技术安全问题的同时，必须尊重《世界人权宣言》和其他国际文书所载的人权和基本自由。”[⑥] 与 2010 年的专家组报告相比，上述内容分别作为 2013 年报告的第 20 号和 21 号条款出现，这是一个巨大的进步，表明网络发达国家和网络发展中国家在网络空间全球治理的认知理念上更为包容。2015 年 7 月，联合国信息安全政府专家组发布了第三份政策报告。相较以往的报告，各国在网络空间中的主权、网络战的基本原则等重大分歧上取得了一定程度的突破，为今后网络空间全球治理取得突破奠定了理论基础。[⑦]

四、网络隐私保护的治理

(一) 网络隐私

网络隐私保护主要涉及用户的个人身份信息、在线活动数据以及在线表达内容，这些不同形式的内容都以网络数据的形式存储在网络空间。随着网络存储设备的容量不断扩大，海量的数据收集和存储成为现实。从原则上说，个人在网上所有的身份信息包括银行卡信息、个人简历、教育经历、乘坐交通工具等所有信息，以及在网络上从事的交易、浏览的网页、聊天内容，甚至是电话通讯记录通通是被存储的。如无相关的监管规定，这些信息将会被终身存储在网络空间中，对保护个人用户隐私造成严重威胁。这在欧洲引起了关于“被遗忘权”的讨论，欧盟在 1995 年的数据保护法律中提出了“被遗忘权”，任何公民可以在其个人数据不再需要时提出删除要求（梁辰曦、董天策，2015，p. 35）。2012 年开始，欧盟委员会建议制定关于“网上被遗忘权利”的法律，提议包括要求谷歌等搜索引擎、新闻网站、门户网站应当根据当事人的请求修改页面结果，以符合欧盟保护个人信息的方针。[⑧]

表面上看来，个人是数据的产生者，私营部门是数据的存储者，国家是数据

的监管者。但实际上,特定的数据对用户来说是一种个人信息,对其治理涉及隐私问题;对国家而言,大规模的用户数据则与政治安全、社会安全、经济安全等国家安全事务息息相关;从企业角度来看,用户数据是有价值的商业信息,通过大数据分析可以改善服务,提高市场的占有率,所以国家有加强数据监控的职责,通过收集、分析各种数据来提高国家安全。然而,企业为了自身市场往往有时会通过数据滥用和数据交易来谋取商业利益,因此,个人用户的隐私权就会在国家安全与商业利益面前牺牲掉。如果对政府和私营部门的行动不进行一定程度上的规范,则会进一步侵犯用户的个人隐私,从而给用户造成人身、经济和社会等方面的安全威胁。

基于上述复杂的原因,隐私保护一直是网络空间全球治理中的重点议题。无论是在联合国和政府主导的"信息安全政府专家组",还是在伦敦进程等机制中,隐私保护自始至终是重要的治理议题。特别是在"棱镜门"之后,美国国内的企业和市民社会纷纷反对美国政府收集公民的电话和网络记录,也引起了其他国家政府对美国的强烈不满。巴西总统迪尔玛·卢塞夫举办了圣保罗全球多利益攸关方大会(NET Mundial Initiative)声讨美国政府的行为。此外,欧盟法院于 2015 年判决鉴于美国政府无法保护欧盟用户的数据安全,运行了十多年的美欧"数据安全港"协议被终止。

关于网络隐私保护的网络空间全球治理机制构建的行为体互动模式,并非是由某一行为体主导而建立,通常是经历着多个行为的反复博弈才最终形成一定的治理模式。这不仅体现在国内立法的过程,同样也体现在本国的相关法律、法规对跨国私营部门和全球市民社会所产生的影响。本文随后通过对美国联邦调查局与苹果公司之间就手机解密事件的分析来进一步描述这一复杂局面。

(二)美国联邦调查局(FBI)与苹果之争

自 2015 年起,苹果公司多次拒绝美国地区法院所发出的破解手机操作系统的命令,法院认为犯罪嫌疑人的手机中存储的文字和图片对于联邦调查局的破案至关重要。苹果公司一直以诉讼的方式应对法院的命令。2015 年 12 月,加利福尼亚州的圣博纳迪诺发生了一起 14 死 22 伤的恐怖袭击,其中一名被击毙的恐怖分子所使用的手机被认为对联邦调查局破案有重要线索,因此联邦政府再次指令苹果解锁。由于苹果采取的复杂加密方式,苹果本身并不拥有现成的解锁工具,除非专门开发一款新的破解软件。苹果的再次拒绝合作引发了美国国内乃至国际社会一场关于国家安全与隐私保护的争论。

美国政府不断通过司法和行政命令迫使苹果公司屈服,一方面不断打反恐牌,指责苹果公司的不配合损害了美国国家安全,另一方面则不断地煽动舆论

向苹果公司施加压力。而苹果公司则坚决顶住压力，通过司法手段维护自己的立场，首席执行官蒂姆·库克则通过公开信的方式向公众解释苹果公司拒绝合作的原因。他提道，第一，苹果公司视用户隐私保护为生命线，因此投入了大量的资源开发加密系统，这种系统的安全性在于苹果公司本身也不掌握解密的技术，从而绝对保证了用户的隐私不会被各种形式的黑客非法获取。第二，在圣博纳迪诺的案件中，苹果公司向联邦调查局提供了大量的协助，但苹果本身不掌握破解手机的程序。第三，联邦调查局命令的风险在于它并不是针对特定手机的一次解密，而是要求苹果开发出一个具有后门的系统以供其使用。如果这样的后门存在，就会给黑客留下漏洞，从而威胁到用户安全。[⑨]

联邦调查局与苹果公司争执不下，表面上看一个从维护国家安全利益出发，一个从保护用户隐私出发。从实质上看，单个案件背后是美国政府与私营部门在“棱镜门”之后持续不断的冲突中的一个注脚。美国政府希望扩大自己的网络权力，加强对网络空间的监管；私营部门则是要维护自身的商业利益，避免因和政府合作而得罪用户，并且双方背后都有自己的法律依据：美国政府是最高法院在 1977 年对最高法院针对纽约电话公司案做出的判决，法院要求电话公司提供合理的技术援助进入电话的通话记录。而苹果公司则回应称，纽约电话公司已经存储了通话记录，而苹果手机并没有这样一个后门可供政府使用，并且政府强迫公司提供后门的观点已经违反了宪法第一修正案。

同时，双方背后也有各自的支持力量。全国警官协会（National Sheriff Association）批评苹果公司把利润放在安全前面，所为与隐私保护毫不相干。此外，联邦执法官员协会（the Federal Law Enforcement Officers Association）检察官协会（the Association of Prosecuting Attorneys）都公开声明支持联邦调查局。苹果公司背后的支持者则更加广泛，首当其冲的是改革政府监控联盟（Reform Government Surveillance Coalition），该联盟是“棱镜门事件”之后由脸谱、微软、苹果、领英等美国互联网企业巨头组成，旨在要求美国停止大规模数据监控。这些互联网企业因被斯诺登揭露配合美国政府的网络监控而一度面临巨大的舆论压力。此外，众多的民权组织和互联网协会也坚定地支持苹果公司的立场。

从利益相关方的角度来看，美国政府与苹果公司在合法性上势均力敌，国家安全与用户隐私都是具有相当高的合法性。从能力和利益的关系来看，两者都不容忽视。苹果公司在加密算法领域具有超强的技术能力，甚至连联邦调查局也需要苹果公司为其开发程序破解软件；然而，苹果公司如果为政府“开后门”的话将会对自己的商业前景造成极大的伤害。特别是苹果产品拥有巨大的海外市场，如果苹果公司向美国政府提供“后门”，一方面会引发海外用户的安全隐患，另一方面苹果公司也难以处理其他国家日后不断提出的“开后门”请求。

对于像苹果公司这样有着大量海外用户的企业来说,毫无疑问会涉牵扯到用户所在国的国家安全问题。因此,苹果公司与联邦调查局之间的争议受到了国际社会的普遍关注。在美国国内,两者可以通过司法或者是"秘密交易"的方式处理争议,但如果此事发生在国外将会面临更加棘手的状况。一方面,苹果公司坚决不对美国政府妥协,那么在今后如果遇到同样的事件也不大可能向其他国家妥协;另一方面,苹果公司如果坚持拒绝提供解密协助的话有可能会触犯其他国家的法律,产品有可能被禁止进入所在国市场。当然,鉴于苹果公司庞大的用户数量,任何一国的政府在作出决策之时都会投鼠忌器。因此,难题又回到了维护国家安全的政府手中,这是政府在网络空间时代所面临的众多挑战之一。鉴于这种情况,如何在国家安全与用户隐私之间做取舍,如何建立一种政府、私营部门和广大用户之间的良性互动,是网络空间全球治理机制构建的重要内容。

联邦调查局与苹果公司之争的最终结果是由匿名的第三方提供了破解程序使得联邦调查局能够进入恐怖分子的手机并获取关键信息。但这场争议的结果并未出人意料,也是双方都能够接受的结果。[10]美国政府并不希望因为隐私问题而削弱高科技企业在全球的竞争力,苹果公司也不希望成为恐怖主义的避风港。但其引发的巨大争议还将持续,政府与私营部门在各自立场上面临的选择也将继续存在,对其严重依赖国外产品的国家来说,今后将会面临越来越多的难题。所以说,网络空间全球治理的多利益攸关方模式并非完全基于合法性,更多情况下也是国家主权与技术、市场之间的博弈,大的趋势是技术与市场的重要性会越来越凸显,而国家主权尽管可以通过立法来彰显,但却越来越难以落实和执行。

(三)网络隐私保护的立法和政策

联邦调查局和苹果公司之争揭露出隐私保护的一个侧面,而大数据技术的发展使得对海量用户数据的加工产生巨大的商业利润,影响社会乃至国家的安全利益,这就使得获取网络空间中的个人用户信息成为网络犯罪集团、情报机构以及商业企业等各种利益团体的目标,这同样构成了对用户隐私权的侵犯。各国政府从不同的角度加强对用户隐私权的立法和政策保护,将保护个人隐私视为对本国公民的基本义务。网络发达国家一直拥有隐私保护的传统,随着公民在互联网和网络空间中活动的不断增加,网络隐私保护成为一项重要的治理议题。如伦敦进程宣言中所提倡的,公民在线下所拥有的隐私保护,在线上应该同样适用。[11]应对用户网络信息隐私保护的治理议题主要是从国内层面立法和国际层面治理机制建设两个方面展开。

美国、欧盟、日本、加拿大等网络发达国家和地区很早就开展网络隐私保护

立法的实践工作，并将其作为长期立法工作之一，目前已经建立了一套较为完善的隐私保护法律体系。美国 1974 年通过了《隐私权法案》(*Privacy Act*)，该法案对个人记录做了定义，是指“行政机关根据公民的姓名或其他标识而记载的一项或一组信息”。其中，“其他标识”包括别名、相片、指纹、音纹、社会保障号码、护照号码、汽车执照号码，以及其他一切能够用于识别某一特定个人的标识。个人记录涉及教育、经济活动、医疗史、工作履历以及其他一切关于个人情况的记载。这是一个较为全面的有关隐私保护具体内容的定义，它为随后美国政府制定的一系列有关网络隐私保护的法案奠定了基础。[12]考察美国网络隐私保护立法过程可以看出，它是从某一领域的隐私保护法案逐步过渡到综合性的法案。如 1986 年颁布的《电子通讯隐私法》(*the Electronic Communication Privacy Act*，ECPA)、《金融服务现代化法案》(*Financial Services Modernization Act of 1999*)，也就是格雷姆-里奇-比利雷法(*Gramm-Leach-Bliley Act*，GLB Act)，它规定了金融机构处理个人私密信息的方式。《儿童在线隐私保护法案》(*the Children's Online Privacy Protection Act*，COPPA)，它规定网站经营者必须向父母提供隐私权保护政策的通知，以儿童为目标的网站必须在网站主页上或是从儿童处收集信息的每一网页上提供链接连接到此通知。它还详细规定了网站对 13 岁以下儿童个人信息的收集和处理。[13]除美国之外，加拿大等国在网络隐私保护方面都建立起了较为完整的隐私保护体系。

政府关于用户隐私保护的立法实施和政策制定还面临着以下几方面挑战。一是用户在网络中的数据信息正海量地增加，这不仅体现在数量上，而且体现在不同类型的信息层出不穷，这就使得用户隐私保护面临着巨大的挑战。政府将相关信息纳入到保护范畴，但却总是落后于新的技术发展，这就使得个人信息的保护进入法律真空期。同时，政府在执法时也面临着诸多挑战，如网络空间的匿名性使得很多违法者难以被发现，增加了政府维护网络安全的成本等等。二是收集、存储和使用用户信息的主体越来越多元化，除了政府以及政府下属的相关机构在收集、存储和使用用户的身份信息，其他很多类型的机构如保险公司、医院、社区服务机构都在收集使用用户信息，而这些机构对于用户隐私保护的意识和能力参差不齐，留下了另一层隐患。即便是政府部门内部也存在着同样的问题。美国联邦人事管理局(OPM)2015 年就曾发生过其所存储的近 2000 万份联邦雇员及其家属的个人信息遭黑客攻击疑似被泄露。[14]此事在美国社会中引起了巨大的争议，联邦人事管理局局长引咎辞职，此事还在中美两国关系中引发巨大争议。[15]美国政府事后的调查表明，联邦人事管理局的信息系统严重老旧，缺乏必要的网络安全保护意识和防范举措是导致黑客攻击的主要原因。除了政府机构掌握的个人用户信息成为黑客的攻击对象之外，大型的医疗保险公司、交通公司、金融公司近年来都曾被曝出被黑客攻击、个人用户资料

被窃取。三是黑客入侵的能力在不断提升。随着个人用户信息的价值在不断提高,获取大型机构所掌握的用户个人信息成为黑客产业的主要目标,巨大的获利不仅吸引更多犯罪集团从事这项业务,庞大的利润还进一步促使黑客不断开发出技术更新、更加隐蔽的网络入侵工具。这对政府机构的网络安全防护水平提出了更高的要求,网络发展中国家的政府和私营机构在很多高级黑客犯罪集团看来是完全不设防的。根据相关网络安全公司的估计,全球关于买卖个人信息的地下黑客产业规模已达上百亿美元规模,已成为威胁网络空间安全和发展的毒瘤。

从国内层面来看,加强网络隐私保护立法和提升网络安全防护能力是政府应当采取的主要举措。但同时,网络的匿名、跨国性使得打击侵犯隐私的网络犯罪需要跨国合作。这方面虽然国际刑警组织和各国警方之间的双边、多边合作已经开展,但距离实际需要还有较大的距离。因此,关于隐私保护的网络空间全球治理机制构建就显得越发重要。各国政府、私营部门和市民社会都非常重视在这一领域构建重要治理机制,从联合国的信息安全政府专家组到伦敦进程、巴西圣保罗多利益攸关方互联网治理大会都将网络隐私保护视为重要的治理议题。《布达佩斯网络犯罪公约》还专门就网络隐私保护作出规定。但在真正的实践过程中,技术层面的归因问题、法律层面的司法管辖问题和政治层面的信任问题一直是阻碍网络隐私保护国际机制构建的主要因素。

注释

① 中央政治局第九次集体学习　李彦宏讲解大数据,《大公报》,2013 年 10 月 1 日,获取自 http://finance.takungpao.com/tech/q/2013/1001/1940595.html

② "Chris Stevens, US ambassador to Libya, killed in Benghazi attack", September 2012, *The Guardian*, 获取自 http://www.theguardian.com/world/2012/sep/12/chris-stevens-us-ambassador-libya-killed

③ Hillary Clinton, "*Secretary Clinton's Remarks on Internet Freedom*", 08 December 2011, 获取自 http://iipdigital.usembassy.gov/st/english/texttrans/2011/12/20111209083136su0.3596874.html#axzz2eIWPYNRu

④ 参见中俄等国向 66 届联大提交的《信息安全国际行为准则》,获取自 http://www.fmprc.gov.cn/chn//pds/ziliao/tytj/t858317.htm

⑤ BBC, "US and UK refuse to sign UN's communications treaty", 14, December, 2012, 获取自 http://www.bbc.co.uk/news/technology-20717774

⑥ *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN General Assembly Document A/68/98, June 24, 2013.

⑦ *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN General Assembly Document A/70/174, July 22, 2015.

⑧ 新浪网(2014 年 5 月 16 日):公民拥有"被遗忘权" 谷歌等互联网巨头或增加运营成本,获取自 http://finance.sina.com.cn/world/20140516/105219131299.shtml

⑨ Tim Cook, "A Message to Our Customers", February 16 2016, Retrieved from http://www.apple.com/customer-letter/

⑩ 文庚淼(2016 年 3 月 29 日):FBI 宣布成功破解 iPhone,库克估计要有几个不眠之夜了,获取自 http://business.sohu.com/20160329/n442667834.shtml

⑪ Global Conference On Cyberspace 2015 Chair'S Statement, 16 April 2015, Retrieved from https://www.gccs2015.com/sites/default/files/documents/Chairs%20Statement%20GCCS2015%20-%2017%20April.pdf

⑫ Department of Justice, "Privacy Act of 1974", Retrieved from http://www.gpo.gov/fdsys/pkg/USCODE-2012-title5/pdf/USCODE-2012-title5-partI-chap5-subchapII-sec552a.pdf

⑬ Federal Trade Commission, "Children's Online Privacy Protection Act of 1998", 15 U.S.C. 6501-6505, Retrieved from http://www.ftc.gov/ogc/coppa1.htm

⑭ Raya Jalabi, "OPM hack: 21 million people's personal information stolen, federal agency says", *The Guardian*, July 09 2015, Retrieved from http://www.theguardian.com/technology/2015/jul/09/opm-hack-21-million-personal-information-stolen

⑮ NBCnews(June 5, 2015). Eric Baculinao And Alastair Jamieson, "OPM Data Breach: China Hits Back at U.S. Over Federal Cyberattack", Retrieved from http://www.nbcnews.com/news/us-news/opm-data-breach-china-hits-back-u-s-over-federal-n370351

参考文献

梁辰曦、董天策(2015):试论大数据背景下"被遗忘权"的属性及其边界,《学术研究》,第 9 期,31-36 页。

鲁传颖(2013):试析当前网络空间全球治理困境,《现代国际关系》,第 11 期,48-54 页。

鲁传颖(2014):奥巴马政府网络空间战略面临的挑战及其调整,《现代国际关系》,第 5 期,54-60 页。

罗伯特·基欧汉、约瑟夫·奈(2012):《权力与相互依赖》(门洪华译),北京:北京大学出版社。

齐爱民、盘佳(2015):数据权、数据主权的确立与大数据保护的基本原则,《苏州大学学报(哲学社会科学版)》,第 1 期,64-70 页。

杨剑(2012):《数字边疆的权力与财富》,上海:上海人民出版社。

Analysis of Data and its Governance Mechanism in Cyberspace

Chuanying Lu

(*Shanghai Institutes for International Studies*)

Abstract　Data are the carrier of information which flows in cyberspace. From the governance perspective, it could be considered as information which means power and wealth, as content having social and political meanings, and as personal online privacy. The current governance mechanisms, however, mix all these different issues, increasing the difficulties of data governance and its mechanism construction. This paper argues that the appropriate data governance mechanism should consist of information, content as well as privacy. Different governance approaches should work together to build up the data governance mechanism in cyberspace.

Key Words　data governance; privacy governance; content governance

(编辑:戴佳)