

数据，而不是将公民的数据都上交给全球范围内的互联网巨头企业，即实现“数据本土化”。

因此，跨境数据流动与“数据本土化”之间的矛盾便不可避免地形成了。不过，有学者指出，这对矛盾双方并非不可调节的完全对立。如果能够构建适合自身国情的数据跨境流动相关制度，那么还是可以实现自由流动与数据安全之间的平衡。

目前看来，如何保护数据安全这一议题对于各国来说，受制于政治经济文化等因素的多样性，还没有“标准答案”，更多的是一种自发行为。这些自发行为，又映射出不同国家对于这一矛盾的不同态度。

从市场价值来看，美国的互联网企业无疑处于领先地位。然而，从2013年“棱镜门”事件再到2018年脸书的数据丑闻，这些都使得走在网络时代前列的美国，在数据安全领域的措施与法规备受关注。国内已有学者指出，在特朗普担任美国总统期间颁布的“云法案”（The Cloud Act），“是美国为建立全球数据霸权所采取的一项重要措施，直接服务于美国‘无限的数据饥渴’”。

具体来说，“云法案”为美国联邦调查局（FBI）等情报调查机构调取境外数据提供了法律依据，如果企业不提供相应内容则属于违法。而“云法案”只允许“符合资格的”且与美国政府签订行政协议的外国政府向美国境内组织发出协助调查、调取数据的请求。

“美国主张互联网自由，但他这种自由并不是真正对等的自由。美国希望自由地调取外国企业在美国境内的数据，但对于自身并没有统一这种要求。”徐德骥告诉《新民周刊》。

与美国不同，欧盟于2018年5月25日正式实施通过的《通用数据保护条例》（GDPR）提供了另一种国家层面保护数据安全的路径。这份条例被视为“史上最严格的个人信息保护规范”，其范围不仅涵盖欧盟全境，而且对与欧盟相关的、但在欧盟境内的第三国企业和机构同样具有法律效力。

GDPR实施后，由于中国并不在其第三国“白名单”之中，所以对国内那些在欧洲也拥有广泛用户的互联网企业带来了巨大压力。部分企业开始成立专门的应对团队，尽快使自己符合GDPR的数据传输要求。

此外，在GDPR的影响下，很多非欧盟国家据此修改了自身的数据保护法，以与欧盟标准保持一致。欧盟在与其他国家之间的跨境数据流动文本通常也是由欧盟起草，这些迹象都显示出欧盟在国际上数据安全领域的话语权。

对于这种限制，中国应该如何应对？2019年6月，《个



扎克伯格的脸书“魔葫”。漫画/崔泓

人信息出境安全评估办法（征求意见稿）》全面加强了对我国个人数据出境的保护。而就在2021年6月10日，第十三届全国人民代表大会常务委员会第二十九次会议通过了《中华人民共和国数据安全法》，其中第七条提出：“国家保护个人、组织与数据有关的权益，鼓励数据依法合理有效利用，保障数据依法有序自由流动，促进以数据为关键要素的数字经济的发展。”而第八条提出：“履行数据安全保护义务，承担社会责任，不得危害国家安全、公共利益，不得损害个人、组织的合法权益。”

再加上《网络安全法》等法规，可以说中国目前在数据保护方面走在了亚洲前列。在徐德骥看来，国内目前面对数据安全与自由的矛盾，正在找到一种自己的模式。“作为后发国家，中国不可能完全照搬欧洲严苛的数据新法，主动给正在壮大的数字经济套上枷锁，放弃‘弯道超车’的机遇。我们是在提高个人保护水平的前提下，尽力促成大数据作为正规经济部门的‘合法兴起’”。

## 无形的战斗

除了政府有关部门对于数据安全的保护，目前国内也有不少专注网络安全的企业在贡献自己的力量。创立于2007年的知