# 数据安全 法律护航

数据，是指以电子或其他方式对信息的记录。数据安全，是指通过采取必要措施，确保数据处于有效保护和合法利用的状态。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《中华人民共和国数据安全法》，自2021年9月1日施行。本期“域外之音”，介绍了域外部分国家和地区数据安全法律制度。

【欧盟】

## 制定数据安全法律框架

欧盟制定了数据安全法律框架，明确了数据收集和使用限制、流动规则、管理方式及处罚原则。

1980年，欧盟通过《关于隐私保护和个人跨境数据转移指南》。该指南对数据安全保护的最低标准作出了规定。1981年，通过《有关个人数据自动化处理的个体保护公约》，规定了成员国之间个人数据的自由流动原则。1995年，通过《数据保护指令》，限制成员国数据向非成员国流动。2018年6月，通过《通用数据保护条例》，完善了数据保护的基本规定。2019年5月，通过《欧盟内非个人数据自由流动框架条例指南》，鼓励各行业在数据服务提供商的转换和数据传输方面制定自律行为准则。2020年2月，发布《欧洲数据战略》，提出构建自由而积极的数据流动体系。

上述文件确认欧盟个人数据保护的机构有欧洲法院、欧盟数据保护专员、个人数据保护工作组和欧洲网络与信息安全局等。确认对数据违法行为作出的处罚，共分为两个档次。对没有安全保障措施、没有提供全面透明的隐私政策、没有签订书面的数据处理协议等违法行为，处1000万欧元罚金；对侵害数据主体的合法权利、拒绝服从监管机构的执法命令等违法行为，处以2000万欧元或者企业上一年度全球营业收入4%的罚金。

【英国】

## 提升数据自我发展能力

英国在数据安全保护方面制定了一系列政策和原则。2000年，英国实施的《信息自由法案》明确了政府数据信息有向社会开放的义务，而公民则有获取政府持有信息的权利。2012年6月，英国发布《开放数据白皮书》，推进公共服务数据开放。并针对个人隐私保护进行了规范：一是在公共数据开放机构中设立隐私保护专家，要求各个部门配备隐私保护专家。二是要求所有政府部门在处理涉及个人数据时都要执行个人隐私影响评估制度。英国《2014数据留存和调查权法案（修正案）》加强了企业数据留存职责，将留存时间规定为1年。

在数据战略能力提升方面，英国于2013年10月发布《把握数据带来的机遇:英国数据能力战略》，确定了推动研究与产业合作、确保数据被安全存取和共享等举措。指定统计局和经济社会研究委员会负责政府的数据能力提升；由信息化基础设施领导理事会负责大数据基础设施建设，各行业协会负责本行业数据能力建设，信息经济委员会负责制定大数据具体战略实施路径。

【印度】

## 加强数据本地化建设

印度作为新兴市场国家，高度关注数据跨境流动对本国经济和社会发展带来的影响，禁止公共数据向境外传输。

2012年，印度政府颁布国家数据共享和开放政策，拟定了一个非共享数据清单，以保护国家安全、隐私、机密、商业秘密和知识产权等数据安全。2014年3月，印度成立数据保护局，其职能是“调查任何数据安全漏洞并发出适当的命令，以保障任何已然或可能受漏洞影响的当事人的安全利益”。数据保护局有权向最高法院提起诉讼。

印度《1993年公共记录法》强调，数据本地化对于确保负责任和透明地使用数据以及对其公民进行可靠的隐私保护至关重要。根据《个人数据保护法案》，仅允许受托人在获得个人同意的情况下处理数据。

印度《个人数据保护法案》采用统一的立法模式，即该法案统一适用于印度境内的所有组织机构，使印度有机会从本国的信息和数据“资产”中受益。《个人数据保护法案》要求互联网公司必须将在印度收集的关键个人数据存储在印度境内，在脱敏后才可转至国外，且只能用于法律许可的目的。2018年4月，印度储备银行要求外国支付公司将所有涉及印度客户交易相关信息全部存储在印度境内的服务器上，以达到合规目的。

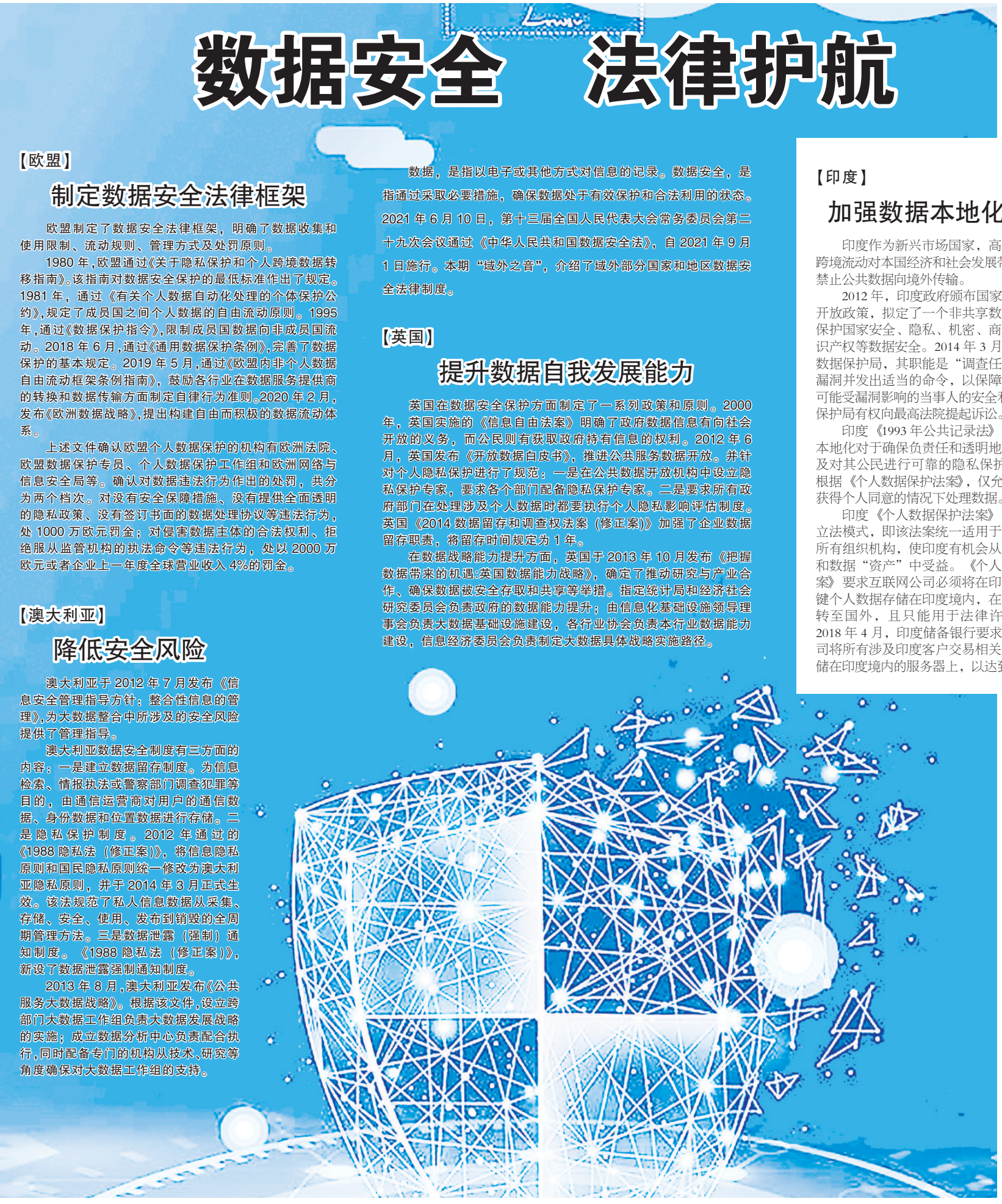
【澳大利亚】

## 降低安全风险

澳大利亚于2012年7月发布《信息安全管理指导方针：整合性信息的管理》，为大数据整合中所涉及的安全风险提供了管理指导。

澳大利亚数据安全制度有三方面的内容：一是建立数据留存制度。为信息检索、情报执法或警察部门调查犯罪等目的，由通信运营商对用户的通信数据、身份数据和位置数据进行存储。二是隐私保护制度。2012年通过的《1988隐私法（修正案）》，将信息隐私原则和国民隐私原则统一修改为澳大利亚隐私原则，并于2014年3月正式生效。该法规范了私人信息数据从采集、存储、安全、使用、发布到销毁的全周期管理方法。三是数据泄露（强制）通知制度。《1988隐私法（修正案）》，新设了数据泄露强制通知制度。

2013年8月，澳大利亚发布《公共服务大数据战略》。根据该文件，设立跨部门大数据工作组负责大数据发展战略的实施；成立数据分析中心负责配合执行，同时配备专门的机构从技术、研究等角度确保对大数据工作组的支持。



【德国】

## 严格数据获取和使用责任

德国细化欧盟的法律规定，建立了完备的数据安全法律制度。

1970年，德国的黑森州颁布了首部地方性数据保护法。1977年，《联邦数据保护法》出台。进入21世纪以来，《联邦数据保护法》根据信息技术的发展和欧盟统一的数据保护指令分别于2001年、2003年、2006年和2009年进行了4次修订。

《联邦数据保护法》在明晰立法目的、数据保护范围的基础上，分别对涉及公共机构的数据处理和涉及私营机构的数据处理进行了规范。该法对数据的合法获取、处理和使用、存储等作出了明确规定。按照规定，信息所有人对于自己被记录的信息、信息记录的主体以及用途享有知情权；私营组织在记录信息前必须将这一情况告知信息所有人。出于广告目的而获取、处理、使用个人信息必须经信息所有人书面同意；非法获取或不再需要的信息必须删除。如果违反法律规定，将被处以5万至30万欧元罚款；如因违法获利，罚款应超出获利金额。此外，还规定要设立数据保护与信息自由专员，专门负责监督和指导执法部门对个人数据的保护。在《2014至2017年数字议程》中，德国进一步提出了加强大数据时代信息安全的要求。

【美国】

## 对进出口数据严加管控

美国早在20世纪80年代就开始关注网络信息安全，相继出台一系列关于通信和自动化信息系统安全政策文件。在大数据出口管理方面，有一系列严格规定。

2002年，《加州数据泄露法案》被欧盟、韩国、澳大利亚等国陆续效仿。2011年，成立大数据高级指导小组，负责协调、促进政府和社会在大数据关键领域的投资，指导和监督包括信息安全项目在内的大数据技术研发和评估工作。2018年2月，美国通过《域外合法使用数据法案》。该法案适用长臂管辖原则，明确美国执法机构有权直接调取美国境外数据。同时取消数据本地化政策，由此让需要从美国调取数据的国家将更多的数据流向美国，最终对美国产生更强烈的依赖。

美国外资安全审查委员会具有广泛的权力阻止外资企业损害美国国家安全，其措施包括要求国外网络运营商与美国电信管理机关签署安全协定、要求通信基础设施位于美国境内，以及要求通信数据、交易数据、用户信息等存储在美国境内。此外，提供数据处理服务的相关主体或者掌握数据所有权的相关主体在数据出口时，必须获得法律规定的出口许可证。

（来源：人民法院报）