国外数据安全政策研究报告（2022年）

V1.0.0

國浩律師（北京）事務所
GRANDALL LAW FIRM (BEIJING)
炼石
CipherGateway

前言

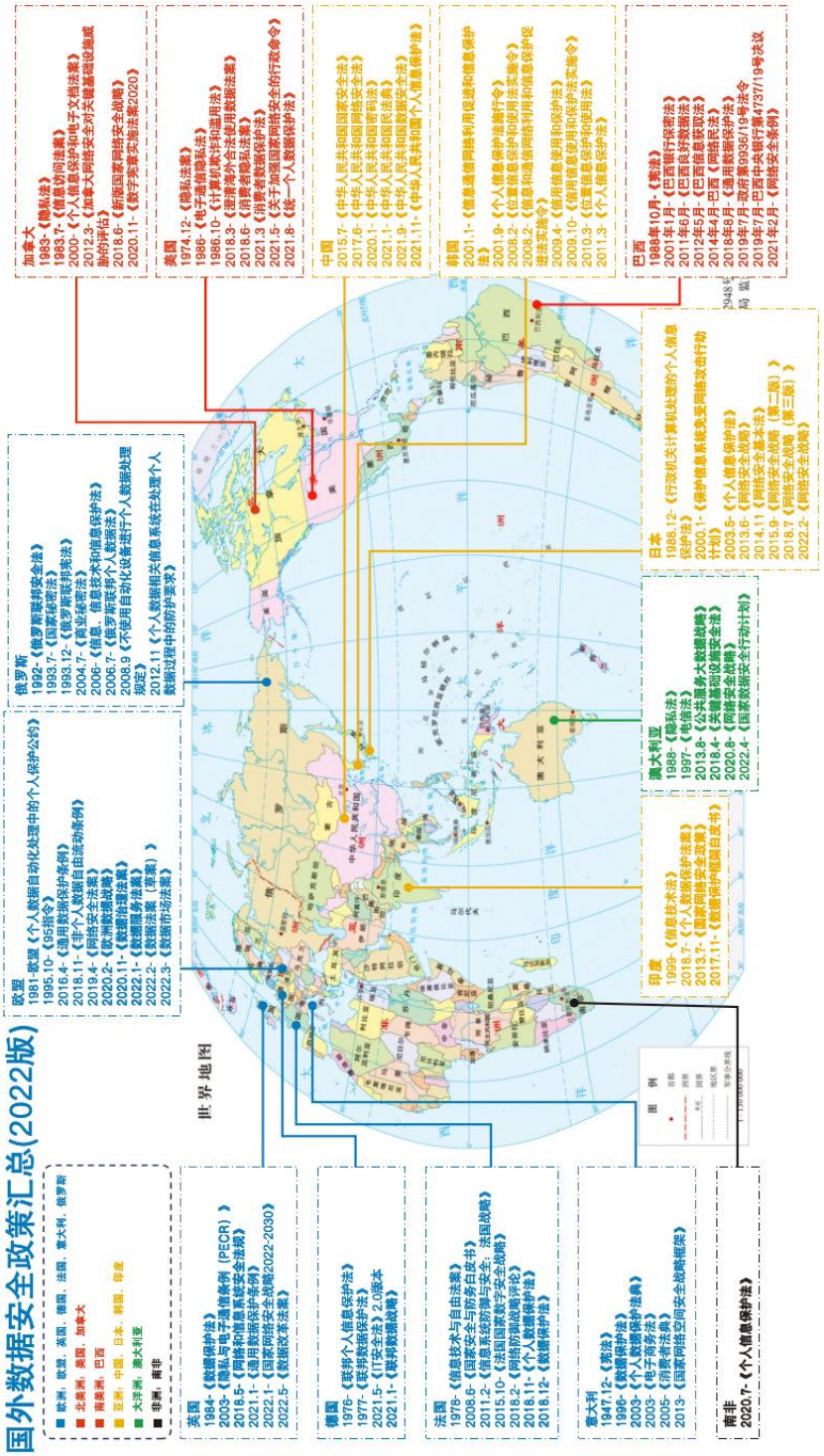
国外数据安全政策研究报告

随着人类进入数字经济时代，世界各国对数据的依赖快速上升，数据已成为国家基础性战略资源，对社会生活方式、经济运行机制、国家治理能力等产生重要影响，国家竞争焦点正从土地、人口、资本、资源的争夺转向对数据的争夺。未来国家层面的竞争力将部分体现为一国拥有数据的规模、开发利用以及掌控的能力，“数据主权”将成为继边防、海防、空防之后另一个大国博弈的空间。近年来，我国《网络安全法》《数据安全法》《个人信息保护法》等数据安全相关法律法规的相继颁布，为数据安全建设提供了制度支撑和法律保障。我国数据安全产业发展相对于世界发达国家，起步较晚，通过参考其他国家地区的数据安全政策和战略方针，能够有助于我们更深入理解我国数据安全产业的发展方向。

炼石网络与国浩律所合作，共同梳理了欧洲、北美洲、南美洲、亚洲、大洋洲、非洲六大洲，包括欧盟、德国、法国、英国、意大利、俄罗斯、美国、加拿大、巴西、日本、印度、韩国、澳大利亚、南非等 14 个国家或组织的 87 项数据安全政策及战略，从各国立法总体情况、法律位阶、法律间关系、各法的定位、内容要点等维度进行分析。由于作者水平有限，难免会有遗漏和偏差，希望读者指正。

国外数据安全政策总览

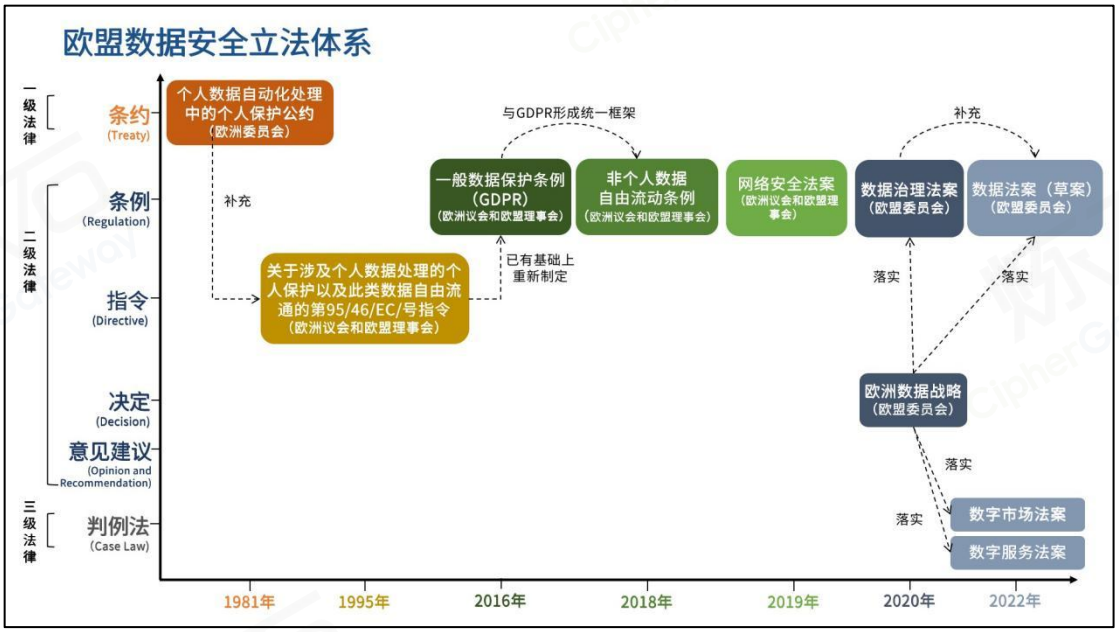
国外数据安全政策研究报告



欧盟：立法趋向统一，平衡数据流动与安全

一、 立法总体情况

欧盟的数据安全立法无论是在立法时间还是立法系统性上，都处于全球领先位置。作为一个经济共同体，欧盟在数据安全立法方面的出发点与一般实体国家存在区别，其更强调技术导向的数据共享与自由流动，消除成员国家间的信息屏障。为达到这一目标，欧盟必须在数据存储处理、公民基本权利、数据安全保护和监管、数据跨境流动等方面构建完善的法律框架。



欧盟的政策决策特点是多方面互动的，欧洲委员会、欧洲议会、欧洲理事会、欧盟理事会、欧盟委员会等机构参与制定欧盟法律法规。欧盟的法律基本框架大体可分为 3 个层次：一级法律，主要指条约；二级法律，

包括指令、法规、决定、意见建议等；三级法律为判例法，主要指根据二级法律作出的对具体事件或案例的判决或裁定。

欧盟针对数据安全立法，一级法律层面上，1981 年《个人数据自动化处理中的个人保护公约》，是世界上第一部关于数据保护的国际公约；二级法律层面上，1995 年《关于涉及个人数据处理的个人保护以及此类数据自由流通的第 95/46/EC/号指令》、2016 年《一般数据保护条例（GDPR）》、2018 年《非个人数据自由流动条例》，形成数据治理的统一框架；2019 年《网络安全法案》，确立了第一份欧盟范围的网络安全认证计划；2020 年《欧洲数据战略》，致力于实现真正的单一数据市场的愿景；2020 年《数据治理法案》、2022 年《数据法案（草案）》、2022 年《数字市场法案》、2022 年《数字服务法案》作为落实《欧洲数据战略》所采取的重要立法举措，为欧洲新的数据治理方式奠定了基础。

二、重点法律解析

01 欧盟《108 号公约》

（1）定位

1981 年，欧洲委员会通过了《个人数据自动化处理中的个人保护公约》（简称“《108 号公约》”）。《108 号公约》是世界上第一部关于数据保护的国际公约。旨在确保在每个缔约方在其管辖范围内的公民，不管其国籍或居住地，在对其个人数据进行自动化处理过程中得到保护，尊重其权利和基本自由，特别是对于隐私权方面的尊重。

随着互联网信息技术的发展及其应用的不断普及化，《108 号公约》也历经数次修订：

- 1999 年，欧洲理事会对《108 号公约》进行了首次修订；
- 2001 年，欧洲委员会对其进行了补充，加入《有关监管机构和跨境数据流通的附加协定》[1]；
- 2012 年，欧洲理事会再次针对其进行修订，通过的建议稿决定将名称

中的“个人数据自动化处理”更改为“个人数据处理”，进一步扩大适用范围；

- 2018 年 5 月，第 128 届部长委员会（Committee of Ministers）会议通过了对该公约的最新一次修订，此次修订侧重吸纳更多的国家加入公约，从而形成以公约为基础的数据保护法律制度[2]；
- 2018 年 10 月，乌拉圭与 20 个欧洲理事会成员国签署了一项欧洲理事会条约，作为《第 108 号公约》的修订议定书[3]。

（2）特点

《108 号公约》作为全球范围内第一份有关数据保护的具有法律约束力的国际性文件，反映了欧洲国家就个人数据保护作为人权保护达成的共识，并推进更多的国家参与和加入。公约建立了有关个人数据保护的基本原则以及各缔约国之间的基本义务，并将对个人基本自由与权利的保护作为缔约国履行条约规定的国家义务的出发点。此外，公约委员会的建立，在一定程度上建立起了针对个人数据保护的多国合作框架。

（3）主要内容

《108 号公约》（2018 年版）由一般规则、数据保护基本原则、个人数据跨境流通、监管机构、相互协作、公约委员会、公约修正案、最后条款等八章节、32 条款构成。

在适用范围上，公约明确是缔约国管辖范围内的个人数据处理活动，涵盖私营部门和公共部门，不再局限于此前版本所界定的“自动化的个人数据处理”活动，不再适用于自然人在纯粹的个人或家庭活动中进行的数据处理活动。

公约针对数据安全方面提出，缔约国应当规定数据控制者，在适当的情形下包括数据处理者，采取适当的安全措施以防范个人数据遭受意外的或未经授权的访问、损毁、丢失、利用、修改或传播。同时，也引入了缔约国应当规定数据控制者将个人数据泄露事件及时通报监管机构的要求。

在义务上，公约对数据处理主体提出了更广泛的义务，如“评估其计划实施的对数据主体的各项权利和基本自由可能产生影响的数据处理行为的风险”，以降低侵害人权或基本自由的风险；“在数据处理的各个阶段，采取考虑到个人数据保护权利的技术和组织措施”。

在个人数据跨境流通上，公约力求确保在处理个人数据过程中给予适当保护的同时，促进数据在各国间实现自由流通。公约明确，任何缔约国不得仅为保护个人数据之目的禁止数据跨境传输，或者设置特别授权条件。非成员国的跨境传输，需在公约规定的适当个人数据保护水平得到保障的情形下进行。

02 欧盟《95 指令》

（1）定位

1995 年 10 月 24 日，欧洲议会和欧盟理事会通过了《关于涉及个人数据处理的个人保护以及此类数据自由流通的第 95/46/EC/ 号指令》（简称《95 指令》）。《95 指令》为欧盟成员国制定和实施数据保护法律提供了一个基本框架和雏形，促成各成员国数据保护标准的趋向统一，推动了全球个人数据保护秩序的建立。

（2）特点

《95 指令》直接以指令而非条约的形式要求各成员国完善数据保护立法，致力于协调各国对自然人在数据处理领域的基本权利和自由的保护，消除个人数据在共同体内部自由流通的障碍。首次提出知情同意原则，将“数据主体已明确表示同意”作为数据处理的合法条件之一；采用统一立法模式，规定建立独立的数据保护机构，是个人信息保护法中主张域外效力的典型代表。

（3）主要内容

《95 指令》包括 72 条序言和 34 条条款，旨在提高欧洲个人信息保护法律的统一程度，弥补 1980 年出台的《第 108 号公约》，虽对成员国具

有约束力，但真正执行国家并不多，实施效果也存在差异的现实情况，进而应对高速发展的信息技术时代带来的保护个人数据权利、消除法规不一所造成的数据流通障碍的双重挑战。

在处理个人数据的安全性方面，《95 指令》提出，会员国应规定，控制者必须实施适当的技术和组织措施（特别是在处理涉及通过网络传输数据的情况下），以保护个人数据免受意外或非法破坏或意外丢失、更改、未经授权的披露或访问，防止所有其他非法形式的处理。考虑到最新技术及其实施成本，此类措施应确保与处理行为潜在的风险和要保护的数据的性质相适应的安全水平。

在数据保护监管方面，《95 指令》提出，各成员国应建立监管机构，并赋予他们完全独立的行使职能。监管机构应被赋予的权利包括调查权、干预权、法律诉讼权等。

在个人数据跨境流动方面，《95 指令》明确，成员国向第三国转移个人数据，需以第三国对个人数据提供充分保护为前提。而判断第三国对个人数据保护是否充分，应围绕数据传输操作的情况来评估第三国提供的保护水平的充分性；应特别考虑数据的性质、拟处理操作的目的和持续时间、数据来源国和最终目的地国、第三国现行的一般和部门法律法规以及该国遵守的专业规则和安全措施。

03 欧盟《通用数据保护条例》

（1）定位

2016 年 4 月 14 日，欧洲议会和欧盟理事会通过了《通用数据保护条例》(简称“GDPR”)，于 2018 年 5 月 25 日正式生效，GDPR 被称为被称为“史上最严隐私法案”。一方面，GDPR 赋予了个体用户对于自身数据更多的自主权和选择权；另一方面，GDPR 针对用户数据的控制主体和处理主体制定了十分严格的限制性规则[4]，有力地推进欧盟数字单一市场的建立。

（2）特点

GDPR 的出台，将个人数据的保护及监管提升到前所未有的高度，欧盟的数据保护立法由“Directive”（指令）提升为“Regulation”（条例）。GDPR 进一步细化权利与义务，在数据主体的权利方面，设立了“被遗忘权”、“携带权”两项新型权利；在数据处理主体的义务方面，GDPR 通过巨额的行政处罚以警示数据处理主体严格履行自身合规义务。GDPR 具有域外效力管辖权设计，全球企业都可能受到 GDPR 的管制，GDPR 同时设立数据保护官等制度辅助企业义务的履行以及监督机构的监管。为推进 GDPR 的落地与有效执行，欧盟数据保护委员会（“EDPB”）进一步陆续推出多种特定情况下的指引（Guidelines），这些指引虽然不具有法律强制力，但是其本质是对于特定场景或者 GDPR 对应条文中规定的指导方针、建议和最佳操作，因此在实践中具有较高的参考价值。

（3）主要内容

GDPR 是在《95 指令》的基础上重新制定，进一步应对《95 指令》逐步出现的化解安全风险挑战能力不足情况，共计 11 章 99 条，相较于仅 34 条的《95 指令》来说，做出了多达 3500 处具体修改，GDPR 生效的两年后《95 指令》被废止。同时，GDPR 整合了之前的隐私保护指令、电子通信隐私保护指令以及欧盟公民权利指令等，通过统一欧盟法规来协调整个欧洲的数据隐私法律，保护所有欧洲公民免受隐私侵犯和数据泄露的侵害，并简化国际业务中对于数据隐私的监管方式[5]。

04 欧盟《非个人数据自由流动条例》

（1）定位

2018 年 11 月 14 日，欧洲议会和欧盟理事会共同颁布《非个人数据自由流动条例》（简称《条例》），并于 2019 年 5 月 28 日正式实施。《条

例》旨在统一有关非个人数据的自由流动规则，与已经实施生效的GDPR形成数据治理的统一框架，以此平衡个人数据保护、数据安全，推进欧盟在单一数字市场战略下打造富有竞争力的数字经济。

（2）特点

《条例》通过废止不合理的数据本地化限制、促进专业用户数据迁移的有关规则，加强成员国监管机构的官方合作机制，推动数据和云服务商行为准则的建立，增强政府与企业对数据跨境存储与处理的信任，以保障非个人数据在欧盟内可以自由流动。

（3）主要内容

《条例》包括39条序言和9条条款，从禁止数据本地化与推动发展新技术两方面，规范非个人数据流动。《条例》界定了非个人数据的范畴，即为GDPR中界定的个人数据(任何已识别或可识别的自然人相关的信息)以外的数据；明确非个人数据在欧盟境内跨境流动的规则，为整个欧洲的数据存储和处理设定了框架，禁止数据本地化限制；允许有权机关为根据欧盟法或国家法履行其职责要求获取数据访问的权力，有权机关对数据的访问不得以数据在另一成员国处理为由受到拒绝；鼓励和促进欧盟层面自律性行为守则的制定，其以透明性和交互性原则为基础，合理考虑开放标准，保障数据转移和数据服务商自由转换。

05 欧盟《网络安全法案》

（1）定位

2019年4月17日，欧洲议会和欧盟理事会通过了《网络安全法案》(简称《法案》)，并于2019年6月27日正式施行，旧版网络安全法案（No 526/2013）被废除。《法案》确立了第一份欧盟范围的网络安全认证计划，对于欧盟各成员国网络和信息通讯安全体系的构建、安全风险防控能力的提升具有十分重要的意义。

（2）特点

《法案》指定了欧盟网络和信息安全署（ENISA）为永久性的欧盟网络安全职能机构，推行通用网络安全认证系统，对合格评定机构的资格标准做了界定。

（3）主要内容

《法案》包括序言、正文和附则三大部分。正文部分包含三个章节共计 69 个条款，涉及为 ENISA （欧盟网络安全局）的职能和任务的重新定位、网络安全认证框架及认证计划、信息和通信技术（ICT）网络安全认证等事项的具体规定。附则部分是关于获得认证资格的评估机构，应当满足的具体要求。其中，针对构建欧洲网络安全认证框架，一方面有助于增加对已根据欧洲网络安全认证计划认证的信通技术产品、信通技术服务和 ICT 流程的信任；另一方面有助于避免冲突或重叠的国家网络安全认证计划的倍增，从而降低在数字单一市场运营的企业的成本。

06 欧盟《欧洲数据战略》

（1）定位

2020 年 2 月 19 日，欧盟委员会发布《欧洲数据战略》（简称《战略》），标志着欧盟在数字一体化进程中迈出了里程碑意义的一步。《战略》概述了欧洲未来五年实现数据经济的政策举措和投资策略，旨在实现真正的单一数据市场的愿景，并在过去几年所取得成就的基础上，解决通过政策和资金措施发现的问题。

（2）特点

《战略》表明，数据是本次变革的核心环节，数据将重塑公民生产、消费和生活的方式，以数据为驱动的创新将对公民产生巨大影响；对于公民权利的尊重是构建单一数据市场的核心，在构建单一数据市场的进程中应当落实欧盟价值理念和基本人权的要求。到 2030 年，将构建一个统一的欧洲数据空间，一个真正向全世界数据开放的统一的数据市场，在这里无论是个人还是非个人数据，包括敏感商业数据都会被妥善保护，企业也

可便捷地访问几乎无限量的高质量行业数据，提高增长和创造价值同时最小化人为碳排放和环境影响。

（3）主要内容

《战略》包括背景介绍、关键点、愿景、问题、战略、国际路径、结论以及附录(欧洲战略部门和公共利益领域公共数据空间创建计划)等八个部分。《战略》的实施，将基于四个方面：有关数据访问和使用的跨部门治理框架；推动者：为数据、及加强欧洲在数据托管、处理和使用上互操作性的能力和基础设施进行投资；能力建设：增强个人能力、投资技能和中小企业；战略部门和公共利益领域的欧洲公共数据空间。其中，针对战略性行业和公共利益领域中的欧洲公共数据空间，《战略》支持建立欧洲工业(制造业)数据公共空间、欧洲绿色交易数据公共空间、欧洲交通数据公共空间、欧洲健康数据公共空间、欧洲金融数据公共空间、欧洲能源数据公共空间、欧洲农业数据公共空间、欧洲行政数据公共空间、欧洲技能数据公共空间，共 9 个欧洲数据公共空间。

07 欧盟《数据治理法案》

（1）定位

2020 年 11 月 25 日，欧盟委员会发布了欧盟《数据治理法案》（简称《法案》）的拟议草案。2022 年 4 月 6 日，欧洲议会就欧盟《法案》进行最终投票表决，并获得议会批准。《法案》的出台，被视为落实《欧洲数据战略》所采取的重要立法举措，一定程度上强化了欧盟对于公共数据的赋能，为欧洲新的数据治理方式奠定了基础。

（2）特点

《法案》构建了三项适于各个行业的数据共享机制：公共部门数据再利用机制、数据中介机构及通知制度、数据利他主义制度。

（3）主要内容

《法案》共九章 38 条，包括一般规定、重复使用公共部门机构持有的

某些类别的受保护数据、适用于数据中介服务的要求、数据利他主义、主管当局和程序规定、欧洲数据创新委员会、国际访问和转移、授权和委员会程序、最终和过渡条款。

《法案》明确了公共部门数据再利用条件。允许自然人或法人在公共部门所提供的安全处理环境中访问并再利用公共数据。《法案》针对可以被再利用的数据进行敏感性方面的限制，要求开展数据再利用的公共部门具有技术设备上的相关保障，各成员国必须设立一个单一联络点，支持研究人员和创新企业使用数据，以及必须建立能够通过技术手段和法律援助对公共部门进行支撑的数据再利用体系。公共部门机构应施加条件，以保持所使用的安全处理环境的技术系统功能的完整性。《法案》倡议建立非营利性质的“数据中介机构”，为公共数据空间提供基础设施。数据中介机构需要在指定的主管当局进行备案[6]。

08 欧盟《数据法案（草案）》

（1）定位

2022 年 2 月 23 日，欧盟委员会正式公布数据治理立法《数据法案》（Data Act）草案全文，是对《数据治理法案》的补充。《数据法案》（草案）旨在确保数据经济参与者之间公平分配数据价值，并促进数据的获取和使用，有助于实现更广泛的政策目标，即确保欧盟所有部门的企业能够创新和竞争，有效增强个人数据权能，并为企业和公共部门机构提供更成比例和可预测的机制，以应对重大政策和社会挑战，包括公共紧急情况和其他特殊情况，具有重要的风控合规风向标意义。

（2）特点

《数据法案》（草案）构建了适用于所有部门的数据使用权基本规则，将促进个人和企业自愿共享数据，并统一某些公共部门数据的使用条件，而不改变数据的实质性权利或既定的数据访问和使用权限。《数据法案》（草案）还补充了《数字市场法案》的提案，该法案将要求某些被确定为

“守门人”的核心平台服务提供商，为通过业务和最终用户活动产生的数据提供更有效的可移植性。

（3）主要内容

《数据法案》（草案）条文涉及数据共享、数据持有人义务、公共机构访问、针对非个人数据的国际传输、云转换和互操作性等诸多方面等规定，监管对象主要为欧盟市场上销售产品的制造商和数字服务提供商，以及此类产品或服务的用户，数据处理服务提供商等。

《数据法案》（草案）提出，在安全、数据保护和隐私以及消费者保护方面，应维护（但不限于）欧盟法律、价值观和标准。为了防止非法访问非个人数据，受该法案约束的数据处理服务提供商，如云和边缘服务，应采取一切合理措施，防止访问存储非个人数据的系统，包括酌情通过数据加密、频繁提交审计、验证是否遵守相关安全保证认证计划以及修改公司政策。

《数据法案》规定了用户可以在不同数据处理服务提供商之间进行服务切换的权利，以及数据处理服务提供商向境外传输非个人数据的义务。一是消除了在数据处理服务提供商之间进行有效切换的技术、组织、合同等方面障碍；二是明确了数据处理服务提供商跨境传输非个人数据的相关要求，如数据处理服务提供商应采取一切合理的技术、法律和组织措施，包括合同安排，以防止国际传输或政府访问在其自身在欧盟境内持有的非个人数据。

09 欧盟《数据市场法案》

（1）定位

2022 年 3 月 24 日，欧洲议会和欧洲理事会就《数字市场法案》（“该法案”或“DMA”）的最终稿暂时达成一致意见。该法案旨在作为对欧盟传统反垄断执法的补充，创设一套以大型数字公司为合规义务主体的“守门人”制度，通过对被指定为“守门人”的数字公司施加法定义务、设置

禁止性行为，从事前监管的角度，实现对于欧洲数字市场的公平性与竞争力的保障。目前，该立法已经于7月18日经欧盟理事会最终批准，接下来，欧洲理事会主席和欧洲议会议长将分别签署该项法律，随后在欧盟公报颁布后6个月生效实施。该法案预计将在今年9月获欧盟成员国批准。

（2）特点

该法案针对主要科技公司的许多核心商业行为，并把此类行为列为非法，例如，谷歌和Meta将不能在多个平台上提供有针对性的广告，即共享获得用户在同一家公司的使用数据；苹果公司将不得不允许用户在其应用商店以外的其他地方下载应用程序，并且可以卸载预装应用；亚马逊将被禁止从第三方卖家收集服务数据等等。《数字市场法案》的提出，标志着打击大型平台滥用行为的理念发生了变化，或将结束多年来欧盟在无休止的法律诉讼中徒劳地追逐这些大型企业的侵权行为。

DMA法案主要有以下两个特点：

“强制规定严格”——针对互联网平台严禁强行推送广告；严禁预装浏览器等应用软件；不能对自己的产品或者服务给予优惠待遇；允许开发者提供第三方支付系统；允许用户从第三方应用商店安装应用；与开发者和竞争对手共享数据和指标等。

“处罚标准严苛”——违反法案企业将面临高达其全球年营业额10%的巨额罚款，再犯可处年营业额20%的罚款，系统性违规可能面临重组等监管要求。

（3）主要内容

DMA设置了对于“守门人”身份认定的标准：

1）对内部市场有重大影响；

2）其提供了一个业务用户接触终端用户的重要网关的核心平台服务；

3）其在经营活动中享有稳固和持久的地位，或者可以预见在不久的将来，其将享有这样的地位。

DMA 法案中同时对上述标准作出了细化，即过去 3 个财年中，欧盟年营业额大于或等于 75 亿欧元，或者市值至少为 750 亿欧元；在欧盟每月终端活跃用户超过 4500 万；控制至少 3 个欧盟成员国的一项或多项核心平台服务，例如应用商店、搜索引擎、社交媒体、云服务、在线广告和浏览器。

另外，“守门人制度”明确了“守门人”的禁止性义务，具体如下：

“守门人”企业不应当

1）以提供在线广告服务为目的而处理最终用户因使用第三方服务的个人数据，且该第三方服务使用守门人的核心平台服务;

2）将来自相关核心平台服务的个人数据与来自其他核心平台服务的个人数据相结合，或与来自守门人、第三方服务平台提供的任何其他服务的个人数据相结合；

3）将来自相关核心平台服务的个人数据交叉使用于守门人单独提供的其他服务中，包括其他核心平台服务，反之亦然；

4）将终端用户登录到守门人的其他服务，以合并个人数据。

10 欧盟《数据服务法案》

（1）定位

当地时间 2022 年 1 月 20 日，欧洲议会以 530 票赞成、78 票反对、80 票弃权的表决结果通过了《数字服务法》。这一法案旨在进一步加强对大型互联网平台的监管，确保平台对其算法负责，并改进内容审核。法案将被用作与代表成员国的理事会主席国法国进行谈判的授权。一旦 9 月 (DSA) 在欧盟理事会正式通过，这项法案将由欧洲理事会主席和欧洲议会议长签署，并在欧盟官方公报上公布，并在公布后 20 天生效。DSA 将直接适用于整个欧盟，并将在生效后十五个月或从 2024 年 1 月 1 日（以较晚者为准）开始适用。关于超大型在线平台和超大型在线搜索引擎的义务，DSA 将在委员会指定为此类平台四个月后提前适用。

（2）特点

《数字服务法案》（Digital Services Act）以信息中介服务提供者（intermediary services）以及网络平台（online platforms）为合规义务主体，侧重于保护用户权利，着眼于普通消费者与强势平台方之间的关系，要求互联网平台企业采取更多措施删除非法和有害的在线内容，旨在从内容及形式等方面规范数字公司提供的服务，主要目的在于构建和谐安全、公平竞争、可信任的网络环境，有效保护《欧盟基本权利宪章》中的基本权利，要求数字服务提供者为消费者提供更加安全、透明和值得信赖的在线服务。

（3）主要内容

该《法案》从主体的角度出发，对网络空间中的平台、用户以及广告商进行区分，并分别设置不同的合规义务与应对特定情形的应对措施。

从平台的角度，该法案要求平台接受审计，进而评估其“风险管理”系统，并且允许特定研究人员以访问其算法，进而打破“黑箱”模式的窘境。

从用户的角度，该《法案》将禁止用户对于非法内容的重复发送行为，并要求相关互联网平台在其平台上设置对应的内部投诉机制，以允许用户对平台内容提出异议。

而从广告商的角度，法案要求自动化决策以及广告精准投放将不得以儿童作为目标，也不能以用户的性行为、性别或者宗教信仰等涉及敏感个人信息的标签来进行广告投送。

三、参考文献

[1]安全内参.欧洲理事会“108号公约”全文中文翻译[EB/OL]. https://www.secrss.com/articles/10012.

[2]互联网法治研究.【域外译评】张余瑞|2018年《个人数据处理中的个人保护公约》译文[EB/OL]. https://mp.weixin.qq.com/s/tTsNcupYh8ejhNOEZ7pqGQ

[3]张衡. 21 国签署个人保护公约 强化个人数据国际保护[J]. 信息安全与通信保密,2018(11):8.

[4]冯梦琦.《通用数据保护条例》内容及实践浅析[J]. 法制与社会,2019(12):35-36. DOI:10.19387/j.cnki.1009-0592.2019.04.251.

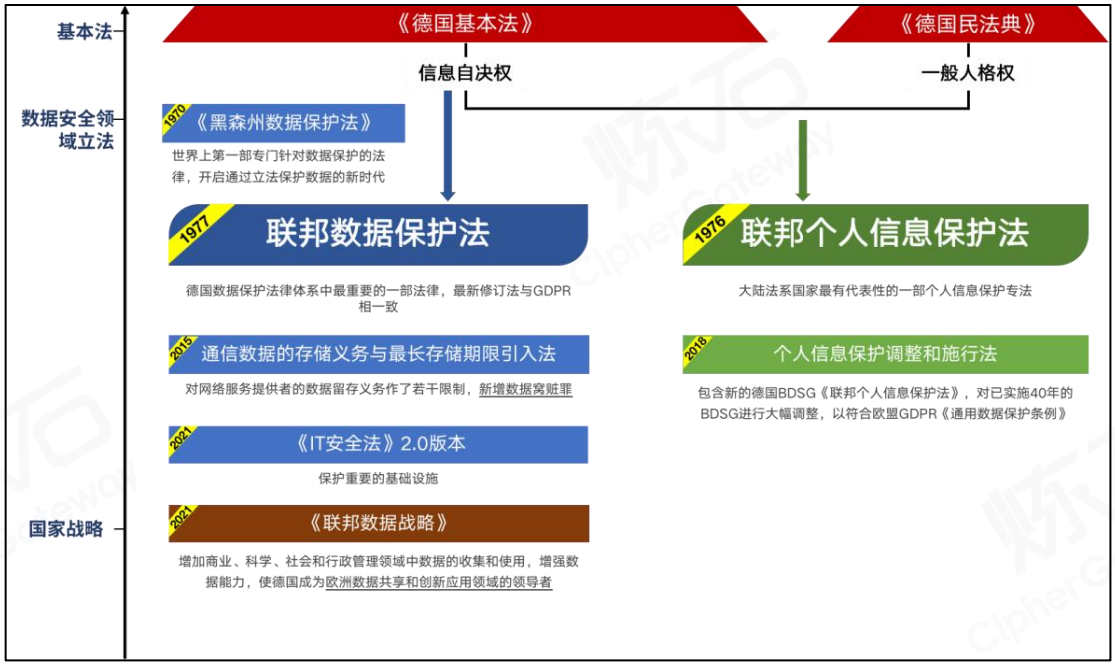
[5]何玉颜. 欧盟《通用数据保护条例》解读及其对我国个人数据保护的启示[J]. 图书情报导刊,2018,3(11):67-72. DOI:10.3969/j.issn.1005-6033.2018.11.013.

[6]董宏伟、王琪、刘佳婕.关键基础设施安全应急响应中心.原创 | 5G 时代下《欧盟数据治理法案》的解读与启示：公共行政数据篇[EB/OL]https://mp.weixin.qq.com/s/j_KHyvi4t1GfUJr1vI8Omg

德国：从中央到地方、从一般到专门

一、 立法总体情况

在世界范围内，德国一直是数据保护方面的“模范生”。德国最早通过明确立法对数据进行严格保护，已建成从中央立法到地方立法、从一般立法到专门领域立法的全方位数据保护法律体系框架，这个体系在世界范围内同样具有领先性。同时，德国在数据保护领域长期致力于欧洲法律一体化的协调发展，深刻影响了欧洲乃至全球的数据立法进程。近年来，德国对电子监控、个人信息存储、电子办公、工业互联网、视频会议等新兴技术发展带来的挑战予以高度关注，通过细化法律形式，强化数据安全风险管理[1]。



二、 重点法律解析

01 德国《联邦个人信息保护法》[2]

（1）定位

1976 年，德国联邦议会通过的《联邦个人信息保护法》，是大陆法系国家最有代表性的一部个人信息保护专法。该法的正式名称是《防止个人

信息处理滥用法》，采取统一立法模式，对个人信息保护进行统一规范、统一保护。

（2）特点

《联邦个人信息保护法》以宪法和民法为理论基础，宪法基础是信息自决权理论，民法基础是一般人格权理论，其目的是在个人信息处理过程中对个人隐私给予统一而充分的保护，使个人信息处理行为合法化。在民法基础方面，海洋法系和大陆法系主张不同。海洋法系的代表国美国认为，隐私权是个人信息保护的理论基础，美国个人信息保护法直接以隐私权命名；而德国认为，依据《德国民法典》，一般人格权是保护个人信息的基础权利。

（3）主要内容

个人信息保护原则是《联邦个人信息保护法》的核心内容。该法建立了完备的原则体系：直接原则、更正原则、目的明确原则、安全保护原则、公开原则、限制利用原则等。

《联邦个人信息保护法》对监督机制做出了完整而系统的规定。该法设置个人信息保护委员监督公务机关处理个人信息的情况。同时，还设置信息保护人对非公务机关处理个人信息的情况进行监督。信息保护人由各单位自行任命，以具备必要的专业知识和良好的品行为任命的基本条件。

损害赔偿制度是《联邦个人信息保护法》的权利救济措施，也是个人信息主体本人补救权利的最终途径。该法将个人信息的侵权行为分为两大类，即行政侵权行为和民事侵权行为。该法对两种侵权行为发生的损害赔偿进行了明确的区分，分别规定不同的归责原则和赔偿范围。

《联邦个人信息保护法》对于跨国传输有明确规定。跨国传输是指德国国家机关将其个人信息传输给外国（或地区）的国家机关或非国家机关（包括国际组织），而不论这些机构是否在德国境内。而国家机关向非国家机关传输个人信息，应满足两个要件：第一，传输行为是国家机关履行

职务的行为，且具备个人信息的利用要件；第二，个人信息接收者对要求传输的个人信息有正当利益，且个人信息主体没有值得保护的利益足以禁止传输实施。这也是德国信息保护法个人信息跨国传输的基本条件[3]。

02 德国《联邦数据保护法》[4][5][6][7][8]

（1）定位

1977 年，德国联邦议会出台《联邦数据保护法》，该法在自出台至今的几十年间经历了多次修正。2019 年 11 月德国议会对《德国联邦数据保护法》进行距今为止的最后一次修订。作为德国数据保护法律体系中最重要的一部法律，该法在德国个人数据保护事业中发挥重要作用。《联邦数据保护法》一直贯彻个人信息自决权理论，通过规定个人信息的知情权、修改权、同意权、披露权及使用权等一系列权利，不断强化个人对个人信息的控制[9]。

（2）特点

《联邦数据保护法》旨在通过数据保护实现一般人格权的保护，同时强化个人信息自决权理论，这意味着德国将个人数据保护的法律站位上升到落实宪法（即《德国基本法》）的高度而不是简单的政府执法工作。该法使德国数据保护法律制度与欧盟 2016 年颁布的《通用数据保护条例》（GDPR）和《关于有权机构在预防、调查、侦察或批捕犯罪嫌疑人或执行刑事处罚中自然人保护和有关数据自由流通的指令》相互衔接。

（3）主要内容[10]

法律主旨优先处理欧洲法而非国内宪法。旧版《联邦数据保护法》指出该法目的在于保护人格权在个人数据处理过程中不受侵害。但是，新版《联邦数据保护法》删除了法律目的这一款，意味着在《联邦数据保护法》中更加优先处理欧洲法而非国内宪法，但个人权的保护仍是基础。

保护的直接客体并非一般意义上的数据，而是与个人具有关联性的个人数据。按照旧版定义，个人数据是指与一个已识别或可识别的自然人具

有个人化或实质化关联的各种具体数据。新版《联邦数据保护法》删除了对个人数据的定义条款，但是“个人数据”这一概念仍然是该法自始至终所使用的基本概念。

立法目标和保护客体决定了该法保护权益的特殊性。该法出台前，立法材料中明确提到，鉴于技术的进步，立法应当采取适当措施保护数据处理过程中个体的私人领域不受侵犯，即：一般人格权在私生活领域的具体化。随着社会发展，在自动化数据处理的现代条件下，人格的自由发展取决于个人有权对抗对其个人信息无限制的搜集、储存、使用与传送，即：个人信息自决权理论。这一转变意味着德国将保护个人数据上升到宪法基本权利加以确证。

明确侵犯公民个人信息自决权行为的犯罪构成要件和罚则。在 GDPR 生效后，为实现欧洲法律的协调化发展目标，该法对罪刑条款大幅度修正。规定在未经授权的情况下，以营利的方式，故意将非开放的个人数据传输给第三方或通过其他方式使其开放，处 3 年以下自由刑或罚金刑。

03 德国《IT 安全法》[11]

（1）定位

2021 年 5 月 28 日，德国联邦议院颁布《IT 安全法》2.0 版本，旨在保护重要基础设施数据安全，通过弥补法律漏洞并扩大监管框架，以提高德国 IT 系统的安全性，并加强国家安全。

（2）主要内容

扩大联邦信息安全办公室（BSI）的权限。包括以技术调查的形式对路由器、智能电视等在内的 IT 产品进行扩展筛选，以确保产品的安全性；从电信服务提供商处提取数据信息，以确定网络攻击的受害者，并为防御此类攻击提供有效支持。存储日志数据的时限可延长到最多 18 个月。

加强对数字消费者的保护。通过“自愿性 IT 安全标签”等手段，推动与安全相关的 IT 产品的透明度，特别是保证消费领域产品的 IT 安全功

能可以被消费者看到和理解。扩展关键基础设施范畴。关键基础设施行业新增“废物处理”为关键基础设施部门；扩展相关性实体，将“具有特殊公共利益的基础设施”和“具有网络关键性”的运营商纳入进来。

新增制造商、供应商和关键基础设施部门的义务。该法规定，关键基础设施部门运营商需安装技术防范系统，以监测对其 IT 基础设施的攻击。BSI 将在未来明确定义关键基础设施核心部件的最低标准，关键基础设施行业将只能采购并安装以发布“可信声明”的制造商组件。

对跨国传输要求设置官方查询联络点。对于住所在国外、因而将数据存储在国外服务器上的供应商，向德国提供服务时，需在德国设立一个官方查询联络点。

对有关罚款的规定进行修订。加大对计算机相关犯罪和数据保护相关犯罪的处罚力度，并修订罚款目录。根据违法行为，罚款金额最高可达 2 000 万欧元，或占公司上一营业年度全球总营业额的 4%，以较高者为准。

04 德国《联邦数据战略》[12]

（1）定位

2021 年 1 月，德国政府发布《联邦数据战略》，该《战略》旨在增加商业、科学、社会和行政管理领域中数据的收集和使用，增强数据安全保障能力，使德国成为欧洲数据共享和创新应用领域的领导者。

（2）主要内容

《战略》确立了四大行动领域，分别为：构建高效且可持续的数据基础设施；促进数据创新并负责任地使用数据；提高数据能力并打造数据文化；使德国成为数据先驱。

（a）构建高效且可持续的数据基础设施：德国和欧洲必须确保在相关标准制定过程中的发言权，以增强数字主权。此外，只有在数据基础设施可靠，能保证数据安全性的情况下，数据生态系统的参与者才愿意共享和使用数据。

（b）促进数据创新并负责任地使用数据：德国联邦政府将创造恰当的框架条件，使政府、社会、产业界和科学界可以负责任且可持续地使用和共享数据，使其成为数字创新的核心组成部分。

（c）提高数据能力并打造数据文化：《战略》提出，发起国家数字化教育行动，提供有关数字化主题的教学，并逐步连接各个联邦州的教育系统；借助教育与研究部“中小企业创新产品和服务研究”资助措施，帮助德国企业开发新型数字化产品和生产系统解决方案等。

（d）使德国成为数据先驱：德国在联邦公共行政研究院中建立数字学院，提高联邦公务员的数字能力和基于数字的行政管理能力；联合联邦外交部、内政部、国防部和总理府构建联邦政府内部数据平台，使各个部门以标准化的格式共享数据。

三、参考文献

[1]王华伟：数据刑法保护的比较考察与体系建构[EB/OL].https://www.law.pku.edu.cn/xwzx/pl/133424.htm

[2]李晓蕊.浅析德国联邦个人资料保护法[EB/OL].http://www.law-lib.com/lw/lw_view.asp?no=22149

[3]齐爱民.德国个人资料保护法简论[J].武汉大学学报(人文科学版),2004(04):465-470.

[4]李爱君,方颖,方宇菲,李昊,李廷达,马军,任依依,姚岚. 德国《联邦数据保护法》[C]//.金融创新法律评论（2017 年第 2 辑・总第 3 辑）.,2017:128-164.

[5]刘悦心,王克萍,李慧瑜,吴惟予,龙怡. 大数据时代下德国数据权利保护的研究[C]//.《上海法学研究》集刊（2021 年第 6 卷 总第 54 卷）——新兴权利与法治中国文集.[出版者不详],2021:186-193.DOI:10.26914/c.cnkihy.2021.032946.

[6]刘金瑞.德国联邦数据保护法 2017 年版译本及历次修改简介[J].中德法学论坛,2017(02):339-388.

[7]李爱君,方颖,方宇菲,李昊,李廷达,马军,任依依,姚岚. 德国《联邦数据保护法》[C]//.金融创新法律评论（2017 年第 2 辑・总第 3 辑）.,2017:128-164.

[8]姜天怡.《德国联邦数据保护法》对我国个人征信权益保护的启示[J].黑龙江金融,2012(12):27-30.

[9]刘悦心等.大数据时代下德国数据权利保护的研究[EB/OL].https://www.thepaper.cn/newsDetail_forward_16352850

[10]张效羽：德国如何保护个人数据[EB/OL].https://www.sohu.com/a/311622918_618422

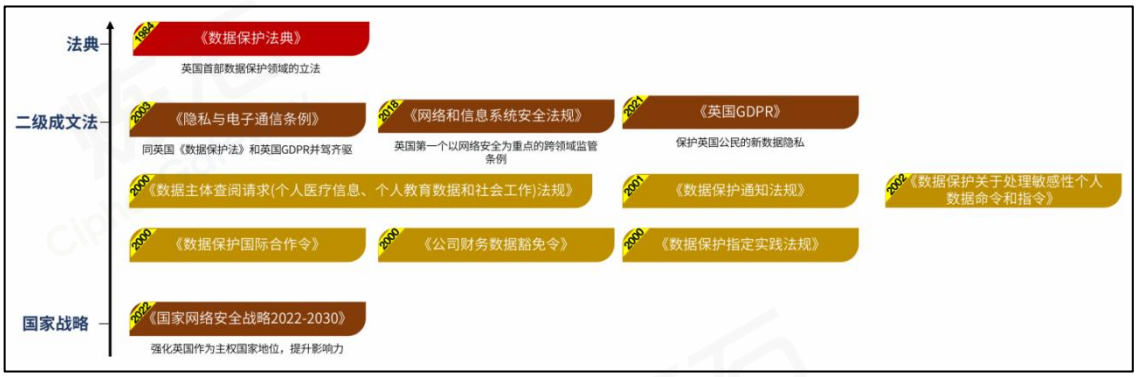
[11]苏州信息安全法学所.德国《IT 安全法》2.0 正式生效，加强关基安全保障[EB/OL]. https://www.secrss.com/articles/32381

[12]科情智库.德国出台《联邦数据战略》，增强数字主权[EB/OL]. https://www.secrss.com/articles/32713

英国：以法典、判例法、二级成文法为基础

一、立法总体情况

英国数据保护制度的建立是西方社会近百年来对于个人隐私权理论发展和延伸的产物。因此，在欧盟数据保护的法律框架影响下，英国对个人数据和隐私的立法保护，以成文法为立法核心，逐渐形成由法典、判例法、民间实践、二级成文法和执法机构组成的数据保护制度体系[1]。



二、重点法律解析

01 英国《数据保护法》[2]

（1）定位

1984 年，英国议会通过的首部《数据保护法》，是英国推动发展数字经济顶层设计中的重要举措。该法提出个人数据保护的基础性原则，禁止数据主体未经注册持有个人数据，设立数据保护登记官和数据保护法庭，分别作为法令执行的监管机构和申诉机构。

（2）特点

维持可信。为使英国经济和社会能最大程度地从数据创新中获益，公众需要知道个人数据是否被安全且合理利用。因此，该法要求有关机构在使用个人信息时必须严格保密。

推动未来贸易发展。数据跨境流动能力对一国未来经济运行至关重要，新的数据保护法案致力于推动英国与欧盟及其他国家之间数据流动最

大化。

确保安全。新法案将采取措施应对各种犯罪行为的威胁，促进各国司法机构之间的数据共享与安全合作。

（3）主要内容

新法案给予公民更多的个人信息控制权，如“知情-同意”权、数据可携权、被遗忘权、用户画像的发言权等。

完善了对企业利益的保护。新法案修改和完善了 1998 年《数据保护法》对于公、私企业的相关要求，以适应数字经济发展的需要，帮助企业更好地保护个人数据，提升企业的声誉和业务。

增加对监管机构 ICO 的授权。英国个人数据保护机构信息专员办公室（ICO）获得更多的权力来维护消费者利益，包括调查权、民事处罚权、刑事追责等。同时，强化对违法行为举报人的保护，对最严重的违规行为进行高达 1700 万英镑或全球营业额 4％的罚款。

为刑事司法机构设定了专门的数据保护框架。新法案考虑到刑事司法机构为处理惩治犯罪行为而需要收集、使用、分享数据和信息的情形，为其量身定做了出于执法目的而处理数据的框架。

02 英国《隐私与电子通信条例》

（1）定位

2003 年，英国议会通过《隐私与电子通信条例（PECR）》，要求电子通信服务商保护终端用户信息，由信息专员负责监督执行。该条例是英国对欧盟《电子隐私指令（指令 2002/58/EC）》的落地实施，同英国《数据保护法》和英国 GDPR 并驾齐驱，赋予公民在电子通信方面享有隐私权，保护消费者免受信息滥用和潜在网络犯罪的危害。

（2）特点

该条例将大规模使用的网络即时通讯服务纳入法律的监管范围之中，

使得民众和企业之间的权利与义务更为明晰，在保护用户隐私的基础上，更好的促进相关行业的发展。

（3）主要内容

该条例是一项数据隐私法规，与 GDPR 一样，规定企业在未经个人数据主体同意的情况下可以进行和不能进行的营销活动，对于企业该如何处理个人和公司数据给出指引。简而言之，该条例适用于至少执行以下一项的所有组织：通过电话、电子邮件、短信或传真进行营销；在网站上使用 cookie 或类似技术；编制电话簿（或类似的公共目录）；网络或通信服务提供商。PECR 和 GDPR 两项法规相辅相成，但二者又存在显著差异：GDPR 要求在 72 小时内报告违规行为，而 PECR 要求 24 小时；与 GDPR 不同，PECR 除适用于个人外，还适用于其他组织。

03 英国《网络和信息系统安全法规》

（1）定位

2018 年 5 月 10 日生效的《网络和信息系统安全法规》，是欧盟 2016 年 7 月 6 日颁布的《网络和信息系统指令》的英国版，是英国第一个以网络安全为重点的跨领域监管条例，在实现英国国家网络安全方面发挥着关键作用，旨在提高网络和信息系统的安全水平（包括网络和物理弹性），以保障基本服务和数字服务。

（2）主要内容

明确法规的适用范围：该法规适用于两类主体，一类为英国能源、交通、健康和数字基础设施部门的基本服务运营商（OES）；另一类为数字服务提供商（DSP）。二者必须采取适当相称的技术和网络安全对策，以管理其基础服务或数字服务所依赖的系统风险。该条例不适用于被视为“微型或小型企业”的 DSP（雇用少于 50 人且年营业额和/或资产负债表总额低于 1000 万欧元（约 870 万英镑）的组织）。

细化责任主体法定义务：OES 和 DSP 必须采取措施，保障网络和信息

系统安全，具体包括：评估风险，预防和尽量减少安全风险事件的影响，且及时向有关当局报告安全风险事件；开展业务连续性管理，监控和测试过程和程序是否符合国际标准。

规定“重大”事件的评判标准：该法规规定组织不得迟于 72 小时，向其主管当局报告“重大”事件。对于 OES ，在确定事件是否为“重大”时必须考虑三个因素：受中断影响的用户数量、中断的持续时间、受事件影响的地理区域大小。对于 DSP，以下情况将判定为重大事件：事件导致超过 500 万用户服务不可用；影响超过 100000 名用户的网络或信息系统访问的数据失去机密性、完整性、可用性或真实性；对公共安全或生命损失的风险；或者对至少一名用户造成的财产损失超过 100 万欧元（约合 86 万英镑）。

明确合规性评估部门：国家网络安全中心 (NCSC) 是英国的国家技术机构，负责提供网络安全方面的建议和协助，为其计算机安全事件响应团队 (CSIRT) 提供技术建议和单点联系 (SPOC)。

04 英国《通用数据保护条例》[3]

（1）定位

由于英国在 2020 年底离开欧盟，不再受《通用数据保护条例》管辖。因此，该国需要一部新的法规保障公民个人数据权利，英国 GDPR 由此诞生。英国 GDPR 是英国通用数据保护条例，于 2021 年 1 月 1 日生效，涵盖了英国处理个人数据时的主要原则及权利和义务，并与 2018 年《数据保护法》并列，适用于向英国个人提供商品和服务和/或监控英国任何个人行为的任何组织。

（2）主要内容

明确适用范围：该法规适用于英国的数据控制者或数据处理者处理的个人数据；英国 GDPR 也适用于不在英国设立的数据控制者或数据处理者，处理英国的个人数据（向英国的数据主体提供商品或服务，或正在监

控数据主体的行为，其中这种行为发生在英国）的情况。

衔接欧盟 GDPR 对于数据控制者的要求：英国 GDPR 延用欧盟 GDPR 数据保护的原则，这些数据原则包括透明度、目的限制、存储限制、数据最小化、准确性、完整性和保密性以及问责制。

规定数据主体的权利：英国 GDPR 下数据主体的权利与欧盟 GDPR 赋予数据主体的权利大致相似，包括知情权、访问权、更正权、删除权、数据可移植性、不受自动决策影响的权利以及反对或选择退出的权利。但英国 GDPR 对于部分内容做了更改：访问权——访问数据主体的个人数据将“影响公司金融工具的价格或相关行动决定”或“损害英格兰银行特定职能”的情况不允许数据主体访问；更正权——“损害旨在保护公众的特定功能”或“与披露个人数据的法定义务相悖”等情况不允许更正其个人数据。

英国 GDPR 对向第三方传输个人数据施加更多限制：根据法律，只有在出于执法目的而需要进行此类转移时，才允许转移；数据转移活动应在第三方国家/地区充分的数据保护措施的前提下开展；或在其他适当的保护措施到位的前提下；或针对特定的特殊情况；或与第三方国家的相关当局或国际组织有关，例如履行执法相关职能的国际机构。

脱欧后重新制定罚则：英国需要一种新的方式，惩罚 2020 年脱欧后发现的违规数据控制者。因此，信息专员办公室或 ICO 有权执行英国 GDPR，罚则与欧盟 GDPR 类似。

05 英国《国家网络安全战略 2022-2030》[4]

（1）定位

2022 年 1 月 25 日，英国政府正式发布《国家网络安全战略 2022-2030》。该战略对英国政府如何确保公共部门有效应对网络威胁进行阐释，并描绘战略愿景，即确保政府核心功能对网络攻击具有韧性，强化英国作为主权国家地位，提升影响力，旨在打造一个民主、负责任的网络强国。

（2）主要内容

该战略的支柱由五个目标支撑：设定了在网络弹性方面需要考虑的维度，提供可应用于整个政府的一致性框架和共同语言。包括：管理网络安全风险、防范网络攻击、检测网络安全事件、将网络安全事件的影响降至最低、培养正确的网络安全技能知识和文化等。

明确阶段发展目标：当所有政府组织满足网络安全保障框架下相应网络评估框架（CAF）配置文件中规定的结果时，该战略的目标将得以实现：到 2025 年，被确定负责关键职能的政府机构将“增强”达到 CAF 简介中规定的成果；到 2026 年，所有中央政府部门都将达到 CAF 简介中规定的成果；到 2030 年，所有其他政府机构将“基本”达到 CAF 简介中列出的成果。

06 英国《数据改革法案》[5]

（1）定位

当地时间 2022 年 5 月 10 日，英国举行国家议会开幕式，英国王储查尔斯王子在演讲中，公布了一项新的《数据改革法案》，旨在指导英国独立于欧盟隐私立法。该法案将用于改革英国现有的《通用数据保护条例》和《数据保护法案》。

（2）主要内容

该法案提出，借助英国脱欧，创建一个世界级的数据权利制度，从而建立一个新的有利于增长和值得信赖的英国数据保护框架，以减轻企业负担、促进经济发展、帮助科学创新并改进英国人民的生活；对信息专员办公室 (ICO) 进行现代化改造，确保其有能力和权力对违反数据相关立法的机构采取更有力的行动，同时要求其对议会和公众更加负责；增加行业对智能数据计划的参与度，使公民及小企业对他们的数据有更多的控制权，并通过帮助改善在健康和社会护理环境中个人数据主体对数据的适当访问来帮助需要医疗保健的人。

同时，该法案指出，通过减轻英国企业所面临的负担提高其竞争力和效率，例如建立一个注重隐私结果的数据保护框架；通过更有效地提供公共医疗保健、安全和政府服务，确保数据可用于赋予公民权利并改善他们的生活；为个人数据使用创造更清晰的监管环境，推动负责任的创新并推动科学进步；确保监管机构对违反数据权利的组织采取适当行动，并确保公民对其权利有更明确的认识；简化研究规则，以巩固英国作为科技超级大国的地位。

三、参考文献

[1]李重照 黄璜.英国政府数据治理的政策与治理结构[EB/OL].https://www.sohu.com/a/364577092_661904

[2]康晋颖. 论英国个人数据保护制度[D].对外经济贸易大学,2005.

[3]英产.英国政府提出新的网络安全法律[EB/OL].https://mp.weixin.qq.com/s/u2Hpw6RlEdYSx9YNbGEQZg

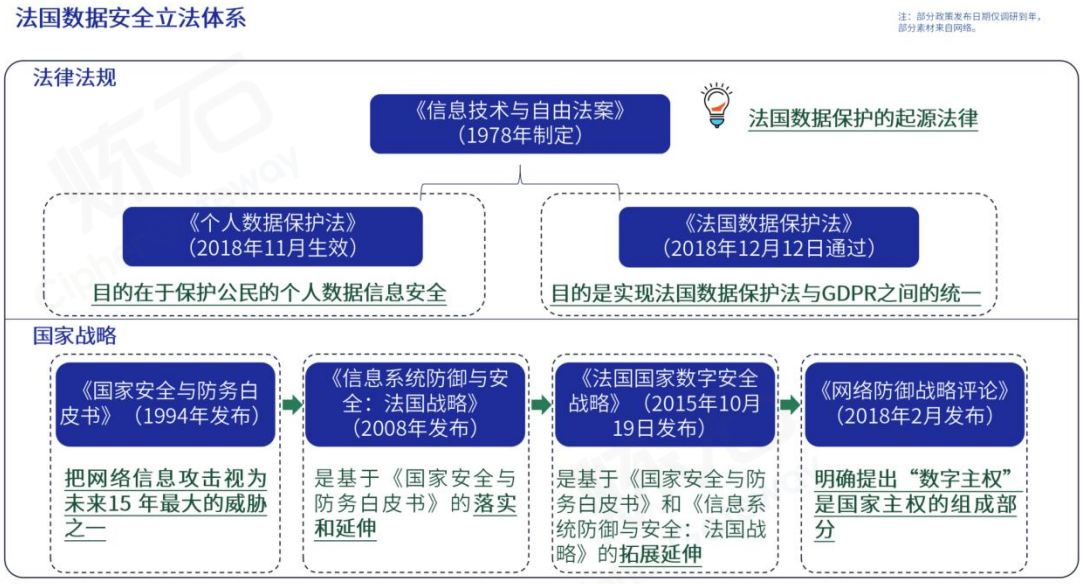
[4]苏州信息安全法学所.英国政府发布《国家网络安全战略：2022-2030 年》[EB/OL].https://www.secrss.com/articles/38733

[5]数据合规公社.英国公布《数据改革法案》：创建一个世界级的数据权利制度[EB/OL].https://www.secrss.com/articles/42289

法国：确定“数字主权”的战略性地位

一、立法总体情况

法国作为最早开发网络技术的国家之一，其互联网已经十分普及。互联网的快速发展，凸显了网络管理的重要性。法国致力于保障个人信息的安全，并力求通过立法的形式来治理数据安全问题。



1978年，《信息技术与自由法案》制定，这部法律是法国保护数据安全的起源法律之一。该方案明确阐述了信息技术发展与信息安全的关系，即：“信息技术应该为每个公民服务。它的发展应在国际合作的背景下进行。它不得侵犯人的身份、人权、隐私及公共自由等。”在该法律的基础上，法国的《个人数据保护法》及《数据保护法》分别在2018年末生效和发布，根本目的在于保障法国的个人数据和重要数据的安全。

1994年,为适应国际战略形势的变化,法国发表了冷战后的第一部国防白皮书，并把网络信息攻击视为未来15年最大的威胁之一，在此基础上，法国分别于2008年和2015年相继推出了《信息系统防御与安全：法国战略》和《法国国家数字安全战略》，体现出了法国对网络信息防护的重视。2018年2月发布的《网络防御战略评论》更是明确提出了“‘数字主权’

是国家主权的组成部分”，数据安全的地位上升到新的战略高度。

二、 重点法律解析

01 法国《信息技术与自由法案》

（1）定位

法国 1978 年制定的《信息技术与自由法案》涉及个人数据保护，也是这是法国数据保护的起源法律之一。2004 年 8 月 6 日在“保障个人信息安全”方面有所修订。

（2）特点

该方案明确阐述了信息技术发展与信息安全的关系，即：“信息技术应该为每个公民服务。它的发展应在国际合作的背景下进行。它不得侵犯人的身份、人权、隐私及公共自由等。”

（3）主要内容

该方案提出了数据跨境的前提：如果作为数据接收方所在国家的非欧洲共同体成员国家，在实际或可能处理的个人数据方面，没有为个人隐私、自由和基本权利提供足够的保护，则数据控制者不得将个人数据传输到非欧洲共同体成员国；国家提供保护的充分性应特别考虑到该国现行规定和该国适用的安全措施，以及数据处理的具体特征，包括其目的和持续时间、数据性质、数据来源、目的地等特征。

以及不满足前提的情况下，依然可以进行数据跨境的例外条件，如：以保护数据主体的生命为目的；以保护公共利益为目的;为履行法律义务，确保法定权利的正常行使；依据法定条件，将信息录入公共登记册，并根据立法和监管规定，信息所录入的登记册本身旨在供公众参考，且公开供公众咨询或由任何证明合法利益的人使用；履行数据控制者与数据主体之间的合同，或为响应数据主体的要求而采取的合同前措施;在数据控制者与第三方之间订立或履行合同，无论是为了数据主体的利益而订立或将要订立的合同。

02 法国《国家安全与防务白皮书》[1]

（1）定位

白皮书是法国发布其国家安全和军事战略的重要途径。1994 年,为适应国际战略形势的变化,法国发布了冷战后的第一部国防白皮书。时隔十余年后,法国对国际安全战略形势做出了新的判断。2008 年 6 月 17 日,法国政府正式发表《国家安全与防务白皮书》。这是一份反映法国国家安全战略和军事战略发展的重要文件。该白皮书对冷战后尤其是 21 世纪的世界形势做出了新的判断,并在此基础上提出了法国主要国家安全战略,明确了法国的欧洲防务政策和北约政策,并确定法国国防发展的方向和原则。

（2）特点

《法国国防与国家安全白皮书》首次将网络安全提升到国家安全的层面，把网络信息攻击视为未来 15 年最大的威胁之一，强调法国应具备有效的信息防卫能力，对网络攻击进行侦查、反击，并研发高水平的网络安全产品。

（3）主要内容

白皮书提出要以更全面的眼光考察国家安全问题，以更全面的方式考虑法国的安全利益，而不是仅局限于防务问题。它将国家安全战略定义为旨在消除“所有可能对国家生存造成损害的危险和威胁”的战略。国家安全领域包括防务政策，但并不局限于此。国家的其他政策，如对外政策和经济政策也将直接服务于国家安全。

03 法国《信息系统防御与安全：法国战略》

（1）定位

2008 年发布的《国防和国家安全白皮书》（简称“《白皮书》”）认为,未来十五年间，法国面临的威胁主要源于针对国家信息基础设施的大规模黑客攻击。这一判断促使法国政府做出大幅加强国家网络防御能力的决定。2009 年成立的国家信息系统安全局(ANSSI)正是履行该承诺的第一步。

该文件（于2011年2月颁发）中陈述的信息系统防御和安全方面的国家战略,正好体现了《白皮书》中蕴含的雄心壮志，该文件也是基于《白皮书》的落实和延伸。

（2）特点

战略明确四个战略目标：成为网络防御的世界级强国；通过保护主权信息，确保法国决策自由；加强国家关键基础设施的网络安全；确保网络空间安全。

（3）主要内容

战略提出七项基本工作:提前准备并分析环境,以便做出合理决定;检测并阻止攻击,警告并实时监控可能的受害者;提高和保持科研、技术、工业和人力资源能力，以便维持必要的自主性;保护国家信息系统和关键基础设施运营商,以便获得更好的国家抗击强度;修订法律以适应技术变革和新用途层出不穷的趋势;在信息系统安全、打击网络犯罪和网络防御等方面开展国际合作，以便更好地保护国家信息系统;沟通、告知和说服,以便法国人能够采取措施应对与信息系统安全相关的挑战。

04 法国《法国国家数字安全战略》[2]

（1）定位

2015年10月19日，法国总理ManuelValls亲自签署并发布新版《法国国家数字安全战略》（FrenchNationalDigitalSecurityStrategy），该《战略》反映了当前和未来法国对网络空间和数字安全的核心主张和总体安排。《法国国家数字安全战略》是法国数字转型时期的一个重要标杆性战略，体现出法国将数字安全作为保障和推动国家经济、政治和社会发展的关键战略布局。该《战略》不仅契合了法国和欧盟的重大现实需要，也对全球各国的网络安全和信息化发展具有良好的借鉴意义。

（2）特点

《战略》强调法国应当发展必要的科学技术和产业能力，保护信息主

权和数字安全，尤其应当在数字安全领域实现自主发展，并在国际舞台上获得更大影响力。具体举措包括通过产业政策和政府采购推动法国和欧洲安全产品和服务的发展，加大法国数字产品和服务的国际宣传力度，推动法国和欧盟作为该领域产品不可或缺的全球利益相关者脱颖而出，在网络空间青少年意识教育和保护妇女儿童方面成为国际标杆，推动《布达佩斯网络犯罪公约》的发展进程和全球适用，加强法国在国际网络安全讨论中的参与度和影响力，协助欧盟以及其他国家建立网络安全能力，促进全球网络空间的稳定。

（3）主要内容

该《战略》目标锁定了五大领域，这五个领域的主线分别是涉及法国国家根本利益相关的关键基础设施和重要信息系统安全；与法国核心价值观直接相关的言论自由、数据安全与隐私保护；法国数字安全的素养和教育，法国数字安全技术和产业发展；以及法国数字安全在欧盟和国际上的布局。虽然五大领域涉及面广，但是《战略》内容具体务实，不仅有理念性和原则性战略方向，还对应了具体的计划、方法、项目和实施主体，且保持了与之前相关战略、政策、法律的延续性，具有较强的指导性和可操作性。

05 法国《网络防御战略评论》[3]

（1）定位

2018 年 2 月，法国国防和国家安全总秘书处（SGDSN）发布《网络防御战略评论》（Revue strategique de Cyberdefense），该报告提出法国网络防御模式，分析其特点，提出六项任务及网络防御的四大操作链。

（2）特点

该文件明确提出“数字主权”是国家主权的组成部分。该报告针对全球互联网巨头大量非法占有、垄断数据财富正式提出“数字主权”概念，称数字主权是国家主权的重要组成部分,是法国维护网络安全,保护其自主

决策和行动能力的重要保障。报告指出,面对不断增长的社会数字化产生的新威胁,法国必须维护其行使主权的权利。

（3）主要内容

法国的网络防御模式将进攻能力和防御能力区分开来，通过将网络保护的任务和手段与情报和进攻行动的目标区分开来，加强国家对政府和经济领域的信息系统安全的干预，重点领域分工，尊重个人隐私，允许私人行为者与负责网络保护的国家服务之间建立信任关系。法国网络防御模式共有六项任务，包括预防、预测、保护、监测、归因、应急响应（补救措施、犯罪惩罚及军事行动）。

06 法国《个人数据保护法》[4]

（1）定位

法国《个人数据保护法》于 2018 年 11 月 7 日生效，该法案系法国落实欧盟《通用数据保护条例》的立法举措，目的在于保护公民的个人数据信息安全。

（2）特点

为避免个人信息数据被滥用，该法扩展了数据控制者和运营商的审查义务，数据控制者和运营商除要遵守“避风港规则”外，还应对特定文件作备案登记，对数据使用人的高风险活动进行事前审查，对重要的数据信息作加密处理等。此外，如数据控制者和使用者系为了社会公共利益而使用数据信息的，相关部门可另行制定规定，明确合理使用的范围。

（3）主要内容

该法提出，满足以下条件时，个人数据的控制者可以传输数据到非欧盟国家：适用于为预防、调查、侦查或起诉刑事犯罪或执行刑事处罚而进行的个人数据处理；如果个人数据来自另一个国家，且传输数据的国家已根据其国内数据相关法律法规的有效授权进行数据传输；一项具有法律约束力的文书，证明为个人数据的保护提供了保障；或者没有此类决定或文

书的情况下，数据控制者已评估数据转移的所有情况，并认为存在有效的保障措施。

07 法国《数据保护法》[5]

（1）定位

2018 年 12 月 12 日，法国政府通过法令通过了新版本的法国《数据保护法》。作为提醒，法国立法者已授权法国政府通过法令进行立法，以实现法国数据保护法与 GDPR 之间相互衔接的周延性。该法律是建立在《信息技术与自由法案》的基础之上。[6]

（2）特点

该法案新版本的可读性有了明显的提升，并针对数据处理的不同操作场景作出规定，比如 GDPR 规定情况下的处理，用于预防、调查、侦查或起诉刑事犯罪或执行刑事处罚的处理，有助于国防或国家安全的处理等。该法案还规定了适用于所有数据处理操作的共同规定。

（3）主要内容

该法案明确了数据合法跨境的法定情形：（a）公安机关和其他行使公共职权的机关、单位（以下简称：主管机关）对犯罪行为的侦查、侦查、起诉、执行刑事处罚，包括防范、预防危害公共安全的威胁。为实现上述目的，必须转让该数据。（b）个人数据转移给在该非欧盟国家设立的财务总监，或在法国移交给主管机关，该主管机关是根据（a）条款受托执行的目的。（c）如果个人数据来自另一国家，只有在获得数据的国家根据其国内法授权转让后才应进行转让。但是，如果不能及时获得事先授权，在为防止对另一国家的公共安全造成直接和严重的威胁或维护法国的基本利益有必要进行新的转移时，未经转移数据的国家的事先授权，可以再次转移个人数据。但在该等情况下数据转移主体需要毫不拖延地通知负责给予事先授权的当局。（d）如果在具有法律约束力的文书中提供了有关保护个人数据的适当保障措施，或在控制人评估了有关数据转移的所有情

况后，认为在保障个人资料方面存在适当的保障措施，控制人可以转让个人数据或授权转让已经传输给非欧盟国家的数据。

三、参考文献

[1]原颖,侯振杰.法国《国家安全与防务白皮书》简析[J].外国军事学术,2008,0(9):13-15

[2]惠志斌.《法国国家数字安全战略》述评[J].信息安全与通信保密,2016(12):67-75.

[3]卢英佳.法国网络空间安全治理体系[J].电子技术与软件工程,2019(10):209-210.

[4]詹 紫 旋.法国加强信息保护制定《个人数据保护法》[EB/OL].(2019-07-22)[2022-05-18].http://www.shfzb.com.cn/images/2019-01/09/B06/B060109.pdf.

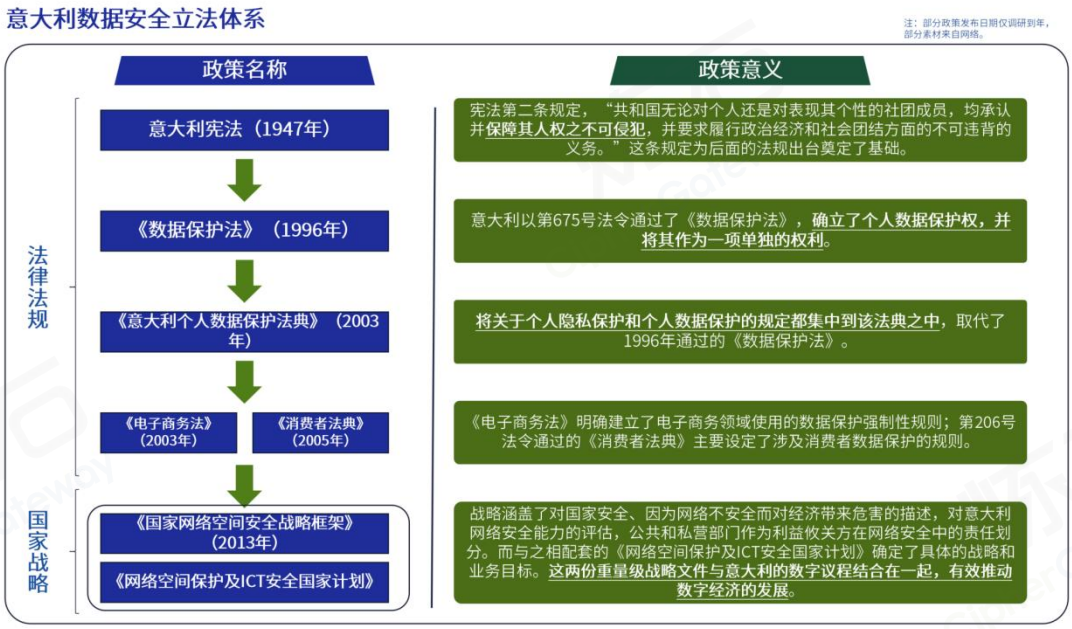
[5]法国数据保护法[EB/OL]. https://www.dataguidance.com/sites/default/files/france_data_protection_act.pdf

[6]法国数据保护法[EB/OL]. https://www.fieldfisher.com/en/services/privacy-security-and-information/privacy-security-and-information-law-blog/french-legislator-amends-french-data-protection-act

意大利：隐私成为“电子公民身份”的基本组成

一、立法总体情况

意大利对个人数据保护源于早期的隐私权概念，并上升到了人权高度。意大利 1947 年宪法第二条规定，“共和国无论对个人还是对表现其个性的社团成员，均承认并保障其人权之不可侵犯，并要求履行政治经济和社会团结方面的不可违背的义务。”在意大利宪法的基础上，1996 年，意大利以第 675 号法令通过了《数据保护法》，将隐私保护视为更大整体的一部分,即：个人数据的处理应“尊重自然人的权利，基本自由和尊严，特别是在隐私和个人身份方面”。因此，隐私成为“电子公民身份”的一个基本组成部分。



2003 年，在意大利宪法和《数据保护法》等法律法规的基础上，国会制定通过了《意大利个人数据保护法典》。提出了“每个人都有权保护与自己有关的个人数据”的个人数据保护基本原则，以及“确保在处理个人数据时尊重数据主体的权利、基本自由和尊严，特别是在保密、个人身份和个人数据保护权方面”的法规义务。后面的《电子商务法》和《消费者法典》则是适应于不同场景的个人数据保护。

国家战略方面，2013 年，意大利发布了《国家网络空间安全战略框架》（National Strategic Framework for Cyberspace Security）。战略涵盖了对国家安全、因为网络安全问题而对经济带来危害的描述，对意大利网络安全能力的评估，公共和私营部门作为利益相关方在网络安全中的责任划分。而与之相配套的《网络空间保护及 ICT 安全国家计划》确定了具体的战略和业务目标。这两份重量级战略文件与意大利的数字议程结合在一起，有效推动了该国的数字经济发展。

二、 重点法律解析

01 意大利《共和国宪法》

（1）定位

意大利共和国宪法是在 1947 年 12 月 22 日的制宪会议大会上通过的。宪法是国家的根本大法，是特定社会政治经济和思想文化条件综合作用的产物，它集中反映各种政治力量的实际对比关系，确认革命胜利成果和现实的民主政治，规定国家的根本任务和根本制度，即社会制度、国家制度的原则和国家政权的组织以及公民的基本权利义务等内容。

（2）特点

1947 年宪法第二条规定：“共和国承认并保障人类不可侵犯的权利，不管是作为个体还是作为在发展其人格的社会结构中，并且要求履行在政治、经济和社会共同体中不可推卸的义务。”这是意大利早期的“人权”。随后，在该法所确立的“人权”基础上，进一步衍生出“隐私权”，并进而产生了“个人数据保护”的概念。

（3）主要内容

该宪法指出：意大利是以劳动为基础的民主共和国，其主权属于人民，人民在宪法所规定的形式和范围内行使主权；共和国无论对个人还是对表现其个性的社团成员，均承认并保障其人权之不可侵犯，并履行其在政治经济和社会团结方面的不可违背的义务。

02 意大利《数据保护法》[1]

（1）定位

1996 年，意大利以第 675 号法令通过了《数据保护法》，确立了个人数据保护权，并将其作为一项单独的法定权利。

（2）特点

意大利数据保护法（1996 年 12 月 31 日第 675 号）提出个人数据的处理应“尊重自然人的权利，基本自由和尊严，特别是在隐私和个人身份方面”。因此，隐私成为“电子公民身份”的一个基本组成部分。

（3）主要内容

意大利《数据保护法》指出，正在被处理的个人数据应受到保存和控制，同时也考虑到其性质和处理的具体特征，通过适当的安全措施，将其破坏或丢失（即使是偶然的）未经授权访问数据或被非法处理或以与数据不一致的方式处理的风险降至最低。此外，该法规也指出了个人信息处理的基本原则：合法和公平地处理;出于特定、明确和合法的目的收集和记录，并以不与所述目的相抵触的方式用于进一步的处理操作;准确无误，并在必要时保持最新状态;与收集或随后处理的目的有关且不超过法定的限度;以允许识别数据主体的形式保存的时间不超过收集或随后处理数据的目的所需的时间。

03 意大利《个人数据保护法典》

（1）定位

进入二十世纪以来，为了落实欧盟数据保护规则改革，意大利也迅速做出立法调整。2003 年，国会制定通过了《个人数据保护法典》，将关于个人隐私保护和个人数据保护的规定都集中到该法典之中。随着情势的变更，该法典也在不断地修正完善。

（2）特点

该法典提出“每个人都有权保护与自己有关的个人数据”的个人数据保护基本原则，以及“确保在处理个人数据时尊重数据主体的权利、基本自由和尊严，特别是在保密、个人身份和个人数据保护权方面”的法规基本目的。

该法案提出了最小化原则：信息系统和软件应该最小化配置个人数据的使用和识别,基于数据处理方式,如果个人数据处理需求通过使用匿名数据或合适的安排可以实现，则“允许识别数据对象”的数据处理模式只应在必要的情况下使用。

（3）主要内容

法典提出，在以下情况中个人数据可以合法的跨境传输：1）数据主体已明确同意，如果涉及敏感数据，需以书面形式表示同意；2）如果传输对于数据处理者而言是作为合同主体的一方履行其合同义务所必须的，或者在签订合同之前应个人数据主体之要求而采取措施，或为了签订或履行以个人数据主体的利益而签订的合同；3）数据传输对维护法律或法规所提及的重大公共利益是必要的；4）如果数据传输对于保护第三方的生命健康是必要的。如果此目的涉及特定个人数据主体，且该特定个人数据主体无法授权同意，则可以由能够合法代理数据主体的实体或直系亲属、家庭成员，与数据主体同住的人，或者其他相关人代为授权同意；5）如果数据传输对辩护律师进行调查是必要的，或者是为了确立或辩护法律索赔（前提是该数据仅为上述目的而转移，并且不超过适用于商业和工业保密的现行立法所需的时间）；6）如果数据传输是应查阅行政记录或公开提供的登记册、清单、记录或文件所载信息的请求而进行的，则按照适用于这一标的物的规定进行；7）如果数据传输是必要的，比如完全出于科学或统计目的、或仅用于历史目的等；8）如果数据传输涉及到法人、机构或协会相关的数据。

04 意大利《电子商务法》

（1）定位

2003 年第 70 号法令通过的《电子商务法》，目的是制定电子商务框架，明确建立了电子商务领域使用的数据保护强制性规则。

（2）特点

法令第 16 条免除了“信息侵权”的赔偿责任，条件是提供者：1）“不了解活动或信息是非法的，并且，关于损害赔偿诉讼，不了解使活动或信息的非法性显而易见的事实或情况;2）立即采取行动，在与主管当局进行适当沟通且知道此类事实后，立即删除信息，或禁止访问此类信息”。[3]

（3）主要内容

法令指出，供应商必须以清晰、可理解和明确的方式通知其他各方如何保留和存档合同。在向消费者发送合同摘要之前，供应商必须向他们提供此信息。上述合约应以持久格式存储。此外，法令指出，为了使“点击包装”合同有效，提供商必须发送交易相关信息供消费者确认，包括：适用于合同的一般和具体条件的摘要;所提供商品或服务的主要特征的详细信息;有关价格，付款方式，交付成本，税收以及消费者悔改和撤回的权利的详细信息，包括行使这些权利的条款和条件。[4]

05 意大利《消费者法典》

（1）定位

2005 年第 206 号法令通过的《消费者法典》，是保护消费者和用户权利的基本参考法律。

（2）特点

该法典主要设定了涉及消费者数据保护的规则，反应了欧盟计划的指导方针。

（3）主要内容

法典提出通过提高消费者的权益意识(教育和消费者信息)来加强对消

费者和用户的保护，并促进协会关系和集体行动工具的发展，进而提高消费者的法律地位(个人和集体层面)。

06 意大利《国家网络空间安全战略框架》

（1）定位

2013 年，意大利发布了《国家网络空间安全战略框架》（National Strategic Framework for Cyberspace Security）。战略涵盖了对国家安全、因为网络安全问题而对经济带来危害的描述，对意大利网络安全能力的评估，公共和私营部门作为利益相关方在网络安全中的责任划分。

（2）特点

目前的《国家网络安全战略框架》强调了网络威胁的性质和不断演变的趋势，以及国家 ICT 网络的脆弱性。它概述了参与网络安全的公共和私人利益攸关方的角色和任务，并确定了工具和程序，以加强国家应对网络空间带来的新挑战的准备。

（3）主要内容

该战略提出了加强国家网络防御能力的六大指导方针：1）增强所有与网络安全相关的机构的技术、运营和分析能力，以利用国家能力对多维度网络威胁进行分析、预防、缓解和有效应对;2）加强保护关键基础设施和战略资产免受网络攻击的能力，同时确保其业务连续性并完全符合国际要求、安全标准和协议；3）促进旨在积极推动保护国家知识产权和技术创新的所有公私伙伴关系;4）在公民和机构中推广安全文化，同时利用学术界的专业知识，提高用户对网络威胁的认识;5）加强有效抑制网络犯罪活动的能力，符合国家和国际规范;6）全力支持网络安全领域的国际合作，特别关注意大利作为其成员的国际组织及其盟国正在进行的举措。

三、参考文献

[1]意大利数据保护法[EB/OL]. https://www.privacy.it/archivio/legge675encoord.html

[2]意大利个人数据保护法典[EB/OL].https://www.privacy.it/archivio/privacycode-en.html

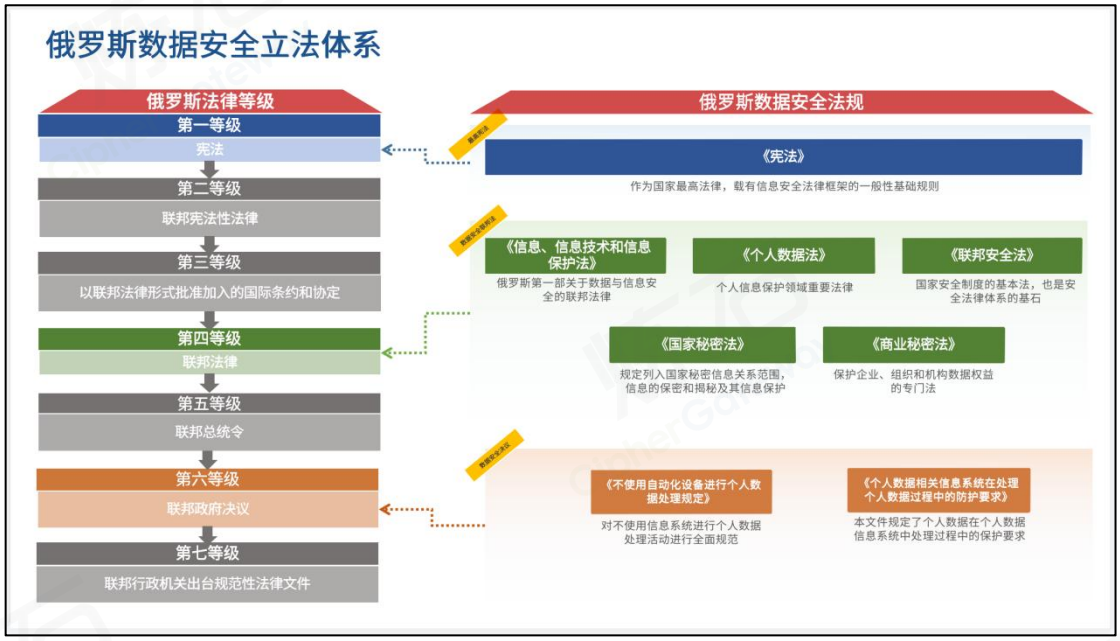
[3]意大利电子商务法[EB/OL].https://www.cyberlaws.it/en/2019/hosting-provider-active-role-and-liability/

[4]意大利电子商务法[EB/OL].https://www.lexology.com/library/detail.aspx?g=7d737068-0ffb-48fe-b2b2-83da1c3fe360

俄罗斯：法规和战略双重落实数据安全保护

一、立法总体情况

俄罗斯数据与信息安全法规体系是以《俄罗斯联邦宪法》为基础的统一立法。1995 年 2 月颁布的《关于信息、信息化与信息保护法》首次提及公民个人信息，并予以法律保护，至 2006 年 7 月才正式颁布《个人数据法》，联合《国家秘密法》《俄罗斯联邦安全法》和《商业秘密法》等法规构建起数据与信息安全法律制度体系。



俄罗斯国家数据安全制度体现在四个重要方面：信息安全贯穿俄罗斯国家数据安全始终，个人数据安全突出俄罗斯国家数据安全特点，网络数据安全凸显网络安全与国家安全的密切关系，商业数据安全凸显国家经济安全[1]。

二、重点法律解析

01《俄罗斯联邦宪法》

（1）定位

《俄罗斯联邦宪法》颁布时间为 1993 年 12 月 12 日，作为国家最高法律，载有信息安全法律框架的一般性基础规则，即信息关系主体法律地

位的关键要素[2]。

（2）特点

《宪法》确立隐私权属于公民宪法权利。人人享有私生活不可侵犯、个人及家庭秘密、保护自己的名誉和名声的权利，“非经同意不允许收集、保管、使用和传播个人的私生活信息”。

（3）主要内容

《俄罗斯联邦宪法》共分为九章 137 条，第一章为宪法根本制度、第二章为人和公民的权利和自由、第三章为联邦体制、第四章为俄罗斯联邦总统、第五章为联邦会议、俄罗斯联邦政府、第七章司法权、第八章为地方自治、第九为宪法的修改和重新审议。

02 俄罗斯《信息、信息技术和信息保护法》

（1）定位

《信息、信息技术和信息保护法》颁布时间为 2006 年（修订前名称为《信息、信息化和信息保护法》），是俄罗斯第一部关于数据与信息安全的联邦法律，也是俄罗斯互联网网络安全和数据安全领域的重要立法。

（2）特点

1）本地化数据存储。互联网信息运营者需要在产生、传播和处理数据的 6 个月内，将相关主体信息存储到俄罗斯境内，包括文字、语音、图像等信息。

2）信息可作为资产。信息资源是财产的组成部分和所有权的客体，明确了信息可为资产，其主体可以是公民、国家机关、地方自治机关或者机构及社会团体。

3）信息拥有者、信息系统运营者需要承担的信息保护义务。数据处理许可及告知制度进行了规定：“非国家机构和私人从事有关个人资料处理和向使用者提供个人资料的活动应经过必需的特许（申请许可证，申领

执照）。”

（3）主要内容

2006 年《关于信息、信息技术和信息保护法》由俄罗斯联邦议会审议通过，该法主要规定了整个信息立法系统的准则，以及包括信息安全的立法保护，调整了相关主体在进行寻找、获得、传递、生产和传播信息以及使用信息技术和进行信息保护时产生的法律关系，旨在保护公民免受恶意信息侵害的要求，并规定搜索引擎应排除在俄罗斯境内发布该国所禁止的信息的网络链接。俄罗斯可通过打造域名系统、自主地址解析系统、可信路由节点等措施，实现俄罗斯互联网和本国数据的自主可控，减少对境外网络的依赖。

03《俄罗斯联邦个人数据法》

（1）定位

《俄罗斯联邦个人数据法》颁布时间为 2006 年 7 月 27 日，是个人信息保护领域重要法律，也是数据与信息安全法律制度体系中主要法律准则。

（2）特点

1）个人信息匿名化处理条件。个人信息的匿名化只能在获得个人同意的情况下进行，或者在俄罗斯联邦法律在个人数据领域中规定的其他情况下才能进行。

2）强化数据安全，保护数据主权。在跨境数据流动方面，实行严格管控制度，推行数据本地化制度其中包括隐私保护、维护网络安全、便利执法等具体监管目标，并且要求开始跨境传输个人数据之前，处理者有义务确保在个人数据传输到的外国国家对个人数据主体的权利提供充分的保护。

（3）主要内容

2020 年 12 月 10 日，俄罗斯联邦会议国家杜马发布《俄罗斯联邦个人数据法》修正案，进一步明确公共个人数据处理规则，旨在建立保护个人数据主体权利和自由的机制。

04《俄罗斯联邦安全法》

（1）定位

《俄罗斯联邦安全法》颁布时间为 1992 年，是国家安全制度的基本法，也是安全法律体系的基石。

（2）特点

1）合规监管齐推进。俄罗斯联邦主体的国家机关和地方政府在其职权范围内确保俄罗斯联邦在安全领域的立法的实施。

2）组建安全理事会。审议俄罗斯联邦与外国的安全、国防组织、军事建设、国防生产、军事技术合作以及其他与俄罗斯宪法秩序、主权、独立和领土完整有关的问题联合会，以及安全领域的国际合作问题。

（3）主要内容

《俄联邦安全法》分四章，共 20 条，第一章是总则部分，明确指出安全法适用于国家安全、公共安全、生态安全、人员安全、法律规定的其他安全活动的内涵和基本原则，确定了俄罗斯联邦安全会议的地位、联邦和地方权力机构的职能，第二章规定了国家权力机关、联邦主体权力机关、自治地方和其他权力机关的职能和权限，第三章明确了安全会议的地位、性质、任务、职能、成员、书记、活动组织、决议，第四章规定了该法生效时间及相应失效的法律。

05 俄罗斯《商业秘密法》

（1）定位《商业秘密法》于 2004 年 7 月 29 日颁布，致力于保护企业、组织和机构数据权益。

（2）特点

1）国家秘密的数据信息应按照规定进行加密，根据其泄露后对俄罗斯国家安全造成的损害程度进行分级管理，接触和使用国家秘密信息的机构和组织应按要求，采取必要的防护措施以确保相关数据信息的安全。

2）从事涉密信息保护手段/工具研发的企业，应具备相关资质。

3）企业、机构和组织取得相应的涉密信息使用许可证后，方可申请和使用涉及国家秘密的相关数据信息，并在使用过程中按照信息的保密级别采取相应的保密措施。

（3）主要内容

《国家秘密法》规范了商业秘密所有者的权利义务。明确指出列为商业秘密的相关数据信息受法律保护，任何第三方未经授权不得随意访问。国家相关权力机关(包括公共机构)为履行职责需要获取此类信息，须出示相关主管机构负责人签署的正式文件，文件应说明数据使用的具体目的，以及其申请获取数据的法律依据。为确保涉及商业秘密的数据安全，该法规定，商业秘密所有者应根据《商业秘密法》及其他联邦法律规定，及时建立相应的商业秘密保护制度，编制构成商业秘密的信息清单，采取必要的技术保护手段和方法，并明确相关数据的访问、处理、存储、对外发布流程和条件。

06 俄罗斯《国家秘密法》

（1）定位

《国家秘密法》于 1993 年 7 月 21 日颁布。活动范围限制在军事、对外经济、侦察、反侦察和相关业务调查领域，进一步防止因国家机密保护活动可能对公民权限制的可能性[3]。

（2）特点

规定了受保护信息载体的法律监管措施，对涉密信息的载体管理作出

了明确规定，如：1）如果载体是由不同密级的信息文件资料组成的，其每部分都应盖有相应的密级印章（密别印），则整个载体要加盖与组成部分中最高密级相同的密级印章（密别印）；当不可能证明所获取（制定）的信息文件资料与现有清单中所包含的信息文件资料相符时，国家权力机关、企业、机构和组织中的负责人应当按照拟定密级对其预先进行保密；3）拥有国家秘密信息文件资料的国家权力机关、企业、机构和组织，当其职能和所有制形式发生改变时，以及当被清算或被终止从事使用国家秘密信息文件资料的工作时，应当采取措施保护这些信息文件资料及其载体；4）国家秘密信息文件资料的载体应当按规定程序予以销毁、上交存档或移交给法定的相应机构等。

（3）主要内容

俄罗斯苏维埃社会主义共和国最高委员会通过了《俄罗斯联邦国家秘密法》（1993 年 7 月 21 日第 5485－1 号），规定了列入国家秘密的信息关系范围，信息的保密和解密，信息保护，以及俄罗斯安全保障问题。在俄罗斯国家历史中，就有关国家安全相关信息的限制与保障问题，建立可以通过公开的法律标准来解决的途径。

07 俄罗斯《个人数据处理规定》

（1）定位

《不使用自动化设备进行个人数据处理规定》（简称：“个人信息处理规定”）于 2008 年 9 月 15 日颁布，其主旨在于为执行“个人数据”联邦法，在不使用自动化工具的情况下处理个人数据的特殊性规定。

（2）特点

1）在不使用自动化工具的情况下处理个人数据时确保个人数据安全的措施。2）对部分个人数据的销毁或去个性化，保持处理记录。

（3）主要内容

《规定》共计包含三章节，第一章节为一般规定，第二章节为不使用

自动化工具进行的个人数据处理组织的特点，第三章节为在不使用自动化工具的情况下处理个人数据时确保个人数据安全的措施，对不使用信息系统进行个人数据处理活动进行全面规范。

08 俄罗斯《个人数据处理防护要求》

（1）定位

《个人数据相关信息系统在处理个人数据过程中的防护要求》(简称：《个人数据处理防护要求》）于 2012 年 11 月 1 日颁布，本文件规定了个人数据在个人数据信息系统（以下简称信息系统）中的个人数据处理过程保护要求及保护级别。

（2）特点

1）个人数据保护系统应考虑因技术安全威胁而确定的组织和（或）技术措施。2）实行分类分级保护，在信息系统中处理个人数据时，建立了 4 个级别的个人数据保护。

（3）主要内容

对个人数据存储系统进行分级并对其安全防护措施进行规范。

三、参考文献

[1]张涛,张莹秋.俄罗斯国家数据安全治理的机制建设[J].俄罗斯学刊,2022,12(02):48-66.

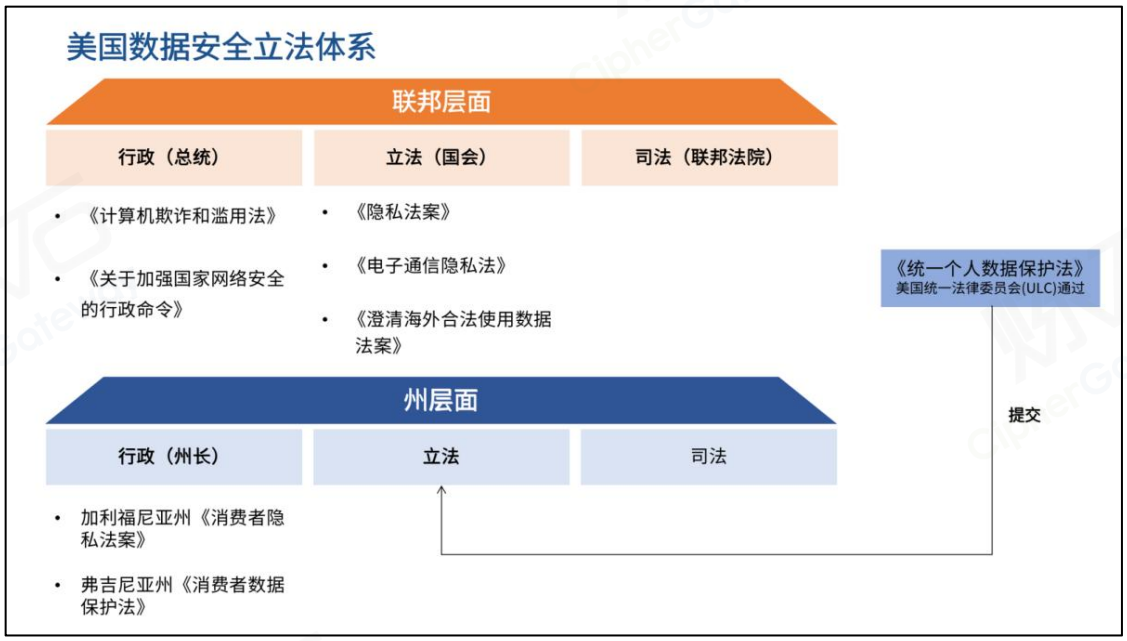
[2]孙祁.俄罗斯强化数据主权保护[EB/OL].http://www.scicat.cn/new/20210627/5427293.html.

[3]制度开门.苏联克格勃没了，俄罗斯如何定义“境外敌对势力”和“国家机密”[EB/OL].https://www.163.com/dy/article/E58MA0VD0521AU53.html.

美国：坚持市场主导和行业自治

一、立法总体情况

美国是世界上最早提出隐私权并予以法律保护的国家之一，政府长期秉持数据开放和数据自由流动相结合的数据治理理念，持以市场为主导、以行业自治为主要手段，但至今仍没有出台全面的联邦数据隐私法。就层级而言，美国在从联邦到州地方各级政府都实行三权分立的基础上，同时实行联邦和州两个层次之间的纵向分权，立法也更加分散多元化。



联邦层面上，1986 年《计算机欺诈和滥用法》、2021 年《关于加强国家网络安全的行政命令》是由总统签署发布，聚焦于网络安全的保护；1974 年《隐私法案》、1986 年《电子通信隐私法》、2018 年《澄清海外

合法使用数据法案》是经由国会通过，针对个人信息和隐私的保护。

州层面上，由州长签署发布的2018年加利福尼亚州《消费者隐私法案》、2021年弗吉尼亚州《消费者数据保护法》，作为专门针对加州消费者的隐私保护法律，对其他州的立法进程具有重要标杆作用和参考价值。

二、重点法律解析

01 美国《隐私法案》

（1）定位

1974年12月，美国国会通过《隐私法案》，该部立法是美国为保护公民隐私权和知情权出台的重要法律，旨在平衡政府保有个人信息需求和个人隐私权保护之间的利益分歧，以保障公民免受联邦机构收集、维护、使用和披露有关个人个人信息，无端侵犯其隐私的权利。

之后，《隐私法案》也经过多次修订：

1988年，美国制定了《计算机匹配和隐私法》，之后被并入了《隐私法案》；

1990年，美国国会颁布了《计算机匹配和隐私保护修正案》，进一步澄清了相关正当程序规定；

2020年，由美国司法部隐私和公民自由办公室（OPCL）编写了《1974年隐私法概述》是对《隐私法》各项条款的讨论，为解释该法案的法院判决提供了参考和法律分析。

（2）特点

《隐私法案》针对联邦行政部门收集、利用和保护个人数据等方面做出规定，适用于美国公民和在美国取得永久居留权的外国人。

（3）主要内容

《隐私法案》明确了信息主体的主要权利、政府机构的主要义务以及民事救济措施等内容，对政府机构应当如何收集个人信息、什么内容的个

人信息能够储存、收集到的个人信息如何向公众开放及信息主体的权利等都做出了比较详细的规定。

《隐私法案》侧重于四个基本政策目标：限制披露各机构保存的个人信息记录，赋予个人更多访问机构保存记录的权利，授予个人修改信息记录的权利，要求政府机构遵守收集、维护和公开记录的法定规范。

02 美国《电子通信隐私法》

（1）定位

1986 年，美国国会制定了《电子通信隐私法》(Electronic Communications Privacy Act of 1986，ECPA)，旨在延伸原先在电话有线监听方面的规制，包含通过计算机的电子数据传输。

（2）特点

《电子通信隐私法》详细规定了执法机关访问电子通信和相关数据的标准，不仅针对动态传输的有线、口头与电子通信保护作出了具体规定，还规范了对静态存储的电子通信的安全保障要求，协调国家安全与个人隐私、通信秘密保障之间的冲突[1]。

（3）主要内容

《电子通信隐私法》包括“笔式记录器法”(Pen Register Act)、“窃听法”(Wiretap Act)、“存储通讯法”(Stored Communications Act)三个主要章节。“笔式记录器法”针对执法机关利用笔式记录器或类似的追踪记录设备，记录或解码由传输有线或电子通信的仪器或设施传输的拨号、路由、寻址或信令信息的设备或过程，但该等信息不包括任何通信的内容；“窃听法”管理实时性拦截通过线路进行传输的通讯，并将范围扩大到电子通信；“存储通讯法”涉及对存储的有线和电子通信或账户记录的访问和披露，特别的是这部分首次界定了“电子储存”的概念。

03 美国《计算机欺诈和滥用法》

（1）定位

1986 年 10 月 16 日，由美国总统 R.里根(Ronald Reagan)签署《计算机欺诈和滥用法》(Computer Fraud and Abuse Act，CFAA)，是美国第一部专门针对计算机犯罪的联邦法律，被认为是惩治黑客攻击计算机网络犯罪的里程碑。

由于当时法案限定范围窄、具有局限性，此后经历了 1988 年、1989 年、1990 年、1994 年、1996 年、2008 年，共六次修订。随着逐步修订，法案的规制范围越来越细密、合理，于 2000 年被正式编入《美国法典》。2022 年 5 月，美国司法部再次修订了《计算机欺诈和滥用法》，该法案首次指示不应起诉善意的安全研究人员。

（2）特点

《计算机欺诈和滥用法》鼓励研究者出于公共利益去根除漏洞，为善意的安全研究人员提供明确的规定以促进网络安全的发展。

（3）主要内容

《计算机欺诈和滥用法》列举了获取国家安全信息、泄露机密、侵入政府电脑、获取欺诈和获取价值、损坏计算机或信息、贩卖密码、威胁要损坏计算机七类犯罪活动，以及“侵入计算机的局外人”、“超出其授权范围的入侵者”两种违法情形。

04 美国《澄清海外合法使用数据法案》

（1）定位

2018 年 3 月 23 日，美国国会通过了《澄清境外合法使用数据法案》(简称《云法案》，打破了以往跨国数据类证据调取过程中遵循的数据属地管辖模式，构建了一套全新的以数据控制者实际数据控制权限为衡量依据的标准框架。

（2）特点

《云法案》单方面赋予美国政府对全球绝大多数互联网数据的“长臂管辖权”,有关人士指出，这是美国政府对他国数据主权的挑衅，不仅侵犯个人隐私，而且与多国立法存在冲突，威胁到跨国企业的互利合作[2]。

（3）主要内容

《云法案》主要规定包括：美国政府证据调取范围、明确服务提供者域外司法协助义务、服务提供者域外司法协助义务的例外、外国政府向美国企业请求获取数据的司法协助等。《云法案》提出，无论服务提供者的通信、记录或其他信息是否存储在美国境内，只要相关通信内容、记录或其他信息为该服务提供者拥有、控制或者监管，均应当按照法令要求，保存、备份、披露[3]。

05 美国加利福尼亚州《消费者隐私法案》

（1）定位

2018 年 6 月，美国加利福尼亚州州长签署公布《消费者隐私法案》（California Consumer Protection Act，CCPA），并于 2020 年 1 月 1 日生效。《消费者隐私法案》为消费者控制个人信息提供了合法途径，被认为是全美当前最严格的隐私立法。

（2）特点

尽管，《消费者隐私法案》是一部专门针对加州消费者的隐私保护法律，但加州的经济体量与科技创新实力居于世界领先，因此该部立法的意义深远超出其原本的立法层级，对其他州的立法进程起到重要标杆作用。

（3）主要内容

《消费者隐私法案》的主要内容包括法案出台的背景、消费者的权利、企业的义务以及法案中用语的详细解释四个部分。《消费者隐私法案》规定 ，一旦企业违反隐私保护要求，将面临支付给每位消费者最高 750 美元的赔偿金以及最高 7500 美元的罚款。

06 美国《关于加强国家网络安全的行政命令》

（1）定位

2021 年 5 月 12 日，美国总统拜登签署《关于加强国家网络安全的行政命令》（简称《行政命令》），旨在采用大胆举措提升美国政府网络安全现代化、软件供应链安全、事件检测和响应以及对威胁的整体抵御能力，是美国政府对 SolarWinds 供应链攻击、微软 Exchange 漏洞攻击，以及 Colonial Pipeline 输油管道等一连串备受瞩目的重大网络安全事件的响应[4]。

（2）特点

《行政命令》将预防、发现、评估和补救网络事件作为首要任务，并提出建立网络安全审查委员会，就影响联邦信息系统或非联邦系统的重大网络事件、威胁活动、漏洞等进行审核和评估。

（3）主要内容

行政命令包括九个部分的内容：政策、移除威胁信息共享的障碍、联邦政府网络安全现代化、增强软件供应链的安全、成立网络安全审查委员会、联邦政府网络安全漏洞和事件应急响应标准化、加强联邦政府网络中网络安全漏洞的检测能力、加强联邦政府网络安全事件的调查、修复能力、国家安全系统。

07 美国弗吉尼亚州《消费者数据保护法》

（1）定位

2021 年 3 月 2 日，美国弗吉尼亚州州长拉尔夫-诺森（Ralph Northam）签署了《消费者数据保护法》（Consumer Data Protection Act ,简称“CDPA”），于 2023 年 1 月 1 日生效。这一法案的出台，使得弗吉尼亚州成为美国第二个具备数据隐私立法的州。

（2）特点

《消费者数据保护法》参考借鉴了加州《消费者隐私法案》以及欧盟 G

DPR 的成果，在推进企业保护消费者数据隐私、赋予消费者相关权利等方面更为完善。

（3）主要内容

《消费者隐私法案》除了赋予消费者访问、更正、删除和获取个人数据副本的权利外，还明确消费者享有自由选择出售自身个人数据以及允许自身个人数据用于定向广告或分析决策的权利。

08 美国《统一个人数据保护法》

（1）定位

2021 年 8 月，美国统一法律委员会(ULC)投票通过了《统一个人数据保护法》（Uniform Personal Data Protection Act ，UPDPA)，这是一项旨在统一各州隐私立法的示范法案，于颁布之日起 180 日生效。

（2）特点

《统一个人数据保护法》基于数据实践有利于或不利于数据主体的可能性，对“兼容”、“不兼容”和“禁止”的数据实践作出区分；对假名数据提供宽泛的豁免。

（3）主要内容

《统一个人数据保护法》主要内容包括：适用范围，个人数据主体所持有的个人数据，个人数据主体的访问权和更正权，假名数据，兼容、不兼容和禁止的数据实践，收集控制者、第三方控制者和实践者的责任，自愿共识标准，执行和规则制定。该法适用于在该州范围内的由数据控制者或者数据处理者开展的活动，包括商务、生产产品或者是为本州居民提供服务。

三、参考文献

[1]徐海宁,詹伟杰,许多奇.《电子通信隐私法》[J]. 互联网金融法律评论,2016(2):190-213,2.

[2]太婉鸣. “功能+忠诚”视角下大数据时代立法文本的翻译--以美国《澄清境外数据合法使用法案》为例[D]. 北京:对外经济贸易大学,2019.

[3]田申.腾讯网络安全与犯罪研究基地.美国《澄清域外合法使用数据法案》分析[EB/OL].https://mp.weixin.qq.com/s/j7BhDknkeuhx-FOpmgO5Ug

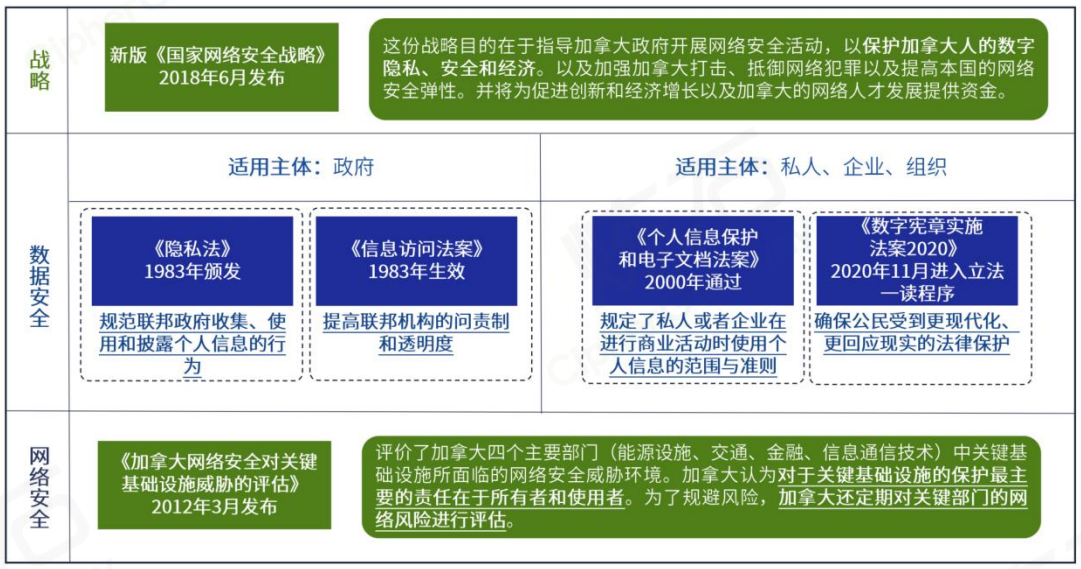
[4]重磅解读丨美国《关于加强国家网络安全的行政命令》[EB/OL].http://www.chinaaet.com/article/3000137516

加拿大：预防为主、综合治理数据安全问题

一、 立法总体情况

加拿大是世界上最早建成国家光纤网的国家之一，其电子政务建设多年处于全球领先地位。互联网的高度普及和服务的飞速发展使得加拿大拥有世界上高水平的互联网基础设施。互联网所引发的安全问题也使得加拿大成为世界上最早倡导保护互联网安全的国家之一。加拿大不但在国家战略和法律层面强调网络安全保护，更倡导政府部门之间的合作和互联网行业的自律，其在互联网治理方面呈现出预防为主综合治理的特点。

加拿大数据安全立法体系



国家战略方面，2018 年 6 月 12 日，加拿大公共安全部长拉尔夫·古德尔、国防部长哈尔吉特·萨詹及加拿大创新、科学与经济发展部部长纳夫迪普·贝恩斯共同发布了该国的新版国家网络安全战略，该战略作为加拿大在网络安全方面的路线图，旨在实现加拿大在安全方面的目标和优先事项。这份战略将指导加拿大政府开展网络安全活动，以保护加拿大人的数字隐私、安全和经济。该战略还将加强加拿大打击、抵御网络犯罪以及提高本国的网络安全弹性。

数据安全方面，加拿大最初的法律适用主体是政府。1983 年，加拿大

颁布《隐私法》，规范联邦政府收集、使用和披露个人信息的行为。《信息访问法案》于 1983 年 7 月 1 日生效，方案目的是提高联邦机构的问责制和透明度，以塑造一个开放和民主的社会，并对这些机构的行为进行合规监督。此外，加拿大后续又出台了以私人、企业、组织为适用主体的法律。2000 年，《个人信息保护和电子文档法案》（以下简称“PIPEDA”）通过，该法案规定了私人或者企业在进行商业活动时使用个人信息的范围与准则。2020 年 11 月 17 日，加拿大政府官网发布公告称，《数字宪章实施法案 2020》已进入加拿大下议院的立法程序。本法适用于个人信息相关的各类组织，比如该组织在商业活动中存在收集、使用或披露个人信息等。

网络安全方面，2012 年 3 月，加拿大发布了针对其安全情报服务的报告《加拿大网络安全对关键基础设施威胁的评估》，评价了加拿大四个主要部门（能源设施、交通、金融、信息通信技术）中关键基础设施所面临的网络安全威胁环境。该报告明确指出，实现充分全面的“态势感知”是业主/运营商面临的主要挑战，并表明减少相互依赖所产生的风险需要私营/公共部门采取协作的方法。

二、 重点法律解析

01 加拿大《隐私法》[1]

（1）定位

1983 年，加拿大颁布《隐私法》，规范联邦政府收集、使用和披露个人信息的行为，于 1983 年 7 月 1 日生效。目的是扩大加拿大现行法律的范围，这些法律保护个人对政府机构持有的关于他们自己的个人信息的隐私，并使个人有权访问该信息。

（2）特点

限制了政府收集信息的尺度：除非与该机构的运营计划或活动直接相关，否则政府机构不得收集任何个人信息，并规定了个人的知情权：政府机构应将收集信息的目的告知该机构所收集个人信息的任何相关个人信

息主体。限制了政府使用信息的尺度：未经相关个人的同意，政府机构不得使用政府机构控制下的个人信息。（除非是政府汇编信息或披露信息等“公共”目的）

（3）主要内容

本部分重点收集了该法关于个人信息定义的主要内容，具体如下：个人信息是指以任何形式记录的有关可识别个人的信息，包括但不限于前述规定的一般性：1）与个人的种族、民族或族裔、肤色、宗教、年龄或婚姻状况有关的信息；2） 与个人的教育或医疗、犯罪或就业历史有关的信息，或与该个人参与的金融交易有关的信息；3） 分配给个人的任何识别号码、符号或其他特定数字；4） 个人的住址、指纹或血型；5） 个人的个人意见或意见，除非是关于另一个人或关于政府机构或条例中规定的政府机构的一部分向另一人提出的补助金、奖励或奖品的提议；6） 个人向政府机构发出的暗示或明示属于私人或机密性质的信函，以及对可能揭示原始信函内容的此类信函的答复；7） 另一人对该个人的看法或意见；8） 另一人对（e）款所指的机构或机构一部分向该个人提出的补助金、奖励或奖品的提议的意见或意见，但不包括与另一个人的意见或意见一致的另一个人的姓名；9） 个人姓名与与该个人有关的其他个人信息一起出现，或者姓名本身的披露会泄露有关该个人的信息；10） 关于现在或曾经是政府机构官员或雇员的个人的信息，这些信息与该个人的职位或职能有关，包括：该人是或曾经是政府机构的高级职员或雇员，以及个人的职务、营业地址和电话号码等。

02 加拿大《信息访问法案》[2]

（1）定位

《信息访问法案》于 1983 年 7 月 1 日生效，方案目的是提高联邦机构的问责制和透明度，以塑造一个开放和民主的社会，并对这些机构的行为进行合规监督。

（2）特点

该法案为政府机构控制下的信息设定了访问权。该法体现了三个原则：政府信息应向公众提供；有权查阅的例外应有具体的限制；政府信息公开的决定应由独立于政府的他方审查。这样，个人信息主体对于政府控制的个人信息在访问权限和审查程序上都有了法律上的有力保障。

（3）主要内容

该方案提出，涉及到一些国际事务和国防的特殊情况，加拿大政府机构负责人可以拒绝披露本部分要求的任何记录，包括信息披露可能损害国际事务的行为、加拿大国防相关的信息等，包括但不限于以下内容：与军事战术或战略相关的，或与军事演习或行动相关的，或与侦测、预防或镇压敌对活动相关的；关于武器或其他国防设备（正在涉及、开发、生产或考虑作为武器）的任何相关事物的数量、特征、能力或部署；有关任何防卫机构、任何军事力量、单位或人员的基本信息；为有关的情报目的而获取或准备的数据；加拿大政府在审议、协商过程中，或在处理国际事务过程中，所使用的关于外国、国际组织或外国公民的相关信息；关于收集、评估或处理（d）条或（e）条所述信息，所采用的方法、技术设备等来源信息；关于加拿大政府、外国政府或国际组织，为目前或今后的国际谈判，所采取或即将采用的立场；与其他国家或组织进行的外交通信或与加拿大驻外大使馆进行的官方通信；与加拿大或其他国家使用的通信或密码系统有关的信息。

03 加拿大《个人信息保护和电子文档法案》[3]

（1）定位

2000 年，《个人信息保护和电子文档法案》（以下简称“PIPEDA”）通过，该法案规定了私人或者企业在进行商业活动时使用个人信息的范围与准则。

（2）特点

作为加拿大最主要的联邦法规之一，PIPEDA 是隐私权的立法保障。加拿大所有企业在从事商业活动的过程中收集、使用和披露个人信息时，均受到《个人信息保护和电子文档法案》制约。

（3）主要内容

该方案关于数据跨境方面，满足以下要求，则可以数据跨境（跨境部分来自于主观解读，具体详情请参照法规原文：有正在或可能就违反外国法律而进行或可能进行的调查或诉讼有关；有必要披露，以便从个人或机构获得有助理进行调查或审计的信息；信息的使用限制在最初共享信息的目的范围内；确保以保密方式处理有关资料，并未经同意，不得进一步披露；开展和发表与个人信息保护相关的研究；特定的用户，比如人员交流、分享知识和专长等。

04 加拿大《关键基础设施威胁评估》

（1）定位

2012 年 3 月，加拿大发布了针对其安全情报服务的报告《网络安全对关键基础设施威胁的评估》（简称：“关键基础设施威胁评估”），评价了加拿大四个主要部门（能源设施、交通、金融、信息通信技术）中关键基础设施所面临的网络安全威胁环境。加拿大认为对于关键基础设施的保护最主要的责任在于所有者和使用者。为了规避风险，加拿大还定期对关键部门的网络风险进行评估。

（2）特点

该报告明确指出，实现充分全面的“态势感知”是业主/运营商面临的主要挑战，并表明减少相互依赖所产生的风险需要私营/公共部门采取协作的方法。

（3）主要内容

报告主要指出，信息安全问题由于技术变革出现，但人们发现，解决这一问题不仅仅需要在技术/操作层面实现，也需要在国家层面采取更全面

的办法。信息安全问题的挑战在于保护整个以信息为基础的社会，而不是仅仅保护关键信息基础设施。因此，加拿大安全和情报部门需要更加重视针对政府和商业机密的网络攻击，阻止通过网络间谍窃取知识产权的非法行为。相关部门或组织应该以适当的方式承担相关的安全成本，确保安全事件发生的低概率，这不仅能够更好地维护相关部门或组织关于关键基础设施的商业利益，同时也造福于公众，从而增加他们对相关主体以及政府的信息。

05 加拿大《新版国家网络安全战略》[4]

（1）定位

2018 年 6 月 12 日，加拿大公共安全部长拉尔夫·古德尔、国防部长哈尔吉特·萨詹及加拿大创新、科学与经济发展部部长纳夫迪普·贝恩斯共同发布了该国的新版国家网络安全战略，该战略作为加拿大在网络安全方面的路线图，旨在实现加拿大人在安全方面的目标和优先事项。

（2）特点

这份战略将指导加拿大政府开展网络安全活动，以保护加拿大人民的数字隐私、安全和经济。该战略还将加强加拿大打击、抵御网络犯罪的执法力度，提高本国的网络安全弹性。加拿大新版国家网络安全战略将为促进创新和经济增长以及加拿大的网络人才发展提供资金。

（3）主要内容

该战略确定了加拿大政府的引导作用，并传达了加强与加拿大利益攸关方和伙伴合作的重要性。该战略包括许多举措，例如将政府的网络安全业务合并到由通信安全机构领导的加拿大网络安全中心的创建中，以及在 RCMP 内建立国家网络犯罪协调单位。

06 加拿大《数字宪章实施法案 2020》[5]

（1）定位

2020 年 11 月 17 日，加拿大政府官网发布公告称，由加拿大科技创新与经济发展部部长贝恩斯提议的《数字宪章实施法案 2020》已进入加拿大下议院的立法一读程序。本法适用于与个人信息相关的各个组织，如在商业活动中存在收集、使用或披露个人信息等情况的组织。

（2）特点

该法通过建立规则以保护个人对其个人信息的隐私权，并保障相关组织只能出于合理适当的目的去收集信息，并使用恰当的方式保护个人信息。该法案试图确保公民受到更现代化、更回应现实的法律保护，同时，在技术不断发展的背景下，也希望创新企业能从明确的规则中受益。提出了技术和防护目的的相称性：对个人信息进行去识别化的组织必须确保适用于该信息的任何技术和管理措施与信息去识别化的目的和个人信息的敏感性成比例。

（3）主要内容

该法案提出去标识化的定义，即：通过技术手段来修改个人信息或从个人信息中创建信息，以确保该信息不会被识别，或者在合理可预见的情况下无法单独使用或与其他信息结合使用来识别个人。此外，该方案提出了“组织问责制”，并规定，每个组织都必须施行隐私管理计划，主要包括基于个人信息的保护、接收和处理信息的索取和投诉、依法合规并组织人员培训、撰写组织为履行义务而制定的政策和程序材料。

三、参考文献

[1]加拿大隐私法[EB/OL].https://laws-lois.justice.gc.ca/eng/acts/P-21/page-1.html#h-397172

[2]加拿大信息访问法案[EB/OL].https://laws-lois.justice.gc.ca/eng/acts/A-1/page-5.html#docCont

[3]各国数据隐私与保护情况[J].中国信息安全,2020(08):56-59.

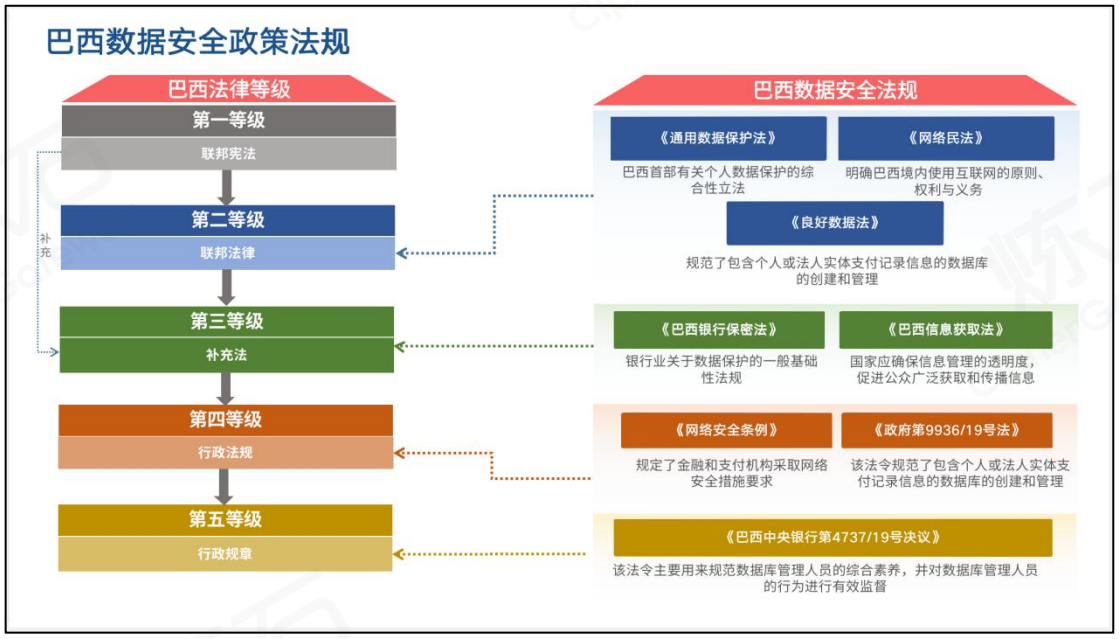
[4]加拿大公共安全部网站[EB/OL].https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx

[5]加拿大议会官方网站[EB/OL].https://www.parl.ca/DocumentViewer/en/43-2/bill/C-11/first-reading#:~:text=HOUSE%20OF%20COMMONS%20OF%20CANADA%20BILL%20C-11%20An,2020%20MINISTER%20OF%20INNOVATION%2C%20SCIENCE%20AND%20INDUSTRY%2090964

巴西：以宪法为核心，合规监管双发力

一、立法总体情况

巴西形成以《巴西联邦宪法》为中心，合规监管双发力的立法体系。《巴西联邦宪法》提出个人隐私权不可侵犯”的要求，成为数据安全立法基石，2018年《巴西通用数据保护法》颁布，形成巴西数据安全行政法规、规章法律框架，成为巴西的主要个人数据保护法律，围绕数据安全和个人信息保护，巴西颁布《巴西信息获取法》和《巴西网络民法》对规范互联网法律框架，对巴西公共信息获取提出保护要求。



经济是肌体，金融是血脉，巴西对于特定行业也有关于数据保护的法规，受巴西中央银行（BCB）监管的实体必须遵守《巴西银行保密法》和《巴西网络安

全条例》。根据《巴西银行保密法》，金融实体必须对“其所有的信贷和借记交易以及提供的服务”保密，《巴西良好数据法》《政府第 9936/19 号法令》《巴西中央银行第 4737/19 号决议》都共同规范了包含个人或法人实体支付记录信息的数据库的创建和管理，旨在建立信用记录。

二、重点法律解析

01 巴西《宪法》

（1）定位

巴西参议院全体会议于 2021 年 10 月 20 日批准了《宪法》修正提案 PEC 第 17/2019 号的文本，该提案已获众议院批准。PEC 第 17/2019 号修改了巴西联邦宪法，将保护个人数据列入基本权利和保障[2]。

（2）特点

巴西《宪法》确立了联邦在保护和处理个人数据方面的专属立法权。

（3）主要内容

巴西于 1988 年 10 月颁布的《宪法》不仅保护包括通信、电报、电话和数据通信保密性在内的隐私权，还涉及消费者保护。此次修正中，《宪法》第 5 条涉及个人和集体权利的修正案增加了一个新部分，指出“保护个人数据的权利，包括在数字媒体中的权利，是根据法律条款得到保障的。

02 巴西《通用数据保护法》（第 13709 号法律）

（1）定位

2018 年 8 月，《通用数据保护法》（LGPD）经巴西总统米歇尔·特梅尔的签署正式通过，自 2020 年 9 月起生效，对违规行为的处罚也在 2021 年 8 月生效。该法是对 2014 年 4 月 23 日第 12965 号法律《巴西互联网法》的修订。《通用数据保护法》受欧盟《通用数据保护条例》（GDPR）的极大影响，是巴西首部有关个人数据保护的综合性立法，显著增加了巴西个人数据保护的要求，

进一步提升了巴西的数据保护能力。同时，巴西根据该法成立了数据保护监管机构国家数据保护局。

（2）特点

LGPD 是一项综合性法律，就个人数据的收集、使用、处理和存储制定了详细的规则，它将覆盖巴西所有的经营行业，影响全部私营和公共实体，且无论个人数据的处理是否发生在数字和物理环境中[1]。在个人权益方面，用户群体将有权要求互联网服务提供者更正或排除其在运营过程中所收集的个人信息，并有权访问此类数据[2]。

（3）主要内容

《巴西通用数据保护法》共分为十章 65 条，包括基本规定、个人数据的处理、数据主体的权利、政府部门对个人数据的处理、数据跨境传输、个人数据处理代理人、数据安全和良好实践、监管、国家保护局和国家个人数据和隐私保护委员会，以及最终和过度条款等内容。

03 巴西《网络民法》

（1）定位

2014 年 4 月，巴西通过《网络民法》（Law No. 12965/2014），它明确了用户、企业和公共机构在巴西境内使用互联网的原则、权利与义务。2015 年 1 月，巴西司法部启动对《网络民法》部分条款的修正工作，对《网络民法》进行修正。2016 年 5 月 20 日，迪尔玛·罗塞夫总统签署了规范互联网法律框架的《网络民法》第 8771/2016 号联邦法令。

（2）特点

关于日志、个人数据和私人通信的保护，修订后的《网络民法》定义了“用户注册信息”，并确定行政当局在要求提供者提供用户注册信息时，必须说明其明确授权访问此类信息的法律依据，以及请求的动机。不收集用户注册信息的提供者应将此事实告知当局，并免除提供此信息的义务。此外，修订后的《网络民

法》特别关注数据隐私，为连接和应用程序提供商采用的日志、个人数据和私人通信建立安全和保密标准[4]。

（3）主要内容

修订后的《网络民法》共四个章节，主要包括一般规定、网络中立性、对记录个人资料和私人通讯的保护、监督和透明度等内容。

04 巴西《良好数据法》

（1）定位

《巴西良好数据法》颁布于 2011 年 6 月 9 日，规范了包含个人或法人实体支付记录信息的数据库的创建和管理，旨在建立信用记录。

（2）特点

账号注册人拥有免费访问数据库中个人及相关信息权利，经理有责任通过电话或其他方式维护安全系统。

处理个人数据过程中，提前告知存储、数据库管理员的身份、处理个人数据的目的以及共享时数据的接收者。

（3）主要内容

《良好数据法》规范数据库的形成和咨询，其中包含自然人或法人的信息所形成信用记录，适用于个人或法人业绩信息数据库的形成和咨询，不影响 1990 年 9 月 11 日第 8078 号法律——消费者保护和辩护的规定，维护的数据库将受特定立法的管辖。

05 巴西《银行保密法》

（1）定位

2001 年 1 月 10 日《巴西银行保密法》通过，作为银行业关于数据保护的一般基础性法规，对银行业被动和主动交易的所有服务中保密行为进行监管。

（2）特点

金融实体必须对"其所有的信贷和借记交易以及提供的服务"保密。《巴西银行保密法》第 1 条第 3 款列出了可以披露信息而不被视为违反《银行保密法》的具体情形，例如。(i)金融实体或辅助实体之间为信用保护而进行的信息交流；(ii)法律规定或主管当局命令的披露；(iii)利益相关方（即客户）明确授权的披露。

（3）主要内容

《巴西银行保密法》共分为十二条 13 款，第一条为金融机构应当为其提供的主动和被动交易和服务保密，第二条为巴西中央银行对其进行的交易和在履行职责过程中收到的信息也负有保密义务，第三条为巴西中央银行、证券交易委员会和金融机构应提供法院命令要求的信息，通过限制相关方的访问来保护其机密性，不得将此类信息用于其他目的那些与调查有关的，第四条为巴西中央银行和证券交易委员会以及金融机构在各自管辖范围内应向联邦立法部门提供履行各自宪法和法律职责无疑必要的机密信息和文件，第 5 条为行政主管部门应规定金融机构向联邦税务机关通报其客户进行的金融交易的标准（包括报告的周期和金额限制），第 6 条为联邦、州、市和联邦区行政当局的当局和税务代理人仅在行政诉讼或税务诉讼结束后，才应审查金融机构的文件、账簿和记录，包括与存款账户和金融投资有关的文件、账簿和记录，主管行政当局认为该审查是必不可少的，第七条为第七条在不违反第二条第三款规定的情况下，证券交易委员会在启动行政调查后，可以要求主管司法机关对金融机构的资产信息和文件保密，受 CVM 监管的个人或法人实体的权利和义务，第 8 条符合第 4 条、第 6 条和第 7 条规定的要求和手续，由主管机关在向中央银行、证券交易委员会或金融机构提出的请求中明确声明，第 9 条巴西中央银行和证券交易委员会在履行职责时，将法律规定的犯罪行为的发生或迹象核实为公开行为时，应向司法部和司法部报告，在该报告中附上核实和证明事实所需的文件，第 10 条除本补充法授权外，违反保密规定构成犯罪，对肇事者处一年以上四年以下有期徒刑，并处以刑法规定的适用刑罚。损害其他适用的制裁，第 11 条为公务员使用或允许使用因违反本补充法所规定的保密行为而获得的任何信息的，应当对由此造成的损害承担个

人和直接责任，但不得损害公众利益，实体的客观责任，只要证明公务员已按照官方指示行事，第十二条本补充法自公布之日起施行。

06 巴西《信息获取法》[6]

（1）定位

2012 年 5 月 15 日，《巴西信息获取法》生效，该法对广泛获取公共信息作了规定，使向社会披露公共信息的方式发生了重要变化。该法颁布之后，任何公民都可以根据要求访问任何政府机构的相关信息，无论是联邦、州还是地方。

（2）特点

该法规定，国家应确保信息管理的透明度，促进公众广泛获取和传播信息，控制任何信息限制或保密以及个人信息的披露。

（3）主要内容

该法提出了以下基本准则：1）所有公开文件均应公开披露，数据保密性应例外；2）所有公开文件均应披露具有公共利益的信息；3）促进发展公共行政的透明文化，并有社会监督公共行政。

07 巴西《网络安全条例》

（1）定位

2021 年 2 月 26 日，巴西《网络安全条例》通过，规定了金融和支付机构采取网络安全措施要求，并且条例要求相关机构按照条例要求在 2021 年 12 月 31 日之前制定机构网络安全政策[5]。

（2）特点

法规要求机构必须任命一名负责实施和监督其网络安全政策的官员，还必须采取控制措施和程序来预防和应对网络安全事件。

相关机构与第三方供应商（包括巴西以外的供应商）签订协议，以确保它们在签订数据处理、数据存储或云计算合同时遵守某些要求，涵盖机构还必须提前向 BACEN 提供有关第三方提供商的某些信息。

数据处理、存储和云计算包服务时，通过物理或逻辑控制识别和隔离机构的客户数据，保护机构客户数据和信息的访问控制的质量。

（3）主要内容

《网络安全条例》共分为五章，第一章是目的和适用范围、第二章是网络安全政策，第一节为网络安全政策实施，第二节为网络安全政策披露，第三节为行动计划和事件响应，第三章是数据处理、存储和云计算承包服务，第四章为一般规定，第五章为最后条款。

08 巴西政府第 9936/19 号法令[7]

（1）定位

该法令颁布于 2019 年 7 月 24 日，规范了包含个人或法人实体支付记录信息的数据库的创建和管理，旨在建立信用记录。

（2）特点

法令提出了要保证存储数据的完整性和机密性，而且相关认证至少每三年更新一次，且需要进行年度审查，证明政策在责任确认方面是有效的，尤其是在信息的保密和保护、客户数据的隐私保护，以及诈骗预防处理等。

（3）主要内容

法令共分为九章内容，分别为数据库信息运作条件、信用记录、授权向消费者提供信用记录、数据库信息查询、数据库管理员职责、注册访问的取消或暂停、按照数据来源发送信息、信息泄露应急响应等内容。

09 巴西中央银行第 4737/19 号决议[8]

（1）定位

该法令颁布于 2019 年 7 月 29 主要用来规范数据库管理人员的综合素养，并对数据库管理人员的行为进行有效监督。

（2）特点

该法令规定了数据库管理人员获得注册的要求以及取消数据库管理者的情

况。

（3）主要内容

该法令强调，数据库管理人员的任职，需要以下要求：第一，拥有无瑕疵的声誉；第二，没有被判犯有逃税罪、渎职罪、腐败罪等相关的刑事处罚；第三，未被宣布为无资格或被暂停行使财务委员会委员、董事会成员、执行官或金融机构授权经营的其他机构的管理合伙人；第四，未被宣布破产。

三、参考文献

[1]巴西《通用数据保护法》全文中文翻译（DPO 沙龙出品）[EB/OL]. https://mp.weixin.qq.com/s/N9KyiOB6k7l2OVYYXrXeXQ

[2]巴西参议院通过数据保护法案[EB/OL]. https://www.secrss.com/articles/3923

[3]Câmara aprova em 2º turno PEC que inclui a proteção de dados pessoais na Constituição[EB/OL]. https://www.camara.leg.br/noticias/801696-camara-aprova-em-2o-turno-pec-que-inclui-a-protecao-de-dados-pessoais-na-constituicao/

[4]Brazil: New Decree Regulating Internet Legal Framework[EB/OL]. https://www.mondaq.com/brazil/data-protection/493324/new-decree-regulating-internet-legal-framework

[5]Jonathan S. Kolodner、Alanna B. Newman,Guilherme Duraes[EB/OL].https://www.clearycyberwatch.com/2018/05/brazil-issues-new-cybersecurity-regulation-regulated-financial-institutions/

[6]巴西信息获取法[EB/OL]. https://www.mondaq.com/brazil/data-protection/184004/infrastructure--law-12527-of-november-18-2011

[7]巴西政府第 9936/19 号法令[EB/OL]. https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/d9936.htm

[8]巴西中央银行第 4737/19 号决议[EB/OL].https://www.machadomeyer.com.br/en/recent-publications/publications/banking-insurance-and-finance/good-credit-history-and-resolution-4-737-19

日本：兼顾综合性与特定性领域

一、 立法总体情况

相较于欧美在个人信息保护方面的立法，日本个人信息保护的立法起步较晚，其在立法过程中，在广泛借鉴欧美先进立法经验的同时，也充分考虑了日本本国的实际情况。基于数据驱动创新和个人信息保护的平衡，

日本采取了较为中立的统分结合立法监管模式，通过采取统一综合立法和特定领域制定个别法的方式，实现对个人信息使用的严格规制，同时也保证数据流动性以激励企业创新。

在个人信息保护方面，自 1988 年《行政机关计算机处理的个人信息保护法》正式公布生效至今，历经多次修订，如今现行的《个人信息保护法》（2020 年）搭建了日本个人信息保护的立法制度体系。

在网络安全方面，2000 年《保护信息系统免受网络攻击行动计划》是日本在该领域首个政策文件，2013 年《网络安全战略》、2014 年《网络安全基本法》、2015 年《网络安全战略（第二版）》、2018 年《网络安全战略（第三版）》、2022 年最新版《网络安全战略》，构建了网络空间相关的法律框架，致力于构建“自由、公平、安全的网络空间”。

二、 重点法律解析

01 日本《行政个人信息保护法》

（1）定位

1988 年 12 月，日本立法机构颁布了《行政机关计算机处理的个人信息保护法》（简称：“行政个人信息保护法”），并于 1988 年 10 月开始实施，这是日本专门针对个人信息保护的首次国家层面的立法。

（2）特点

《行政机关计算机处理的个人信息保护法》仅适用于行政机关，而且仅对计算机处理个人信息进行保护，而不涉及人工处理信息的行为。

（3）主要内容

《行政机关计算机处理的个人信息保护法》的主旨有两个方面，一是保护个人权利利益，也是首要的目的，二是为了确保对个人信息的保护不会成为行政机关正常运行的阻碍，促使行政机关平稳顺利的运行。该法将保护对象分成了三类，分别是个人信息、持有的个人信息以及个人信息档案。

02 日本《个人信息保护法》

（1）定位

2003 年 5 月，日本正式通过《个人信息保护法》，于 2005 年 4 月 1 日正式施行。该法是在《行政机关计算机处理的个人信息保护法》的基础上制定，明确了基本理念方针等总则性内容及与民间企业相关的一般法性

内容，在日本个人信息保护法制体系中相当于基本法的重要地位。

随着互联网技术的不断发展，后续又多次进行修订：

2015 年，《个人信息保护法》进行了大幅修正，于 2017 年 5 月 30 日全面实施。修正核心内容包括引入“敏感信息”概念、向国外第三方披露要求、退出同意机制、记录保留义务、匿名处理信息等。

2020 年，日本对《个人信息保护法》进行了第二次修改，并于 2022 年 4 月 1 日正式施行。此次修订迎合时代技术创新要求，防范和化解潜在各类风险，增加了很多相关内容。

（2）特点

日本《个人信息保护法》（2020 年）增强了用户权利，加重了数据处理者的义务，新增假名化信息加工相关条款，扩大域外适用范围，加重了惩罚措施。

（3）主要内容

日本《个人信息保护法》（2020 年）主要包括总则、国家及地方公共团体的职责、个人信息保护措施、个人信息处理者的义务、个人信息保护委员会、杂则、罚则等内容。新版《个人信息保护法》重点关注人脸识别信息使用，引入了“假名加工信息”和“匿名加工信息”两类新的信息类型，细化了数据泄露报告制度，加强了数据跨境传输监管。

在数据跨境监管方面，新版《个人信息保护法》从两方面增加了个人信息处理者向日本境外第三方传输数据的限制要求。一方面，在个人同意的情况下进行数据跨境传输时，数据输出方应当向数据主体提供国家名称、相关国家的个人信息保护制度、应当采取的安全保障措施等相关信息；另一方面，采取数据传输合同的方式进行数据跨境传输时，合同必须采用与《个人信息保护法》等效的数据安全保护标准和必要措施，持续确保数据输入方对个人数据的正确适当处理[1]。

03 日本《网络安全战略》

（1）定位

2013 年 6 月 10 日，日本国家信息安全中心发布《网络安全战略——构建世界领先的坚强而充满活力的网络空间》。这一战略明确提出构建“世界领先的”、“坚强的”、“充满活力的”网络空间，标志着网络安全政策从信息安全政策中独立出来。

- 2015 年 9 月，日本政府发布《网络安全战略（第二版）》，明确表达了日本在网络空间领域的战略目标；
- 2018 年 7 月，日本政府发布《网络安全战略（第三版）》，强调“将网络安全治理视为成本而非必要投资”是错误观念；
- 2021 年 7 月 12 日，日本内阁网络安全中心（NISC）公布最新版《网络安全战略》（草案）并征求公众意见。
- 2022 年 2 月 1 日发布了最新《网络安全战略》的彩色手册版，明确今后 3 年日本要实施的各项措施的目标和实施方针。

（2）特点

《网络安全战略》最新版制定了三个网络安全战略目标：提高经济社会活力与持续性发展、营造国民安心舒适生活的数字社会、为国际社会的和平稳定和日本的安全保障做出贡献。

（3）主要内容

《网络安全战略》最新版主要包括制定的宗旨和背景、战略的基本理念、围绕网络空间的课题认识、为达成三个战略目标采取的措施以及推进体制。《网络安全战略》确定了规划和实施有关网络安全措施的五项基本原则：确保信息的自由流通、法治、开放性、自主性和多方合作。为确保“自由、公平、安全的网络空间”目标的实现，《网络安全战略》还给出了三大推进方向：在数字化改革的基础上，同步推广数字化转型与网络安全；纵观整个网络空间，确保公共空间的互联互通和链条化；强化安全防护能力。

04 日本《网络安全基本法》

（1）定位

2014 年 11 月 6 日，日本国会表决通过《网络安全基本法》，旨在加强日本政府与民间在网络安全领域的协调和运用，更好地应对网络攻击。

（2）特点

《网络安全基本法》首次从法律上定义了“网络安全”的概念，在 2000 年基本法的基础之上明确了网络安全的基本原则与政策，规定设立网络安全战略总部，负责制定网络安全战略并保障其实施。

（3）主要内容

《网络安全基本法》包括总则、网络安全战略、基本政策、网络安全战略本部、罚则五个章节。其中，在网络安全战略方面，《网络安全基本法》提出，政府为确保必要资金作为实施网络安全战略所需之经费，应采取必要措施以顺利实施战略，诸如每年在国家财政允许的范围内将其纳入预算等。在网络安全战略本部方面，日本政府于 2015 年 1 月将信息安全政策委员会升级为获得法律授权的“网络安全战略本部”，作为日本推进网络安全政策的最高指挥机构[2]。

三、参考文献

[1]杨春白雪.信通院互联网法律研究中心.聚焦四大问题，日本更新《个人信息保护法》指南问答[EB/OL].https://mp.weixin.qq.com/s/WsOOxVeNZqZZoBNxQyi2Og

[2]福州先知信息咨询有限公司. 日本网络安全战略发展及实施情况[J]. 网信军民融合, 2018(12):6.

印度：构建数据安全保障新法律体系

一、立法总体情况

作为实施数据本地化与跨境流动限制政策的典型国家，印度随着其数字经济的发展，近年来相继颁布了一系列的重要法律或文件，形成了以《信息技术法》为母法、以《个人数据保护法案》为基础，以中央立法为中心，以各邦具体行政法规为辅助的数据安全保障法律体系，其中涵盖电子签名、电子政务、网络犯罪等数字时代的诸多问题，为印度的电子商务发展、网络信息安全提供了全面的法律框架[1]。

二、重点法律解析

01 印度《信息技术法》[2]

（1）定位

1999 年，印度信息产业部以联合国国际贸易法委员会的《电子商务示范法》为蓝本制定了《信息技术法》，该法在 2000 年 5 月经印度国会通过，并于 2000 年 10 月 17 日正式生效。《信息技术法》是印度颁布的第一部有关网络活动的基本法，自此印度成为在计算机和互联网领域拥有专门立法的国家。

（2）特点

实体法与程序法并举：该法不仅规定电子合同、电子签名等实体法律

内容，而且对电子证据、管辖权、上诉法庭等程序问题进行了规定。

注重效率与安全：该法出于交易安全的考虑，规定“确认回执”。随着电子商务的快速发展，2008 年《信息技术法案》删除了“回执”的要求，有利于加快电子商务流通。同时，印度政府试图改革国家加密政策，以方便电子商务的发展，以及对于网络恐怖主义和网络洗钱行为的监控。此外，该法 2008 年加强网络犯罪的惩罚，2011 年细化网络服务提供商的责任，既保障了安全，又实现了效率。

政府主导，兼顾当事人自主：印度采用政府主导模式，对于电子认证机构均实施强制许可制度，任何未获得官方许可的机构不得从事电子认证服务。

（3）主要内容

明确立法目的：主要包括两个方面，一是确认电子商务活动的法律地位；二是规范电子商务活动，并防范与打击针对计算机和网络的犯罪。

提出成立专门受理计算机和网络领域案件的“网络上诉法庭”：明确其人员组成、法庭组成、管辖范围、审理程序和权限。

规定 8 类行为构成“破坏计算机和计算机系统”犯罪：一经查实，犯罪者要负担的民事赔偿金额最高可达 1000 万卢比(约合 200 万元人民币)。这八类行为包括未经许可侵入他人计算机、计算机系统和网络，私自下载他人计算机或系统中的数据信息，制造和散播计算机病毒等。篡改计算机源文件，故意隐瞒、销毁、破坏、更改计算机源代码的行为可判处 3 年监禁或多达 2 万卢比的罚款。

印度在 2006 年和 2008 年修正增加新的计算机犯罪类型：两次修改主要对新型的网络犯罪作出规定，并在 2008 年的修正案中重点规定网络恐怖主义的内容，将网络反恐上升到新的高度。

02 印度《个人数据保护法案》[3][4]

（1）定位

2018 年 7 月 27 日，印度“数据保护专家委员会”起草的《个人数据保护法案》公布并公开征求意见；2019 年 12 月 4 日，印度总理纳伦德拉·莫迪领导的联邦内阁批准了修改后的法案，即《2019 年印度个人数据保护法案》（2019 年第 373 号法案）。该法案旨在为印度“确立强有力的数据保护框架和设立数据保护局，赋予印度公民相关个人数据权利，以确保他们关于‘隐私和个人数据保护’的基本权利”。

（2）特点

立法目的具有多重性：该法案强调“隐私权” 是一项基本权利，法律有必要将个人数据作为隐私信息的重要方面予以保护。法案也提出保护公民利益、贸易和工业利益、国家利益，希望以公民利益为重点，但也同时强调“为了国家安全，政府机构有权访问个人数据并进行调查”。可见，该法案目的虽以保护个人自由和基本权利为核心，终极目的仍是“国家利益至上”，并兼顾其他不同目标。

采用统一立法模式：印度各邦可以制定各自的法律，但若该法案的条款与现行有效的任何其他法律不一致时，本法案具有优先效力。

立法内容具有印度特色：从数据保护立法内容上看，印度制定的个人数据保护法在许多方面与欧盟《通用数据保护条例》趋同，体现了国际数据保护立法的大趋势。在域外管辖方面，效仿欧盟规定了宽泛的涉外管辖范围，只要涉及收集和处理本国居民的个人数据，则不论企业是否在境内有实体均受管辖。

（3）主要内容

明确法案的适用范围：包括在印度境内进行的个人数据收集、披露、共享、处理活动；由印度各邦、公司、公民或其他个人以及根据印度法律成立的团体进行的个人数据处理活动；在印度进行的业务、向印度数据主体提供商品或服务的活动、对印度境内数据主体画像活动有关的个人数据处理活动。但法案不适用于匿名数据的处理行为。

明确数据受托人对数据主体应承担的数据保护义务：确保数据受托人必须以符合数据主体的最佳利益行事。主要包括处理个人数据的禁止行为、处理个人数据目的的限制、收集个人数据的限制、收集或处理个人数据的通知要求、处理的个人数据质量、保留个人数据的限制、数据受托人的责任、处理个人数据所必需的同意。

明确数据主体的权利：规定数据主体的权利和行使权利的一般条件，包括确认和访问权、数据可移植权、被遗忘权、纠正权、删除权、申诉权等。其中删除权即当处理目的不再需要时删除其个人数据的权利，作为数据主体限制或阻止数据受托人继续披露个人数据“被遗忘权”的补充。

个人数据跨境传输：法案提出个人数据跨境传输须在境内留有副本。每个数据受托人应确保在位于印度的服务器或数据中心存储至少一份个人数据服务副本。法案规定，关键个人数据仅能在位于印度的服务器或者数据中心处理。此外，法案给予政府对个人数据出境的自由裁量权。

提出最严厉的处罚措施：法案规定任何未经客户同意共享客户数据的组织将被处以 1 亿 5 千万卢比的罚款或占其全球营业额 4%的罚款。数据泄露的处理、报告延迟将处以 5 千万卢比的罚款或占全球营业额 2%的罚款。

03 印度《国家网络安全政策》[5]

（1）定位

2013 年 7 月 2 日，印度通信与信息技术部发布了《印度国家网络安全政策》文件，旨在组建国家网络安全治理机制。

（2）主要内容

该《政策》提出拟实现的 14 项目标和拟采取的若干战略：包括创建一个安全的网络生态系统，使 IT 系统和在网络空间中发生的交易得到足够的信任，并强化 IT 在印度所有经济部门中的利用；创建一个可信框架，以实现安全策略的设计，并通过产品、过程、技术和人员的一致性评估，

促进其与全球安全标准和最佳实践的兼容；加强监管框架以确保安全的网络空间生态系统；创建和加强全国性的、部门性的全天候无间断的网络安全机制等。

明确拟采取的战略：包括创建稳固的网络生态系统以及保险框架、鼓励开放标准、加强监管框架、创建安全威胁早期预警、漏洞管理和应对安全威胁的机制、保障电子政务服务安全、关键信息基础设施的保护与弹性、推动网络安全的研究与开发、降低供应链风险以及人力资源开发等。

04 印度《印度数据保护框架白皮书》[6]

（1）定位

2017 年 11 月底，印度电子信息技术部发布《印度数据保护框架白皮书》，向社会公众征求意见。《白皮书》为数据保护提供固定法律框架，也为后续起草数据保护法做准备，旨在推动数字经济增长，保护公民个人数据安全。

（2）特点

《白皮书》结合当前印度现有法律法规中相关数据保护条款，并参考欧盟、美国、英国、澳大利亚、南非等国家的立法实践，在数据保护范围和豁免、数据处理、机构义务和个人权利、监管和执行等方面进行深入探索和论证。

（3）主要内容

《白皮书》提出数据保护框架的七大原则：技术不可知原则、整体应用原则、知情同意原则、数据最小化原则、控制者责任原则、结构化执行原则和威慑性惩罚原则。

明确使用范围：《白皮书》为明确其数据相关法律法规的适用范围，提出了诸多观点，并共公众提出建议。《白皮书》提出对于数据保护地域范围，应适用于印度领域内，还是可适用于领域之外。应当如何规制在印度没有常驻地的外国机构处理印度居民数据。对于数据保护主体范围应适

用于自然人还是法人，对于公共机构和私人机构应该一般法律规制还是分别立法规制，数据保护法是否应该溯及既往，是否应该给予一定的宽限期。

明确个人数据、个人敏感数据、数据处理、数据控制者和数据处理者定义：对于关键定义的阐述，《白皮书》参照印度 SPDI 规章、欧盟 GDPR 等多项法律文件，进一步明确其核心定义。

提出数据保护豁免：《白皮书》中列举个人数据保护的豁免情形，例如以家庭、新闻、艺术或文学、学术研究、历史学、统计、刑事调查保护或国家安全为目的进行的数据处理。对于上述豁免情形，该类数据应合法获取，且法律已给予该类个人数据足够程度的保护。

规定跨境数据流动细则：对于是否应该在数据保护法中设置专门的跨境数据流动促进条款，如何设置标准、门槛或测试予以保护，对于一些特殊类型的数据如个人敏感信息是否应该禁止跨境流动，《白皮书》广泛征询意见。

数据处理、机构义务和个人权利：包括同意、儿童同意、通知、目的说明和限制使用、个人敏感数据处理、存储限制和数据质量、个人参与权等。

监管和执行：《白皮书》对于执行方式、职责承担、执行工具、审判程序、救济手段等方面提出建议。

三、参考文献

[1]公安三所网络安全法律研究中心.印度数据本地化与跨境流动立法实践研究[EB/OL].https://www.secrss.com/articles/16702

[2]李静.印度信息技术立法的发展与特色[J].暨南学报(哲学社会科学版),2012,34(11):83-88.

[3]嵇绍国,王宏.印度《个人数据保护法案》浅析[J].保密科学技术,2020(02):57-61.

[4]王捷 .漫谈《印度 2019 个人数据保护法案》[EB/OL].https://mp.weixin.qq.com/s/mqmEOvkbDDPWKP3eHUvFMQ

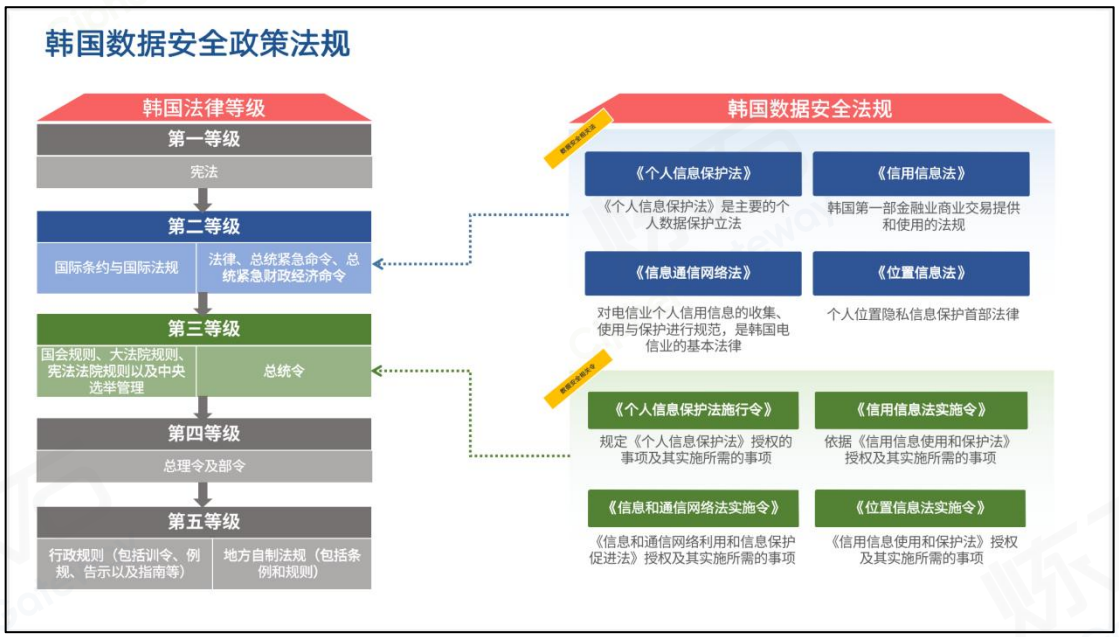
[5]印度发布国家网络安全政策[EB/OL].https://max.book118.com/html/2017/0727/124577783.shtm

[6]“欧系”印度数据保护立法？——《印度数据保护框架白皮书》介评，京东法律研究院高级研究员 魏铭

韩国：“四法四令”构筑数据安全防线

一、立法总体情况

韩国“四法四令”编织数据安全合规密网。《个人信息保护法》（PIPA）作为韩国数据保护的一般法律，主要适用于私人部门和公共机构处理个人信息的情形。韩国国会又通过了《个人信息保护法》《信息通信技术与安全法》和《信用信息保护法》数据法律的修正案，并将数据保护条款纳入《网络法案》，至此《个人信息保护法》最终成为了一部真正意义上的个人信息数据保护法律，与《信息通信技术与安全法》、《信用信息保护法》相互联系，又各有侧重，共筑数据安全体系。



二、重点法律解析

01 韩国《个人信息保护法》

（1）定位

《个人信息保护法》颁布时间为2011年3月29日，作为韩国管辖权范围内具有统一性、一般性、专门性的个人数据保护法律。对个人信息保护的基本原则、个人信息保护的基准、信息主体的权利保障、个人信息自决权的救济等问题作出了全面的规定。

（2）特点

1）明确数据跨境流动的多种渠道。扩大跨境数据流动的合法途径，以承接国际上通常采取的跨境数据流动机制，同时规定，个人信息在跨境的过程中，一旦存在违法行为，则立刻中止跨境行为以确保个人信息安全。

2）建立隐私政策审查机制。引入隐私政策的审查系统，以辅助个人信息保护委员对企业的隐私政策进行评估，确保隐私政策的充分性。

3）引入数据可携权。企业必须有能力为其用户提供其拥有的所有关于数据主体个人信息的拷贝，以及将个人信息传至另一个服务提供商的能力。

4）对于自动化决策的拒绝权和解释权。数据主体不受对个人有法律影响或重大影响的纯粹自动化决策（包括画像）的限制和制约，有权提出异议。同时，个人有权获知关于自动化决策的相关信息。

（3）主要内容

《个人信息保护法》主要包括十章节 76 条，主要包括个人信息保护原则、数据主体权利、国家责任和与其他法律关系、隐私策略制定、个人信息处理和安全管理、数据主体权利保障、信息通信服务提供者等处理个人信息的特殊情况、个人信息纠纷调节委员会、个人信息集体诉讼等，规定了个人信息的管理、个人信息的安全措施、信息主体的权利保障、个人信息的团体诉讼等制度，旨在保护所有公民的个人信息权益，以防信息收集、泄露、不当使用与滥用。法律的适用范围涵盖公共与私人部门管理的一切个人信息，通过规定与个人信息的处理和保护有关的事项，保护个人的自由和权利，实现个人的尊严和价值[1]。

02 韩国《信息保护法》

（1）定位

《信息通信网络利用促进和信息保护法》（简称“信息保护法”）颁布日期为 2001 年 1 月 16 日，法规从电信业个人信用信息的收集、使用与

保护进行全面和具体的规范，是韩国电信业的基本法律。

（2）特点

1）重要信息的限制跨境流动

该法明确限制重要信息向国外流出。规定政府可要求信息通信服务提供者或用户采取必要手段防止任何有关工业、经济、科学、技术等的重要信息通过信息通信网络向国外流动，这类的重要信息包括：（A）国家安全与主要政策相关信息；（B）国内开发的尖端技术或设备相关内容的信息。政府可要求处理这些信息的信息通信服务提供者采取下列措施：（A）安装可防止非法利用信息通信网络的系统性或技术性设备；（B）建立相关制度，安装相关技术设备；（C）可防止非法破坏或操作信息的系统性与技术性措施；（D）可防止信息通信服务提供者泄露履行职务过程中了解到的信息的措施。

2）对于公职人员收集、处理数据要求

（A）科学技术信息和通信副部长或韩国通信委员会信息和通信服务提供者收到提交或收集的文件和数据的保护请求时，不得向第三方提供或向公众披露。（B）科学技术信息和通信副部长或韩国通信委员会信息和通信通过网络接收数据提交等，或者对收集的数据进行数字化处理的，应当采取制度和技术安全措施，防止个人信息和商业秘密泄露。

（3）主要内容

《信息通信网络法》分为九章76条（其中第三章已删除）致力于促进网络使用信息和通信，除了保护服务用户信息和通信其目的是通过创造一个健全和安全的方式使用网络的环境，为改善人们的生活和促进公共福利做出贡献。第一章为总则、第二章为信息和通信促进网络使用、第四章信息和通信营造安全的服务使用环境、第五章信息和通信网络中的用户保护等、第六章信息和通信确保网络稳定性等、第七章电信计费业务、第八章国际合、第九章附则[2]。

03 韩国《信用信息使用和保护法》

（1）定位

《信用信息使用和保护法》颁布时间为 2009 年 4 月 1 日，是韩国第一部关于金融业商业交易中信用信息提供和使用的法规。

（2）特点

1）规定数据处理的流程。“处理”数据是指征信信息的收集（包括调查，下同）、创建、连接、联锁、记录、存储、保存、处理、编辑、检索、输出、更正、恢复、使用、组合等。

2）明确个人信息通过“化名处理和匿名处理”，要求在不使用附加信息的情况下无法被识别“化名信息”是指以化名方式处理的个人信用信息。“匿名处理”是指对个人信用信息进行处理，使其无法再识别特定个人、信用信息主体。

（3）主要内容

《信用信息法》共计分为 7 章 52 条，致力于健全信用信息相关产业，促进信用信息的有效使用和系统管理，妥善保护个人生活机密，防止信用信息被滥用和滥用，建立健全信用秩序。其中共包括：第一章总则、第二章信用信息业务许可等、第三章信用信息的收集和处理、第四章信用信息的分发与管理、第五章信用信息相关行业、第六章信用信息主体保护、第七章补充。

04 韩国《位置信息保护和使用法》

（1）定位

《位置信息保护和使用法》颁布时间为 2010 年 3 月 22 日，是个人位置隐私信息保护首部法律。

（2）特点

明确个人位置信息的法律定义，并要求个人位置信息的处理者应当采

取技术措施保护，首先应当采取安装防火墙、使用加密软件等技术措施，其次位置信息经营者等应确保确认位置信息的收集、使用和提供的数据自动记录保存在位置信息系统中。

（3）主要内容

《位置信息法》分为六章 43 条，第一章为总则、第二章位置信息业务登记、第三章位置信息保护、第四章个人位置信息用于紧急救援、第五章建立使用位置信息等的基础、第六章处罚，致力于保护个人生活的机密性，不被泄露、误用和滥用位置信息，并通过安全使用位置信息促进位置信息的使用，从而改善民生和促进公共福利。

05 韩国《信息和通信网络法实施令》

（1）定位

《信息和通信网络利用和信息保护促进法实施令》颁布日期为 2008 年 2 月 29 日，该法令进一步落实《信息和通信网络利用和信息保护促进法》中个人信息全生命周期保护需求（简称：信息和通信网络法实施令）。

（2）特点

该法规支持信息和通信服务提供者的政策调查、研究和制度建立等手段加强信息保护，分析与信息和通信服务使用相关的对策研究，提高信息通信服务提供者的信息保护能力和专业知识，如首席信息安全官的教育，与信息通信服务安全相关的国际交流与合作，其他安全所需的项目信息通信系统和信息安全管理。

（3）主要内容

《信息和通信网络法实施令》共计分为七章（原第三章已删除）74 条，致力于本信息和通信规定网络利用促进和信息保护法委托及其实施所需的事项。第一章章节为总则、第二章信息和通信促进网络使用、第四章信息和通信营造安全的服务使用环境、第五章信息和通信网络中的用户保护等、第六章信息和通信确保网络稳定性等、第七章补充。

06 韩国《信用信息使用和保护法实施令》

（1）定位

《信用信息使用和保护法实施令》颁布日期为 2009 年 10 月 1 日，细化落实《信用信息使用和保护法》规定要求的具体事项。

（2）特点

落实数据处理中的数据保护要求。具体而言，包括数据收集、存储、使用、加工、传输等处理活动中对于数据保护的要求。1）机构向数据专业机构提供信息集，应当采取以下措施提供：多个信息集链接多个信息，应替换为不能识别个人但可以区分的信息（以下简称“组合键”）；包含个人信用信息的数据集应作为假名处理。2）合并请求机构向数据专业机构提供信息集或者数据专业机构向合并请求机构交付合并信息集时，采取加密等保护措施，使第三方无法知晓其内容。3）信息传输时，必须使用商用加密软件或安全算法进行加密 4）信用信息公司等应实施技术、物理和行政安全措施：访问控制设备的安装和运行事宜，例如阻止第三方非法访问信用信息的入侵防御系统；防止录入征信系统信息被篡改、毁损、毁损的事项；按岗位、任务区别授予信用信息处理查询权的事项，定期检查信用信息查询记录的事项；为保证信用信息稳定所必需的其他事项。

（3）主要内容

《信用信息法实施令》共计分为五章 38 条，致力于对于《信用信息法》具体法律细化执行落实。其中第一章为总则、第二章征信业务等许可、第三章征信信息采集与处理、第四章信用信息分发与管理、第五章信用信息相关行业。

07 韩国《个人信息保护法施行令》

（1）定位

《个人信息保护法施行令》颁布日期为 2001 年 9 月 29 日，规定《个人信息保护法》授权的事项及其实施所需的事项。

（2）特点

个人信息的处理要求确认是否采取了确保安全所需的措施，例如假名化或加密。确保个人信息安全的措施则如下：1）个人信息安全处理的内部管理计划的制定和实施；2）控制访问个人信息和限制访问权限的措施；3）应用可以安全存储和传输个人信息的加密技术或与之对应的措施；4）个人信息侵害事件的访问记录保存和防止伪造、篡改的措施；5）个人信息安全程序的安装和更新；6）提供存储设施或安装锁定装置等物理措施以安全存储个人信息。

（3）主要内容

《信用信息法实施令》共计分为五章38条，致力于对于《信用信息法》具体法律细化执行落实。其中第一章为总则、第二章征信业务等许可、第三章征信信息采集与处理、第四章信用信息分发与管理、第五章信用信息相关行业[3]。

08 韩国《位置信息保护和使用法实施令》

（1）定位

《位置信息保护和使用法实施令》颁布日期为2008年2月29日，落实《信用信息使用和保护法》中位置信息实施要求。

（2）特点

1）设定位置信息管理负责人。制定处理和管理程序和指南，规定位置信息处理者的职责和责任，记录提供位置信息等事实的处理台账的运行管理。

2）位置信息保护措施的定期自查。实施身份验证，确认位置信息和位置信息系统的访问权限，安装防火墙等措施，阻止向位置信息系统发起的未经授权的访问。

3）采取必要技术手段保护位置信息安全。位置信息系统应当接入电

子自动记录保存装置的运行，安全程序的安装和运行，以防止位置信息系统被侵犯，应使用可以安全存储和传输位置信息的加密技术或与之对应的措施。

（3）主要内容

《位置信息法实施令》主要分为 40 条内容，从个人位置信息收集、登记到安全保护措施及细化到人责任落实《信用信息法》。

三、参考文献

[1]个人信息保护法[EB/OL].https://www.law.go.kr/lsSc.do?section=&menuId=1&subMenuId=15&tabMenuId=81&eventGubun=060101&query=%EA%B0%9C%EC%9D%B8+%EC%A0%95%EB%B3%B4#undefined.

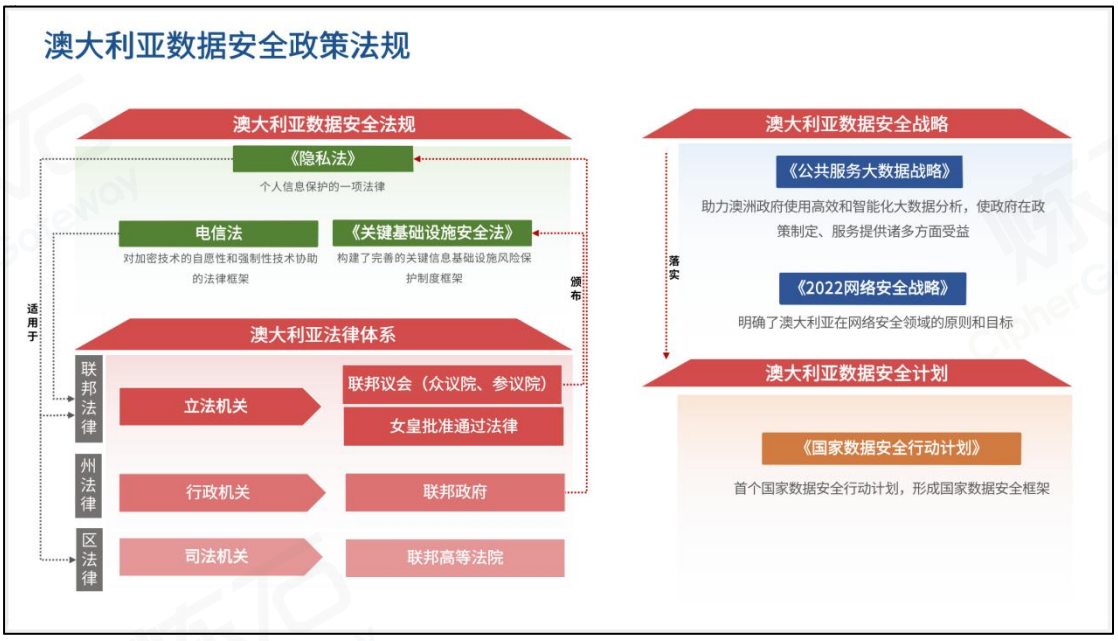
[2]信息通信网络利用促进和信息保护法[EB/OL].https://www.law.go.kr/lsSc.do?section=&menuId=1&subMenuId=15&tabMenuId=81&eventGubun=060101&query=%EA%B0%9C%EC%9D%B8+%EC%A0%95%EB%B3%B4#undefined.

[3]个人保护法施行令[EB/OL].https://www.law.go.kr/lsSc.do?section=&menuId=1&subMenuId=15&tabMenuId=81&eventGubun=060101&query=%EA%B0%9C%EC%9D%B8+%EC%A0%95%EB%B3%B4#undefined.

澳大利亚：隐私安全保护上升为国家顶层战略

一、立法总体情况

澳大利亚是最早重视隐私安全的国家之一，该国于 1988 年颁布的《隐私法》在首都堪培拉和联邦层面内得到适用，此后该国其他州也相继颁布了适用于自身隐私法规。这些法律法规经过历年修订，该国将信息隐私原则和国民隐私原则统合为澳大利亚隐私原则，规范了私人信息数据从采集、存储、安全、使用、发布到销毁的数据生命全周期管理方法，后续将隐私安全保护上升为顶层战略，颁布了《公共服务大数据战略》和 2020《网络安全战略》，为了落实战略，颁布了《国家数据安全行动计划



二、重点法律解析

01 澳大利亚《隐私法》

（1）定位

《隐私法》于 1988 年颁布，是个人信息保护的一项法律。

（2）特点

1）APP 实体必须采取合理措施保护个人信息免遭滥用、侵犯和丢失，以及未经授权的访问、修改或披露，并在收集个人信息的目的不再需要时销毁或取消其身份。2）制定了有关收集、管理、处理、使用、披露和以其他方式处理个人信息的要求。3）向境外传输个人信息之前，APP 实体必须采取合理措施，确保海外接收方不会违反与该个人信息有关的 APP。

（3）主要内容

澳大利亚隐私权的相关立法体现在联邦、省和地区的法案中。1988 年制定的澳大利亚《隐私权法》(the Privacy Act 1988)是关于个人信息保护的一项法律，该隐私权法最大的特色即为制定隐私权保护原则，该原则是对于有关个人信息的操作管理设定概括性的标准，它所适用的情形包括：个人信息的收集(例如，填写表格)；个人信息的使用和透露；个人信息的准确性:个人信息持有的安全性；个人取阅个人信息的权利等等。

《隐私权法》的规范范围甚广，包含税务、医疗、信用资料等范畴，其就隐私权问题处理模式的规定也相当完整，各类别信息的处理方式均深受信息隐私权的限制。《隐私权法》中规定的原则不是规范性的原则，也就是说该法并没有规定组织机构在每种情形下应该做什么。相反，该法提供了如何操作个人信息的原则，每个组织或机构需要根据各自情况遵守这些原则。如果组织或机构违反了隐私原则，隐私权专员办公室可以进行调查，如果个人的隐私权益受到了侵犯，个人主体也可以向办公室投诉实施侵权行为的组织或机构[1]。

02 澳大利亚《关键基础设施安全法》

（1）定位

《关键基础设施安全法》于 2018 年 4 月 11 日颁布，构建了完善的关

键信息基础设施风险保护制度框架，提升与关键基础设施资产管理相关的核心安全实践，以及确保负责任的实体采取全面、主动的方法来识别、预防和降低风险[2]。

（2）特点

1）法规中提到40次“安全性和可靠性”字眼，其中涉及电力网络或电力系统、天然气输送管道、金融服务和市场等方面。

2）数据存储或处理服务是指，在商业基础上提供，涉及使用一台或多台计算机，使最终用户能够存储或备份数据。

3）严格落实信息保护监管要求。部长要求关键基础设施资产的报告实体或运营商提供某些信息或文件。在特定情况下授权制作记录、使用或披露受保护信息，但在其他情况下属于犯罪行为，禁止自证其罪的特权不适用于根据本部分提供信息或文件的要求。

4）对国家最重要的资产所有者和运营者提供更高的网络安全义务，主要围绕加强与政府的关系。

5）完善了信息共享的规定，使受监管实体和政府更容易共享信息以履行其义务。

（3）主要内容

《关键基础设施保护法案》颁布后，经历了2次修订。作为2018年《关键基础设施安全法案》的最新修正案，2021年修正案将在获得总督御准后的第二天生效。这些变化将为责任主体设立新的义务，以建立和维护关键基础设施风险管理计划，以及关键基础设施资产运营者所需的网络安全义务的新框架。2021年修正案是对2018年修正案的第二部分的改革。在确定需要加强监管框架后，澳大利亚政府在SOCI法案现有要求的基础上，通过2021年安全立法修正案（关键基础设施）法案，颁布了第一部分改革。

2022年修正案旨在加强关键基础设施资产的所有者和运营者的风险

管理、准备、预防和复原能力，以保障正常经营活动。他们还寻求改善行业和政府之间的信息交流，以更全面地了解威胁，规定了大多数相互关联和依赖的关键基础设施资产属于具有国家战略意义的系统。这些关键基础设施资产对国家至关重要，因为它们在各个部门之间相互依存，如果受到干扰，可能会对其他关键基础设施资产和部门造成潜在的连锁后果。

03 澳大利亚《电信法》

（1）定位

《电信法》于 1997 年颁布，确立了执法和情报部门要求私营部门提供针对加密技术的自愿性和强制性技术协助的法律框架[3]。

（2）特点

被纳入国家关键基础设施范围内的电信运营商按照电信安全改革框架，采取措施全面提高网络安全水平。

（3）主要内容

《电信法》共计包括四个附表，附表一为标准运营商许可条件包括是个章节 88 条，附表二为标准服务提供商规则包括六章节 20 条，附表三为承运人的权利与豁免包括三章节 63 条，附表四 ACMA 可审查决定包括两章节。

04 澳大利亚《公共服务大数据战略》

（1）定位

《公共服务大数据战略》于 2013 年 8 月颁布，该战略将助力澳洲政府使用高效和智能化大数据分析，使政府在政策制定、服务提供诸多方面受益。

（2）特点

数据公开要注意保护公民的隐私。政府要求各部门各机构在开放数据之前首先要考虑到数据隐私和安全问题，尤其是在跨部门使用的时候更要认真检查。从

各类数据的产生，到聚集成各类数据集，直至数据流向目的地，数据应用分析的整个过程每个环节都要设立有效的控制手段。

（3）主要内容

《公共服务大数据战略》设定了澳大利亚到2030年成为现代数据驱动型社会的愿景，并表明政府致力于以消费者受益和保护消费者的方式促进有价值的数据流动。

05 澳大利亚《网络安全战略》

（1）定位

《网络安全战略》于2020年8月6日颁布，明确了澳大利亚在网络安全领域的原则和目标。

（2）特点

《战略》要求提高社区的网络安全系数，政府将推行“数字身份”计划使民众可以选择使用可信任的数字身份证书来访问政府和私营部门提供的网络服务，以保护相关主体免受身份盗窃、网络犯罪的侵害，保证相关主体更轻松、更安全地使用网络服务。同时还要做到以下几点：一是积极努力提高民众对网络安全威胁的认识，并推动整个社区采取安全可靠的在线行为；二是建立针对家庭和澳大利亚老年人的7×24小时网络安全建议热线；三是增加对受害者支持的资金；四是引入自愿性的物联网业务守则，以帮助消费者做出明智的购买决定。

（3）主要内容

《网络安全战略》（以下简称“《战略》”）旨在加强未来10年内澳大利亚的网络安全，强调要将打击网络犯罪、推进“数字身份”计划、扶持中小企业和扩大地区影响等方面作为今后国家网络安全战略的政策目标，这是澳大利亚现任政府在结合历史和现实的基础之上，针对当前新冠疫情的客观环境进行分析判断后得出的结论[4]。

06 澳大利亚《国家数据安全行动计划》

（1）定位

《国家数据安全行动计划》于 2022 年 4 月 6 日颁布，首个国家数据安全行动计划，形成国家数据安全框架。

（2）特点

1）保护公民的数据（收集、处理和存储在数字系统和网络上的信息）免受侵害。2）为政府、企业和个人建立数据安全设置和要求，以安全、问责和控制为重点运作。

（3）主要内容

《行动计划》旨在补充莫里森政府加强澳大利亚网络安全的工作，其中包括：通过启动打击网络犯罪的国家计划来支持各行业在线发展；通过资助由澳大利亚联邦调查局领导的专门的网络犯罪中心，打击网络犯罪分子，确保对国家安全立法进行里程碑式改革，以更好地保护关键基础设施；通过重要立法彻底改变澳大利亚机构调查和起诉网络犯罪的方式，使所有澳大利亚人更安全；确保执法机构拥有打击暗网犯罪的权力；通过勒索软件行动计划打击网络攻击，保护澳大利亚人免受勒索软件的侵害；通过与美国签署 CLOUD 法案协议，促进与美国当局的数字信息交流；发起公共信息运动，以提高澳大利亚的网络安全[5]。

三、参考文献

[1]刘晓丹.澳大利亚《隐私权法》述评及其启示[J].法制与社会,2018(08):5-7+9.DOI:10.19387/j.cnki.1009-0592.2018.03.117.

[2]崔聪聪,许智鑫.澳大利亚关键基础设施安全法解读及其启示[J].重庆邮电大学学报(社会科学版),2020,32(06):40-48.

[3]新华网.维护网络安全不能奉行双重标准——评澳大利亚《2018 年电信和其他法律修正(协助和访问)法案》[EB/OL].http://www.xinhuanet.com/world/2019-04/16/c_1210110615.htm.

[4]卢英佳.2020《澳大利亚网络安全战略》主要特点和动向评估[J].中国信息安全,2020(11):64-67.

[5]熊小熊.澳制定《国家数据安全行动计划》完善数据安全框架[EB/OL].https://www.esensoft.com/industry-news/dx-8709.html.

南非：完善数据保护立法，维护国家数据主权

一、立法总体情况

随着非洲数字基础设施的不断完善，数字技术已渗透延展到非洲各国的政治、经济和军事等各个领域。因此，加强个人信息保护，保障数据安全已成为非洲各国建设的重中之重。为此，非洲各国通过不断完善数据保护立法，以实现维护国家的数据主权，保障国家的安全、促进经济健康发展。目前，在南非、肯尼亚、卢旺达等国，已拥有全面的数据保护法律，而南非《个人信息保护法》最具特色。

二、重点法律解析

01 南非《个人信息保护法》[1]

（1）定位

南非《个人信息保护法》的实质性规定已于 2020 年 7 月 1 日生效（对于信息获取的监督规定于 2021 年 6 月 30 日生效）。该法案通过规定处理个人信息的条件，确定处理个人信息的最低要求，明确数据主体的相关权利，以此来保护公共和私人机构处理的个人信息安全。

（2）特点[2]

首次在立法层面全面加强数据安全保护。该法是南非第一部全面的数据保护法，旨在促进公共及私人机构加强对所处理个人信息的保护。该法对组织实现合规给予了 12 个月的宽限期；明确细化罚则，违反规定的组

织可能面临最高 1000 万南非兰特（约合 400 万人民币）的行政罚款、还可能被提起民事诉讼或被要求承担刑事责任等。该法是全球为数不多的为法人（例如公司和信托公司）提供数据资产保护的法律之一。

推动南非的数据保护立法与国际接轨。该法的实施是南非隐私保护领域的重大进步，通过规范自然人和法人的信息处理行为、为南非处理个人信息的企业设置更多义务，使南非在数据保护立法方面与国际接轨。

（3）主要内容[3][4]

明确适用范围及个人信息定义：从适用对象看，POPIA 普遍义务适用于“责任方”（即确定处理目的和处理方式的个人数据主要处理者），其有限义务也适用于“运营商”（即数据处理者）。从地域范围看，该法适用于责任方负责处理个人信息且其住所地在南非，或虽然住所地在其他地方但是其在南非使用自动或非自动手段来处理个人信息的情形。同时，法律包含“个人信息”的开放式定义，该定义通常是指可识别的在世的自然人、可识别的公司或类似法人的有关信息。

规定合法处理个人信息的条件：该法提供了一种通用的信息保护机制，同时适用于公共与私营部门。与欧盟《数据保护指令》（95 指令）相似，该法规定了合法处理个人信息的八个条件，包括：问责制、处理限制、目的规范、进一步处理限制、信息质量、开放性、安全保障、数据主体的参与。

要求企业采取措施，落实安全保障：该法确保其持有和控制的个人信息免遭未经授权的访问、使用和丢失。其中包括采取适当的物理、技术及组织措施保护个人信息安全，确保安全措施级别与所涉及的个人信息的数量、性质和敏感程度保持一致。该法还要求企业应任命一名信息官和一名副信息官，以确保企业行为符合规定，且可以处理数据主体的投诉，企业还应保留所有与处理相关的过程性文件。

提出特殊个人信息处理要求：该法禁止处理特殊的个人信息（有关个

人的宗教信仰、种族、犯罪行为、健康、性生活，政治立场，甚至工会会员）。虽然可以通过征得数据当事人的同意来取消此禁止，但是数据当事人可随时撤消该同意。

丰富数据跨境流动要求：该法规定企业不得将数据主体的个人信息转让给国外第三方，除非作为信息接收者的第三方受到具有同等保护水平的法律、约束性公司规则或约束性协议的限制。

细化监督机构的权责与职能：该法规定监督机构的权责与职能包括：提供教育，监控与强制执行，与利害关系人协商，处理投诉，组织研究并向国会报告等。

明确罚则，并赋予数据主体救济性权利：不遵守该法的处罚包括最高10年的监禁或不超过1000万南非兰特（约577176美元）的行政罚款。此外，该法制定了新的民事救济办法，使数据主体有权在严格责任的基础上对个人信息负责的各方提起索赔。

三、参考文献

[1]Nerushka Bowa.历时七年，《南非个人信息保护法》终于正式生效[EB/OL].https://www.secrss.com/articles/23776

[2]华为云.南非个人信息保护法（POPIA）[EB/OL].https://www.huaweicloud.com/securecenter/compliance/compliance-center/south-africa-popia.html

[3] SCA.南非《个人信息保护法》全面生效[EB/OL].https://www.smart-alliance.com/zh-cn/news_ms_4595.html

[4]非洲数据保护法律介绍[EB/OL].https://www.sohu.com/a/348503308_99941697

声明

北京炼石网络技术有限公司对国外数据安全政策研究报告（以下简称报告或本报告）的内容及相关产品信息拥有受法律保护的著作权，未经授权许可，任何人不得将报告的全部或部分内容以转让、出售等方式用于商业目的使用。转载、摘编使用本报告文字或者观点的应注明来源。报告中所载的材料和信息，包括但不限于文本、图片、数据、观点、建议等各种形式，不能替代律师出具的法律意见。违反上述声明者，本公司将追究其相关法律责任。报告撰写过程中，为便于技术说明和涵义解释，引用了一系列的参考文献，内容如有侵权，请联系本公司修改或删除。

北京炼石网络技术有限公司

联系电话： 010-88459460

邮箱： support@ciphergateway.com

关于炼石

数据实战化防护 安全新合规平台

炼石网络是一家数据安全技术创新厂商，先后获得安天、国科嘉和、腾讯等投资，面向个人信息和商业数据保护等场景，开创自研“免改造数据安全”产品，以及 DSM 数据安全管理平台。炼石免改造数据安全夺得第七届互联网安全大会（ISC 2019）首届“创新独角兽沙盒大赛”总冠军，技术特色是免开发改造应用的数据保护、高性能国产密码和去标识化技术，为政府、金融、运营商、交通、教医旅、工业等用户提供个人信息保护、商业数据保护、DSM 数据安全管理合规改造、国密合规改造。面向《密码法》《数据安全法》《个人信息保护法》等法律法规，企业重要数据与个人信息亟待提升防护水平与合规改造。炼石基于免改造数据安全技术，通过高覆盖率的数据控制点，横向覆盖广泛应用，纵向叠加发现识别、加密、去标识化、检测/响应、审计追溯等安全能力，有效保护结构化与非结构化数据，实现集中式管控、分布式保护，可应用在数据存储、使用、加工、传输、提供等环节。炼石方案可在不影响业务的前提下敏捷实施上线，将安全与业务在技术上解耦、但又在能力上融合交织，实现主体到应用内用户、客体到字段/文档级的有效保护，打造实战化数据安全防护体系。

关于国浩

高效、诚实、信用、审慎、果断

国浩律师集团事务所成立于 1998 年 6 月，是中华人民共和国司法部批准组建的中国第一家集团性律师事务所，2011 年 3 月更名为国浩律师事务所。国浩律师事务所由北京市张涌涛律师事务所、上海市万国律师事务所、深圳市唐人律师事务所发起设立，并在司法部登记注册。前述三家事务所均成立于 1992 年及 1993 年间，至今已有近三十年的执业历史。

国浩律师事务所开创了中国律师业规模化、专业化、规范化、国际化、品牌化之先河，创立伊始即设有公司与商业专业委员会、银行与金融专业委员会、国际投资专业委员会等专业化法律服务部门，上述相关部门现已发展成为国浩资本市场、民商事争议解决、知识产权、建工地产、刑事法律、跨境投资等二十余个研究中心暨业务委员会。

国浩律师事务所在全球设有 35 个执业机构，涵盖北京、上海、深圳、杭州、广州、昆明、天津、成都、宁波、福州、西安、南京、南宁、济南、重庆、苏州、长沙、太原、武汉、贵阳、乌鲁木齐、郑州、石家庄、合肥、海南、青岛、南昌、大连、银川、香港、巴黎、马德里、硅谷、斯德哥尔摩、纽约。其于 2017 年 7 月发起设立的“一带一路”法律服务协作体，成员为来自 20 多个国家和地区的近 40 家律师事务所;2019 年 10 月与西班牙 ECIJA 律师事务所签订战略合作协议，法律服务网络延伸至拉美诸国。

炼石免改造数据安全

北京炼石网络技术有限公司
BEIJING LIANSHI NETWORKS TECHNOLOGY CO.,LTD.

010-88459460

北京市海淀区北三环西路32号恒润国际大厦710

sales@ciphergateway.com