腾讯研究院

中美欧个人信息保护法比较——

- 中国《个人信息保护法》
- 欧盟GDPR
- 美国加州隐私保护法（CCPA&CPRA）

引　言

2021 年 8 月 20 日，《个人信息保护法》颁布，并将于 2021 年 11 月 1 日起正式实施。《个人信息保护法》是我国迈入数字化社会，彰显“以人为本”的法律制度里程碑，也是我国为全球数字治理贡献的中国方案。

近年来，个人信息保护立法在世界范围内如火如荼地展开，目前已经有 128 个国家通过立法保护个人信息和隐私。[1]其中，结合市场规模，规制范围等因素，以欧盟《通用数据保护条例》（以下简称 GDPR），美国加利福尼亚州隐私保护法（CCPA&CPRA）[2]，以及中国刚刚出台的《个人信息保护法》为最具有影响力的法律文本。以这四部法律文本为基础，开展条款比较工作，能够系统展现当今世界个人信息保护立法在最为主要的区域及国家的共性与差异，为企业合规工作及学者研究带来积极价值。

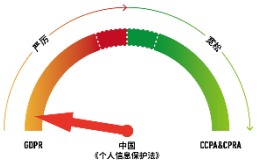
腾讯研究院依托对个人信息保护领域法律制度的长期积累和专业洞察，完成了《中美欧个人信息保护法比较——以中国<个人信息保护法>、欧盟 GDPR，美国加州 CCPA&CPRA 为样本》的专题报告，以飨读者。其中有不完善甚至谬误之处，欢迎指出！

[1] See: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide, 最后访问日期：2021 年 8 月 17 日。

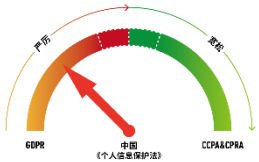
[2] 2018 年 6 月 28 日签署的 CCPA 是一项旨在增强美国加利福尼亚州居民隐私权和消费者保护的州法规。在其基础上，2020 年 11 月 3 日加州选民投票通过了 CPRA，对 CCPA 的一些重要条款进行了修正，扩展了 CCPA 的范围并制定了新的执行机制。CCPA 和 CPRA 共同构建了加州隐私保护法的主要制度框架，两者均是对《加利福尼亚民法典》（California Civil Code）第三章第四部分进行的修改，因此下文加州隐私法（CCPA&CRPA）引用条文的均是《加利福尼亚民法典》（以下简称《加州民法典》）的相关条款。

报告目录

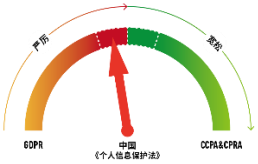
图标说明



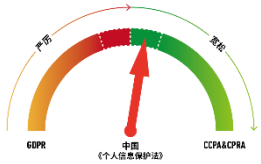
图一



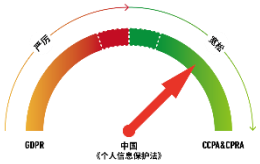
图二



图三



图四



图五

每个二级标题均有一个矢量图说明比较结论。指针代表中国《个人信息保护法》，左侧（即橙红色区域）代表 GDPR 模式，右侧（即绿色区域）代表加州隐私法（CCPA&CPRA）模式。

- **指针方向：**指针指向左侧说明就此部分规则而言《个人信息保护法》更接近 GDPR 模式，指向右侧则说明《个人信息保护法》更接近加州隐私法（CCPA&CPRA）模式。
- **指针指向的颜色：**
  - 橙色向红色渐变说明法律的严厉程度递增，白色虚线内的红色区域表示严厉程度超过 GDPR；
  - 深绿向浅绿渐变说明法律的宽松程度递增，白色虚线内的深绿色部分表示严厉程度超过 CCPA&CPRA。
- 五种矢量图具体说明如下
  - 图一：《个人信息保护法》模式和 GDPR 相似，但比 GDPR 更宽松。
  - 图二：《个人信息保护法》模式和严厉程度上与 GDPR 基本一致。
  - 图三：《个人信息保护法》模式上与 GDPR 相似，但是比 GDPR 更严格。
  - 图四：《个人信息保护法》模式上与加州隐私法（CCPA&CPRA）相似，但是比加州隐私法（CCPA&CPRA）更严格。
  - 图五：《个人信息保护法》模式上与加州隐私法（CCPA&CPRA）相似，宽松程度与其基本一致。

一、立法模式与适用范围

中国《个人信息保护法》采取了类似于 GDPR 的综合立法模式，而加州隐私法（CCPA&CPRA）是在消费者保护领域的个人信息保护专门立法。两种立法模式下，法律的适用范围有显著的不同：

适用范围概览：

立法模式		GDPR——综合性立法	中国《个人信息保护法》——综合性立法	加州隐私法（CCPA&CPRA）——消费者保护领域的专门立法
适用地域范围	境内	欧盟境内：**在欧盟内部设立**的数据控制者或处理者对个人数据的处理，不论其实际数据处理行为是否在欧盟内进行。[3]	中国境内：**数据处理活动发生**在境内	1.在加利福尼亚州**进行商业活动**的企业 2. 任何控制或被第（1）段所界定的业务所控制并与该业务有共同品牌的实体[4] 3.由多个企业组成的合营或合伙企业，每个企业至少拥有合营企业或合伙企业 40%的权益 4. 在加利福尼亚州开展业务且不受第 (1)、(2) 或 (3) 款约束的人，自愿向加利福尼亚隐私保护局证明其遵守并本法规定的。
	境外	欧盟境外：在欧盟境外**向欧盟境内个人提供商品或服务，或对其监控**的情形[5]	中国境外：在境外处理，但：以**向境内自然人提供产品或者服务为目的**，或分析、评估境内自然人的行为；以及法律、行政法规规定的其他情形[6]	

[3] GDPR 第三条
[4] 《加州民法典》1798.140 条（d）；
[5] GDPR 第三条
[6] 中国《个人信息保护法》第三条；

受保护的人	境内	+欧盟**境内**自然人[7]： （data subject）	+中国**境内**的自然人[8] (个人)	加州居民[9]：（1）非临时或临时目的而**在该州**的每个人，以及 (2) **居住在该州**但临时或因暂时的目的而在该州之外的每个人
	非境内	在欧盟设立的机构所处理的个人数据（不限于欧盟境内的自然人）；	在中国境内处理的个人数据（不限于中国境内的个人）	

	GDPR	中国《个人信息保护法》	加州隐私法（CCPA&CPRA）
受规制的实体类型	数据控制者和数据处理者[10]	个人信息处理者和受托人[11] （注：个人信息处理者相当于欧盟 GDPR 中的数据控制者；）	符合一定条件的企业[12]
适用的数据活动	数据处理活动：对数据的操作行为（以概括＋列举方式的全面界定。）[13]	个人信息的处理： 个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等[14]。	收集（collect）； 出售（sale）； 共享（share）。[15]

[7] GDPR 第三条
[8] 中国《个人信息保护法》第三条；
[9]《加利福尼亚州管制法典》第 17014.条（a）款：居民包括(1) 非临时或临时目的而在该州的每个人，以及 (2) 居住在该州但临时或因暂时的目的而在该州之外的每个人
[10] GDPR 第四条
[11] 中国《个人信息保护法》 第七十三条 ，第五十九条
[12]《加州民法典》第 1798.140.条（CCPA）：企业是指：（1）年收入超过 2500 万美元；（2）购买、收取、出售或共享 100,000 人甚至更多的消费者、家庭或设备的个人信息；（3）通过销售或共享消费者的个人信息获得其年收入的 50％甚至更多。
[13] GDPR 第四条第（2）项："处理"是指任何一项或多项针对单一个人数据或系列个人数据所进行的操作行为，不论该操作行为是否采取收集、记录、组织、构造、存储、调整、更改、检索、咨询、使用、通过传输而公开、散布或其他方式对他人公开、排列或组合、限制、删除或销毁而公开等自动化方式。
[14] 中国《个人信息保护法》第四条第二款
[15] 《加州民法典》第 1798.140.条："收集"（Collects）、"已收集"（collected）或"收集集合"（collection）是指以任何方式购买、出租、收集、获取、接收或访问与消费者有关的任何个人信息。这包括主动或被动地从消费者那里接收信息，或者通过观察消费者的行为来接收信息；出售（sale）："出售"、"出售中"、"销售"或"已出售"是指企业以金钱或其他有价值的对价，通过口头、书面、电子或其他方式，向一家企业或第三方出售、出租、发布、披露、传播、提供、转让消费者的个人信息；共享（share）：是指企业为了实现行为广

排除适用的范围	欧盟法管辖之外的活动中所进行的个人数据处理；		该商业行为的所有要素都完全发生在加利福尼亚州以外[16]
	欧盟成员国为履行《欧盟基本条约》（TEU）第 2 章第 5 款所规定的活动而进行的个人数据处理；		
	自然人在纯粹个人或家庭活动中所进行的个人数据处理；	自然人因个人或者家庭事务处理个人信息	
	有关主管部门为预防、调查、侦查、起诉刑事犯罪、执行刑事处罚、防范及预防公共安全威胁而进行的个人数据处理[17]。		遵守联邦、州或地方法律；遵守联邦、州或地方当局的民事、刑事或监管调查、调查、传票或传唤；与执法机构进行的合作；行使或者辩护法律主张。
		法律对各级人民政府及其有关部门组织实施的统计、档案管理活动中的个人信息处理有规定的[18]。	
			医疗、征信、驾驶、金融、政府公开信息、雇员信息、车辆信息以及（车辆）所有权信息[19] （注：*加州隐私法通过对数据处理活动的限缩解释以及在个人信息的定义中排除多种具体的信息类型，

告的目的，通过共享、出租、发布、披露、传播、提供、转移或以其他方式口头、书面、电子或其他方式向第三方传输消费者的个人信息，无论是否出于金钱或其他有价值的考虑。

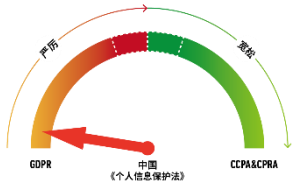
[16] 《加州民法典》1798.145 条（a）（7）

[17] GDPR 第二条第二款

[18] 中国《个人信息保护法》第七十二条

[19] 《加州民法典》第 1798.145 条

			从而限制了适用范围，具体分析见下文“规制的数据活动”、“排除适用的范围”以及“个人信息的定义”部分。）



适用的地域范围

各部法律均具有域外适用的效力。但从域外适用的范围看，GDPR 的范围最为宽泛，中国《个人信息保护法》在地域范围上做了适当延伸，但相较 GDPR 更为克制。

GDPR:

在地域范围上，GDPR 采取的**机构设立地标准和目标指向标准**建立了较为宽泛的地域管辖范围。

1.机构设立标准：如果个人数据控制者或者处理者在欧盟境内设立了**实体（establishment）**，在实体开展业务的场景下发生的数据处理行为受到该法管辖，无论数据处理行为的具体位置是否在欧盟境内。

（1）在实体的认定问题上，GDPR 序言第 22 条明确，“设立机构意味着经过稳定安排的活动的真正有效执行。这种安排的法律形式，无论是一个分支机构还是一个具有法律人格的子公司，并非决定性因素”。

（2）而针对数据处理行为是否发生在此实体开展业务活动的场景中，EDPB 在指南中指出，应该结合具体案情分析。一方面，为了确保对欧盟个人

数据提供充分有效的保护，不应该对该问题进行限缩解释；另一方面，某些数据处理行为虽然发生在欧盟境内但是与欧盟鲜有联系（或者偶有联系），也不能对该行为的法律适用进行过度扩大解释，最终导致将 GDPR 错误地适用于上述行为。

在判断“特定的数据处理行为”是否可以被认定为“发生在此实体开展业务活动的场景中”时，EDPB 建议围绕两大因素进行考虑：第一，欧盟境外的数据控制者或处理者与他设立在欧盟境内的经营场所之间的关系。第二，是否在欧盟境内产生盈利。[20]

2.目标指向标准是指，即使数据控制者或处理者不在欧盟设立，只要它为欧盟境内的数据主体提供商品或服务或对发生在欧洲范围内的数据主体的活动进行监控，即应当适用 GDPR。

中国《个人信息保护法》：

中国《个人信息保护法》在地域范围上采取了信息处理活动发生地标准和目标指向标准。总体借鉴了 GDPR 思路，但信息处理活动发生地标准与 GDPR 的机构设立地标准存在一定差异,前者在扩展域外适用方面，具有更大的谦抑性。

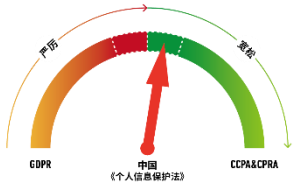
一方面，组织、个人在中华人民共和国境内处理自然人个人信息的活动应当适用中国《个人信息保护法》（信息处理活动发生地）；另一方面，在境外处理中华人民共和国境内自然人个人信息，且有：（1）以向境内自然人提供产品或者服务为目的；（2）分析、评估境内自然人的行为；（3）法律、行政法规规定的其他情形，也适用中国《个人信息保护法》。

加州 CCPA&CPRA:

加州隐私保护法（CCPA&CPRA）的地域适用范围以商业活动发生地作为主要判断标准，但是由于法案本身并未对为进行商业活动（doing business）进行定义，而根据加利福尼亚税法和公司法，商业活动是指 “为获得经济利益、金钱收益、利润而积极参与任何交易”，因此可以对“商业活动”进行广义

[20] Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) : https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf

的解释。



受规制的对象类型

在规制主体方面，GDPR 中明确区分了数据控制者与数据处理者两类主体，而中国《个人信息保护法》和**加州隐私法（CCPA&CPRA）更为接近，两者都未采取主体的二分法，**而是在建立类似于控制者的概念后，通过委托关系明确受托人的义务。从定义上看，中国《个人信息保护法》中的个人信息处理者的概念和 GDPR 的数据控制者概念类似，其是数据处理活动的决定者和主要负责者。

GDPR:

数据控制者和数据处理者的概念在 GDPR 的应用中起着至关重要的作用，因为它们决定了谁负责遵守不同的数据保护规则，以及数据主体在实践中向谁主张权利。[21]数据控制者决定个人信息处理目的与方式，因此确保个人数据的处理需具有合法性理由是针对控制者提出的。数据控制者对于数据主体权利的行使、非法数据处理造成的损害、以及采取安全保护措施等方面有重要的责任。[22]

同时 GDPR 的一个重要特点是直接对处理者施加了一定的数据保护义务，例如数据处理者必须遵守保密义务、保存处理活动记录、遵守数据跨境流动的规则等等。对于控制者和处理者明确指向各自应负担的法定义务，为企业合规和合同责任分配提供了较为明确的规则指引。在云计算的场景下，数据

[21] **Guidelines 07/2020 on the concepts of controller and processor in the GDPR，see：https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/guidelines-072020-concepts-controller-and_en**

[22] **Opinion 1/2010 on the concepts of "controller" and "processor"，see：https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf**

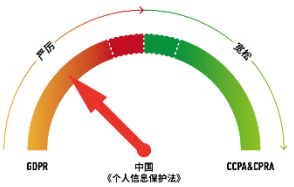
控制者一方面需要履行好选任处理者的义务，保证数据处理者有足够的技术能力保障数据主体的个人数据安全，另一方面需要通过合同条款保留对通过云服务执行的个人数据处理的控制权（确定目的和方式）。而数据处理者则需要按照合同约定和法律规定协助数据控制者履行其数据保护义务，特别是后者对行使数据保护权利的数据主体提出的访问、阻止、纠正和删除请求的迅速响应。[23]

中国《个人信息保护法》，CCPA&CPRA

中国《个人信息保护法》笼统规定受托处理者应当采取必要措施保障所处理的个人信息的安全，并协助个人信息处理者履行本法规定的义务。“相关义务”较为模糊无法为企业提供明确的指引，还留待后续实践中逐步清晰。加州隐私法也存在类似问题。

加州 CCPA&CPRA 中区分了企业（Business），服务提供商（Service Provider），承包商（Contractor），三者的义务要求存在一些差异。例如，服务提供商和承包商有如下义务：（1）配合企业响应可验证的消费者请求，在企业的指示下删除或使企业能够删除，关于消费者的个人信息；[24]（2）在收到企业的指示后，协助企业实现目的的服务提供者或承包商，在实际知道个人信息属于敏感个人信息的范围内，不得使用敏感个人信息。从表述上看不难发现，服务提供商、承包商的以上义务受限于服务提供商、承包商与企业的关系。例如在删除权的行使上，当服务提供商或承包商是作为该企业的服务提供商或承包商收集、使用，处理和储存消费者个人信息的，其无需满足消费者直接向其提出的删除要求，[25]而在敏感个人信息的问题上，服务提供商和承包商业仅需限制其根据与企业签订的书面合同收到的敏感个人信息的适用，以响应企业的指示，并且仅限于与该企业的关系。[26]

[23] Guidelines on the use of cloud computing services, see https://edps.europa.eu/data-protection/our-work/publications/guidelines/guidelines-use-cloud-computing-services-european_en
[24] 《加州民法典》第 1798.105 条（3）（c）
[25] 《加州民法典》第 1798.105（3）（c）
[26] 《加州民法典》第 1798.121 条（c）



规制的数据活动

GDPR 与中国《个人信息保护法》较为类似，对于规制的数据活动都采取了较为宽泛的解释，而加州隐私法对规制活动作出了明确的限缩。

GDPR，中国《个人信息保护法》：

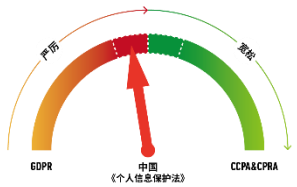
GDPR 调整的数据处理活动是指，任何一项或多项针对单一个人数据或系列个人数据所进行的操作行为，不论该操作行为是否采取收集、记录、组织、构造、存储、调整、更改、检索、咨询、使用、通过传输而公开、散布或其他方式对他人公开、排列或组合、限制、删除或销毁而公开等自动化方式。

中国《个人信息保护法》列举的调整行为少于 GDPR，但同样具有宽泛性。

加州 CCPA&CPRA:

CCPA&CPRA 则仅规制收集（collect），出售（sell），共享（share）数据三类行为。根据《加州民法典》第 1798.140 条，该法案中的“出售”、“出售中”、“销售”或“已出售”是指企业以金钱或其他有价值的对价，通过口头、书面、电子或其他方式，向一家企业或第三方出售、出租、发布、披露、传播、提供、转让消费者的个人信息。 可见“出售”一词也具有很大的解释空间，包括就个人信息进行价值交换（“对价”）的任何安排。[27]

[27] https://www.osano.com/articles/ccpa-definition-sell



排除适用的范围

立法模式的不同决定了各部法律对于适用的信息类型和实体范围存在差异。中欧法律适用更为广泛，加州隐私法依旧作出了许多排除。

GDPR，中国《个人信息保护法》：

GDPR 和中国《个人信息保护法》是综合通用性立法，并未像加州隐私法（CCPA&CPRA）一样，从个人信息类型上对适用范围进行限制。但是在信息处理行为的类型中，**GDPR 在适用范围上排除了“自然人在纯粹个人或家庭活动中所进行的个人数据处理”，中国《个人信息保护法》也做了类似排除。**同时，考虑到中小企业的情况，GDPR 序言第十三条和正文第三十条明确，减免雇员人数在 250 人以下实体的备案（record-keeping）义务。但中国《个人信息保护法》未做类似限制。

加州 CCPA&CPRA:

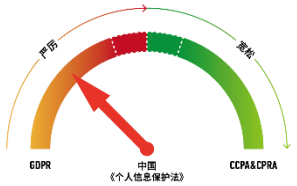
CCPA&CPRA 的适用范围从数据类型上排除了医疗、征信、驾驶、金融、政府公开信息、雇员信息、车辆信息以及（车辆）所有权信息等受其他部门法（eg:《医疗信息保密法》、《健康保险可携带性和责任法案》、《健康信息技术促进经济和临床健康法案》、《公平信用报告法》、《联邦格莱姆-里奇-布莱利法案》、《驾驶员隐私保护法》）调整的信息。

并且，通过年收入和收集信息的数量等条件对受规制的实体进行了限制（年收入超过 2500 万美元；购买、收集、出售或共享 100,000 人甚至更多的

消费者、家庭或设备的个人信息；通过销售或共享消费者的个人信息获得其年收入的 50％甚至更多。）[28]

[28] See Voss, W. Gregory, The CCPA and the GDPR Are Not the Same: Why You Should Understand Both (January 18, 2021). W. Gregory Voss, 'The CCPA and the GDPR Are Not the Same: Why You Should Understand Both,' CPI Antitrust Chronicle, Jan. 2021, Vol. 1(1), pp. 7-12, available at https://www.competitionpolicyinternational.com/the-ccpa-and-the-gdpr-are-not-the-same-why-you-should-understand-both/. , Available at SSRN: https://ssrn.com/abstract=3769825

二、个人信息的定义及分类



个人信息的定义

关于个人信息的定义，各部法律在具体的界定方式、概念的内涵和外延上均存在区别。中国《个人信息保护法》与 GDPR 在定义方法上更接近，将所有可识别与已识别的自然人有关的个人信息纳入了调整范围，保护范围更广。同时，两法也都明确排除了匿名化信息。

而 CCPA&CPRA 则通过定义+列举+排除的方式界定个人信息，范围更加限定和明确。CCPA&CPRA 强调“合理性”和“连接触达性”来进一步限缩个人信息的范畴。[29]同时，加州北区联邦地区法院在 Gardiner 诉 Walmart Inc.一案中对可以提起民事诉讼的个人信息进一步限缩为加州隐私法明确列举的个人信息类型，即：（1）未经加密的姓名、名字首字母和个人姓氏与社会安全号码、驾驶证号码、账号、信用卡号码等的组合，（2）用户名或电子邮箱地址与密码或安全问题和答案的组合（使得在线账户可访问）。[30]最后，CCPA&CPRA 排除适用的信息类型（去识别化信息、汇总的消费者信息、可公开获取的信息、合法获得的、引起公众关注的真实信息）大大多于 GDPR 和中国《个人信息保护法》。

	GDPR （第四条）	中国《个人信息保护法》 （第四条）	加州隐私法（CCPA&CPRA） （第 1798.140.条（v）项）
定义	与任何已识别或可识别的自然人（“数据主体”）**相关**（relating to）的信息	以电子或者其他方式记录的与已识别或者可识别的自然人**有关的各种信息**	直接或间接地识别、关联、描述、能够**合理地**与某一特定消费者或家庭相关联**或可以合理地与之相关联的信息。**

[29] 王融：《美欧隐私立法是否走向趋同，加州 CCPA 给出答案》，腾讯研究院微信公众号，2019 年 9 月 26 日：https://mp.weixin.qq.com/s/JLrrsGRSXwzECLbZ0la33w
[30] https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=3423&context=historical

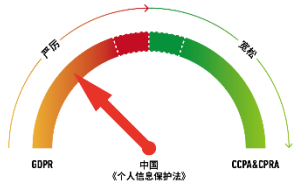
列举类型	姓名	无列举	
	身份编号		
	地址数据		
	网上标识		识别码
	自然人所持有的一项或多项身体性、生理性、遗传性、精神性、经济性、文化性或社会性身份		生物识别信息
			地理位置数据
			专业或就业相关信息
			受保护的特征
			网络活动信息
			用户画像的推论
			商业信息
			教育信息
排除	匿名化信息[31]	匿名化信息	1.去识别化信息 2.汇总的消费者信息 3.可公开获取的信息 4.合法获得的、引起公众关注的真实信息[32]

不同类型个人信息的保护规则

对于特殊类型个人信息的规则，各法有共通之处也有显著的不同。**一方面，各部法律均对特殊类型数据（敏感个人信息）、未成年人个人信息的收集**

[31] 参见 GDPR 第四条。
[32] 《加州民法典》第 1798.140.（v）（2）

和处理制定了特别的规则。另一方面，在具体的处理规则上，各部法律存在明显差异,加州隐私法在规则上仍相对宽松。



敏感个人信息

	GDPR （第九条）	中国《个人信息保护法》 （第二十八条）	加州隐私法（CCPA&CPRA） （第 1798.100 条）
敏感信息定义	特殊类型数据（无概括性定义）	敏感个人信息是指一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息[33]。	列举“敏感个人信息”类别（无概括性定义）
敏感信息列举	种族或民族背景	特定身份	人种与民族信息
	工会成员的个人数据		工会会员身份
			社会保障、驾驶执照或护照号码
			个人通讯
	政治观念		
	宗教或哲学信仰	宗教信仰	宗教信仰
	基因数据	生物识别	遗传数据
	为了特定识别自然人的生物性识别数据		生物特征
	和自然人健康相关的数据	医疗健康	健康信息

[33] 《个人信息保护法》第二十八条

	和个人性生活或性取向相关的数据		有关性生活或性取向的信息
		金融账户	财务账户信息
		行踪轨迹	精确的地理位置
		不满十四周岁未成年人的个人信息	

敏感个人信息的处理规则

	GDPR （第九条）	中国《个人信息保护法》 （第二十八条）	加州隐私法（CCPA&CPRA） （第 1798.100 条）
处理的要求	特定情况下可以处理： 1.数据主体明确同意 2.处理对于数据控制者履行责任、保护数据主体权利、另一自然人的核心利益是必要的 3.非盈利机构的正当性活动 4.已经明显公开的相关个人数据的处理 5.司法活动 6.公共利益（包括医学、公共健康、科学或历史研究）	处理必须具有特定的目的和充分的必要性，并采取严格保护措施	
可公开获取的敏感个人信息		在合理范围内处理个人自行公开或者其他已经合法公开的个人信息不适用同意规则[34]	可公开获取的敏感个人信息不再是敏感个人信息或个人信息[35]，因此不适用相关的处理规则

[34] 《个人信息保护法》第十三条

[35] 《加州民法典》第 1798.140 条（ae）（3）：根据第 (v) 款第 (2) 项“公开”的敏感个人信息不应被视为敏感个人信息或个人信息。

同意规则	明确同意	取得信息主体的单独同意或书面同意[36]	无规定
自动化决策	只有在数据主体明确同意或者处理是对实质性公共利益是必要的情况下，才能利用此类数据进行对数据主体具有法律影响或类似严重影响的自动化决策。[37]	无规定	无规定
其他	无规定	法律、行政法规对处理敏感个人信息规定应当取得相关行政许可或者作出其他限制的,从其规定。[38]	无规定

其他

	GDPR （第九条）	中国《个人信息保护法》 （第二十八条）	加州隐私法（CCPA&CPRA） （第 1798.100、1798.121 条）
知情权	无特殊规则,适用一般类型个人数据的相关条款	处理敏感个人信息的必要性以及对个人权益的影响[39]	1.收集个人敏感信息的类别 2.收集或使用敏感个人信息的目的 3.该信息是否出售或共享。

[36] 《个人信息保护法》第二十九条
[37] GDPR 第二十二条
[38] 《个人信息保护法》第三十二条
[39] 《个人信息保护法》第三十条

限制处理请求权	无规定	无规定	1.消费者有权随时指示收集消费者敏感个人信息的企业将其对消费者敏感个人信息的使用限制在提供服务或商品所必需的范围内。[40] 2.企业需要在主页提供“限制使用或披露我的敏感个人信息”的链接。[41]
数据保护影响评估	**大规模处理**特定类型个人数据必须进行数据保护影响评估[42]	处理敏感个人信息应当进行个人信息保护影响评估[43]	无规定
数据保护官的任命	控制者或处理者的核心活动包含对某种特殊类型数据的**大规模处理**，则应当委任数据保护官。[44]	无规定	无规定

针对敏感个人信息的处理，GDPR 和中国《个人信息保护法》均采取了以禁止处理为原则，允许处理为例外的保护模式。GDPR 第九条规定，只有在数据主体明确同意、处理对于控制者履行责任以及行使其特定权利是必要的等情况下，才可以在采取合适与特定措施的前提下处理特殊类型个人数据。GDPR 第二十二条第四款还对利用特殊类型数据进行自动化决策提出了要求，只有在数据主体明确同意或者处理对公共利益是必要的情况下，才能利用此类数据进行对数据主体具有法律影响或类似严重影响的自动化决策。中国《个人信息保护法》也要求处理敏感个人信息必须具有特定的目的和充分的必要性，采取严格的措施，同时取得个人的单独同意。

---

[40] 《加州民法典》1798.121 条（a）：消费者有权随时指示收集消费者敏感个人信息的企业将其对消费者敏感个人信息的使用限制在符合一般消费者预期的，提供服务或商品所必需的用途或者执行第 1798.140 条第 (e) 部分第 (2)、(4)、(5) 和 (8) 段中规定的服务，并经授权根据第 1798.185 节 (a) 分节 (a) 第 (19) 节 (C) 项通过的法规。出于本条规定以外的目的使用或披露消费者敏感个人信息的企业应根据第 1798.135 条第 (a) 条向消费者发出通知，告知该信息可能会被使用或披露给服务提供商或承包商，用于其他特定目的，并且消费者有权限制使用或披露其敏感个人信息。

[41] 《加州民法典》1798.135 条（a）（2）： 在企业的互联网主页上提供一个清晰显眼的链接，标题为“限制使用我的敏感个人信息”，使消费者或消费者授权的人能够限制第 1798.121 节 (a) 部分授权的对敏感个人信息的使用和披露。

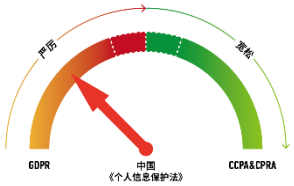
[42] GDPR 第三十五条

[43] 《个人信息保护法》第五十五条

[44] GDPR 第三十七条

此外，中欧立法对敏感信息处理过程也提出了额外的要求，对此类数据处理需展开隐私保护评估。

CPRA，则采取了对敏感信息处理课以特殊义务的方式加强保护，例如特殊的披露、告知义务，以及消费者的选择退出权、限制处理权等。



未成年人个人信息

针对未成年人个人信息的处理，GDPR 和中国《个人信息保护法》要求数据处理者必须获得父母的同意或授权，而 CCPA&CPRA 则仅要求企业在实际知悉消费者未满 16 岁的情况下，取得明确授权。GDPR 和中国《个人信息保护法》均未通过主观要件对企业的义务进行限制，考虑到网络环境下识别未成年人、监护关系和监护人存在一定的困难，强制要求所有网络服务都要满足监护人同意要求，也将带来超范围收集信息问题，产生新的数据安全隐患。

GDPR 第八条的适用进行了两方面的限制：1.仅在数据控制者为儿童“直接提供信息社会服务”的情况下，才适用第八条的特殊同意规则；2.控制者应当采取合理努力，结合技术可行性确保获得授权和同意。对于第二点，EDPB 的指南进一步明确，控制者应尽合理努力验证用户已超过数字同意年龄，这些措施应与处理活动的性质和风险相称，年龄验证不应导致过度的数据处理。[45]

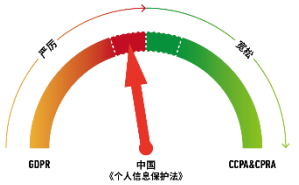
[45] **Guidelines 05/2020 on consent under Regulation 2016/679：https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf**

	GDPR （第八条）	中国《个人信息保护法》 （第三十一条）	加州隐私法（CCPA&CPRA） （第 1798.120 条（c））
儿童/未成年人信息	**基于个人同意的数据处理，当儿童不满 16 周岁（成员国可降低 13 周岁），只有当对儿童具有父母监护责任的主体同意或授权，此类处理才是合法的[46]。**	个人信息处理者处理不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的同意。 个人信息处理者处理不满十四周岁未成年人个人信息的，应当制定专门的个人信息处理规则。[47]。	要求实际知晓消费者年龄，排除了不知晓消费者年龄的情况： 如果企业**实际知悉消费者未满 16 岁**，则企业不得出售消费者的个人信息，除非消费者已满 13 岁且未满 16 岁，或未满 13 岁的父母或监护人已经明确授权销售其个人信息。故意无视消费者年龄的企业，视为实际知悉消费者年龄。[48]

[46] GDPR 第八条

[47] 《个人信息保护法》第三十一条

[48]《加州民法典》第 1798.120 条（c）：尽管有（a）小节的规定，但如果企业实际知悉消费者未满 16 岁，则企业不得出售消费者的个人信息，除非消费者已满 13 岁且未满 16 岁，或未满 13 岁的父母或监护人已经明确授权销售其个人信息。故意无视消费者年龄的企业，视为实际知悉消费者年龄。这项权利可以称为“选择加入的权利”



死者个人信息

GDPR 序言第二十七条明确，GDPR 不适用死者的个人数据，成员国可以对死者个人数据处理自行作出相关规定。而从欧盟各成员国的立法看，奥地利、比利时、荷兰、瑞典等国均未明确死者的个人信息保护问题；捷克、芬兰、德国、波兰等国的数据保护法明确规定，不适用死者的个人信息；丹麦、法国、意大利、西班牙等国家虽然对死者的个人信息保护作出了相关规定，但也存在一定的限制。例如，2018 年的《丹麦数据保护法》第 2 条第 5 款规定，该法与欧盟《一般数据保护条例》适用于死者死后十年内的个人数据的保护。同样，加州隐私法 CCPA&CPRA 也未对死者的个人信息保护做任何规定。

而中国《个人信息保护法》明确规定了近亲属在特定情形下可以行使死者的个人信息行使相关权利。

	GDPR （序言 Recital 第 27 条）	中国《个人信息保护法》 （第四十九条）	加州隐私法（CCPA&CPRA）
死者的个人信息	本条例不适用死者的个人数据，成员国可以对死者个人数据处理自行作出相关规定。[49]	自然人死亡的，其近亲属为了自身的合法、正当利益，可以对死者的相关个人信息行使本章规定的查阅、复制、更正、删除等权利；死者生前另有安排的除外。[50]。	无规定。

[49] GDPR 立法理由第 27 条（Recital 27）
[50] 《个人信息保护法》第四十九条

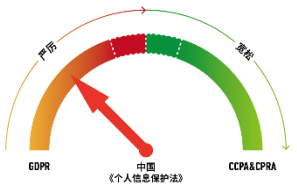
这是中国《个人信息保护法》的突破性规定，这一规定如在实践落地中过于宽松，可能会带来以下问题：

其一，允许死者的近亲属行使死者的个人信息权益，可能会明显违背死者生前的意愿。死者的个人信息尤其是隐私信息，是不愿意为他人所知悉的，即便是自己的近亲属也不例外，若规定近亲属可以对这些信息悉数行使查阅、更正修改，复制等权利，势必有悖保护死者的初衷。

其二，可能侵害第三人的隐私权。死者在生前通过电子邮箱或者即时通讯工具等与他人产生各种社会交往，相当一部分也将涉及到他人的隐私。而同时，他们通过电子方式进行的通信也属于通信秘密，受到宪法和法律的保护。不做任何限制的由死者的近亲属行使个人信息处理中的权利，也不利于保护第三人的隐私权。

甚者，近亲属可以行使死者的个人信息权益，如查询权、删除权，这方便了近亲属假借“死者”名义，与第三方通信互动，违背公序良俗，甚至滋生诈骗行为。

建议在后续落地中，能够与民法典保持一致，如《民法典》第 984 条的规定 “死者的姓名、肖像、名誉、荣誉、隐私、遗体等受到侵害的，其配偶、子女、父母有权依法请求行为人承担民事责任；死者没有配偶、子女且父母已经死亡的，其他近亲属有权依法请求行为人承担民事责任”，也即仅在“受到侵害”时，特定近亲属可以行使相关防御性权利，以避免造成社会秩序的混乱。立法者也正是考虑到这些因素，在公布的二审稿的基础上，继续对该条文予以了限定，包括：“近亲属为了自身的合法、正当利益”，死者的“相关个人信息”，以及“死者生前另有安排的除外”等。



匿名化、去识别化信息的规则

在确定个人信息的定义与范围上，还有一类非常重要的概念，包括：**匿名化信息（anonymous information）、假名化信息（Pseudonymisation）和去标识化信息（de-identified)。**

一方面，各部法律采取了不同的术语，并且在使用上有所差异：

GDPR 使用了匿名化和假名化两个概念。将匿名化信息定义为“已识别或可识别的自然人无关的信息或者以数据主体不可识别或不再可识别的方式匿名呈现的数据”，将假名化定义为“在采取某种方式对个人数据进行处理后，如果没有额外的信息就不能识别数据主体的处理”。前者不再适用 GDPR,后者仍作为个人信息，依旧适用 GDPR。

而 CCPA&CPRA 则采取了“去标识化”和 “假名化” 两个概念，将去识别信息化定义为“无法合理地用于推断特定消费者的信息或以其他方式链接到特定消费者的信息”，将假名化定义 “在不使用附加信息的情况下，个人信息不能再被关联到特定消费者” 的技术。

中国《个人信息保护法》则采取了匿名化和去标识化两个概念，中国《个人信息保护法》将匿名化定义为“个人信息经过处理无法识别特定自然人且不能复原的过程”，将去标识化定义为“个人信息经过处理，使其在不借助额外信息的情况下无法识别特定自然人的过程”。

从各法类比来看，关于匿名化概念，GDPR 与中国《个人信息保护法》接近。关于去标识化概念，CCPA&CPRA 中的去标识化范围最广泛，与《个人信息保护法》类似，同时也大致相当于 GDPR 中的假名化。但最大的区别是：CCPA&CPRA 将去标识化这一广义概念，全部排除在了法律的适用范围之外，而 GDPR 与中国《个人信息保护法》均未做排除。

	GDPR （第四条定义（5），序言 Recital 第二十六条）	中国《个人信息保护法》 （第四条、第七十三条）	加州隐私法（CCPA&CPRA） （加州民法典第 1798.140 条）
匿名化	排除匿名化信息（anonymous information）：匿名化信息是指已识别或可识别的自然人无关的信息或者以数据主体**不可识别或不再可识别的方式匿名呈现**的数据。匿名化信息不是 GDPR 的调整范围。	排除匿名化信息：匿名化，是指个人信息经过处理**无法识别特定自然人且不能复原的过程**。个人信息不包括匿名化处理后的信息。	
假名化	1. “假名化”指的是在采取某种方式对个人数据进行处理后，**如果没有额外的信息就不能识别数据主体的处理方式**。 2.此类额外信息应当单独保存，并且已有技术与组织方式确保个人数据不能关联到某个已识别或可识别的自然人。 3.假名化信息依然是 GDPR 的调整范围，但是相较于未进行假名化处理的个人数据，假名化信息适用更为宽松的处理规则。[51]		“假名处理”或“假名化”是指以如下这种方式处理个人信息：在不使用附加信息的情况下，个人信息不能再被关联到特定消费者，但附加信息应单独保存，并应采取技术和组织措施确保个人信息不能再被关联到已识别或可识别的消费者。[52]
去标识化		去标识化（de-identified），是指个人信息经过处理，**使其在不借助额外信息的情况下**无法识别特定自然人的过程。[53]	排除去标识化（de-identified)的消费者个人信息：“去识别化”是指**无法合理地用于推断特定消费者的信息或以其他方式链接到特定消费者的信息**，此类信息不是 CCPA&CPRA 的保护范围。[54]

[51] GDPR 第四条定义（5），及引言立法理由第二十六条（Recital 26）
[52] 《加州民法典》第 1798.140 条（aa）项
[53] 《个人信息保护法》第四条，第七十三条
[54] （加州民法典第 1798.140 条(m) “去识别化”是指不能合理地用于推断有关特定消费者的信息或以其他方式链接到特定消费者的信息，前提是拥有该信息的企业：
(1) 采取合理措施确保信息不会与消费者或家庭相关联。
(2) 公开承诺以去标识化的形式维护和使用信息，并且不尝试重新识别信息，除非企业可能仅为了确定其去识别化过程是否满足本节的要求而尝试重新识别信息。
(3) 根据合同，信息的任何接收者有义务遵守本分部的所有规定。
（加州民法典第 1798.140 条（o）（3）：“个人信息”不包括去识别化或集合的消费者个人信息。

加州 CCPA&CPRA:

大多数美国学者认为，去标识化和匿名化具有不同的含义，去标识化是一个边界明确的过程，而匿名化本身只是一种目标，而不是一种方法且并不意味着一个标准，也不指定需要做什么来实现该目标。[55]因此美国 CCPA&CPRA，HIPPA 等立法中，均采用了去标识化的用语，HIPPA 明确了去识别化的具体方法，例如在 HIPAA 确定的去识别化途径中，安全港规则规定只要消除 18 种列举的个人标识符（姓名、小于州的地理位置信息、相关的日期、手机号码、设备识别码和序列号、传真号码、邮箱地址、URLs、社保号码、IP 地址、医疗记录号码、生物识别码、健康计划号码、全脸照片和类似的图片、账号、资格证/执照号码。）则该信息应当被视为去标识化信息。[56]

CCPA&CPRA 直接将去标识化信息排除于其适用范围之外，去标识化的具体要求包括：（1）已实施了技术保障措施，禁止重新识别信息所属的消费者；（2）已实施了明确禁止重新识别信息的业务流程；（3）已实施业务流程以防止无意中发布已识别的信息；（4）不尝试重新识别身份信息。

因此，与 GDPR 在背景部分关于匿名化数据的抽象介绍和相关的指南解读中确立的高门槛相比，CCPA&CPRA 沿袭了美国隐私立法的传统，从技术措施和管理流程着手，使得判断标准更为明确和易于操作。[57]这一方式有利于激励企业采取去标识化技术以实现保障数据安全和数据利用的双重目标。

GDPR，中国《个人信息保护法》:

在 GDPR 的语境下，匿名化和假名化是两种不同的技术，区别在于数据是否可以被重新识别，匿名化要求该信息无法再识别到特定自然人。欧盟第 29 条工作组在其意见中指出，真正的数据匿名化是一个极高的标准，数据控制者往往无法真正实现数据的匿名化[58]。各国的数据保护机构也提示企业希望通过匿名化技术规避 GDPR 的适用可能面临较大的风险。而中国《个人信息保护法》中匿名化和去标识化的术语从内涵上更类似于 GDPR 的匿名化与假

[55] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5977668/
[56] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5977668/
[57] 王融：《美欧隐私立法是否走向趋同，加州 CCPA 给出答案》，腾讯研究院微信公众号，2019 年 9 月 26 日：https://mp.weixin.qq.com/s/JLrrsGRSXwzECLbZ0la33w
[58] EU WP 29 :Opinion 05/2014 on Anonymisation Techniques：https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

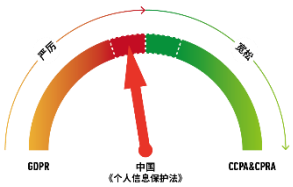
名化。

中国《个人信息保护法》虽然区分了匿名化信息和去标识化信息，并明确匿名化信息不再属于中国《个人信息保护法》保护的个人信息，但是针对去标识化信息并未规定特殊的处理规则。

三、合法性基础

由于适用范围的不同，各部法律在确立数据处理合法性基础方面存在重要差别。GDPR 和中国《个人信息保护法》作为通用性法律，更为全面的列出了合法性基础,但同时，前者给出的合法理由更为周延。

CCPA&CPRA 由于仅适用于企业收集、出售和披露个人信息的场景，因此其合法性基础更为简单明确，且符合美国法一直以来贴合实践的传统，在同意机制方面，也主要仍采取了选择退出模式（opt-out）。

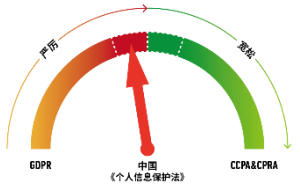


合法性基础的范围

GDPR （第六条）	个人信息保护法 （第十三条）	加州隐私法（CCPA&CPRA） （第 1798.120 条）
数据主体的同意	信息主体的同意	Opt-out 为主要机制
履行合同所必要	订立或者履行个人作为一方当事人的合同所必需	无规定
数据控制者履行法定义务所必需	为履行法定职责或者法定义务所必需	
保护数据主体或另一自然人的核心利益所必要	紧急情况下为保护自然人的生命健康和财产安全所必需	
处理是为了公共利益或基于官方权威而履行义务	公共利益：为应对突发公共卫生事件，为保护自然人的生命健康和财产安全所必需；为公共利益实施新闻报道、舆论监督等	
控制者或第三方的正当利益（不违背数据主体的优先性理由、基本权利与自由）	依照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需	
	在合理的范围内处理个人自行公开或者已经合法公开的个人信息	不适用于可公开获取的信息以及合法获得的、引起公众关注的真实信息。[59]

[59] 《加州民法典》1798.140.（v）（2）：“个人信息”不包括公开可用的信息或合法获得的、真实的、引起公众关注的信息。

比较中国《个人信息保护法》第十三条和 GDPR 第六条列举的合法性基础可以发现，**中国《个人信息保护法》和 GDPR 都将知情同意、履行合同所必需、履行法定义务所必需等作为合法性基础，但是中国《个人信息保护法》并未笼统的借鉴 GDPR 中关于“控制者或第三方的正当利益”作为合法性基础，而仅是认可了一种正当性——人力资源管理的需要，这大大压缩了理论上可以具有合法性的情形。**个人信息保护涉及三个方面的利益，即信息主体的个人利益、与个人信息处理紧密结合的信息使用者（数据控制者）的利益和公共利益，个人信的保护必须恰当考虑三重价值和利益的实现，才能构建正当合理的个人信处理法律基础。[60]中国《个人信息保护法》简化处理个人信息的合法性基础，看似偏重个人权益的保护，但在落地中可能会带来新的问题，即很多理论上具有正当性的数据处理可能将陷于于法无据的情形。



同意规则

依照规则愈加严苛的程度排序，依次为加州隐私保护法（CCPA&CPRA），欧盟 GDPR,中国《个人信息保护法》。

1.中国《个人信息保护法》最为严苛，其与欧盟 GDPR 都采取了选择加入（opt-in）模式，即以个人同意作为数据处理合法性理由的，非经个人同意，不得对其个人信息进行处理，并且都对同意的有效性提出了实质性要求，即自愿，明确，充分知情。而加州隐私法仍以选择退出（opt-out）为主要模式，即除非用户拒绝或退出，则公司可以继续处理用户的个人信息，这体现了美国一直以来在数据保护方面的务实思路。

2.在对同意作出高标准要求的同时，中国《个人信息保护法》提出了比欧盟 GDPR 更细致严格的要求。《个人信息保护法》区分了同意、单独同意和

[60] 高富平：《个人信息上使用的合法性基础——数据上利益分析视角》，载《比较法研究》2019 年第 2 期。

书面同意等情形：在向他人提供个人信息、公开其所处理的个人信息、所收集的个人图像、身份识别信息用于维护公共安全以外的目的，处理敏感个人信息都需要获得个人的单独同意，而法律、行政法规规定应当取得书面同意的情况下应当取得书面同意。而 GDPR 除了对同意提出一些实质性要求，如“充分知情的”“无争议的”外，并无类似要求。

	GDPR （第四条、第七条、第九条）	个人信息保护法 （第二章第一节部分）	加州隐私法（CCPA&CPRA） （第 1798.120 条、1798.140（h））
同意模式	选择加入（opt-in）	选择加入（opt-in）	选择退出（opt-out）
同意的要求	数据主体的“同意”指的是数据主体通过一个声明，或者通过某项清晰的确信行动而**自由**作出的、**充分知悉的**、**不含混的**、表明同意对其相关个人数据进行处理的意愿。	**充分知情、自愿、明确**[61]	“同意”是指消费者或消费者的法定监护人、拥有授权书的人或作为消费者保护人的人自愿作出的、具体的、知情的和明确的消费者意愿指示。
同意类型	处理特殊类型数据：明确同意[62]	同意	无对应条款
		单独同意： （1）向他人提供个人信息； （2）公开处理的个人信息 ； （3）所收集的个人图像、身份识别信息用于维护公共安全以外的目的； （4）处理敏感个人信息； （5）向境外提供个人信息；	
		书面同意：法律、行政法规规定处理敏感个人信息应当取得个人书面同意的。	

[61] 《个人信息保护法》第十四条。
[62] GDPR 第九条第二款

目前 GDPR 生效已经有三年的时间，其所倡导的选择加入模式也展现出了两方面的影响。NBER 的一项调查显示：一方面，在选择加入模式下，Cookie 总数减少了约 12.5%，这表明消费者正在利用 GDPR 要求增加的退出功能；另一方面，没有选择退出的消费者表现出了更持久的可追踪性，在 GDPR 下，消费者的可追踪性提高了 8%。[63]

四、个人信息的跨境提供

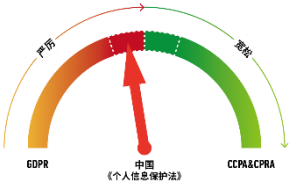
在数字经济时代，跨境数据流动成为备受关注的议题。因本报告讨论的四部法律中，由于 CCPA&CPRA 是州层面的隐私保护立法，因此不涉及到个人信息的跨境提供问题。而 GDPR 和《个人信息保护法》均构建了个人信息跨境提供制度框架：欧盟 GDPR 从保障基本权利的角度出发，规定了允许个人数据转移的两种基本场景和八种例外情况；而中国《个人信息保护法》则主要从网络安全和数据主权出发，规定了可以向境外提供个人信息的四种条件，以及特定情况下的数据本地化要求，即关键信息基础设施运营者和处理个人信息达到国家网信部门规定数量的个人信息处理者，应当将在中华人民共和国境内收集和产生的个人信息存储在境内。其具体标准还有待于进一步细化。

[63] The Effect of Privacy Regulation on the Data Industry: Empirical Evidence from GDPR | NBER

	GDPR (第五章)	个人信息保护法 （第三章）	加州隐私法 （CCPA&CPRA）
向境外提供个人数据的条件	具有充足保护[64]		无相关规定
	控制者或处理者提供适当的保障措施[65]（包括公共机构或实体之间具有法律约束力并可执行的文件、有约束力的公司规则[66]、标准合同条款等）	按照国家网信部门制定的标准合同与境外接收方订立合同，约定双方的权利和义务	
		通过国家网信部门组织的安全评估	
		按照国家网信部门的规定经专业机构进行个人信息保护认证；	
		法律、行政法规或者国家网信部门规定的其他条件	
	其他特殊情况： 1.数据主体被明确告知后的明确同意 2.履行合同所必须； 3.对于实现数据主体的利益是必要的； 4.对于实现公共利益是必要的； 5.对于确立、行使或辩护法律性主张是必要的； 6.为了保护数据主体或其他人的关键利益是必要的； 7.转移是根据登记册而进行的 8. 转移是非重复性的；关乎很小一部分数据主体的权利；对于实现控制者压倒性的正当利益是必要的……[67]		
数据主	控制者期望将数据转移到第三国或国际组织的事实、欧盟	境外接收方的**名称或者姓名、联系方式、**处理目的、处	无相关规定

[64] GDPR 第四十五条
[65] GDPR 第四十六条
[66] GDPR 第四十七条
[67] GDPR 第四十九条

体的知情权	委员会作出或未作出充分决定的事实，采取的适当保障措施的参考资料、获取它们备份的方式，或者在哪里可以获取它们。[68]	理方式、个人信息的种类以及个人向境外接收方行使本法规定权利的方式和程序等事项	
数据本地化要求	无境内存储的强制要求	关键信息基础设施运营者和处理个人信息达到国家网信部门规定数量的个人信息处理者，应当将在中华人民共和国境内收集和产生的个人信息存储在境内。	无境内存储的强制要求



数据本地化和出境安全评估

需关注到，相比《网络安全法》，《个人信息保护法》扩展了适用于数据本地化的主体，即除了关键信息基础运营者以外，还增加了个人信息达到国家网信部门规定数量的个人信息处理者。

对于这两类以外的其他个人数据处理者，则扩充了数据出境的合规路径，包括：

（一）依照本法第四十条的规定通过国家网信部门组织的安全评估；

（二）按照国家网信部门的规定经专业机构进行个人信息保护认证；

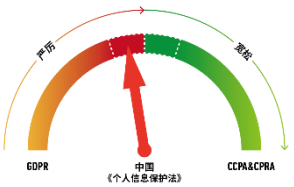
（三）按照国家网信部门制定的标准合同与境外接收方订立合同，约定双方的权利和义务；

（四））法律、行政法规或者国家网信部门规定的其他条件。

中华人民共和国缔结或者参加的国际条约、协定对向中华人民共和国境外提供个人信息的条件等有规定的，可以按照其规定执行。

此外，对于境外接收方的披露和同意要求，《个人信息保护法》的要求也较高，包括：境外接收方的名称或者姓名、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外接收方行使本法规定权利的方式等事项，并取得个人的单独同意。

[68] GDPR 第十三条



跨境证据调取

数据跨境流动有两个场景，一是伴随着数字服务的全球化，数字贸易场景下的数据流动，发生在商业主体之间或内部，是大规模而持续的；二是执法协作场景中的数据跨境，发生在国家执法部门与商业主体之间，相对个案偶发。GDPR 和《个人信息保护法》均对境外执法部门调取存储在本国的数据进行了限制。同样，加州隐私法作为州法律，并没有涉及此类规定。[69]

GDPR 第四十八条规定："任何法庭判决、仲裁裁决或第三国行政机构的决定，若要求控制者或处理者对个人数据进行转移或披露，同时满足以下条件时方能得到认可或执行：一是该判决、裁决或决定必须基于提出请求的第三国与欧盟或其成员国之间订立的法律互助协议等国际条约，二是该判决、裁决或决定不会对本章规定的其他转移形式产生消极影响"。

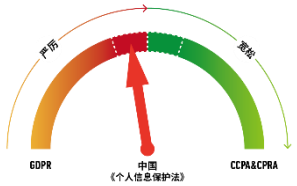
《个人信息保护法》第四十一条规定了境外司法和执法机构跨境调取境内个人信息的规则："中华人民共和国主管机关根据有关法律和中华人民共和国缔结或者参加的国际条约、协定，或者按照平等互惠原则，处理外国司法或者执法机构关于提供存储于境内个人信息的请求。非经中华人民共和国主管机关批准，个人信息处理者不得向外国司法或者执法机构提供存储于中华人民共和国境内的个人信息"。这一规定体现出我国对国家主权和安全利益的考量，但是相关的批准程序、法律责任还有待配套的法律法规进一步细化。

此外，《个人信息保护法》第四十二条还明确了限制或禁止提供个人信息的黑名单制度。

---

[69] 美国主要通过《澄清域外合法使用数据法案》（CLOUD 法案）构建跨境取证体系，由于篇幅所限本报告对此不作展开。如需了解详情，可参见 2019 年腾讯研究院数据治理报告——《云深处的数据规则——CLOUD 法案与它的蝴蝶效应》，链接：https://mp.weixin.qq.com/s/Esku27Tuab8XLQH8-BNiBg

五、信息主体权利



知情权

GDPR 与《个人信息保护法》规定的知情信息范围更为全面，且后者进一步对提供的环节予以更高的要求：应当在信息处理之前向信息主体提供此类信息，这与个人信息处理与处理规则披露往往同步发生的实际情况有所脱节。

对于披露个人信息的接收方，GDPR 与 CCPA&CPRA 都允许仅披露接收者的类型，而中国《个人信息保护法》要求更高，要求披露到个人信息处理者的具体姓名/名称，和联系方式。这将为规则的实际落地带来更大挑战，数字服务往往涉及了多方数据主体的参与，以数字广告为例，在一次自动化的广告需求和广告位的匹配中，广告主、数据管理平台、第三方数据提供商、广告验证和归因提供商等主体在短时间内（毫秒级）处理大量的个人信息，要求处理者对所有参与方的身份信息在事前予以详实披露，仍需要在实践中探索可行方案。

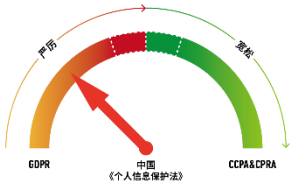
CCPA&CPRA

CCPA&CPRA 规定的消费者知情权的范围比较有限，在实践中也更具可操作性。其区分收集和出售个人信息的场景，分别规定了消费者的知情权内容。

		GDPR （第十三条）	中国《个人信息保护法》 （第十七条）	加州隐私法（CCPA&CPRA） （1798.100 条、1798.110 条、1798.115、1798.130 条）
收集个人信息时的知情权	内容	包括控制者的身份、联系方式、处理的目的及法律基础、**个人数据接收者或接收者的类型**、数据转移到第三国或国际组织欧盟委员会做出的充分性决定、个人数据存储期限、相关权利等几乎所有相关信息[70]	个人信息处理者的名称或者姓名和联系方式、处理目的、处理方式，个人信息种类、保存期限、 个人行使权利的方式和程序、其他事项[71]	重点强调信息的类别：个人信息类别、来源类别、经营或商业目的、信息是否会被出售或共享、收集有关个人信息的具体部分、储存期限。[72]
	方式	简洁、透明、易懂和容易获取的形式，以清晰和平白的语言来提供[73]	显著方式、清晰易懂的语言	1.消费者要求提供相关信息：应向消费者提供两种或两种以上指定的提出请求的方式，其中须包括通过免费电话提出请求的方式[74] 2.需要通过在线隐私政策披露一个或多个最能准确描述过去 12 个月内收集的个人信息的类别清单 3.控制消费者个人信息的第三方企业 ，可通过在其网站主页的显著位置提供要求的信息[75]
	时间	获得个人数据后的合理时间；特殊情况下至少在一个月内	个人信息处理者在处理个人信息前	在收到消费者可以核实的请求后 45 日内提供相关信息；在线隐私政策至少每 12 个月更新一次

[70] GDPR 第十三条
[71] 《个人信息保护法》第十七条
[72] 《加州民法典》第 1798.100、1798.110 条
[73] GDPR 第十二条
[74] 《加州民法典》第 1798.130 条
[75] 《加州民法典》第 1798.100 条

向他人提供个人信息时的知情权	内容	个人信息的接收者或接收者的**类型**	**接收方的名称或者姓名**、联系方式、处理目的、处理方式和个人信息的种类[76]	重点强调信息的类别： （1）收集的个人信息类别。 （2） 出售的个人信息类别，以及根据个人信息类别区分的出售个人信息的**第三方类别**。 （3） 企业出于商业目的披露的消费者个人信息类别。
	时间	如果个人数据可以合法地披露给其他接收者，则最晚应在首次向接收者披露个人数据时告知数据主体。[77]	无规定	在收到消费者可以核实的请求后 45 日内提供相关信息；在线隐私政策至少每 12 个月更新一次



访问权（查阅权）

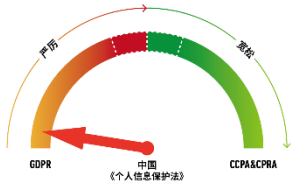
在访问权方面，GDPR 和中国《个人信息保护法》的规定较为类似。可访问信息较为全面，与知情权范围基本重合。

CCPA&CPRA 则从时间和访问频率上对访问权进行了限制，《加州民法典》第 1798.130 条明确，企业没有义务在 12 个月内向同一消费者提供两次以上第 1798.110 节和第 1798.115 节规定的信息。

[76] 《个人信息保护法》第二十三条
[77] GDPR 第十四条（3）（c）

	GDPR （第十五条）	中国《个人信息保护法》 （第四十五条）	加州隐私法（CCPA&CPRA） （第 1798.110、1798.115、1798.130 条）
访问权的范围	处理的目的；	个人有权向个人信息处理者查阅、复制其个人信息	经营或商业目的
	相关个人数据的类型		个人信息类别
	个人数据已经被或将被披露给接收者或接收者的类型		信息是否会被出售或共享
	个人数据将被储存的预期期限（如果不可能的话，确定此期限的标准）		储存期限（或确定期限的标准）
	数据主体的权利（包括向监管机构进行申诉的权利）		
	数据来源的任何信息（当个人数据不是从数据主体那里收集的）		来源类别[78]
	自动化决策的相关信息[79]（详情见本报告第七部分）		
			收集有关个人信息的具体部分
例外		法律、行政法规规定应当保密或者不需要告知的；国家机关为履行法定职责处理个人信息，按照法律、行政法规应当保密或不需要告知的，或者告知将妨碍国家机关履行法定职责的。[80]	企业没有义务在 12 个月内向同一消费者提供两次以上相关信息。[81]

[78] 《加州民法典》第 1798.110、1798.115 条
[79] GDPR 第二十二条
[80] 《个人信息保护法》第十八条第一款、第三十五条
[81] 《加州民法典》第 1798.130 条（b）：企业没有义务在 12 个月内向同一消费者提供两次以上第 1798.110 节和第 1798.115 节规定的信息。



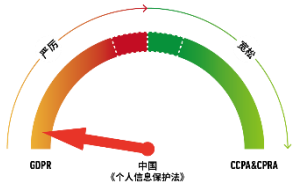
反对权/撤回权

从反对权行使范围看，GDPR 规定的反对权的范围最广泛，在基于数据主体的同意、公共利益、控制者或第三方的正当利益处理个人数据的情况下，均可行使反对权。中国《个人信息保护法》规定可以在基于个人同意处理个人信息的处理活动中，以及自动化决策活动中行使反对权。CCPA&CPRA 则仅限于出售或共享个人信息的情况。

	GDPR （第七条、第二十一条、第二十二条）	中国《个人信息保护法》 （第十五条）	加州隐私法（CCPA&CPRA） 第 1798.120 条
行使反对权的情形	数据主体应当有权随时撤回其同意。[82]	基于个人同意而进行的个人信息处理活动，个人有权撤回其同意。	对于向第三方出售或共享其个人信息的企业，消费者有权随时要求其不得出售或共享其个人信息（**选择退出权**）。
	处理是数据控制者为了公共利益或基于官方权威而履行某项任务而进行的[83]		
	处理对于控制者或第三方所追求的正当利益是必要的		
	因为直接营销目的而处理个人数据[84]		
	完全依靠自动化处理——包括用户画像——对数据主	1.通过自动化决策方式进行商业营销、	

[82] GDPR 第七条
[83] GDPR 第二十一条
[84] GDPR 第二十一条

	体做出**具有法律影响或类似严重影响的决策。**[85]	信息推送[86] **2.通过自动化决策方式作出对个人权益有重大影响的决定[87]**	



删除权

1. CCPA&CPRA 并未规定删除权行使的具体情形，而中国《个人信息保护法》和 GDPR 则明确列出了删除权行使的具体情形，且列举情况基本相同。

2.对于删除权的例外，CCPA&CPRA 规定的例外情况最为广泛，GDPR 次之，中国《个人信息保护法》删除权行使的例外情形较为有限。CCPA&CPRA 和 GDPR 均规定了言论自由、法律程序、科学研究和法定义务等情形作为删除权行使的例外，CCPA&CPRA 还将履行合同所必须、侦测安全事故、调试以识别和修复损害现有预期功能的错误、符合消费者预期的内部使用作为删除权行使的例外。中国《个人信息保护法》则仅规定了保存期限为届满和技术上无法实现作为例外。

3.GDPR 在删除权基础上，进一步提出了超出请求权边界的对世权——被遗忘权，这在 CCPA&CPRA 与《个人信息保护法》中均未有体现。

整体上看，CCPA&CPRA 删除权的制度设计充分考虑到了个人和企业之间的利益平衡，在保障消费者删除权的同时兼顾了企业的正当利益。

---

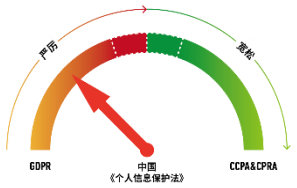
[85] GDPR 第二十二条
[86] 《个人信息保护法》第二十四条第二款
[87] 《个人信息保护法》第二十四条第三款

	GDPR （第十七条）	中国《个人信息保护法》 （第四十七条）	加州隐私法（ CCPA&CPRA） （1798.105 条）
行使情形	个人数据对于实现其被收集或处理的相关目的不再必要	处理目的已实现、无法实现或者为实现处理目的不再必要；	消费者请求删除作为前提：企业收到要求删除个人信息的可经验证的消费者要求应当在其记录中删除消费者个人信息88
	数据主体撤回同意且无其他合法性基础；	个人撤回同意；	
	数据主体行使反对权；		
	已经存在非法的个人数据处理	个人信息处理者违反法律、行政法规或者违反约定处理个人信息	
	为了履行欧盟或成员国法律为控制者所设定的法律责任个人数据需要被擦除		
	已经收集了第 8（1）条所规定的和提供信息社会服务相关的个人人数据[89]		
		个人信息处理者停止提供产品或者服务，或者保存期限已届满	
		法律、行政法规规定的其他情形	
删除权的限制	为了行使表达自由和信息自由的权利；		保障另一消费者行使他/她的该消费者的言论自由的权利，或行使法律赋予的其他权利
	基于公共利益，履行法定职责		
	公共健康		
	公共利益、科学或历史研究或统计目的处理中的安全保障与克减		科学、历史或统计的为公众利益的研究

[88] 《加州民法典》第 1798.105 条（c）（1）：根据本条（a）款之规定 ，企业收到要求删除个人信息的可经验证的消费者要求应当在其记录中删除消费者个人信息并通知任何服务提供商或承包商从他的记录中删除该消费者个人信息并通知所有其出售或共享个人信息的第三方删除该消费者个人信息，除非证明此做法不可行或涉及过多的工作。

[89] GDPR 第十七条

情形	为了提起、行使或辩护法律性主张		
		法律、行政法规规定的保存期限未届满	
		删除个人信息从技术上难以实现的	
			遵守法律义务
			产品召回 ，提供其要求的商品或服务、履行合同
			为侦测安全事故、防止恶意的、诈骗的、欺诈的或非法活动一或者对上述行为负有责任的人追责。
			调试以识别和修复损害现有预期功能的错误。
			合法的内部使用



复制权/可携权

1.各法均在复制权（访问权）基础上，延伸规定了可携带权。

2.对于可携带权，美欧立法均强调了技术可行这一前提，这也更符合实践。可携权的推进，需要数据处理者之间就技术支持标准展开探索。

3.GDPR 在条文中对哪些数据可以适用数据可携，作出了明确的限定——即建立在同意或合同的合法性基础上自动化处理数据，其他场景所处理的数据并不适用。

4.考虑到可携带来的数据安全问题，加州隐私立法强调了企业支持消费者数据可携的请求，应当是在可核实身份的请求的前提下。GDPR 也明确排除了对他人隐私保护等权利产生负面影响的情形不适用可携。

相较而言，《个人信息保护法》关于可携的规定，较为开放，具体的行使条件授权国家网信部门制定。考虑到《个人信息保护法》同欧盟 GDPR 一样，是一部综合性通用性法律，适用于公私领域各个机构，包括国家机关，医院、银行等，这些主体之间的数据可转移问题，本身就更为复杂。事实上，可携权一直是一个比较有争议的话题，涉及第三方用户的隐私保护、数据安全以及市场竞争问题，迄今为止并没有明确定论。即便是最早引入数据可携的欧盟 GDPR，到目前为止也没有落地的具体方案。

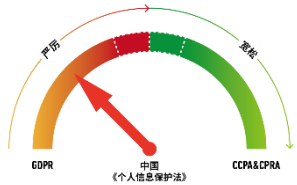
实践中，有大量的个人信息涉及他人的隐私保护，例如手机通信录，通话记录、聊天信息转账记录，如果赋予一方用户直接转移此类信息的权利，信息中涉及的其他个人根本没有机会得知自己的数据被他人提交给了新的数据处理者，从而也没有机会行使自己的权利。即使在一个企业内部不同业务之间，支撑用户直接转移此类信息，也可能会引发严重的隐私保护问题。例如：Google 曾擅自默认用户将 google　gmail 的通信录信息，直接转移至其社交业务 google buzz，从而被 FTC 施以重罚。从相互独立的 A 平台到 B 平台的转移过程中，在传输方和接收方之间如何分配责任？谁最终对转移的数据安全负责？在这些问题没有解决之前，贸然引入可携权，可能会带来更大的安全隐患。FACEBOOK 丑闻事件暴露的问题之一，就在于平台对用户将个人数据披露、迁移给第三方的政策过于开放，从而最终导致安全事件。

	GDPR (第二十条)	中国《个人信息保护法》 （第四十五条）	加州隐私法（CCPA&CPRA） （1798.130 条）
行使可携权的情形	1.处理是建立在数据主体的同意的基础上的，或者6（1）条所规定的合同的基础上的； 2.处理是通过自动化方式的。	个人请求将个人信息转移至其指定的个人信息处理者符合国家网信部门规定的条件	规定：收到消费者可验证的请求[90]
可携权的要求（复制）	数据主体有权获得其提供给控制者的相关个人数据，且其获得个人数据应当是经过**整理的、普遍使用的和机器可读的**	个人请求查阅、复制其个人信息的，个人信息处理者应当及时提供。	企业应当以**普通消费者易于理解的格式**，并在技术上可行的范围内，以**结构化的、常用的、机器可读的格式**提供从消费者那里获得的特定个人信息
可携权的要求（转移至另一个处理者）	1. 数据主体有权无障碍地将此类数据从其提供给的控制者那里传输给给另一个控制者。 2.如果技术可行，数据主体应当有权将个人数据直接从一个控制者传输到另一个控制者。	个人请求将个人信息转移至其指定的个人信息处理者，符合国家网信部门规定的条件的，个人信息处理者应当提供**转移的途径**	消费者提出的传输给另一个实体请求也应当无阻碍地被实现
可携权的限制	1. 可携权的行使不能影响第 17 条的规定（被遗忘权） 2. 控制者为了公共利益，或者为了行使其被授权的官方权威而进行的必要处理，这种权利不适用。 3. 不能对他人的权利或自由产生负面影响。	网信部门规定的条件	无规定

[90] 《加州民法典》第 1798.130 条（a）（3）(A)：根据第 1798.110 或 1798.115 节收到可验证的消费者请求的企业应直接或间接（包括通过或由服务提供商或承包商）向消费者披露其收集的有关消费者的任何个人信息……(B)（iii）:以普通消费者易于理解的格式，并在技术上可行的范围内，以结构化的、常用的、机器可读的格式提供从消费者那里获得的特定个人信息，消费者提出的传输给另一个实体请求也应当无阻碍地被实现.

六、信息处理者的义务

对于信息处理者的义务设定，中欧立法更为详尽，体现了合规清单（check list ）思路。GDPR 和中国《个人信息保护法》均通过独立的章节规定了信息处理者（或数据控制者、处理者）的义务，主要包括：采取安全保障措施的义务、发生数据安全事件时的通知义务、隐私保护影响评估、任命数据保护官等的义务，而 CCPA&CPRA 则仅在 1798.100 条笼统提出采取安全措施的要求。

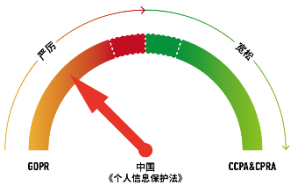


采取安全保障措施的义务

各法规定具有相似性，即强调根据个人信息处理的风险，采取与之相适应的安全保障措施。在列举的具体措施方面，《个人信息保护法》相较于 GDPR 更为细致全面，明确了个人信息处理者对个人信息应当实行分级管理、对从业人员定期展开安全培训。

	GDPR （第三十二条）	中国《个人信息保护法》 （第五十一条）	加州隐私保 CCPA/CPRA （第 1798.181.5 条）
采取安全措施的考虑因素	1.**最新水平、实施成本、处理的性质、处理的范围、处理的语境与目的**之后，以及处理给自然人权利与自由**带来的伤害可能性与严重性；** 2．在评估合适的安全级别的时候，应当特别考虑**处理所带来的风险**，特别是在个人数据传输、储存或处理过程中的的意外或非法销毁、丢失、篡改、未经授权的披露或访问。	个人信息处理者应当根据**个人信息的处理目的、处理方式、个人信息的种类以及对个人的影响、可能存在的安全风险等**，采取措施确保个人信息处理活动符合法律、行政法规的规定，并防止未经授权的访问以及个人信息泄露、篡改、丢失：	收集消费者个人信息的企业应根据按照**个人信息的性质**实施合理的安全程序和做法 [91]
具体的安全措施	个人数据的匿名化和加密	采取相应的加密、去标识化等安全技术措施；	无具体规定
	保持处理系统与服务的保密性、公正性、有效性以及重新恢复的能力	合理确定个人信息处理的操作权限，并定期对从业人员进行安全教育和培训；	
	在遭受物理性或技术性事件的情形中，有能力恢复对个人数据的获取与访问		
	具有为保证处理安全而常规性地测试、评估与评价技术性与组织性手段有效性的流程		
		制定并组织实施个人信息安全事件应急预案；	
		对个人信息实行分类管理；	
		制定内部管理制度和操作规程；	
		法律、行政法规规定的其他措施。	

[91] 《加州民法典》第 1798.100 条（e）项：收集消费者个人信息的企业应根据第 1798.181.5 条按照个人信息的性质实施合理的安全程序和做法 ，以保护个人信息免遭未经授权的或非法的访问、破坏、使用、修改或披露。1798.81.5 条(b)： 拥有、许可或维护加州居民个人信息的企业应实施和维护适合信息性质的合理安全程序和做法，以保护个人信息免遭未经授权的访问、破坏、使用、修改、 或披露。



保存（储存）期限

各部法律均关注了个人信息的保存期限，但是在具体的规则设计上有所不同：

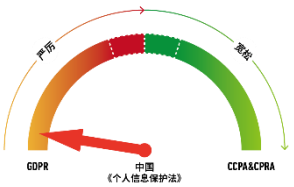
（1）明确保存期限不得超过实现处理目的所必需的时间，但《个人信息保护法》在这一基础上进一步提出了“最短”时间的要求。

（2）从保存期限的例外来看，GDPR 规定了公共利益、保障数据主体权利等例外，《个人信息保护法》则以法律、行政法规另有规定进行概括。

（3）从涉及储存期限的信息主体权利来看，各部法律中信息主体的知情权均包括个人信息储存期限（或储存期限的确定标准），而《个人信息保护法》中删除权的情形也包括保存期限届满。

	GDPR （第五条、第二十三条）	个人信息保护法 （第十九条）	加州隐私法(CCPA&CPRA) 第 1798.100 条
保存期限的要求	限期储存： 1.个人数据储存时间不得超过实现其处理目的所必需的时间；[92] 2.储存期限的制定需要考虑处理的性质、范围和目的或处理类型[93]	最短保存期限：个人信息的保存期限应当为实现处理目的所必要的最短时间。	合理储存期限：1.企业储存消费者个人信息 ，应当是合理、必要 ，以及与收集或处理个人信息的目的相符的[94] 2.企业不得储存消费者个人信息或个人敏感信息超过披露目的所需的合理时间[95]
例外情况	为了实现公共利益、科学或历史研究目的或统计目的，为了保障数据主体的权利和自由，并采取了合理技术与组织措施。	法律、行政法规对个人信息的保存期限另有规定的，从其规定。	
涉及储存期限的信息主体权利	知情权、访问权——个人数据将被储存的期限，以及确定此期限的标准[96]	知情权：个人信息处理者应当告知信息主体个人信息的保存期限[97]	知情权：收集消费者个人信息的企业应当在收集个人信息时告知储存期限或确定储存期限的标准。
		删除权：保存期限届满作为删除权行使的条件之一[98]	

[92] GDPR 第五条
[93] GDPR 第二十三条
[94] 《加州民法典》1798.100（c）：企业收集、使用、储存和共享消费者个人信息 ，应当是合理、必要，以及与收集或处理个人信息的目的相符的，或用于与收集个人信息的背景相适应的其他披露目的，并且不以与这些目的不相符的方式作进一步处理。
[95] 《加州民法典》1798.100（a）（3）：……企业拟对每类个人信息（包括个人敏感信息）储存期限，若不可行，则为确定该期限所用的标准，前提是企业不得储存消费者个人信息或个人敏感信息超过披露目的所需的合理时间。
[96] GDPR 第十三条、十四条、十五条
[97] 《个人信息保护法》第十七条
[98] 《个人信息保护法》第四十七条第一款第（二）项



发生数据安全事件时的通知义务

GDPR 与中国《个人信息保护法》的主要区别在于：

（1）GDPR 明确应当在 72 小时内告知，中国《个人信息保护法》则无具体的时间要求；

（2）GDPR 列明了告知监管机构的例外情况，但是中国《个人信息保护法》并未规定任何例外；

（3）GDPR 明确只有在“当个人数据泄露很可能给自然人的权利与自由带来高风险时”，需要通知数据主体，但是中国《个人信息保护法》则规定只有在“采取措施能够有效避免信息泄露、篡改、丢失造成危害”的情况下才可以不通知信息主体；

（4）告知个人信息主体的内容上，GDPR 并未对信息数量和类型做要求，但是中国《个人信息保护法》则要求说明个人信息的种类。

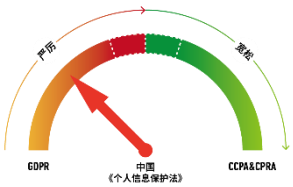
CCPA&CPRA 中并未对个人信息泄露时企业的义务作出特别规定。但是《加州民法典》第 1798.82 条和 1798.29 条规定了企业和国家机构的数据安全违规报告制度（ Data Security Breach Reporting）。[99]

[99] 《加州民法典》1798.82 条中规定了企业在数据泄露事件发生时的通知义务。根据该条规定，企业有义务通知任何加利福尼亚州居民，其未加密的个人信息（如定义）已被未经授权的人获取，或被合理地认为已被获取。如果由于安全系统的单次违规而需要向超过 500 名加利福尼亚州居民发出安全违规通知，则企业应以电子方式提交该安全违规通知单个样本的副本给总检察长。

通知信息主体			
	GDPR （第三十四条）	中国《个人信息保护法》 （第五十七条）	《加州民法典》 （第 1798.82 条）
情形	当个人数据泄露很可能给自然人的权利与自由带来高风险时	原则上发生或可能发生个人信息泄露、篡改、丢失时则应当通知，例外情况下不通知	加州居民(1) 其未加密的个人信息被未经授权的人获得；(2) 其加密的个人信息被未经授权的人获得，并且（可以使该个人信息可读或可用的）加密密钥或安全凭证由未经授权的人获得。
例外	控制者已经采取合适的技术与组织保证措施（特别是已经应用那些使得未被授权访问的个人无法辨识个人数据的措施加密）	个人信息处理者采取措施能够有效避免信息泄露、篡改、丢失造成危害的，个人信息处理者可以不通知个人	无规定
	控制者已经采取后续措施，给数据主体的权利与自由带来的高风险不再有实现的可能；		
	告知将需要付出不相称的努力		
监管机构要求告知	如果控制者仍然没有将个人数据泄露告知数据主体，监管机构在考虑了个人数据泄露所可能带来的高风险可能性后，可以要求其告知，或者可以认为符合第 3 段所规定的情形。	履行个人信息保护职责的部门认为可能造成损害的，有权要求个人信息处理者通知个人	无规定

通知信息主体的内容		
GDPR （第三十四条）	**《个人信息保护法》 第五十七条**	**《加州民法典》 （第 1798.82 条）**
	泄露、篡改、丢失的个人信息的种类	泄露的个人信息类型列表
	个人信息泄露、篡改、丢失的原因	泄露事件的一般描述
告知数据保护官的姓名与详细联系方式，或者可以获取更多信息的其他联系方式；	个人信息处理者的联系方式。	报告人或企业的名称和联系信息。
描述个人数据泄露的可能后果	可能造成的危害	
描述控制者应对个人数据泄露已经采用或计划采用的措施，包括减少负面影响的措施。	采取的补救措施；个人可以采取的减轻危害的措施	有关个人或企业为保护信息遭到泄露的个人所做的工作的信息；就信息遭到泄露的人为保护自己而可能采取的步骤提供建议。
		泄露日期；预计泄露日期，或泄露事件发生的时间范围；通知的日期（如可确定）
		通知是否因执法调查而延迟
		主要信用报告机构的免费电话号码和地址，如果泄露行为暴露了社会安全号码或驾驶执照或加州身份证号码。
		在涉及生物识别数据的违规行为中，关于如何通知使用相同类型的生物识别数据作为身份验证者的其他实体不再依赖数据进行身份验证的说明。
		如果提供通知的个人或企业是泄露的源头，则应在不少于 12 个月的时间内免费向受影响的人提供提供适当的身份盗用预防服务。

通知监管机构			
GDPR （第三十三条）		中国《个人信息保护法》 （第五十七条）	《加州民法典》 （第 1798.82 条）
时间要求	72 小时内	无具体规定	在最合适的时间内进行，不得无故拖延
通知监管机构的条件	无规定	无规定	如果一个实体需要通知超过 500 名加州居民，该实体应以电子方式向总检察长提交一份通知的副本。
例外情况	个人数据泄露对于自然人的权利与自由不太可能会带来风险	无规定	
告知内容	描述个人数据泄露的性质，在可能的情形下，描述包括相关数据主体的类型和大致数量，以及涉及到个人数据的类型与大致数量；	个人信息泄露、篡改、丢失的信息种类原因和可能造成的危害	同通知信息主体的内容（见上表）
	告知数据保护官的姓名与详细联系方式，或者可以获取更多信息的其他联系方式；	个人信息处理者的联系方式	
	描述个人数据泄露的可能后果		
	描述控制者应对个人数据泄露已经采用或计划采用的措施，包括—减少负面影响的措施。	采取的补救措施；个人可以采取的减轻危害的措施	



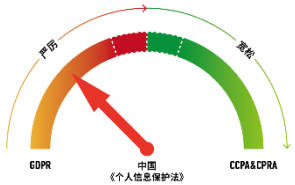
个人信息保护影响评估

GDPR 和中国《个人信息保护法》均规定了个人信息保护保护影响评估制度，且后者的适用情形更为宽泛。

加州隐私法（CCPA&CPRA）中并未规定类似的制度。

	GDPR （第三十五条）	中国《个人信息保护法》 （第五十五条、五十六条）
需要进行风险评估的情形	对与自然人相关的个人因素进行系统性与全面性的评价，此类评价建立在自动化处理——包括用户画像——基础上的，并且其决策对自然人产生法律影响或类似重大影响；	利用个人信息进行自动化决策；
	以**大规模处理的方式**处理第 9（1）条所规定的特定类型的数据	处理敏感个人信息；
	处理定罪与违法相关的个人数据	
		委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息
		向境外提供个人信息
	以大规模的方式系统性地监控某个公众可以访问的空间	其他对个人有重大影响的个人信息处理活动
风险评估的内容	对计划的处理操作和处理目的的系统性描述，以及——如果适用的话——对控制者所追求的正当利益的描述；	个人信息的处理目的、处理方式等是否合法、正当、必要；
	对和目的相关的处理操作的必要性与相称性进行分析；	
	对给数据主体的权利与自由带来的风险的评估；	对个人权益的影响及安全风险；

	结合数据主体和其他相关个人的权利与正当利益，采取的计划性风险应对措施	所采取的保护措施是否合法、有效并与风险程度相适应。
记录保存期限	无规定	3 年



DPO/个人信息保护责任人制度

GDPR 关于数据保护官的制度更为系统和全面，包括需要任命 DPO 的情形，DPO 的专业能力要求，保障 DPO 职责得以履行职责的资源支持，DPO 的角色和利益冲突保护等。相较而言，《个人信息保护法》对个人信息保护责任人的规定较为笼统。

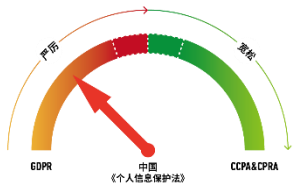
DPO/个人信息保护责任人在实践中常常会面临利益冲突，作为企业的雇员，他/她首先应当为企业负责，其次，作为组织的联系人，需要面向个人信息保护监管机构展开合作。因此，GDPR 重点对其利益冲突问题予以了重点关注，从保护 DPO 的角度，明确 DPO 的独立性，其不应为履行职责而被数据控制者或处理者解雇。

而《个人信息保护法》似乎并没有关注到这一问题，反而更进一步强调 DPO 对违法行为的责任承担，在各项行政处罚中，个人信息保护负责人似乎都可以被归入直接负责的主管人员或者其他直接责任人员，这可能会进一步加剧个人信息保护责任人的职业困境。

正如 GDPR 以及后续指南中对 DPO 的定位，DPO 是合规落地的核心，对 DPO 给予更多的法律上的职业保障，才能真正有助于 DPO 职业群体的繁荣。

	GDPR （第三十七、三十八、三十九条）	中国《个人信息保护法》 （第五十二条）
需要任命数据保护官（个人信息保护责任人）的企业	1.处理是公共机构或公共实体进行操作的，法庭在履行其司法职能时除外； 2.控制者或处理者的核心处理活动天然性地需要大规模性地对数据主体进行常规和系统性的监控； 3.控制者或处理者的核心活动包含了对某种特殊类型数据的大规模处理和对定罪和违法相关的个人数据的处理。	处理个人信息达到国家网信部门规定数量的个人信息处理者
数据保护官（个人信息保护责任人）的责任	1.对控制者或处理者，以及那些履行处理责任的雇员进行告知，提供建议； 2.确保遵守 GDPR、其他欧盟或成员国数据保护条款、和个人数据保护相关的控制者或处理者的政策； 3.根据要求，应当对数据保护影响评估以及对其实施进行监管的事项提供建议； 4.和监管机构进行合作； 5.在与处理相关的事项中……**充当监管机构的联系人。**[100]	负责对个人信息处理活动以及采取的保护措施等进行监督
专业能力要求	数据保护官的委任必须基于其专业性的素质，其需要具有数据保护法律与实践的专业知识，以及完成第 39 条所规定的任务（见上栏）的能力[101]	无规定
履行职责的资源支持	控制者和处理者应当支持数据保护官责任，应当提供其履行此类责任、访问个人数据、进行处理操作，以及维持其专业性知识的必要资源[102]	无规定
角色和利益冲突保护	1.**个人数据保护官不能因为完成其任务而被控制者或处理者解雇**。其可以直接向控制者或处理者的最高管理层进行报告。 2.数据保护官可以完成其他任务或责任。控制者或处理者应当保证任何此类任务和责任不会导致利益冲突。[103]	无规定

[100] GDPR 第三十九条
[101] GDPR 第三十七条
[102] GDPR 第三十八条
[103] GDPR 第三十八条



守门人条款

作为特色创新之一，中国《个人信息保护法》借鉴欧盟《数字市场法（草案）》引入了针对重要的互联网平台的特别义务（守门人条款）。

守门人（**gatekeepers**）是欧盟《数字市场法》（草案）中的核心概念，该草案通过定性和定量等多种标准，明确了哪些平台可能会作为守门人。《数字市场法》实质是欧盟的反垄断法，因此对于守门人的界定也重点指向“平台性”，即：业务形态中是否具有为用户提供服务的其他第三方的商业客户，第三方商户（third party /business user）的存在，**是“平台”的核心特征。**因此在该法下，对于守门人的要求多体现为竞争法上的考虑，即守门人不得与其生态中的第三方商户展开不平等的竞争，如：商户可以在平台上发现商业机会，但也应允许商户通过自己的应用程序或网站完成交易。

而中国《个人信息保护法》实质上借鉴了这一思路，但将其应用在了个人信息保护治理领域中，让平台企业在个人信息保护治理中发挥更大作用，例如要求平台对严重违反法律、行政法规处理个人信息的平台内的产品或者服务提供者，停止提供服务。中国《个人信息保护法》增设守门人企业在个人信息保护方面的义务符合互联网治理的世界潮流，能够更有效地保护自然人的个人信息。[104]但是守门人企业的认定标准以及义务的内容上还有待进一步论证和细化。

[104] 参见张新宝：《互联网生态“守门人”个人信息保护特别义务设置研究》，中国民商法律网：https://www.civillaw.com.cn/zt/t/?id=37845

	《数据市场法（草案）》[105] （第二条、第三条、第四条、第五条、第六条）	个人信息保护法 （第五十八条）
领域 限制	八大核心平台服务（core platform services）：在线中介服务； 在线搜索引擎； 在线社交网络服务；视频分享平台服务；与号码无关的人际通信服务；操作系统;云计算服务；广告服务。	重要互联网平台服务
典型 特征	1. 对内部市场有重大影响 2.运营一个或多个通往客户的重要门户 3.在其运营中享有或预计将享有牢固的和持久的地位	提供重要互联网平台服务、用户数量巨大、业务类型复杂
具体的 认定标准	1.企业在过去三个财政年度在欧洲经济区（EEA）实现的年营业额等于或超过 65 亿欧元，或者在上一财政年度其平均市值或等值公平市价至少达 650 亿欧元，并在至少三个成员国提供核心平台服务。 2.如果公司运营的核心服务平台在上一财政年度在欧盟建立或位于欧盟的月活跃终端用户超过 4500 万，并且在欧盟建立的年活跃商业用户超过 1 万。 3.企业在过去三个财政年度中的每个年度都符合其他两个标准。	尚无具体认定标准
认定 程序	1.企业符合上述标准后需要在三个月内通知委员会，委员会在收到相关信息的 60 天内进行认定； 2.委员会有权根据市场调查将未满足具体的认定标准，但是具备典型特征的企业认定为守门人。	尚无具体的认定程序
法定义务 及其他	个人数据保护方面： 1.避免在没有获得用户同意的情况下将原则核心平台服务的个人数据与源自其他服务的个人数据结合 2.仅在与终端用户就相关商业用户通过相关核心平台服务提供的产品或服务实现的	1. 按照国家规定建立健全个人信息保护合规制度体系，成立主要由外部成员组成的独立机构，对个人信息处理活动保护情况进行监督； 2.遵循公开、公平、公正的原则，制定平台规则，

[105] Proposal for a Regulation on Digital markets act：https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en

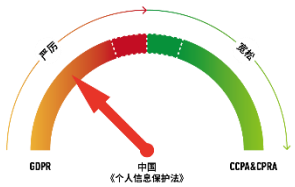
	使用直接相关的情况下提供个人数据的访问和使用，并且获得终端用户的同意 3.搜索引擎应当对构成个人数据的查询、点击和查看数据进行匿名处理	明确平台内产品或者服务提供者处理个人信息的规范和保护个人信息的义务； 3.对严重违反法律、行政法规处理个人信息的平台内的产品或者服务提供者，停止提供服务； 4.定期发布个人信息保护社会责任报告，接受社会监督。
	针对商业用户（business users）的义务和竞争法上的义务： 1.允许商业用户通过第三方在线中介服务以不同价格或条件向终端用户提供相同的产品或服务； 2.允许商业用户向通过核心平台服务获得的终端用户推广优惠，并与这些最终用户签订合同；允许终端用户通过守门人的核心平台服务，通过商业用户的软件应用程序访问和使用内容、订阅、功能或其他项目 3. 避免阻止或限制商业用户向任何相关公共当局提出与任何守门人做法有关的问题； 4.避免要求商业用户使用、提供或互操作网守的身份识别服务； 5.避免将商业用户或终端用户订阅或注册核心平台服务作为访问、注册核心平台服务的条件； 6.应其要求广告商和出版商提供有关发布特定广告价格和服务的相关信息。 7.避免在与商业用户竞争时使用通过商业用户获得的任何非公开数据； 8.允许最终用户在其核心平台服务上卸载任何预安装的软件应用程序； 9.允许安装和有效使用第三方软件应用程序或软件应用程序商店； 10.在服务和应用排名时适用公平和非歧视性条件； 11.避免在技术上限制终端用户切换服务和应用的能力； 12.允许商业用户和辅助服务提供者访问和互操作相同的操作系统、硬件或软件功能；	遵循公开、公平、公正的原则，制定平台规则

	13.应广告商和出版商的要求，免费向他们提供守门人的绩效衡量工具以及广告商和出版商对广告库存进行独立验证所需的信息； 14.为通过业务用户或最终用户的活动生成的数据提供有效的可移植性，为最终用户提供工具以促进数据可移植性； 15.免费向商业用户或商业用户授权的第三方提供有效、高质量、连续和实时的访问和使用集合或非集合数据； 16.应任何第三方在线搜索引擎提供商的要求，向其提供以公平、合理和非歧视性条款访问排名、查询、点击和查看的在线搜索引擎； 17.对企业用户适用公平和非歧视性的一般访问条件。[106]	

七、其他特别条款

对于社会公众普遍关注的热点话题，各部法律均予以了制度回应，特别是关于数据处理的“算法规制”，以及“人脸识别”问题。

[106] REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on contestable and fair markets in the digital sector (Digital Markets Act)第五条、第六条：https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A842%3AFIN



自动化决策条款（算法规制）

各法均关注了自动化决策中信息主体的访问权、知情权，GDPR 和中国《个人信息保护法》更强调了对于有重大影响/法律层面的影响(如信贷评估，入学入职资格等）的自动化决策中信息主体的反对权。

	GDPR (第二十二条)	个人信息保护法 (第二十四条、七十三条)	加州隐私法（CCPA&CPRA） （第 1798.140 条）
自动化决策的定义		自动化决策，是指通过计算机程序自动分析、评估个人的行为习惯、兴趣爱好或者经济、健康、信用状况等，并进行决策的活动。	
用户画像的定义	用户画像：“用户画像”指的是为了评估自然人的某些条件而对个人数据进行的任何自动化处理，特别是为了评估自然人的工作表现、经济状况、健康、个人偏好、兴趣、可靠性、行为方式、位置或行踪而进行的处理。		“用户画像”是指任何形式的个人信息自动化处理，以评估与自然人相关的某些个人方面，尤其是分析或预测与该自然人的工作表现、经济状况、健康、个人喜好、兴趣、可靠性、行为、位置或活动相关的方面。
自动化处理和	1. 合法性、合理性和透明性	利用个人信息进行自动化决策，应当保证	

决策的一般要求	2.目的限制 3.数据最小 4.准确性 5.限期储存 6. 数据的完整性与保密性 7. 可问责性[107]	决策的透明度和结果公平、公正，不得对个人在交易价格等交易条件上实行不合理的差别待遇。	

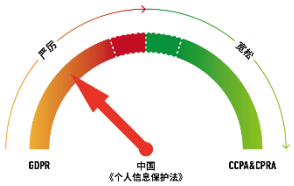
	GDPR (第二十二条)	个人信息保护法 (第二十四条)	加州隐私法（CCPA&CPRA） （第 1798.185 条）
知情权或要求解释说明的权利	控制者必须确保他们向个人清楚、简单地解释分析或自动决策过程的工作原理。[108]	通过自动化决策方式作出对个人权益有重大影响的决定，个人有权要求个人信息处理者予以说明	关于决策过程所涉及的逻辑以及与消费者有关的结果的描述有意义的信息。
访问权	1.访问用于用户画像的任何个人数据的详细信息。 2. 对于相关逻辑、包括此类处理对于数据主体的预期后果的有效信息。[109]		检察长应当发布关于自动化决策的条例，以保障消费者在自动化决策中的访问权，访问权应当包括关于决策过程所涉及的逻辑以及与消费者有关的结果的描述有意义的信息。
反对权	1.对于数据处理和用户画像数据主体有权随时反对 2.数据主体有权反对完全依靠自动化处理——包括用户画像——对对数据主体做出**具有法律影响或类似严重影**	1.通过自动化决策方式进行信息推送、商业营销，应当向个人提供便捷的拒绝方式 2. 通过自动化决策方式作出对个人权益	选择退出权：检察长应当发布有关企业使用自动化决策技术的选择退出权的条例

[107] GDPR 第五条

[108] **Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679：https://ec.europa.eu/newsroom/article29/items/612053/en**；GDPR 第十三、十四条。

[109] GDPR 第 15 条，

	响的决策。	有重大影响的决定时个人有权拒绝仅通过自动化决策的方式作出决定权	



采集图像信息和身份识别信息

中国《个人信息保护法》第二十七条规定了收集图像信息和个人身份特征信息的特别要求。一方面，在公共场所安装此类设备应当为维护公共安全所必需，遵守国家有关规定，并设置显著的提示标识；另一方面，收集的此类信息，除非取得个人的单独同意，只能用于维护公共安全的目的，不得公开或者向他人提供。

在 GDPR 和 CPRA 中，生物识别信息可被认定为敏感信息，从而适用特殊类型个人数据更为严格的处理规则。为更为全面呈现规制特点，除了本报告中比较的四部法律，我们还补充了其他相关立法和司法解释来说明。

		欧盟人工智能法案（草案） 前言第十一条，正文第五条[110]	《个人信息保护法》第二十六条；《最高法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》
公共领域	适用原则	原则上禁止出于执法目的，在公共场所使用“实时”远程生物识别系统	收集的信息只能用于维护公共安全的目的，不得用于其他目的，取得个人单独同意的除外。
	适用条件	1.仅限于特定目的：(i)有针对性地寻找特定的潜在犯罪受害者 (ii) 防止对自然人的生命或人身安全或恐怖袭击造成具体的、实质性的和紧迫的威胁；(iii) 侦查、定位、识别或起诉特定刑事犯罪的肇事者或嫌疑人； 2.必要和适当的保障措施和条件 3.司法机关或行政机关的事先授权	1.应当为维护公共安全所必需 2.遵守国家有关规定 3.并设置显著的提示标识
私人领域		尚无相关法律法规	1.处理人脸信息侵害人格权益的典型情形 2.处理人脸信息的免责事由 3.举证责任分配 4.侵权责任的承担、损害赔偿的认定、人格权侵害禁令 5.格式合同的效力 6.程序性问题

2021 年 7 月 28 日，最高人民法院发布《最高法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》，该司法解释明确处理人脸信息应当公开处理规则，明示处理目的、方式和范围，并采取应有的技术措施或者其他必要措施确保其收集、存储的人脸信息安全。同时禁止物业服务企业或其他建筑物管理人以人脸识别作为出入物业服务区域的唯一验证方式。

欧盟《人工智能法案（ARTIFICIAL INTELLIGENCE ACT）》（草案）第五条明确，禁止出于执法目的，在公共场所使用“实时”远程生物识别系统（即

[110] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS：https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

使用人脸识别进行大规模的公共监控），除非人脸识别的适用对寻找犯罪受害者、防止自然人人身安全或恐怖袭击、以及侦查定位特定犯罪嫌疑人是必要的。[111]

加州：2019 年 10 月，加利福尼亚州州长加文·纽瑟姆 (Gavin Newsom)签署 AB1215 法案，加利福尼亚州成为美国第三个禁止在警用随身摄像机中使用面部识别技术的州。该法案于 2020 年 1 月 1 日生效，该法案禁止在随身摄像机中使用生物识别监控技术，以及携带随身摄像机并稍后通过面部识别软件进行处理。

八、法律责任

法律责任包括了民事、行政与刑事责任。除了本报告比较的四部法律，还结合了其他相关法律予以综合评价，总体说来：

1.中国关于个人信息保护违法行为的责任追究体系十分完整，涵盖了民事、行政与刑事领域，且十分严厉；

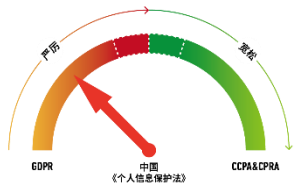
2.在民事诉讼方面，加州隐私法特点突出，其从实体上和程序上，大大限制了个人信息违法行为的可诉性，更倾向于由检察长行使监管职权。在具有行为规模性、事前可规范性的个人信息保护领域，行政规制的确彰显了更高的执法效率[112]。

3.行政监管方面，中欧都可以以违法主体的营收总额为基准作出处罚，区别在于欧盟各国均采取了独立的专门的数据保护监管机构机制（DPAs）,而中国仍维持多部门执法机制。

4.刑事领域，中国较为严厉。个人信息违法犯罪相关罪名适用主体广泛，入罪门槛极低。

[111] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS：https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

[112] 王融，黄致韬：《迈向行政规制的个人信息保护：GDPR 与 CCPA 处罚制度比较》，腾讯研究院微信公众号：https://mp.weixin.qq.com/s/87qPnJ7OK2KZpmoRSZbYxg



民事诉讼

在民事诉讼中，各部法律的一个重要区别在于私人诉权的范围。根据 GDPR 和中国《个人信息保护法》，自然人可以针对违反该法的有关行为提起民事诉讼，但是 CCPA&CPRA 则严格限定了私人诉权的范围：首先，《加州民法典》第 1798.150 条（CCPA&CPRA）明确规定，消费者仅能在企业违反安全保障义务，致使消费者原始个人信息[113]受到未经授权的访问和泄漏、盗窃，或披露的情况下，才能提起民事诉讼。该条（c）款以及近期 McCoy 诉 Alphabet, Inc.案[114]中都明确了 CCPA&CPRA 中其他条款不能作为提起民事诉讼的依据；

其次，法院在 Gardiner 诉 Walmart Inc.[115]等案件中，通过将可以提起民事诉讼的个人信息概念限定为《加州民法典》第 1798.81.5 条列举的两大类特定的个人信息[116]，进一步限缩了私人诉权的成立范围

---

[113] 《加州民法典》1798.150 条（a）（1）第 1798.81.5 节第（d）小节第（1）段（a）款所定义的**未加密和未编校**（nonredacted）的个人信息，因企业违反执行和维护与信息性质相适应的合理安全程序和做法以保护个人信息义务，而致使消费者的个人信息受到未经授权的访问和泄漏、盗窃，或披露的，消费者可以提起如下民事诉讼……

[114] https://www.classaction.org/media/mccoy-v-alphabet-inc-et-al.pdf

[115] https://www.classaction.org/media/gardiner-v-walmart-inc.pdf

[116] (1) “个人信息”是指以下任一信息：
(A) 当姓名或数据元素未加密或编校时，个人的名字或名字首字母和个人姓氏与以下任何一个或多个数据元素的组合：
(i) 社会安全号码。
(ii) 驾照号码、加利福尼亚州身份证号码、税号、护照号码、军人身份证号码或在政府文件上签发的其他唯一身份证号码，通常用于验证特定个人的身份。
(iii) 帐号或信用卡或借记卡号码，以及允许访问个人金融账户的任何必需的安全代码、访问代码或密码。
(iv) 医疗信息。
(v) 健康保险信息。
(vi) 通过对人体特征（例如指纹、视网膜或虹膜图像）的测量或技术分析生成的独特生物特征数据，用于验证特定个人的身份。除非用于或存储用于面部识别目的，否则独特的生物识别数据不包括物理或数字照片。
(B) 允许访问在线帐户的用户名或电子邮件地址和密码或安全问题及答案的组合。

再次美国最高法院以及各巡回法庭在有关数据泄露的一系列民事诉讼中，确立了“没有具体损害，就没有诉讼地位”等立案裁判规则，进一步提高了数据泄露情况下，私人诉权的行使门槛；

	GDPR （第七十九条）	中国《个人信息保护法》 （第六十九条）	CCPA/CPRA （1798.150 条；第 1798.81.5 节第（d）小节）
可诉范围（私人诉权）	违反 GDPR 的行为[117]	处理个人信息侵害个人信息权益造成损害，个人信息处理者不能证明自己没有过错的，应当承担损害赔偿等侵权责任。	消费者原始个人信息受到未经授权的访问和泄漏、盗窃，或披露的[118]
归责原则	过错推定[119]	过错推定[120]	过错
损害赔偿	物质或非物质性伤害[121]	所受损害或所得利益；根据实际情况确定赔偿数额（损失或利益难以确定）[122]	100 美元到 750 美元的损害赔偿金或实际损害赔偿金，以数额较大者为准
公益诉讼	无相关规定	个人信息处理者违反本法规定处理个人信息，侵害众多个人的权益的,人民检察院、法律规定的消费者组织和由国家网信部门确定的组织可以依法向人民法院提起诉讼。	无相关规定

最后 CCPA&CPRA 给予了企业在民事诉讼中 30 天的豁免期：如果在 30 天内，企业实际补救了所发现的违规行为，并向消费者提供了一份明确的书面声明，说明违规行为已得到补救，不再发生违规行为，那就不得对企业提起个人或集体的法定损害赔偿诉讼。

---

[117] GDPR 第七十九条：在不影响其他任何行政或司法救济的前提下，包括在不影响第 77 条规定的向监管机构提交申诉的前提下，任何数据主体认为，由于违反本条例而处理其个人数据，导致其被本条例所赋予的权利被侵犯，在这些情形下其都有获取司法救济的权利。

[118] 《加州民法典》1798.150 条（a）（1）第 1798.81.5 节第（d）小节第（1）段（a）款所定义的**未加密和未编校**（nonredacted）的个人信息，因企业违反执行和维护与信息性质相适应的合理安全程序和做法以保护个人信息义务，而致使消费者的个人信息受到未经授权的访问和泄漏、盗窃，或披露的，消费者可以提起如下民事诉讼……

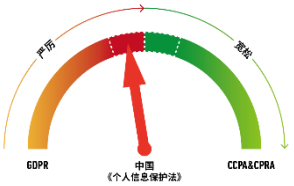
[119] GDPR 第八十二条第 3 款：控制者或处理者**如果证明自己对引起损失的事件没有任何责任**，那么其第 2 段所规定的责任可以免除。

[120] 《个人信息保护法》第六十九条第一款：个人信息权益因个人信息处理活动受到侵害，**个人信息处理者不能证明自己没有过错的**，应当承担损害赔偿等侵权责任。

[121] GDPR 第八十二条第一款：任何因为违反本条例而受到物质或非物质性伤害的人都有权从控制者或数据者那里获得对损害的赔偿。

[122] 《个人信息保护法》的六十九条

此外，在民事诉讼中，中国《个人信息保护法》与 GDPR 在归责原则上均采取了过错推定原则，而 CCPA&CPRA 则采取过错原则。处理个人信息的主体将在民事诉讼中将承担更重的证明责任。《中国个人信息保护法》还明确规定了公益诉讼机制。



行政监管

在具有行为规模性、事前可规范性的个人信息保护领域，行政规制的确彰显了更高的执法效率。[123]因此各部法律都将行政监管制度作为重点。

在执法机构方面

美欧更为类似，倾向于统一的专门的个人信息保护监管机构；而中国确立了多头监管机制。

GDPR 规定由各国专门的独立数据保护机构（DPAs）进行行政监管，而美国 CCPA 则规定由总检察长通过提起民事诉讼的方式进行罚款（在美国权力体系中，总检察长属于行政部门。通过 CCPA，总检察长获得了个人信息保护领域的广泛执法权，这与 GDPR 对独立监管机构的授权本质上并无二致），而 CPRA 则进一步要求建立加州数据保护局（CalPPA）。

中国《个人信息保护法》则明确：以网信部门为核心发挥统筹协调作用、与其他具有个人信息保护职责的部门，推进个人信息保护工作。据不完全梳理统计，目前各行业，各领域至少有十多个部门具有个人信息保护监管职责，包括：工信、公安、市场监管总局，一行两会、教育部、交通部、卫健委、

[123] 王融，黄致韬：《迈向行政规制的个人信息保护：GDPR 与 CCPA 处罚制度比较》，2020 年 3 月 18 日，腾讯研究院微信公众号：https://mp.weixin.qq.com/s/87qPnJ7OK2KZpmoRSZbYxg

文化与旅游部、国家邮政局、商务部、人力资源和社会保障部等。且这些部门的县级以上机构均有行政处罚的权限。当然，基于营业额为基准的处罚权限仍然保留给省级以上部门。

除了多头监管问题外，与 GDPR 建立的独立监管机构相比，中国《个人信息保护法》建立的监管机构只是在现有的政府部门职责的基础上明确个人信息保护职责，这里可能带来的一个问题是，中欧均是通用性立法，均适用于公私领域，但欧盟独立的数据保护机构(DPAs)也可监管政府部门，如 2018 年 9 月,保加利亚数据保护机构对保加利亚税务局开出罚单，理由是后者未能够提供足够的数据安全保障，导致数据泄露。而我国以网信部门为核心的政府监管部门，对其他政府机构的监管仍缺乏实现路径。

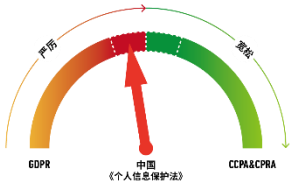
在行政处罚梯度方面：

美欧立法对违法行为进行了分类，以规定对应的处罚梯度。中国《个人信息保护法》仅以情节是否严重作为梯度的区分标准，给予了执法机关较大的自由裁量权。GDPR 根据违反的具体条款的不同，将罚款分为两个梯度：较轻的一类，处罚上限是 1000 万欧元或全球营收的 2%之中的高者（针对不需要识别的处理规定，以及一般性义务等）；较重的一类是 2000 万欧元或全球营收的 4%之中的高者（针对违反处理个人信息的原则，数据主体权利等）。

CCPA&CPRA 则根据主观心态规定了不同的罚款数额：如果企业故意违反义务或者是侵害儿童权利则处以 7500 美元的罚款，如果不是则处以 2500 美元的罚款。

中国《个人信息保护法》则以情节严重为标准将罚款划分为 100 万元以下和 5000 万元以下/上一年度营业额百分之五以下两档。可能导致执法机关因为缺乏明确的执法标准而差异化、选择性执法。

	GDPR （第八十三条）	中国《个人信息保护法》 （第六十六、六十七、六十八条）	CCPA/CPRA （《加州民法典第 1798.155 条》）
执法机构	各国 DPAs	履行个人信息保护职责的部门（多个）	总检察长或 CalPPA
罚款数额	根据违规行为的性质不同，分为轻重两类。较轻的一类，处罚上限是 1000 万欧元或全球营收的 2%之中的高者（针对不需要识别的处理规定，以及一般性义务等）；较重的一类是 2000 万欧元或全球营收的 4%之中的高者（针对违反处理个人信息的原则，数据主体权利等）。	**区分一般违法和情节严重：一般违法的情况下有关部门**责令改正，给予警告，没收违法所得，对违法处理个人信息的应用程序，责令暂停或者终止提供服务；拒不改正的,并处一百万元以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。情节严重的，由省级以上履行个人信息保护职责的部门责令改正，没收违法所得，并处五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务或者停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员和个人信息保护负责人。	**区分一般违法、故意违法和侵害儿童权利的情况：**每次违规不超过 2500 美元、每次**故意违规**或者是涉及企业、服务提供者、承包商或其他人实际知悉**未满 16 周岁未成年人个人信息**不超过 7500 美元的民事罚款，



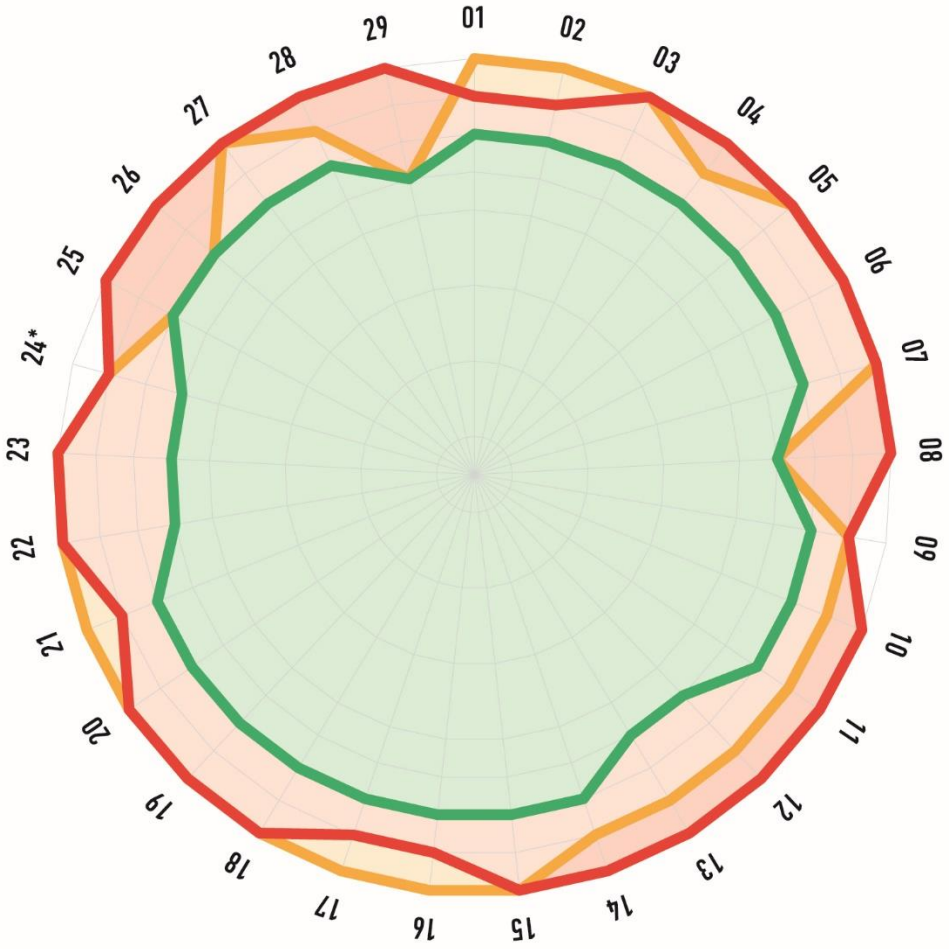
刑事责任

在刑事责任方面，各国立法存在较大的不同。GDPR，中国《个人信息保护法》以及加州隐私法（CCPA&CPRA）中并无关于刑事责任的具体规定。而比较个人信息保护刑事犯罪的相关立法可以发现，中国个人信息保护的刑事立法更为严厉：1.犯罪主体广泛：我国侵犯公民个人信息罪对行为主体并无任何限制，而美国仅在医疗等特殊领域针对医疗机构及其工作人员规定了刑事责任。2.适用刑罚严厉：在我国，侵犯公民个人信息罪的法定最高刑期是七年有期徒刑，而丹麦《个人信息处理法》规定的最高刑期为 4 个月有期徒刑[124]，芬兰刑法中最为严重的侵犯个人信息犯罪（“个人数据档案犯罪”）最高也仅处以 1 年有期徒刑[125]。此外，我国个人信息领域刑事司法活跃，据统计 2017 年 6 月至 2021 年 6 月，全国法院新收侵犯公民个人信息刑事案件 10059 件，审结 9743 件，生效判决人数 21726 人，对 3803 名被告人判处三年以上有期徒刑，比例达 17.50%。[126]

[124] 丹麦《个人信息处理法》（The Act on Processing of Personal Data）第七十条。
[125] https://www.globalcompliancenews.com/data-privacy/data-protection-enforcement-in-finland/
[126] 中国惩治侵犯公民个人信息犯罪 四年近 4000 人获刑三年以上-新华网 (xinhuanet.com)

对比概览图

欧盟GDPR　中国《个人信息保护法》　加州隐私立法 (CCPA&CPRA)



适用的地域范围 01
受规制的对象类型 02
受规制的数据活动 03
排除适用的范围 04
个人信息的定义 05
敏感个人信息的处理规则 06
未成年人个人信息 07
死者个人信息 08
匿名化、去识别化信息 09
合法性基础 10
同意规则 11
数据本地化和出境安全评估 12
跨境证据调取 13
知情权 14
访问权 15
反对权 16
删除权 17
可携带权/复制权 18
采取安全保障措施的义务 19
保存（储存）期限 20
发生数据安全事件时的通知义务 21
个人信息保护影响评估 22
DPO/个人信息保护责任人制度 23
守门人条款* 24
自动化决策 25
图像信息和身份识别信息采集 26
民事诉讼 27
行政监管 28
刑事责任 29

制图说明：

本图表采取了雷达坐标图方式。对中美欧四部个人信息保护法律的29个方面进行了横向比较。每个方面坐落在一个坐标轴上，同一坐标轴上由圆心从内向外，表示法律的严厉程度递增。落点越靠近圆心表示在该项规则上该部法律越宽松，越靠近外圈表示该部法律越严厉。

以“01适用的地域范围”为例：GDPR在该坐标轴的落点最靠近外圈，CCPA&CPRA最靠近圆心，《个人信息保护法》在中间位置，这说明：GDPR适用的地域范围最广，《个人信息保护法》次之，加州CCPA&CPRA的地域适用范围最有限。

*因守门人条款并非 GDPR 中的概念，故此处为《个人信息保护法》与欧盟《数据市场法（草案）》相关条款进行比较的结论

结论概述

从上页四部法律严厉程度比较的概览图可以看出，**中国《个人信息保护法》在规则的严厉程度上基本对标欧盟 GDPR**，加州隐私立法（CCPA&CPRA）相较于其他两部法律更为宽松：

- **适用范围：**在地域范围上 GDPR 最宽泛，《个人信息保护法》更为克制，CCPA&CPRA 最有限；而在排除适用的范围上，CCPA&CPRA 排除范围最广，GDPR 次之，《个人信息保护法》最有限；在规制的数据活动方面，《个人信息保护法》和 GDPR 调整范围更宽泛，CCPA&CPRA 更为限缩。
- **在个人信息处理的合法性基础、**同意规则、死者个人信息保护、数据本地化要求、数据出境安全评估、跨境证据调取、信息主体的知情权、行政监管方面，中国《个人信息保护法》比 GDPR 更严格，CCPA&CPRA 最宽松。
- **在个人信息的定义、**敏感信息的处理规则、未成年人个人信息的处理规则、匿名化、去识别化信息的处理规则、采取安全保障措施的义务、保存（储存）期限、个人信息保护影响评估、DPO/个人信息保护责任人制度等方面，《个人信息保护法》和 GDPR 严厉程度基本一致，CCPA&CPRA 最宽松。
- **在受规制的对象类型、**信息主体的反对权、删除权、发生数据安全事件时的通知义务等方面，GDPR 最严格，《个人信息保护法》次之，CCPA&CPRA 最宽松。

结　语

一、总体而言，中国《个人信息保护法》和 GDPR 具有更多的相似性，体现了大陆法系体系全面，制度健全的特点，以此两部法律为参照背景，美国加州隐私保护法灵活弹性，实用主义的特点也得到了充分体现，例如：

在个人信息定义方面，中欧法律都倾向于非常广泛的定义，只要与特定个人相关即可，个人信息似乎无所不包。而加州隐私保护法除了对“个人信息”概念做明确收缩外，还非常务实地排除了“集合信息”、“去标识化数据”，政府公开数据等。

在规制主体方面，中欧法律作为通用性综合性立法，并没有对规制主体加以限缩，而是不区分规模大小和服务性质，从公共领域到私营领域，从中小企业到跨国公司，甚至是个人，只要收集处理个人数据，均受规制，遵守相同的高标准合规要求；而 CCPA&CPRA 作为聚焦于消费者隐私保护的立法，在仅适用于盈利性机构的背景下，对适用的企业的规模进一步做了门槛要求，将大部分中小企业排除在外。

再如，在儿童个人信息保护方面，加州立法也遵循了联邦《儿童在线隐私保护法（COPPA）》的原则，明确排除了企业并不明知所处理的信息是儿童信息的情形。在网络环境下，依赖于“监护人知情同意”的保护机制在实践落地中将遭遇巨大挑战。如果不对适用范围加以限制，会导致大量面向大众服务的网络运营者，在本不需要去收集用户年龄、监护人信息、监护人同意的情况下，超出业务的需要范围开展此类数据处理活动，增加实际执行难度，也无益于数据保护，滋生新的数据安全问题。

此类例子不一而足，呈现出中欧与美国在个人信息保护立法领域的鲜明区别，前者在制度层面更为严谨，但后者与实践结合更好。

二、中欧立法更多以“个人”为中心，将个人权利居于核心位置，而加州立法体现了消费者保护的实际效果，以及与促进企业发展，技术创新之间的平衡：

首先，集中体现在同意机制方面。中欧立法对基于同意的数据处理中的同意均提出了较高的要求，要去同意必须是特定的，明确的，是在个人充分知情的情况下作出。而加州立法仍然保持了美国隐私立法中的核心原则——即选择退出（“opt-out”）模式。即对于 16 岁以上的消费者的个人信息处理（出售以外），除非用户拒绝或退出，则公司可以继续处理用户的个人信息。“opt-out”模式对消费者而言更为真实有效，同时对新进入市场的企业的发展阻碍也更小。

其次，在规制范式方面，中欧立法都体现了合规清单（check-list）的思路，即在立法中详细规定行为规范，企业只有逐项符合这些规定，才能达标。但在加州立法中类似的规范较为少见。例如中欧立法中的数据保护官制度，个人信息保护影响评估制度，数据安全保障制度的具体措施在 CCPA&CPRA

中均未有对应规范。

再次，在责任机制方面，中欧立法规定均十分严厉，如基于营业额基准的处罚标准。而在加州立法中，除了对罚款配合以限定机制外，私人诉权也受到了限制和弱化，以避免过度诉讼、滥诉的发生，这有助于提升违规行为纠正效率，实现监管资源有效利用。

三、尽管中国《个人信息保护法》更多借鉴了 GDPR，且在某些方面，体现出更为严格的特点：

其一：二者均为通用性立法，但中国《个人信息保护法》对数据处理的合法性事由的限定更为严格，例如并没有借鉴欧盟 GDPR 的规定，将数据控制者或第三方的正当利益作为合法性事由；此外，在同意机制方面，更为严格。一是如果将“用户同意”作为处理个人数据的合法理由，用户同意必须是清晰明确的，这是底线要求，与欧盟相同；二是对于敏感个人信息的处理，以及个人数据处理的高风险环节（出境，公开，向他人提供等），还要求单独同意，此处比欧盟严格。

其二，在信息披露方面，欧盟 GDPR 和美国加州隐私立法对于数据接收方的身份披露，均只要求披露到类型即可，但中国《个人信息保护法》的披露颗粒均要求到数据处理者的具体姓名/名称和联系方式等，且必须在数据处理活动之前披露。

其三，在法律责任方面，中国建立了更为严格的追责体系，民事、行政、刑事领域对于违法行为的追责力度都力度空前。在民事领域确立过错推定，连带责任，公益诉讼等机制；在行政责任领域，引入了基于营业额的处罚基准；而在刑事领域，通过近年来陆续出台的刑事司法解释，入刑门槛低，刑罚重已然成为个人信息刑事责任体系的突出特点。

四、作为基于中国国情的法律方案，中国《个人信息保护法》也体现了鲜明的中国特色：

在监管体制上，区别于美欧推行的统一监管机构模式，目前《个人信息保护法》确立的仍然是以网信部门为核心的多头监管模式，据不完全梳理，除了网信部门外， 具有履行个人信息保护职责的部门，包括：工信、公安、市场监管总局，一行两会、教育部、交通部、卫健委、文化与旅游部、国家邮政局、商务部、人力资源和社会保障部等超过十五个部门，且在法律授权下，此类政府体系中的县级以上部门均具有非常广泛的职权和行政处罚权力：包括对违法行为给予警告，没收违法所得，对违法处理个人信息的应用程序，责令暂停或者终止提供服务；罚款等。

在多头监管机制中，网信部门将发挥统筹协调的核心作用。《个人信息保护法》对其统筹协调有关部门，至少作出了四方面明确授权（第六十二条）：

（一）制定个人信息保护具体规则、标准；

（二）针对小型个人信息处理者，处理敏感个人信息以及人脸识别、人工智能等新技术、新应用，制定专门的个人信息保护规则、标准;

（三）支持研究开发和推广应用安全、方便的电子身份认证技术；

（四）推进个人信息保护社会化服务体系建设，支持有关机构开展个人信息保护评估、认证服务等

除了统筹协调角色外，《个人信息保护法》还对网信部门独立监管职能作出了明确授权，至少涉及九个方面：包括：

建立个人信息跨境中的安全评估机制、标准合同机制、第三方安全认证机制；

(一) 确定哪些个人信息处理者需采取和关键信息处理者同样的跨境数据管理机制，哪些情形可以免于安全评估；

(二) 确立哪些国家列入我国采取限制或者禁止提供个人信息的清单；

(三) 数据可携带权的具体规定；

(四) 必须设立个人信息保护负责人的机构范围；

(五) 以及对于可以提起公益诉讼的组织的指定权。

这意味着在未来个人信息保护法的进一步的落地实践中，需要依赖网信部门制定大量的更为具体的规范要求，网信部门在个人信息保护中的地位尤为重要。

总体上，《个人信息保护法》在一些设涉及数据安全，特别是国家安全的领域，体现了作为发展中国家的考量。这集中体现在个人信息的跨境数据流动制度。《个人信息保护法》承接《网络安全法》的规定，针对关键信息基础设施运营者重申了数据本地化政策，并把这一要求扩展至达到国家网信部门规定数量的个人信息处理者。对于其他的个人信息处理者的出境场景，也强化了监管部门在其中的作用。此外，在执法场景下的跨境数据流动，明确非经中华人民共和国主管机关批准，不得向外国司法或者执法机构提供境内个人信息。

五、作为对全球数字治理的中国方案，中国《个人信息保护法》围绕热点问题，也作出了相关的制度创新与回应：

第一，对于“死者”个人信息保护问题的回应。伴随着数字化和老龄化的同步推进，死者的个人信息保护问题已成为各方关注的焦点。尽管对于死者是否具有基于个人信息的人格利益，目前在学界仍然是一个具有争议性的问题，各国立法与司法实践对死者的个人信息保护问题均持谨慎态度。我国《个人信息保护法》在民法典确立的侵权救济机制基础上又向前迈出一步，在立法中明确承认了死者的个人信息利益，并提出了具体的保护机制——即由死者近亲属为了自身的合法、正当利益，可以对死者的个人信息行使本章规定的查阅、复制、更正、删除等权利，但是死者生前另有安排的除外。当然考虑到现实生活中，有大量的个人信息具有着交叉属性，也涉及想对方的隐私和个人信息利益，如通信内容，邮件信息等，如果泛泛由近亲属行使，恐带来对相对方的隐私侵害和数据安全风险，需要对未来实践做进一步精细化的规定。

第二，对于数据复制权/可携带权的考量。

数据复制权/可携带权是近年来个人信息保护法领域的一个热点话题。一方面，基于对用户权利的尊重，需要在立法中为用户实现对其个人信息的控

制提供更为强大的权利保障，但另一方面，由于数据可携同时涉及第三人的隐私保护、数据安全以及市场竞争问题，迄今为止并没有明确定论。即便是最早引入数据可携的欧盟 GDPR，到目前为止也没有落地的具体方案。特别是为解决第三方用户的隐私保护问题，GDPR 也明确对数据可携做了限定，要求可携权的行使不得对他人的隐私保护及正当权利产生负面作用。从 A 平台到 B 平台的转移过程中，在传输方和接收方之间分配责任？谁最终对转移的数据安全负责？对于这些具体实操问题，目前还缺乏清晰的答案，特别是考虑到我国的个信法是一部综合性通用性的立法，因此，理论上各个机构都要适用，包括医院、银行、国家机关。这些主体之间的数据可转移问题，还需结合行业、领域来看，难以一刀切适用。因此条文表述上，《个人信息保护法》对于该权利的规定也较为弹性，留待后续在实践中探索。

第三，将“守门人制度”引入到个人信息保护领域。

在《个人信息保护法》制定过程中，国内也正掀起对大型互联网平台加强监管的风暴，同期，欧盟在竞争法领域提出了《数字市场法案》，我国将其中的“守门人”制度加以借鉴，并引入《个人信息保护法》，对其提出了特定的义务要求，包括成立主要由外部成员组成的独立机构，对个人信息处理活动进行监督；遵循公开、公平、公正的原则，制定平台规则；对严重违反法律、行政法规处理个人信息的平台内的产品或者服务提供者，停止提供服务；定期发布个人信息保护社会责任报告，接受社会监督。虽然与欧洲立法的规制领域不同，但二者有异曲同工之处，皆旨在发挥平台在治理中的关键角色。

《个人信息保护法》实现了与国际个人信息保护通用原则的接轨，同时也体现了中国作为发展中国家的鲜明国情特色。她全面彰显了我国政府在数字时代遵循法治理念，“以人为本”的决心，承接《网络安全法》、《数据安全法》，正式拉开了个人信息权益法律保护的大幕，尽管有许多领域仍待具体规范，但整体制度已向前迈进，一切未来可期！

腾讯研究院公众号

腾讯研究院视频号