

数字经济时代下的数据隐私保护法律研究

●董冠森



[摘要] 在数字经济时代,数据已成为推动创新和社会经济发展的关键资产。然而,在对数据收集、存储和处理的过程中,数据隐私问题备受关注。随着社交媒体、电子商务平台和物联网设备等数字技术的发展与应用,大量的个人数据存在未授权访问、信息滥用的风险。此外,数字系统的互联性质加剧了数据泄露风险。了解数字经济对数据隐私保护的深远影响是制定有效的法律框架、保护个人数据隐私权利的重要基础。本文先论述了数据隐私的概念和重要性;然后,从公平性与透明度、用户控制和同意、数据最小化和安全性三个方面分析数据隐私保护法律制定原则,阐述了数据隐私保护法律的具体内容;最后,提出了保护数据隐私的法律监管和执行机制。

[关键词] 数字经济时代;数据隐私保护;法律

在数字经济时代,法律框架在保护个人隐私权方面发挥着强有力的作用。法律通过为数据处理制定明确的标准、设定权利和义务,为数据处理提供了处理依据,提高了数据处理流程的透明度,并加强问责。此外,法律还赋予个人访问、更正和删除个人数据等权利,从而增强他们对隐私信息的控制。因此,法律在保护数据隐私中的作用不容忽视,法律框架的建设和完善符合数字经济发展的实际情况。

Q 数据隐私的概念和重要性

数据隐私,是指人们控制个人信息的收集、使用和传播的权利,它包括保护敏感数据免遭未授权访问、滥用和泄露。数据隐私通过确保以负责任和道德的方式处理个人信息来保护个人的自主权、尊严和基本权利。

数据隐私对于在数字时代维持信任、促进创新和保护个人权利至关重要:首先,数据隐私保护能够对个人信息进行控制,使人们能够就如何收集、使用和共享其数据做出明智的选择;其次,强有力的数据隐私保护可以在个人、企业和其他机构之间建立信任,增强不同主体对数字服务的信心,并促进数据主体和数据控制者之间形成良好的关系;再次,数据隐私保护个人免受各种形式的伤害,包括身份盗窃、金融诈骗、监视等。同时,尊重数据隐私原则反映了人们的价值观,如对人的尊严、责任的维护等。制定数据隐私标准可以促进组织和个人之间负责任的数据管理和道德行为;最后,遵守数据隐私法规可避免组织声誉受损以及承担不必

要的法律后果。

Q 数据隐私保护法律的制定原则

(一)公平和透明

公平和透明是制定有效的数据隐私保护法的基本原则。公平原则意味着确保公平对待个人数据,消除身份、背景、职业等不同因素的影响,以非歧视的方式处理数据,采取措施防范不公平的数据处理现象。透明原则涉及向个人提供有关其数据如何收集、使用和共享的清晰且易于访问的信息,这包括以所有人都易于理解和访问的方式披露数据处理过程、目的和接收者,使个人能够对其数据做出明智决策并使数据控制者对其行为负责。

(二)用户控制和同意

用户控制和同意是赋予人们对其个人信息行使自主权的基本原则。用户控制是指个人决定数据控制者如何收集、使用和共享其数据的能力,它涉及为个人提供有关数据处理的有意义的选择和选项,如选择加入或退出数据收集实践。同意是个人基于清晰明确的信息自愿同意为特定目的处理其个人数据,这种同意是自由的、具体的、知情的和可撤销的。有效的数据隐私保护法律应优先考虑用户控制和同意,要求数据控制者在处理个人数据之前获得个人的明确同意,并尊重个人在数据处理实践方面的选择和偏好。

(三)数据最小化和安全性

数据最小化和安全性是防控隐私泄露风险和保护个人信息免遭未授权访问或滥用的关键原则。数据最小化涉及仅

收集和处理特定目的所需的最少量个人数据，强调将数据收集限制在相关、充分和相称的范围内，以实现预期目标，从而减少不必要的个人隐私暴露。安全性需要采取适当的技术和组织措施来保护个人数据免遭未经授权访问、披露、更改或破坏，这包括加密、访问控制、假名和定期安全评估，以识别和解决漏洞。数据隐私法应要求数据控制者采取强有力的安全措施和数据最小化实践，以确保个人数据的机密性、完整性和可用性，从而增强个人对数据处理活动的信任和信心。

Q 数据隐私保护法律的具体内容

（一）个人数据收集和处理的法规

数据隐私保护法通常包括管理数据控制者收集和处理个人数据的法规，这些法规旨在确保合法、公平和透明地收集和处理个人数据，并采取适当的保障措施来保护个人的隐私权。个人数据收集和处理的法规主要包括如下内容：（1）处理的法律依据。数据控制者必须拥有收集和处理个人数据的有效法律依据，例如同意、合同必要性、法律义务、切身利益、公共任务或合法利益。（2）目的限制。个人数据应出于指定、明确和合法的目的而收集，并且不得与这些目的的不相符的方式处理个人数据。（3）数据最小化。数据控制者应将个人数据的收集限制在达到预期目的所需的范围内，并避免收集过多或不相关的信息。（4）数据准确性。数据控制者有责任确保个人数据的准确性、完整性和时效性，并采取合理措施纠正或删除不准确或过时的信息。（5）问责和透明度。数据控制者应对其数据收集和处理实践保持透明，为个人提供清晰易懂的信息，说明其数据的使用方式以及与数据处理活动相关的权利。

（二）数据使用目的限制

数据隐私法可能会对数据控制者使用个人数据的目的施加限制，这些限制旨在防止未经授权或不当使用个人数据，并确保数据处理活动符合个人的期望和权利。数据使用目的限制主要条款包括以下内容：（1）目的限制原则。个人数据只能出于指定、明确和合法的目的进行处理，不得与这些目的的不相符的方式处理个人数据。（2）同意其他目的。如果数据控制者希望出于最初收集目的之外的目的处理个人数据，他们必须获得数据主体的明确同意，除非适用其他处理的法律依据。（3）禁止二次使用。如果没有充分的法律依据，并且（如果需要）获得数据主体的明确同意，为某一目的收集的个人信息不得用于其他目的。（4）数据保留限制。数据控制者保留个人数据的时间不应超过其收集目的所需的时间，并且他们应制定政策和程序，以便在不再需要数据时安全地处置或匿名化数据。

（三）数据传输和存储规定

数据隐私法通常包括规范个人数据传输和存储的条款，以确保数据在司法管辖区之间传输或以电子或物理格式存储时受到保护。数据传输和存储规定主要条款包括以下内容：（1）跨境数据传输。数据控制者在跨境传输个人数据时必须遵守适用的法律要求，包括获得适当的保障措施，例如数据传输协议、具有约束力的公司规则或认证机制，以确保对数据的充分保护。（2）数据本地化要求。部分司法管辖区可能对将个人数据传输到境外设立一些限制，或要求数据控制者将数据存储在该国境内，但须遵守某些例外或条件。这些要求旨在保护国家安全和个人隐私，并且通常需要满足特定的条件方可豁免。（3）安全措施。数据控制者负责实施适当的技术和组织措施，以保护个人数据免遭未经授权访问、披露、更改或破坏，包括加密、访问控制和定期安全评估。（4）数据泄露通知。数据控制者应制定程序，在发生对个人权利和自由构成风险的数据泄露事件时立即通知数据主体和相关部门，使他们能够采取适当措施减轻数据泄露的不利影响。

（四）保护数据主体权利

数据隐私法通常包括旨在保护数据主体权利并授权他们对其个人数据行使控制权的条款，这些权利使个人能够访问、纠正、删除、限制和反对对其数据的处理，以及获取有关其数据如何使用的信息并向监管机构提出投诉。关键数据主体权利包括以下内容：（1）访问权。数据主体有权从数据控制者处获得关于其个人数据是否正在被处理的确认，如果是，则有权访问该数据并获取有关处理目的、正在处理的数据类别以及向其披露数据的接收者或接收者类别。（2）更正权。数据主体有权要求更正数据控制者持有的不准确或不完整的个人数据，并要求立即更正此类数据。（3）删除权。在某些情况下，数据主体有权要求删除其个人数据。例如，当数据不再用于其收集目的时、当数据主体退出时同意，或数据被非法处理时，数据主体有权要求删除其个人数据。（4）反对权。数据主体有权反对出于某些目的处理其个人数据，除非数据控制者能够给出充足的理由和证据。（5）数据可移植性的权利。数据主体有权以结构化、常用和机器可读的格式接收其个人数据，并在技术可行的情况下将该数据无障碍地传输给另一个数据控制者。（6）限制处理的权利。在某些情况下，数据主体有权要求限制其个人数据的处理。例如，当数据的准确性受到质疑、处理非法或数据主体提出反对时，处理待验证数据控制者的合法理由是否优先于数据主体的合法理由。（7）提出投诉的权利。如果数据主体认为自己在数据保护法下的权利受到侵犯，则有权向监管机构提出投诉，且不影响任何其他行政或司法补救措施。

Q 数据隐私保护法律的监管和执行机制

（一）设立监管机构，明确监管职责

有效的数据隐私保护需要强有力的法律监督和执行机制，通常由负责强制监督遵守数据保护法律法规的监管机构进行监督。这些监管机构在监控数据处理活动、调查投诉以及对不合规实体实施制裁方面发挥着重要作用。

第一，设立监管机构。负责数据隐私执法的监管机构通常是通过立法或设立监管框架，这些机构可以在国家、区域或超国家层面运作。

第二，明确监管机构职责。监管机构被赋予各种旨在促进和执行数据隐私合规性的职责，这些责任包括以下内容：制定和发布数据保护指南、标准和最佳实践；为组织和个人遵守数据隐私法提供指导和帮助；调查投诉和违反数据保护法的行为，包括对数据控制者和处理者进行审计和检查；发出警告、谴责和纠正措施，以解决不遵守数据隐私要求的问题；对违反数据保护法的组织实施行政处罚和处罚；与其他监管机构、执法机构和国际同行合作解决跨境数据保护问题。

第三，独立性和问责。监管机构应独立、公正地运作，不受不当影响或干扰，以确保有效执行数据保护法。监管机构应该对公众负责并接受公众监督，以确保机构活动的透明度，强化问责。

（二）制定处罚和违规制裁机制

为了阻止违规行为，数据隐私保护法通常包括针对违规行为的处罚和制裁机制，具体的处罚和制裁决定取决于违规的严重性和性质、造成的伤害程度以及适用的具体法律规定。常见的处罚和违规制裁包括以下内容：（1）行政罚款。数据保护机构可能会对被发现违反数据隐私法的组织处以罚款，可能是固定金额，也可能根据组织规模、营业额或违规严重程度等因素进行计算。（2）纠正措施。监管机构可能会发布命令，要求组织采取具体的纠正措施，以解决不遵守数据保护法的问题。这些措施包括停止非法处理活动、纠正不准确的数据或实施额外的安全措施。（3）禁令。监管机构可以发布禁令，以防止组织从事非法数据处理活动或迫使他们遵守数据保护要求。（4）公开谴责和警告。数据保护机构可以公开谴责被发现违反数据隐私法的组织。（5）刑事制裁。如果严重或故意违反数据保护法，可能会对违法

行为负责的个人或组织实施罚款或监禁等刑事制裁。（6）损害赔偿。受到非法数据处理活动影响的数据主体有权就因侵犯其隐私权而遭受的任何伤害寻求损害赔偿。

Q 结束语

综上所述，为了应对数字经济带来的挑战，数据隐私保护法律在进一步发展和完善，主要体现在提升透明度、加强问责和用户控制、加大执法力度及国际合作等重要方面。为了应对数字环境中新出现的风险和机遇，未来的法律应强调跨司法管辖区的协调，简化跨境数据传输机制，并制定相关的有效措施，以减轻个人数据隐私权的潜在风险。此外，促进利益相关者之间的合作、增强公众的法律意识，也有助于数据隐私保护法制定的稳健，并增强其法律的适用性。

参考文献

- [1]李谨文.数字经济时代下企业治理的范式创新与实践研究[J].商展经济,2023(10):161-164.
- [2]刘奕含.数据隐私保护的反垄断监管探析[D].石家庄:河北经贸大学,2023.
- [3]李振利.数字经济高质量发展下数据隐私权保护新途径的研究[J].宏观质量研究,2022,10(01):107-126.
- [4]任超,李雅瑜.数字经济时代数据隐私的反垄断保护:理论证成,适用困境及破解之道[J].重庆邮电大学学报:社会科学版,2023,35(04):65-75.
- [5]王蕊.论数据隐私保护[D].郑州:郑州大学,2022.
- [6]沈俊翔.数字经济时代个人信息跨境保护的机制研究——兼论 CPTPP 视野下人民法院参与全球数据治理的新型路径[J].法律适用,2022(06):174.
- [7]马光,毛启扬.数字经济协定视角下中国数据跨境规则衔接研究[J].国际经济法学刊,2022(04):45-62.

作者简介:

董冠森(2000—),男,汉族,山东青岛人,硕士研究生,青岛科技大学法学院,研究方向:法学。