【宪法学】

个人信息国家保护义务及展开

王锡锌

【作者简介】王锡锌，教育部人文社会科学重点研究基地北京大学宪法与行政法研究中心教授。
【原文出处】摘自《中国法学》（京），2021.1.145~166

一、问题提出及界定

个人信息保护的权利基础为何？为何保护？谁来保护？针对何种威胁而提供保护？只有在厘清这些问题的基础上，方可更好地回答如何保护的问题。

本文认为，个人信息保护的宪法基础是国家所负有的保护义务。国家负有对公民人格尊严和隐私、安宁进行保护的义务；随着信息时代的来临，该种义务扩展到对个人信息相关权益的保护。个人信息国家保护义务对应着“个人信息受保护权”这一基本权利，但此种权利并非民法意义上的权利，而是国家履行其保护义务的价值基础与宪法依据，其功能主要在于对抗和缓解“数据权力”对个人信息造成的侵害风险。这种权利并不等于公民对其个人信息拥有排他性的、支配性的权利。从功能上讲，相比于“个人信息权”的保护路径，“个人信息受保护权”通过强调国家保护义务及其落实，更有利于个人信息保护的目标实现，因为面对数据平台和国家机关所拥有的强大“数据权力”（data power），通过私法路径和方式，很难为个人信息提供充分、全面和有效的保护。

二、个人信息国家保护义务的概念提炼

（一）个人信息保护的两种基本模式

如何进行个人信息保护？对此问题的回答可类型化为“权利保护”与“权力保护”两种基本模式。“权利保护”模式将个人信息视作私权客体，试图构建一种对抗不特定主体的个人信息权；“权力保护”模式则强调在个人信息处理活动中，国家负有保护个人合法权益的义务；相应地，个人信息保护制度倚重的并非赋予个人针对其信息的私人权利，而是国家设定的监管与合规框架及配套执法机制。

主张“权利保护”模式的观点在我国民法典编纂过程中达到一个高峰。诸多论者尝试结合域外经验，证成个人针对个人信息的民事权利。其中一种被许多学者接受的观点认为，欧盟与欧洲国家的立法与司法实践将个人信息保护建立在个人享有的民事权利基础上，即“个人信息权”或“个人信息自决权”这一排他性的、带有人格属性的私权，进而主张我国应以民法权利的框架展开个人信息保护的规则设计。

然而，从规范逻辑、制度功能、域外经验等维度观察，将个人信息私权化的路径缺乏相应的支撑。首先，从权利本身的规范逻辑上看，基于个人信息交互性、分享性、公共性的特点，其难以成为民法所有权逻辑下一个排他性的个人控制的客体。一旦认为个人可以“基于自己意思自主地决定个人信息能否被他人收集、储存并利用”，将妨碍基本的社会交往，也无法释放信息的公共价值。同时，个人信息具有动态性、场景性的特征。随着大数据技术的发展，个人信息可识别性和相关性标准的边界不断扩张。静态的民事权利客体的理念无法有效回应这一趋势，

强行将个人信息私权化也会造成民法的体系混乱。

其次，从制度功能上看，依托于意思自治、主体平等基础的私权保护路径无法应对强大的私人机构以及国家机构处理个人信息时的非对称权力结构。认为“无论国家机关处理自然人的个人信息，还是非国家机关处理自然人的个人信息，也无论处理者处理自然人个人信息的目的是行政管理、公共服务还是营利目的，处理者与自然人都属于平等的民事主体”的观点，忽视了个人与信息处理者之间明显的不平衡关系。正如张新宝指出，面对强大的个人信息处理者，抽象的民事权利规定容易被虚化，沦为“纸面上的权利”；个人信息保护的有效性必然有赖于国家规制，实践中站在维权第一线的其实往往是监管者而非个人。

最后，从比较法的经验观察，认为欧洲确立了民法上的个人信息权的观点，其实属于对域外经验的误读。实际上，欧盟个人数据保护的权利来源是宪法性权利，而非民事权利。欧盟数据保护专员公署（European Data Protection Supervisor）亦明确指出：欧盟数据保护规则并非赋予个人针对其个人信息排他性的民法权利，那种认为个人针对其个人信息享有“所有权”或“决定权”的观念是一种误读。

（二）个人信息国家保护义务溯源

从比较法视角看，在宪法层面确立个人信息国家保护义务的做法来源于欧盟。1953年生效的《欧洲人权公约》第8条为欧洲国家的个人信息保护提供了初步规范依据。之后，欧洲委员会通过了第(73)22号和第(74)29号决议，提出了保护私营部门和公共部门自动化数据库中的个人数据的原则。1981年，《有关个人数据自动化处理中的个体保护公约》即《第108号公约》成为全球范围内有关个人信息保护的第一份具有法律约束力的国际性文件。《第108号公约》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。

步入21世纪后，在宪法层面确立个人信息受保护的基本权利与国家相应的保护义务，渐成欧盟成员国的价值共识。《欧盟基本权利宪章》（以下简称《宪章》）第8条第1款规定：“任何人都享有对关乎自身的个人信息的受保护权利”。《欧盟运作条约》第16条第1款亦采用了“个人信息受保护权”（the right to the protection of personal data）的表述。在法权结构上，这彰显了宪法层面对国家提出的规范要求，而非旨在建构个人针对其信息的“个人信息权”（the right to personal data）。

三、个人信息国家保护义务的内涵

“个人信息受保护权—国家保护义务”是一体两面的概念，本质上是“基本权利—国家义务”体系在个人信息保护领域的运用。个人享有的个人信息受保护权必然要求国家对个人在信息处理领域中的个人进行保护与支援。在此语境下，确立与澄清个人信息国家保护义务的内涵，便需要对个人信息受保护权的价值基础、主要类型与权利结构进行识别与辨析。

（一）个人信息国家保护义务的两种类型

1.国家的消极义务与个人信息受保护权的防御权功能

基本权利最原始的机能是防御权，即公民对抗国家不当干预其自由和侵害其财产的权利。当国家试图侵害被基本权利所保障之法益时，公民可以直接按照基本权利规范来请求国家不得干预或侵害。该种要求停止干预或侵害的请求权机能，反射至国家一方，也就是国家身负不得侵犯的禁止作为义务。

2.国家的积极义务与个人信息受保护权的客观法功能

虽然个人信息国家保护义务曾长期以消极义务为主要呈现姿态，但随着时间的推移，尤其是进入21世纪后，传统“私人生活保护”所遵循的“权利具有绝对性质，信息获取便推定违法”的古典自由权逻辑在许多场景下已不再适用。相较而言，个人信息受保护权在大数据时代的基本假设是，个人信息本身便具有一定的交互性与公共性，个人信息处理在现代社会中是必要的。尽管应考虑到某些条件和保障措

施，但对个人信息的基本推定是“可以被处理”。而真正需要国家介入的关键在于：个人此时面对的不是普通的私人主体，而是强大的、组织化的信息处理机构；加之信息时代下个人信息处理往往是动态化、复杂化、风险不确定的过程，因此个人难以在参与及做出选择的过程中保持清醒、警惕、知情及自治。为使个人免于受到信息处理机构的支配，就需要国家积极保护相关个人。由此，个人信息受保护权变成了一项积极的权利，具备了客观价值秩序（客观法）的功能，即国家必须创造和维护有利于实现个人信息保护的制度环境。

3.个人信息受保护权在我国宪法上的安顿

个人信息国家保护义务在我国宪法上的首要根据便是《宪法》第33条第3款规定的“国家尊重和保障人权”。对应前述两种类型的国家义务，“尊重”侧重国家对私人生活的不得侵犯，是个人信息受保护权主观防御功能与国家消极义务的体现；“保障”则更侧重个人信息受保护权的客观方面功能，其中就包含了要求国家积极通过立法和其他公权力行为，以保护基本权利主体在个人信息处理中免于受支配或陷入信息处理者制造的危险或风险的含义。这两种类型的义务又可以被统摄于《宪法》第38条对公民人格尊严的保护之中。

（二）个人信息国家保护义务的规范结构

基于个人信息受保护权实现的宪法规范要求，个人信息国家保护义务的规范逻辑结构由“侵害来源”和“保护方式”两部分构成，也就是针对何种侵害源的保护、如何进行保护的问题。

1.个人信息国家保护所针对的侵害风险源

在现代社会，信息处理活动很大程度上决定了人们的选择空间与可能获得的结果。亦即，数据权力（data power）已经成为一种广泛而普遍的社会事实。当下诸多具备大数据挖掘能力的专业或商业机构具有以下特征：“掌握庞大的数据量、超乎常人想象的收集速度、多元的数据种类、潜在的详尽范围以及强人工智能技术下的数据关联与整合能力。”可以说，在金融、教育、医疗、社会保障等各个领域都已形成“数据依赖”的时代，个人信息的利用与保护不仅关涉个体，还与整个社会的权力结构及运行机制相关联。

可以说，面对这些来自数据权力的侵害风险，希望通过象征性的、形式化的个人自主决定和支配来进行个人信息保护的私法机制，看似体现了对个人主体地位的尊重，实际上是将个人的选择置于数据权力的控制之下，缺乏制衡能力与信息资源的个人并无法凭借“信息自决”来实现对上述侵害风险的防御与保护，以事后救济为主的“权利模式”对于控制大规模、持续性的信息处理风险而言显得捉襟见肘。只有通过国家保护义务这一兼具公共强制与理性治理的机制，才能有效防范数据处理风险，使个人与个人信息处理者之间构成合理的制衡状态，从而避免个人时刻处于被数据权力支配的恐惧之中。这构成了国家落实个人信息保护义务的必要和正当理由。

2.控制侵害风险的基本路径

基于对数据权力这一侵害风险源进行控制的需要，国家应从不同路径展开其保护义务。

一方面，国家需要意识到，其自身也是一个侵害风险源，应尽可能减少和避免对公民私人生活的干预与监控。在大数据时代，主要挑战是如何将“监控国家”之实践（surveillance state）纳入法治框架。“监控国家”表现为政府基于国家安全、预防犯罪与社会管制的考虑，通过通讯技术、摄像头监控、网络流量监测等方式，对个人的生物、行为等信息进行采集与处理，并用于执法、监管和风险控制。例如，公共区域图像采集、人脸识别、行程轨迹追踪等就是典型的监控工具。虽然监控技术的应用和大数据驱动的数字化治理有助于精准、智能化地预防和应对不确定风险，但同时也会带来过度监控风险。如果不能在法律上明确和强调国家的消极义务，滥用监控工具的风险就会成为现实危险。落实国家消极保护义务，需要厘清国家进行个人信息收集与处理的负面清单。

另一方面，《个人信息保护法》的制定过程更多

贯彻了个人信息受保护权的客观法功能所指向的积极义务，这要求国家针对数据权力这一侵害风险源而提供积极保护。若是从体系化视角观察国家积极义务的实现途径，基于客观法功能导出的国家义务包括制度性保障、组织与程序保障、保护公民免受第三人侵害的义务（侵害的防止义务）这三项基本要求。也就是说，国家权力需要对大数据时代下的个体人格和尊严提供制度性保障和秩序担保。

四、个人信息国家保护义务的展开

个人信息国家保护义务的展开和落实，是一个综合不同法律技术与制度工具的系统过程，需要国家统筹协调不同部门法工具，吸纳多元主体参与，兼顾对个人信息的消极保护和积极保护。

（一）消极保护义务的落实

在传统上，消极保护义务所指向的个人防御权要求国家不得侵入个人信息领域。但在以大数据和信息技术广泛应用的“信息国”时代，以对个人数据的采集和处理为核心的“监控”已成为一个普遍事实。在这个背景下，落实国家消极保护义务的关键，并非禁止国家使用监控等数据处理技术，而在于强调监控手段运用的价值理性和工具理性。监控（surveillance）是在传统安全观念和治理手段基础上，为回应复杂、多样的安全风险而孕育的权力和技术工具，在反恐、传染病监控、自然灾害和市场风险、公共安全等领域已普遍使用。但数据监控工具如果不能被有效控制在以宪法为根基的法秩序之内，则极易被滥用，甚至导致工具的“反噬效应”。因此，不能仅关注监控的有效性，应当在消极保护义务的价值规范要求下，考虑工具有效性和私人生活安宁之间的平衡，具体可从立法规则表达、过程控制与救济机制三个层面进行落实。

（二）积极保护义务的落实

1.制度性保障

国家首先需要建构个人信息处理的基本制度，设定个人与个人信息处理者之间的权利义务关系结构，确保个人实质性参与信息处理过程，对信息处理者形成制衡，以充分实现权益保障目标，这便是个人信息国家保护义务的制度性保障面向。制度性保障课予国家建构和维护一套关于个人信息处理基本制度的“客观”义务。基于支援个人对抗数据权力的需要，立法机关有必要通过制度建构，赋予个人在信息处理中的工具性权利，同时设定信息处理者的相应义务与行为模式，从而建立起个人与信息处理者之间的制衡结构。由于数据处理者与个人在资源、技术等方面的明显不对称地位，个人单凭其自身力量将无法对抗数据权力的压迫和支配，因此，个人信息国家保护义务必然要求国家介入，提供一套制衡性的个人信息处理权利义务规则。

2.组织与程序保障

制度性保障重点关注的是“个人—信息处理者”之间的权利义务关系结构；组织与程序保障则主要指：在基本的权利义务关系结构之外，需要通过组织和程序设计，为国家保护义务之落实提供担保性和辅助性制度，以促进个人信息受保护权之实现。这具体涉及到三个方面。首先，负有保护职责的组织系统如何设计；其次，信息处理者组织结构如何优化；最后，面向个人提供哪些基本的法律程序保护。

3.侵害防止义务

在制度性保障、组织与程序保障之外，国家保护义务的落实还指向侵害防止义务。国家需要综合运用多重工具，通过构建预防机制和协同法律责任来营造个人不受数据权力侵害的法秩序环境。 由于单一部门法所提供的责任机制无法独自完成国家保护个人信息的任务，因此，应从整体的国家保护义务框架来思考和建构个人信息保护法律责任体系。在这个意义上，宪法、民法、行政法、消费者法、刑法都可以为个人信息保护提供有针对性的法律责任机制，这意味着个人信息保护法是一个典型的“领域法”。我们应当摆脱部门法本位主义的路径依赖，考虑多元法律责任机制的协同。