权力结构失衡视角下的个人信息保护机制研究——以信息属性的变迁为出发点

雷丽莉

摘要

本文以信息属性的变化为出发点，指出数字经济时代个人信息的多重属性使得个人信息具有多个权利主体，而各主体之间的权力结构是失衡的。造成多元主体间权力失衡的原因在于，在个人信息问题上，不仅“私权力”有了双重角色，公权力也有了双重角色，都既是监管者又是利用者。这也使得个人在三方权力结构中处于弱势地位。随着“数字政府”已经成为现代政府的基本标志之一，公权力给个人信息带来的风险也会增加，这有可能导致围绕个人信息的权力结构更加失衡。而传统的私权保护制度和限制公权的机制在个人信息问题上都难以使三方权力结构重归平衡。在私权保护制度受到挑战、不足以为个体提供有效保护的背景下，需要立法以新的形式使技术为个人“赋能”，使个人成为权力结构中有力的行动者，而不是无力的被保护者。只有个体对其个人信息具有真实的、动态的知情权和控制力，才能有效监督公私权力的数据行为，进而实现权力结构的平衡。

关键词

个人信息、信息属性、信息主体、权力结构

作者简介

雷丽莉，大连理工大学新闻传播系讲师，电子邮箱：lilian.lei@qq.com。

本文得到国家社科基金一般项目“网络安全发展视角下‘平台型’网络运营商法律责任研究”（项目编号：17BXW090）的资助。

Research on Personal Information Protection Mechanism from the Perspective of Power Structure Imbalance——Taking the Changes of Information Attributes as the Starting Point

LEI Lili

Abstract

Taking the change of information attribute as the starting point, this paper points out

that the multiple attributes of personal information in the era of the digital economy make personal information have multiple rights subjects, and the power structure among the subjects is unbalanced. The reason for the imbalance of power among multiple subjects lies in the dual role of "private power" and public power, both of which are managers and users of personal information, which makes individuals in a weak position in the tripartite power structure. As "digital government" has become one of the basic symbols of modern government, the risks brought by public power to personal information will also increase, which may lead to more unbalanced power structure on personal information. However, the traditional protection system for private right and the approaches of restricting public power are difficult to maintain the balance among the three parties. At last, this paper points out that the legislation on personal information should regain the balance of power structure which was broken by information technology. Under the background that the protection system of private rights is challenged and insufficient to protect individuals, it is necessary for legislation to empower individuals in a new form and make them become powerful actors in the power structure, instead of passive subjects need others' protection. Only when individuals have real and dynamic rights to know and control over their information can they effectively supervise the data behavior of public and private power and realize the balance of power structure.

Keywords

Personal Information, Information Attribute, Information Subject, Power Structure

Author

Lei Lili is an assistant professor of Department of Journalism and Communication, Dalian University of Technology. Email: lilian.lei@qq.com

This paper is sponsored by National Social Science Fund Project "Research on Legal Responsibilities of Platform Network Operators from the Perspective of Cyber Security and Development" (No.17BXW090).

一、研究背景：信息革命、信息行为属性的变迁与社会重构

随着数字经济时代的到来，个人信息保护已经成为近年来立法的关注点。尤其是随着欧盟《通用数据保护条例》（GDPR）的颁布，个人信息保护议题在全球升温。2018年6月，美国加州通过了《2018加州消费者隐私保护》（CCPA）；2018年7月27日，印度公布《2018个人数据保护法（草案）》（The 2018 Personal Data Protection Bill）；2018年8月14日，巴西总统米歇尔·特梅尔签署通过了《通用数据保护法》（*LEG Geralde Proteçãode Dados*，缩写LGPD），该法将于2020年2月15日正式生效。[1]在中国，《个人信息保护法》也被列入第十三届全国人大常委会五年

立法计划中。除拟议的专门立法外，中国继在2017年10月1日实施的《民法总则》第111条规定“自然人的个人信息受法律保护”之后，拟议中的《民法分则（草案）》也在“人格权编”中将“隐私权和个人信息”单列一章（第六章）进行了规定。而在此之前，中国就已经通过《刑法修正案（九）》，增加了“侵犯公民个人信息罪”（第253条之一），并将其列入“侵犯公民人身权利、民主权利罪”（第四章）中。

个人信息保护之所以会成为全球普遍的立法焦点，与人类进入到信息社会这一背景密切相关。因此，探讨个人信息保护的问题，需要结合这一背景进行分析。1959年，丹尼尔·贝尔（Daniel Bell）在奥地利萨尔茨堡的一次演讲中首次提出了“后工业社会”的概念，并在1973年的专著《后工业社会：对社会预测的一项探索》（*Post-Industrial Society: A Venture in Social Forecasting*）中详细阐述了后工业社会是以信息为主导的社会。1980年，未来学家阿尔文·托夫勒（Alvin Toffler）在其著作《第三次浪潮》中对“信息社会”进行了预言式描述，这本书和他的另外两部专著《未来的冲击》（1970）和《权力的转移》（1990）被合称为“未来三部曲”。经过过去几十年信息通信技术的快速发展，这些学者所预言的“未来”已经成为现实：基于信息通信技术的互联网已成为社会生活的基础设施，信息和数据成为数字经济的基本生产资料，且因与物质能源同样重要而被称为“数字石油”。

随着互联网信息技术的发展，人类社会正在经历由“经济社会”向“信息社会”的新一轮重构。在这一轮的社会重构中，个人在技术“赋能”“赋权”的背景下被激活，形成了以个人为基本单位的信息传播新格局。“个人”被激活之后，信息传播生态的重构本质上是一场革命（喻国明等，2015）。在此之前，人类社会已经经历了从“宗教社会”到“政治社会”再到“经济社会”的两轮重构。生产力的发展使原有的社会结构和运行模式受到冲击并重构，这也带来权力结构的变化，使得社会生活的主导力量依次由教权转向世俗的君权再转向资本权力。这种权力结构的调整逐渐或交替触及人类的认知层面、态度层面和行为层面（如立法活动），从而使社会结构的调整呈现于制度层面。

信息技术的革命使得互联网从最初的通讯工具发展成为新媒体，进而又发展成为社会生活的基础设施。信息革命对社会权力结构的冲击和调整主要体现在社会生活的方方面面都与之绑定。也因为互联网在社会生活中有重要的地位和作用，故而普遍被认定为是“公共平台”，具有很强的公共属性。但互联网在归属上又隶属于一个个私人企业，由私人投资、私人所有、私人运营。它们不仅是网络空间新的权

力，而且正在改变着传统的“公”“私”边界，改造着整个社会的权力结构（雷丽莉，2018）。在此期间，个人虽然被互联网赋能、赋权，但在社会权力结构中作为一支崛起力量的却是网络运营商。在当前数字经济为主导的信息社会中，网络运营商因其在社会生活的地位和作用而被称为“私权力”。“私权力”的崛起主要体现在以下四个方面：1.数据成为互联网时代的重要生产资料，而这些生产资料主要由“私权力”掌握。2.“私权力”成为网络空间的规则制订者，并深刻地影响着社会生活。3.“公权力”和“私权利”的行使都越来越依赖“私权力”。网络运营商利用其平台和技术掌握着大量信息，使得公权力在履行职能的过程中越来越依赖其配合与协助。4.“私权力”越来越深入地参与到社会管理中（雷丽莉，2018）。有研究者认为，互联网“基于法律授权、公权力委托以及某些私主体在技术、平台和信息等方面的优势，打破了传统的‘公权力：私权利’的二元架构，形成了‘公权力：私权力：私权利’的新架构。”（周辉，2017）

对个体而言，信息通信技术的发展改变了其社会互动模式。人与社会之间的联系已经变得更数字化和网络化，在线活动大大取代了现场社交互动的基本方式。互联网用户在网络空间的信息活动产生海量个人信息，为网络运营商带来巨额财富。

在今天的数字时代，“人类”既是信息的“消费者”，也是“生产者”。在“人”的视野中，无论在哪个时代，人类都是世界的核心。因此，与“人”有关的信息成为“数字石油”中最有价值的部分。人们的在线活动——包括有意识的信息活动（如创建个人资料，与他人建立联系，在线演讲，或在各种在线平台上的其他社交活动）和无意识的信息活动（如“数字足迹”“行为痕迹”）——已不仅仅是信息传播活动，也是数字经济原材料的“生产”活动。个人的信息传播活动除了马克思所说的“精神交往”的属性之外，又具有了“生产”属性。

随着个人信息成为生产的“原材料”，越来越多的信息被挖掘、利用、互联和传播，人们变得越来越“透明”。信息的商业化利用、公共利用，使个人在被互联网“赋权”“赋能”的同时，也在失去对自身信息的控制力和不被打扰的安宁。保护个人信息不仅是与日常生活密切相关的公共议题，也成为立法者和研究者的庙堂议题。上述个人信息活动的“生产”属性使得“个人信息/数据”保护问题具有了多重含义，它不仅是一个关于公民权利议题，也成为一个政治经济学议题。

鉴于信息已成为信息社会中重要的“生产资料”[2]，且任何生产资料只有被开发、利用和流转才能实现其价值，因此，信息的充分、自由地流动以及数据的共享

和互连成为信息社会的基本需求。然而，目前全球性保护个人信息的立法趋势要求限制个人信息的收集、挖掘、利用和自由流动。因此，冲突便产生了。

回溯源头，个人信息曾被认为是数字时代的隐私，在美国，PI（Personal Information）/ PII（Personal Identifiable Information）仍然被用来判断隐私的界限。但从最近的立法趋势看，个人信息作为一项独立的权利已基本成为共识。除美国以外的许多其他国家和地区，个人信息都被认为是一项单独的权利，其与“隐私”被认为是分别受法律保护的两个交叉的圆。

与通过满足人们的好奇心和窥私欲，为黄色新闻业带来零星利益的隐私不同，个人信息已成为数字经济的“原材料”，可以直接买卖，产生价值。没有对隐私的挖掘利用，工业社会不会受到任何影响，隐私的贩卖并不是工业社会必不可少的；但在信息社会，许多产品和服务都是基于“个人信息/数据”产生的，如果没有对“个人信息/数据”的挖掘、使用，数字经济就无法运转，信息社会就不可能存在。此外，“个人信息/数据”与传统隐私之间的区别还体现在：隐私问题仅存在于二维关系中，即隐私主体与媒体或其他传播者之间，但“个人信息/数据”问题存在于四维关系（用户、平台、第三方平台和政府）中，这就使得情况更加复杂。

因此，谈论个人信息保护，只有立足于信息社会、数字经济的大背景下，分析个人信息在社会政治、经济生活结构中的位置，才能理解个人信息保护背后的权力结构以及相关主体间的权力关系。在个人信息保护问题上，中国与欧盟、美国，面临的同样挑战，但需要解决的问题实际上却不尽相同。在此认识的基础上，本文将通过对美国和欧盟关于“个人信息”的保护路径、国内立法、司法中的个人信息保护情况的考察，分析在普遍性的立法趋势下，个人信息保护机制所反映的权力关系和权力结构状况的共性和差异，以期引起立法部门的关注，为未来个人信息保护立法提供参考。

需要说明的是，本文所称的“权力关系”和“权力结构”中的“权力（power）”不是特指公权力，其所指代的是各类主体（包括“公权力”“私权力”和作为“权利主体”的个人）都具有的对个人信息的控制能力和救济能力。在这个意义上使用此概念是为了便于阐述个人信息相关的利益主体——个人、网络平台和政府在个人信息问题上的力量对比和制衡关系。

二、数字经济时代个人信息的多重属性、多元主体及其权力关系

（一）个人信息的多重属性与多元主体

信息技术的发展催生了新的经济形态，Don Tapscott在1994年撰写的《数字经济：智力互联时代的希望与风险》中首先提出了数字经济的概念（Tapscott，1994）。1998年，美国商务部发布了《新兴的数字经济》报告，由此数字经济成为通行的提法。二十国集团数字经济发展与合作倡议把数字经济定义为“以‘数据’为关键生产要素、以‘网络平台’为主要组织形式、以‘信息技术’的有效使用作为效率提升和经济结构优化的重要推动力的经济形态”。数字经济对个人信息的利用不可或缺：对社会而言，个人信息成为了重要的生产资料，同时也是进行公共管理和提供公共服务的重要资源；对个人而言，个人信息成为打开各项权利（包括人身权、财产权）的钥匙，让渡一定的个人信息，又成为个人享受各种公共服务、社会服务和企业服务的前提。因此，个人信息兼具个体属性、商业属性和公共属性三重属性。

正因为个体属性并非个人信息的唯一属性，因此，当立法规定个人信息受法律保护时，学界关于个人是否是其所保护的唯一主体以及个人信息该以何种路径进行保护产生了分歧。例如，刑法学界关于“侵犯个人信息罪”究竟保护的是个人法益还是超个人法益，以及何种具体法益就有三类观点。一类是个人法益说[3]，持此类观点的研究者认为个人信息立法保护的是个人的人格尊严和自由，或者是个人的“信息自决权”。另一类是超个人法益说，该类观点从现实出发，指出大数据技术下的个人数据信息具有数量大、价值密度低、智能处理以及信息获得和其使用结果之间相关性弱等特征，使得个人无法以私权制度为工具实现对个人数据信息的产生、存储、转移和使用进行符合自己意志的控制。因而私权制度在大数据技术下正逐步失去作用，所以，应该放弃以私权观念来规制个人数据信息的立法意图，而将大数据下的个人数据信息作为公共物品加以治理（吴伟光，2016）。[4]还有一类是个人法益与超个人法益综合说，该类观点认为“公民个人信息”首先是个人法益，“公民个人信息权”是公民个人自决权范围内的个人权利，因此，合法与非法的界限在于公民是否许可、同意。但个人信息处理行为的规制原则是防止滥用，而非严格保护，出于公共利益和公共安全的需要，可以无须个人同意，实现个人数据信息的自由共享（曲新久，2015；任龙龙，2016）。还有学者提出，在我国，“公民个人信息”长期处于附属保护模式，依附于国家法益、社会法益以及公司商业秘密等相关法益进行“连带”的保护，从我国刑法关于“公民个人信息”保护的立法、司法思路来看，无不体现着对其他相关犯罪的预防性、前置性立法思维，而非单纯对“公民个人信息”的保护（于冲，2018）。

从上述分析可以看出，个人信息所负载的远非其字面意义上的个人基于其自身信息的人格利益，而是更加复杂，也更加抽象。当我们在讨论个人信息时需要明确个人信息只是“关于”个人的信息（information about a person），而不是“属于”个人的信息（information of a person）。就像“我的照片”（照片拍摄的是我）未必是“我的照片”（照片并不属于我），它上面可能附着着其他主体的权利，如拍摄者的著作权、所有者的物权等。而且，在实践中，数据的使用权往往比所有权更重要，只要能够使用就能产生价值，因此，归属问题变得不那么重要。同时，个人信息的使用权不论是在政府公共管理中还是数字经济的商业运转中都有至关重要的作用，因此，它有了积极利用的支配性属性，这与传统人格权只是消极的防御性权利不同（王利明，2019）。个人信息的这一属性，使得其权利主体变得多元。因为“公权力”和“私权力”主体基于其职权、法律授权或与用户授权也有对个人信息积极利用的权利，这使得围绕个人信息的权力关系和结构比其他人格权更复杂。

（二）“私权力”和“公权力”在个人信息法律关系中的双重角色及其对信息主体的影响

个人信息的多重属性，使其对不同主体具有不同的价值，也带来了相关主体间权力关系的调整。个人信息所涉及的多元主体中，APP背后的网络运营商最有条件和能力获取海量个人信息。目前个人信息相关的立法和规范性文件也主要针对这些网络运营商。各网络运营商也根据立法和各项安全标准调整自身的数据行为，包括调整隐私政策、设立个人数据保护官（DPO）等，来确保自身数据行为的合规性。在国际上，受欧盟GDPR影响最大也最直接的就是谷歌、Facebook等美国的全球性互联网巨无霸，他们因侵犯用户隐私信息不得不面临欧盟或本国政府开出的巨额罚单。因此，个人信息保护立法影响最大的就是新崛起的“私权力”。

但是，网络立法并不是一味限制私权力接触和使用个人信息。这是因为“发展”和“安全”都是网络立法要考量的因素。从“发展”的要求看，禁止或过度限制“私权力”获取、使用公民个人信息显然是不利于数字经济发展的。从“安全”的角度看，也不能过度限制“私权力”，反而需要更多地赋权于“私权力”。网络安全立法有两个重要矛盾需要解决，一是无限的网络信息和有限的行政执法资源之间的矛盾，二是不断推陈出新的信息技术和法律的稳定性要求之间的矛盾（雷丽莉，2018）。目前对于此矛盾的解决路径是，由作为市场主体的网络运营者承担网络安全管理职能。如我国《刑法修正案（九）》首次明确规定了“拒不履行信息网络安全管理义务罪”，网络服务提供者不履行安全监管义务将可能承担刑事责任。

《网络安全法》也是以给网络运营商设定义务的形式使其承担安全监管责任。

对个人信息而言，一方面，个人信息安全也是网络安全的组成部分，保障个人信息安全是网络运营商安全管理义务的范畴。另一方面，网络服务提供者履行安全监管责任也需要利用用户个人信息。因此，尽管从立法上看，这是为网络运营商设定了义务，但相对于用户而言，是为网络运营商赋权，增强了其对用户的监管，从而使得二者的地位变得更加不平衡。

鉴于网络运营者已经不是纯粹的市场主体，而是对网民的信息活动具有监管职责的主体，个人作为“私权利”主体是没有能力将“私权力”关进笼子里的。尽管个人信息立法对个人进行了“赋权”，使个人信息成为一项独立的人格权利，但却并没有为个人“赋能”，即个人并没有能力监督“私权力”对个人信息的使用行为进而保护自身个人信息。因此，如何把“私权力”关进笼子里，使其发挥应有作用而不损害个人权利，是网络法要解决的重要问题。个人信息保护立法作为网络安全立法的重要组成部分，也试图解决这一问题。

另外，在个人信息保护的制度设计中，“公权力”的角色是监督“私权力”，保护“私权利”。但现在，在个人信息问题上，公权力的角色也发生了变化。不同于传统隐私权保护中政府超然的中立地位，在个人信息保护和利用中，政府积极加入其中， 具有了双重身份角色：不仅是作为管理者监督其他主体对个人信息的非法利用，同时，政府自身也是公民个人信息积极的利用者。一方面，政府作为社会管理和社会福利的承担者，公共安全、公共管理和公共福利的推进都离不开对居民个人信息的掌握；另一方面，出于对行政效率的追求，政府也会不断积极探索个人信息利用的限度和价值（张新宝，2015）。公权力获取个人信息的渠道可分为两类，一类是基于自身职权直接从个人或其他公权力机构获取，另一类是基于相关法律法规的授权，从“私权力”处获取个人信息。如《网络安全法》规定网络运营者对网信部门和其他有关部门的监督检查予以配合，为公安机关、国家安全机关提供技术支持和协助。同时，鉴于公民和法人都有配合执法的义务，从理论上讲，只要是“私权力”掌握的信息，“公权力”都有可能获得。当然，不同的公权力部门之间获取个人信息的渠道和权力有很大差异。

因此，个人信息保护立法不仅仅要在“私权力”和“私权利”之间进行平衡，“公权力”也是权力结构中的重要一方。围绕个人信息的立法，正是通过规范相关主体的数据行为，完成了对各主体围绕个人信息的权力关系的调整。而在此权力结构中，尽管私权力是一支崛起的力量，但真正被“赋能”的，还是公权力。而个人

在个人信息保护上尽管被“赋权”，但是由于其“无能”监督公权力和私权力对个人信息的收集和利用，因而普遍处于“有权无能”的地位。

（三）个人信息立法需要实现多元主体的权力平衡

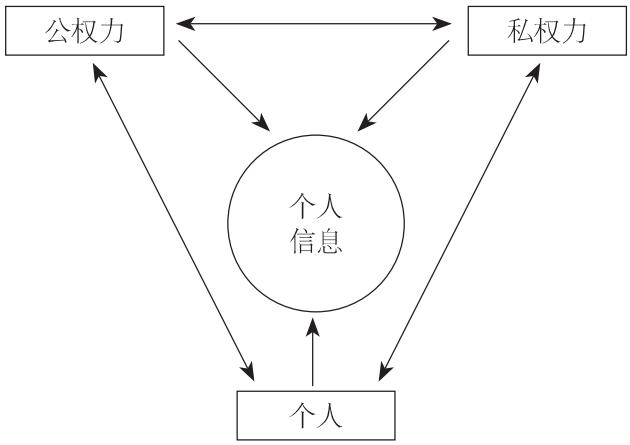

图1：个人信息的三类权利主体

对于围绕个人信息的三类权利主体，张新宝教授提出“三方平衡”的主张。“三方平衡”是指个人对个人信息保护的利益（核心是人格自由和人格尊严利益）、信息业者对个人信息利用的利益（核心是通过经营活动获取经济利益）和国家管理社会的公共利益之间的平衡。平衡是一种张力状态，各利益主体的核心利益得到保护和实现，并让渡非核心利益作为他方实现其核心利益的条件和基础（张新宝，2015）。

本文认为，相比利益平衡，权力平衡更重要。利益平衡是一种静态的制度设计，利益通常表现为立法中的“权利”，但与权利同样重要甚至更加重要的是权利的实现能力，即维护各自利益的能力也要平衡。权力结构失衡是无法实现利益平衡的。只有各个主体都“平等武装”才能形成互相制衡的稳定的三角结构，才能有动态的平衡和真正的个人信息的安全，利益平衡才能实现。本文后文将结合欧盟、美国和中国围绕个人信息的立法和司法实践，考察欧盟、美国和中国在个人信息保护中的权力结构。

三、欧盟和美国个人信息保护机制中的权力结构概述

（一）欧盟

根据GDPR，个人信息是自然人保护其个人资料的权利，属于自然人的基本权利和自由。这一权利在学界常被称为个人的“信息自决权”。1983年，德国联

邦宪法法院在对“人口普查案”的判决中最早确认了个人信息自决权。判决称，“在现代数据处理环境中，公民个人信息不受无限制的收集、存储、利用和传递。这是《基本法》第2条第1款（每个公民都享有自由发展人格的权利）与第1条第1款（人的尊严神圣不可侵犯）的保护范围。该基本人权保障每个人原则上有权自行决定其个人信息的交付与使用”。可见，“信息自决权”是由德国联邦宪法法院通过判例发展出来的，是公民个体享有的宪法权利，是一般人格权的下位概念。在研究领域，最早提出“信息自决权”（Das Recht auf informationelle Selbstbestimmung）概念的是施泰姆勒（Steinm ü ller，1972）。他在《联邦数据保护法（草案）说明》中将这项基本权利的内涵表述为“人们有权自由决定外在世界可多大程度获知自己的思想及行动”。第2条第1款规定的人格自由发展权的防御基本权（Abwehrgrundrecht），是由一般人格权发展出、独立作为宪法法益的具体人格权，内涵为面对国家时，公民个体对搜集、使用和处理其个人信息的行为的决定权（敬力嘉，2018）。从此概念产生的背景看，其最初的功能是防止国家公权力对个人信息的滥用，是通过设定私权来对抗公权力的制度设计。

随着社会信息化进程的推进，对个人信息的挖掘和使用成为个人得以享受各种公共服务、社会服务和企业服务的前提。于是，最初作为对人格权防御性保护的个人“信息自决权”受到挑战。在德国，联邦宪法法院通过判决，明确对个人信息的搜集、使用和处理要符合显著公共利益、基于法律保留的合目的、透明必要与合比例这四项基本原则。此后，联邦宪法法院又在2008年网络搜索案的判决中，明确认定“IT系统（包括任意虚拟或实体的、存储个人数据的系统）的私密性与完整性”是公民享有的基本权利，作为信息时代对公民个体“信息自决权”的补充，间接实现公民个体对IT系统中关于自己个人数据自决权的保护。有学者认为这么做的目的是为了给个人数据使用应遵循的法律保留原则松绑，找到信息自决权保护与信息自由流动之间的平衡点（敬力嘉，2018）。GDPR也指明其所保护的是自然人的基本权利和自由，尤其是自然人保护其个人资料的权利的同时，规定不得以保护个人与数据处理相关的自然人为由，限制或禁止个人数据在欧盟内部的自由流动。2018年10月，欧盟还通过了《非个人数据自由流动条例》，可见，欧盟也在寻求个人信息保护与信息自由流动之间的平衡。

从实际情况看，受GDPR影响最大的主要是“私权力”，尤其是美国的互联网巨无霸。根据GDPR，违规企业可能会被处以高达2000万欧元或全球营业额4%（以较高者为准）的罚款。欧盟国家依据GDPR对美国互联网企业的个人信息收集和使

用展开调查，并开出了巨额罚单。2018年10月，谷歌因数据泄露影响近5000万用户，被爱尔兰数据保护委员会（DPC）调查。2019年1月21日，谷歌因违反GDPR的透明性原则和提供充分信息义务，以及针对个性化广告缺乏数据处理的合法性基础（不符合用户同意的要件）被法国数据监管机构CNIL处以5000万欧元的罚款。被处罚的除了美国的互联网巨无霸，也有欧盟本土的互联网企业。如2018年7月，德国的社交软件Knuddels被黑客入侵，盗走并在互联网上发布超过80万个电子邮件地址，以及超过180万名用户的用户名称及密码，Knuddels因此被当局开出2万欧元的罚单予以警告。除了互联网企业，很多传统行业由于都有网上服务，也因涉嫌数据违规而被开罚单。如万豪酒店网站自2014年起就遭黑客攻击，但直到2018年11月才被发现，由此导致涉及全球3.39亿条客户记录数据泄露（其中包括3000万欧洲人的信息），被英国信息委员会办公室（ICO）以未能充分保护客户数据处以9900万英镑（1.24亿美元）罚款。英国航空公司（ICAGY）也因泄露50万客户的数据而被ICO罚款1.834亿英镑（2.3亿美元）。

可见，保护个人信息立法的最初使命是对抗公权力对个人的伤害。但进入数字经济时代后，情况发生了变化，被处罚的主要是“私权力”。而政府以数据违规为由处罚企业的模式实际上是以“公权力”对抗“私权力”的形式实现对“私权利”的保护。不管是在欧盟还是美国，个人以保护私权为由寻求司法救济以对抗“私权力”的情形都不多见（Schwartz & Solove，2011）。而由个人启动的对抗“公权力”侵犯个人信息的情况，在欧盟仍然能够看到有，但很少见。例如，在比利时，曾有投诉人向比利时数据保护局投诉比利时市长滥用投诉人的个人邮箱向投诉人发送了竞选选举（拉票）信息。原因是投诉人之前曾委托一名建筑师向市长就房地产交易事项进行了咨询沟通，这位建筑师在其发送的邮件中附上了投诉人的电子邮件地址。后来市长在选举的前一天，使用投诉人的电子邮件地址，以“答复”的形式向投诉人发送了竞选（广告）信息。2019年5月28日，比利时数据保护局对该市长处以2000欧元罚款，理由是其违反了GDPR中的目的限制原则，市长获得的电子邮件地址必须用于特定目的，不得以与这些目的不相容的方式进一步处理。同时，比利时数据保护局指出，GDPR适用于任何控制人，当然也适用于市长等公权力拥有人。

值得注意的是，即使公权力因侵犯或未能有效保护其所掌握的公民个人信息而被罚，最终责任也有可能仍落在受害者自己身上。2019年6月，保加利亚发生了一场针对税务机关的网络攻击，造成公民个人信息泄露，受害范围几乎涉及所有成年

国民。被盗的信息包括姓名、住址以及个人收入等。盗取信息的黑客还给保加利亚媒体发了一封电子邮件，批评保加利亚政府网络安全状况，还分享了访问被盗数据的途径。邮件还声称，超过500万个人以及企业的信息被窃。据保加利亚个人数据保护委员会的代表称，该国税务机关目前面临高达2000万欧元的罚款。此类事件反映出的问题是：税务机关用于缴纳罚款的资金来自于纳税人，即税务机关因未能有效保护其个人信息，致使纳税人个人信息泄漏，而如果对其进行罚款，用的也是纳税人的钱。纳税人本是信息泄露的受害人，却需要用其所纳税款承担由此带来的罚款。

总之，在欧盟的个人信息保护机制中，主要是通过“公权力”对“私权力”的数据行为进行监督，达成对个人的保护。对于公权力的数据行为，个人是具有一定行动能力的“行动者”，但是其行动能力还是很有限的，毕竟公权力对个人信息的侵犯很少会以能被个人清楚知晓并掌握证据的方式进行。无论是对“私权力”还是“公权力”的数据违法行为，个人都很难得知，进而去监督和维权。

（二）美国

与欧盟不同，美国有着深厚的隐私法传统，并没有将“个人信息/数据”作为独立的权利进行保护，而是将其置于隐私这一大概念之下，将个人可识别信息，即Personal Identifiable Information（PII）作为界定信息是否属于隐私的重要因素。这是因为英美法的重要特点之一是“拟制”，即把新的权利纳入到旧的概念和体系中，“糅合了确定性与进化力之双重功能”（庞德，2001：128）。也正是由于PII在互联网普及之前就已经被纳入到美国隐私法中，因此，此后互联网的普及并没有导致个人信息作为一种超越隐私权的全新的权利被提出。但是，尽管美国在联邦层面没有个人信息立法，但却有多部地区性的或专门针对特定群体的成文法，如2018年的《加州消费者隐私法》（California Consumer Privacy Act，CCPA），以及此前的《家庭教育权利和隐私法》（1974）（Family Educational Rights and Privacy Act，FERPA)和《儿童在线隐私保护法》（1998）（Children’s Online Privacy Protection Act，COPPA）等。根据相关立法和案例，进行了“匿名化”（anonymization）或不可识别处理的信息就不再是个人信息。但是，随着信息技术的发展，即使对个人信息进行了“匿名化”处理，仍有可能被再次识别，给信息主体带来伤害。Paul Ohm认为，PII已经无法用来划定隐私的保护范围，因此应当放弃PII作为界定隐私的核心概念（Ohm，2010）。但是，多数学者仍然认为PII是隐私权的核心概念，如Paul M. Schwartz和 Daniel J. Solove认为，用PII界定隐私范围固然有缺陷，但不能

因此抛弃PII，他们提出应当将PII发展为PII2.0，解决目前用PII划定隐私范围中存在的问题（Schwartz，Solove，2011）。

与德国一样，美国最初也是在1970年代政府进行人口普查的时候提出PII这一概念的。美国在人口普查中第一次使用计算机对各种身份标识信息进行批量处理，由此创设了PII，对这种并不会使人产生羞耻感的信息进行保护，以防御公权力对个人信息的过度掌握和利用。美国1974年的《隐私法》也是针对联邦行政机构的行为而制定的。1977年，联邦最高法院在Whalen诉 Roe案中确立了信息隐私权（Right to informational privacy），Stevens大法官把信息隐私权归纳为：其一，自然人所享有的控制其个人信息被披露的利益；其二，自然人所享有的独立做出某种免受政府影响的决定的利益。1989年，最高法院在美国司法部诉记者自由委员会[5]一案中也认为信息隐私权是指自然人所享有的对关乎其自身信息的控制权（张民安，2014：4）。至此，对个人信息的保护仍然是私权保护的路径，针对的也主要是作为“公权力”的政府。后来，个人对个人信息的“控制权”才由对政府机构收集、处理和使用的限制延展到私人机构。有学者指出，在美国，针对政府机构的是宪法性信息隐私权，而针对私人机构的则是非宪法性的信息隐私权（何渊，2018）。

与欧盟情况类似，在美国，个人直接以保护个人信息为由对抗“公权力”或“私权力”的数据违法行为的情况也很鲜见。另外，在美国，“私权力”在个人信息问题上在一定程度上是能够对抗“公权力”的。前文提到，公权力获取公民个人信息主要有两条路径。一是依职权直接获取，二是依据法律法规授权从“私权力”获取。在第二条路径上，“私权力”可以在一定条件下对抗“公权力”对个人信息的获取，但是，“私权力”对公权力的这种对抗能力也在弱化。例如，2013 年，美国纽约联邦地区法院向微软公司签发了一份搜查令，要求其协助一起毒品案件的调查，将一名用户的电子邮件内容和其他账户信息提交给 FBI。微软以该用户的电邮内容数据存储在微软位于爱尔兰的数据中心而非美国境内为由拒绝向 FBI 提供，并提出废除搜查令的动议。美国司法部因此提出对微软的诉讼。但该案还未审结，CLOUD 法案（Clarify Lawful Overseas Use of Data）就出台了。根据 CLOUD 法案规定：无论通信、记录或其他信息是否存储在美国境内，服务提供者均应当按照规定的义务要求，保存、备份、披露通信内容、记录或其他信息。据此，美国政府得以跨境调取科技公司存储在海外服务器上的美国公民信息。这一法案明显增强了政府获取用户隐私信息的权力。

不管在欧盟还是美国，都很少有个人能以自己的名义，作为积极的“行动者”

参与到个人信息权利的实现中。最常见的情形是，“公权力”履行管理者职能，依职权处罚“私权力”，间接实现对个人“私权利”的保护。而当“公权力”作为个人信息利用者向“私权力”索取个人信息时，“私权力”也会以保护“私权利”的名义与之对抗。个人信息的私权保护机制已经改变了形态。尽管根据立法规定，个人仍然可以以自己的名义、通过自己的行为保护个人信息，但这已经不再是私权实现的主要路径。私权制度原本是对抗公权的制度设计，但现在私权的实现却主要是依赖公权力，这种改变带来权力结构的失衡。在个人信息保护问题上，个人不是有力的“行动者”，而是被公权力或私权力“代表”，成为权利实现过程中的“旁观者”。而无论在欧盟还是美国，“公权力”都是强势的行动者。这种改变会带来什么样的后果？能否实现利益的“三方平衡”？目前还缺乏深入的研究。

四、中国个人信息保护机制中的权力失衡问题及对策

（一）个人信息立法所形成的权力结构

中国关于个人信息保护的规定散见于多部不同的法律法规、部门规章和司法解释中。尽管专门的《个人信息保护法》还未颁布，但在《民法总则》规定个人信息受法律保护之前，《身份证法》《保险法》《旅游法》《公共图书馆法》《出入境管理法》《反恐怖主义法》《国家情报法》《核安全法》《测绘法》《统计法》《消费者权益保护法》以及《电子商务法》等专门法都对其所规范的特定领域的个人信息进行了规定。这些部门法所规范的大多都是政府机构和部门的行为。政府机关处理个人信息是履行法定职责、实施行政管理的必然要求，从法律性质上看属于行政法律关系。相反，其他个人信息处理者处理个人信息是一种民事主体的自主活动，在法律性质上属于民事法律关系（张新宝，2019）。因此，个人信息首先是在行政法律关系中被调整，然后才被纳入民事法律关系中调整。个人信息出现在立法中的最初目的也在于防止公权力对个人信息的滥用，从这点上看，中国和欧美是一致的。

此外，刑法对个人信息的规定也走在民法之前。中国刑法中关于个人信息的保护始于2005年《刑法修正案（五）》增设的“窃取、收买、非法提供信用卡信息罪”。 2007年的《刑法修正案（七）》又增设了“侵犯公民个人信息罪”，“出售或者非法提供”和“窃取或者以其他方法非法获取”公民个人信息都构成此罪。但该罪的犯罪主体仅是“国家机关或者金融、电信、交通、教育、医疗等单位的工作人员”。在2012年12月28日全国人大常委会颁布了《关于加强网络信息保护的决

定》之后，2015年的《刑法修正案（九）》又将此罪的犯罪主体扩展为一般主体，这是对《关于加强网络信息保护的决定》从刑法层面的呼应。与此前“窃取、收买、非法提供信用卡信息罪”被列入《刑法》第三章“破坏社会主义市场经济秩序罪”中不同，“侵犯公民个人信息罪”被列入到《刑法》第四章“侵犯公民人身权利、民主权利罪”中。2016年11月7日，《网络安全法》颁布，第四章“网络信息安全”也主要是对网络运营者义务的规定。直到2017年《民法总则》的颁布，个人信息才开始被纳入民事法律关系中进行调整。这一立法过程反映出个人信息立法的两个趋势，一是“刑先民后”，二是立法针对的主要对象由“公权力”转向“私权力”。

在民法领域，“个人信息”主要见于《民法总则》第111条，和《民法分则（草案）》第3编“人格权”的第6章“隐私权和个人信息”中。根据杨立新教授对《民法总则》立法过程的介绍，在最早的2015年8月28日《民法总则（草案）·民法室室内稿》中，并没有规定对“个人信息”的保护。随后在2015年“征求意见稿”、2016年5月27日“征求意见稿修改稿”，以及2016年6月27日《民法总则（草案）》“第一次审议稿”，也都没有对个人信息保护作出规定（杨立新，2018）。但是，在此期间发生了两起电信诈骗案，引起了立法机关的高度重视。一是徐玉玉案。犯罪嫌疑人杜某攻击了山东省2016高考网上报名信息系统，盗取了包括徐玉玉在内的大量考生报名信息，并将其以每条0.5元的价格卖给陈文辉，陈文辉利用此信息对徐玉玉实施了电信诈骗，造成徐玉玉心脏骤停离世。二是清华大学教授案。清华大学一位教授被冒充公检法的人员电信诈骗人民币1760万元。这两起电信诈骗案使立法机关受到震动，促使在《民法总则》中增加了个人信息保护的内容（杨立新，2018）。有学者指出，《民法总则》正是由于考虑到个人信息的复杂性，因而没有简单以单纯民事权利特别是一种人格权的形式加以规定，而是笼统规定个人信息受法律保护，为未来个人信息如何在利益上兼顾财产化，以及与数据经济的发展的关系配合预留了一定的解释空间（龙卫球，刘保玉，2017：404）。从这一立法过程看，“个人信息”被写入《民法总则》，并非因为考虑到其作为一项独立权利所具有的价值，而是基于对个人信息的侵害可能给个人人身财产安全带来的风险。因此，当个人基于个人信息（个人敏感信息除外）的利益和公共利益、商业利益发生冲突时，只要不会给人身财产安全带来风险，立法的天平是倾向于后者的。

从上述关于个人信息的立法历程看，先有部门法和刑法中关于个人信息的规定，然后才有民法总则关于个人信息的确权性规定，“个人信息”首先是出现在各

种行政管理法中，然后才出现在权利保障法中，刑法和行政法都走在民法前面，呈现出“行先民后”“刑先民后”的立法轨迹。尽管从“行先民后”的立法顺序看，在个人信息立法中首先被约束的是公权力机构，但是由于这些专门法中往往只是规定不得滥用依职权所掌握的个人信息，但并没有明确的责任后果，而且缺乏对非法使用个人信息行为的界定，因此，为公权力合法侵犯公民个人信息留下空间，因而对公权力处理个人信息行为的约束很有限。

此外，无论是《网络安全法》还是《刑法》关于个人信息的规定，义务主体都是网络服务商，即立法的主要监管对象是“私权力”的个人信息违法行为。公安部网络安全保卫局联合北京网络行业协会、公安部第三研究所发布《互联网个人信息安全保护指南》以及全国信息安全标准化技术委员会的个人信息安全标准，也主要是为私权力的数据行为提供指引，进行规范。从对数据行为的监管看，私权力的数据行为受到来自网信办的有力监督，但对公权力的数据行为却缺乏真正有效的监督机制。在当前的个人信息保护机制中，约束公权力的专门法缺乏有效的监督和问责机制，而《刑法》《网络安全法》则旨在约束私权力。目前的立法和安全标准都对“私权力”获取、利用公民个人信息进行了很全面细致的规定，但对于公权力获取和利用公民个人信息却缺乏明确细致的要求，对于公权力通过私权力间接获取和利用个人信息更是缺乏有效的规范和约束。因而，在围绕个人信息的权力结构中，公权力是受到约束和限制最小的主体。而且，在个人信息安全保障机制中，公权力往往作为“私权利”的“代表者”对“私权力”进行监督，从而使得公权力更加有力。

“私权力”作为最有能力直接获取、利用个人信息的主体，自然应当被关进笼子里。个人信息保护立法也主要对其数据行为进行约束。但是，把“私权力”完全交给“公权力”去监管，会使“私权力”服务于“公权力”，这样一来，“私权利”就难以真正得到保障。公权力作为个人利益的保护者的身份在法律中被确认，但立法对其作为个人信息利用者的身份重视显然不够，致使在三方利益平衡中，公权力自身围绕个人信息的利益被淡化处理。作为信息主体的个人对来自私权力的侵犯往往无能为力，但被忽视的是，其对于公权力以“合法”形式侵害个人信息的行为更加无力。因此，个人在围绕个人信息的权力结构中处于“被代表”的“有权无能”的弱势地位也就是很自然的结果了。因此，在“私权力”崛起的背景下，应当更加警惕“公权力”。“私权力”被关进笼子里的后果，不应该是“公权力”坐大。而且，相比“公权力”，“私权力”是去中心化的，保持“私权力”与“公权

力”的制衡，才能更好地保护“私权利”。

前述各专门法中关于个人信息的规定，虽然体现出对公权力的限制，也意在保护行政管理相对人的信息安全，但总体是为了保障行政活动的安全有序。从个人信息的立法轨迹也可以看出，个人信息保护制度体系呈现更多的是安全本位而非权利本位。网络安全是国家安全的重要方面，而信息安全是网络安全的重要内容，个人信息是网络信息的重要组成部分，由此，个人信息安全才成为法律所保护的对象。因此，在关于个人信息的制度设计中，个人被设定为一个被动的被保护者，而不是具有行动能力的独立主体，权力失衡就是很自然的现象了。

（二）从司法实践看个人信息保护机制中的权力失衡及其原因

根据笔者于2018年12月28日访问中国裁判文书网检索相关数据结果显示，案由为“非法获取公民个人信息罪”的共有635条记录，没有附带民事诉讼的案件，因而也没有对被害人的赔偿。其中自诉案件仅2起（一起以原告撤诉告结，另一起一审以罪证不足裁定驳回，二审裁定发回重审，查不到后续的公开判决）。案由为“出售、非法提供公民个人信息罪”的案件共54条记录，没有附带民事诉讼的案件。自诉案件仅1起，且因“未能提供相应的证据材料且申请法院调取的证据不在法院依职权调取证据范围内”，而被法院裁定“不予受理”。[6]在民事案件中，根据张新宝教授的统计，截至2018年9月2日，真正涉及个人信息且援引《民法总则》第111条做出判决的案件只有一起（张新宝，2019）。

由此可见，尽管立法规定公民个人信息受法律保护，但是，个人通过司法途径寻求对个人信息的救济并没有成为个人保护其个人信息的主要路径。其原因可以归纳为两个方面。一方面，侵害个人信息所造成的人格和财产利益的损害十分难以证成。由于个人信息价值密度低，侵害“个人信息”往往很难有具体可见的利益损害，也不会产生像侵害名誉权、隐私权那样的精神损害。例如，在庞理鹏以隐私侵权为起诉北京趣拿信息技术有限公司（去哪儿网：www.qunar.com）和东方航空公司侵害其姓名、身份证号、手机号、行程等信息一案中，判决仅要求被告在首页以公告形式向庞理鹏赔礼道歉，而且，由于“现有证据无法证明庞理鹏因此次隐私信息被泄露而引发明显的精神痛苦”，因此法院对其精神损害赔偿的诉讼请求也未给予支持[7]。个人信息与名誉、隐私等直指人格利益的权利不同，它侵害的客体既包括个人的人格及人身财产安全等利益，此外还有数据市场的秩序和其他公共利益。而一旦侵权人利用个人信息进行其他的违法活动，又属于另外的违法行为。例如，电信诈骗造成财产损害，可以以欺诈或诈骗的诉由获得救济，而不是以个人信息的名

义。这就使得个人缺乏启动个人信息诉讼的动力。另一方面，信息通信技术的发展和普及使得整个社会平台化，经营各个电子平台的是无数的网络运营商，用户每天都在无数个平台上活动、留下自己的信息，这使得个人往往难以确认究竟是谁泄露了其个人信息，因而难以有效寻求法律救济。张新宝教授指出，维权的成本高、因果关系证明困难、赔偿数额低是民事诉讼途径保护个人信息不力的主要原因。“难度系数”高，赔偿额度低，难以为自然人个人踊跃运用民事诉讼手段为自己的个人信息维权提供足够的激励（张新宝，2019）。这都使《民法总则》对个人信息保护的立法成为“无牙老虎”，无法使个人以自己的行动捍卫其作为信息主体的利益。

据张新宝教授统计，涉及个人信息案的被告几乎都是法人，原告与被告之间的“能力天平”具有较大倾斜，二者的实力差距悬殊（张新宝，2019）。鉴于个人维权的难度极大，因而将“私权力”置于“公权力”监管之下就成为了解决的路径。但是，由“公权力”来监管“私权力”下尽管看起来能解决个人救济能力不足的问题。但是，这一路径难免会“按下葫芦浮起瓢”。首先，在个人信息问题上，国家不再单纯以超然利益关系的治理者出现，它同时也是最大的个人信息收集、处理、储存和利用者（张新宝，2015）。公权力对个人信息的占有和利用的动力并不比私权力少。而且，即使在“私权力”崛起的背景下，“公权力”仍然比“私权力”要强大，“公权力”所能够掌握的信息并不会比“私权力”少，但立法并没有为“公权力”从“私权力”获取信息设定明确细致的条件，对“公权力”如何使用信息也缺乏有效的监督。因此，这一路径使得公权力的手能够借助“私权力”伸得更长，控制力更强，最终是不利于“私权利”安全的。因此，把私权力完全置于公权力的监管下，并不能实现三方平衡的效果，反而会使个人在三方主体的权力结构中处于更加弱势的地位。

值得注意的是，在个人信息所涉及的三方主体关系中，无论是涉及个人信息的行政法律关系中，还是民事法律关系中，在法律关系确立之时，相关主体的权力就已经不平衡。例如，关于“个人信息”的诸多立法都要求对“个人信息”的收集、使用应当“合法”“正当”“必要”，并且要明示和经过被收集人同意。“知情同意”原则可以说是民事活动中需要遵循的基本原则。但在“个人信息”问题上，这一原则似乎变得无效了。用户同意隐私政策，看似使用户“知情”，而且获得了其“同意”，但这种同意等同于“放弃”。很多分析把原因归结为隐私协议过于冗长专业，用户不可能读完，也看不懂。也有一些研究在对大量隐私政策文本进行的分析的基础上，提出改进对策。但如丁晓东教授所指出的，如果强行要求网站的隐私

公告以简单的政策来表述其复杂的实践，那么其结果只能是个体更不能有效地理解信息收集者的隐私政策（丁晓东，2019）。因此，问题的核心原因在于对于数据合规的种种制度设计没有充分考虑到信息属性在数字经济时代和信息社会的变化。人格利益不是“个人信息/数据”所附着的唯一法益，其作为社会管理资源的公共属性，其作为生产资料的商业属性都使得传统的私权、人格权保护原则受到挑战。因此，从现象来看，人们一方面重视个人信息，希望保护个人信息，另一方面又轻易地放弃了个人信息。这正是因为除了其所体现的人格利益，个人信息的社会价值、商业价值的实现也是每个个体的需要。正因如此，有学者提出，进一步赋予公民以限制处理权等权利也未必能很好地保护公民的权益。赋予公民被遗忘权、限制处理权等权利意在克服个体在行使初始同意后对其信息的进一步控制，但在实践中，这种对于信息收集后的进一步控制权常常难以行使。公民个体很难理解其信息如何被储存、使用和转移，从而也就很难对后续的种种信息处理行为进行控制（丁晓东，2019）。

此外，还值得注意的是，虽然个人通过司法诉讼寻求救济的案例很少，但是，在网络运营商之间的不正当竞争之诉中，却屡屡看到网络运营商将保护个人信息作为对抗其他运营商使用数据的理由。例如，在“新浪微博”诉“脉脉”不正当竞争案[8]中，“新浪微博”就以保护其用户的个人信息作为其禁止“脉脉”使用其数据的理由之一。在美国的hiQ诉LinkedIn案中，LinkedIn也以同样的理由禁止hiQ使用其用户数据。可见，保护用户的个人信息往往成为网络运营商保护其竞争利益的借口和工具。这进一步说明，司法实践中的个人信息与我们认为的保护个人信息就是保护信息主体个人利益的认知之间是存在很大差异的。

立法对个人信息的保护，不仅成为了私权力对抗其他私权力的借口，在美国，保护用户个人信息也成为公权力和私权力互相对抗的理由。私权力的崛起，使得个人信息保护制度的主要矛头由最初的针对公权力，转向针对私权力。尽管私权力在一定程度上可以对抗公权力，但这种力量也在弱化。如前文所述，CLOUD法案一出台，私权力只能乖乖地把用户信息奉上，尽管信息存储于境外。可以说，个人信息各主体的权力失衡状况在全球普遍存在，但是，其力量对比还是有很大差别的。在中国，保护个人信息只能作为公权力约束私权力的理由，私权力还很难以保护个人信息为由对抗公权力。由此，公权力成为个人信息的权力结构中的最有控制力的一方。而个人在执法和司法实践中常常被公权力或私权力代表，这样的权力格局显然更有利于“代表者”，而不是作为“被代表者”的个人。因此，尽管在个人无力

维权的背景下，由公权力代为维权有其现实意义，但是，其所带来的新问题是：谁有能力监督公权力？如果行政不作为、乱作为，个人该怎么办？个人以民事诉讼寻求救济尚且很难，通过行政诉讼寻求救济的难度就可想而知了。同时，鉴于私权力也难以有效监督公权力，那么，就只能依靠公权力内部的互相制约了。但鉴于公权力内部监督缺乏有效的动力机制，因而其效果也是存疑的。因此，在私权制度在个人信息保护上并不能有效地武装个人，而个人又不能过度依赖公权保护的情况下，立法应考虑的是，应该如何“赋能”于个人。在网络空间，“私权力”代“公权力”监督“私权利”的网络行为，“公权力”则代替“私权利”监督“私权力”，那么，该由谁来监督“公权力”？公权力保护私权利的动力来源于哪里？如果个人无法有效监督公权力，如何保证它会保护私权利？公权力对个人信息是有其自身的利益的，尤其是面对利益冲突的时候，个人作为信息主体的权利很难得到保障。因此，如何“赋能”于个人，使个人有能力监督公权力的数据行为及其对私权力的监管行为成为未来个人信息保护机制要解决的核心问题。

（三）个人信息保护的路径选择：使技术为个人“赋能”

在学界，多位学者已指出了私权制度在保护个人信息问题上的不足。如，张新宝教授指出，仅仅规定权利是不够的，因为它们太容易被虚化，沦为“纸面上的权利”。即便在以法院为中心的美国，个人信息的保护也多由美国贸易委员会（FTC）承担，而非经由诉讼解决，站在维权第一线的都是监管机构，而非权利人。而且，私权模式也不足以防范国家对个人信息的侵犯（张新宝，2018）。王利明教授指出，侵害个人信息通常是“大规模的微型侵害”，因而对个人信息的保护应注重预防（王利明，2013）。丁晓东教授也认为，强化个体赋权对于真正保护公民的隐私权益并无帮助，而且无条件地强化个体信息赋权无疑会给企业、政府与社会带来信息障碍（丁晓东，2019）。将个人信息“权利化”的私法进路会面临隐私权益保护过度与保护不足的双重问题。在美国，阿兰·威斯丁在《隐私与自由》中也没有将个人信息泛化为一种私法意义上的权利，其所说的个人对信息的控制权主要针对的是计算机、现代科技以及与此相结合的权力对个体的威胁，并没有以私法的视角看待“个人信息权”（丁晓东，2018）。

目前，也已经有多位学者提出超越私权制度的对策建议。王利明教授提出，对于此种诉讼动力不足的情况，需要由国家公权力机关作为公共利益的代理人去追究侵害人的责任，保护公共利益（王利明，2013）。张新宝教授指出，面对国家对个人信息权利的威胁，民法并不能提供充分的保护，《网络安全法》的主要规制对象是

“网络运营者”，个人信息保护法应当将“公权力机构”明确纳入调整范围，为政府对个人信息的收集、处理和利用设定公法架构（张新宝，2018）。除了借助公权外，张新宝教授还提出通过公益诉讼、集团诉讼发挥第111条的作用，用民事司法手段保护个人信息的设想（张新宝，2019）。丁晓东教授也提出，单一个体或消费者很难对企业等信息收集者与处理者进行监督，但各类公益组织和政府机构可以成为消费者集体或公民集体的代言人，对个人信息保护进行有效监督。各级消费者权益保护委员会可以针对企业在个人信息保护方面的一些不当行为提起公益诉讼，检察机关也可对此开展公益诉讼的探索（丁晓东，2018）。目前，司法中也已经出现了公益诉讼第一案。此外，丁晓东教授还提出美国的个人信息保护措施和相关立法带有明显的消费者法保护或公法规制的特征，我国也应通过“消费者法化”，即将个人信息视为派生于消费者法保护与公法保护的权利，而非一般性的私法权利，重新激发个人信息私法保护的活力（丁晓东，2018，2019）。

本文认为，首先，私权制度确实不足以对抗公私权力、保护信息主体的权益，这使得个人在个人信息问题上被解除了“武装”。相关机构对个人信息的收集、储存与流通已经大大超出了普通公民的个体预期，一个普通公民个体已经很难对伴随信息流通的风险进行预判（丁晓东，2019）。尽管民法学者力主确立个人信息的人格权地位，强调个人的信息主体地位，但在私权制度无效的情况下，赋权的象征意义就远大于其实际效用。在“赋权”的实际效果变得极为有限的情况下，解决问题的路径应该是为个人“赋能”，使赋权变得有意义，而不是不予赋权。尽管学者们提出了公权力机构和消费者协会等其他机构可以提供替代性保护措施，这些措施也都是具有现实意义的，但应当明确的是，公民应是个人信息法律关系中的“行动者”之一，而不是“旁观者”。个人信息权力结构的不平衡，使得公民个人面对企业、国家都是透明的，而国家、企业对个人信息的收集利用情况对信息主体却不透明。因此，立法不能因个人没有能力实现自己的权利，就不予赋权，或是由其他主体代为行使权利，而是应该思考如何为个人“赋能”，使其成为能够实现自身权利的积极的行动者，改变其“有权无能”的地位。这样，才能实现权力结构的平衡。

其次，有学者指出，尽管隐私权益保护的表现形式是防御第三人或共同体对私人空间的介入，其目的却在于促进个体在共同体中更好地交流信息，而非使其脱离社会，化为信息孤岛（丁晓东，2018），据此担心强化个体信息赋权，将个人信息视为一种可以对抗他人的权利，可能同时产生个人信息与隐私权益保护不足与保护过度的问题，即个体可能会轻率地放弃某些权利，从而使得自身的隐私权益受损；

个体又会过度行使自身的某些权利，从而妨碍个人信息的合理流通与使用，使每个人都成为一座孤岛，既无法进行正常的社会交往，也无法有效获取社会信息（丁晓东，2018，2019）。本文认为对此无需过于担心。尽管个人选择不是绝对理性的，但个人也是具有有限理性的，强化个体赋权并不会使个人任意限制他人对个人信息的使用，因为个人信息的社会价值、商业价值的实现也是个人的需要。但每个个体的利益都不同，不能交由他人代庖。立法所应当做的，是促进个人的理性选择。而这建立在个人对其他主体处理其个人信息行为的可知情、可监督的前提下。目前个人的知情仅限于隐私政策所描述的内容。而隐私政策只能让个人了解个人信息“可能会”被如何收集、处理，但却不能使其知晓个人信息“实然”的、动态的运行状态。而这些才是对信息主体的知情权、控制权最重要的。

再次，上述学者的对策性建议都存在一个未能解决的问题，就是其他主体对保护个人缺乏动力和缺乏来自个体监督的问题。首先，本文不否认国家规制的必要性，也并不反对借助公权、利用公法调整数据行为的现实意义和有效性。但这些路径只应当是对个人保护路径的补充，而不能是替代。无论是由公权力机构代为维权，还是社会团体，或者是专门的数据保护机构，都不是放任个人作为旁观者的理由。其次，正如王利明教授所指出的，应在法律上实现信息主体和信息控制者之间的地位平衡,从而赋予信息主体以知情权和控制权（王利明，2013）。这些代为维权的路径并不能使信息主体与信息控制者之间的地位平衡。张新宝教授也提出应通过国家主导、行业自律和个人参与, 实现个人对个人信息保护的利益、企业对个人信息利用的利益和国家管理社会的公共利益之间的三方平衡（张新宝，2018）。但本文认为，比利益平衡更重要的是权力平衡。只有三方主体平等武装，才能实现利益的动态平衡。即使有其他更便捷省力的途径，也不能成为让个人在个人信息权力结构中处于弱势地位的理由。只有个人能够知情、监督，这些代替个人维权的主体才有动力真正保护个人。

此外，“数字政府”已经成为现代政府的基本标志之一，公共秩序、公共安全和公共福利的推进，都离不开以个人信息为基本单位的数据库的支撑（张新宝，2015），这意味着未来公权力对个人信息的控制力将更强。中共中央办公厅、国务院办公厅2015年4月13日公布的《关于加强社会治安防控体系建设的意见》第10条指出，我国将建立以公民身份号码为唯一代码、统一共享的国家人口基础信息库，建立健全相关方面的实名登记制度，建立公民统一社会信用代码制度，并探索包含公民所有信息的一卡通制度。张新宝教授指出，政府机关对个人信息巨细靡遗的收

集，可能滑入“全方位监控型社会”；而打破信息壁垒， 形成个人信息资源共享体系也有可能诱发一次性泄露所有信息的风险；同样， 政府机关在执法、司法和行政过程中推进的信息公开， 也有可能忽略了所涉及个人的人格权利（张新宝，2018）。但其所提出的防控对策是，通过法律严格限制政府公权力， 将国家中心数据库的运作情况作为政务公开的重要内容加以公开，便于公众和社会进行监督，确保国家机关对国家中心数据库的正当利用（张新宝，2018）。张新宝教授也提出了加强个人监督的措施，具体包括在相关法律政策制定、执行和救济的各个环节借助网络平台等方式拓宽公民参与途径，强化公民利益表达、救济和监督，立法听证、通过开放网络平台征求社会公众意见、个人信息保护专门机构也可以建立网络平台， 为信息主体提供更为便捷的举报、投诉、申诉、监督方式，政府部门和信息业者也应当通过建立相应网络平台、市民热线等方式，听取公众意见并及时反馈，及时发现问题以实现更好的治理（张新宝，2015）。在民法典人格权编的审议过程中，也有法学教学研究机构和社会公众建议明确规定国家机关及其工作人员对履职过程中知悉的个人信息等的保密义务[9]。但本文认为，这些措施并不能真正为个人“赋能”。如多数措施不能由公民个人的启动，由公民个人启动的个人往往只有建议权，难以实现有效监督。而听证制度在我国的实行状况也有目共睹。尽管法律可以规定公权力如实披露所掌握的公民信息，也可以限制公权力任意从“私权力”处获取信息，但如同个人在司法诉讼中面临的困境一样，也会因个人没有监督能力而归于无效。张新宝教授提出，成立专门的信息保护机构，就我国目前的机构设置现状来看，可以考虑以现有的国家互联网信息办公室为平台，适当整合信息产业、工商管理等部门的部分职能，建构该专门管理机构，由其负责监督个人信息保护法的实施、展开个人信息保护执法调查、进行个人信息保护与利用研究等，并适时向立法机关提出立法意见和建议等（张新宝，2015）。权利对权力的制约最终会转化为权力对权力的制约，但在个人信息问题上，对这种制约的有效性，公民无法监督、控制。因此，传统的约束公权力的路径也已经不适应新的技术环境。在新的技术环境和条件下，必须探索为公民赋权、赋能的新路径。

最后，本文认为，不能因为个人无能力捍卫权利就不赋权，而应通过赋能使个人有能力捍卫权利。私权制度是为个人赋能的传统方式。实现个人信息权力平衡的出路在于探索为个人赋能的新路径。对个人的赋能方式需要革命性变革。技术发展带来的问题，还需要技术解决。立法不能仅要求公权力、私权力按传统的模式公开个人信息的利用情况，因为这样的公开已被证明是没有现实意义的，个人也难以监

督。私权力应当用技术反哺个人，使技术为个人赋能，使个人信息的收集、使用、转让情况以个人看得见、可监督的方式公开。进而解决公权力保护个人的动力不足的问题。而立法需要以给个人信息利用者设定义务的方式保障这种赋能的有效性。就目前来看，区块链技术的发展可能为给个人赋能提供技术条件。区块链技术的本质是去中心化的数据库，分布式记账具有可查证、难做伪的特性。如果对该技术的应用能使数据的收集、使用、流通可追踪，就能使个人信息以个人看得到的方式被收集、被处理，从而使个人能够像查阅自己的账户资金变动和明细一样查阅个人信息被收集、使用、流转的实时状态。而建立在掌握个人信息的真实状态、变动情况的基础上的动态监督，是促使各信息利用者保护个人信息的重要动力。一旦个人发现企业或政府部门违规或非法利用其个人信息，也可提出警告或拒绝其使用其个人信息。当然，这里还涉及个人对个人信息的使用状况的知情权与商业秘密和国家秘密的平衡问题。对于国家，除追究犯罪、反恐等少数涉及国家秘密的情况外，其使用个人信息的情况都不应该对信息主体保密，个人都应该是可查的。而对于企业，既然个人已经让渡了自己的个人信息，企业作为个人信息的利用者让渡一定的商业秘密，向用户呈现其个人信息是如何被利用的，也是其应该付出的代价。只有个人对其信息具有真实的、动态的知情权和控制力，才能有效监督公私权力的数据行为，才能实现权力结构的平衡。

五、结论与启示：探索为个人“赋能”新路径

信息的本质是对不确定性的消除。当技术越来越能预测和控制未来，没有什么力量能让人类停止追逐的脚步。大数据环境下，数据就是黄金，也是权力，企业和国家都兑变为“渴望数据的利维坦”（敬力嘉，2018）。以利用个人信息进行广告推送为例，随着营销从大众营销（mass marketing）发展到行为营销（behavioral marketing），对个人信息的收集、分析和利用已经使得对人的行为选择的操控变得更加容易。而这种对个人信息的利用还可能造成区别对待，例如有网络服务商通过识别用户手机品牌对相同产品进行差异化定价，更是形成了价格歧视，挑战了基本的平等原则。同时，这种利用个人信息对人的操控也会给个人的自由行为带来寒蝉效应。所有立法的最终目的都是服务于个人的安全、自由，但传统的私权制度和限制公权的机制都难以达成此目的。在个人信息问题上，不仅私权力有了双重角色，公权力也有了双重角色，都既是管理者又是利用者，这使得个人在三方权力结构中的地位风雨飘摇。公权在行动决策时会把公共利益放在首位，使个人利益难以保

障。个人信息的立法应当使新技术带来的社会权力关系的失衡状态重回平衡。在私权保护制度受到挑战、不足以保护个人的背景下，就需要立法以新的形式为个人赋能，使个人成为权力结构中有力的行动者，而不能仅靠寻求他人的保护。

（责任编辑：骆静雨）

注释 [Notes]

1. 截止2017年各国就个人信息/数据的立法参见Greenleaf–Global Tables of Data Privacy Laws and Bills (5th Ed, January 2017)。
2. 还有人认为，“个人信息/数据”从静态的“资产”变为动态的“生产资料”。
3. 持此观点的学者有高富平、王文祥等，他们认为本罪被置于《刑法》分则第4章“侵犯公民人身权利、民主权利罪”中，说明个人信息所保护的法益是公民人格尊严与个人自由。参见高富平，王文祥（2017）。
4. 持此类观点的还有皮勇、王肃之，参见皮勇，王肃之（2017）。
5. U. S. Department of Justice v. Reporters Committee for Freedom of the Press，489 U. S. 749 (1989).
6. 李论诉中国移动通信集团江苏有限公司仪征分公司、中国移动通信集团、江苏仪征农村商业银行股份有限公司、江苏省农村信用社联合社、中国电信股份有限公司仪征分公司、中国电信股份有限公司的相关负责人及其相关责任人员非法提供公民个人信息罪暨赔偿相关经济损失一案，参见江苏省扬州市中级人民法院刑事裁定书（2017）苏10刑终130号。
7. 参见北京市第一中级人民法院民事判决书（2017）京01民终509号。
8. 参见北京市海淀区人民法院民事判决书（2015）海民（知）初字第12602号，北京知识产权法院民事判决书（2016）京73民终588号。
9. http://www.npc.gov.cn/zgrdw/npc/cwhhy/13jcwh/2019-04/21/content_2085547.htm

参考文献 [References]

丁晓东（2018）。个人信息私法保护的困境与出路。《法学研究》，40（6），194-206。

丁晓东（2019）。论个人信息法律保护的思想渊源与基本原理——基于“公平信息实践”的分析。《现代法学》，41（3），96-110。

高富平，王文祥（2017）。出售或提供公民个人信息入罪的边界——以侵犯公民个人信息罪所保护的法益为视角。《政治与法律》，（2），46-55。

敬力嘉（2018）。大数据环境下侵犯公民个人信息罪法益的应然转向。《法学评论》，（2），116-127。

何渊（2018）。《信息性隐私权是如何在美国产生和发展的》。检索于https://mp.weixin.

qq.com/s/0GTsj4-022m_4Ur4hytATA

雷丽莉（2016）。网络安全发展中网络运营者的法律责任研究。《新闻记者》，（11），87-93。

雷丽莉，王丹（2018）。“私权力”崛起背景下的网络安全机制再思考——兼议建立网络安全机制要解决的三个主要矛盾。载《互联网与国家治理蓝皮书（2018）》（第48-60页）。北京：中国社科文献出版社。

刘艳红（2016）。《刑法学（下）》。北京：北京大学出版社。

龙卫球，刘保玉（2017）。《中华人民共和国民法总则释义与适用指导》。北京：中国法制出版社。

马改然（2015）。出售公民个人信息最相关问题研究。《刑法论丛》，（2），328-346。

皮勇，王肃之（2017）。大数据环境下侵犯个人信息犯罪的法益和危害行为问题。《海南大学学报人文社会科学版》，（5），114-124。

曲新久（2015）。论侵犯公民个人信息犯罪的超个人法益。《人民检查》，（11），5-9。

任龙龙（2016）。论同意不是个人信息处理的正当性基础。《政治与法律》，（1），126-134。

王利明（2013）。论个人信息的法律保护——以个人信息权与隐私权的界分为中心，《现代法学》，53（4），62-72。

王利明（2018）。人格权的属性：从消极防御到积极利用。《中外法学》，30（4），845-861

王利明（2019）。数据共享与个人信息保护。《现代法学》，41（1），45-57。

王肃之（2016）。试论信息法益的扩张与刑法回应。《华北电力大学学报（社会科学版）》，（12），33-37。

吴伟光（2016）。大数据技术下个人数据信息私权保护论批判。《政治与法律》，（7），116-132。

杨立新，扈艳（2016）。《中华人民共和国人格权法》建议稿及立法理由书。《财经法学》，（4），39-54。

杨立新（2018）。个人信息：法益抑或民事权利——对<民法总则>第111 条规定的“个人信息”之解读。《法学论坛》，（1），34-45。

喻国明，焦建，张鑫（2015）。“平台型媒体”的缘起、理论与操作关键。《中国人民大学学报》，2015（6），120-127。

于冲（2018）。侵犯公民个人信息罪中“公民个人信息”的法益属性与入罪边界。《政治与法律》，（4），15-25。

张民安（2014）。《信息性隐私权研究：信息性隐私权的产生、发展、适用范围和争议》。广州：中山大学出版社。

赵军（2011）。侵犯公民个人信息犯罪法益研究——兼析<刑法修正案（七）>的相关争议问题。《江西财经大学学报》，（2），108-113。

张明楷（2011a）。《刑法学》。北京：法律出版社。

张明楷（2011b）。《刑法分则解释原理》。北京：中国人民大学出版社。

张新宝（2015）。从隐私到个人信息：利益再衡量的理论与制度安排。《中国法学》，03（22），38-59。

张新宝（2018）。我国个人信息保护法立法主要矛盾研讨。《吉林大学社会科学学报》，58（5），45-56+204-205。

张新宝（2019）。《民法总则》个人信息保护条文研究。《中外法学》，31（1），54-75。

中国信息通信研究院（2018）。《电信和互联网用户个人信息保护白皮书》。7。

周辉（2017）。技术、平台与信息：网络空间私权力的崛起。《网络信息法学研究》，（2），68-99。

Don, T. (1994). *The Digital Economy: Promise and Peril in the Age of Networked Intelligence.* New York, NY: McGraw-Hill.

Martin, K., & Nissenbaum, H. (2016). Measuring Privacy: An Empirical Test Using Context to Expose Confounding Variables. *Columbia Science and Technology Law Review,* (18), 176-218.

Ohm, P. (2010). Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review,* (57), 1701-1777.

Schwartz, P. & Solove, D. (2011). The PII Problem: Privacy and a New Concept of personally Identifiable Information. *NYU Law Review,* (57), 1814-1894.