个人信息保护：从个人控制到社会控制

高富平*

内容提要：欧洲基于对人的尊严的保护，美国基于对个人自由的保护，形成了个人信息的个人控制论，以实现个人自治，保护人的基本权利。但个人信息保护权并不是一项全面的、绝对的支配权。个人信息不仅关涉个人利益，而且关涉他人和整个社会利益，个人信息具有公共性和社会性。传统的个人信息个人控制理论是建立在个人主义观念下，忽视了个人信息的社会性、公共性，不仅不能全面反映个人信息的法律属性，而且不能适应大数据时代个人信息利用的新环境和新方式。这预示着个人信息保护应从个人控制走向社会控制。我国应当从个人信息的法律属性出发，以社会控制论指导个人信息保护立法，建立平衡个人利益和社会整体利益的、适应大数据时代的个人信息保护制度。

关键词：个人信息　个人信息保护　隐私保护　个人信息社会控制

一、引　论

伴随信息技术的发展，人类进入到以数据化、网络化和智能化为特征的大数据时代。这个时代最主要的特征是数据化生存，科学研究、商业活动、社会治理等无不依赖数据，数据成为支撑这个时代发展的新资源。在数据资源中，能够识别个人的数据被称为个人数据（亦称个人信息，本文交叉使用）。[1] 个人信息是个人在社会中标识自己、建立联系的工具，也是社会了解和识别每一个体并开展活动的依据。但是，个人信息的不当使用可能侵害个人权益，危害人的尊严和自由，甚至带来人身和财产安全风险。于是，个人信息保护成为个人信息利用的前提，也成为大数据时代的重要法律问题。

2012 年 12 月 28 日，全国人大常委会通过的《关于加强网络信息保护的决定》宣布："国家保护能够识别公民个人身份和涉及公民个人隐私的电子信息"。由此开启了我国个人

* 华东政法大学教授、数据法律研究中心主任。

本文为国家社科基金重大项目"信息服务与信息交易法律制度研究"（项目批准号：13&ZD178）的阶段性成果。

〔1〕 欧盟立法文本通常采"个人数据"（personal data）的表述，而美国立法文本主要采"个人信息"（personally identifiable information），我国立法采个人信息之表述。因此，本文原则上采个人信息之表述，涉及欧盟法部分时，采个人数据之表述。

信息保护立法之路。之后，个人信息保护逐渐成为许多法律的必备条款，尤其成为消费者权益保护法（2013 年修订）、网络安全法（2016 年 11 月颁布，2017 年 6 月实施）的重要内容。个人信息保护是否要明确为一种具体人格权，也成为民法总则制定过程中的争议焦点。最终通过的民法总则仅宣布个人信息受法律保护，未采纳“个人信息权”的表述。[2] 这些法律初步建立起我国的个人信息保护利用规则。

根据我国现行法律，收集和使用个人信息须经被收集人（在国际社会称为“数据主体”或“信息主体”，本文称为“信息主体”）同意。[3] 这意味着，未经同意收集和使用个人信息即构成违法行为，应当承担相应的法律责任，其责任形态包括民事侵权责任、行政责任和刑事责任。目前，已经有一些涉及个人信息的工商行政处罚案例，以未经被收集人同意作为行政处罚的理由。[4] 根据《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》，“违反法律、行政法规、部门规章有关公民个人信息保护的规定的”即为“违反国家有关规定”；而根据目前的消费者权益保护法、网络安全法等之规定，同意是收集、提供个人信息的必要条件，进而是否获得同意成为判定是否构成侵犯公民个人信息犯罪的重要要素。但是，并没有太多的民事侵权案例支撑“未经同意收集和使用个人信息构成侵权”的判断。[5] 依据最高人民法院的解释，公开个人信息致人损害的才构成侵权，仅未经同意的使用尚不充分。[6] 由此出现了在是否构成侵权尚不确定或没有定论的前提下，行政和刑事责任先行的现象。

使用个人信息须经信息主体“同意”，暗含着法律认可个人信息由个人支配或控制，个人享有个人信息的使用决定权，包括是否允许他人使用、如何使用。这种个人信息使用的个人控制论源自域外个人数据保护或隐私保护的理论支撑。不过，我国是世界上唯一一个在立法上明示个人信息收集、使用一律须经信息主体的同意从而将同意一般化的国家，[7]

---

〔2〕 民法总则第 111 条规定：“自然人的个人信息受法律保护。任何组织和个人需要获取他人个人信息的，应当依法取得并确保信息安全，不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息。”

〔3〕 例如，消费者权益保护法第 29 条规定：“经营者收集、使用消费者个人信息，应当遵循合法、正当、必要的原则，明示收集、使用信息的目的、方式和范围，并经消费者同意。”网络安全法第 41 条规定：“网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。”

〔4〕 例如，2015 年 7 月，上海市工商局因炳恒金融信息服务有限公司非法收集、使用消费者个人信息，对其罚款 50 万元。2017 年 6 月，中国人民银行宁波市中心支行针对民生银行宁波分行未经同意查询个人信息的违法行为，对其罚款 53 万元。

〔5〕 目前涉个人信息的民事侵权典型案件有朱烨诉百度案，（2014）宁民终字第 5028 号；庞理鹏诉趣拿、东航案，（2015）海民初字第 10634 号等。以朱烨案为例，百度公司利用 cookies 收集朱烨的行为轨迹等上网记录，据此分析其行为偏好并向其浏览的网页上投放广告。案件的主要争议在于，百度公司是否构成侵犯隐私权。一审法院认为，未经朱烨明示同意收集个人信息，且在默示同意情况下未尽提醒义务，构成侵权；但二审法院认为，cookies 收集的信息不属于个人信息范畴，且默示同意具有合法性，不构成侵权。庞理鹏案中，原告能够证明确实是被告泄露了其个人信息，在收集、使用个人信息的合法性上未作讨论。

〔6〕《最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》（2014 年 6 月）第 12 条规定：“网络用户或者网络服务提供者利用网络公开自然人基因信息、病历资料、健康检查资料、犯罪记录、家庭住址、私人活动等个人隐私和其他个人信息，造成他人损害，被侵权人请求其承担侵权责任的，人民法院应予支持。”

〔7〕 美国法上目前并无明文规定收集个人数据必须经过数据主体同意，欧盟最新立法也只是将同意作为收集个人数据的合法性基础之一，并非必须事先征得数据主体的同意。欧洲国家受欧盟立法影响，也均未如此规定。目前只有我国立法如消费者权益保护法、网络安全法等明文要求收集个人信息必须事先获得信息主体的同意。

而个人控制在世界范围内并没有上升为法律上的权利。那么，个人信息是否应完全由个人控制，非经其同意不得使用？同意能否成为保护个人信息的手段？这是个人信息保护法律制度的核心问题。对此，已经有学者注意到我国一律采同意规则的弊端，建议采取或者依情况采取拒绝规则（又称“选退规则”）来缓和一律同意带来的弊害。[8] 这对完善同意规则无疑具有指导意义。本文则旨在从更为宏大的视角出发，重新审视个人信息的个人控制论的源流和内涵，寻找大数据时代个人信息保护的新的理论基础和法律实现方式。

“个人信息使用”是本文的核心术语，个人信息使用是否应当由个人控制是本文讨论的主题。若依据法律，信息主体对个人信息的使用享有同意、拒绝、删除等权利，就意味着信息主体可以控制个人信息的使用，个人信息的使用体现信息主体的意志力，具有赋权效果。为了避免权利性质的讨论（人格权、财产权或其他性质的权利），本文将之笼统地称为“个人信息控制权”。个人信息控制论诞生于互联网（更不用说物联网）还没有普遍应用的上世纪末。随着个人信息多样化、全系化采集、分析和应用的出现，非直接源自个人的信息收集和再利用成为个人信息使用的主流，建立在过去环境下的制度规则和理论需要反思和重构。

二、个人控制论的含义：基本权利视角下的个人信息保护

个人信息保护控制论有两个理论源头：一是欧洲基于人的尊严保护的个人数据保护理论，另一个是美国基于个人自由保护的隐私理论。尽管两个法域中个人信息保护的理论基础不同，但其结论是相同的，即个人应当有权控制其个人信息的使用，以实现对个人自治（独立人格和自由意志）等基本权利的保护。这两个理论相互配合，共同影响了国际社会上世纪 80 年代隐私保护规则的形成，[9] 成为当今世界主流的个人信息保护（隐私保护）的理论支撑。

（一）欧洲个人数据保护理论：基于人的尊严的个人自治

欧洲大陆将个人信息（一般称为个人数据）保护植根于基本权利或人权保护。他们认为，个人数据保护与人格保护有关，而这里的人格是指人的尊严。欧盟及其成员国的个人数据保护立法旨在落实欧洲委员会（Council of Europe）的《个人数据自动化处理中的个人保护公约》（下称《公约》）。[10]《公约》的理论和法律基础是《欧洲人权公约》[11] 中个人应当享有的 17 项基本权利和自由，尤其是其中的第 8 条（尊重私人和家庭生活的权利）。《欧洲人权公约》第 8 条来源于《世界人权宣言》第 12 条，[12] 但内容稍窄，且没有使用“隐私”，而直接用

〔8〕 参见任龙龙：《论同意不是个人信息处理的正当性基础》，《政治与法律》2016 年第 1 期，第 133 页。

〔9〕 上世纪 80 年代初，在国际社会有两部有影响的隐私保护国际文件先后发布，一个是经济合作与发展组织（OECD）于 1980 年发布的《隐私保护与个人数据跨境流通指南》；另一个是欧洲委员会于 1981 年发布的《个人数据自动化处理中的个人保护公约》。这两个国际文件几乎成为之后各国立法的重要参照文件。尤其是前者，虽然不具有国际法效力，但其确立的个人隐私保护八项原则成为各国个人数据保护法或隐私保护的基本原则。

〔10〕 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (CETS No. 108, Strasbourg, 28/01/1981). 2012 年 11 月，欧洲委员会第 29 届全会通过公约修正案，删除了“自动化”，改为《个人数据处理中的个人保护公约》(Convention for the Protection of Individuals with Regard to the Processing of Personal Data)。http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108，2015 年 12 月 10 日访问。

〔11〕 该公约由欧洲委员会于 1950 年起草，于 1953 年生效，并据此设立了欧洲人权法院。European Convention on Human Rights, http://www.echr.coe.int/Documents/Convention_ENG.pdf，2017 年 2 月 10 日访问。

〔12〕 The Universal Declaration of Human Rights, http://www.un.org/en/universal-declaration-human-rights/，2016 年 4 月 12 日访问。其第 12 条规定：“没有人应受到别人对他的隐私、家庭、住宅或通讯的任意干涉，他的荣誉和名誉也不受侵犯。每个人也有权利对这样的干涉和侵犯请求法律的保护。”

“尊重私人和家庭生活”。因此，尊重私人生活是个人数据保护的法律基础和目的。欧盟于1995年颁布的《欧盟议会与欧盟理事会关于涉及个人数据处理的个人保护以及此类数据自由流通的第95/46/EC号指令》（下称《指令》），[13] 对个人数据保护作了相对全面的规范。在这个基础上，2000年由欧盟主导的《欧盟基本人权宪章》[14] 明确将个人数据保护作为一项独立的基本权利加以规定。可以说，《公约》影响了整个欧盟的个人数据立法，而后欧盟关于个人数据保护的立法（无论在国家层面还是整个欧盟层面）又反过来影响了欧洲委员会的《公约》，尤其影响之后对《公约》的修订。正是这样的相互关系，我们可以肯定地说，整个欧洲是在公民基本权利层面定位个人数据保护的，将对个人数据的保护视为对基本人权的保护。

《公约》或欧盟层面对个人数据保护的定位也得到了欧洲国家的响应。早在1983年，德国法院就在一项开创性的判决中确认了个人信息自决权。[15] 一些成员国的宪法也明确将数据保护作为一项基本权利。[16] 现在，所有的欧盟成员国都有个人数据保护方面的法律。这在一定程度上是落实欧盟《指令》和各国宪法对个人数据的保护。

以上表明，欧盟是在基本权利（人权）意义上规范个人数据保护的；在国家层面，个人数据保护源自于宪法，落实于专门的数据保护立法。在欧洲，人的尊严被视为个人数据保护的根基。在《公约》起草者看来，个人数据保护涉及保障人的尊严问题，因为需要防止个人在个人数据处理中被仅仅视为客体对待。因此，对个人数据处理的决定不能仅仅基于系统自动运行而发生，而没有个人参与其中或考虑其意见。也就是说，数据处理不能忽视数据主体（data subject）[17] 的意志，否则就是对个人的不尊重。

正因此，在欧盟数据保护法中均有个人不受被动处理决定约束的条款。[18] 其核心意思是，除法定例外情形（包括数据主体的同意）外，数据主体有权不受仅基于自动化处理行为得出的决定的制约（意味着数据主体有拒绝自动分析的权利）。另外，1995年《指令》

---

〔13〕 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, in Official Journal L 281, 23/11/1995, pp. 0031 – 0050.

〔14〕 其第8条第1款规定：“每个人有权保护涉及他或她的个人数据。”（英文原文为：1. Everyone has the right to the protection of personal data concerning him or her.）《欧盟基本人权宪章》由欧盟主导起草并于2000年发布，该宪章吸收了许多宪法传统、国际人权公约文本（其中包括《欧洲人权公约》）中所规定的公民享有的政治、社会和经济权利，构成欧盟法律的基础。该宪章最初只是政治宣言，2004年被正式纳入《欧盟宪法条约》，实现了欧盟基本权利的宪法化。后来，《欧盟宪法条约》陷入僵局，宪章再次被并入2009年生效的《里斯本条约》（在原《欧盟宪法条约》基础上修改而成，被视为简版的《欧盟宪法条约》）。由此，《欧盟基本人权宪章》正式成为具有法律效力的文件。2000年文本参见 The Charter of Fundamental Rights of the European Union (2000/C 364/01), http://www.europarl.europa.eu/charter/pdf/text_en.pdf, 2017年2月10日访问。

〔15〕 参见德国联邦宪法法院1983年12月15日关于“人口普查案”的判决（Bundsverfassungsgerich. 65 BVerGE1）。1982年德国联邦政府颁布《人口普查法》，该法计划在全国范围内对公民进行全面的个人信息收集，包括人口、职业和住所等几乎全部个人数据。有人就此提起宪法诉讼，要求宣告《人口普查法》违宪。在该案判决中，德国联邦宪法法院认定该法有违宪情况，以判例形式确立了“信息自决权”（Recht auf informationelle Selbstbestimmung）作为宪法上的公民权利。

〔16〕 如比利时宪法、塞浦路斯宪法、法国宪法、葡萄牙宪法、西班牙宪法、瑞典宪法等。转引自［德］Christopher Kuner：《欧洲数据保护法：公司遵守与管制》，旷野等译，法律出版社2008年版，第20页，注释4。

〔17〕 英文“subject”是哲学意义上的主体（有意识的人），但 data subject 强调“数据”与个人相关，是“数据的主体”，而非“属于个人的数据”。因此，不能将该词混同于 data owner（数据所有者），否则将导致个人数据的客体化（成为个人支配的对象）。

〔18〕 分别参见《指令》第15条“不受自动处理结果约束的权利”和2016年《统一数据保护条例》第22条“自动的个人决定，包括画像”。

和 2016 年《统一数据保护条例》[19]（以下简称《条例》）均赋予个人数据主体很多权利，以保障数据主体了解有关他的什么数据被谁用于何用途，并及时更正错误、删除或拒绝处理，体现对个人的尊重。

在笔者看来，欧洲个人数据保护的逻辑是：个人数据是人的延伸，而人应当独立自主（自治），因而个人数据亦应当由数据主体掌控，体现个人的意志。建立在人的尊严基础上的个人数据保护理论，内涵着个人数据由个人自主控制的基本论调，而个人数据控制论本源于个人独立和个人自治。这也是康德的“以人作为目的”的观念体现。保障数据主体对个人数据的处理事务的自主、自治、自决，应是个人数据保护的应有之义。

但是，在基本权利或宪法权利层面个人对个人数据的自决权或控制权，不能理解为个人对个人数据的全面的、绝对的支配权。从《公约》层面讲，《公约》将个人数据受保护的权利表述为个人数据保护权（the right to protection of personal data）而不是个人数据权，该权利的核心内容是“控制某人的个人数据和该数据的处理的权利”（the right to control one's personal data and the processing of such data）。《公约》的宗旨是保护个人尊严和基本人权和基本自由，个人数据保护权只是其中一项权利。对《公约》的“个人保护”的立意必须作全面的理解，必须在保护个人基本权利和自由的意义上理解其目的。不能将《公约》的目的仅仅理解为保护个人数据，而应理解为保护个人所应当享有的所有基本权利和自由。个人数据保护权是保护人的尊严派生出的个人自治（自由）、身份利益（正确识别）、不歧视（平等）利益。个人数据保护权只是对个人基本权利保护的法律表述。

《公约》起草者注意到，个人数据保护“必须就其在社会中的作用来加以考虑，必须与其他人权和基本自由（包括表达自由）相协调”，“考虑公众获取官方文件权”，“有利于信息的自由流通”。[20] 这是因为，保护个人对个人数据的控制权在某种程度上与信息的自由获取和传播（表达自由）存在冲突。《欧洲人权公约》第 10 条规定了“表达自由”，包括持有观念、接受和传播观点的自由。[21] 表达自由依赖信息自由，即人们可以自由地获取信息和传播信息（信息流动）。如果信息获取受到限制，人们就无从自由地作出判断，形成和表达观点。不仅思想表达，其他的权利和自由也依赖于信息自由，保护信息自由本身成为保护个人基本权利和基本自由的重要内容。这决定了个人数据保护权不能妨碍信息自由、公众知情权等基本权利，欧盟《条例》也正是遵循了这样的立法逻辑，[22] 充分印证了个人

〔19〕 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation).

〔20〕 参见《个人数据处理中的个人保护公约》（2012 年 11 月欧洲委员会第 29 届全会通过修正）序言。

〔21〕《欧洲人权公约》第 10 条：1. 人人享有表达自由的权利。此项权利应当包括持有主张的自由，以及在不受公共机构干预和不分国界的情况下，接受和传播信息和思想的自由。本条不得阻止各国对广播、电视、电影等企业规定许可证制度。2. 行使上述各项自由，因为负有义务和责任，必须接受法律所规定的和民主社会所必需的程式、条件、限制或者是惩罚的约束。这些约束是基于对国家安全、领土完整或者公共安全的利益，为了防止混乱或者犯罪，保护健康或者道德，为了保护他人的名誉或者权利，为了防止秘密收到的情报的泄漏，或者为了维护司法官员的权威与公正的因素的考虑。

〔22〕《条例》鉴于条款第 4 条：“个人数据的处理应当为人类服务。保护个人数据的权利不是绝对权，必须根据比例原则，考虑其在社会中的作用，并与其他的基本权利相较权衡。本条例尊重所有基本权利，并且遵守《宪章》所承认的载于《条约》中的自由和原则，特别是尊重私人和家庭生活、家庭和通讯、个人数据的保护、思想自由、道德和宗教自由、表达和信息自由、开展生意的自由、有效救济和公平审判的权利，以及文化、宗教和语言的多样性。”该鉴于条款明确指出保护个人数据的权利不是绝对的，应与其他权利进行权衡。

数据保护不是一项绝对的权利。

同样，在国家法层面，个人数据保护权作为公民一项宪法上的基本权利，也存在与其他基本权利的平衡协调问题。德国司法实践最先确定的“信息自决权”并没有被德国成文法承认为一项独立的权利，它反映的内容正是德国基本法第 1 条第 1 项规定的一般人格权，即“人之尊严不可侵犯”。[23] 德国联邦宪法法院在“人口普查案”中也明确表示没有绝对不得限制的个人信息自决权。亦即，个人对其个人信息并没有绝对的支配权，因为，个人是社会团体中的一员，个人人格的自由发展正是仰赖于社会交往，即使是那些与个人事务密切相关的个人信息，实际上也是社会生活的写照，不能排他地属于当事人所有。[24] 对此作出专门研究的杨芳得出结论，认为“信息自决权至多只是学说上关于个人信息支配的误导性理论表述，而不是私权体系中的具体权利类型，更不是受侵权行为法保护的民事权利”。[25] 王泽鉴指出，在“人口普查案”的判决中，德国宪法法院尽管提出了“信息自决权”的概念，承认个人在其个人数据上享有个人自治和自决的法益，但并不认可个人对其个人数据享有绝对的排他支配权，个人数据保护仍然要受比例原则等的限制。[26]

因此，在研究和借鉴欧洲个人数据保护制度时，我们必须尊重一个基本事实，即欧洲是在基本权利或宪法权利上规范个人数据保护权的，通过宪法法院、欧洲人权法院来提供保护和救济。虽然该权利内包含了个人对个人数据及其处理的控制权，但是，这种控制权必须受到其他基本权利的限制，必须在其他基本权利获得充分保障的框架中才能得以行使。正因如此，欧盟的数据保护法始终坚持将合法性作为个人数据处理的基础，数据主体的同意只是合法性基础之一。根本上，欧盟没有将“同意”上升为一种权利，而是附之以例外或权利限制作为个人数据保护的基本模式。[27] 这样做的根本目的是给法院在提供救济时保留充分的自由裁量空间，从而平衡个人数据保护与其他基本权利保护。也就是说，个人数据保护权本质上体现为一组宽泛的原则和详细的行为规范。[28]

---

〔23〕 完整的条文为：“人的尊严不可侵犯。尊重和保护人的尊严是国家所有机构的义务。” See Basic Law, https://www.bundesregierung.de/Content/EN/StatischeSeiten/breg/basic-law-content-list.html，访问日期：2018 年 5 月 6 日。

〔24〕 BVerfG 65, 1, 43. 转引自杨芳：《个人信息自决权理论及其检讨——兼论个人信息保护法之保护客体》，《比较法研究》2015 年第 6 期，第 29 页。

〔25〕 同上文，第 33 页。

〔26〕 参见王泽鉴：《人格权法》，北京大学出版社 2013 年版，第 200 页。

〔27〕《条例》将数据主体的“同意”作为合法性的六种基础之一（第 6 条），而不是作为一种权利出现在第三章“数据主体权利”中。《条例》一方面赋予数据主体维护其权利不受侵害的权利，如知情权、访问权、拒绝权、删除权（被遗忘权）、限制处理权、数据移转权（the right to data portability，又称“数据便携权”）等；另一方面，对数据控制人（使用人）施加相应的义务，以实现这些权利。《条例》未赋予数据主体对个人数据单一的控制权，然后再限制权利行使，而是直接赋予数据主体一组具体的权利，并给予其司法救济权利，以实现对个人权益的保护。

〔28〕《公约》修订之际，修订专家委员会曾向公众发布有关《公约》的公开征询函，《计算机法与安全评论》期刊联合国际 IT 律师协会等机构，组织了几位有影响力的专家，代表学术界对《公约》修订提出基本看法。针对《公约》是否应当对数据保护和隐私权（the right to data protection and privacy）有一个定义的问题，专家们认为在数据保护公约中试图界定隐私权是没有用的。因为隐私权本身是在不同的场景有不同表现方式的一组权益（a set of interests），有时需要与其他权益进行平衡。将其表达为一组宽泛的原则更适当。存在其他公约（如《欧洲人权公约》等）和判例来解释它，采用宽泛的隐私保护表述是适当的，这样可以运用不同机制来实现保护。See Sylvia Kierkegaarda, Nigel Watersb, Graham Greenleafc, Lee A. Bygraved, Ian Lloyde and Steve Saxbyf, *30 Years on-The Review of the Council of Europe Data Protection Convention 108*, 27 (3) Computer Law & Security Review 223-231 (2011).

（二）美国的信息隐私理论：基于自由的个人自治

在美国，并没有与大陆法相对应的人格权理论和制度，而是发展出了发达的隐私权（right to privacy）保护体系。1890 年，沃伦与布兰德斯在《哈佛法学评论》发表了一篇名为《论隐私权》的文章，首次提出了“隐私权”的概念，并将其定义为“个人独处的权利”。[29] 显然，支撑独处或避免干扰的理念是“个人自由”，隐私权实质上是政治或宪制意义上个人自由在法律上的表述。可以说，美国法中的隐私权产生于公民基本权利，在纳入司法救济体系保护后形成普通法意义上的隐私权。[30] 因此，美国的隐私救济既可以保护宪法上的公民基本权利，也可以用来保护民事权利。1965 年，美国联邦最高法院在 Griswold v. Connecticut 一案的判决中明确宣布，个人享有宪法性的隐私权，处于对《权利法案》进行扩大解释后创设出的自由领域或边缘地带。[31] 其后，美国联邦最高法院又在 Roe v. Wade 一案的判决中宣布隐私权“包含一个女人对是否终止其妊娠的决定权”。[32] 从这个角度考虑，隐私权是指一种免受政府干涉的权利。[33] 这种隐私权既包含了消极的或防护性的保护，也包含了自治权与自决权（例如决定堕胎的权利）。

20 世纪 60 年代，计算机逐渐开始应用，在给人们带来便捷的同时，也使个人逐渐丧失对个人信息的控制，隐私权逐渐被理解为是一种维持对个人信息的内在领域和对某人身体和能力的一定程度的控制的权利。“控制权”理论的发展，催生了“信息隐私权”的出现。对此作出完整论述的是艾伦·F. 威斯汀。他于 1967 年出版了《隐私与自由》一书，面对计算机带来的严重的隐私问题，提出了“隐私权”的新定义，认为隐私是“个人、群体或机构自主决定在何时以何种方式在多大程度上将有关自身的信息披露给他人的权利（claim of individual）”，[34] 由此形成个人信息控制论的源头。[35] 后人将威斯汀的贡献评价为从信息控制视角审视隐私的先驱，提出了一种新型隐私权——“信息隐私权”。[36] 由此，隐私权

〔29〕 S. Warren and L. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 – 220 (1890).

〔30〕 主要包括禁止对个人私人事务的侵入、对私事的披露以及对个人形象的使用等。1960 年，普罗塞（William Prosser）通过整理美国各州 300 多个关于隐私权的判决，将隐私侵权行为具体划分为四种类型：（1）侵入独处状况（intrusion upon seclusion）；（2）公开私人事务（public disclosure of private facts）；（3）扭曲他人形象或公开（false light or “publicity”）；（4）为谋利使用他人姓名肖像（appropriation）。该观点被美国《第二次侵权法重述》吸收，侵害隐私被归纳为：侵入私人空间、利用他人形象、公开他人私生活和使某人被公众误解的公开行为。

〔31〕 Griswold v. Connecticut, 381 U. S. 479 (1965). 具体案情为：原告康涅狄格州计划生育联盟执行董事和医疗董事（持照医师）被起诉向已婚人士提供关于如何避孕的信息和医疗咨询，并在检查之后，开具避孕工具或药物供妻子使用。上诉法院和州最高法院均判决原告有罪。康涅狄格州的一部法律禁止使用任何药物、医疗器械阻止怀孕，否则构成犯罪。原告认为该法律违反了宪法第四修正案。原告上诉至联邦最高法院。联邦最高法院判决：原告有权为已婚人士主张宪法上的权利；康涅狄格州禁止使用避孕药物的法律侵犯了夫妻隐私权（the right of marital privacy，显然这里的隐私权就是自由），而夫妻隐私权在《权利法案》特别赋权的范畴之内。该案判决具有标志性意义。

〔32〕 Roe v. Wade, 410 U. S. 113, 153 (1973).

〔33〕 Darien A. McWhirter and Jon D. Bible, *Privacy as a Constitutional Right: Sex, Drugs and the Right to Life*, New York: Quorum Books, 1992, p. 33.

〔34〕 Alan F. Westin, *Privacy and Freedom*, New York: Atheneum, 1967, p. 7.

〔35〕 威斯汀认为隐私权能够实现以下四种功能：（1）实现个人自治，控制自己何时公开个人信息；（2）实现情感释放，保持自己的个性，保有社会或制度规范所允许的个体差异；（3）实现自我评价，自我反省，树立正确的自我认知；（4）实现有限且受保护的通讯，不受到外界监听或拦截。

〔36〕 从该书的表述来看，威斯汀并未用“information privacy”等词汇来表述他的隐私权概念，他始终坚持用“privacy”一词来涵盖新的隐私权内容。

被认为是对个人追求自由的法律保障，个人自由的保护被视为美国隐私权的理论基础。

1977 年，美国联邦最高法院在 Whalen v. Roe 一案的判决中主张受宪法保护的“隐私领域”包括了两类不同的利益：一是“作出某些重要决定的独立性”；二是“防止披露个人事务中所体现出的个人利益”。[37] 前者在 Griswold 和 Roe 两个案件中已经被正式确立下来，即决定隐私权（decision privacy）；而后者所保护的利益被称为“信息隐私的宪法权利”，即所谓的信息隐私权。自此，信息隐私权从理论层面落实到司法实践，作为具有法律效力的私人权利，被正式纳入到了广义隐私权的框架之中。信息隐私权用来保护个人信息处理与流通领域中的个人隐私，是当事人个人信息上相关权利被侵犯时起诉侵权主体的一项合法依据。正因此，在许多场合下，隐私保护与个人信息保护具有相同的含义。

在美国，信息隐私的主导范式是隐私控制论（Privacy-control），即对个人数据使用的控制权。对此，美国联邦最高法院也有明确的阐述：“普通法和隐私的字面含义均内含个人对有关她或他的信息的控制。”[38] 隐私控制是自由自治原则的产物，该原则置个人于个人信息使用的核心位置，通过个人管理个人数据和个人决定数据使用来实现信息自治（informational autonomy）。[39] 这里的自治有两层含义。其一，个人有能力创设自己的身份（identity）并借此定义自己。[40] 允许个人看管个人信息，人们就可以控制他们的身份。尤其是，可以限定和圈定其他人享有的关于自己的个人信息，借此可以影响他人对自己的看法。其二，自治也意味着对自己的事务作出决定，尤其是重要的事务，比如对自己诊疗方案的同意。隐私控制理论支持个人对个人数据使用的选择及其数据使用谈判，以促进个人自治。隐私控制论还有利于鼓励个人信息的商品化（财产化和合同化），将个人信息转化为财产并允许人们交易它，签署有约束力的转让合同。在这个意义上，隐私控制范式不仅与自治相联系，而且也与财产和合同联系在一起。

个人信息控制理论肇始于美国，成为美国个人信息保护的理论基础。不过，在美国，个人对个人信息的控制也不是一项绝对权，对于美国个人信息的自由流动也未造成实质上的影响。美国仍然是世界上个人信息保护相对宽松的国家。这主要是因为，美国的隐私保护根基于宪法上自由，由此延伸到个人对个人信息的自主控制，而美国又是一个崇尚和坚守信息自由（或言论自由）的国家，个人对信息的控制要受到宪法第一修正案的制约。赋予个人对信息的绝对控制会妨碍信息自由，因而宪法层面的个人信息控制需要与信息自由相平衡。显然不可能基于个人自由而赋予个人对个人信息的绝对意义上的控制权（这很容易被信息自由所对抗）。但是，法学家一直在此之外寻求赋予个人信息控制权的正当性，而隐私的财产（经济）价值为个人信息控制理论提供了论证基础。于是，基于个人自由的隐私控制论被学者（尤其法经济学者）演绎成为一个宽泛的财产权，并被置于个人自治的大“帽子”中。但是，这种理论并没有成为现实。这可以从两个方面加以说明。其一，美国的隐私保护依赖普通法救济，这种救济本质上是以个人利益（包括自由）受到侵害为前提。

---

〔37〕 Whalen v. Roe, 433 U. S. 425, 599 – 600 (1977).

〔38〕 United States Dep't of Justice v. Reporter's Comm., 489 U. S. 749, 763 (1988).

〔39〕 See Edward J. Janger & Paul M. Schwartz, *The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 Minn. L. Rev. 1219, 1247 (2002).

〔40〕 Robert C. Post, *Three Concepts of Privacy*, 89 Geo. L. J. 2087, 2092 (2001).

而当事人要证明他人未经其同意利用其信息给个人造成的损害是相当困难的事情，[41] 而且法院在裁决是否侵犯隐私时需要依据法律（包括制定法和判例）和常识（common sense）在具体情形中作出具体判断，其中隐私权保护仍然受到信息自由等宪法原则制约。其二，美国联邦层面制定的有关个人信息保护的特别立法不仅没有将个人控制一般化，而且严格限制个人同意（尤其是收集使用前同意）的范围。[42] 同样，也由于对个人信息法律属性和个人控制程度的意见分歧，致使美国联邦有关个人信息的立法提案一再受阻。[43]

综上，欧美对于个人数据（隐私）保护的出发点不同，但是目标和结论都是人的独立自主或自治，因而均将个人信息归由个人控制，法律保护这种控制即是保护个人自治。虽然个人信息控制论是国际社会个人信息保护的理论基础，但并没有建立起非经同意不得使用个人信息的规则，也没有将个人信息客体化为个人绝对支配的对象。这是因为，个人信息保护的基本目的是保护个人的基本权利不因个人信息的使用而受侵犯，而不是让个人控制其个人信息。国际社会以合法性为基础，建构个人信息使用规则对使用人施加法定义务，维护个人权利不受侵害。根本上，个人信息保护是对人的保护，旨在防止对与个人有联系的信息的滥用而导致对人的尊严、自由、独立、平等带来消极影响或损害。准确地讲，个人对个人信息的控制只是实现保护的手段，根本没有上升为一种排他性的个人权利。不能将在基本权利或宪法意义上使用的个人信息控制权或个人信息保护权直接转化为个人对个人信息的排他、积极的支配权。这不仅是因为基本权利保护具有原则性、抽象性，还因为个人信息也具有公共性，不能为个人所排他控制。

三、个人信息的非个人控制性：个人信息的公共属性

个人信息保护法律规则的形成和实施过程中，一直充斥着信息主体对个人信息收集、使用的控制与数据控制人（即数据使用人）意图最大可能地自由使用个人信息的冲突。国

〔41〕 许多个人数据泄露案件基于原告没有充分证据证明他们因数据曾经被不正当地使用而遭受损害而被法院驳回。例如，在 Hammond v. The Bank of N. Y. Mellon Corp. 一案中，消费者认为银行在磁带中存储了他的个人信息，而磁带在运输中丢失，因而向法院提起集体起诉，要求损害赔偿。法院认为："原告诉讼无理，因为其诉讼请求面向未来的、假设且是概念性的，因而不予支持或无可争辩。"［No. 08 Civ. 6060（RMB）（RLE），2010 WL 2643307，at * 7］（S. D. N. Y. June 25，2010）］。另外，在 Reilly v. Ceridian Corp.（664 F. 3d 38，40（3d Cir. 2011））一案中，法院认为，仅因为被告公司遭受安全事故导致泄露原告信息而起诉被告，理由不充分。在 Lambert v. Hartman（517 F. 3d 433，437（6th Cir. 2008））案中，法院认定被告在其网站中公布援引交通罚单个人识别信息并不足以构成起诉被告的理由。

〔42〕 美国联邦在通信、金融、健康、信用等领域颁布有个人信息保护法律，这些法律并没有将个人控制（同意决定）一般化。例如，《格雷姆-里奇-比利雷法》（1999 年，又称《金融服务现代化法》），其调整对象是个人提供给金融机构的或者其保有的非公开个人信息，该法的核心内容是确立金融机构向非关联第三方披露个人信息的条件，其中一个重要条件是事先通知并有机会选择退出。再如，《健康保险移转与责任法》（1996 年），主要规范以商业利用为目的的个人健康信息使用和披露行为。该法只是要求健康医疗提供者在将健康信息以电子方式转移给可能市场化利用该信息的卫生保健清算所或健康计划等主体前，须得到个人同意。

〔43〕 在一般的商业领域，在美国联邦层面不存在制定法，各企业根据公正信息准则实行自律。为了确保消费者对敏感个人信息的一定程度的控制，确保公司对个人数据承担清晰的管护责任，白宫于 2011 年和 2015 先后两次向议会提交消费者隐私保护法案：H. R. 1528 - Consumer Privacy Protection Act of 2011［112th Congress（2011 - 2012）］；S. 1158 - Consumer Privacy Protection Act of 2015［114th Congress（2015 - 2016）］，均未获通过。2017 年，Patrick Leahy 等六位参议院又向国会提交了 2017 年消费者隐私保护法［Consumer Privacy Protection Act of 2017 H. R. 4081 - 115th Congress（2017 - 2018）］，同样未有任何结果。

际社会及主要国家在个人信息保护立法时虽然强调个人信息的流通利用目的，但是因为传统个人信息保护或隐私保护理论过分强调个人信息的私人属性并将基本权利上的自治延伸至个人信息，导致个人信息由个人控制成为普遍接受的观念。事实上，个人信息具有公共属性，关涉他人和社会利益，个人信息的使用不应当由个人决定。

（一）个人信息的识别功能

个人信息是指可识别具体个人（仅指自然人）的信息。凡是能够识别特定个人的信息，无论是直接识别到还是间接识别到特定个人的信息，均为个人信息。识别指的是根据与特定人有关的外部信息来认识、辨识或指认该特定个人，所依赖的信息通常是个人特有的或描述个人属性、特征的信息。识别的结果就是认出特定个体，使某个人与其他人区分开来。作为识别的手段，个人信息是个人标识自己的工具，也是他人识别特定个人的工具。

标识自己和识别个人是社会的必然现象。前者是个人（数据主体）主动利用个人信息的过程，也是向社会提供个人信息的过程；后者则是由社会主体（收集和使用个人数据的主体，称为数据控制人或数据使用人）对来源于个人（主动提供或散落于社会中的）的数据的使用过程。个人需要利用可以识别自己的符号，向社会推介、展示自己，需要利用它开展各种活动，将活动结果归属于其本人。在这一过程中，个人信息必然要向外提供，为其他主体所掌握。一个人要进入社会或参加社会活动，就需要向他人披露、公开身份。封闭个人信息就意味着与世隔绝。从社会的角度出发，社会也需要利用个人提供的个人信息和散落于各处的、可被搜集掌握到的相关个人信息来了解、判断某个人。这两个方面构成个人信息应用的基本场景。工具性质决定了个人信息的社会性、公共性。

社会中存在两类识别。一是识别个体的身份，用来表示你是谁，最直接表示一个人身份的就是姓名及与姓名直接对应的身份标识（如身份证号、指纹等）。[44] 实际上，由于姓名没有唯一性，在同一个单位都需要补充额外信息（部门、年龄大小等）进行辨识。我们也可以借助工作单位、职称或职务、性别、年龄等个人属性信息间接识别出一个人的身份（谁）。也就是说，识别一个人的身份既可以是通过姓名和身份证等唯一标识符，也可以借助一些个人属性信息识别到具体个人。二是识别个体的个性特征。在社会交往中除了需要知道是谁外，还需要知道他是什么样的人，而且根据不同的目的，需要了解的个人的个性特征也不完全一样。如果是借贷，那么需要了解他有没有偿还能力；如果是招聘，就需要了解他是否适格、诚实、合作等。这些识别需要借助某个人的行为记录、过往经历、行为偏好等信息进行分析。基于网络用户的行为记录形成的用户画像（profiling，又译“个性档案”），即属于个性特征识别，它通过搜集用户的各种信息（社会属性、生活习惯和消费行为等）给用户抽象出一个个特征标识，判断某个用户是一个什么样的人。

在过去，我们往往先识别个体身份，然后再识别他有什么特征。现在，我们借助个体特征信息，也能够识别出特定的个人。在大数据环境下，我们可以通过了解一个人的个人属性（如职业、经历等）、网络浏览记录等数据来认识某个人的个性特征，然后将个性特征联系到某个具体个人。个人提供给社会的信息丰富了，不仅能够精确地识别一个人的特征，

〔44〕 在笔者看来，一个人借助姓名标识其社会身份，使其由一个纯自然人转化为社会可认知的个体。姓名之外的所有个人信息，并不具有这样的直接标识功能，这些个人信息只具有联系功能（与特定人联系起来以描述一个人）和增加可识别度的功能。因此，个人经历、背景、行为信息、心理、生理、习惯等个人信息可以描述一个个体，但是如果没有姓名，仍然无法识别到一个具体的人，除非在一个已经特定化的语境中。

而且很容易识别一个人的身份。基于此，现在识别个体，甚至不需要识别个体身份（知道你是谁），而仅仅识别特定的抽象的个体。我们在网络环境中有许多身份标识符，典型的如用户名甚至 IP 地址、硬件识别号（如手机 IMEI 号），均可以视为一个个体。这样的个体实际上是“人格面具”（persona）。至于这个个体是谁，对应到现实中哪个具体的个人，则需要进行身份识别，即将具有某些特征的个体与具体的个人联系起来。识别并不必然要识别身份，更不必然跟一个人通信或联系。[45] 在一些商业应用中，即使不知道用户的姓名，也可以达到认识该用户甚至与他（她）联系的目的。因此，在网络社会中，识别的基本含义就是通过分析关联数据以识别某个用户的个性特征。至于能否识别用户的身份，则取决于所掌握的数据是否匹配到某个人。

大数据给人们提供的巨大便利就是识别个体的便利性、精准性、全面性和及时性。大数据技术背景下，一切能够关联到某个人的或了解某个人个性特征的数据都可以归入个人信息的范畴，因为各种信息可以通过关联、联系、结合识别出具体的个人（此即所谓的间接识别），并且结合的信息越多，识别的结果就越准确和全面。所谓发挥大数据的红利，就是鼓励利用尽可能多的信息进行分析识别，然后用于实现各种社会发展目的。

（二）个人信息的公共性

个人信息保护所面临的核心问题是：这些可识别个人的数据是否归属于个人或者由个人控制，社会主体是否必须经过个人的同意才能对其进行识别？笔者认为，个人信息本身只是一种可以识别某个人的事实或记录，并不当然地应该由个人拥有或控制。个人信息与个人的联结点是：这些信息指向或描述某个人，可以将之概括为该信息与某个人有联系、有关联。但是，纯粹与特定个人有联系不足以使个人对该数据具有支配利益。因为这种关联只在于信息所表达的意义、内涵，而不在于数据本身。

自古以来，信息一直是处于公共领域的公共素材或材料，是任何人均可以使用的资源。[46] 在知识产权体系中，著作权、专利权和商标权均没有赋予对信息的支配权，信息并非专有权的对象。例如，专利权是专利权人公开专利信息换取对技术方法的商业上实施的垄断权；著作权法保护的是思想的表达，而非思想本身，公众对于一切公开的作品均可以接触、学习并合理利用；商标专用权只是在特定类别的商品或服务上使用注册标识的权利，本质上是对因使用而建立的商誉的保护，而不是保护权利人对标识本身的垄断。而之后进入知识产权体系的商业秘密也并不是对秘密商业信息的支配权，而是以事实控制力（保密措施）为基础的财产权（丧失保密控制即丧失权利），本质上是对抗他人以不正当手段获取、使用和披露商业秘密的权利，而非对特定商业秘密的排他支配权。因此，知识产权制度通过一些精妙的制度安排，在赋予权利主体某种专有权的同时，刻意地将创新成果的内容或信息置于公众可接触的公共领域，由此通过信息的公开、思想成果的自由使用（限于学习研究和继续创作或创新），推动科学艺术文化的不断进步。那么，个人信息是否应当存在例外，

〔45〕“识别”与“通信”或“联络”无关。住址、电话、电子邮件、微信账号等在识别中所担任的角色，仍然是识别该用户是谁，识别本身并不导致与该用户通信、联络或对其进行推销甚至实施诈骗。联系被识别的人，不属于识别行为，也不是可识别个人身份的个人信息所导致的必然结果。

〔46〕信息的产生和再生的成本很低，信息本质上不具有排他性，再加上排除他人使用信息的成本过高，因此，应将信息视为公共资源。See J. E. Stiglitz, *The Contributions of the Economics of Information to Twentieth Century Economics*, 115 (4) Q. J. Econ. 1441 – 1478 (2000).

需要将个人信息置于个人的排他控制之下？

就个人信息而言，当信息用来标识、记录、描述某个人时，并不因此而使该信息（数据）归属于该人，这些信息（数据）仍然可以用来标识、记录、描述其他人。数据或信息的公共性、可共享性，决定了个人数据本身的公共性。个人最多可以控制不联系或如何联系，但不能控制信息本身。比如，购买减肥霜的消费记录虽然与个人有关，却并不一定导致该人对该记录享有支配、控制的权利。因此，网络、传感器等记录的与个人有关的活动、浏览记录，只是与特定个人产生了联系从而赋予该信息某种含义，而不足以使该个人对该记录信息拥有排他支配权。

即使可以直接标识个人身份的信息，个人也不享有支配权。以姓名为例，姓名是最直接标识自然人的标识符（文字），它具有等同于本人或代表本人的功能。虽然法律赋予个人以姓名权，〔47〕但并不包括对姓名信息（符号）的支配权。姓名权主要保护个人的两种利益：其一，个人有独立命名的自由，不受任何人干涉。它所保护的法益是人格独立和自由，而不是个人对自己姓名的垄断，个人不能阻止别人使用相同的姓名（文字）。〔48〕其二，个人有使用自己姓名的权利。〔49〕姓名的功能在于让一个人在社会活动中标识自己，将社会活动的结果归属于其本人，如在作品上署名、取得各种荣誉等。法律保护每个人正当使用自己姓名的人格利益。因此，姓名权本身并不是对特定文字符号的支配权，法律只是保护个人排除他人干涉、冒用、盗用姓名，但不能排除他人使用相同的姓名。简言之，姓名权本质上是对人格利益的保护，而不是对姓名本身的支配权。

在网络化、数据化、智能化的时代，全息化、多样化的大规模个人数据，不仅成为社会治理、企业管理创新和改善的资源，也成为科学文化艺术创新进步的资源池。处于公共领域的信息或数据仅因为与个人存在联系或具有识别性，即赋予个人对个人数据的排他控制权，使个人信息“私有化”，有失法律正当性，甚至与人类社会进步发展的制度基础相悖。这也是各个国家将数据开放和流通作为推动大数据产业发展、促进经济转型的重要措施的原因。没有丰富的、处于公共领域的“原材料”，是不可能有创作和创新成果的。法律之所以不能赋予某个主体对信息的专有权，是因为信息（数据）承载着人类文化传承和社会运行发展的公共元素。正如荷兰蒂尔堡大学的普林斯教授所说，“目前个人数据在定义上几乎被视为公共领域的组成部分，是可以广泛获得和使用的。无论从实践还是从法律目的上，个人数据均处于公共领域。”〔50〕美国的扬格和施瓦兹撰文认为：“信息隐私作为一种公共物品，像干净空气或者国防一样发挥着作用，从宪法的角度看，隐私也是一种公共物品。”〔51〕还有学者把隐私看作是经济学的公共物品，由此认为“确切的隐私单元是群体而非个人”，隐私保护需要群体协调（group coordination），而个人主义的隐私保护的结果是无隐私。〔52〕

---

〔47〕 民法通则第99条规定：“公民享有姓名权，有权决定、使用和依照规定改变自己的姓名，禁止他人干涉、盗用、假冒。”

〔48〕 参见刘文杰：《民法上的姓名权》，《法学研究》2010年第6期，第69页。

〔49〕 参见程啸：《侵权责任法》，法律出版社2015年版，第138页。

〔50〕 Corien Prins, *Property and Privacy: European Perspectives and the Commodification of Our Identity*, 16 Information Law Series 223 – 257 (2006).

〔51〕 前引〔39〕，Janger & Schwartz 文，第1253页以下。

〔52〕 Joshua A. T. Fairfield & Christoph Engel, *Privacy as a Public Good*, 65 Duke L. J. 385, 456 (2015), http://scholarship.law.duke.edu/dlj/vol65/iss3/1，2017年8月22日访问。

可见，个人信息的公共性或公共物品性已经得到越来越多的学者认可，而这必然进一步地得出个人信息保护的非个人决定性的结论。

（三）个人信息保护的社会决定性

个人信息的公共性、社会性决定了个人信息保护的范围和程度的公共性和社会性。在这个意义上，个人信息不应当完全为个人所控制。

从保护个人信赖或交易安全的角度，一个社会不应当赋予个人控制自己的个人信息的绝对权，或者说法律不应当作出非经本人同意就不能获取其个人信息的规定。因此，一旦人们参加各种社会活动进入到具体社会关系，法律就应当保护公众的“识别权”，而不是拒绝识别或拒绝“曝光”。放任或鼓励人们隐藏身份或个人信息，会妨碍合作甚至鼓励人们从事不负责任的社会行为。我们所讲的个人信息，除了姓名、照片、体征、生物信息等外，大多数是人们社会活动和行为的结果。在计算机网络应用之前，这些信息除了少数被口耳相传得以传播或被档案或传记记载外，基本上不留痕迹，无据可查。而今天，人们的一切行为轨迹几乎都可以被记录下来，成为可以用来查询和分析个人的消费偏好、健康状况、资信状况和信用能力等的依据。这些信息来源于（至少是部分来源于）个人，而一旦被记录下来，则成为社会成员可以获取和利用的数据资源。这些信息资源是否要经个人同意才能为社会成员使用的关键是，一个社会是否承认我们每个人都需要客观、公正、准确地识别社会中的个体。笔者认为，个人的确希望有更多的“隐私”，有时甚至会刻意隐藏、掩饰或美化自己，但也应当保护社会公众（尤其是与之打交道的人）的“识别权”。

在波斯纳看来，隐私成了“不当呈现某人特性的权利”。他认为，人们希望通过选择性地披露有关自己的事实来操控他们周边的世界，而其他人有合法利益揭穿这样的不当呈现。[53] 在波斯纳看来，隐私权并不能被视为完全由个人自主的事情，而应当有所限制。托马斯·汉尼斯指出：“身份（identity）和构筑它的个人信息本质上是不可分的。它是匿名的对立面，我们不能两头都想要：你可以拒绝与其他人打交道而保持匿名，一旦你开始打交道，你必然失去匿名，获取了在他人眼里关于你的身份的认知。在这一点上，你的身份不是也不可能是你的私人控制。”[54] 因此，保护和提供救济以使人们对抗个人信息的不当使用不应当与构成个体识别的个人信息集合体的权属混为一谈。

进一步讲，个人信息本身具有社会价值，这是个人信息的使用不能由个人完全决定的深层理由。里根认为，隐私不仅对个人有价值，而且在三个方面对社会整体也具有价值。首先，隐私具有共同价值，因为所有个人对隐私会有某种评价，有某些共同看法。此外，隐私不仅对个人（作为个人或者所有共同体的成员）具有价值，对民主体制也具有价值。最后，隐私具有集体价值（collective value），技术和市场力量正在使个人信息保护相互联系在一起，在所有人没有相同的最低隐私保护水平的前提下，某个人很难享有隐私。[55] 在此基础上，她认为隐私并不是个人说了算的，而是反映着社会对哪些个人权益应当给予保护的共同价值观。一个社会应当存在隐私标准（norms of privacy）以指引我们的行为和我们的

〔53〕 Richard A. Posner, *An Economic Theory of Privacy*, 2 (3) Regulation 17 – 30 (1978), https://object.cato.org/sites/cato.org/files/serials/files/regulation/1978/5/v2n3 – 4.pdf, 2017 年 8 月 22 日访问。

〔54〕 Thomas Hemnes, *The Ownership and Exploitation of Personal Identity in the New Media Age*, 12 J. Marshall Rev. Intell. Prop. L. 1, 35ff (Fall, 2012).

〔55〕 Priscilla M. Regan, *Legislating Privacy: Technology, Social Values and Public Policy*, Chapel Hill, NC: University of North Carolina Press, 1995.

期待，即使技术和法律上可行，不符合隐私习惯的实践准则也不为社会所接受。如果社会价值观支持人们不当表述自己或提供错误的信息，鼓励人们“伪装”或“撒谎”，就会导致社会中有关个人的信息丧失真实性，不能作为判断个人的依据。因此，对隐私的界定应当反映社会认知或社会标准。[56]

施瓦兹也认为，隐私不应当被看作是封闭的“数据堡垒”。在绝对隐私或绝对公开两端，不可能实现个人数据的最优使用。信息隐私规则应当创设变化的、多维度的数据保护规则，以使个人数据为不同主体作不同观察。构筑隐私就是根据不同的调整界线，形成允许的查阅层级。[57]“信息隐私应当被理解为民主社会的基准。获取和限制访问个人信息有助于构筑我们生存的社会性质并塑造我们个人的身份。”[58] 隐私信息保护规则本质上就是个人信息收集、使用规则，而这样的规则不是由个体决定的，而应当是由社会共同决定的。这样的规则时常出现在社会习惯中，也可以来自制定法。他最终建议在联邦层面通过立法确立公平的信息隐私规则，以促进网络环境下的民主自由和个人自治。[59]

可见，他人或社会使用个人信息的正当与否不应当由个人决定，而应当由社会决定，由法律决定。个人信息保护和使用规则的制定须识别个人信息保护和使用所涉各方主体的利益，并依此进行利益衡量，实现合理的制度安排。这样的定位符合个人信息本身的特征和在社会中的实际状况，应当成为我国个人信息保护的基础理论。

四、个人信息保护模式的转型：社会控制论的提出

国际社会关于个人信息保护的制度规则和理论是建立在上世纪70至80年代的社会条件的基础上。这个时期基本上是以个人向特定主体提供个人信息被电子化存储利用为主的时代，个人信息的被动收集还没有大量出现，个人对个人信息还具有一定的控制力。但是，伴随互联网、物联网、大数据等信息通信技术的发展和应用，个人数据的多样化、全息化采集和应用已经成为网络社会的基本生态环境，数据采集、分享、分析和应用已经发生了巨大变化。在个人信息收集和利用环境发生变化的情况下，国际社会一直在反思这样的理论及其上升为法律规则后的弊端。[60] 欧美传统的个人数据保护或隐私理论完全建立在个人

〔56〕 Priscilla M. Regan, *Privacy as a Common Good in the Digital World*, 5 (3) Information, Communication & Society 382 – 405 (2002).

〔57〕 Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 Vand. L. Rev. 1607, 1664 – 1665 (1999), http://scholarship. law. berkeley. edu/facpubs/1162, 2017年9月10日访问。

〔58〕 参见前引〔39〕, Janger & Schwartz 文，第1221页。

〔59〕 同上文，第1701页。

〔60〕 例如，OECD于2010年启动1980年《隐私保护与个人数据跨境流通指南》的修订工作，并于2013年7月11日通过《关于隐私保护与个人数据跨境流通的指南建议（2013）》。修订采取稳健温和态度，仅通过增加部分原则的具体实施要求以提高原则的可操作性。但是，其他官方组织与社会人士则认为，在大数据时代，原先确立的八项基本原则已经显得过时了，要真正实现大数据的经济与社会价值并且同时保障数据主体的个人利益与自由，需要彻底改革基本原则的内容。这些异议声音中最具代表性的是微软公司。自2012年起，微软公司开始广泛号召全世界的专家学者关注数据保护问题，并组建针对OECD指南修订的工作组。2012年9月，微软公司在其总部举行了一场全球隐私峰会，邀请来自政府机构、工业领域、公益组织以及学术界的研究隐私与数据保护的70多位专家与会。微软工作组在经过一系列的理论研讨与实践调研后整理发表了一份学术报告，即《21世纪的数据保护原则——修正1980年OECD〈指南〉》（中译本参见高富平主编：《个人数据保护和利用国际规则：源流和趋势》，法律出版社2016年版，第32页以下）。

主义的基础上，这不仅与个人信息本身的法律属性不相吻合，而且无法解决个人信息的个人控制与社会化利用之间的矛盾。本文对个人信息的公共性和个人信息保护的社会性的分析，实质上构成了对个人信息控制理论的反思和批判，提倡个人信息保护的基本理论从个人本位到社会本位的转变或从个人控制到社会控制的转变。

首先，个人信息控制论极易导致个人信息的私权化。个人信息与个人的关联在于识别和联系到特定的个人，这并不足以使个人控制（或所有）个人信息及信息的使用（形成排他支配权）。个人信息是个人进入社会和社会了解个人的必要手段，个人信息的工具性决定了它应当处于可以为人使用的公共领域，而不是私人控制的客体。虽然欧美法律并没有将个人对个人信息的控制上升为一种绝对的私权，但是基本权利意义上的“控制”极易被私法化为一种私人权利，演绎成个人信息支配权。这便是今天将个人信息视为具体人格权（个人信息权）的根源。实质上，个人信息控制是维护个人自治的手段，而不是让个人控制个人信息（赋权）。在赋权意义上理解个人信息控制与个人信息的公共性相悖。

其次，个人信息控制论导致了个人决定个人信息的使用。在检讨域外个人信息保护的法律文件时，我们发现几乎所有的国际性和国家性法律文件均将个人信息流动或流通使用作为最终的目标，试图在保护个人基本权利的前提下实现个人信息的流通利用。但是在效果上，过度强调了保护，而忽略了流通利用。这是因为，在这些规则的形成年代，个人尊严或个人自由被着重强调，有关个人的信息被作为个人的“东西”，个人信息的使用被作为个人决定的“事务”，于是通过对个人信息的控制实现个人自治成为顺理成章的事情。但是，从个人信息具有社会性的角度，个人信息不仅关涉个人利益，也关涉他人利益和社会利益，因而个人信息的使用就不是个人可以决定更不应当是个人决定的事情。个人信息控制论导致个人信息的使用由个人决定，这一规则的泛化和绝对化，导致个人意志过度地渗入到个人信息的使用上。人是一种社会存在，而不是孤立的个体，因而个人信息的使用必然应当由社会决定，而不是由个人决定；同样，个人信息上哪些利益需要保护，哪些利用行为应当允许，哪些行为应当限制或禁止，也应当由社会决定，而不是由个人决定。

最后，个人信息控制论的社会基础不复存在。个人信息一旦脱离个人就意味着失去控制，因而个人只能通过特定的接受人（控制人）来控制个人信息，个人信息的控制人缺失或者不确定，就无法实现控制。在计算机应用之初，互联网还未出现或普及的时代，所出现的主要问题是，个人提供给政府、企业等的个人信息可能被控制人用于其他目的，这种滥用可能危害个人尊严或自由，因而需要给予个人知情、访问、更正甚至删除等权利。这便是个人信息控制论建立的基础。但是如今，虽然个人提供个人基础信息（尤其是身份信息）仍然是个人信息的基础，但是绝大多数可识别个人的信息并非由个人提供，而是由信息系统、网络运行、各种传感器等实时记录形成，无处不在、无时不在的网络形成了能够关联到个人或识别个人的数据海洋，而个人却不知道哪些信息被收集和使用，甚至不知道被谁收集和使用。数据的收集人（控制人）对于来源多样的海量数据的用途，也无法事先作出准确的判断，无法在收集时告知被收集人特定目的或用途，也就不能合法地实施告知同意。如果需要告知使用目的或任何目的变化都需要实施告知同意，实质上就等于扼杀大数据红利。如果征得个人同意时不告知使用目的或者只是一般性的概括同意，对个人信息的个人控制就将流于形式，不能实现制度设计的目标，反而成为数据控制人规避法律风险

的工具。因而，信息通信技术的发展已经摧毁了个人信息控制论建立和实现的社会基础，个人控制不再具有现实性，个人力量已经不能维护个人尊严和自由。如果法律仍然坚守这样的维权模式，要么无法实现保护个人的目的，要么成为大数据应用的障碍。

笔者认为，对应于过去的个人控制论，可以将社会控制作为大数据时代的个人信息保护和使用的理论基础。个人信息的社会控制论不再把个人信息视为个人的“东西”，也不将个人信息的使用视为完全由个人控制的事情（或成为个人自由的范畴），而是将个人信息视为社会的共同资源，由社会决定个人信息的使用。笔者认为，在个人信息的社会控制论下，个人信息保护将会产生三个方面的转变：

其一，个人信息的社会控制意味着个人信息的使用由社会习惯或法律确定，而不是由个人意志决定。由于个人信息的使用是社会运行和交往的必然，因而让个人控制其使用有失偏颇或不合正义。当然，社会控制并不否定信息主体对个人信息使用的必要控制。个人信息的社会控制旨在否定个人对于个人信息的绝对的、普遍的控制，尤其否定将其上升为私人控制权。在个人信息的收集和使用环节，要建立“以一般允许为原则，以个人控制（同意决定）为例外”的个人信息使用规则。个人信息非常宽泛，包含许多敏感性信息，蕴含有主体价值，需要给予个人必要的控制。有些信息本身敏感（如个人私生活、财务信息等），有些信息的使用场景或方式需要控制，否则就会给个人带来隐私或安全风险（比如个人通信方式、基因信息等）。对于这些敏感信息仍然需要个人同意，由信息主体控制其收集和使用。个人信息本身的敏感性和个人信息使用对个人权益的侵害风险，是限定同意范围的两个重要依据。同时，一旦进入到使用过程中，个人是否可以取回并将个人信息移转给他人或要求删除个人信息等，也必须审慎决定，使个人控制建立在正当的法律基础之上。各国应当在对个人权益和个人数据使用涉及的社会公共利益的全面判断的基础上，区分信息种类，结合使用场景和方式作出详细规范。社会控制论需要通过一套复杂的法律规范来实现。

其二，个人信息的社会控制意味着保护个人信息的责任主体由以个人为主转向以社会为主。在个人信息海洋中，个人的控制力非常无力和渺小，个人的同意越来越被证明不能控制个人信息的流向和生命周期，[61] 不能实现对个人权利的保护；甚至在个人信息与特定服务或交易联系在一起时，默示同意也仍然是流于形式。[62] 取回或删除个人信息只有在不接受服务的情形下才能兑现，而这也意味着个人拒绝网络或数据化生存方式。从欧盟《条例》可以看出，欧盟虽然也强调赋予数据主体许多权利以寻求司法救济，但主要是建立专门的个人数据行政监管体系来实现对个人信息的保护。《条例》共用了两个章节即第六章和第七章对独立的监管机构设立、职责及各监管机构之间的合作进行详细规定。此外，相比《指令》，《条例》新增了高额的行政罚款作为其制裁手段。[63]

其三，个人信息的社会控制还意味着法律规范的重心应从收集行为转向使用行为。重

〔61〕 美国联邦贸易委员会提出了数据生命周期的概念，可分为四个阶段：收集、编译与整合、分析、使用。See Federal Trade Commission, *Big Data: A Tool for Inclusion or Exclusion*, January 2016, https://www.ftc.gov/reports/big-data-tool-inclusion-or-exclusion-understanding-issues-ftc-report，2018 年 3 月 14 日访问。

〔62〕 参见王玉林：《默示同意在数据收集中的适用问题研究》，《情报资料工作》2017 年第 2 期，第 25 页以下。

〔63〕 参见《条例》第 83 条。

视对个人信息收集的控制变得越来越没有意义。除非个人信息一经使用即会给个人带来人身或财产上危害，否则应当将规范重点放置于如何安全使用上，减少使用给个人带来不必要的风险。正如托马斯·汉尼斯指出的："如有可能，规制个人可识别信息的潜在滥用行为并给予救济，而不是规制其收集和正当的使用行为。"〔64〕因此，个人信息控制的重心应当从收集环节转向信息的使用环节。

这些转变并非不保护个人权利或者个人权利保护的减弱，而是保护模式的转变。个人信息保护权本来就是个人信息上的法益保护，而不是对个人信息控制权的保护。三重转变的实现意味着不是依赖简单的赋权和个人维权实现法益保护，而是通过对个人信息控制人（使用人）的行为（义务）规范来实现法益保护，或者按照法律经济学者的观点，是采取责任规则而不是财产规范来保护个人信息。〔65〕同时，这样的转变，也意味着个人权利和社会整体利益更好地平衡。一旦我们不再将个人信息视为个人可以完全控制的东西，就需要由法律来决定个人信息使用的情形和条件，通过对数据使用人的行为规范来避免个人信息滥用行为对个人权益的侵害，通过对违法行为的惩治来实现对个人权利的保护。

基于个人信息保护模式从个人控制到社会控制的转变，我国个人信息保护规则就不仅需要校正缺陷，而且更要重新定位、全新设计。

我国立法中将"同意"作为收集和使用个人信息的前提条件，是对国际社会个人信息保护理论和制度规则的误读。收集和使用个人信息必须经被收集人同意，意味着赋予个人事先决定个人信息是否为公众使用的权利，具有将个人控制上升为一种私权的实际后果。这种在法律移植过程中的错误迫切需要得到校正。

问题不仅在于校正错误或与国际接轨上，还在于如何立足本国国情和大数据时代的需要建立我国的个人信息保护制度。国际社会的个人信息保护理论和制度是在特定时期形成的，与当时的个人信息收集和使用方式相联系，而当今的信息技术已经发展到以大数据为代表的新时期，国际社会的个人信息保护理论和制度规则也面临变革。我们不仅要正确理解和移植国际社会过去已经形成的规则，而且要创设适应大数据时代需要的个人信息保护制度。个人信息保护本身就是源自于对个人基本权利的保护，必须结合本国政治、经济、文化等社会环境，提炼社会的共同认知，形成既保护个人尊严和自由，又能够促进个人信息合法使用的规则。

在国际规则的借鉴方面，我们必须对个人信息保护从个人控制到社会控制的转变有清醒的认识。这是因为，深受个人信息控制论影响的国家，推翻已经延续很长时间的理论和制度规则不仅需要勇气，而且面临艰难的法律修改程序。尤其是在欧盟，刚刚颁布的《统一数据保护条例》全面地完成了个人控制论的法律表达，要在短期内实现这样的转变是难以想象的。而美国对信息隐私主要采取司法救济（普通法保护）模式，由法院最终确定哪些行为构成侵犯隐私权，所以美国的信息隐私保护始终保持规则的灵活性，代表社会控制

〔64〕 前引〔54〕，Hemnes 文，第 32 页。

〔65〕 财产规则与责任规则是由卡拉布雷西和梅拉米德两位学者在 1971 年联合发表的论文中提出的。中文译文和介绍参见［美］吉多·卡拉布雷西、道格拉斯·梅拉米德：《财产规则、责任规则与不可让渡性："大教堂"的一幅景观》，凌斌译，载《法律经济学文献精选》，法律出版社 2006 年版；凌斌：《法律救济的规则选择：财产规则、责任规则与卡梅框架的法律经济学重构》，《中国法学》2012 年第 6 期，第 9 页以下。

的隐私理论研究成果能够随时为法院审判所吸收。可以预见，个人信息的社会控制论将首先在美国成为现实。相对来讲，我国个人信息保护制度才刚刚建立，只有分散的几部法律中简单地加入了个人信息保护的内容，对如何保护个人信息还没有一致的看法。[66] 甚至可以说，在个人信息保护的理论和制度建设方面，我国还是一张白纸。在这种情形下，我们就可以没有任何负担地率先实现个人信息保护理论和模式的转型。

要实现这样的转型，我们必须抛弃简单移植国外立法的陋习，结合我国国情形成我国的个人信息保护理论，然后在该理论指导下设计符合我国国情和当今社会需要的个人信息保护制度。希冀笔者在借鉴国外理论分析基础上勾勒的个人信息的社会控制论，成为我国个人信息保护理论和制度重构的重要理论基础。

Abstract: The theory of individual control over personal information, which is based on the principle of human dignity in Europe and the principle of personal freedom in the U. S. , aims at protecting the citizen's fundamental rights and personal autonomy. The right to the protection of personal information, however, is not an independent and absolute right, but an institutional arrangement at the level of fundamental rights. Personal information has social and public properties because it concerns not only the interests the individual whose personal information is to be protected, but also the interests of other individuals and the society as a whole. Because of its individualistic foundation and its disregard for the social and public properties of personal information, the traditional theory cannot fully reflect the properties of personal information and adapt to the new situation and methods of the use of personal information in the age of big data. This means that the theory of personal information should undergo a transition from one based on personal control to one based on social control. China should develop a new personal information protection system adapted to the big data era by taking the legal properties of personal information as the starting point and the social control theory as the legislative guidance and striking a balance between individual interests and the interests of the society.

Key Words: personal information, personal information protection, privacy protection, social control of personal information

〔66〕 民法总则第 111 条未正面规定如何保护个人信息就是重要的证明。