

位置信息的社会控制和差异保护——基于社会控制论

徐培倩, 沈格平

杭州师范大学, 浙江 杭州

收稿日期: 2022年5月8日; 录用日期: 2022年6月8日; 发布日期: 2022年6月15日

摘要

在大数据时代, 个人信息具有了类公共物的属性。但我国在公民个人信息保护上采用个人控制论的观点, 不利于数据的流通和利用。此外, 个人控制论下公民个人保护能力弱、诉讼效益低, 实质上不利于个人信息的保护。而位置信息内涵丰富, 是难以明确界定的个人信息, 其价值内涵差异化。对于如何解决个人信息、位置信息因其差异化产生的困境, 个人信息社会控制论提供了新的视角。社会控制论构建个人信息收集和处理的新型“同意”规则, 允许社会主体普遍收集和控制数据化的个人信息, 通过建立健全相关监管体制, 使个人信息的保护责任由个人责任转变为社会责任, 使之具有公益诉讼的色彩, 增强保护能力, 提高诉讼效益。数据化的位置信息的保护应当适用一般信息的社会控制原则, 但对作为敏感信息的位置信息, 应该保留公民个人的“同意”授权。

关键词

社会控制, 位置信息, 数据权, 个人信息, 隐私

Social Control and Differential Protection of Local Information—Based on Social Control Theory

Peiqian Xu, Geping Shen

Hangzhou Normal University, Hangzhou Zhejiang

Received: May 8th, 2022; accepted: Jun. 8th, 2022; published: Jun. 15th, 2022

Abstract

At the time of big data, personal information existed as data is no more the own material which is

personal and private. The feature of public goods turns up in the essential concept of personal information, where the value connotation differs. The personal information which exists as data is the fundamental factor of production, even to be the petroleum to maintain the society working normally. However, the personal control theory, without adequate benefits of personal information's protection, is widely accepted in our country. In addition, the theory, attributing to weak individual ability to protect their own rights and poor benefits of proceeding litigation, is substantively useless for the protection. With various and varying connotation, the location information is hard to defined clearly. In the dilemma how to solve these issues, the social control theory raises brand new views. The theory requires constructing a new rule about consent to collecting and processing personal information, allowing the society to collect widely and control the data personal information. By refining the regulation construction, the responsibility of personal information protection transforms from individual into society, and the lawsuits feature of public interest litigation, thus improving the ability to protect and the benefits of litigation. Existed as data, the common personal information should be controlled under the society in principle. As for the location information which is more than sensitive, it is necessary to allow individual control through informed consent, therefore constructing a protection system based on the difference.

Keywords

Social Control, Location Information, Data Rights, Personal Information, Privacy

Copyright © 2022 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

1. 问题的提出

个人数据和个体(数据主体/信息主体)的人格权、财产权以及社会的商业价值等密切相关, 是重要的数据分析、处理原料, 被称为大数据时代的“石油”。随着时代发展, 个人信息不能被局限于隐私的外沿范畴, 其界限逐渐向公共领域发展, 构成了一个私人生活和公共领域相交织的特殊地带。位置信息具有动态变化内涵, 是这个特殊地带中一颗悬空的明珠, 虽然发着特别的光亮, 但始终难以落地。

个人控制论随着时代的发展暴露了一些弊端, 而社会控制论则为解决个人信息问题提供了新的理论视角, 本文基于个人信息的权益属性、保护规则及位置信息的差异保护, 来探讨个人信息、位置信息的社会控制和差异保护。

2. 个人信息的权属: 从隐私走向数据

个人信息是否为私人专有的“物品”, 是否具有商业价值的可交易性, 确定其权属内涵, 是分辨个人控制论或社会控制论的前提。

德国《联邦数据保护法》第三节对“个人数据”的定义是“已识别或可识别个人(数据主体)的个人情况或实质情况的信息”, 我国《个人信息保护法》第四条第一款规定, “个人信息以电子或其他方式记录的与已识别或可识别的自然人有关的各种信息, 不包括匿名化处理后的信息”, 在概念上, 我国的个人信息和德国的个人数据相同。欧洲以德国为例, 在允许个人数据作为数据合法处理、交易的基础上, 规范其处理、交易行为以保护个人隐私, 但在我国, 个人信息偏指向隐私权和人格尊严, 数据偏指向财产和商业价值, 两者存在截然的区别。

但不可否认, 个人信息的利益至少包括三个方面, 即个人(数据主体/信息主体)的人格尊严、数据控

制者对信息的处理、使用, 以及个人信息所涉及的公共利益[1], 三者对应的分别是个人、社会和国家/政府。从个人和社会利益的私法角度来看, 个人信息的权益属性包含人格权和财产权两个方面, 即个人信息作为隐私的范畴时, 具有人格权属性, 个人信息作为数据的范畴时, 具有财产权的属性。

2.1. 个人信息的人格权价值

个人信息的人格权价值体现在个人信息和隐私的重合性, 美国是最早研究和建立隐私权理论和立法的国家, 对个人信息收集、处理和使用的规范不像德国一样严密复杂, 其个人信息的立法较分散、灵活, 只有与人格利益关系密切的个人信息采用隐私权的方式保护。

美国学者尼森鲍姆认为隐私利益涉及多重维度的关联, 本质上是社会成员对于信息的独占利益, 在判断隐私的成立时要置于特定的社会群体关系中考察“场合的完整性”、群体的共同利益等因素[2]。美国法官托马斯·库利将隐私权定义为“不受干扰的权利”, 沃伦和布兰代斯合著《隐私权》一文提出隐私的本质是基于自由意志、感情的支配和原理[3]。隐私权理论的核心是基于人格尊严和自由权利, 对私密活动、空间及信息享有的限制他人接触的自决权, 因此, 与人格、人身等关系密切的个人信息应当属于隐私的范畴。

敏感的位置信息具有和人格尊严、人身和财产安全等切身权利关联密切的特点, 当行踪轨迹结合其他的数据, 并经过算法的分析, 往往很容易能判断出个人的健康状况、家庭住址、性取向等隐私的个人信息。因此, 位置信息的人格权价值不仅体现在信息本身, 还体现在位置信息具有的结合分析的特点, 一旦位置信息的收集、处理和使用侵犯这种敏感私密性, 个人信息的侵害就能升格为隐私的侵害。

可以看到, 隐私权和个人信息权具有法律属性、内容、保护方式和客体等差异[4], 并不能完全通过隐私保护代替集中统一的个人信息保护, 我国借鉴德国经验, 通过《个人信息保护法》等法律集中规范个人信息处理行为, 保护隐私和人格利益。但个人信息的人格权价值并不能掩盖一个基本事实——个人信息正逐渐衍生出财产性, 或者说, 个人信息其实天然地带有财产性。

2.2. 个人信息的财产权价值

位置信息具有重要的财产权意义, 能帮助数据、信息控制者更好地做出决策。商业决策离不开区位因素、人口流动和消费偏好等数据, 个人信息是这些原始数据、二次数据获得和产生的前提。商业主体获取个人信息(原始数据)或经分析、处理个人信息后所得的二次数据, 好比个人订购提供天气预报服务而获得预报数据, 其中数据与提供数据的服务乃是可交易、订购的商品和服务。所以可将位置信息及其提供行为视作是一种商品或商品性劳务, 商业主体获取位置信息等数据以提高决策有效性, 这发挥位置信息的财产权效益, 促进位置信息及数据的流动和利用, 既能挖掘位置信息作为数据要素的商业价值, 也有利于商业主体做出更有效的决策, 提高经营效率。

个人信息具有经济利益, 但这并不意味着其可成为独立的商品, 匿名化处理更不是个人信息成为商品的必要条件。根据可识别性的强弱, 个人信息分为直接个人信息和间接个人信息, 匿名化处理的个人信息并不能直接识别自然人的身份, 不属于法律意义上“个人信息”的范畴, 但匿名化是相对的, 而且大量匿名化的数据经过整合、分析往往能得出个人信息。以位置信息为例, 匿名化的位置信息在结合其他的数据而牵连出其他的个人信息, 这种现象尤能印证这个结论。可以看到一般个人信息的匿名性保护实质上不妨碍数据的分析和处理, 完全脱离个人信息范畴的数据化的信息交易并不具有实质保护意义。因此, 匿名保护应该被视作是一种脱敏措施, 针对与人格利益、人身和财产安全的敏感个人信息应当进行充分的脱敏处理, 但对于一般的个人信息, 匿名化处理作为其数据化、商品化成立前提的意义并不大。

2.3. 个人信息区别于个人隐私——公共属性

确立个人信息的公共产品属性是社会控制理论成立的基本前提。信息像商品一样是一般性质的公共产品,而个人信息就像是私有使用的个人物品,虽然个人信息具有私人性,但当个人信息在公共领域内存在而非仅在私密领域产生、存在时,应当认定为个人信息是一种数据,带有公共产品属性。个人信息的特点是直接或间接地指向个人,但本质还是信息,并不意味着个人对之就有直接的支配关系[5]。

从隐私到个人信息再到数据,三者之间存在时序发展和保护逻辑上的演进,隐私范畴中的私密信息及个人信息和数据,都以信息为保护对象,而区别个人信息和个人隐私是个人信息在权利属性上实现商业数据化、公共数据化可能的逻辑起点[6]。个人控制论坚持个人信息天然为个人私有的基本价值逻辑,将个人信息和个人隐私绑定在一起,主张效仿欧美以个人信息保护代替隐私权的保护,但这因个人隐私、个人信息及个人数据三者的内容、法律属性和保护规则等范畴的复杂而具有“可预见的失败”[7]。隐私概念的内涵确定,但外延却有极大延展空间,这导致了“隐私”无限扩大的可能,个人信息的保护必然和隐私的保护有交叉区间,但如果过分强调个人信息权中的隐私属性,那么两者将会错位,隐私权保护容易泛化。

信息是公共领域的材料,集合化的大数据是大数据时代信息表达的普遍存在形式,信息、数据存在的目的是被利用而非垄断,所以个人信息权、数据权实现的逻辑不是垄断,而是保障个人信息、数据在合法的范围内得到恰当的流动和利用。个人信息是公共领域数据处理的最为丰富的“原材料”,信息一旦进入公共领域,即使本身具有个人性质,便天然地成为公共领域的组成部分,法律不应该赋予某个主体对信息的专有权以阻断信息的流通和使用,“个人主义的隐私保护结果是无隐私”,甚至涉及公共领域的“隐私”也应该被视为是一种“公共物品”,因而隐私权利归属的基本单元乃是群体而非个人,所以隐私保护也蒙上了一层社会性和群体性保护的理论色彩[5]。

不论是数据财产观、工业产权观还是消费伴生观,现代社会生活中绝大多数的个人信息,至少是一般个人信息,是在社会公共领域产生的,具有一定程度的公共属性。从隐私到个人信息再到数据,公共属性是个人信息区别于个人隐私的重要判断标准。

3. 个人信息的保护立场:从个人控制走向社会控制

基于个人信息不同于隐私的性质,应坚持社会控制的立场,将个人信息及隐私保护的任務交给个人信息数据的控制者,允许个人信息的普遍收集,将规范重心从收集行为转移到处理行为,加强社会和政府的监督,督促控制者合法合理地行使处理行为,履行保护义务,并为个人设定完善的救济制度。这实际上是将个人信息数据保护的责任进一步地过渡给社会主体性质的数据控制者,个人信息和数据绑定在一起,通过社会、政府对个人信息、数据的监督性和救济性保护而非个人对信息和数据的专断性保护,既提高了个人信息和数据的利用效率,也通过数据权整合个人权利,以社会力量和政府公权力代为行使,增强了个人信息的保护能力。

3.1. “一般允许为原则,特别同意为例外”的同意规则

“一般允许”是社会控制的要求,“特别同意”是差异保护的体现。“同意”是一种私法意义上的法律行为,“告知-同意”的同意规则体现了对个人(数据主体/信息主体)的知情权和个人信息权的保障。知情权是个人对自己信息被收集、处理和使用的状态及程度的知悉权利,是个人对数据控制者的处理行为做出监督的前提。一些学者认为个人信息权的核心是个人信息的自决,“同意”实际上是基于自决权的意思自治,具有法律效力。然而,这可能是对《民法典》的不当解读。在我国《民法典》中,若要表

示“授权”，一般会采用“许可”、“授权”等词汇，而甚少采用“同意”一词。另外，我国《民法典》中对个人信息采取的是行为规制模式而非权利规范模式，这意味着个人的“知情同意”仅仅是合法收集、使用的必要不充分条件，取得“同意”并不意味着行为合法。因此，我国法律并未完全承认个人信息自决权。新型同意规则的构建，虽然保留了知情权，但是在现有的行为规制模式上更进一步，使一般允许(默示同意)成为原则，特别同意为例外[8]。

具体而言，个人信息的获取和收集，要基于个人信息价值内涵的差异，通过“一般允许”和“特别同意”的方式进行差异化规制，从基本个人信息到伴生、匿名的个人信息，应该相应地采取纸面同意、电子同意和无需同意的方式[9]。数据财产权的保护是消极的，以个人的“一般允许”为原则，而对涉及隐私的敏感性个人信息则以“同意”为例外，上文提及，根据不同敏感性的个人信息，采集(同意)和交易的规则也应该不同，在同意方式上采取“无需同意-线上同意-线下同意”递进的程序规制，是对“同意”规则的进一步发展。

对于位置信息来说，社会控制视角下的同意规则要求位置信息区别一般位置信息和敏感位置信息。在《个人信息保护法》第二十八条中，将敏感个人信息分为两个方面：其一是一旦泄露或者非法使用容易使信息主体受到危害的信息；其二是不满十四周岁未成年人的个人信息。但在该定义下，几乎所有的个人信息都是“敏感个人信息”。因为在收集手段、分析技术发达的大数据时代，通过对信息的整合与分析，几乎所有个人信息都具有广义上的利益性。因此，该条文对敏感信息的界定在实际上未能对一般信息和敏感信息起到较好的区分作用。笔者认为，可将识别性强弱作为敏感信息判断标准的重要因素。敏感信息应是指具有直接识别性的个人信息，即能够独立识别信息主体的信息，如行踪轨迹等。区别、划分不同类型的行踪轨迹及其他的位置信息，既是位置信息差异化保护实行的必然要求，也是其实现的重要理论基础。

3.2. 保护责任的转变——由个人到社会

个人信息的保护路径有两种，一是公权上的国家管理和保护，称为“权力保护”，表现在刑事责任、行政责任的承担，二是私权上的个人管理与保护，称为“权利保护”，表现在民事责任的承担。个人控制到社会控制的转变需要改变这两种保护路径，在“权力保护”层面构建国家的个人信息和数据收集、处理、使用和交易等监管体制机制；在“权利保护”层面，应转变个人信息的保护方式，从防御性的侵权法保护转变为积极性的财产权保护。

转变个人信息的控制、管理和保护的权利与义务，并不是弱化对个人信息的保护，而是转变保护的模 式。大数据时代，个人(数据主体/信息主体)对个人信息的管理、控制和保护的能力相对有限，由于位置信息风险的滞后性，个人难以预测到当前个人的做出的“同意”行为所带来的后果。明显，相比于组织化、集团化的社会企业等组织，个人将处于弱势地位，如果采用损害的保护模式，既在实质上增大了个人管理和保护的 压力，同时限制了个人将个人信息变现的可能，数据主体/信息主体只能消极地在个人信息受损时做出防御性的保护，提出救济补偿，而数据控制者非法处理、使用个人信息/数据只需一定的补救，个人在维权方面的成本较高，诉讼效益较低，实质上不利于个人信息的保护。

此外，制度经济学认为侵权法保护下的个人信息获取的成本较高，而个人信息的财产化数据化，降低了个人信息的个人保护成本和商家的交易成本，而促进个人信息保护的方式在于个人信息交易、处理和使用的监督管理。个人向商家披露个人信息以换取财产利益是合同订立行为，应用合同的观点来认识、规范个人信息的流转，同时设立“数据交易市场”来规范和促进数据交易行为，加强对数据控制者处理、使用行为的法律规制[10]。

4. 结语

基于社会控制论的新型保护模式,并不是对人格的漠视,而是站在现实的角度更加充分、合理地保护位置信息乃至个人信息。我们应当承认,在大数据时代,在数据企业面前,个人的力量是极其渺小的。繁多冗杂的信息条款让普通人疲于应对,而个人与企业力量的悬殊让有心维权者无可奈何。而当我们把信息的控制权给予社会的同时,我们也将把保护个人信息的责任部分转移至社会、转移至国家,依靠国家与社会的力量对我们的信息给予更全面的保护,减轻群众的负担。同时,对于企业而言,也将降低信息流通的成本,从而更好地发挥信息资源的效益。

致 谢

感谢学院对本项目的支持,给予了笔者莫大的动力。其次衷心地向指导老师表示感谢,通过老师的指导,使笔者能够提出保护个人信息的新思路。此外,感谢指导老师对论文结构提出的宝贵意见,使论文逻辑更清晰顺畅。最后,本论文的完成离不开无数研究个人信息保护的学者的真知灼见,笔者不过是站在了巨人的肩膀上才得以完成拙作。

参考文献

- [1] 高富平. 个人信息使用的合法性基础——数据上利益分析视角[J]. 比较法研究, 2019(2): 72-85.
- [2] 吴伟光. 从隐私利益的产生和本质来理解中国隐私权制度的特殊性[J]. 当代法学, 2017, 31(4): 50-63.
- [3] 张里安, 韩旭至. 大数据时代下个人信息权的私法属性[J]. 法学论坛, 2016, 31(3): 119-129.
- [4] 王利明. 论个人信息权的法律保护——以个人信息权与隐私权的界分为中心[J]. 现代法学, 2013, 35(4): 62-72.
- [5] 高富平. 个人信息保护: 从个人控制到社会控制[J]. 法学研究, 2018, 40(3): 84-101.
- [6] 孔祥俊. 商业数据权: 数字时代的新型工业产权——工业产权的归入与权属界定三原则[J]. 比较法研究, 2022(1): 83-100.
- [7] 徐明. 大数据时代的隐私危机及其侵权法应对[J]. 中国法学, 2017(1): 130-149.
- [8] 高富平. 同意≠授权——个人信息处理的核心问题辨析[J]. 探索与争鸣, 2021(4): 87-94+178.
- [9] 张新宝. 个人信息收集: 告知同意原则适用的限制[J]. 比较法研究, 2019(6): 1-20.
- [10] 刘德良. 个人信息的财产权保护[J]. 法学研究, 2007(3): 80-91.