doi: 10.15936/j.cnki.1008-3758.2017.02.012

数据库开发与应用中的隐私权限制

李延舜[1,2]

(1. 苏州大学 王健法学院, 江苏 苏州 215021;
2. 河南科技大学 法学院, 河南 洛阳 471023)

摘 要: 以个人数据为直接对象的数据库上存在着两种权利:数据库权利和数据主体权利。对前者而言,它的核心是财产利益;对后者来说,它的核心是人的尊严和人格利益。两种权利在数据库的开发和应用过程中经常冲突,体现在个人敏感数据被非法收集和处理,以及公民被无处不在的数据监控包围。然而,现代文明是向尊重和保护隐私权的社会不断迈进的过程,数据资源的整合与挖掘不能以牺牲个人隐私为代价。数据库的开发与利用必须尊重数据主体围绕隐私的基本权利,并从数据分类、数据处理行为、数据库控制者责任三个方面设置相应的法律保护条款。

关 键 词: 数据库; 隐私权; 知情同意权; 被遗忘权; 数据库控制者责任

中图分类号: DF 523 **文献标志码**: A **文章编号**: 1008-3758(2017)02-0187-08

Restrictions from Privacy Rights in Database Development and Application

LI Yan-shun[1,2]

(1. Kenneth Wang School of Law, Soochow University, Suzhou 215021, China; 2. Law School, Henan University of Science and Technology, Louyang 471023, China)

Abstract: There are two types of rights for those databases that take personal data as their direct object, i. e., database rights and data subjects' rights. To the former, its core is property interests, and to the latter, its core is human dignity and personality interests. These two kinds of rights are always conflicting in database development and application, represented by such cases that personal sensitive data are illegally collected and utilized, and citizens are surrounded and monitored by ubiquitous data. However, modern civilization is moving towards respecting and protecting privacy rights; accordingly, data integration and data mining cannot be achieved by sacrificing personal privacy rights. Database development and application should respect the fundamental privacy rights of data subjects, and relevant protection laws should be set from such aspects as data classification, data processing behavior and data controllers' responsibility.

Key words: database; privacy right; right of informed consent; right to be forgotten; database controller's responsibility

如果将数据比做人体的血液,那数据库就是供血液流淌的血管,数据存储于数据库之中并通过数据库的流转而流转。然而,在全民热议数据隐私保护的同时,却少有学者及实务人员问津数据库开发与应用中的隐私权限制问题。实际上,最容易对数据隐私造成侵犯的正是数据库的控制者:从数据库的结构设计到数据的收集、存储、传输及其他处理,数据隐私保护的背后离不开对数据库的开发和应用进行规制。

收稿日期: 2016-09-07

作者简介: 李延舜(1981-),男,山东莱芜人,苏州大学博士研究生,河南科技大学讲师,主要从事隐私权法与个人信息保护法研究。

一、问题的提出

我们常将“数据”和“信息”替换使用,但严格说来两者有很大区别。“数据是对信息数字化的记录,其本身并无意义;信息是指把数据放置到一定的背景下,对数字进行解释、赋予意义。例如:‘1.85’是个数据,‘奥巴马身高1.85米’则是一则信息。但进入信息时代之后,人们趋向把所有存储在计算机上的信息,无论是数字还是音乐、视频,都统称为数据。”[1]35 这种解释在凸显了大数据时代隐私保护重要性的同时,与《欧盟数据保护指令》中的“数据”不谋而合,它将数据定性为“自动化处理”的数据,而这种“自动化处理”基本上是在数据库中完成的。数据库中无疑包含许多个人敏感信息,那么,在“保护数据库中的个人隐私”与“数据库的开发与使用”之间该怎么平衡呢?这里存在两个难题。首先,个人数据和个人隐私存在交叉,对个人数据的非法收集和使用必然会涉及隐私权保护问题①。但基于政府管理和一大堆产业健康运行的需要,个人数据的收集和使用在特殊行业必须被允许,如信用报告行业、金融行业、高等教育及科研行业、保险行业、健康护理行业等。其次,以个人数据为直接对象的数据库事实上已经分裂出两种权利:数据库权利和数据主体权利。根据前者,数据库权利人可以追求数据库的利用最大化,并尽可能实现数据库的有偿使用;而根据后者,“信息主体主张尽可能控制自己的个人信息不被不当传播和利用”[2]。这两种权利因基于同一客体而常常引发冲突。一方面,数据库的产生凝结着开发者的劳动和智慧,“数据库控制者对数据库建设还投入了金钱,需要通过市场交易实现价值补偿及相应的利益。如果他们的数据库不需付钱就能够使用,持续投资的动力就会丧失或被严重减损”[3]。无论是欧盟1996年发布的《数据库保护指令》,还是美国以盗版侵权为基础的救济路径,都对数据库权利人的“收益”权能予以保护。近些年来,随着商家对个人信息的渴望升级,一个新的产业即数据库产业形成。在美国,“数据库产业好比信息时代中的交易市场,商家将收集而来的个人信息在市场中进行销售与交易。信息列表的租金价格从几美分到每个姓名1美元不等。超过550家公司都加入到了个人信息产业之中,并且这些公司的年收入都达到数十亿美元。单单邮件列表的销售金额就达到了每年30亿美元”[4]126。但另一方面,伴随数据库的生成及交易,数据主体的隐私权状况堪忧。2010年Facebook网站遭遇“泄密门”,2011年韩国“赛我网”3 500万用户资料泄露,2013年中国人寿80万保单信息泄露后我国又接连发生开房信息泄露案和圆通快递客户信息泄露案,接连不断的个人信息泄露使得我们认清:数据库的开发与应用不能以牺牲隐私权为代价。

俄裔美国哲学家、文学家艾因·兰德说过:“文明,就是向拥有隐私权的社会不断迈进的进程。”[1]157 庞德也指出:“隐私权是产生于今天越来越拥挤的社会生活条件下的一种现代性需要,……把纯属个人性的事务中有关私人的问题予以公开是对人格权的伤害。它损害人们精神上的平静与舒适,而且可能造成比单纯肉体伤害尖锐得多的痛苦。”[5]从数据库的形成来看,个人成为源源不绝的数据来源,不仅仅是个人身份信息,还有地理位置、消费记录、医疗情况、健康档案、社交网络等。数据的形式也从纯粹的文字变成了视频、音频、图像及文字的综合。可以说,现实中活生生的人被数据化、格式化,由“主体”变成了被处理的“客体”,这种转变与康德所言的“人是目的、而非手段”相悖。正是在此层面上,美国著名法学家Jessica Litman认为“数据库开发者的行为和活动对个人尊严是一种伤害,这种活动理应受到谴责”[4]519。然而,大数据时代数据的收集与使用已经成为不可逆的潮流,任何严格意义上的个人数据禁用都与时代的发展要求相悖,所以“美国政府一向主张隐私法的宗旨是防止滥用,而不在于保护”[6]。即使在保护力度最大的欧盟,也只规定了特殊种类的个人敏感信息不得收集,而非完全禁止。立法者需要谨慎设计的,不仅是数据收集和使用的正当情形及正当过程,还需结合数据库的

① 一般认为,敏感个人信息属于隐私,故而隐私权法和个人信息保护法因保护对象存有重叠而产生竞合现象。但两种法律显然又是不同的:首先,传统隐私权是一种消极性权利,它的基本理念是原则自由、例外禁止;而个人信息保护法含有积极权能,它的基本理念是原则禁止、例外允许;其次,隐私权只保护敏感个人信息,而个人信息保护法对所有信息都提供保护;再次,判断隐私侵权必须经过利益衡量,因为它是一项框架性权利,而侵犯个人信息的违法性认定无须进行衡量,直接推定;最后,隐私侵权赔偿必须以现实损害的存在为前提,而侵犯个人信息无此种考量,任何个人信息的泄露都隐含着人格或财产受损失的危险。

开发与应用，毕竟，数据库一头连着数据主体，一头连着数据库权利人。

二、数据库开发与应用过程中侵犯隐私权的类型

公民作为数据来源的最大制造者，其一言一行都引起数据库开发者的深切关注。数据库开发与应用过程中对公民隐私权的侵犯类型主要有两种：一是数据隐私的非法收集与处理，二是数据监控的无处不在。

1. 数据隐私的非法收集与处理

对个人数据收集最全面、最详细的永远是政府。以人口普查为例，虽然我们可能对德国的1983年人口普查案更为熟悉，但实际上，美国人口普查的密度和信息收集的种类之多也毫不逊色。美国1790年开始第一次人口普查时，仅询问了4个问题。1830年普查中有两个私人问题——答卷人是否失聪或失明。但到了1860年，人口普查却罗列了142个私人问题，如疾病情况、残疾情况、经济情况等。与数据的爆炸式增长相伴随的是数据库和数据处理中心的增多，还以美国为例，“1998年，联邦政府共拥有432所数据中心，专门负责各类数据的存储和维护工作。2010年，数据中心的总数跃升到2 094所，翻了几倍”[1]38。

除政府外，商家对个人数据的收集也不遗余力。各种网络社交平台及购物网站虽然丰富着我们的日常生活，但不可否认的是我们的个人信息也在一次次“上传与发布”中被收集，包括我们的位置、照片、评论、视频、消费等等。也许会有人质疑，这些五花八门的个人数据能分门别类、条理清楚地存储到数据库中吗？答案是肯定的。传统的数据库限制很多，由于“结构化”的原因，每个“域”中都包含特定种类和长度的信息，但“新型数据库的诞生，打破了关于记录和预设场域的陈规——非关系型数据库的出现，它不需要预先设定记录结构，允许处理超大量五花八门的数据。……据统计，只有5%的数字数据是结构化的且能适用于传统数据库”[7]61-64。也就是说，诸如网页和视频等也已经可以入驻数据库，并与特定的数据主体相关联。

某些数据库的产生基于特定目的，所以数据库中的个人信息比较单一和零散，这给普通民众造成一种假象，即：一些不太相关的个人信息被收集对他们来说无关紧要。这种认识真的需要改变了，著名的“马赛克理论”告诉我们：若干信息片段的结合比单个信息本身更具有价值。美国著名计算机学家Latanya Sweeney所作的一项研究表明：“将邮编、出生日期及性别集合起来基本上可以确定这个人的身份，这种可能性达到了87%。”[4]460-461德国联邦法院在1983年人口普查案判决中指出：“在综合性资料系统下，可以将个人资料组合成部分或相当完整的人格图像，以致会对于个人人格产生威胁，因此原本无关紧要的一项资料，可以在资料整合之下产生新的价值，所以在此情形下已不再有所谓不重要的资料。”[8]因此，以“可识别性”为基础的个人信息保护在数据库的“联结与比对”面前步履维艰，大量的个人数据与“可识别性”不再直接相连，而需要在个案中作出具体衡量。

2. 数据监控的无处不在

数据库对公民隐私侵犯最严重的就是数据监控，因为它不是针对个人而是全体。当我们的一言一行、一举一动都以数据的形式被记录，整个天地不过是放大了的牢狱。巴拉巴西在其名著《爆发》中说：“我们正处于一种不断变化但却日趋精密的被监视状态中，……正是这些记录的存在引爆了个人隐私危机，而这一问题的严重性再怎么夸大也不为过。”[9]

(1) 政府数据监控

数据监控已经遍布物理空间和网络世界，人生的每个重大步骤都能在政府数据库中找到痕迹。以美国为例，“美国联邦机构与部门拥有差不多2 000个数据库，其中涉及的事项包括移民、破产、社会保险、军事人员及不计其数的其他事项。州政府保存有许多公共记录，涉及包括逮捕、出生、刑事诉讼、结婚、离婚、财产所有、选民登记、工伤保险及其他各种类型的事项”[4]123。可见，政府已经完成了对公民从生到死的立体式监控，这种监控让学者们无比悲观：“行为人侵犯个人隐私权的行为不仅是对我们人格尊严的践踏，而且还将造成社会性的恐慌，或者预示着极权主义社会的到来”[10]342。奥威尔笔下的《一九八四》描述的就是这样一种极权社会，人们称其为“Big Brother”。

国家中心数据库的建立本质上是扩张公权力对公民私生活的介入[11]，而私生活权是基本人权，必须对公权力的扩张予以防范。因为事情往

往就是这样,一旦作出了退让,对私生活自主的下一步限制便会接踵而至,直至最后的一点自由完全消失。9·11事件后,美国迅速通过了《爱国者法案》并加大了监控的力度,直至"棱镜门"事件,人们才恍然惊醒:"随着诸如扩展存储器之类的新技术的诞生,我们很容易就能获得个人记录、现金交易和汽车注册等电子数据,从而迅速建立起任意对象的全面档案。……如此强大的监控力量需要有人来对它进行不间断的监管。这些系统会在侦查犯罪分子时担当重要角色。但危险在于,这些设施事实上是一个巨大的监控工具,如果政治环境发生改变,这些工具也会迅速更换其监控对象"[12]。无处不在的监控不仅会侵犯人的尊严,让人人格分裂,带来"偏好伪装",还会给民主政治带来灾难。"由于我们的言行都给记录在随时可存取的数位记忆中,要面对的不再仅是当代的批判,甚至还得面对未来的批判。……我们可能就变得如同惊弓之鸟,对于发表言论过度谨慎;换句话说,'未来'对我们现在的言行造成了寒蝉效应。"[13]一句话,如果不对政府监控实施强有力的监督和约束,人民终将会自食其果。

(2) 商事数据监控

如果说"Big Brother"的隐喻指向政府,那么私营部门就是"Little Brother"。正如David Lyon所言:"Orwell所描绘的是中央政府集权统治下的反乌托邦的景象。然而,他万万想不到分散式的消费主义趋向也能够对社会控制形成如此大的影响。"[14]一些拥有庞大数据库的商家对个人数据的挖掘和使用甚至超过了政府,如2009年甲型H1N1流感爆发的前几周,谷歌的工程师就在《自然》杂志上发文揭示谷歌能准确预测冬季流感传播的原因——特定的检索词条,如"哪些是治疗咳嗽和发热的药物";《纽约时报》记者查尔斯·杜西格也报道过美国折扣店塔吉特公司利用20多种"关联物"从而给"怀孕趋势"评分,在完全不和准妈妈对话的前提下实现了对一个女性在什么时候怀孕的预测。商事主体对个人数据的收集和挖掘更加贴近生活,尤其集中在身份、疾病、健康、职业、爱好、收入、教育、婚姻、育儿、房产等方面,并以此有针对性地推销他们的产品和服务。

有商家曾预言:"我们的爱好、癖好、倾向及需求被他人掌握得一清二楚的时代终将会到来。在那时,我们将会被分类、整理、归类,我们鼠标的每一次点击都会被监控。"[15]这样的预言已经成真:互联网经济已经成为新的经济增长点,人们越来越多地在网上购物、支付、开展全球性商务洽谈和合作;基于Web 2.0技术开发的社交网站也让民众迎来了"秀"时代,个人信息发布与互动交流变得异常简单。然而,换个角度看,这些方便了我们生活的新兴科技在不知不觉中完成了对我们全方位的监控:"亚马逊监视着我们的购物习惯,谷歌监视着我们的网页浏览习惯,Twitter窃听到了我们心中的'TA',Facebook似乎什么都知道,包括我们的社交关系网"[7]195。这个结论不禁让我们毛骨悚然,进而作出如下判断:互联网的发展使得监视变得容易、成本也更低廉,"如果放任网络时代的发展而不对其加以限制,那么Orwell式的隐喻就会产生一种截然不同的效果,即社会中主要的隐私权威胁并非来源于政府,而是来源于商业企业领域"[16]。

三、数据主体围绕"隐私"的基本权利

虽然数据库开发者或控制者拥有对于数据库的相关权利,但数据库中的数据并不像普通物品一样能被随意处理,因为大量的个人数据凝结着人格、附着着尊严。历史上曾有过类似案例,大仲马曾因贫穷将其与一位女星的艳照卖给一个摄影师,后来反悔并在试图阻止摄影师传播、发行这些照片的时候遇到了难题,因为摄影师对这些照片拥有财产权,而财产权是神圣不可侵犯的权利。但巴黎上诉法院却认为:"大仲马还享有一个全新的权利,即隐私权。……即便他人在一开始就同意行为人公开披露其令人尴尬的照片,他人必须保留在随后撤销其同意的权利,并且行为人公开披露此类照片应事先通知他人这些照片有可能会对其个人形象造成不良影响,提醒他私人生活必须用围墙隔开。"[10]360数据库权利人对数据库的处理与该案有相似之处,即要受到数据主体基本权利的限制。《欧盟基本权利宪章》第8条规定每个人都有权保护自己的个人数据,一些成员国的宪法也明确将数据保护作为一项基本权利来对待,如1975年《瑞典宪法》第2条、1976年《葡萄牙宪法》第26条、1978年《西班牙宪法》第18条、1993年修正的《比利时宪法》第22条等。那么,数据主体围绕隐私的基本权利有哪些呢?

1. 知情同意权

知情同意权兼有“程序性权利”和“实体性权利”的双重性质。首先，它是一种程序性权利，通过被“充分告知”且“自由、明确”地表达“同意”这个正当程序从而彰显数据主体的权利地位；其次，它又是一种实体性权利，什么程度的“告知”才能让数据主体“知情”，且什么情况下作出的“同意”是有效的同意，这些构成知情同意权的实质性标准。欧盟 95 指令将“同意”定义为：“数据主体在被充分告知信息的情况下自由作出的、明确表明其同意处理与其有关的个人数据的意思表示。”[17]71 该定义涵盖了知情同意权的所有标准：同意的前提是被充分告知信息；同意的作出必须清楚而不含糊；同意的作出基于自由判断；同意必须是明确的。

知情同意权可以说是个人数据保护法中的基础性权利，它在以下三个方面发挥自己独特的作用。第一，知情同意权与数据库开发和利用的默示规则有关，即个人信息不得被随意收集或使用，除非经过个人明示同意，这也被称为“选择性加入”(opt-in)制度。“选择性加入”是尊重数据主体个人信息权利的最好体现，那些信息性隐私权的坚定拥护者都毫无疑问地站在“opt-in”这边。美国联邦通信委员会在 U. S. West v. Federal Communications Commission 案中主张，“选择性加入程序可能是使消费者享有知情同意权利的最低限度的措施”[4]32。1988 年的《录像带隐私保护法》就规定录像服务提供商若要将消费者购买或租用录像的信息分享给第三方，就必须要在每一次分享信息之前得到消费者的允许；1994 年的《驾驶员隐私保护法》也有类似规定。这种做法尽管会给数据库买卖和第三方对个人信息的使用带来成本上的增加，但它能迫使数据库权利人和第三方人们披露更多的数据交易和使用信息；第二，知情同意权是判断数据库权利人或第三方侵犯数据主体隐私权成立与否的直接标准。举例而言，在通过网络收集个人信息的场合，各大网站经常采用“隐私声明”的方式告知网页浏览者信息收集的情况，似乎访问者只要在隐私声明的页面逗留，就视为访问者同意网站的做法，且不说绝大多数网民根本就不会阅读这些条款，仅从形式上而言，网站的隐私声明鲜有采用“显著”的标题和链接来吸引访问者的注意力，而且，繁琐冗长的声明不仅难懂，还让人失去阅读的兴趣。因此，隐私政策通常都无法反映这些网站真实的信息收集利用活动的本质[18]。第三，知情同意权是数据库权利人或第三方侵犯数据主体隐私权的“抗辩理由”。“自愿者无损害”是古老的拉丁格言，美国 Prosser 院长认为：“虽然被告能够主张的隐私侵权抗辩事由多种多样，但被告能够主张的最主要的还是证明原告同意被告披露自己的相关隐私”[10]434。

2. 获取权、拒绝权、被遗忘权

知情同意权多发挥作用于数据库的开发、生成阶段，即个人信息的收集阶段，而在数据库的使用和挖掘阶段，数据主体享有获取权、拒绝权和被遗忘权。

欧盟 95 指令第 12 条即数据主体的获取权，包括知情权和修改、删除或限制使用权。具体说来，即数据主体有知悉个人数据是否被处理、数据处理目的、数据种类及数据接收者的权利，有修改、删除或者限制使用不完整、不准确、已过时的个人数据的权利。

欧盟 95 指令第 14 条规定了数据主体的拒绝权，指除国内法律另有规定外，数据主体有权根据自身状况或其他合法理由强制性拒绝对其个人数据的相关处理，尤其是未经允许将个人数据对第三方披露，或者出现其他违反公平实践原则的个人数据处理情形。

被遗忘权最早出现在欧盟于 2012 年提出的《一般数据保护条例立法提案》，并因 2014 年的谷歌西班牙案成为焦点。它的本意是大数据时代，“记忆”成为常态，“遗忘”成为例外，如果不能将那些过时的、与数据收集处理目的无关或数据控制者没有正当理由继续保存的个人信息删除，人将永远伴随“记忆的乌云”生存。“被遗忘权暗含了一种权利和义务，数据主体有权利控制有关自己的信息，可以删除那些已经过时或不希望第三人看到的信息，而作为数据控制者，有义务尊重数据主体的意见，依据数据主体的意愿，移除并终止传播相关错误的、过时的数据。”[19]《一般数据保护条例》已于 2016 年 4 月 14 日通过，并将于 2018 年正式生效，其第 17 条即规定的被遗忘权。

在数据库中，我们被重新构建成一个由各种数据构成的“数字人”。但矛盾的是，“隐私权问题既来源于信息的无处不在，也来源于信息的局限性，信息既包含了我们生活的许多方面，又无法对我们进行准确地描述，并且可能会扭曲我们的人格与生活”[4]144。所以，数据库的开发和利用应建

基于尊重数据主体的基本权利之上,即便我们生活的世界较之过去已经可以更自由地分享个人信息,但信息隐私保护的价值永不过时。

四、数据库开发与应用中的隐私权保护

数据库开发与应用中的隐私权保护要侧重三个方面:首先,"内容"方面的区分,即对数据库中的"数据"进行分类,将普通数据与涉及个人隐私的数据相分离;其次,"行为"方面的限制,即数据库的开发与应用要遵循特定规则或原则;最后,"责任"方面的承担,即数据库的控制者要对数据库开发与应用过程中侵犯公民隐私权的行为负责。

1. 数据的"分类"

并非所有与个人相关的数据都是隐私,对于何种数据才算隐私,要想分得一清二楚并不容易。实际上,对数据的分类是一个不断"细化"的过程,即围绕公民的私人领域,将其隐私信息剔除出来,予以特殊保护。这个"细化"过程可分为两步走。

第一步,确定"可识别"的个人数据。"可识别"的个人数据是指能够与具体个人相连接的数据,分为"已被识别"的个人数据和"可以被识别"的个人数据。"已被识别"的本质是"直接识别",如公民的身份证号、驾驶证号、社会保险号、姓名、指纹、DNA等,不需其他就能直接指向本人;"可以被识别"是一种"间接识别",往往需要几个数据相结合才能判断出数据主体是谁,如同时出现邮编、出生年月、性别三组数据的情形,就属于"可以被识别"的数据。尽管直观上"已被识别"的个人数据更值得重视,但随着"匿名化""模糊化""数据库比对"等数据处理技术的发展,区分直接识别与间接识别的重要性在减弱。世界范围内的普遍立法也证明了这一点,如在欧盟,一个"可以被识别的个人"的信息和"已经被识别出的个人"的信息的地位是一样的。《经济合作发展组织隐私指引》(1980)中个人数据被定义为"任何与一个已经被识别的个人或者可以识别的个人有关的信息";《亚太经合组织隐私框架》(2004)也将"可以识别个人身份的信息"定义为"与一个已经被识别的或者可以被识别的个人有关的任何信息"。

第二步,在具备"可识别性"的基础上将个人数据分为"一般数据"和"敏感数据"。将个人数据分为"一般"和"敏感"是欧盟各国的立法特色,欧洲理事会通过的《有关个人数据自动化处理的个人保护协定》(1981)最早进行了此类划分,95指令延续了此分。某数据属于"一般"还是"敏感"对数据库的开发和应用至关重要:一方面,"资料敏感性的高低不同,资料处理对个人资料隐私造成风险的大小也各异"[20],另一方面,"一般"与"敏感"数据的划分也旨在适用不同的保护和利用规则,对敏感信息予以特殊保护,"同时给其他个人一般信息的利用松绑,更好地调和个人信息保护与利用的利益冲突。不同类型的个人信息对于实现主体的利益需求的影响不同,以此为导向对个人信息加以类型化,实现个人信息保护与利用中多方主体的利益平衡"[21]。然而,"一般"与"敏感"区分的标准为何呢?德国联邦法院早在判断一般人格权的侵权程度时就提出过"领域理论",即将个人私生活分为"隐密领域""私密领域"和"个人领域"。依据该理论,离私生活中心越近的数据越敏感,离私生活中心越远的则一般,"不远不近"的则需通过利益衡量来作出具体判断。虽然有学者认为"领域理论"在"大数据"时代已"过时"[22],但作为一种理论模型,在无法提供清晰、明确、确定的"敏感"数据列表之前,该理论的生命力不会衰减。

2. 遵循数据保护的一般原则

在数据库的开发与应用过程中,除数据库本身的结构及功能外,数据的收集与处理要遵循数据保护的一般原则是关键要素。个人数据处理的原则基本上有:①合法性原则,仅能为了明确、具体、合法的目的去处理数据,欧盟95指令第7条、《一般数据保护条例》第6条即相关规定;②目的限制原则,数据的收集与处理不得以与该目的相矛盾的方式进行;③比例原则(又可称为最少数据原则),个人数据应当充分、相关,不超出处理目的所需的限度;④准确性原则,且保持数据时新;⑤附期限原则,即数据储存的期限不得长于为达到目的所需的时间;⑥安全原则,数据控制者应根据处理所导致的风险采取适当技术和管理措施以保护数据安全。

《一般数据保护条例》第5条在上述原则之外,提出了一项新原则:透明性原则。该原则要求数据控制者向数据主体披露正在处理的与其有关个人数据的基本信息,包括"①控制者的身份;②确认与其有关的数据是否正在被处理,以及与

处理目的有关的信息；③相关数据的类型、数据传输的接收者或者接收者的类型；④与其有关的数据自动处理的理由；⑤对于未遵守一般指令而处理的数据进行更正、删除或者封锁，并将该数据的更正、删除或者封锁通知接受数据的第三方”[17]22。透明性原则的实质是要求数据控制者实施一种达到“充分”程度的披露行为，美国联邦贸易委员会曾在两个案子中对“透明性”进行了解读：在 2009 年针对 Sears 公司的诉讼中，美国联邦贸易委员会指出，“虽然 Sears 公司在让消费者使用该款软件之前提供了一份许可协议，但是该许可协议所用词汇模糊，大概说清了要对用户进行追踪，但没有充分告知数据被收集的范围，这种行为就是欺诈”[4]473。透明性原则是抵消数据控制者与数据主体之间巨大“权力鸿沟”的重要设计，也是高悬在数据库权利人头上的“达摩克利斯之剑”，对公民的数据隐私保护极具意义。

3. 数据库控制者责任原则

与欧盟 95 指令相比，《一般数据保护条例》规定了巨额罚款，这种规定已经超出了对侵犯隐私权所产生的精神损害抚慰金的赔偿范围，并进而转向重视“侵权人获利”因素。迪特尔·施瓦布指出：“对于对一般人格权的严重侵害给予金钱赔偿，按照德国联邦最高法院的观点来说并不是抚慰金的‘原本意思’，而是一种‘法律救济’，用以防止对人的尊严和名誉的侵害得不到制裁及防止对人格的法律保护日渐萎缩。”[23] 这种考量特别重要，尤其是面对现行法律对数据主体的隐私权保护不力的情形。数据库控制者侵犯隐私权的表现往往是程度微小而数量巨大，数据主体寻求法律救济存在“集体行动难题”，大家都想搭便车，所以，除特殊情形外，对数据库控制者设置数额巨大的“罚款”无疑是一条“威慑”数据库控制者的可行道路。

没有制裁就没有法律，数据库开发与应用中的隐私权保护必须设置有力、可行且有效的责任条款。一方面，面对大数据时代的隐私权保护难题，仅将法律的重心放到“让人们自主决定是否、如何及经由谁来处理他们的信息”是远远不够的，因为人们的这种“自主”“自决”几乎只在“数据收集”及“初次使用”上有效，而现实情况是数据的价值很大程度上体现在数据挖掘等二次或三次应用上。“知情同意权”固然是隐私规范的核心准则，但并不能“包治百病”，舍恩伯格也说：“在大数据时代，我们需要设立一个不一样的隐私保护模式，这个模式应该更着重于数据使用者为其行为承担责任，而不是将重心放在收集数据之初取得个人同意上”[7]220。另一方面，将风险承担由民众转移到数据库控制者存在充分理由，因为对他们来说，不管是自行开发并自用的数据库，还是通过交易实现数据库价值的进一步放大，数据库控制者比任何人都明白如何利用它。就此而言，作为数据库价值挖掘的最大受益者，数据库控制者理应对自己的行为负责。具体说来，数据库控制者的责任涵盖了民事、行政、刑事三大责任。在民事责任方面，《侵权责任法》第 2 条第 2 款明文规定了隐私权，《最高人民法院关于审理旅游纠纷案件适用法律若干问题的规定》第 9 条对旅游者个人信息提供保护；在行政责任方面，《治安管理处罚法》将“偷窥、偷拍、窃听、散布他人隐私”认定为违法行为，《社会保险法》《统计法》《彩票管理条例》分别对主管行政部门、社会机构及其工作人员泄露个人信息的行为承担行政责任，造成损失的，还要承担国家赔偿责任；在刑事责任方面，《刑法修正案(七)》第 253 条新增了侵犯个人信息罪，包括“出售、非法提供公民个人信息罪”和“非法获取公民个人信息罪”。《居民身份证法》《护照法》规定对主管机构及其工作人员的侵犯个人信息行为承担行政责任外，构成犯罪的，也要依法追究刑事责任。

五、结　　语

从历史发展来看，隐私权与科技有着千丝万缕的联系，布兰代斯和沃伦首创隐私权的技术背景就是“快拍相机”的发明。一个有趣的现象是我们对待隐私权总是采取亡羊补牢的态度——在科技发展引发一定社会危害后果后才作出回应。数据库开发与应用中的隐私权问题就是如此，巨量的个人敏感数据被收集、存储和交易，现实和网络上的数据监控让人无所遁形，我们在享受科技发展带来的高效和便捷的同时，付出的却是隐私的代价。然而，我们“习惯”了大数据时代隐私数量的减少并不意味着它是正当的，隐私权之于人的尊严和人格完善的重要性时刻警醒我们，数据资源的开发和利用必须以尊重和保护公民隐私权为前提，否则，就是“手段”和“目的”的本末倒置了。

参考文献:

[1] 涂子沛. 大数据:正在到来的数据革命,以及它如何改变政府、商业与我们的生活[M]. 桂林:广西师范大学出版社, 2015.

[2] 齐爱民. 私法视野下的信息[M]. 重庆:重庆大学出版社, 2012:1-5.

[3] Pass C, Lowes B. Collins Dictionary of Economics[M]. 2nd. Glasgow: Harper Collins Publisher, 2002:325.

[4] 张民安. 信息性隐私权研究[M]. 广州:中山大学出版社, 2014.

[5] 罗斯科·庞德. 法理学:第三卷[M]. 廖德宇,译. 北京:法律出版社, 2008:45.

[6] 理查德·C. 托克音顿,阿丽塔·L. 艾伦. 美国隐私法:学说、判例与立法[M]. 冯建妹,石宏,郝倩,译. 北京:中国民主法制出版社, 2004:209.

[7] 维克托·迈尔-舍恩伯格,肯尼思·库克耶. 大数据时代:生活、工作与思维的大变革[M]. 盛杨燕,周涛,译. 杭州:浙江人民出版社, 2013.

[8] 萧文生. "一九八三年人口普查案"判决[C]// 西德联邦宪法法院裁判选集(一). 台北:"司法院"印行, 1991:288.

[9] 艾伯特·拉斯洛·巴拉巴西. 爆发:大数据时代预见未来的新思维[M]. 马慧,译. 北京:中国人民大学出版社, 2012:8.

[10] 张民安. 隐私权的比较研究[M]. 广州:中山大学出版社, 2013.

[11] 陈新民. 德国公法学基础理论:下[M]. 济南:山东人民出版社, 2001:358.

[12] 约翰·帕克. 全民监控:大数据时代的安全与隐私困境[M]. 关立深,译. 北京:金城出版社, 2015:43.

[13] 麦尔荀伯格. 大数据·隐私篇:数位时代,「删去」是必要的美德[M]. 林俊宏,译. 台北:远见天下文化出版股份有限公司, 2015:23.

[14] David L. The Electric Eye: The Rise of the Surveillance Society[M]. Minnesota: University of Minnesota Press, 1994:78.

[15] Jim S. What Makes People Click: Advertising on the Web [M]. Indianapolis: Macmillan Computer Publishing, 1997:225.

[16] Katrin S B. Privacy in Cyberspace: Constructing a Model of Privacy for the Electronic Communications Environment [J]. Rutgers Computer & Tech. Law Journal, 1998,24(1):50.

[17] Christopher K. 欧洲数据保护法——公司遵守与管制[M]. 2版. 旷野,杨会永,译. 北京:法律出版社, 2008.

[18] 张民安. 公开他人私人事务的隐私侵权[M]. 广州:中山大学出版社, 2012:479-480.

[19] 周丽娜. 大数据背景下的网络隐私法律保护:搜索引擎、社交媒体与被遗忘权[J]. 国际新闻界, 2015(8):145.

[20] 孔令杰. 个人资料隐私的法律保护[M]. 武汉:武汉大学出版社, 2009:213.

[21] 张新宝. 从隐私到个人信息:利益再衡量的理论与制度安排[J]. 中国法学, 2015(3):38-59.

[22] 王泽鉴. 人格权的具体化及其保护范围·隐私权篇(上)[J]. 比较法研究, 2008(6):1-21.

[23] 迪特尔·施瓦布. 民法导论[M]. 郑冲,译. 北京:法律出版社, 2006:262.

(责任编辑:王 薇)