大数据环境下精准诈骗治理难题的伦理反思

Ethical Reflections on the Governance of Precise Fraud in the Era of Big Data

陈高华 /CHEN Gaohua 蔡其胜 /CAI Qisheng

（大连理工大学哲学系，辽宁大连，116024）
(Department of Philosophy, Dalian University of Technology, Dalian, Liaoning, 116024)

摘 要：当代精准诈骗问题的多发和难以解决的特点，与大数据背景下客观环境的改变和个体防范意识的缺失息息相关。一方面，“数据化”带来了本体论层面的新假设，社会中个人身份的建构被还原为“数据挖掘”和“数据解释”的过程，这一过程固有的偶然性容易产生隐私泄露问题。另一方面，大数据话语体系的加强导致了个体行为的被动态势，个人批判性思考能力的缺失，则进一步加深了个人在面对这一问题时的判断能力和反思意识不足。为了防范精准诈骗问题所带来的诸多危害，一方面，应当进一步完善数据和信息立法，重新确立组织对个人数据访问或挖掘的技术行为规范；另一方面，应当反思社会教育中自我意识和价值观培养，增强个体行为和反思能力的适应性。惟有综合技术防范和社会教育两方面的考察和研究，才能为防范精准诈骗寻求一种有效治理。

关键词：大数据 电信诈骗 信息哲学 隐私伦理

Abstract: The phenomenon of precise fraud is closely related to the change of objective environment and individual behavior in the background of big data. On the one hand, big data brings a new assumption on the ontological of the world. As a kind of "information body", matter has evolved into a direct composition of data and its related relationship. In the process of forming personally identifiable information, the "contingency" inherent in the two processes of "data mining" and "data interpretation" easily lead to privacy problems, which is then exploited by "precise fraud". On the other hand, big data also has a direct impact on the changes of personal privacy concepts and behavioral judgments, leading to the lack of self-awareness of individuals and raising ethical risks. In the discourse system of big data, we must re-examine the connotation of contemporary information privacy, establish the organization's specifications for accessing and mining personal data and timely adjust individual self-behavior and privacy concepts. Only by taking these measures will we be able to seek a possible effective prevention for the privacy issues revealed by "precise fraud".

Key Words: Big data; Telecommunications fraud; Information philosophy; Privacy ethics

中图分类号：N0 **文献标识码：**A DOI: 10.15994/j.1000–0763.2018.11.004

“诈骗”作为当下社会关注的热点并不是这个时代所特有的现象，只是随着大数据技术的兴起并被不法分子所利用，诈骗形式和手段发生了重大改变，这一现象才显得尤为突出。“精准诈骗”是“通过深入利用用户个人信息实施的诈骗”，[1] 有别于以往的“盲骗”，其最大特征是掌握了受害者的有效信息，并依此编造契合目标对象的诈骗剧本，往往成功率高且令人难以防范。山东临沂女孩徐玉玉被骗身亡事件是精准诈骗中的典型案件，该案于2017年9月15日二审裁定，其中作另

基金项目：国家社科基金重大委托项目/马克思主义理论研究和建设工程重大项目“社会主义核心价值观研究”（项目编号：2015MZD011）。
收稿日期：2018年3月7日
作者简介：陈高华（1980–）男，江西永新人，大连理工大学人文学部哲学系副教授，研究方向为国外马克思主义思潮、技术伦理。Email: cghdlut@126.com
蔡其胜（1989–）男，湖北黄冈人，大连理工大学人文学部哲学系博士生研究生，研究方向为科技伦理。Email: caiqisheng@126.com.

案处理的涉嫌倒卖个人信息的“黑客案”则于同年9月7日一审判决生效。[①]在这一事件中，“数据”无疑发挥了重要的作用，它存在于黑客窃取和转卖个人信息、诈骗团伙设计并分工实施诈骗等诸多环节。然而，“诈骗”并不是大数据技术的“原罪”，透过两起案件中暴露的大数据公开与共享中的一系列隐私问题，我们仍可以体会到对大数据技术进行伦理探究的紧迫性。本文以大数据时代信息本体结构变化为出发点，从“数据挖掘”和“数据解释”两个环节对的精准诈骗现象中产生隐私问题的客观原因予以探究，并站在个体主观层面上加以反思，将有助于回应大数据背景下这一现象所面临的伦理挑战。

一、数据本体化假设与信息结构变革

当代信息哲学中关于“信息”概念的解释存在着诸多视角，以一种“从物质世界自身显示自身的层面上，以及信息与物质在存在方式的根本区别的尺度上”来看，信息是“标志间接存在的哲学范畴，它是物质（直接存在）存在方式和状态的自身显现”。[2]在这种解释下，物体被认为是“物质体”和“信息体”的双重存在，信息无处、无时不在，甚至有些已被人类认识，有些有待被认识。而数据是信息的一种表征方式，信息可以通过不同介质、不同渠道来传递，数据则是“通过声音、语言、体态、符号、文字、信号、图形、视频反映的认识论信息”，所以“数据是信息的子集，或更准确地说是认识论信息的子集。”[3]以此可见，信息内涵的范围是远大于数据的。

随着大数据时代的来临，上述信息与数据之间的关系已悄然发生改变，大数据不仅意味人类技术的革新，还带来了世界本体论层面的全新假设。在历史上，从古希腊哲学家毕达哥拉斯开始，人类就尝试以“数”来表征世界并赋予其本体论层次的意义，但“数”的本体论地位真正得以突破则发生于当代信息革命之中。带来这一改变的是“数据化”，美国科学家舍恩伯格把“数据化”视为人类认识论的一个根本性转变，所谓“数据化”，即“一种把现象转变为可制表分析的量化形式的过程”，[4]其核心是“量化一切”，如此以来，世界上各种实体的特征及其属性开始通过数据来加以界定，数据作为一种计算机语言，也逐步取代了信息的其他不同表征方式。进而，信息的呈现开始依赖于对数据的读取，数据化也进一步确证了人类关于物质作为一种“信息体”存在的认识，“我们不会再将世界看作是一连串我们认为或是自然或是社会现象的事件，我们会意识到本质上世界是由信息构成的。”（[4]，p.96）有学者指出这是一种信息领域的“重新本体化”，它使得人们对于事物的描述已“从客观世界迁移到信息自身”，在数据的话语权下，人类生活的世界是一种由数据组成的世界，“客观世界和信息之间区分已不再是逻辑上的差别，只是抽象层次的不同。”[5]

数据虽然参与信息的组建，却并不等同于信息本身。在信息哲学视野中，信息的本质在于物质自身显现，它是间接标志着物质存在的概念，因此信息是一种具有指向性的概念，事物传递出来的信息也应该是具体的、对象化的。但是，作为信息构成因素的数据最初却只是计算机符号语言，它并无指向性，换句话说，数据只是一种客观化和具体化的元素，是一堆“离散型”的存在。通常情况下，计算机处理数据的“第一步需要将不断变化的实时事件转换为离散型的机器可读的数据”，这一过程往往不是由人类完成的，而是由计算机完成的，在此意义上，不仅自然科学中世界结构正经历着由“原子”到“比特”的转换，数据本身也意味着世界被还原成了一堆“没有意义的比特”。[6]

因此，在数据没有被加工成人类所需要的信息之前，数据并不能传递出对象化的信息，那么我们就需要从众多“离散型”数据中识别有效数据并予以整合。面对大数据的海量性特点，人类在技术上有许多方法可以实现对数据的分析和整合，但是更值得反思的是，这一整合过程何以可能？实际上，分析数据并不需要一种预先设定好的模式，而只需基于一种不断衍生和修正“智能假设”，机器其实是在反复地“假设”中建立数据之间的联系并验证其效用，这些模式都是“新的假设，是通过被用于在数据集中寻找结构的计算

①杜天禹“黑客案”于2017年8月24日宣判，同年9月7日判决生效，详细宣判经过参考2017年9月9日《法制日报》第8版《“徐玉玉案”黑客一审判决生效》一文，记者徐鹏。

技术来发现的”。（[6]，pp.371–390）然而，这种假设性活动之所以成立，乃源于数据间“相关关系”的存在。有学者认为，人类处理大数据的认识和实践活动可以称作一种“创构性”活动，数据作为信息的构成因素，在尚未进入相互作用过程之前，“表现为具有某种结果指向的因素和因素之间的关系——大数据所最具价值的相关关系之一。正是这种相关关系，给创构特定的结果留下了广阔的实践操作空间。”[7]

综上所述，在大数据时代，数据与信息之间的“描述与被描述”关系已发生变化，数据由一种表征符号演变为信息本体的构建因素，世界作为“信息体”也被视为由数据及其相关关系直接构成，从而能够被人类予以清晰地掌握。数据本体地位的提升，使得数据、信息和个体身份建构之间的关系在大数据话语体系下重新定义，人类信息隐私也必然在这一新的话语体系下重新思考。

二、客观信息建构过程中的隐私困境

经数据和信息的概念对比可知，数据本身只是客观化、离散化的存在，数据若要加工成为信息，还需要有效的识别和整合。信息本体结构的变化揭示出了两个不同的步骤——“数据挖掘和聚合的过程”和“数据的解释与翻译，即信息的输出过程”，在这两个过程中，“计算机的自主运算实际上隐藏着一种‘双重偶然性’的可能，并且随着数据的不断增长，这些偶然性将永远无法完全排除”。[8]这是在大数据话语体系下建构信息所面临的固有的推断性难题，并且随着数据的迅速增长而愈发难以消除，两种“偶然性”的存在正是“精准诈骗”得以利用的地方，进而导致这一现象层出不穷。

徐玉玉事件中第一个关键性案件便是“黑客”案，以社会大众视角来看，“黑客”是徐玉玉被骗的始作俑者。报道显示，犯罪嫌疑人杜天禹作为一名程序技术员，业余时间经常浏览一些网站并测试其“安全性”，一旦发现漏洞便利用木马侵入内部，打包下载个人信息、账号、密码。徐玉玉的个人信息正是来自于“山东省2016高考网上报名信息系统”的“战利品”，最终杜天禹以“侵犯公民个人信息”一案作为独立案件单独移送并起诉。① “黑客”暴露出的漏洞问题，一方面，意味着隐私保护在技术层上尚有亟待加强的地方；另一方面，还提示出“数据挖掘和聚合的过程”中的一种推断性难题。

上文提及，有别于过往的一种“描述性”活动，大数据时代的人类实践作为“创构性”的活动，它“更多是根据人的需要及其发展创设满足和开发人的需要的感性对象”，所以“创构活动的主要特征是创设从未存在的可感对象。”[9]因此，人类挖掘数据的活动，其实是在基于一种以第三人视角加以“假设”建立起来的相关性。以往的描述活动依赖于因果关系，搜集数据时考虑的往往是如何尽可能真实、精确地反映目标对象；而大数据时代的数据挖掘活动则不再拘泥于精确性，为了要“比以前更容易、更快捷、更清楚地分析事物”，数据间联系的建立只考虑“通过识别有用的关联物来帮助我们分析一个现象，而不是通过揭示其内部的运作机制”。（[4]，p.53）因此，数据挖掘的服务目的是以满足主观需要的使用效益为主的，面向的也只是未来可能的结果，从而这一活动是广泛的、宽泛的，其内部蕴含着诸多的可能性。

正是源于这种创构性，大数据具有规模上的“整全性”，“大数据的‘大’不仅意味着数据量大，而且意味着维度全。”[9]所以，被黑客窃取的关于徐玉玉的资料，它们的价值不在于数据本身，其用途也不局限于信息来源网站上的高考报名这一目的，关键在于，这些数据在未来的某时、某地，经由某种“偶然性”，可以聚合为个人身份信息而被诈骗分子所利用，这才是应提高警惕的地方。因此，“黑客案”给予我们的警示不仅是如何从技术上防范数据被窃取，更为要紧的是组织如何确保有效地挖掘数据，以防未来产生不必要的隐私问题。

另一起与徐玉玉事件直接相关的是电信诈骗案。诈骗分子冒充教育局的人，谎称向徐玉玉发放助学金，在拨打了“教育局”提供的“财政局”电话后，徐玉玉按照对方以“激活账户”的指令，将预备的9900元学费打入了骗子提供的账号。侦

①“徐玉玉”案详细案情及侦办历程参考2017年6月28日《检察日报》第2版《公诉人详解徐玉玉被电信诈骗致死案办案历程》一文，记者徐日丹。

案过程显示，这起诈骗案并非只针对徐玉玉一人，在侦案中被检察机关查实认定的被骗考生多达20余人，其中绝大部分是山东籍考生，这一切均始于诈骗分子购买了被黑客所窃取的山东省高考学生信息。可见徐玉玉所接到的电话只是诈骗分子拨通的数百通电话之一，嫌疑人通过数据“读取”徐玉玉的信息实施精准诈骗，只是不断地、反复地校验数据的适应性，并没有对徐玉玉的身份背景加以确认,它反映出内在于“数据的解释与翻译”过程中的信息推断的另一困境。

这种诈骗模式揭示出大数据时代“数据解释”的方法发生了重大转变。在以往，若要证实一则信息是否真实，必须充分考虑到其背景载体，也就是需要将信息放置于具体的环境当中，在个人的境况中予以检验。但是，信息本体结构的改变带来了人类对信息认知的改变，大数据时代隐私问题产生的关键并不在于“相关软件‘有我们的数据’，而是互联网机器将如何‘读取’我们。它们‘读取’我们‘是对还是错’都不无关紧要，换句话说，如果机器将情境定义为真实的，那么其后果便是真实的。”[6]并且，机器“读取”我们的结论还往往是正确的。发生于2016年的大麦网“撞库”事件也充分地说明这一点，它曾导致该网站大量用户的个人信息被窃取并用于诈骗。所谓“撞库”，即黑客“通过搜集网络上已经泄露的用户账号信息，使用技术手段前往其他网站通过软件自动尝试登录，利用部分互联网用户在不同网站使用相同账号密码的习惯，筛选出可供登录的用户账号。”（[1]，pp. 26–29）这充分表明，在大数据背景下，信息的效用与机器以何种方式去翻译数据相关，不再去考虑目标对象的真实境况，只需要对数据的适应性进行反复地检验和调整即可。

因此，信息推断的这种困境意味着人类对信息认知的改变，令人担忧的不仅是“一些原本不危害个人隐私的数据，通过数据挖掘也能关联出个人隐私”,更在于计算机对数据“解释”的话语权，它并不在人类的控制范围之内，从而导致数据被二次甚至多次利用，“主体失去了数据的所有权，即失去了控制关于自身信息的权利，从而造成隐私伦理问题。”[10]诈骗分子只需不断地调整数据之间相互作用可能生成的结果，并在此间进行选择，“通过引导这种因素关系，使它们以特定的方式进入特定的相互作用，从而得到所想得到的特定结果。”（[7]，pp.22–42）这种改变造成了受害者在信息面前的被动地位，在精准诈骗中，受害者往往失去了原本该有的辨识和反思意识，从而导致诈骗屡屡得手。

三、主体批判性思维缺失的伦理风险

在大数据的话语体系下，人类的生活充斥着海量的数据存储。作为当下正在发展的信息文明的基础，可以说，到了大数据时代才有了人类信息文明的真正奠基，甚至说，“没有大数据，人就不可能成为信息文明意义上‘一切社会关系的总和’。”[9]大数据带来的绝不仅仅是信息本体建构的改变，它还深刻地影响了我们的行为习惯和思维方式，这是“数据化”中信息隐私之所以产生伦理问题的关键所在。近年来，“精准诈骗”现象之所以屡打不止，不仅与数据挖掘和共享过程中暴露的隐私漏洞相关，还显示出个体行为判断和反思能力的缺失,这令我们不得不认真地反思,“我们到底还是不是自主的人？到底是技术决定我们还是我们决定技术？”“如果我们完全由大数据技术来决定我们的生存方式，那么我们的人格尊严就无从谈起，因为我们已被技术异化了。”[11]

一方面，大数据的“预测”能力直接影响到人们的行为判断。首先，大数据技术核心就在于“预测”，“它是把数学算法运用到海量的数据上来预测事情发生的可能性。”（[4]，p.11）在实际操作中，这个过程主要依赖于计算机的分析来完成，它导致了在一种凭数据说话的环境中，人们不需要也很难将自己的理性判断置于机器的预测行为之中。比如，商家基于客户的消费数据，设计出适合于客户的个性服务，这一服务进而影响着顾客的消费行为，我们有理由怀疑此时消费者的行为到底是基于自身的实际需求，还是基于数据的分析。这是一个全新难题，一般情形下我们会根据对方的行动来考虑自己将会采取的行动，然而，在大数据时代这种交往模式却发生了变化。大数据带来了一种存在于人与数据“预测”之间的不对称行为，人们无法去了解计算机会于何时、何地，以何种方式来描述自己，甚至也很难对这种预测行为产生质疑。由此可知人的行为在大数据面前实际上是被动的，个体容易在行动上沉迷于这种

转变。进而，随着数据技术的完全普及，当这一共享模式普遍地被人们所接受时，个人的信息隐私观念底线会日益降低，隐私伦理问题更加凸出。更为重要的是，大数据时代中的“个体的选择权显得微不足道，某些人虽然具有明确的隐私意识，但常常默认数据被组织搜集”。（[10]，pp. 44–48）

另一方面，大数据带来了人类反思意识的缺失，当人们开始“沉沦”于大数据带来的一切改变，个体的反思意识也会随着这种变化而逐步丧失。首先，认识论上的“量化一切”是数据化的必然结果，人们以“量化”考察万物，这种考察模式不仅发生在自然界，还蔓延到了人文领域，“通过大数据，人类及其社会也想自然界一样，能够被全面数据化和计量化，实现人文社会科学的量化工作。”[12]除此之外，个人身份也交由大数据刻画，“个人的身份乃至行动以数据的形式在数据平台呈现，导致个体在社会中表征成各种数据的集合”，如此一来，“不是主体想把自身塑造成什么样的人，而是客观的数据来显示主体是什么样的人”。（[10]，pp. 44–48）至此，大数据已成为一种万能的“社会之镜”，人们开始习惯于听从数据所“告诉”我们的一切，也接受了数据刻画我们的身份。

在更深远的意义上，人类在大数据面前所处的被动态势也将随着数据的日益扩大而变得越来越明显。对于计算机而言，随着技术系统接收到的数据越来越多，它们可以开始自己改善自己，“可以聪明到自动搜索最好的信号和模式”，甚至未来“许多现在单纯依靠人类判断力的领域都会被计算机系统所改变甚至取代。”（[4]，p.12）当人们开始被这种智能化所支配，反思能力的丧失将使得人类彻底失去自由。因此，作为大数据时代标识个人身份的数据对于隐私显得尤为关键，它使得隐私问题存在着诸多的可能。

四、精准诈骗中的隐私问题及其伦理回应

大数据技术的发展标志着一场重大革命的到来，它带来了前所未有的商业价值，改变了人们的生活方式，并进一步影响着人们思维方式的变革。当今社会，电信诈骗由“盲骗”发展为“精准诈骗”，大数据似乎成为了这一现象转变的“利器”，究其原因，一方面，源于海量的数据不可避免的被挖掘和共享，信息建构过程中又存在固有的“双重偶然性”，从而引发了一系列的隐私问题；另一方面，也源于个体隐私观和行为能力的改变，它意味着普通民众对数据的一种应变能力的缺失。总的来说，是人们对刚刚兴起的大数据革命的反思不足，遭到了诈骗分子所利用，才造成这一现象屡打不绝。当然，解决大数据的隐私伦理问题并不成于一朝一夕，带着上述的反思，作为一种对前文叙述的数据“本体化”趋势及其造成的信息本体结构变化的回应，首先，我们有必要重新定义个体信息的隐私概念；其次，重新确立各类组织对个人数据的访问或挖掘行为的规范；最后，作为目标对象的个人，还应适时调整自我的行为及隐私观念。

1. 个人信息隐私内涵的重新定义

有人际互动关系发生的地方，必定会产生隐私概念。一般来说，个人隐私有着三种不同的形式：躯体隐私、空间隐私和信息隐私，并且随着现代社会中个人数据使用的不断增长，人们对信息隐私的关注日益增加。有学者指出，个人信息可包括：“（1）固有特征。这个人来自何处？他或她是谁？出生日期、性别、国籍等；（2）获得性特征。这个人的历史，例如地址、医疗记录和购物史；（3）个人偏好。这个人喜欢什么？包括兴趣、业余爱好、喜欢的品牌和电视节目等。”[13]这些信息十分丰富，我们可以通过它们去轻易地辨识一个社会中有身份的人，然而以历史的角度来看，隐私一词的涵义是不断变化的，大数据时代信息隐私的内涵应不限于此。

黑客窃取的徐玉玉的个人信息，虽然都可以视为她的不同身份标识，但是当这些信息显示在计算机电子表格当中时却是一些聚合在一起的个人数据，它们本身所能揭示的个人信息量其实是有限的。既然大数据技术是人类的一种“创构性”的活动，那么它绝对“不是根据预先设定的具体目的由抽样形成的干枯数据标本，而是动态反映事物相互作用过程的数据流。”[9]所以，在大数据主导的话语体系下，个人的身份不是一种静态的、固定的赋予，而是动态的、流变的，随着信息构建中的“偶然性”变化而不断改变的。也就是说，山东省高考报名系统确认的徐玉玉信息，应当被看成是动态的一种暂时身份，其个人隐私所涵盖的内容已超出了系统搜集的数据和认可的身份。

目前，计算机隐私保护技术主要针对于“静态数据集”，但是“数据总是动态变化的，包括数据模式，属性变化和新数据的增加”，“在这种复杂的情况下实施有效的隐私保护是一个挑战。”[14]所以，人们首先得转变自我的隐私观念，好比将“数字革命”理解为“信息基础的重新本体化一样”，隐私的内涵也亟需给予新的意义，新的解释必须考虑到大数据背景下人作为一种“信息社会的代理人”，在本质上具有信息特质，即“将每个人视为由他的信息构成，并以此将对个人信息隐私的侵犯理解为对个人人身侵犯的一种形式”。（[5]，pp.185–200）

2. 确立前期数据访问和挖掘的伦理守则

这个时代，数据的应用规模呈“指数级”增长，给动态数据监控和安全防护带来巨大挑战。前文“数据挖掘和聚合”过程的分析已指出，其中存在着固有的推断难题，这一难题深藏于大数据之“大”中，“大”不仅意味着数量之大与维度之全，还意味着数据在未来随时可有某些“偶然性”建构成有用的信息。更为紧要的是，这种偶然性又具有不可消除性，它是由数据挖掘的先在预设所决定的。根据以往的经验，“预先设定”决定着挖掘的精度，要获取精确的数据，必须详尽地确定目标和方案，然而，大数据之所以维度全，是因为“大数据的获取只有最基本因而也是最少的在先设定”，它不需要样本取样般的具体、精确，“在先预设越基本从而越少，数据相应维度就越全。”[9]面对这种“求大、求全”的特点，若个人数据再未得到有效的保护的话，则不可避免的会产生诸多的隐私伦理问题。因此，数据挖掘是隐私问题产生的基础性一环，在实践中发展挖掘技术的同时还应该较好地顾及到可能产生的伦理问题。

“与传统的安全方法不同，大数据的安全性应表现在如何处理数据挖掘而不暴露用户的敏感信息。”（[14]，pp.1–19）对于如何谨慎地处理个人数据的访问或支配，从技术的角度来看，“数字信息通讯技术（ICTs）”等专业技能，可以在数据挖掘过程中通过“加密化、匿名化、密码编程、防火墙、设计协议及服务，以及在外部盗用数据的情况下的警告系统等各种防御形式来提升私人数据的保护性能。”（[8]，pp.33–36）虽然，这些方法可以为信息隐私提供技术支持，但站在行为主体角度的层面，如何加强组织在数据挖掘过程中的自律更为紧要。笔者认为，在大数据时代相关约束性法律尚不完善的时候，组织在访问和搜集个人数据时应做好换位思考，给予用户在数据挖掘整个过程的知情权。比如在数据访问前，向目标对象明确地告知需要收集的数据，以及未来适用的范围；在数据处理过程中，向用户明示数据处理的过程，并且切实做好数据技术保护工作；在处理后，对相应的使用情况亦予以告知，即使发生了伦理纠纷，也应当积极地配合用户采取适时措施。这些相应的伦理守则的确立，可以为技术支持提供保障，从源头上做好个人数据访问和控制过程中的隐私保护。

3. 个体行为判断和反思能力的培养

在“精准诈骗”中，既然个人身份信息的泄露和被利用是产生隐私问题的重要原因，那么，培养个人的信息权利意识、调整自我的隐私观念，对隐私问题的预防和解决显得尤为重要。一般意义上，即使在大数据话语体系下，人们还是可以通过一种“刻意”的行为来绕开大数据对我们的“预测”活动，譬如，在某些需要搜集个人数据的地方，我们可以谨慎地对待是否留下真实信息。但是，这类做法只是一种粗略、防守式的做法，不太可能顾及到生活中的方方面面，我们也不太可能为了逃避大数据的预测而刻意地隐瞒自己的真实想法，弄不好它还有可能为我们带来其他的问题。因而，“大数据时代信息隐私所引发的个体自由问题并非能通过一种简单的‘撤离’或‘退守’方式就可以彻底解决。”（[8]，pp.33–36）

其实，“通过数据来测度信息，是信息表征和测度的一种普适方法。”（[12]，pp.90–94）在“万物皆数”境况下，信息隐私的核心问题不在于我们如何去逃避数据化，或去规避大数据的预测行为，而在于如何去提高我们在数据共享过程中的认知和辨识能力。目前，个人在数据面前尚处在弱势地位，如前文所述，大数据已经带来了个体身份的数据化，个人也应调整自我的隐私观念使之与时代相适应，并进而寻找保护隐私的方式。很多时候，个人信息实在一种无意识的状态下被侵犯的，因此提高这种“意识”能力，有助于从源头上加强个人信息的保护。除此之外，个人也应加强信息共享过程中的主动性，有意识地去了解和跟踪数据的使用目的和方式，对于个人信息滥用所造成的后果应予以积极主动的维权。

五、结　语

综上所述，当今社会“精准诈骗”现象的多发，表面上来看似乎是以往诈骗现象的延续和翻新，实质上则是大数据时代数据本体化对当代信息结构的动摇与冲击。“信息”是间接地标志作为物质的世界的存在，当信息本体发生变化之后，人们的行为、观念就应当做出适当的调整和适应。大数据时代的隐私界限远远超出了以往时代的内涵，它是动态变化的，并对现代社会伦理反思提出了新的要求。从这个意义上来说，惟有对大数据时代的隐私权利予以充分的理解和保护的基础之上，制定新的伦理与规范，“精准诈骗”所揭示的隐私问题方能得到有效的保护。

［参 考 文 献］

[1] 靖力. 从盲骗到“精准”诈骗 [J]. 方圆, 2016,（10）: 26–29.

[2] 邬焜. 中国信息哲学核心理论的五种范式 [J]. 自然辩证法研究, 2011,（11）: 48–53.

[3] 叶继元、陈铭、谢欢、华薇娜. 数据与信息之间逻辑关系的探讨——兼及DIKW概念链模式 [J]. 中国图书馆学报, 2017,（5）: 34–43.

[4] Mayer-Schönberger, V., Cukier, K. *Big Data: A Revolution That Will Transform How We Live, Work, and Think* [M]. New York: Houghton Mifflin Harcourt, 2013, 96.

[5] Floridi, L. 'The Ontological Interpretation of Informational Privacy'[J]. *Ethics & Information Technology*, 2005, (4): 185–200.

[6] Hildebrandt, M. 'Who Needs Stories if You Can Get the Data? ISPs in the Era of Big Number Crunching'[J]. *Philosophy & Technology*, 2011, (24): 371–390.

[7] 王天思. 大数据中的因果关系及其哲学内涵 [J]. 中国社会科学, 2016,（5）: 22–42.

[8] 张铁瑶、田海平. 大数据时代信息隐私面临的伦理挑战 [J]. 自然辩证法研究, 2017,（6）: 32–36.

[9] 王天恩. 从信息文明基础层次研究大数据 [N]. 中国社会科学报, 2017–09–26（2）.

[10] 薛孚、陈红兵. 大数据隐私伦理问题探究 [J]. 自然辩证法研究, 2015,（2）: 44–48.

[11] 陈仕威、黄欣荣. 大数据时代隐私保护的伦理治理 [J]. 学术界, 2016,（1）: 85–95.

[12] 黄欣荣. 大数据的本体假设及其客观本质 [J]. 科学技术哲学研究, 2016,（4）: 90–94.

[13] 邱仁宗、黄雯、翟晓梅. 大数据技术的伦理问题 [J]. 科学与社会, 2014,（3）: 36–48.

[14] Ji, C. Q., Li, Y., Qiu, W. M., Jin,Y. W. 'Big Data Processing: Big Challenge and Opportunities'[J]. J*ournal of Interconnection Networks*, 2013 (13):1–19.

［责任编辑　李斌　赵超］