CCID 赛迪智库 译丛

2017 年 8 月 14 日　　第 31 期　　总第 316 期

大数据伦理

【译者按】电子信息技术和服务的快速发展带来数据的海量收集和处理，给现行法律和社会管理模式带来新的挑战。欧洲经济和社会委员会于 2017 年 3 月发布《大数据伦理——在欧盟政策背景下，实现大数据的经济利益与道德伦理之间的综合平衡》报告，对大数据伦理进行了总体概括，并对与大数据相关的道德伦理问题进行了详细的总结。在此基础之上，报告重点讨论并融合各方面的见解，为平衡欧洲经济增长与大数据应用下个人隐私权的保护，提出了保护基本人权的五项制衡措施。赛迪智库政策法规研究所对该报告进行了编译，期望对我国相关部门有所帮助。

【关键词】 大数据　伦理　隐私权　制衡措施

一、法律框架

（一）引言

人们普遍认为，大数据的应用代表着欧洲经济的一个重大进步。然而，它也带来了重大的法律问题，尤其是数据保护相关问题。有一些社会机构报告认为，欧盟基于 n46/95/EC 指令的现有法律框架和基于《个人数据保护通则》的法律框架，已经为公民基本权利提供了充分保护。但数据保护的新边界不仅涉及个人数据，还涵盖各种数据。除能够确定某特定自然人的数据外，人们还能借助数据识别某个群体而非个体的特定行为、消费方式及健康状况等信息。

大数据的收集和汇总不适用于数据保护条例。最初，隐私权规则的制定是为了保护私生活不受侵犯，并避免因信息收集带来的歧视。目前，大数据的定量分析和结构化信息可以形成新的洞察力，从而能够造成商业歧视和群体歧视。随着群体变小（按地理位置、年龄、性别等因素划分群体），更容易引发歧视问题。

因此，在法律框架下有必要重新思考保护公民的全新方式，即使理论上现有法律适用于各种新情况，但已经无法提供适当和全面的保障。

（二）大数据、个人数据和匿名数据的定义

大数据：欧洲法规并未提供明确的大数据定义。根据欧洲数据保护工作组 3/2013 的观点（第 29 条款组），大数据的概念如下:

“大数据是指，由于可获取和利用的信息大幅增加，而使得企业、政府和其他大型组织控制的海量数字数据，对其可利用算法进行全面分析。大数据可以用来判断一定的未来发展趋势与相互关系，也可以直接用来影响个人。”然而，即使该定义具有一定实用性，但其关注重点是数据的体量，并未将个人数据的再利用及其二次价值纳入考虑因素。

个人数据：第 2016/679 号条例（第 4 条第一段）将个人数据定义为“与特定或可识别自然人相关的任何信息；尤其是能通过名字、身份证号、定位数据、在线标识或特定的一个或多个该自然人的物理、生理、遗传、心理、经济、文化和社会身份等信息，可以直接或间接识别的自然人，就称为可识别的自然人”。此类数据可以是姓名、住址、性别、职业、出生日期、电话号码、电子邮件地址、城镇、国家、车牌号、用户名和密码等。在个人数据中，有一个特殊类别是敏感数据，它受特定法律规则的约束，包括有关民族或种族、政治和哲学观点、宗教信仰、性行为及其偏好和健康数据等个人信息。

匿名数据：匿名信息不受欧盟法规约束，但根据一般数据保护条例第 26 条规定，“数据保护的原则应适用于任何一个特定或可识别自然人的相关信息。经过匿名处理的个人数据，如通过使用附加信息就能确定某个可识别的自然人，此类信息仍归为可识别自然人的相关信息。判断一个自然人是否可被识别，应考虑所有可行方法和客观因素，如识别成本和所需时间，同时还应考虑在进行识别之时技术的可行性及技术发展情况。因此，匿名信息，即与特定或可识别自然人无关的信息，或以匿名方式提供的无法识别主体的个人数据，不适用于数据保护原则。

此外，根据第 4、5 条规定，“‘匿名化’是指对个人数据匿名的处理方式，在未使用附加信息的情况下不能确定数据的主体，前提是附加信息被分开存储，并采取了技术和管理措施以确保个人数据不具有特定自然人或可识别自然人的属性”。这其中关键的一点是，个人数据一旦经过匿名处理后，在未经数据主体任何事先授权的情况下，可对该数据进行任意处理。但其至少存在以下两种课重新识别数据主体的可能性：第一，应用去匿名化技术追溯原始个人数据；第二，通过多种或特定数据组识别特定自然人或某个特定群体。

二、伦理问题

（一）意识

当人们注册在线服务时，数字身份（如脸书与谷歌账号）的创建或使用往往会得到迅速处理，但在此过程中，人们往往不会留意这类信息。由于用户愈加频繁地使用数字身份访问第三方服务，上述问题就愈发凸显。虽然数字身份使在线资源的利用更为简单快捷，但同时也造成了身份提供者和所使用服务之间数据共享的不透明。如果人们认识到，数字身份提供者除用户在订阅时提交的细节外，还能收集用户登录浏览时生成的数据，那么这个问题就更值得关注，因为这些数据极为详尽且事关个人隐秘。

由于人们丧失了必要的知情权，即哪些个人数据正被收集，以及如何处理这些被收集的个人数据，这种使用大数据的方式削弱了个人权利与自由。

（二）控制

相关文献早已指出，“面对相关数据，个人或会感到无力把控。这是因为人与数据之间的关系存在不对等性，而数据控制方面的不对等性似乎更为突出”。用户经常面对这样的情况：当用户决定要把他们提供给某个服务商的部分或全部数据删除时，即便服务商听从了用户的请求并确实删除了相关数据，对已出售给

其他公司或已进行了大量处理的用户数据却不会造成影响，从而导致用户丧失对个人数据访问权的掌控。

（三）信任

在当今大数据背景下，信任成为一个复杂的话题，因为它与广义的一般隐私权和意识问题具有千丝万缕的联系。迄今为止，人们更多的从严格的技术层面应对信任问题，这也是该问题的一大突出特征。人们还没有透彻了解如何在计算机环境下建立人际信任关系，因此，在物联网等环境下，创建一个有助于建立人机信任关系的硬件和软件架构，仍有待时日。

即使在线服务略微改善了人际互动（如在线健康咨询）,信任问题依然是基础，决定了用户对提供个人资料的接受程度。在交换私人信息之前，患者需要知道机器背后操控者的情况。

（四）所有权

围绕原始数据集被处理后生成的用户数据，还存在着一个更为复杂的所有权问题：它们究竟属于用户，还是属于从事数据分析的公司抑或原始数据的收集者？

这一问题的解决办法是限制数据的物理存储空间，即服务器的所在国。欧盟的做法是，逐步限制欧盟公民的数据被存储在“欧洲云”之外的地方。这种方法仍然无法解决已被处理的数据应存储在何处的问题，且在落实为具体法律与政策之前，无法解决理

论上如何定义数据所有权的道德难题。

（五）监视与安全

由于数据源的增加和技术进步，分析数据以生成有价值的信息这一过程变得更加便捷。在许多情况下，利用某种方式，定位某人的位置已变得不足为奇。利用无处不在的闭路监控，加之移动设备内置的 GPS 定位功能，以及信用卡和储蓄卡进行的付款和取款操作，都能成为追踪某人位置的手段。

监视贯穿整个社会，且没有方向性，在社会的各个层级，包括层级内部，监视无处不在。监视可以自上而下，也可以自下而上。这些特征形成了不同的监管类别：严格监管（自上而下的监视，例如雇主对雇员的监视）；监督（自下而上的监视，例如公民监督政府）；互相监督（平行监督，例如脸书用户查看彼此的简介和状态更新）；自我监督（自我纪录每个行动）。

（六）数字身份

创建数字身份具有明显的好处，它可以使访问在线内容与其所有相关服务成为可能。数字身份的广泛应用为获取个人在线公开信息提供了丰富数据（例如查询求职申请者），使人们在实际见到某人之前就能对其有所了解。

虽然上述过程在一定范围内具有合法性，但由于是基于数据而非某人本身对自己的评价，因此很有可能造成歧视。这就是人

们常说的“数据独裁”。即“我们不再根据某人的行为，而是基于数据所提示的某人可能的行为模式加以推断”。如此一来，数字身份分析的顺序就排在了个人互动之前。

（七）经过裁剪的真实性

每当人们使用搜索引擎通过关键字搜索、从在线商城购买某个商品或提交个人详细信息时，这些数据都可能被存储。在随后的网络访问中，人们利用数据处理及分析，就能在搜索页面上显示个性化结果，并向人们的电子邮箱发送营销信息，在社交网络与其他服务页面上推送广告，从而为用户带来一种更加个性化却更狭窄的在线体验（即所谓的“泡沫过滤”）。

这种极端个性化的好处之一是用户仅需点击几次鼠标，就找到他们所需的内容。然而，如若长期缺乏对不同产品、视角，甚至于思想的接触，可能会破坏在共享政治与社会生活中所必须的参照点，从而对创造力和宽容态度的形成构成强大的阻碍。

（八）去匿名化

近来，随着现代计算机计算能力的增强，去匿名化技术得到应用。传统的匿名化技术侧重于数据，主要通过删除(或替换)特殊的可识别信息(例如税控码、医保号码)使数据条目失去指定性。虽然这一方法非常奏效，但无法解决由各种资源(例如投票清单和社交网络概况)组成的数据集所生成的强大信息。一旦获得这种信

息，即使是完全匿名的信息，例如出生日期，再辅之以居住城市和婚姻状况等信息，某种程度上就能大致确定某个个体。

（九）数字鸿沟

数字鸿沟是指借助新技术（如互联网）获得各种服务时遭遇的困难，以及由于不熟悉新技术导致的对其工作原理的理解困难。在求职的时候，目前招聘信息主要在网上发布，因此年龄较大的人员可能会因不熟悉这一处理方式，导致找工作困难。鉴于当前就业市场的高度流动性，这可能会给很多人造成影响。

在老年人群中还可能发生另一种类似情况:在失去伴侣之后，他们通过在线交友服务寻找新的伴侣，但这种新的社会互动方式，很可能令他们感到沮丧，而最终导致他们选择放弃与逃避。

（十）隐私权

隐私权是指人们拥有的个人信息非经许可，他人不得使用的权利。隐私权是一个包罗万象的主题，上述讨论的各种问题都会对公民的隐私权造成某种影响，其重要性超过上述讨论的各种问题及其伦理意义。

虽然有观点认为，公民或愿意放弃部分隐私权以换取更大的人身安全和安全保障，但却无法确保所有人都有此愿望。此外，把隐私权当作交换筹码这一行为本身在某种程度上就有违道德。

当人们谈论隐私权时，往往会涉及信任问题。尤其在医疗领

域，病人及其行为细节异常重要，所以病人和数据收集者(如医生和医务人员)之间的信任关系关乎病人的利益。与先前的讨论不同的是，在此情况下，拒绝披露所要求的全部信息会被认为是不道德的，因为这会直接影响该病人的健康状况，并间接阻碍在此领域的研究进展，进而给他人造成影响。

从这一点看来，依据个人判断决定隐私权的使用似乎是明智之举，但因人而异的原则运用却不是明智之举，因为这给人们对原则的解读留下过多空间。而建立有序的社会，需要大家共同遵守清晰的指导原则。

三、平衡措施及有效平衡的局面

为平衡欧洲经济增长与大数据应用下个人隐私权的保护，现提出五项平衡措施。

（一）平衡措施 1——欧盟隐私权管理平台

1、概述

《一般数据保护条例》指出“自然人应有权掌控其个人数据”，第一项平衡措施即源于这一理念。此外，最新条令 679/2016 强调指出，在参与方激增及实际技术复杂性使数据的主体难于认识和理解个人数据是否与该自然人相关、以及如何在运用透明度原则的前提下使该自然人应用与其相关的个人数据。因此，直接赋予

公民控制其个人数据和虚拟身份信息的权力和有效手段，显得至关重要。

初步设想是建立泛欧门户网站作为欧洲唯一的隐私权管理中心，欧洲公民可自愿注册并登陆其个人页面，浏览已经获得和当前存储、处理、共享及再利用其个人数据的所有公私实体列表。每个企业、服务供应商、公共机构等，在该平台可以看到:

- 各实体所收集个人数据的种类（如姓名、出生日期、购买的商品、信用卡号码），而非实际数据;
- 该实体如何管理个人数据及欧盟法律，特别是《一般数据保护条例》的遵守情况;
- 实体提供哪些服务以交换何种数据，哪些服务当前有效;
- 相关数据是否与第三方共享;
- 个人数据自动化处理流程背后的逻辑，以及当上述处理流程进行数据分析时获得的结果;
- 如何撤销授权并请求删除数据和/或停用服务的信息;
- 数据管理人员和数据保护专员的身份验证。

由于人们通常不熟悉如何在网络或移动环境下管理隐私权设置，该平台可以轻松找到退出某些特定服务的页面，用户由此即可拒绝授权该实体处理其个人数据。理想情况下，平台还可帮助用户了解，若其决定撤销授权将会产生哪些后果。

将所收集的数据与提供的服务加以对比，有助于了解该公司是否遵循了数据最小化原则。该原则规定所收集的个人数据必须适当、相关且仅限于与处理该数据的目的密切相关的必要数据。

从需要个人数据的实体的角度看，有两种方式：一个是强制注册；另一个是企业和机构自愿选择是否分享所请求的信息。

2、优点

该措施是将数字通信中的个人数据处理的直接控制权归还给数据所有人，因此，这是强化意识和授权情况知情权的一项强有力的措施。而且，该系统也有助于解决数字服务用户对平时扩散数据缺乏留意的状况。该平台还将为人们行使访问权、为人们请求纠正或删除其个人数据提供支持。

在此情况下，各实体具有是否对其所收集和处理的个人数据实行强制性注册并向所有用户提供相关信息这两种情况。在以上两种情况下，尤其是不强制各实体进行注册的情况下，加入该平台的企业和实体将赢得更高声誉和信任。

一旦企业具备了数据政策和个人数据管理体系，用户即可直接核查该企业对个人数据的处理方式，并因此与该企业建立基于透明和信任的新型关系。

3、风险及缓解措施

最明显的风险是各企业不订购该数据管理门户，可通过上节所述的强制性措施加以解决。由于平台只显示所收集数据的类型（而非实际数据；例如门户网站将显示“生日数据”，而非具体生日信息如“1984 年 8 月 18 日”），因此目前尚未出现安全问题加剧的迹象。

另一个潜在的风险是，各企业提供信息的积极性较低，因为公开信息对企业没有直接利益。因此可建立一个由指定的欧盟专家管理的控制系统，用以发布各种违规举报，确保各企业通过门户网站传达的信息与提供服务期间所收集的实际数据的一致性。

（二）平衡措施 2——伦理数据管理协议

1、概述

第二项平衡措施的目标与第一项类似，即增加透明度，使人们了解公、私大数据拥有者对于欧盟法律的遵守程度。但该措施并非由用户直接采取的行动，而更类似于企业、机构或任何其他出于商业、科学研究或其他原因拥有和处理大量（个人）数据的主体的自觉行为。

初步设想是设计一个可靠的欧洲认证体系，在数据保护领域进行各种企业认证。欧盟立法委员在《一般数据保护条例》（第 42 条）中大致论述了该项措施，研究小组已与各相关方进行了讨

论，以了解该项措施的适用范围。

自愿认证须基于《一般数据保护条例》的主要原则，特别是以下原则：数据最小化；特别谨慎对待敏感数据和健康数据；尊重被遗忘的权利；数据可移植性；数据保护成为默认和规定状态。

为建立一个适用于各类企业及其所提供服务的通用体系，按照数据最小化原则确定质量标准，进行专门的“行业研究”，确定支持各项服务所需的数据类型，同时明确要求临时存储于企业服务器数据的时间跨度（数据保留延迟）以及预先规定的用途。

换言之，该设想有必要进行行业研究，以阐明如何在过程中运用欧盟标准和原则。可由国际标准化组织按照新的欧盟法规进行标准的设计。

2、优点

从客户的角度看，经过个人数据伦理管理的标准化程序认证后所获得的标识是该企业值得信赖的保证。

而私营企业想积极获得个人数据管理认证的原因是：首先，这是展示企业从事商业活动中，对法律和公民权利的尊重。第二，企业可将隐私权和数据保护作为一项资产，从而推动企业其他经济目标的完成。最直接的受益是此举可提升公司的声誉，对本企业与客户及其他企业之间的关系均有积极作用。此外，认证对于企业而言也是作为一种手段，用来定期检查其对欧盟法规的遵守

情况。

3、风险及缓解措施

主要风险是各企业对该认证的参与度不高。将该项认证作为某些特定欧洲或国家投标项目的强制性标准可作为一种激励手段，改善上述状况。申请认证的企业通常重视认证过程而非最终结果，针对这一问题，应制定严格的认证流程标准，以防止认证工作流于形式。

（三）平衡措施 3——数据管理声明

1、概述

第三项平衡措施建立在自愿的基础上。这一设想的出发点在于，当今社会，企业的成功越来越仰仗于企业股东、客户、员工和公众的信任。为增强各利益方的信心，一些企业或愿意声明将如何收集、利用和销售商业活动中获得的个人数据。

该项措施旨在创建一份“数据管理声明”，包含以下内容：采用政策；所收集数据的定性描述；未来用途。企业应定期在“数据管理声明”中阐述其所采用的政策（包括一次性和永久性政策）、以及为确保数据安全和隐私权控制而采取的具体措施。

本项平衡措施旨在防止、降低或评估下列问题：过度的数据收集；用户隐私权面临的风险；第三方对数据有害/不道德的运用；安全漏洞。自愿采取这一措施的企业可为各种数据管理措施提供

依据，从而提升用户的信任和隐私保护意识。

相关声明应包含企业在执行或为使相关措施保持有效性时所遇到的法律、技术、基础设施等方面的具体困难，以及根据欧盟政策提出的建议或意见。企业还应说明将收集哪类数据、如何收集、根据哪些类型的个人信息进行收集、从什么来源获取上述数据以及收集频率。

另一个重要内容是数据的处理策略，例如数据聚合级别，或在数据处理之前/之后其数据集是否会汇入其他数据集。在这种情况下，必须明确说明次级数据源。此外，必须明确说明从服务器中删除数据的准确时间范围，并对使用加密和匿名化技术的情况作明确说明。

为鼓励企业采用程序化方案，该声明模型还应包括专门针对伦理数据管理框架进行持续改进的设计内容，并为未来数据应用提供依据。这将为用户和企业提供一个机会，以评估数年来企业所取得的进步。评估重点涵盖上述各项内容，并就如何改进每项指标进行定量评估。

为确保不同主体的声明以及在伦理方面各方的表现具有可比性，相关声明应遵守一定的指导方针。为此，可以根据不同的相关方、参与方和欧洲层级的管理机构之间的讨论，制定一个标准。

2、优点

从民众的角度看，该措施的主要好处是提高了个人数据的使用、存储和处理的透明度，进而加深对上述问题了解。另一方面，如能认真遵守相关规定，作为一种营销手段，企业也可以借此提升声誉。

3、风险及缓解措施

此类声明的主要风险是影响力有限，在某种意义上，该措施可能由于声明本身的传播范围有限而无法真正改善客户对企业的信任度。为避免这种情况，声明标准应包括将此文件发布至企业网站的内容，通过电子邮件发送给注册客户，并可在企业各信息点打印相关信息。

（四）平衡措施 4——欧洲健康电子数据库

1、概述

本项措施包括创建包含欧盟公民医疗相关数据的欧洲数据库。当欧盟公民在公立医院或接受政府补贴的私立医疗机构接受治疗时，院方会就其将个人数据收录并存储于由欧盟管理的数据库一事征得患者同意。该授权还包括授权院方，可使用病人治疗相关的数据。数据的收集与传送应遵守标准交换协议，如在欧洲层级事先制定的健康水平等类似领域的标准。医疗数据在科研领域的应用，按照欧盟法规 679/2016 规定，个人有权决定其个人数

据仅用于某些特定领域的研究工作。

科学家和研究机构必须向管理该数据库的欧盟机构提交申请才能使用数据库。申请必须包含有关科学家和研究小组、其所服务的机构等具体细节信息，以便进行身份核查。申请书必须说明申请使用某数据的研究项目（或该研究项目申请书）及其资助机构，附加需求信息的详细清单、各领域数据的申请理由和预期结果。该申请由欧盟管理机构进行评估，决定是否授予数据访问权限，数据将以适当匿名的方式提供，并粗化到足以实施该研究的细化水平。

欧洲公民个人可使用其法定数字身份信息（例如，意大利公共数字身份认证系统）通过门户网站访问数据库，浏览、下载、管理和变更有关其个人医疗数据的使用授权信息。

一般公众有权访问可以浏览和下载公开数据的门户网站。在此公开的数据必须匿名且其粗化程度必须足以防止数据去匿名化处理和危及隐私权。通过门户网站本身和网络服务进行数据下载的授权，以此鼓励公众使用此类数据，核查数据的使用情况。

鉴于未来某些信息可以免费获得，医疗公开数据将在公民个人、公民协会和决策者、企业和日常决策流程中得到普遍应用。可以预见，基于医疗公开数据的服务有望得到大力发展。

2、优点

健康电子数据管理系统最重要的益处总结如下:

- 欧盟公民对个人医疗健康数据将拥有更大的掌控权。
- 欧盟公民将更加了解与自己有关的医疗数据在什么时间、以何种方式被收集，这些数据以何种方式、在哪里、以及由谁进行储存和应用。
- 透明度的提高将增加人们对医疗健康服务与研究的信任。
- 该系统还将丰富欧洲公民的数字身份信息，同时欧盟鼓励使用数字身份信息。

此外，随着医疗费用的降低，人们的生活品质得到改善。借助公开数据，人们还能了解各医疗机构的表现，更清楚地了解各医院的优势领域，从而在保健方面做出明智决策。

3、风险及缓解措施

欧盟数据库面临的主要风险包括安全性和可能的数据泄露。具体说来，一旦数据库中的信息遭到泄露，就可能出现非法监视公民个人习惯，以及出于非法目的将个人健康数据出售给一些企业，譬如保险公司等，从而干涉自由市场。上述问题通常通过数据加密（使泄露的数据无法使用）、用联合数据库代替物理中央数据库，以及防止包含数据的服务器过于集中等手段加以解决。

在科学研究方面一个潜在风险是，科学家一旦被授权拥有某

个人的健康数据，即有可能永久保存在其电脑中。为防止此类数据被非法使用或超出其最初指定用途，应设计一套机制，使科学家对授权数据的正确使用和存储负责，一旦发生违法事件，法律责任由该科学家承担。

（五）平衡措施 5——大数据的数字化教育

1、概述

此项措施旨在普及欧洲数字文化，尤其是使公众更加了解大数据，以及大数据对欧盟公民一生的影响。为不断提升这一意识，人们设想了针对不同年龄段人群的各种教育计划，通过义务教育和选修课程的方式加以实施。

在采取这一平衡措施之后，还应采用以下提案:

- 小学、初中和高中数字课程的主要内容是介绍大数据，具体包括什么是大数据、如何收集、大数据的各种风险、如何避免过度泄漏个人信息，以及数字身份的利与弊。
- 大学学位教育以培养数据科学家和相关专业人才为主，通过一系列伦理学选修/必修课程，创建和使用大数据的伦理学方法。
- 由欧盟赞助、针对全体民众开放的在线课程（MOOC）为欧盟公民了解大数据提供了必要工具，有助于发展更全面的数字教育。该课程根据人们对大数据的不同需求水平，采用多样化和模块化设计，以适应不同类型学习者的当前知识水平。

- 在每个城市举办面对面专题研讨会。按照各年龄段学习者，特别是中老年人的具体需求，量身打造各种专题，内容包括如何建立账户和与朋友及家人（例如 IP 电话服务）进行交流，如何使用网络银行、电子医疗服务，以及如何接受福利系统服务。

2、优点

全面了解“大数据”有助于公民主动利用由此衍生的各种机遇。具体而言，欧盟公民将:

- 有意识地使用互联网（和物联网），避免因个人数据泄漏导致的麻烦。
- 进一步了解大数据与所提供服务之间错综复杂的关系，从而接受如下观念，即为获得各种服务，人们必须牺牲一些个人数据，以增加人们对新技术的信任度。
- 接受过伦理培训的数据科学家将认识到，从中长期看，基于伦理原则处理个人数据有助于减少隐私泄露。
- 使中老年人和无法全面享受网络服务的人士具备数字化技能，有助于失业者有效地找到工作，以及如何利用在线社会福利的服务。

3、风险及缓解措施

面对面研讨会和课程面临的主要风险之一，是无法充分利用财政资源，这意味着有些受到资助的教育项目可能并不会为目标

人群数字知识的提升、或更全面的信息通信技术的学习和使用带来实际改善。为防止出现这一局面，资金支持的教育项目应仅限于具备互联网连接基础设施的城市。

译自：*The ethics of Big Data: Balancing economic benefits and ethical questions of Big Data in the EU policy context, March 2017 by European Economic and Social Committee*

赛迪智库
面向政府 服务决策

研究，还是研究
才使我们见微知著

信息化研究中心	工业化研究中心	规划研究所
电子信息产业研究所	工业经济研究所	产业政策研究所
软件产业研究所	工业科技研究所	军民结合研究所
网络空间研究所	装备工业研究所	中小企业研究所
无线电管理研究所	消费品工业研究所	政策法规研究所
互联网研究所	原材料工业研究所	世界工业研究所
集成电路研究所	工业节能与环保研究所	安全产业研究所

编 辑 部：赛迪工业和信息化研究院
通讯地址：北京市海淀区万寿路27号院8号楼12层
邮政编码：100846
联 系 人：刘 颖　董 凯
联系电话：010-68200552 13701304215
　　010-68207922 18701325686
传　　真：0086-10-68209616
网　　址：www.ccidwise.com
电子邮件：liuying@ccidthinktank.com

报：部领导

送：部机关各司局，各地方工业和信息化主管部门，
相关部门及研究单位，相关行业协会

编 辑 部：工业和信息化部赛迪研究院

通讯地址：北京市海淀区紫竹院路 66 号赛迪大厦 15 层国际合作处

邮政编码：100048

联 系 人：韩宇雪

联系电话：（010）88559543　18610215602

传　　真：（010）88558833

网　　址：www.ccidgroup.com

电子邮件：hanyx@ccidgroup.com