

关于中国互联网金融健康发展的建议

黄奇帆

摘要：互联网、物联网、大数据、云计算、人工智能、移动通讯等现代信息技术正在深刻影响着经济领域，任何一个传统产业链与信息科技结合就会立即形成新的经济组织方式，从而对传统产业构成颠覆性的冲击。现代信息技术带给经济更高质量、效率、效益的同时，也给社会公众和社会管理带来大量超乎传统的风险。鉴于“三元悖论”无解但客观存在，也鉴于六大信息科技带给互联网金融超高的集合力和传染力，更鉴于金融行业特殊的安全诉求和发达国家的成熟经验，建议尽快采取措施以确保中国金融安全和健康发展。

关键词：互联网金融 风险管理 数据监管 政策建议

作者简介：黄奇帆，中国国际经济交流中心副理事长。

一、五大特征、颠覆传统

颠覆已经成为我们这个时代见怪不怪的经济现象。互联网、物联网、大数据、云计算、人工智能、移动通讯——六大现代信息技术的基础平台，正在极其深刻地影响着传统经济领域。可以说，任何一个传统产业链与这六大信息科技结合，就会立即形成新的经济组织方式，从而对传统产业构成颠覆性的冲击。

为什么六大现代信息技术会有如此强大的颠覆性？研究表明，六大现代信息技术实际存在“五全特征”：全时空、全流程、全场景、全解析和全价值。所谓“全时空”是指：打破时间和空间障碍，从天到地、从地上到水下、从国内到国际可以瞬间连成一体，信息每天24小时不停地流动。所谓“全流程”是指：关系到人类所有生产、生活流程的每一个点。所谓“全场景”是指：跨越行业界别，把人类所有行为场景全部打通。所谓“全

解析”是指：通过收集和分析人类所有行为信息，产生异于传统的全新认知、全新行为和全新价值。所谓“全价值”是指：打破单个价值体系的封闭性，穿透所有价值体系，并整合与创建出前所未有的、巨大的价值链。

恰因上述“五全特征”，六大现代信息科技的基础技术和应用技术产生强大的互动，正反馈循环，极致性地提升了互联网“对社会公众的聚合与整合”能力，极大地提升了社会公众个性化需求的识别能力，极大地提升了互联网功能业务线的派生能力，极大地提升了互联网商业价值和资本价值的增值能力。用一个不很准确的描述：六大现代信息科技可以把经济肌体上数以亿计价值极低的单体细胞群幻化为在某个领域具有极高价值的、差异化的功能干细胞；进一步，它可以把所有功能干细胞集合一体幻化为全能干细胞——具有超级价值的全息价值体系，从而成就了经济肌体的基因突变，大大增强了企业的经济预见性，大大增强了企业的经济质量、效率、效益。

正因为六大现代信息科技的上述特点，目前世界各国在此领域的竞争异常激烈，基础技术和应用场景日新月异，资本价值不断攀升。依据《中国互联网发展报告 2018》提供的数据，2017 年，以互联网为核心的我国数字经济规模已经高达 27 万亿元人民币，而截至 2018 年 6 月，我国网民数量超过 8 亿，普及率 57.7%；手机网民规模达 7.88 亿，占网民总数的 98.3%。尤其是六大现代信息科技的基础平台深度融合之后，互联网产业进一步爆发，对传统经济领域构成更加深刻的影响。可以说，任何一个传统产业链与这六大现代信息科技平台结合，就会立刻幻化出全新的经济或商业的组织模式，从根本上改变了传统经济、产业和企业的概念，并带来新的价值。这类事例几乎贯彻所有巨无霸式的互联网平台。比如，2018 年 10 月，某新型保险机构和支付宝合作开发了一款名曰“相互保”的互助保险产品，仅仅 42 天便聚集了 2000 万人参保，涉及金额近 40 亿元。为什么会有这样的效果？就是因为阿里巴巴电商平台所形成的巨大客户数据造就了支付宝庞大的客户群，而支付宝的庞大客户群又造就了更加细分的“相互保”市场，把全部业务线加总所形成的相互支撑、相互依托的业务集群和效益，又造就了阿里巴巴巨大的资本价值。再比如腾讯，以社交网络平台起家，跟随六大现代信息科技的不断进步聚集了庞大的用户数据群，而这样的数据群除传统广告价值外，并不存在超乎寻常的商业价值；但腾讯以此庞大数据为基础进行业务分化，分化出不同功能的业务线，从而产生新的产业链群和价值链群；各个功能业务线——产业链和价值链进一步形成彼此依托、相互促进的产业集群，不仅将为企业带来巨大的超额利润，同时也会带来传统思维方式难以企及的资本价值。最典型的例证就是：当互联网帝国开发了网络金融业务之后，金融打通和附能所有业务线，使得金融业务和所有互联网业务都产生更大的杠杆效应，并带来传统

方式之下难以想象的巨额商业价值和资本价值。

二、祸福相依、利弊相伴

利弊永远相伴相生。六大现代信息技术带给经济更高质量、效率、效益的同时，也给社会公众和社会管理带来大量超乎传统的风险。比如，巨额资本堆积使公众聚集速度、规模动辄数以千万计，与传统产业根本就不在一个数量级上。这使得互联网帝国一开始就“大到不能倒”，而且其所形成封闭独立的管理体系，很容易让资本意志绑架公众认知，从而对抗政府管理。再比如，中国消费者协会最近公布的数据显示，中国 100 款头部 App，有 91 款存在过度采集客户隐私信息的问题；2018 年 9—11 月，苹果手机使用者的支付宝账户就被大面积偷盗；而近年来互联网“黑客”门槛也越来越低，浙江网警 2018 年抓获一个只有初中文化的刑满释放犯，他仅自学五年电脑“黑客”知识，就成功侵入一家上市公司网站，窃取数据、阻断订单、勒索钱财，造成公司 1000 多万元损失。尽管此犯已经落网，却凸显我国互联网安全环境的脆弱性。

毫无疑问，我国在信息安全方面已经出台了一些法律法规，同时也在针对国家信息安全问题投入大量人力、物力、财力，但是否能在短期内从根本上解决问题？估计不行。这不是谁努力不努力的问题，而是六大现代信息技术基本特点所决定的，正所谓道高一尺、魔高一丈。尤其在必须保障数据安全的金融方面，其安全隐患更是：平时看不见，偶尔露峥嵘；一旦出风险，损失难数计。风险防不胜防是最为令人担心的问题。关键有两条：一是六大现代信息技术的发展速度过快，过去 10 年一代，现在可能 2~3 年一代，而新的应用技术更是层出不穷，高速迭代；二是互联网企业对客户体验感有着天然的极致性追求，这会导致大量“尚无法研判成熟程度的技术”被无条件地应用在金融业务方面。

我们不能仅仅看到六大现代信息技术带给传统金融业务方式的颠覆性进步，更应看到它对我国金融安全意识和信用意识会构成严重颠覆。截至 2018 年 6 月，我国通过互联网购买理财产品的网民数量已经高达 1.69 亿，同比增长 30.9%；使用互联网第三方支付系统的用户数量更是高达 5.69 亿。2017 年 12 月末，网民线下使用支付宝、微信等支付手段进行消费的人数比例是 65.5%，而半年之后的 2018 年 6 月末，人数比例则升至 68%。与此同时，中国民众尤其是青年人过度消费、超前消费蔚然成风，《2018 年第三季度支付体系运行总体情况》报告显示，透支消费所形成的逾期 6 个月以上的不良贷款已经高达 880 亿元，而 2010 年年底，这个数据仅为 76.86 亿元，8 年增长 10 倍。这显然是国民金融安全意识和信用意识日趋淡漠的结果。

还有，过去 5 年间，我国以 P2P 为代表的互联网金融爆炸式发展，2016 年巅峰之时数量近 5000 家；但 2017 年一年之间，就有 3000 多家不合格、不合规平台自行或被迫退出，并暴露出大量爆仓、跑路的骗子。涨潮迅猛、退潮急速，短短几年 P2P 已经处于高危状态，恶性循环不断扩展，2018 年上半年倒闭的 P2P 平台达 721 家，仅 7 月份新增问题和停业平台超过 100 家，大量人民群众落入 P2P 设下的庞氏骗局，使原本极其珍贵而稀缺的金融资源变成少数骗子的财富。目前，所谓网贷平台大约还有 5000 万用户，人均 2.27 万元投资，总规模超过 1 万亿元。另外，以互联网为通道的货币基金近年高速增长，2018 年 6 月总规模达到 8.7 万亿元，其负债与资产的严重错配已经构成巨大的流动性风险，也引起金融监管当局的强烈担忧。还有，互联网金融环境下，资金运转速度高出过去若干倍，这会不会影响货币政策有效性？这个问题至少值得研究。

三、下大决心、兴利除弊

从理论上说，六大现代信息科技在安全问题上存在“三元悖论”：安全、廉价、便捷三者不可能同时存在。但是，金融特质要求金融企业在安全问题上必须无限趋近于 100%。在此前提下，互联网金融必须在确保安全的前提下，在廉价和便捷之间寻找平衡。而目前情况看，互联网金融巨头推崇和炫耀的就是“极其便捷+极其廉价（免费使用就是极致廉价）”，并以此吸引公众使用。凭什么做到“极其便捷+极其廉价”？是不是牺牲了安全系数？其实，千奇百怪、防不胜防的安全风险出现在互联网金融领域，已经回答了上述问题。

当然，有一种解决方案被互联网金融公司采用：既保证便捷和安全，但通过其他方式支付高昂的成本。比如，互联网支付平台通过海量资本投入，超高速度聚拢客户人群，然后利用客户存入支付账户的保证金去搞投资，从而获利，覆盖便捷和安全必须支付的高成本。其一，这已经构成了典型的非法集资；其二，必须确保安全的客户保证金被暴露在投资风险和流动性风险之下。目前，中国央行已经发现问题，认为一些互联网金融平台并不关心金融服务质量，而更关心能够汇集多少客户保证金。于是出台法规，上收支付保证金至央行账户。尽管这样做可以防止互联网金融公司滥用客户支付的保证金，但又会带来新的问题：其一，导致货币政策操作“收长放短”，形成紧缩货币政策效应；其二，互联网金融公司无法平衡运营成本，要么降低安全标准，要么提高收费而保持便捷使用。调查发现，蚂蚁金服等垄断某一电商平台的互联网金融公司，正在利用垄断优势，不断拉长小微电商商家的“回款周期”，一来更长时间地无偿占有商家货款；二来逼迫电商商家增加周转性商业信贷数额，以此增加互联网金融公司的盈利水平。如此所为，

不仅导致电商商家经营更加艰难，同时也极易使商家背后的家庭落入金融陷阱。

鉴于“三元悖论”无解但客观存在，也鉴于六大信息科技带给互联网金融超高的集合力和传染力，更鉴于金融行业特殊的安全诉求和发达国家的成熟经验，建议尽快采取以下措施以确保中国金融安全和健康发展。

第一，稳妥而坚决地割除行业毒瘤，通过牌照管理将 P2P 等互联网金融公司数量压缩至 50 家以内，使之回归到实验或试点阶段。互联网金融本质就是金融，既然如此，互联网金融必须由银保监会实施统一的牌照管理和专业管理，这一点没有讨论的余地。现在，互联网金融交由各地政府金融办管理，这不可行，原因是技术能力和专业能力都无法满足要求。发达国家的 P2P 公司是在银行信用卡违约市场上成长起来的，其基础是个人征信体系极其完备，偶然违约者为寻求远低于银行信用卡罚息，通过 P2P 平台借入较低成本的资金归还银行信用卡。但中国 P2P 业务 100% 是假的，是 P2B 模式，属于个人群体针对小企业的借贷行为，极易发生两大问题：其一，按照现行法律法规，P 端只要超出 200 人，B 端则属非法集资，而中国 P2P 公司大量存在此类违规问题；其二，网贷公司根本没有能力向投资者提供真实有效的企业信息，大都依靠借新还旧不断滚大雪球以维系 B 端企业还款能力，投资者不仅不能分辨企业真实还款能力，而且极易落入庞氏骗局的陷阱。有人说，大数据、云计算等六大现代信息科技可以解决企业信用评估的问题，笔者认为不能。其一，真要利用六大现代信息科技解决信用评估问题，那将意味着巨大而无底洞式的科技投入，如此巨额成本，中国没有哪家 P2P 平台有能力支付，一旦支付则意味着永远亏损，因为六大信息科技更新换代非常快，而每次迭代都需要支付巨额成本；其二，六大现代信息科技只是从理论上说可以解决企业信用评估问题，但实际应用并未获得足够的历史数据支持；其三，小偷和警察都在使用同样的信息科技工具，只要警察的技术稍有漏洞或小偷的技术稍微超前，警察就不是小偷的对手。所以，互联网金融只能被控制在试点阶段，绝不能遍地开花。

第二，互联网金融公司必须“独立建构”，即实施有效的物理设备独立、数据信息独立、注册资本独立、法人资质独立、运营团队独立，绝不能继续容忍互联网金融公司与电商、娱乐等非金融平台混为一体、跨行业经营，更不能容忍跨行业经营所带来的数据交互使用。金融业务必须独立的根本原因在于：金融业务对数据安全性的要求完全与电商平台、娱乐平台不可同日而语，传统金融机构为了确保客户数据安全，100% 采用内网、外网绝对隔离制度，凭什么允许互联网金融公司低成本依托一般性、开放度很高的互联网平台开展金融业务？这既是金融安全问题，也是金融市场竞争公平性问题。另外，跨行业经营的模式下，非金融业务风险极易转化为金融风险。比如，因打假导致电商平台

上大量贩假商户破产，而这些商户拥有一定数量的贷款，也许规模不大，但因其对市场心理构成影响，结果导致较大金融风险及金融风险的快速传染。从国际经验看，一般性互联网平台公司绝不敢随意染指金融业务，美国的脸书、亚马逊、雅虎等平台公司都很大，股价市值同样可以达到数千亿、上万亿美元，但它们再大都不敢轻易染指金融业务。这里至少有四个因素：其一，成熟的商人懂得术业专攻，懂得长期坚守自己，不断创新自己才能使自己炉火纯青，获得足够的行业地位和进入门槛，才有可能获得超额利润；其二，一般性的互联网商品销售平台，其底层技术的安全等级无法满足金融要求，要满足金融业务要求，必须投入巨额成本，这往往得不偿失；其三，美国对金融公司有非常严格的监管要求，一般性互联网公司从事金融业务，一旦发生风险，公司根本承担不起动辄数十亿美元的巨额罚款；其四，鉴于所有业务点的风险都可能迅速转化为金融风险，而金融风险反过来又会拖垮所有非金融业务，所以成熟商人绝不愿去冒这么大的风险。

第三，政府必须建立商业机构数据分级管理制度，所有互联网公司都必须接受政府数据监管，而且政府必须确保数据信息从低级到高级单向流动。比如，一般性个人数据信息可以流入互联网金融公司，互联网金融公司数据可以流入政府金融监管机构、国家安全机构、税务审查机构、特许征信机构等。但绝不允许反向流动和交叉流动。另外，国家需要立法，保证政府拥有强制性信息采集权利，通过这一制度建立有效的“国民综合数据总库”，并以此为公共服务平台，针对特定对象（比如金融和征信企业）提供有序、有偿、有限、有效的数据服务，可以帮助互联网金融公司大幅降低企业或个人的征信成本，更好地发展普惠金融；还可以帮助中小微企业增强融资能力，降低融资成本；同时，这也是数据化时代政府管理适应发展的必然要求。

第四，客观上说，数据存在等级高低之分。两个层面：从数量层面，客户群体数量越大，数据级别和价值越高；从品质层面，对单一客户数据掌握的越全面，数据级别和价值越高。现代互联网业务发展已经呈现出一个明显特点：以巨大的资本实力，通过对社会公众个体给予小利，而急速将十几万、几十万甚至百万、千万人群汇聚在一起；同时，通过横向交易、交叉互助，迅速将支离破碎的低价值数据，拼接为更加全面的高级别、高价值数据。正因如此，政府的社会管理职能必须适应数据时代要求，构建确保数据有序而安全流动的制度体系。否则，任由数据随意交易、随意交互，势必导致资本实力雄厚的机构掌握最多、最全面、最有价值的的数据，从而形成最强大的社会影响力、最精准的资本利益索取，以及最大化的、为资本利益服务的公共平台。这不仅对国家信息安全构成严重威胁，同时还会达成“通过绑架公众而绑架政府”的目的，非常危险。此类事例并不少见，比如余额宝为代表的货币市场基金，用虚假宣传和蝇头小利诱惑社会

公众，立即形成上亿公众参与而使货币基金规模急速膨胀，从而形成大规模的金融空转，严重拉高社会金融成本，但就因为涉及公众利益，结果尾大不掉，绑架了金融监管。如果类似情况发生在数据控制方面，社会管理是否会出现国家信息安全被绑架的问题？还有共享单车项目，明显找不到盈利模式，但却获得巨额资本追逐。为什么？为了流量（流量=人群+数据）。资本要流量做什么？不知道。所以从现在起，一是政府必须以强有力的技术和行政手段，建立网络数据流动的交通法规，同时建立网路警察制度，绝不允许任何商业机构，以任何形式从事无序的数据交易、交互业务。二是所有数据只可以从低到高单向流动，而绝不允许反向流动或交叉流动。三是为有效地体现数据时代的政府公共管理职能，政府必须是国民最高级数据的拥有者，以及数据公共服务平台的建设者和提供者。四是只有政府提供有序、有偿、有限、有效的数据服务，中小微企业的融资成本才有可能大幅降低，这也是一个国家建立有效的、普惠性金融服务的基础设施。五是政府必须对互联网公司数据收集做出层级管理安排，需要对社会明确什么样的数据可以收集，什么样的数据不能收集，采集不同级别的数据应当接受不同层级的监管。也就是说，政府对网络社会实行差别化管理措施，商业机构涉及数据级别越高，政府管理要求越高。

第五，在数据时代，数据信息是一个国家最重要的资产和资源，也是国家最重要的安全领域之一，所以政府必须强化网络国界建设，任何商业机构都无权将中国数据信息对外国提供，更不允许以此从事商业经营，否则等于中国信息情报泄露。

第六，通过立法，坚决打破“互联网商业王国”的金融垄断。现在，互联网金融公司可以任意向外拓展业务，但绝不允许其他金融机构侵入自己的领地，这几乎就是一种“王国”性质的商业模式。阿里巴巴的蚂蚁金服可以对任何社会成员提供金融服务，但阿里内部所有业务的金融需求却只能由蚂蚁金服提供，京东如此，腾讯同样如此。这样的商业模式不仅限制了金融市场公平竞争，而且极易对“王国”内部的人群构成盘剥式的伤害。比如前文提到的例子，电商平台通过拉长回款周期，迫使商户借重内部唯一的金融机构提供资金周转，从而使内部金融机构获得巨额垄断收益，这实际是让全社会为其金融行为买单。有人说，传统企业不是也搞金融公司吗？这些金融公司不是也为企业集团内部提供金融服务吗？但不一样，关键问题有二：其一，传统大型企业所设金融公司依然属于传统金融企业，不存在排他性和对内垄断问题，自己为集团公司提供金融服务的同时，并不排斥其他金融机构为集团公司提供服务；其二，企业内部的服务对象数量很少，不构成强大的社会性，但“互联网商业王国”不一样，电商商户数量动辄数以千万计，涉及千万量级的家庭利益，其已经具有强大的社会属性，万一出现问题就很可能

演化为社会问题。所以，政府对于大型互联网商业平台公司的管理也必须打破传统，绝不能简单遵循一般性法人公司管理原则。也就是说，政府社会公共管理职能必须渗入这些大型平台公司，以《反垄断法》为准则，打破互联网“王国”的垄断，营造公平竞争环境，这是政府的基本职责之一。尤其是对互联网金融的管理，必须把它从“互联网商业王国”中剥离出来，变成一般性金融服务企业，让所有金融企业都能为同一互联网商业平台公司提供服务，这才是公平的市场竞争。实际上，在互联网电商平台大规模挤出传统商业企业之后，传统银行失去了大量零售商业客户，眼睁睁看着互联网电商平台公司利用技术优势、资本优势、法律优势，用“烧钱”的方式大搞金融垄断，属商业垄断；而法律又不允许传统银行自行投资互联网商业平台，这是极不公平的金融和商业环境。从国际情况看，没有任何一个国家的政府能够允许几家商业寡头控制 95% 的公共服务行业，也没有任何一个国家的政府允许互联网商业平台公司建立畸高的商业霸权地位，更没有允许其一出手就“大到不能倒”。所以，在六大信息科技突飞猛进、数据技术应用场景日新月异的情况下，政府必须从国家安全角度出发，突破传统管理禁区，将大型互联网商业平台公司视为社会的组成部分，并加以有效管理，塑造数据时代的公平市场。

第七，鉴于互联网商业平台公司的商业模式已经远远超出传统商业规模所能达成的社会影响力，所以，互联网商业平台公司与其说是在从事商业经营，不如说是在从事网络社会的经营和管理。正因如此，国家有必要通过立法，构建一种由网络安全、金融安全、社会安全、财政安全等相关部门参加的“互联网技术研发信息日常跟踪制度”。也就是说，政府在人民代表大会的法律授权之下，有权以恰当的技术和物理手段，跟踪观摩所有大型互联网商业平台公司技术研发的进展状况，而所有大型互联网商业平台公司也有义务接受政府技术的询问。在数据时代，政府要管好网络社会的公共事务，摆脱资本绑架社会公众所带来的管理被动，政府必须时时刻刻在技术上与商业机构保持同水准、同进度的研究状态。否则，在技术高速推进的前提下，监管将永远处于落后而被动状态。更重要的是，网络技术只要有微小的级差，就会导致人群效应和传播速度呈现出几何级数的变化。政府管理技术稍有迟疑或滞后，就很可能导致极其严重的社会风险。所以，政府及时掌握互联网商业技术进步的信息，提前介入风险控制点的发现和控制手段的研发，及时提示互联网商业公司必须注意的风险问题，对政府监管和互联网商业公司都是大好事。因为，公司可以据此强化新技术项目的完善，避免巨额成本投入之后突然被叫停的风险。当然，这样的做法或许会使互联网应用技术的进步速度略有减缓，但这是必要的，互联网应用技术本来门槛就不高，它们往往比拼的是资本实力，比拼的是瞬间垄断市场的能力。所以，这样的放缓反而有利于市场公平，有利于把社会风险降到最低，

至少降低到可控的程度。

第八，既然互联网商业平台公司的运营带有强大的社会性特征，出现错误就会穿透一切屏障急速传播，从而带来巨大的社会影响，甚至动荡，所以这类公司的商业行为必须充分担负起必要的社会责任。如果因为降低商业成本而疏于管理，导致数据信息倒买倒卖，或出现类似“滴滴司机强奸杀人的事件”，政府必须予以此类公司超乎寻常的重罚，要罚到它倾家荡产，甚至判罚出局，这样才能向全社会宣誓互联网商业公司的社会责任及其价值。其实，西方国家的社会文明都是严厉处罚之下的产物。据了解，美国对互联网企业的发展有着明确的法律约束，尽管各州有所差异，但涉及反垄断和信息安全方面的法律多达 52 部。

第九，网上安全认证技术，比如生物、二维码、虹膜、指纹、刷脸、声音等辨别认证技术必须“特许经营”，凡此类技术公司设立必须“先证后照”，必须有较高的进入门槛。认证识别系统属于重大国家安全范畴，但在未经长时间的安全检验的情况下就在互联网金融业务上大量运用，这明显违背了金融行业安全必须无限趋近于 100% 的要求。所以，目前互联网金融公司的支付、资金划转必须坚持小额原则，同时各类互联网认证识别技术，只能允许线下使用，而经过长时间的技术积累和试错之后，才能在国家技术管理部门授权之下，上线试点，逐步成熟，逐步推开。现在，互联网金融业务经常受到黑客攻击，这些攻击实际都是突破了网络认证系统。所以，如果网上传递识别信息，而没有较高的技术门槛做保障，任由谁都可以开发，而且以廉价和便捷为出发点而忽视安全水准，那伪造就不可避免，网络黑客也将大行其道。所以，所有互联网识别技术必须接受公安部门的技术监控。网络社会是虚拟社会还是真实社会？界限已经变得非常模糊了。但毋庸置疑，正因中国有近 14 亿的人口，而且主要发达地区人口密度很高，所以在数据时代，中国天然具有数据经济的比较优势，并以极快的速度跻身于互联网大国、网上消费大国，同时也是一个数据大国。互联网电商在人口密度较小的国家就会发展艰难，因为物流成本过高，但在人口密度很高的中国则是另一番景象。所以，从数据的规模和品质考量，中国优势明显，而且一定是未来中国经济、社会发展的一个重要比较优势。但与此同时，这一优势同样也是各国数据经营者、网络黑客和敌对势力都迫切希望掌控的巨额价值。所以，中国丝毫没有懈怠的理由，政府必须尽快认真、切实、有效地介入互联网数据管理、信息管理，刻不容缓地主动作为，这才有可能使政府摆脱对网络虚拟社会管理的被动性，并防患于未然，确保国家信息安全。

责任编辑：沈家文