

网络强国时代 领导干部要注重提高四种能力

□ 陆 峰

核心阅读

4月20日,习近平总书记在^①全国网络安全和信息化工作会议上的讲话中强调:各级领导干部特别是高级干部要主动适应信息化要求、强化互联网思维,不断提高对互联网规律的把握能力、对网络舆论的引导能力、对信息化发展的驾驭能力、对网络安全的保障能力。这四种能力是新时代领导干部顺应时代发展要求必须具备的素质。领导干部要注重提高这四种能力,在工作中转变工作思路、创新工作方法、开创工作新局面。

4月20日,全国网络安全和信息化工作会议在北京召开,习近平总书记在讲话中强调:各级领导干部特别是高级干部要主动适应信息化要求、强化互联网思维,不断提高对互联网规律的把握能力、对网络舆论的引导能力、对信息化发展的驾驭能力、对网络安全的保障能力。习近平总书记对各级领导干部提出的四种能力要求,是作为新时代领导干部顺应时代发展要求必备的素质能力,有助于各级领导干部在工作中转变工作思路、创新工作方法、开创工作新局面。

提高对互联网规律的把握能力

互联网正在深刻地影响人类发展历史,深入理解和紧紧把握互联网规律,已经成为各级领导干部适应网络强国时代的必备技能之一。一是提高互联网创新引领意识。互联网作为基

础性、战略性和先导性基础设施,已经成为技术创新、产品创新、服务创新、业态创新和管理创新等各类创新最为活跃的领域。要深刻领会互联网创新的引领作用,大力推动互联网和经济社会各领域的融合创新,把互联网作为培育经济发展新动能、促进治理体系和治理能力现代化、落实创新驱动发展战略的重要抓手。二是提高网络空间发展意识。网络空间已经成为人类活动的第二空间,与物理空间并驾齐驱,对物理空间技术流、资金流、人才流、物流等资源优化配置发挥着越来越重要的作用,是世界主要国家抢占未来发展主导权的必争之地。要积极推动网络空间发展,拓展网络经济发展新空间,完善网络空间运行规则,更好地提高对网络空间发展的驾驭能力。三是提高互联网普遍服务意识。互联网在推动均等化发展、缩小发展鸿沟、共享发展成果等方面正在发挥着无可替代的作用,已经成为世界各国提高发

展包容性的重要抓手之一。要持续扩大互联网基础设施覆盖面,提高网络速率,降低网络资费,为老百姓提供用得上、用得起、用得好的网络信息服务,让亿万人民在共享互联网发展成果方面有更多获得感。四是提高互联网风险管控意识。互联网互联互通,网络空间纷繁复杂,世界各国围绕网络空间的争夺日趋激烈,利益博弈日趋激烈,网上网下事件相互串烧,加上网络空间运行规则还在不断完善中,新事物引发的风险层出不穷。要加强对互联网事物的研判,提高对潜在风险的预测能力,及时做好风险防范和管控,提高对互联网的驾驭能力。

提高对网络舆论的引导能力

积极融入网络社会,主动开展网络调研和问政,已经成为各级领导

干部适应网络强国时代的必备技能之一。一是培育网络社会融入意识。网络社会打破了物理社会时空限制,在为人类交流、沟通、合作提供极大便利的同时,也成为当前创新社会治理的主战场。要积极拥抱网络社会,主动参与网络社会活动,摸清和把握网络社会发展规律,提高网络社会驾驭能力,为参与网络舆论引导提供经验支撑。二是善于应用网络开展调研和问政。网络调研和网络问政是新时代领导干部走群众路线的必备技能,有助于更好、更快、更全面、更深入地了解群众所思所想。要善于应用微博、微信、论坛等社交工具,开展网络调研和问政,了解群众所思所愿,收集好想法好建议,积极回应网民关切、解疑释惑。三是发挥网络舆论引导先锋作用。网络舆论对经济社会发展的影响越来越深入,加强网络舆论引导已经成为保发展、维稳定、促和谐的重要工作内容之一。要经常上网看看,潜潜

水、聊聊天、发发声,提高通过互联网组织群众、宣传群众、引导群众、服务群众的本领,善于为网络舆论做疏导。

提高对信息化发展的驾驭能力

信息化代表新的生产力和新的发展方向,已经成为引领创新、驱动转型、塑造优势的先导力量,加快推进信息化发展,已经成为各级领导干部适应网络强国时代的必备技能之一。一是提高信息科技发展把握意识。以互联网、大数据、人工智能为代表的信息科技已经成为通用目的技术,对产业转型、社会治理和国际竞争都产生了深远影响。要全面强化信息科技的前瞻意识,以时不我待、只争朝夕的精神加快推动信息领域核心技术突破,推进信息产业全面创新发展,紧抓产业体系建设,推动技术、产业、政策协同发力。二是提高信息化应用发展推进意识。信息化应用是信息科技服务经济社会的主要途径,大力推进信息化应用,有助于更好、更快地释放信息红利。要以推行电子政务、建设智慧城市、发展智能工业等为抓手,大力推进互联网、大数据、人工智能等信息技术在经济社会各领域的融合创新应用,以信息化应用来推动模式创新、管理提档和服务升级。三是提高信息化发展政策创新意识。信息技术的发展和普及应用对社会发展和治理带来了新的机遇和挑战,要加强对信息化发展的前瞻性研究,敏锐抓住信息化发展的历史机遇,及时调整和完善已有政策体系,让政策体系更好地护航信息化发展、促进信息红利加速释放。

边界与责任： 对 facebook 数据泄露事件的反思

□ 陈自富

今年3月中旬,美国《纽约时报》和英国《卫报》报道一家名为“剑桥分析”的公司,未经许可收集了超过5000万Facebook用户的信息资料,通过工具分析这些数据并给用户画像,用于在美国大选中推送精准的政治广告,从而影响美国选民在竞选中的投票。由于Facebook作为社交网络巨头的影响力,加上白宫前幕僚长班农曾担任剑桥分析公司的母公司董事,数据泄露事件中又有俄裔心理学家深度参与,使得这起“泄密门”事件在美国掀起了轩然大波。

Facebook事件暴露的对生态链中数据分享机制的监管缺位,目前来看已经是一个迫切需要着手考虑和采取行动的问题。

当代信息社会的一个核心特征就是基于计算机、智能手机、物联网等信息采集和加工设备的万物互联世界,这已经成为人类生活的基本背景,对人类行为数据的产生、采集和存储无所不在。

同时,互联网经济天生具有垄断和平台化、中心化的特点,用户从一开始,就在与互联网各大平台的博弈中天然处于下风。但这个观点只反映了硬币的一面:互联网提供的服务确实对人们有帮助;但硬币还有另一面:用户可以选择的互联网平台确实不多,而且平台对于数据和隐私的保护,并没有严格的道德约束和第三方监督机制,很多用户是“不得不”而不是“愿意”用隐私来交换便捷。

不可否认的是,无论是各国监管当局还是互联网企业在数据隐私问题上都在探讨如何更好地保护用户,但最终都囿于两个关键问题而很难达成广泛共识:监管部门担心过度

管制会使行业失去繁荣,新进入者大大减少,从而导致本国在全球经济竞争中错失良机,而互联网企业虽然想制定和遵循更广泛的行业自律性要求,但商业化却是推动互联网技术发展和应用的重要推手,面对公司市值降低和股东回报的压力,企业很难自觉自愿地设定和执行严格的用户隐私保护政策。类似于谷歌、Facebook、这样的中心化平台,其以广告为核心的商业模式是基于用户个人行为数据的精确分析和画像来提高广告转化率,在这种情况下,用户不让渡个人数据的若干权利给平台的话,企业很难获得商业资本投入来为用户提供便捷高效的服务。

看来似乎我们陷入了一种困境:商业化投入、技术进步带来的便捷和用户权利(如数据隐私权、知情权、选择权)之间相互制约,难以找到平衡点。

但事实并非如此,互联网社会并非是凭空产生的空中楼阁,它仍然与传统社会共享不少共同的主题,例如对边界与责任这两个主题的探讨将有助于推动解决隐私、便捷之间的二难困境。

在传统社会,隐私往往是个人与社会交往的边界,也是一种特殊的社会安排,即个人控制谁可以在物质和信息层面上与其接近,长期的生活历史经验告诉我们人类需要有一些隐私权比完全没有要好,但隐私权并不是生命权这样的绝对自然权利,在不同的社会文化场景中,并不存在绝对、抽象并至高无上的个人隐私权,这里的关键在于如何确定用户隐私数据的使用边界并让数据的托管者能按照这个边界条件来使用它。Facebook“泄密门”事件中,至少超越了两个重大的边界:个人数据被用于政治竞选的精准广告,Facebook的生态链中有

企业将个人用户数据用于影响政治选举结果,前者超越了用户设定的边界,后者超越了社会对企业数据应用场景设定的边界。

互联网的本质是连接及其产生的人和组织之间的关系,但其连接的场景和规模比传统社会要庞大得多,因此如何确定用户让渡个人数据的某些权利也比传统社会复杂,但这并不意味着传统的边界设定规则在互联网中并不适用,有些原则就在两种不同的社会背景都适用:为改进产品或服务水平,提高用户体验的个人数据运用,滴滴和Uber都需要用户的位置数据;为公共利益需要开放的个人数据,例政府提供的政务App中需要对用户身份进行实名认证,需要身份证和个人头像;针对特殊群体利益需要开放的个人数据,老年人专用手机中包括自动报警、定位、摄像头等特殊功能。

互联网的连接场景与传统社会相比是开放和动态的,因此某种程度上用户隐私边界的设定是一个与便捷、效率与信任相权衡的过程,用户多大程度上愿意让渡自己的一些隐私数据,这取决于数据使用者的责任及其履行,监管部门可能无法穷举各种场景来设定边界在哪里,但是却可以制定用户和互联网企业之间如何协商数据使用的原则,这些原则未必都以法律形式体现,但有效的伦理规范和原则只要有利于大多数利益相关者,那么对这些原则的执行则会自愿的,也就成为每一个参与方应履行的责任。因此在明确若干制定、协商原则之后,最重要的主题就是如何让各方

理解自己的责任并切实履行,如何让不尽责的企业受到商业伦理上的谴责并承担后果,这就是基于原则和承诺的责任主题。

在隐私和便捷问题上,有以下原则可以考虑:第一是“若非必要,切勿使用”,除上述的若干公认的情形,不必要的数据采集和运用都应禁止;第二是选择性加入优先,即在搜集用户数据时,应由用户来主动选择加入,而不是默认用户许可后让用户选择性退出;第三是“举证倒置”,即信息的收集方和使用方有责任定期公布数据使用情况,并接受第三方审计,以避免用户和企业之间的不对称地位导致的信息不对称;第四是“算法透明”原则,即企业应公开用户数据的具体加工方式和利弊,例如用户画像、智能推荐、动态定价等;第五是公正原则,即企业在运用算法加工数据并应用到各种场景中时,应遵循传统社会中的公平正义,不得因用户身份或行为数据导致歧视、伤害和损失。

按照以上原则对互联网企业的责任要求,应作为涉及隐私、信任和效率之间权衡的基石,当企业违反这些伦理规范时,需要监管部门、股东、媒体、用户共同监督,促使企业切实履行,Facebook的数据泄露事件也提醒了我们,互联网作为新的虚拟社会形态有一定的特殊性,但在商业伦理上仍应共享传统社会中一些共同的价值观。

随着信息技术的快速发展,基础设施领域对计算机网络的依赖程度日渐提高,关键信息基础设施已经成为关键基础设施的重要组成部分。面向公众提供网络信息服务或支撑能源、通信、金融等重要行业运行的关键信息基础设施一旦发生数据泄露、遭到破坏或丧失功能,将严重危害国家安全与社会公共利益。

伴着信息化与工业化的相互渗透和融合,智能化控制产品被广泛应用于关键基础设施领域。关键基础设施越来越依赖于网络信息系统,在实现智能控制的同时也增加了脆弱性,由此也带来了严重的信息安全威胁隐患。目前全球已查获的恶意代码样本早已超过60亿种,对关键核心基础设施的网络安全防范水平提出了更高要求。这都要求我们必须凝神聚力筑牢关键信息基础设施的“安全防火墙”。

关键信息基础设施安全保护是网络与信息安全的基础性工作,更是事关国家安全和国防军队建设重大问题,这就尤其要求我们打好基础设施信息安全保护的“组合拳”。

尽快制定和完善相关法律法规,为保障基础设施信息安全提供法律后盾。一些国家将信息活动纳入法律框架,通过立法确保信息安全已经是较为普遍的手段。我们应向欧美等在关键基础设施信息安全保护领域处于领先水平的国家看齐,加大关键信息基础设施保护投入,尽快从国家层面上完善相关顶层设计、制定战略性文件和法律条文,为我国进一步保护基础设施信息安全、打击非法网络攻击和网络犯罪行为提供充足的法律依据。

加大研究投入和技术升级力度,为保障基础设施信息安全提供技术武器。网络时代的信息安全具有典型的高技术特性,近年来一些国家一直持续加大网络信息技术投入,不断升级相关技术标准。美国一直致力于牢牢掌握互联网顶尖技术来维持自身的网络霸主地位,英国、德国、俄罗斯等国一直注重关键信息基础设施的网络安全强化。我们不仅要抓紧对关键领域信息基础设施的网络设备和技术进行全面升级,更要加快推动基础设施核心产品“自主可控”进程,逐步实现关键信息基础设施的国产化水平。同时,我们还要加强对相关领域人员的指导与培训,抓紧培养能适应当前

提高对网络安全的保障能力

网络安全问题和社会问题相互交织,其复杂程度已经超越了技术本身,成为影响经济社会发展的全局性问题,主动防范和化解新技术应用带来的潜在风险,加强网络空间治理,提升网络安全保障能力,已经成为各级领导干部适应网络强国时代的必备技能之一。一是提高网络安全警惕意识。随着互联网、物联网向经济社会各领域的深度渗透,传统网络安全已经蔓延到了经济社会各个领域,未来网络安全问题可能无处不在,网络安全引发的问题将不仅仅是断网本身,在推进信息技术普及应用过程中,要把网络安全保障意识挺在前面,无论是推行电子政务、建设智慧城市还是发展智能工业的过程中,都要时刻提高网络安全警惕意识,强化网络安全保障,完善管理制度和技术支撑,筑牢安全发展基石。二是提高网络空间治理意识。网络空间安全已经远远超过了传统网络安全范畴,互联网和经济社会各领域融合产生的新业态引发了网络空间新风险,诈骗、偷窃、色情、恐怖主义等传统违法犯罪行为的数字化和网络化,已经成为网络空间最大的安全隐患。要加快行业治理向网络空间领域拓展,加强对新业态发展引发风险的研判,加快治理手段革新,强化新技术在网络空间治理中的应用,提高网络社会时代行业治理能力。

信息化发展浪潮正在席卷全球,以互联网为代表的信息技术正在加速重塑整个经济社会运行模式。各级领导干部作为各地区、各部门、各行业发展的推动者,需要与时俱进,用新思想、新方法、新技能武装自己,才能不断提高自己为人民服务的本领。

科技战略

夯实基础设施信息安全之基

□ 陆天歌 张乃千

信息安全态势的网络核心技术人才。强化具体操作和协调配合,为保障基础设施信息安全提供统一步调。关键信息基础设施安全涉及范围广,除了要共享网络安全信息以应对网络攻击外,还必须强化网络安全管控的具体操作与协调配合。美国目前基本形成了依托司法系统的网络信息安全管控机制,英国则通过制定相关计划与法律,为阻击常规网络犯罪与严重信息安全事件提供了统一运作平台。我们应尽快建立关键信息基础设施风险和漏洞共享机制,同时可对基础设施信息安全风险进行分级管理。在应对和处理关键信息基础设施各种安全问题时,我们必须进一步加强组织、协调与配合,化被动为主动,打赢关键信息基础设施领域的“安全保卫战”。

科技评论

