“个人信息保护”该怎么立法?

■本报记者 赵广立

在5G即将商用之际，一部有针对性的专门法律更利于应对当前的态势，同时也更加便于法律条文的逐步完善。

告别“裸奔”！今年两会上传来好消息，一部立足于对个人信息保护的法律规范终于呼之欲出。

3月4日，十三届全国人大二次会议新闻发布会上，新闻发言人张业遂透露，全国人大常委会已将一些与人工智能相关的立法项目，如数字安全法、个人信息保护法等列入本届五年立法规划。

“我从2014年就开始呼吁，连续好几年都提交了相关的议案，今年终于看到了曙光。”在接受《中国科学报》采访时，全国人大代表、南京邮电大学校长杨震告诉记者，我国在5G（第五代移动通信技术）即将商用之际将个人信息保护立法列入规划，不仅非常及时，而且意义重大。

5G时代挑战更大

“科技的进步一方面带来极大便利，另一方面也为个人信息保护带来巨大挑战，尤其是5G。”杨震说，从4G时代人与人之间的通信，到5G时代的联通万物，万物互联将使得信息的采集变得空前全面，每个人在网络中将变得如“透明人”一般，“这个时候，以立法的形式对个人信息加以保护尤为重要”。

个人信息安全问题是社会各界关注的焦点，因个人信息不当采集、滥用、泄露乃至非法买卖，导致公民权益受到侵害的案件时有发生。“5G即将投入商用，对个人信息保护提出了更为迫切的需求。”杨震说，人们在日常生活消费和信息通信体验中的各种信息，将随着通信技术的升级被更便捷地、无感地采集，即使商家不是主动侵犯个人隐私，也带来了各种隐患。

事实上，个人信息保护在我国并非无法可依。目前，我国已有刑法总则、民法总则、消费者权益保护法、网络安全法、电子商务法等多部法律、法规和规章涉及个人信息保护。不过，杨震认为，这些法规总体较为分散，在5G即将商用之际，一部有针对性的专门法律更利于应对当前的态势，同时也更加便于法律条文的逐步完善。

难以一步到位

近年来，全球范围内掀起了一股加强个人隐私保护的热潮，并随着Face-Book创始人兼CEO扎克伯格因深陷“用户数据遭窃事件”频上头条达到顶峰。2018年5月，欧盟颁布的“史上最严”数据保护法案《通用数据保护条例》（GDPR）宣告生效。

我国专门针对个人信息保护的立法，会是中国版的GDPR吗？

“在立法过程中，可以参照国外好的做法，吸取其长处，但也要立足我国国情，制定符合我国大多数公民利益的法律条款。”杨震告诉记者，我国的网络覆盖强度、用户习惯与国外不同，这些因素需要在立法中考虑进去。

不过，杨震也坦言，针对个人信息保护，需要回答的基本问题很多，比如怎么定义个人信息？哪些信息要保护？如何进行保护？应该对未成年人个人信息保护采取哪些妥善措施？诸如此类的问题，此前还没有哪部法律有专门的解释。

比如，全国政协委员、公安部原副部长陈智敏就认为，数据在数字时代应属于私有，相当于农业革命的土地、工业革命的资本，但现行法律并没有赋予其资产属性，数据的所有权、使用权、管理权、交易权等也没有被充分地认同和明确地界定。因此，他提出，要在立法中明确数据的属性。

此外，杨震还提出，个人信息保护法在维护公民隐私的基础上，也要注意保护的“适度”。“个人信息保护法从长远看不应成为互联网企业头上的紧箍咒，而是要成为促进行业规范发展的利好因素。”他表示，这就考验立法者的智慧，如何让立法更科学，既能保护用户个人信息，又能促进科技发展和应用。

全国政协委员、搜狗公司CEO王小川认为，保护与开放并不矛盾，他建议，在确保数据收集、分发、使用等得到国家立法规范与保护的前提下，加快面向人工智能的公共数据开放，营造包容的公共数据流通法治环境。

“如何找到这个平衡点，这是立法的一个难点。”杨震说，这也表明了个人信息保护立法确实有其难度，“要很容易，早就出来了”。他说，类比中国首部电子商务法的制定与实施，个人信息保护法也不可能一下子十全十美，“要根据实际情况不断地完善”。

一靠法律，二靠技术

立法保护个人信息的另一层要义，是维护数据安全。“防止数据被‘黑’，一靠法律，二靠技术。”杨震说，随着技术的革新，攻防双方都在进步，“道高一尺魔高一丈”。

这需要法律和技术综合运用。全国政协委员、中国科学院院士尹浩认为，互联网用户信息安全，需要技术和管理综合施策。

“安全界有一种说法：三分技术，七分管理。一方面要通过法律管理手段让非法攫取和滥用信息的人承受代价，严厉打击盗用互联网用户信息的非法行为，另一方面管理和技术必须相辅相成。”尹浩举例说，例如，如何快速发现窃取和非法使用公民信息行为并进行准确定位，这就需要网络安全防护技术的支撑，如借助人工智能技术建立攻击者的行为模型，通过算法分析快速识别和准确定位非法入侵者等。

不过，随着物联网、信息化、智能化的发展，网络安全防护还面临一些重大挑战。全国政协委员、360集团董事长兼CEO周鸿祎向《中国科学报》介绍道，未来联网设备数以百亿计，不可能在每个终端上都部署防护软件；此外，黑客只要利用一个未知漏洞在未知的时间和地点就能发动攻击，而漏洞却是难以预知的。

“面对这些威胁和挑战，当务之急是能够及时发现网络攻击，靠单点发现是不可能的，唯一的方法要靠大数据。”周鸿祎说，虽然现在各单位建立了很多网络安全防御系统，但是数据没有打通、各自为战，无论是企业、网络安全公司、运营商还是政府部门，都各自掌握一部分数据，只能看到局部情况。

“迫切需要把数据统一起来，建设国家级的网络空间防御系统——网络安全大脑，实现对网络攻击的第一时间发现和及时处置。”周鸿祎介绍说，360过去几年构建了一个安全大脑的原型，综合运用了物联网、移动通信、人工智能、区块链、云计算、大数据、边缘计算等技术，能够发现潜在威胁，初步解决了“谁进来了不知道、是敌是友不知道、干了什么不知道”的问题。

周鸿祎进一步建议，若构建国家级的网络安全大脑，迫切需要发挥制度优势，由国家相关部门牵头，协调网信、工信、公安、科技等部门和单位，组织国企、民企、科研院所等广泛参与。

全国政协委员、360集团董事长兼CEO 周鸿祎：

加强应对人工智能网络安全风险

“小孩子玩的10元一支的激光笔，攻击者拿来对着智能汽车的激光雷达乱照，汽车就可能因突然刹车而被追尾；360公司一个技术团队，花不到一千元做出来一款民用级别的GPS欺骗设备，就可以对汽车的行车路线实施欺骗，导致交通安全事故发生。”

这不是危言耸听。全国政协委员、360集团董事长兼CEO周鸿祎在其《关于加强应对人工智能网络安全风险的提案》中写道：“传感器被干扰是人工智能系统面临的首要安全问题。”此外，他还提到，使用被污染的数据训练过的人工智能（AI）会“学坏”、AI内部算法不完善易导致决策失误、用以实现AI的软件系统被劫持，是人工智能网络所面对的另外三大安全隐患。

人工智能的引入，涌现了许多无人值守系统。但一旦这些系统（极端情况如智能武器系统）被黑客控制，可能会产生严重后果。“人工智能并不是像人们想象得那样美好。”周鸿祎在举出这个例子后说道，它在提高人们生产生活水平的同时，也可能带来各种安全隐患，甚至成为人类安全的杀手。

“没有人工智能安全，就没有国家安全、社会安全和个人安全，必须引起高度重视。”针对上述四大安全隐患给人工智能系统带来的潜在挑战，周鸿祎建议：“要加快国家级网络安全人工智能开放创新平台建设。”

为何要上升到“国家级”网络安全平台的建设？周鸿祎认为，人工智能网络安全问题非常复杂，迫切需要建立一个开放创新平台，整合各种资源，协同推进和解决。

他看到，国家对新一代人工智能开放创新平台的建设高度重视，已分别在自动驾驶、城市大脑、医疗影像、智能语音、智能视觉五大领域批准建设人工智能开放创新平台，但在人工智能网络安全领域还是空白。

“建议国家加快国家级网络安全人工智能开放创新平台的审批和政策支持，确保人工智能健康有序发展。”周鸿祎说。

前沿扫描

高维量子密钥分发方案获验证

本报讯（记者赵广立）记者从中科院量子信息重点实验室获悉，郭光灿院士团队日前在高维量子密码领域的研究中取得新进展：韩正甫研究组利用量子态的不同自由度之间的映射方法，设计并实验验证了一种保真度和稳定性极佳的高维量子密钥分发方案。该研究成果已于近日发表在学术期刊《应用物理评论》（*Physical Review Applied*）上。

高维量子密钥分发利用高维量子态编码，可以在单个量子态上加载多于1比特的经典信息，从而有效提高安全密钥生成率；同时，高维量子密钥分发可容忍更高的系统误码率，因此具有更强的抗噪能力。但与BB84协议等常用的二维量子态编解码技术相比，实现光子轨道角动量等高维量子态的高保真、高速率编解码的难度极大。因此，现有的高维量子密钥分发技术仍停留在原理验证阶段。制约该技术实用化发展的核心问题是高维量子态的制备、传输和测量。

量子密码组陈巍、银振强等人基于光子的偏振—轨道角动量不可分离态，提出了偏振和轨道角动量双自由度之间的态映射方法和实现方案，进而实现了对高维量子态的高精度制备和测量。该方案在操控光子偏振态的同时，可以通过映射装置同时高精度地操控光子的轨道角动量量子态，从而实现高保真度的信息加载和提取。与现有技术相比，该方案的最大优势在于编解码过程不需要进行光子态的干涉操控，因而具有很低的本底误码率和极佳的稳定性。

结果显示，基于该方法实现的高维量子密钥分发系统的平均误码率仅为0.60%±0.06%，利用弱相干光源实现了1.849比特/脉冲（理论极限为2比特/脉冲）的高筛后安全密钥率。并且，由于系统只需操控光子的偏振态，有望实现与二维量子密钥分发系统相同的高工作速率，因此具有很好的应用潜力。

该研究工作为解决高维量子密钥分发的态制备和态测量两大难题开拓了一条有效的解决思路，为高维量子密钥分发技术的实用化起到了积极的推动作用。

相关论文信息：*DOI:10.1103/PhysRevApplied.11.024070*

速递

云从科技和上海交大联合发布NLP最新成果：

机器阅读理解首次超越人类高中生

本报讯 3月8日，中科院旗下人工智能创业企业云从科技和上海交通大学联合宣布，双方基于原创算法提出的全新模型，在自然语言处理（NLP）上取得重大突破：该模型在大型深度阅读理解任务中取得了超越人类高中生的准确率，成为世界首个机器阅读理解超过人类排名的NLP模型。目前，该成果已在arXiv网站预发布。

研究人员在论文中称，云从科技与上海交通大学基于原创DCMN算法，提出了一种全新的模型，使机器阅读理解正确率提高了4.2%，并在高中测试题部分首次超越人类（机器正确率69.8%、普通人类69.4%）。

该模型这一成绩是在大型深层阅读理解任务数据集RACE上取得的。据了解，RACE是一个来源于中学考试题目的大规模阅读理解数据集，包含了大约28000篇文章以及近100000个问题。它的形式类似于英语考试中的阅读理解（选择题），给定一篇文章，通过阅读并理解文章，针对提出的问题从四个选项中选择正确的答案。该题型的正确答案并不一定直接体现在文章中，只能从语义层面深入理解文章，通过分析文章中的线索并基于上下文推理，选出正确答案。相对以往的抽取类阅读理解，算法要求更高，被认为是“深度阅读理解”。

云从科技创始人周曦表示，基于这一研究成果，在应用领域搭配文字识别OCR（光学字符识别）或语音识别技术后，NLP模型将会帮助机器更好地理解人类文字或语言，并广泛应用于服务领域，比如帮助企业判断客户风险、审计内部文档合规、从语义层面查找相关信息；在社交软件、推荐引擎软件内辅助文字审阅工作等，“从枯燥的人工文字工作中解放人类”。（赵广立）

IBM抛出“量子摩尔定律”

本报讯 在近日召开的2019年美国物理学会三月会议上，IBM抛出了“量子摩尔定律”的概念。IBM发现，量子计算机遵循一种“摩尔定律”：其量子计算机实现的“量子体积”每年增加一倍。

“量子体积”是IBM提出的一个专用性能指标，用于测量量子计算机的强大程度，其影响因素包括量子比特数、门和测量误差、设备交叉通信以及设备连接和电路编译效率等。量子体积越大，量子计算机的性能就越强大，能够解决的潜在实际问题就越多。

IBM的量子研究团队还发表了一篇论文，详细描述了这个指标以及如何计算。在论文中，他们指出，新的度量标准“量化了计算机成功实现的最大宽度和深度相同的随机电路”，并指出它还与错误率密切相关。

按照IBM的计算方法，IBM自2017年连续三年推出量子计算设备，三台设备的量子体积分别为4、8和16。IBM认为，今年1月在国际消费电子展（CES）上亮相的IBM Q System One提供了“迄今为止最大的量子体积”。（赵鲁）

腾讯58篇论文入选CVPR 2019

本报讯 全球计算机视觉会议IEEE国际计算机视觉与模式识别会议（CVPR 2019）将于6月在美国长滩召开。腾讯公司有58篇论文被本届CVPR大会接收，其中腾讯优图实验室25篇、腾讯AI Lab 33篇。腾讯此次被收录的论文涵盖深度学习优化原理、视觉对抗学习、人脸建模与识别、视频深度理解、行人重识别、人脸检测等领域。

CVPR官网显示，今年有超过5165篇的大会论文投稿，录取了1299篇论文，比去年增长了32%（2017年论文录取979篇）。这些录取的最新科研成果，涵盖了计算机视觉领域各项前沿工作。（赵鲁）

微软粤港澳战略以人工智能为突破口

本报讯 在近日举办的“大湾区——微软科技创新峰会”上，响应国家印发的《粤港澳大湾区发展规划纲要》，微软宣布将以人工智能与物联网技术创新、大湾区产业数字化转型、新一代科技人才培养、提升区域企业国际竞争力等方向为突破口，发挥微软在云计算、大数据、物联网、人工智能等领域的技术优势，为大湾区建设全球科技创新高地和新兴产业重要策源地贡献力量。

根据国家最新颁布的《粤港澳大湾区发展规划纲要》，由香港、澳门、珠三角九市组成的粤港澳大湾区，将深入实施创新驱动发展战略，深化粤港澳创新合作，构建开放型融合发展的区域协同创新共同体；还将着力提升科技成果转化能力，推动互联网、大数据、人工智能和实体经济深度融合，大力推进制造业转型升级和优化发展；同时，推动大湾区企业联手走出去，在国际产能合作中发挥重要引领作用。（计红梅）

学术经纬

CPU从自主可控走向安全可信

■张承义

自主可控是实现国家网信安全的必要条件，但自主可控不等价于安全。中央处理器（CPU）安全设计可以从三个方面来看：一个是防后门，一个是堵漏洞，一个是CPU级的可信设计。

主动的恶意后门可以通过自主设计来实现，只要CPU功能由自己人设计、芯片由自己人实现，就做到了知根知底，避免了恶意后门的植入。

非主观的漏洞则来自于设计能力的不足，或者由于芯片日益复杂不可避免引入的缺陷，需要我们练内功、长经验。2018年年初被曝光的“熔断”“幽灵”漏洞本质上是设计缺陷，而不是后门。这一类攻击方式就像是打开了一个潘多拉魔盒，针对CPU旁路信息的攻击和窃取方式一波接一波，直到前几天还曝出新的变种。这一漏洞直接影响的是现代CPU赖以提高性能的基本机制——推断执行和乱序执行，所以夸张一点说，如果这类漏洞得不到根本的解决，CPU单核的微体系结构研究将倒退回上世纪八九十年代。

这类非主观的CPU安全漏洞是由设计能力缺陷或者设计认识缺陷导致的，所以即便是自主设计的处理器也不能绝对避免。解决CPU的安全漏洞一方面需要雄厚的CPU设计技术积累，另一方面也需要与国际主流安全社区的紧密合作。

除了防止后门和漏洞之外，主动的CPU安全设计是信息系统安全可信设计的重要设计理念和重要环节。安全可信并不是一些孤立的技术点，必须在处理器设计的整个流程中贯穿相关设计思想，从架构上、从软硬件总体上去把握。同时，为了安全可信应用的真正落地，必须联合生态圈内各家企业一起，在一个稳定的、定义清晰规范的CPU架构平台上去推进，有了规范才能真正把生态圈的作用发挥出来。因此，飞腾定义了自己的安全处理器架构规范PSPA1.0（Phytium Security Platform Architecture）。

PSPA1.0规范涵盖了CPU的硬件、固件、OS、启动流程、量产管理、漏洞免疫等各个方面，对其中的关键安全特性都进行了定义，以此保障安全特性在设计的全流程中无遗漏地贯穿，并且为客户提供规范的标准接口，指导CPU设计以及客户的软硬件设计和可信软件栈的开发移植。PSPA覆盖了飞腾从嵌入式到高性能的所有应用，定义了对国产商密算法的支持，可以遵循国内的TPCM标准构建可信的系统。

飞腾目前已经实现了CPU设计的自主可控，下一步的目标就是从自主可控走向安全可信，将安全设计理念融入到国产CPU设计的方方面面，走出一条具有中国特色的独立的演进路线，为用户提供安全可信的CPU产品，为国产安全可控事业做出自己的贡献。

（作者系天津飞腾信息技术有限公司战略规划部总经理）