“智能+”更应重视安全挑战

（来源：信息化协同创新专委会公众号，2019-04-19）

人工智能技术和应用飞速发展，在推动经济社会创新发展的同时，也带来安全、伦理、法律法规等方面的风险挑战。随着数据越来越多被收集，应用场景增加，用户个人信息泄露的风险也随之提升。人工智能的研究和应用要有伦理和法律界限，即应以人类的根本利益和责任为原则。

在今年的全国两会上，“拓展‘智能+’”首次被写入今年的《政府工作报告》，作为未来的重要基础性技术，人工智能已连续三年出现在《政府工作报告》中。可以预见，随着人工智能、大数据的深入应用，生产生活的数字化转型是大势所趋。

人们在拥抱人工智能、迈向数字社会的同时，也需要正视人工智能等新技术应用在安全、伦理、法律法规、社会治理等方面的挑战。只有未雨绸缪，研判和防范潜在风险，才能安享“智能+”的时代红利。

人工智能应用方兴未艾，同时也带来安全风险隐患

前不久，一项人工智能深度换脸技术引发争议。原来，这项技术能做到几乎毫无痕迹地给视频中的人物“换脸”，引发人们对隐私和肖像权被侵犯的担忧。更深的担忧在于，如果这一技术被滥用，是否意味着大量视频会被“移花接木”？

今年全国两会上，人工智能、大数据等技术应用带来的安全风险，成为代表委员关注的焦点之一。全国政协委员、360集团董事长兼首席执行官周鸿祎就表示，安全应该成为人工智能发展的基础与前提。全国人大代表、苏宁控股集团董事长张近东也提出，数据安全是数字中国建设的重中之重，发展高质量的数字经济，需要加强对数据的安全保护和合规共享。

从信息安全角度看，当前人工智能应用的安全风险点主要有哪些？

中国信息通信研究院移动安全联盟秘书长杨正军说，人工智能高度依赖海量数据的采集和训练分析。随着数据越来越多被收集，应用场景增加，用户个人信息泄露的风险也随之提升。

“人工智能算法不仅能直接采集用户个人信息，也会深度挖掘分析看似不相关的数据。”杨正军介绍，他们开展的一项调研显示，当前滥用个人信息现象较为普遍。同时，人工智能及大数据场景下无所不在的数据收集、专业化多样化的数据处理技术，使得信息主体难以了解、控制其信息是如何被收集和利用的。信息安全保护已经成为人工智能发展的重要课题。

专家表示，技术本身是中性的，只要利用得当，人工智能也能用来提升网络安全水平。比如，人工智能在识别恶意代码方面就很有优势。

北京神州绿盟科技有限公司安全研究员吴子建说，恶意代码往往是基于一些开源代码修改而成，它们通常有相似的行为模式。借助人

工智能技术训练的检测工具，能够比较高效地发现恶意代码。

人工智能技术也普遍用于企业内网安全防护。吴子建介绍，传统的防护手段是在网络的入口处设置防御措施，但内网之间很少进行防御。采用人工智能等技术手段关联数据，可以有效检测内网中的异常。与传统的方法相比，这种方法不仅能发现已知威胁，还可以检测到未知风险。

吴子建认为，业内还需要做更多深入的研究，不断提升人工智能在安全防护上的价值。

应提前研判智能时代的法律伦理风险，引导人机良性合作

人工智能的应用越来越多，衍生出一系列伦理、法律难题。比如，无人驾驶汽车发生交通事故时如何界定责任，医疗外科手术机器人出现意外怎样处置……

“人工智能的研究和应用要有伦理和法律界限，即应以人类的根本利益和责任为原则，以实现人类根本利益为终极目标。这一要求也是人工智能和人的关系决定的。”中国人民大学法学院副教授郭锐认为。

“当前技术条件下，智能机器尚未具备伦理决策的能力，但其决策会引发有伦理意义的后果。”郭锐认为，通常法律针对的是能够遵循这些原则的主体，也就是自然人或者法律看作是主体的组织（法人），但考虑到人工智能的特征是对人的智能的模拟、延伸和扩展，因此伦理原则应当适用于人工智能系统。

北京师范大学哲学学院教授田海平认为，人工智能的主体构成不

是孤立的个体，而是多种关联形态的总和。“人工智能的构成主体分为研发者（包括算法的开发者）、生产商、运营商、电信网络服务商等。一旦发生交通或医疗事故，由于无法找到某个确定的责任主体，给责任界定带来很大困难，因此需要确立代理人来界定责任与权利。”

近年来，学界和产业界日益重视人工智能中的伦理与法律问题，并推动制定相关技术标准及社会规范。专家表示，人工智能伦理法律涉及科学界、企业界，哲学、法学等多个领域，有必要成立应对人工智能发展的联盟组织，吸纳各方面的力量，共同推进相关研究。

郭锐建议，要考虑到人工智能开发和部署过程中的权责归属，通过为技术开发者、产品生产者或者服务提供者、使用者界定权利和义务，让自动驾驶、无人机等人工智能应用安全落地。

专家表示，人工智能大规模进入人们生活之前，还应建立相对统一的风险评估指标体系，设立具体、可操作的指标，为相关研究及应用提供指引。

专家特别提醒，人和机器各有优势，要互相了解才能实现人机协作，但人还是人机关系的主导者。惟其如此，才能将人工智能引向人机合作的良性发展道路。

全球人工智能法律治理面临共同难题，当前应加强个人隐私安全管理

针对人工智能应用在安全、伦理等领域的潜在威胁，世界各国已经开始了相关法律治理研究。

杨正军介绍，各国对人工智能风险的关注重点和重视程度有所不同。以安全为例，美国关注人工智能对国家安全的影响，2018 年 3 月美国国会发起提案，建议成立国家人工智能安全委员会，并将制定相关法案；欧盟和英国关注人工智能对隐私、就业及伦理的影响；俄罗斯、以色列、印度则重点关注人工智能在国防领域的应用以及对军事安全的影响。

北京师范大学刑科院暨法学院副教授、中国互联网协会研究中心秘书长吴沈括表示，在规范人工智能发展方面，我国起步较早。2017 年 7 月，国务院颁布《新一代人工智能发展规划》；2017 年 12 月，工信部发布《促进新一代人工智能产业发展三年行动计划（2018—2020 年）》，都对人工智能产业的规范发展提出了要求。

“这些政策能够引导和助推相关产业的发展。关于人工智能技术标准，我国也发布过一些文件。然而，当前立法中对于人工智能带来的安全问题还存在比较大的空白，这也是全球人工智能的法律治理面临的共同难题。”吴沈括说。

随着人工智能应用的深入，其附属的相关风险也日益凸显，加强对人工智能相关的法律治理至关重要。人工智能法律治理呈现出哪些趋势，现实中又有哪些需要迫切注意的问题？

吴沈括认为，人工智能立法治理上可能会呈现出三个趋势：一是立法将更加细化，更有针对性。比如，针对自动驾驶、机器人、生物识别等领域颁布一些规范性文件，立法监管也会更加多元；二是立法将与产业特性紧密结合；三是立法将以规范为主，监管则重在为产业

发展提供指引。

“由于法律往往存在一定的滞后性，考虑到人工智能等新技术应用前景广阔，立法需要预留一定的空间，尽量实现产业应用与风险前瞻的恰当平衡。在确定监管什么内容、如何监管以及怎样执行时，要把握好力度，不宜影响产业的发展活力。”吴沈括说。

杨正军说，从行业调研情况来看，当前应该加强个人隐私安全管理。他建议，隐私保护应从立法监管和技术能力提升两方面入手：一方面，针对我国个人信息保护法律条款分散、不成体系的现状，加快统一立法，明确数据不当收集、使用、泄露等的责任，同时也要界定好数据归属权等问题；另一方面，应加强新技术在个人隐私保护方面的应用。

数据的合理合法收集是数据利用的前提。专家表示，我们不应回避智能化与隐私安全保护的冲突，而应积极作为，找到智能时代技术应用与风险防护的最大公约数，为智能生活保驾护航。

原文链接：https://mp.weixin.qq.com/s/CkShOElQabbBjVczclDGfQ，转载请注明。