重庆大学学报(社会科学版) 2020年第26卷第4期
JOURNAL OF CHONGQING UNIVERSITY(Social Science Edition) Vol. 26 No. 4 2020

Doi:10. 11835/j. issn. 1008-5831. fx. 2020. 03. 003

欢迎按以下格式引用:祝高峰. 论人工智能领域个人信息安全法律保护[J]. 重庆大学学报(社会科学版),2020(4):150-160. Doi:10. 11835/j. issn. 1008-5831. fx. 2020. 03. 003.

Citation Format: ZHU Gaofeng. On the legal protection of personal information security in the field of artificial intelligence[J]. Journal of Chongqing University(Social Science Edition),2020(4):150-160. Doi:10. 11835/ j. issn. 1008-5831. fx. 2020. 03. 003.

论人工智能领域个人信息安全法律保护

祝高峰

(桂林电子科技大学 法学院,广西 桂林 541004)

摘要:人工智能时代的个人数据和信息支撑着人工智能系统的运行,个人信息在当下的重要性和具有的价值已不言而喻。个人信息的识别要素包括"可识别性"和"可固定性",人工智能领域的个人信息在此基础上呈现出不同形式,包括被"智能物"收集的个人信息和被智能系统分析得出的个人信息。而人工智能在不同情形中侵犯个人信息,其侵权主体在现行法律的规定下难以判定。"智造时代",人工智能严重威胁着个人信息的安全。因此,在人工智能时代到来的同时,更应当对人工智能领域中的个人信息安全问题提供有效的法律保障。

关键词:人工智能;智能物;智能系统;个人信息安全;法律保护

中图分类号:D912. 8;TP18;TP309 **文献标志码**:A **文章编号**:1008-5831(2020)04-0150-11

当下,人工智能的讨论炙手可热。国家之间的人工智能"较量"也愈演愈烈,2019年2月,美国启动"人工智能倡议",希望集中联邦政府资源发展人工智能[1];俄罗斯也在2019年6月制定了人工智能领域的国家战略[2];我国各地的人工智能政策或项目也逐渐落地,比如北京正式揭牌成立人工智能创新发展试验区,引领人工智能科技前沿和发展方向[3]。各国基本上都将人工智能纳入了本国的发展战略,人工智能将会给社会的发展和变革带来深层次的影响。

人工智能的高速崛起对当下的法学研究也提出了诸多新问题与挑战。已有学者对人工智能领

修回日期:2020-03-02

基金项目:中国法学会2018年度部级法学研究课题"重要数据安全法律保障机制研究"(CLS(2018)D127);桂林电子科技大学英才计划资助

作者简介:祝高峰(1978—),男,山东潍坊人,桂林电子科技大学法学院/知识产权学院副教授,知识产权法博士,硕士研究生导师,主要从事网络信息法、知识产权法研究,Email:845021165@qq. com。

域的人格权保护问题、知识产权保护问题、刑法保护问题等进行了研究，但对人工智能领域的个人信息安全问题研究目前鲜有涉及。尽管人工智能的定义比较广泛且多变，但在人工智能的基础层面基本上无异议。毕业于美国密歇根州立大学法学院的马修·胡默里克（Matthew Humerick）博士认为，“在人工智能最基础层面上，人工智能是一个能够学会学习的系统”[4]。在笔者看来，人工智能不仅仅是智能系统自主学习的体现，对于人工智能的分析应当从两个层面进行，目前人工智能领域的主要应用在于智能系统和“智能物”两大模块，智能系统主要指软件系统，该部分的软件系统不同于硬件或者是软件与硬件的结合类型，当然软件系统部分起核心作用的仍是程序。“智能物”则包括智能机器人和被智能化的物品，比如工业机器人、服务机器人、智能手机、智能扫地机器人等智能终端产品，“智能物”仍是依靠程序驱动，但主要体现的是其有形存在的一面，而软件系统则多是以无形的方式存在。人工智能发挥作用主要依赖于对数据和信息的收集、分析、利用，个人数据信息的处理尤为凸显。因此，个人数据信息的安全和保护成为亟待解决的法律问题。

一、人工智能危及个人信息安全

（一）人工智能危及个人信息安全的收集和利用

1. 个人信息收集方式的隐秘性

与传统收集个人信息的方式不同，人工智能通过各种端口侵入个人生活，收集个人信息[5]。这些智能端口无处不在，遍布我们的生活空间，如头顶的摄像头、电脑的 USB 接口、手机的指纹识别触控、行车导航的定位仪，以及我们完全意识不到的其他位置等领域。人工智能领域，不论是智能物还是智能系统都离不开智能端口，当这些智能端口收集个人信息时，我们不仅很难察觉，而且也缺乏必要的防范意识，更不会考虑甚至是没有能力追寻我们的个人数据信息通过这些智能端口到底将个人数据信息传向哪里。比如 iPhone Operating System（简称 iOS）系统记录用户的指纹和面容，大部分用户只能意识到指纹和面容用来解锁手机，根本不会察觉到系统收集到所有用户的指纹和面容信息会进行什么样的分析和计算，更不会考虑从终端用户获取的这些指纹和面部信息是否会被用于其他地方。人工智能领域个人信息安全面临严重威胁的同时，人工智能对个人信息的隐秘收集对国家和社会也会造成一定程度的威胁。

2. 个人信息的收集极易侵犯个人隐私

人工智能不仅隐秘地收集个人数据信息，而且鉴于人们对智能物和智能系统的被动的无理由的信任，被人工智能收集到的个人信息更多地涉及个人隐私。传统收集个人隐私信息的方式，大多是跟踪偷拍、监视监听、非法搜查，而人工智能却很容易就能通过其自主学习和分析获取包含个人隐私的隐秘数据信息。作为人工智能产物的聊天机器人就是典型的事例体现。与过去只能简单对话的机器人不同，人工智能聊天机器人的终极目标是通过“图灵测试”①（Turing test），即超过 30%的测试者不能判断被测试的到底是机器还是人类。可见聊天机器人可以做到像人类一样分析对方的心理活动，在用户毫无防范意识的状态下，通过聊天获取终端用户不会随意透露的隐私数据，甚至

①图灵测试（又译图灵试验）是图灵于 1950 年提出的一个关于判断机器是否能够思考的著名试验，测试某机器是否能表现出与人等价或无法区分的智能。测试的谈话仅限于使用唯一的文本管道，例如计算机键盘和屏幕，这样的结果是不依赖于计算机把单词转换为音频的能力。维基百科. 图灵测试[EB/OL]. [2019-10-29]. https://wikipedia.hk.wjbk.site/baike-%E5%9B%BE%E7%81%B5%E6%B5%8B%E8%AF%95.

还会通过其自带的算法诱导终端用户说出更多的私密信息。

此外,在大数据技术的支持下,人工智能随着自主学习能力和人机交互能力的不断提高,日后可以为人类提供越来越细致和周密的服务,包括做饭、打扫、陪伴、聊天、学习、恋爱等完全属于个人私生活领域的服务,智能物和智能系统将在服务过程中不断地将终端用户的相关个人数据信息记录其中。同时,随着人工智能学习能力的逐渐提高,通过关联性分析和数据技术分析,很可能使过去一般存在的个别信息变为可以识别个人主体的信息。比如根据一般的使用痕迹和轨迹,人工智能通过汇总分析可以得出相对具体的个人数据信息,而终端用户在使用人工智能时,并不能轻易地将操作信息记录从人工智能中完全移除。随着人工智能所有权或使用权的流转,其记录的个人信息会继续在网络空间中流动传播,也会随着人工智能所有权、使用权的变动而发生改变。通过读取人工智能代码和操作记录,个人信息在专业人士手中一览无遗,没有任何隐私信息秘密可言。

人工智能搜集个人数据信息超出原有目的使用范围也已成为常态,新兴技术的不断涌现还将带来更多新的个人信息保护等问题。以目前人工智能技术水平,仅从收集和利用个人信息的角度看,人工智能收集和利用个人信息已没有过多的障碍,不论是对于智能物还是智能系统来说,人工智能都可以在当事人不知情的情况下擅自收集、处理、利用个人信息,而此时个人信息受到侵犯的侵权主体就需要从法律层面进行明确的界定。

(二)人工智能作为侵犯个人信息主体的认定复杂性

人工智能包括智能物和智能系统,人工智能侵犯个人信息权利的主要方式有两种:人工智能被人利用发生的侵权行为或者人工智能算法本身存在侵权可能性[6]。在笔者看来,人工智能侵犯个人信息主体的认定也应当在此两种情况下分别讨论。

1. 人工智能的被动侵权

人工智能的被动侵权主要是指人工智能被第三方利用侵权的一种侵权方式,此种情形下的侵权需要明确界定侵权主体,因为即使人工智能被利用,人工智能也未必就一定被认定为侵权主体。早在20世纪40年代,科幻作家艾萨克·阿西莫夫(Isaac Asimov)提出“机器人三定律”②,根据该原则,机器人在必须服从人类命令的同时不得做出伤害人类的事。显然人工智能被人利用侵权时,与“机器人三定律”的原则相悖。例如人工智能在快递领域的普及应用,快递业务是最容易导致个人信息被侵犯的领域。寄件人在邮寄快递时,必须进行实名认证,填写真实的姓名、电话、邮寄内容、寄件地址以及收件人的基本信息,当快递获得的个人数据信息被泄露之后,侵权人利用人工智能系统,可以轻易分析出收件人的“画像”,甚至能够对收件人的心理信息和后续行为信息进行预判,进而实施犯罪活动[7]。侵权人利用人工智能实施违法行为,即使根据现阶段的法律制度,对其进行追责,其也应当要承担法律责任。也就是说,此时人工智能并不是侵权主体,而利用人工智能进行侵权的人才是真正的侵权主体。

2. 人工智能的主动侵权

人工智能由于算法本身导致侵权也存在两种情况,其一是人工智能存在算法缺陷,软件系统在运行中无法实现保护个人信息的功能,根据《中华人民共和国侵权责任法》(以下简称《侵权责任

②机器人三定律,第一法则:机器人不得伤害人类,或坐视人类受到伤害;第二法则:除非违背第一法则,否则机器人必须服从人类命令;第三法则:除非违背第一或第二法则,否则机器人必须保护自己。维基百科.机器人三定律[EB/OL].[2019-10-30].https://wikipedia.tw.wjbk.site/wiki/%E6%9C%BA%E5%99%A8%E4%BA%BA%E4%B8%89%E5%AE%9A%E5%BE%8B.

法》)第5章第41条[3]的规定,该侵权责任由生产者承担。目前的人工智能尚处于高级函数决定的阶段,还不具备自主侵权的"意识",所以不具有主体资格,自然没有承担责任的能力。在这种情况下,人工智能侵权只是表象,并不是真正意义上的侵权主体,而侵权主体实质上还是具有注意义务的生产者。但根据《中华人民共和国产品质量法》(以下简称《产品质量法》)第41条[4]的规定,生产者应当对人工智能侵权负有责任,但是同时生产者的责任亦存在免责事由,且笔者认为,在一定程度上看,必须严格适用生产者的免责事由。人工智能技术本质上是算法和程序的更新进步,程序开发者在开发人工智能的过程中,难免存在一些尽到注意义务后仍然不可避免的算法缺陷,因此应当严格适用免责事由,如此,有利于激励创新,给予生产者应有的宽容。其二是人工智能自主侵权。当人工智能技术发展到与人类交互甚至超越人类的智慧之时,人工智能可能完全不受人类控制,做出侵权行为。比如一辆无人驾驶汽车在自主驾驶的过程中将乘客的出行信息自主上传到网络空间,此时所有人或使用人并未对其进行操作,表面上看似乎完全是汽车的责任,但是在现行法律框架下,汽车并不具有主体资格。在人工智能没有被认定为法律主体的情况下,其做出的侵权行为应当由谁承担责任是现行法律无法解决的问题。有部分学者认为,人工智能无法成为责任主体,可以由制造者承担"公平责任"。但是人工智能技术的研究和发展本来就是人类难以预测的,人类制造人工智能的核心目的不是探索科技可以达到什么样的高度,而是希望人工智能提供越来越高端理想的社会服务。当人工智能完全可以代替人类体力及脑力活动的时候,人类本应当预料到人工智能有失去控制的可能性。因此笔者认为,让制造者承担"公平责任"有违科技发展的目的,甚至会阻碍制造者的研发积极性。在人工智能不具有侵权主体资格的情况下,可以考虑从技术源头防止人工智能的侵权行为发生。

(三)人工智能的追责机制缺失

1. 人工智能侵犯个人信息的法律保护机制缺失

目前在人工智能领域涉及具体的个人信息保护的法律法规几乎未有,仅在2017年实施的《中华人民共和国网络安全法》(以下简称《网络安全法》)和部分行政规章[5]中有比较分散的对个人信息的保护规定。《网络安全法》对个人信息的含义、侵犯个人信息应当承担的法律责任,以及经营者收集个人信息的方式都作了较为明确的法律规定,但是人工智能领域的个人信息保护问题远不止现行法律规定的情形,鉴于人工智能强大的运算分析技术和对个人信息安全的影响力度,应当明确以下问题:首先,应当界定人工智能领域个人信息的含义及范围;其次,人工智能对个人信息的使用方式应当有明确的界定;再次,人工智能领域侵权责任的承担不应当直接适用《网络安全法》的规定。总之,人工智能侵犯个人信息的保护机制要综合考虑人工智能技术和发展问题,不能局限于当前的法律框架和已经存在的问题。

---

③《侵权责任法》第5章第41条:"因产品存在缺陷造成他人损害的,生产者应当承担侵权责任。"

④《产品质量法》第41条:"因产品存在缺陷造成人身、缺陷产品以外的其他财产损害的,生产者应当承担赔偿责任。生产者能够证明有下列情形之一的,不承担赔偿责任:(一)未将产品投入流通的;(二)产品投入流通时,引起损害的缺陷尚不存在的;(三)将产品投入流通时的科学技术水平尚不能发现缺陷的存在的。"

⑤《互联网电子公告服务管理规定》第12条:"电子公告服务提供者应当对上网用户的个人信息保密,未经上网用户同意不得向他人泄露,但法律另有规定的除外。"《互联网电子邮件服务管理办法》第9条:"互联网电子邮件服务提供者对用户的个人注册信息和互联网电子邮件地址,负有保密的义务。互联网电子邮件服务提供者及其工作人员不得非法使用用户的个人注册信息资料和互联网电子邮件地址;未经用户同意,不得泄露用户的个人注册信息和互联网电子邮件地址,但法律、行政法规另有规定的除外。"

2. 人工智能产品开发缺乏有效的法律保障机制

智能物和智能系统都是人工智能产品,人工智能产品的核心技术在于软件程序,因此在人工智能产品开发中就会对个人信息保护问题造成决定性的影响,我国法律对此并无规定。软件开发规范(GB/T8566-2007《信息技术 软件生存周期过程》)仅规定了计算机软件系统和软件产品以及服务的获取,软件产品的供应、开发、运行和维护等问题,关于软件可能涉及的信息安全问题完全没有规定。中国电子技术标准化研究院编写的《人工智能标准化白皮书(2018)》(以下简称《白皮书》)梳理了人工智能产品应当符合的"安全/伦理标准",其中明确涉及隐私保护规范。根据《白皮书》的分析,人工智能算法、系统和产品都应当符合一定的安全要求和测评方法,在人工智能的开发和部署过程中应当充分考虑责任和过错问题,制定完善的相关安全法规[8]。但是现实制度中,对人工智能产品中个人信息的规制和监管力度相对较弱,弗里曼·戴森(Freeman J. Dyson)曾经说过:"技术只会给我们提供工具,人类的欲望和制度决定了我们如何利用它们。"[9]

二、人工智能领域的个人信息界定

"智造时代",在数据驱动的经济中,个人信息通常被认为是"免费"的数字服务,同时客户数据已经被视为商业资产[10]。而作为终端用户的个体似乎完全没有意识到自己的个人信息运转于人工智能的庞大数据系统,更意识不到自己的信息驱动着人工智能的经济价值。因此,有必要对人工智能领域个人信息的概念进行界定,并分析人工智能领域个人信息被运转的方式。

(一)个人信息的界定

人工智能的核心技术依靠算法和数据完成,在智能物和智能系统中被收集利用的个人信息本质上是在网络空间中运转。因此,笔者认为人工智能领域的个人信息与网络空间中的个人信息本质上具有同质性,从法律层面看,人工智能领域的个人信息与网络空间中的个人信息法律属性具有一致性 。

1. 个人信息的概念

美国SP 800-122《保护个人身份信息的保密指南》以概括加列举的方式规定了个人身份信息的定义,可以概括为用于区别或追踪个人身份以及可以被链接到一个人的任何信息,诸如社会安全号码、出生地、医疗信息等[11],根据该定义,个人身份信息具有"识别性"和"关联性"。

我国对个人信息的概念明确界定在《网络安全法》中,该法第76条第5款将个人信息定义为以某种方式记录的,能够单独或者与其他信息结合而识别出自然人身份的信息,包括自然人的姓名、出生日期、证件号码、住址和电话号码等。《网络安全法》同样以概括加列举的方式解释个人信息的含义,从此款规定可以看出,所有能以一定方式固定下来,并能以此识别出个人身份的信息就是个人信息,也就是说此处的个人信息应当包括直接可识别的个人信息和间接可识别的个人信息。在笔者看来,没有必要非要对个人信息进行直接和间接的分类,因为网络空间中的个人数据信息具有动态性及可变性的存在形式,但是不论其存在形式如何变化,其个人数据的法律属性应当是固定的,即使个人信息具有价值,体现其财产属性的一面,但个人信息的存在不是以个人信息交易为目的,个人信息权的权利基础应当属于一项具体人格权范畴,否则个人信息将失去规范的基础。

2. 个人信息的识别要素

根据《网络安全法》第76条对个人信息的解释,"可识别性"和"可固定性"是识别个人信息所

应当具有的两个基本要素。首先,根据现有的个人信息能够“识别”出具体的自然人,在现行社会制度下,能够通过自然人的姓名、肖像、身份证号、住址等常规信息识别出自然人,人工智能则可以通过分析个人爱好、购买记录、浏览记录、行走路线等就能识别出具体自然人。也有学者认为,个人信息不应局限于本人所知[12],对于本人不知道的信息,但能识别出自然人的也属于个人信息,例如被阿里巴巴收集的购买记录、被支付宝收集的付款记录,以及被行车导航收集的出行路线等,都是应当给予保护的个人信息。其次,个人信息具有“可固定性”,即个人信息被利用的前提是被收集,而被收集的个人信息也不可能凭空存在,其必然是通过一定的方式固定存储在某个介质中,该介质既可能是有形的载体也可能是无形的数据库,《网络安全法》第 76 条中的“记录”当属此意。比如机场的安检通关系统,通过人脸识别认定个人信息与机票信息一致,并对通关旅客进行记录。那么进行这一操作的前提必然是将所有可能通关的自然人肖像以及其他身份信息存储在安检系统中,当旅客持机票和证件通过时,登机牌、证件和人脸所能识别出的信息一致即可。我国民航管理部门认可了首个人工智能安检通关系统,代替人工验证岗,“站立”在安检岗的人工智能系统能够在 8 秒内完成人证票核验,可见其中记录的个人信息达到怎样的完善程度[13]。当前的社会运行体系中,几乎所有的个人信息都实现电子化,对信息的处理也大都实现在线处理,即在网络空间中完成处理过程。过去纸质化的个人信息已经不适应信息迅速流动的社会环境,现代社会的信息需要实现快速传递甚至即时共享,以人工智能领域为例,发挥个人信息最大价值的方式就是“处理”个人信息,通过一系列的挖掘、分析、应用,获取隐藏在个人信息下具有更大内涵和价值的信息资源。

(二)人工智能领域的个人信息分类

1. 人工智能物存储的个人信息

人工智能物通常是收集、存储个人信息的来源,机器人、智能家电、苹果 iOS 系统等,只要对其进行操作,所有的操作行为都会被记录下来。比如我们所熟悉的 iPhone 中有一项称为“健康”的应用程序,将手机中的时钟、信息、支付宝、淘宝、QQ 等其他应用作为数据来源,记录机主每天的步行距离、步数、已爬楼层等个人信息。此类个人信息直接反映机主的生活记录、健康状况、活动轨迹等,称为直接个人信息,即不需要经过特别分析就能直接识别出机主的身份。

在弱人工智能时代,智能物只是借助自动化的程序和代码,代替人类进行简单的重复性劳动,不需要机器通过分析数据进行深度学习。到强人工智能时代,智能物将能够完成像人类一样的思考和行为,甚至比人类更“聪明”。但是在笔者看来,不论弱人工智能时代还是强人工智能时代的智能物都需要对终端用户的操作进行记录,否则无法为终端用户提供真正意义上的智能化服务。比如自动驾驶技术必须能够记录终端用户的出行路线,聊天机器人也必须记录与终端用户的聊天过程。

2. 人工智能系统分析数据获取的个人信息

人工智能系统的运行通常是分析、利用个人信息的阶段,智能系统通过深度挖掘,获取与个人相关的所有信息,再分析出有更大利用价值的信息。比如淘宝智能系统,根据用户的“足迹”、购买记录、搜索记录,分析用户的喜好和消费倾向,根据分析结果在淘宝首页向用户推送类似产品,此后用户将在淘宝首页的所有模块看到相关推送,包括“猜你喜欢”“抢购”“特卖”等模块。

墨尔本大学微软社会自然用户界面研究中心(SocialNUI)和墨尔本科学画廊合作研发出一款“生物智能镜”,这面“镜子”将人的面部和一个面部数据库进行对比,进而得出人的幸福程度、内向

程度、侵略性等智能分析结果。虽然这项研究的目的是反思人工智能看似合理的未来是否是我们希望看到的成形的未来,但如果仅着眼于技术,这项研究证明人工智能系统利用算法分析数据很容易获取更多相关的个人信息[14]。除了从镜头和图像中分析性别、年龄和种族之外,人们甚至担心人工智能系统可以准确地预测出个人的性取向甚至政治倾向,人工智能系统对个人信息的获取影响到个人信息安全的程度可见一斑。

人工智能要想扩展到人类的智能,就需要不断地用于模拟、延伸其自主学习的智能系统能力,当人工智能系统通过不断的自主学习直到强人工智能时代,其智能系统将达到人类无法想象的程度。人工智能系统对个人信息的分析和利用,可能会因为制造者的恶意侵犯个人信息安全,也可能会因为人类无法解释的算法黑箱⑥造成更大的损害。计算机程序员负责编写源程序,计算机负责转化出由"0"和"1"组成的目标代码,而源程序如何在计算机内部转化成目标代码,这是程序员也无法解释的问题。例如一台专门为慈善制造的机器可能自己会"变恶",进化和学习算法可能会导致一个本质上是黑匣子的系统,这个系统如此复杂以至于专家们可能无法完全理解它的内部运作。和人类一样,这种机器可能有极其复杂的"心理",所以智能机器具有恶意的可能性是非零的[15]。因此,有必要对人工智能领域个人信息的收集、处理、应用等方面进行有效的法律规制,以更好地保护个人信息。

三、人工智能领域个人信息安全法律保障制度的构建

目前我国仍没有对个人信息进行专门立法保护,在立法保护不足的前提下,人工智能领域涉及的个人信息安全问题更加难以保证。来自美国计算机法专家乔治.S. 科尔(George S. Cole)在20世纪90年代就指出:"在将来,任何一般的人工智能产品都不会在现实世界中漫游,无论是作为移动机器人,还是作为一个自由流通的程序,都会在一定的限制环境中应用,不可避免的是,特定的环境应用程序将造成一些相关的经济损失、财产或人身伤害或死亡。"[16]在立法保护和完善程度上,欧美国家对个人信息的保护相对比较成熟,欧美国家在保护个人信息方面主要体现在对个人信息所有者的权利、增加企业的义务,尤其注重个人隐私方面的保护。可以借鉴国外立法经验,结合人工智能和网络环境的特性,完善我国人工智能领域个人信息保护的法律制度。

(一)制定人工智能领域个人信息安全标准

1. 制定人工智能领域个人信息使用标准化制度

我国《个人信息保护法》呼之欲出,但是人工智能领域的个人信息在网络环境中其动态变化可能超出《个人信息保护法》涵盖的范围。《网络安全法》对个人信息的解释可以适用于人工智能领域,但是在司法实践中应当对其范围作出更加详细的解释。首先,可以制定特殊法条,专门规定人工智能领域的个人信息概念范畴,为保护人工智能领域个人信息奠定基础。其次,应当明确人工智能领域使用个人信息的标准。在人工智能领域对个人信息的处理通常与大数据技术交叉结合,具体包括收集、存储、分析、使用等模式。笔者认为,《中华人民共和国个人信息保护法(草案)》(2017年)中对于收集、处理和利用个人信息的规定,可以适用于人工智能领域对个人信息的处理使用。根据该草案,"收集"是指以使用为目的获取个人信息,"处理"包括输入、存储、编辑、删除等操作,

⑥算法黑箱也被称作"黑匣子",通常是指程序设计者无法探明原理的计算机运行过程。

“利用”是指对个人信息进行目的内且“处理”之外的合法使用[17]。

2. 确立人工智能领域终端用户的信息选择权

人工智能创造的经济价值与个人信息的保护本身存在一定的冲突和矛盾,这是一个需要平衡和制约的问题。若不顾终端用户信息权利取得科技进步,将违背人类制造人工智能的本意,人工智能应当处于为人类服务的地位,而不应该给人类带来安全隐患。为了加强对个人信息安全的保护而抑制对科技的探索,也会导致人类的科学发展止步不前。部分人认为科技的发展必然会产生安全隐患,用户基于保护信息安全,可以选择不使用人工智能。笔者认为这不利于从根本上解决问题,并且用户的“选择权”可以用于对人工智能技术的选择。比如讯飞的翻译机,为了防止终端用户信息的泄露,公司在产品中设计了离线翻译版本,用户在离线状态下使用翻译机,并不会将信息上传到网络空间。因此,法律可以对人工智能制造者进行规制,凡是能实现离线使用的产品,制造者应当设计这一选择程序,增强终端用户的信息选择权。

(二)建立人工智能领域个人信息安全法律保护制度

1. 明确个人信息的权利属性

2018 年 5 月 25 日欧盟《一般数据保护条例》(General Data Protection Regulation,GDPR)正式生效,意味着欧盟对个人信息的保护达到前所未有的高度。《GDPR》对个人信息的处理主要体现在以下几个方面:首先,其规定欧盟用户不仅可以查阅被收集、处理的信息,并且有权了解人工智能自动化决策的程序、目的以及处理后果。笔者认为这一规定正面应对了人工智能的特性,人工智能制造者为人工智能设计自动化程序,制造结束投入使用后,制造者和使用者在正常使用中不再对程序进行修改,人工智能自主完成目标任务。因此,当终端用户预先知晓自动化决策的目的和后果时,可以选择是否进行下一步操作或使用人工智能,可以对个人信息的处理作出选择。我们所熟悉的淘宝平台的隐私权政策中有类似声明,其写明将“约束信息系统自动决策”,但明确提出在某些业务功能中会自动作出决定。很明显这样模糊不清的声明并不利于保护终端用户的个人信息,当发生侵权案件时,仍需要对其声明条款和侵权行为详细分析。其次,规定欧盟用户有权反对以商业目的进行个人信息分析的数据控制者,并有权要求删除其个人信息。人工智能最大的商业或经济价值之一就是分析个人信息,根据分析结果给终端用户推送相关产品和服务,刺激终端用户的行为和消费。如果终端用户有权反对数据控制者的分析行为,并要求删除个人信息,对终端用户来说可以有效避免被人工智能推送影响而产生的冲动性消费。再次,欧盟用户有权将其携带的个人信息,在不同的数据控制者之间进行存储和转移[18]。笔者认为,如果个人信息被法律明确界定为某种权利,欧盟的这一规定对于权利交易来说具有一定的保障功能。在维护数据所有者权利这方面,我国法律存在很大的完善空间,可以从界定个人信息的属性出发,明确个人信息既是一项绝对权利,又是一项具体的人格权,为个人信息的保护夯实法律依据。

2. 完善与人工智能领域相关的立法

《网络安全法》第 41 条规定网络经营者应当合法收集个人信息,并经过被收集者的同意。《网络安全法》虽然规定了用户同意机制,但这一规定仍然不能够应对由人工智能所引起的个人信息安全问题。智能物收集个人信息时,会直接越过用户同意的步骤。智能系统分析个人信息时,通常也不会经过用户的同意。笔者认为,法律制度可以从技术源头遏制个人信息侵权问题。首先,人工智能制造者根据对个人信息数据的分析结果制造用户需求的智能产品,因此在制造之前,规定制造者

必须合法获取个人信息。其次,在人工智能制造之初,规定人工智能的制造者设计用户同意程序,此处的用户同意程序,不应当是简单的格式条款,而是在收集存储用户信息之前必须经过用户的同意。最后,在人工智能运行过程中,扩大“知情—同意”机制的适用范围,原则上任何处理用户信息的步骤都要经过用户的同意,涉及用户隐私的信息更要有清晰的提示,且不得设计强制用户接受同意的程序。

(三)建立人工智能领域个人信息安全的责任机制

1. 确立人工智能主体的追责机制

确立人工智能主体的追责机制是保护人工智能领域个人信息安全的必要前提,也是追责人工智能侵权个人信息时承担责任的基础。目前,人工智能还没有被认为其具有法律上的主体资格,尽管存在其具有主体资格的论述;但笔者一直主张人工智能不具有法律上的主体资格,在笔者看来,此处人工智能的主体并不是指人工智能作为自身的主体,而应当是指人工智能的实际控制者,不论是智能系统的软件人工智能,还是仅仅指智能物,这是目前规制人工智能侵犯个人信息的追责依据,否则很难从法律上认定人工智能自身作为侵权主体而存在。在笔者看来,人工智能无论进化到什么程度,都不能够取代人类的主体资格,也不应当存在所谓的“拟制人”之说,否则将违背自然规律。若真的强人工智能到来,再讨论人工智能主体的追责机制也无实际意义,到那时人类生存权将是首要面对及考虑的。

2. 建立人工智能产品的监管机制

建立人工智能产品的监管机制有助于加强人工智能领域个人信息安全的保护。首先,应当参照《产品质量法》和《侵权责任法》的规定,明确生产者在开发过程中设置保护个人信息功能的通用标准,避免出现缺陷产品。其次,建立人工智能监管和召回机制,生产者以及销售者在人工智能产品售出后应当定期监督人工智能产品对个人信息的收集和使用情况,监督人工智能产品保护个人信息功能的实现,一旦发现人工智能产品缺陷或者有危及个人信息安全的情形,应当立即召回或停止服务。再次,可以制定人工智能领域个人信息安全的行业标准体系,推动发挥人工智能领域行业的自律作用。最后,可以增设人工智能产品的责任保险,该责任机制的设置可以借鉴《中华人民共和国保险法》相关条文中类似于交通事故责任强制保险的规定,在难以确定人工智能侵权责任主体的情况下,可以为被侵权人和生产者提供各自相应的保障。

3. 建立健全企业责任机制

首先,用户对企业在公共平台披露、存储的个人信息应当有获知其信息状态与信息权利运行的知情权。《网络安全法》对此没有相关规定,而我国部分网络平台会在法律声明中说明用户的信息权利。但是笔者认为,当网络平台违反与用户达成的协议后,用户只能围绕违约行为提出法律诉求,而双方的协议中通常不会约定违约责任如何承担,因此并不能为用户提供实质性的保护。其次,当发生个人信息重大泄露事故时,企业应当及时向监管机构报告。欧盟新规明确规定,如果发生用户重大数据泄露,企业应当在72小时内向监管机构或数据所有者报告。而《网络安全法》第47条规定只在发现法律法规禁止发布或传输的信息时,网络运营者才有向有关部门报告的义务。该法也并未对法律法规禁止发布或传输的信息进行明确的解释,可见此条规定并不是对个人信息权利的专门保护。再次,限定人工智能自动化系统对个人敏感信息进行自动决策和自动处理的行为。企业的这项义务有赖于法律对个人敏感信息的界定,应用到人工智能领域,更应当首先明确人工智

能领域个人信息的涵盖范围。

4. 明确人工智能侵害个人信息的处罚机制

欧盟《GDPR》对违规行为的罚款数额相当可观,最高达到 2 000 万欧元或全球年营业额的 4%。我国《网络安全法》对侵犯个人信息的惩罚额度仅规定 100 万元以下的罚款,对直接责任人员的罚款数额仅为 1 万~ 10 万元,该惩罚额度不能够起到严惩和警示的效果。人工智能创造的经济价值是不可预估的,其对个人信息侵权造成的不只是经济损失,甚至包括精神损害,因此对侵权人的处罚数额应当进行详细的划分。我国可以借鉴欧盟对个人信息的保护,进一步完善处罚机制。对于违法收集、利用个人信息的行为规定合理的处罚数额,并将数据控制者和数据处理者纳入处罚范围。

四、结语

大数据时代,人工智能离不开数据的深度挖掘和应用,数据是人工智能的血液,人工智能的深度应用也必将给人类的学习、生活、工作产生深层次的变革,随着人工智能学习的不断深入,人工智能对个人数据信息的应用也不断加强,人工智能对个人信息的收集、存储、传输、应用等形式是科技进步和发展的必然结果。我们无法阻止科技浪潮的来袭,但我们可以提供与之相适应的制度构建。计算机只能发出强制性指令——它们没有被编程来行使自由裁量权[19],即使强人工智能时代真的到来,对人工智能赋予“自由裁量权”,该“自由裁量权”也应当是限定性的权力。“智造时代”,应当尽快建立人工智能领域个人信息安全法律保护制度。当下《网络安全法》难以应对人工智能领域的个人信息安全保护,对个人信息的保护显得单一和不足。在即将到来的《个人信息保护法》中,应当明确该法是否适用于人工智能领域的个人信息保护,同时在相关条文中或者司法解释中明确人工智能领域个人信息安全的相关标准。从法律上明确人工智能侵犯个人信息权利的归责原则和责任承担方式,同时积极制定行业标准,建立人工智能领域个人隐私保护制度、用户选择制度。总之,人工智能领域的个人信息安全问题要综合考量,从技术、法律、政策等多维角度出发,结合人工智能的应用环境给予保护。

参考文献:

[1]周舟. 美国人工智能计划的三大看点[EB/OL]. (2019-02-26)[2019-10-29]. http://www. jjckb. cn/2019-02/26/c_137850529. htm.

[2]刘洋. 俄罗斯将制定人工智能国家战略[EB/OL]. (2019-03-01)[2019-10-29]. http://www. jjckb. cn/2019-03/01/c_137859040. htm.

[3]袁于飞. 三问人工智能创新发展试验区[EB/OL]. (2019-02-26)[2019-10-29]. http://epaper. gmw. cn/gmrb/html/2019-02/26/nw. D110000gmrb_20190226_1-08. htm.

[4]HUMERICK M. Taking AI personally: How the E. U. must learn to balance the interests of personal data privacy & artificial intelligence[J]. Santa Clara High Technology Law Journal,2018,34(4):393-418.

[5]许天颖. 人工智能时代的隐私困境与救济路径[J]. 西南民族大学学报(人文社会科学版),2018,39(6):166-170.

[6]邵国松,黄琪. 人工智能中的隐私保护问题[J]. 现代传播(中国传媒大学学报),2017,39(12):1-5.

[7]严贝妮,叶宗勇,段梦丽. 快递用户个人信息安全隐患成因解析:基于用户角度的调查研究[J]. 现代情报,2018,38(2):91-95.

[8]信息技术研究中心.人工智能标准化白皮书(2018 版)[EB/OL].(2018-01-24)[2019-11-16].http://www.cesi.ac.cn/images/editor/20180124/20180124135528742.pdf.

[9]TSCHIDER C A. Regulating the internet of things: Discrimination, privacy, and cybersecurity in the artificial intelligence age[J]. Denver Law Review,2018,96(1):87-144.

[10]MALGIERI G, CUSTERS B. Pricing privacy - the right to know the value of your personal data[J]. Computer Law & Security Review,2018,34(2):289-303.

[11]许东阳.SP 800-122《保护个人身份信息的保密指南》标准研究[J].信息技术与标准化,2013(09):44-47.

[12]齐爱民.论个人信息的法律属性与构成要素[J].情报理论与实践,2009,32(10):26-29.

[13]雍黎.人工辅助验证智慧安保系统上线[EB/OL].(2019-03-01)[2019-11-18].http://www.stdaily.com/index/kejixinwen/2019-03/01/content_752970.shtml.

[14]Biometric mirror[EB/OL].[2019-11-18].https://socialnui.unimelb.edu.au/research/biometric-mirror/.

[15]PAVLACKA B. Artificial general intelligence and the future of the human race[J]. Berkeley Scientific Journal,2012,16(2):1-3.

[16]COLE G S. Tort liability for artificial intelligence and expert systems[J]. Computer Law Journal,1990,10(2):127-232.

[17]齐爱民.《中华人民共和国个人信息保护法(草案)》(2017 版)[EB/OL].(2017-11-12)[2019-11-29].http://www.sohu.com/a/203902011_500652.

[18]KISHOR N. Will artificial intelligence be illegal in Europe next year?[EB/OL].(2017-08-10)[2019-11-29].https://houseofbots.com/news-detail/941-1-will-artificial-intelligence-be-illegal-in-europe-next-year.

[19]GERSTNER M E. Liability issues with artificial intelligence software[J]. Santa Clara Law Review,1993,33(1):239-270.

On the legal protection of personal information security in the field of artificial intelligence

ZHU Gaofeng

(*School of Law, Guilin University of Electronic Technology, Guilin 541004, P. R. China*)

Abstract: The personal data and information in the era of artificial intelligence support the operation of AI systems. The importance and value of personal information in the present is self-evident. The identification elements of personal information include "identifiability" and "fixability". Personal information in the field of artificial intelligence presents different forms on this basis, including personal information collected by "intelligent objects" and analyzed by intelligent systems. While artificial intelligence infringes personal information in different situations, the infringing subject is difficult to determine under the current law. In the "intellectual era", artificial intelligence seriously threatens the security of personal information. Therefore, while the era of artificial intelligence is coming, it is necessary to provide effective legal protection for personal information security issues in the field of artificial intelligence.

Key words: artificial intelligence; intelligent object; intelligent system; personal information security; legal protection

(责任编辑 胡志平)