 DOI: https://doi.org/10.12345/xdjyjz.v3i7.25087

Criminal law protection of citizens' personal information in the era of artificial intelligence

Yanxiang Wang

Beijing Normal University, Beijing, 100875, China

Abstract

with the rapid development of artificial intelligence technology, citizens 'personal information collection, analysis and use of new challenges, the application of artificial intelligence, intelligent and automation, causing a large number of citizens' personal information is exposed, a threat to personal security, the existing criminal law protection in the new situation, in the lack of areas such as intelligent recognition, data mining, the current law is difficult to effectively cope with the personal information in the application of artificial intelligence. On the basis of analyzing the current situation and problems of personal information protection in the application of ARTIFICIAL intelligence and referring to foreign legislative experience, this paper puts forward suggestions on strengthening the protection of citizens 'personal information in China's criminal law, so as to strengthen the regulation of new infringement caused by artificial intelligence technology and improve the protection of criminal law.

Keywords

application of artificial intelligence; personal information; protection of criminal law; data mining

人工智能时代公民个人信息的刑法保护

王彦翔

北京师范大学，中国 · 北京 100875

摘　要

随着人工智能技术快速发展，公民个人信息的收集、分析以及利用面临全新挑战，人工智能应用的精准化、智能化以及自动化，致使大量公民个人信息被暴露，对个人安全形成威胁，现有的刑法保护在这一新情形下存在欠缺，在智能识别、数据挖掘等领域，现行法律难以有效应对人工智能应用里的个人信息侵害问题。本文在剖析人工智能应用中的个人信息保护现状与问题，参考国外立法经验的基础上，提出加强我国刑法对公民个人信息保护的建议，以强化对人工智能技术引发的新型侵权行为的规制，完善刑法的保护力度。

关键词

人工智能应用；个人信息；刑法保护；数据挖掘

1 引言

在智能化时代这个大背景之下，公民个人信息的敏感性持续不断提高，这与人身安全以及财产安全直接相关联，一旦个人信息出现泄漏的情况，说不定带来难以挽回的后果，在 2019 年的时候，国内有一家人工智能安防企业，因为大规模的数据泄露而引发了广泛的关注，这家公司运用人脸识别技术收集了大量敏感的个人信息，使得数据泄漏之后精准营销以及网络诈骗的风险有所加剧 [1]。随着人工智能不断向前发展，信息收集呈现出精准化、全面化、简便化以及隐秘化的趋势，公共领域当中暴露的信息数量急剧增加，这就加大了信息保护的难度。我国现行刑法在应对人工智能应用给个人信息造成的侵害方面存在不足之处，并且主要是以事后保护为主，没办法有效地避免信息泄露所带来的后果。本研究主要探讨的是怎样在人工智能应用当中完善个人信息的刑法保护，借助国外成熟经验，提出相应的改进举措 [2]。

【作者简介】王彦翔（2001–），男，中国山东招远人，在读硕士，从事刑法学研究。

2 强化人工智能应用中公民个人信息刑法保护的必要性

2.1 人工智能应用中公民个人信息刑法保护的不足

在人工智能的应用领域里，公民个人信息的刑法保护遭遇了诸多方面的挑战，现行的刑法在面对人工智能技术对个人信息进行收集、分析以及利用的情况时，存在着较为突出的缺陷，现有的“侵犯公民个人信息罪”主要是集中关注传统的侵犯行为，像是窃取个人信息、非法获取个人信息、出售个人信息或者提供个人信息等，然而却没能有效地覆盖人工智能应用所带来的新型问题 [3]。人工智能技术借助智能分析以及数据挖掘的手段，可对个人信息进行整合、分析构建个人画像，在这个过程当中的数据利用以及处理情况，往

往难以被现有的法律框架判定为犯罪行为，有许多涉及人工智能技术收集和使用个人信息的行为，并未受到刑法的有效规范和制约，刑法当中对于个人信息的定义以及范围缺少清晰明确的界定，在面对人工智能技术所涉及的生物识别信息等新型敏感信息的时候，现有的法律没办法给出明确的保护标准。这就导致对于一些高度敏感的个人信息，刑法无法及时且有效地做出反应。

2.2 其他部门法规制人工智能应用中公民个人信息侵权的局限性

我国对于公民个人信息的保护依赖于《个人信息保护法》等相关部门法规，这些法律主要借助行政手段来处理侵权行为，一般会采取责令改正以及罚款等举措，不过这些措施多数时候无法有效抑制侵权行为的发生，在面对涉及大规模数据处理的人工智能技术时，其处罚力度显得不够，现有的法规没能充分顾及人工智能应用所引发的新型侵权行为，像数据的精准分析与智能挖掘等，这些行为在传统的法律框架当中很难进行界定 [4]。公民个人信息的删除权和修正权尽管在《个人信息保护法》里有相关规定，但仅仅赋予个人请求权，并非强制性措施，这就导致侵犯行为一旦发生，个人信息的保护大多时候难以获得及时修复。

2.3 人工智能应用中已公开公民个人信息的刑法保护问题

虽然《个人信息保护法》针对已公开公民个人信息的处理作出了相关规定，然而在人工智能的应用领域，公开信息的再利用问题尚未得到全面妥善的解决，不少人觉得收集和整理已公开的个人信息是合乎法律规定的，然而实际状况较为复杂，人工智能技术往往借助深度学习以及数据挖掘等方式，对已公开的信息进行二次利用，而这种利用超出了用户最初所给予的授权范围 [5]。在此种情形下，怎样去界定信息的合法使用范围，以及当超出授权使用时怎样实施刑事处罚，成为了法律方面的一个现实难题，现有的法律对于已公开公民个人信息的二次授权以及合理使用标准并未作出清晰明确的界定，以至于在司法实践当中难以对这些问题进行处理，尽管存在一种观点认为，二次授权可充分尊重公民个人对于自身信息的处置权利，但是怎样合理区分第一次授权和第二次授权，在人工智能应用里信息的自动化处理与分析方面，成为了司法裁定过程中的难点所在。

3 人工智能应用中公民个人信息刑法保护的域外启示

3.1 美国个人信息的刑法保护

美国在个人信息保护方面构建了多层次的法律体系，虽然没有制定统一法律专门应对人工智能的影响，不过现有的刑法以及相关法规对个人信息保护起着关键作用，美国法律体系借助《隐私权法》等一系列法规，对政府及其他机构收集、使用与披露个人信息的方式进行了规范，美国的隐私保护法着重保障公民对个人信息的自决权，保证个人在信息被收集时拥有知情权以及修改权，还规定了违反这些权利应承担的刑事责任 [6]。这些法律的施行保证在个人信息获取与使用过程中，一旦出现未授权行为，就会面临严厉刑事处罚，然而尽管这些法律在一定程度上起到了保护效果，随着人工智能技术的发展，现行法律没能全面囊括所有可能的隐私侵犯形式，人工智能在数据挖掘和智能分析方面的应用。

3.2 德国个人信息的刑法保护

德国在个人信息保护方面构建了严格的法律框架，在刑法领域，虽说没有专门针对人工智能的法律，但现有的法律体系依旧可有效地应对人工智能应用过程中的个人信息保护问题，德国的《联邦数据保护法》以及《德国刑法典》都为个人数据的保护给予了详细的法律依据，《联邦数据保护法》规定所有处理个人数据的主体，不管是公共部门还是私人企业，都要遵循严格的数据保护规定，保证数据的收集、存储以及使用都符合法律要求。《德国刑法典》借助多项条款强化了对个人隐私的保护，比如针对未被授权收集、处理以及利用个人数据的行为，刑法设定了相应的刑事责任，要求从业者在获取数据之前要经过明确的授权 [7]。

3.3 对我国公民个人信息刑法保护的启示

在个人信息保护主体这一方面我国需要明确责任主体，美国与德国相关法律规定清晰明确，在不同领域针对从业者设定了个人信息保护义务，我国刑法中关于信息主体的规定并不明确，很多侵犯信息的行为缺少具体法律责任划分，使得法律适用存在较大自由裁量空间，其次我国应当考虑对隐私和个人信息实施双重保护，如同美国和德国那样将个人信息与隐私加以区分，制定针对不同类型信息的保护举措 [8]。如此做能提高刑法适应性，也能保证更细致的法律规制，另外对于滥用数据的行为，美国和德国已专门制定相关法律对滥用个人信息加以规制，我国刑法尚未涉及滥用数据犯罪，随着人工智能广泛应用，这一漏洞可能致使大量个人信息被滥用。

4 人工智能应用中公民个人信息刑法保护的完善措施

4.1 扩大侵犯公民个人信息罪的适用范围

在当下的法律框架之中，侵犯公民个人信息罪的适用范围呈现出一定的局限性，随着人工智能应用不断发展，个人信息的获取以及利用方式变得变得日益多样，传统刑法无法将所有新型侵权行为都囊括在内，扩大侵犯公民个人信息罪的适用范围十分必要，现有的法律主要对窃取、非法获取、出售以及提供个人信息等行为进行了规制，然而却没有充分考虑到非法利用行为 [9]。人工智能技术可借助大数据分析以及智能挖掘，从碎片化的个人信息里提取出有价值的数据，这种行为不一定涉及传统意义上的“窃取”或者“出售”，但其侵害性同样不容小觑，人工智能在信息处理方面所有的

智能化、自动化特性，致使数据的非法利用变得更为隐蔽且复杂，这种利用行为虽不会直接破坏信息的物理所有权，却对信息主体的隐私以及数据控制权产生了深刻影响。故而刑法应当将范围扩展至包含非法利用行为，明确对那些合法获取信息但未依照约定使用的行为给予规制。

4.2 前置完善：明确公民个人信息的概念范围

在人工智能的实际应用里，清晰明确公民个人信息的概念范畴是完善刑法保护的关键起始步骤，随着技术不断取得进展，人工智能有了收集以及处理大量数据的能力，信息的种类和维度变得越发多样广泛，目前来看，刑法针对个人信息的定义与分类依旧存在不清晰的地方，在如何区分“个人信息”与“隐私信息”的界限这一方面[10]。随着人工智能日益普及，个体的敏感信息，像是生物识别信息、轨迹信息等，变得格外关键，这些信息一旦出现泄露情况，说不定造成严重的社会危害，刑法需要细化并明确个人信息的层级分类，针对不同类型的个人信息制定相应的保护举措，基于此，可以参考《个人信息保护法》的信息分类方式，把隐私信息和其他关键信息区分开来，并且对其采取更为严格的保护手段。对于生物识别信息、医疗信息等高风险信息，刑法应当设定较低的入罪标准，以便在信息泄露或者被非法利用时可及时开展法律追责。

4.3 实质强化：明确人工智能应用平台的刑事法律责任

人工智能应用平台于处理公民个人信息进程里，负有相当严格的保护义务，要是平台没能履行这些义务，甚至还纵容侵犯个人信息的行为，那它就应当承担刑事责任，在人工智能平台牵涉个人信息泄露的案件中，平台的责任大多时候被忽视，一般只是对直接实施侵犯行为的主体给予处罚[11]。法律应清晰明确人工智能平台的刑事法律责任，把它归入帮助犯罪或者共同犯罪的范畴，平台要对自身行为负责，还得承担对其他侵权行为的责任，未履行信息保护义务的时候，应当视作不作为的帮助犯，与直接行为人共同犯罪，当下刑法在平台管理失当致使信息泄露的情形里缺乏明确规制，在过失泄露个人信息的状况中，尚未能全面落实刑事责任。

4.4 分类保护：已公开的公民个人信息的刑法规制

鉴于人工智能应用过程中存在的实际问题，为切实保护已公开的个人信息，刑法需依据信息公开程度划分不同保护类别，完全公开的个人信息处于信息主体事先授权或法律许可范畴，在此情形下，使用此类信息一般不被视作犯罪，然而对于限制开放的个人信息，即便信息已公开，其使用一般存在限制，超出授权范围的使用行为应受刑法惩处。这类信息囊括借助特定权限获取的个人数据，，尽管这些信息已进入公共领域，但信息主体仍享有删除、修正等权利，当这些已违法公开的信息再度被非法利用时，依然可依据侵犯公民个人信息罪给予处理，另外针对信息的公开程度与实际损害状况，法律应制定明确标准，防止司法实践中出现不同判决[12]。

5 结语

当下我国刑法对于保护公民个人信息方面存有一定欠缺，在人工智能应用里出现的新型隐私侵犯行为方面，经对美国以及德国相关法律的参考借鉴可发现，完善公民个人信息刑法保护的要点在于明晰法律责任主体、拓宽法律适用范围、细化信息分类保护标准以及强化人工智能应用平台的法律责任。当前，我国需加大对人工智能应用中公民个人信息的刑事保护力度，在已公开信息的使用与滥用问题上，借助法律的预先完善以及实质强化，可有效应对人工智能带来的隐私风险，同时保证公民的基本信息安全，未来随着法律持续完善以及技术进步，公民个人信息的保护会变得日益全面且有效。

参考文献 .

[1] 麦买提 · 乌斯曼,阿不都米吉提 · 吾买尔.人工智能算法个人信息利用刑法规制与个人信息安全刑法保护——从新型权利转向新型法益谈起[J].重庆邮电大学学报(社会科学版),2022,34(01):48-60.

[2] 张欢.人工智能应用中公民个人信息的刑法保护[D].北京交通大学,2023.

[3] [沈言,焦舒.数字经济时代侵犯公民个人信息的防控路径[J].人民司法,2022,(10):14-20.

[4] [叶小琴,王肃之,赵忠东.大数据时代公民个人信息可识别性认定模式的转型[J].法治社会,2021,(06):24-33.

[5] 张旭芳.人工智能时代侵犯公民个人信息犯罪研究——以犯罪情境为视角[J].河南警察学院学报,2021,30(02):38-44.

[6] 吕游.人工智能背景下的脑-机接口技术应用的刑事风险分析[J].犯罪研究,2020,(04):90-96.

[7] 刘国华,罗欣,张力之.论我国公民个人信息的刑法保护[J].黑龙江社会科学,2020,(04):108-113.

[8] 黄陈辰.大数据时代侵犯公民个人信息罪行为规制模式的应然转向——以“AI换脸”类淫秽视频为切入[J].华中科技大学学报(社会科学版),2020,34(02):105-113.

[9] 孙靖珈.侵犯公民个人信息罪的犯罪属性及对刑罚边界的影响[J].海南大学学报(人文社会科学版),2019,37(06):68-76.

[10] 缪文升,蒋浩.人工智能时代公民信息数据利用与保护的动态平衡[J].公安研究,2019,(09):69-74+91.

[11] 董琼丽.大数据背景下公民个人信息的刑法保护[D].云南大学,2021.

[12] 李宁乐.论大数据背景下公民个人信息的刑法保护[D].郑州大学,2020.