大数据时代公民隐私信息的刑法保护方法

◆丁　旋

（西北政法大学法治学院，陕西 西安 710063）

【摘要】在大数据时代，随着科技的快速发展和数字化信息的广泛应用，公民隐私信息面临着前所未有的威胁和侵犯。为了维护公民的隐私权利和保护个人信息安全，刑法保护成为一种重要的手段。本文旨在探讨大数据时代公民隐私信息的刑法保护方法，在阐明隐私信息基本内涵的基础上，表明公民隐私信息保护的重要性。通过提出审慎平衡的原则，从法律界限的明确性与适用性的考量，法律标准与科技发展的同步性的平衡，刑事处罚与预防措施的合理性等方面，达成公民隐私信息的保护和科技进步推动之间的平衡。以期适应大数据时代的公民的信息保护需求，进而维护公民的隐私信息。

【关键词】隐私信息；法律界限；法律标准；刑事处罚

大数据时代，个人信息的重要性越来越受到关注。由于大数据时代对个人信息处理范围、利用方式的拓展，个人信息被侵犯的范围也随之扩大。例如，在互联网环境中，个人信息会被用于广告营销、骚扰电话、垃圾邮件等方面。因此，刑法对个人信息的保护必须结合大数据时代个人信息处理与利用方式的变化展开。但是，由于当前刑法对公民隐私信息保护规定较少，且相关司法解释不够明确与具体，导致在面对上述变化时难以形成统一、合理的标准。例如，在“非法获取计算机信息系统数据罪”中，就存在合法收集与利用公民隐私信息与非法收集利用公民隐私信息之争。这些问题都表明了当前刑法对个人信息保护存在着一定的困境。因此，有必要在明确大数据时代个人信息处理与利用方式变化的基础上对刑法对公民隐私信息保护提出合理建议。

一、大数据时代的隐私信息

隐私信息，即在传统法律领域中被认为具有隐私属性的信息。在传统的法律中，个人信息的保护主要通过隐私权进行保护。在隐私权被确立为一项基本权利后，人们对个人信息的保护也逐步由对隐私权的保护转变为对个人信息的保护。随着科技的发展，人们逐渐认识到网络环境下个人信息收集、处理和利用方式发生了巨大变化。互联网的普及改变了传统个人信息收集和处理的方式，使得个人信息被收集和处理方式更加多样，同时也导致了公民隐私保护面临着新挑战。在大数据时代，人们获取个人信息的途径更加广泛、形式更加多样、处理更加频繁。因此，需要对这些新出现的隐私信息进行分类与界定，以确保刑法对这些隐私信息进行保护。

（一）隐私信息的内涵

在我国对于隐私信息的内涵，学界没有统一的认识，主要有以下几种观点：第一种观点认为隐私信息是指“不愿为他人知晓或知晓程度较低的信息”；第二种观点认为隐私信息是指“公民在社会生活中不愿被他人知道或知晓的个人信息”；第三种观点认为隐私信息是“公民不愿为他人知晓或知晓程度较低的个人信息”。综合以上观点，笔者认为，在大数据时代背景下，隐私信息是指公民在社会生活中不愿为他人知晓或知晓程度较低的个人信息，具体而言主要包括以下几类：公民的行踪轨迹、通讯录、生活记录等；公民在互联网上发布的关于自己或他人的日记、信件、照片等；公民在互联网上发表的对社会热点事件和现象进行评论和评价的文章。

（二）隐私信息在刑法上的保护范围

我国《刑法》第 253 条之一规定：“违反国家有关规定，向他人出售或者提供公民个人信息，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。”刑法对于侵犯公民个人信息犯罪行为的规定比较原则，使得司法实践中对侵犯公民个人信息犯罪行为的认定存在较大困难。为了更好地打击侵犯公民个人信息犯罪行为，本文认为对于侵犯公民个人信息犯罪行为的认定可以根据不同类型的个人信息采取不同的标准进行认定。具体而言，侵犯公民个人信息犯罪行为可分为两类：一是违反国家有关规定，向他人出售或者提供公民个人信息的行为；二是窃取或者以其他方法，非法获取公民个人信息的行为。

二、公民隐私信息保护的重要性

公民隐私权的保护是现代社会法治和个人权利保障的重要组成部分。公民隐私信息保护是个人权利的体现，每个人都有权决定自己的个人信息是否被他人获取和使用。作为个人的基本权利之一，隐私权是个人对于个人信息的自主

控制权。 公民的隐私权受到保护，能够确保个体的尊严和自由，使其能够享受基本的权利和自由。 公民隐私信息保护对于个人社交和信任关系的建立至关重要。 人们在社交媒体上分享大量的个人信息，而这些信息可能被滥用和泄露。 一旦公民无法信任自己的隐私信息得到保护，他们将越来越谨慎地选择分享信息，从而影响社交互动和信任基础。

公民隐私信息泄露和滥用可能导致身份盗窃、欺诈行为、网络犯罪等问题的增加，给社会秩序和经济发展带来不利影响。 保护公民隐私信息有助于维持社会秩序，促进经济发展，并提高人们对科技和数字化的信任。 个人隐私权的保护有助于确保公平竞争和创新环境，在个人信息得到妥善保护的情况下，企业和组织能够合法、透明地收集和利用这些信息，促进科技发展和社会进步。 同时，法律对于保护公民隐私权和惩治侵犯隐私行为的规范起到重要作用，公民隐私信息保护法律的健全和有效执行，可以维护公正、公平和法治的社会秩序。

三、公民隐私信息刑法保护与科技发展的协调

(一)法律界限的明确性与适用性的考量

为了解决公民个人隐私信息保护中的法律界限问题，需要明确规定侵犯公民隐私的行为范围。 随着科技的不断创新和进步，新型的侵犯公民隐私的手段层出不穷，刑法规定应及时更新和完善，以覆盖新兴的隐私侵犯行为。 例如，在网络空间中出现的个人信息偷窃、网络钓鱼等新案例，应设立相关罪名，如个人信息盗窃罪、网络钓鱼罪等，并规定相应的刑判标准，确保对违法行为能够给予适当的刑事处罚。 法律界限的适用性对于协调公民隐私信息的刑法保护与科技发展非常关键。 在完善刑法保护法规时，需要考虑到不同科技场景下的实际应用情况。 例如，在人脸识别和数据挖掘等新兴技术的应用中，应该明确个人隐私信息的保护原则，明确数据收集、使用和存储的要求，以及对违法行为的刑事责任。 同时，根据科技的快速发展，及时更新法律法规，权衡公民隐私权与科技发展之间的利益，确保刑法规定能符合科技发展的要求，并保护公民隐私信息不受滥用。

随着科技的迅速发展，不断涌现出新的技术和应用，导致旧有的法律界限可能不再适用或存在漏洞。 因此，应该建立由行政部门、学术界、业界等多个利益相关方共同组成的专门机构，负责监督和评估现有法律体系中出现的法律不足，确保多方利益的平衡。 通过定期跟踪和研究科技发展的趋势与前沿的方式，深入了解新技术的特点和应用，预测可能出现的法律漏洞并及时调整法律界限。 机构还应该定期的法律审查，评估和检查刑法规定与科技发展的契合度，包括对相关法律条文的调整、修订或废止，以适应新兴技术和应用的需求。 在法律审查过程中，鼓励各部门之间的合作与协同，促进知识共享，确保刑法保护方法能够持续适应科技发展和社会变革。 同时，为了提高公民隐私信息刑法保护与科技发展的协调性，行政部门和科技行业应建立紧密合作的机制，共同监管和引导科技发展。 行政部门可以与科技行业建立对话渠道，了解其技术发展趋势和挑战，并及时调整法律框架和监管政策。 科技行业可以积极配合，主动参与并遵守相关法律法规的要求，确保科技发展在符合法律和道德标准的范围内，进而确保科技发展与个人隐私权利之间的平衡，并为社会的可持续发展提供更好的支持。

(二)法律标准与科技发展的同步性的平衡

随着大数据、人工智能和互联网等技术的广泛应用，公民个人隐私信息的保护面临了更多的挑战。 在制定公民隐私信息的刑法保护方法时，需要综合考虑法律标准与科技发展之间的关系，以实现公民隐私信息的刑法保护与科技发展的协调和平衡。 在制定公民隐私信息刑法保护方法时，应充分理解和分析科技的具体应用场景和潜在风险，包括人脸识别、数据挖掘、智能家居等，理解这些科技的具体功能、数据流程以及潜在的个人隐私风险，制定相应的法律措施以平衡个人隐私与科技发展之间的关系。

科技企业在大数据和人工智能领域扮演着关键的角色，承载着大量的个人隐私信息。 因此，要求科技企业加强自身的内部监管与合规机制，确保公民隐私信息的安全和保护。 科技企业应该组建专门的隐私保护团队，负责制定和执行隐私保护策略，并提供合规咨询和指导。 为员工提供必要的隐私保护培训，确保他们了解隐私保护的重要性，并具备相关的法律和伦理知识。 向用户公开收集、使用和存储个人隐私信息的目的、方式和范围，并尊重用户的隐私意愿，提供选择权和控制权。 同时，行政部门应加强对科技企业的监管，建立和完善个人信息保护的法律法规体系，明确科技企业在收集、使用和存储个人隐私信息时的责任和义务。 加大对违反隐私保护法律法规的行为的惩处力度，提高违法成本，对违法行为实施严格执法。 组织各方合作，制定相关行业标准，明确科技企业在个人隐私信息保护方面的最佳实践，引导行业按照规范和标准进行操作。 加强对科技企业的监督和审查，确保其遵守隐私保护法律法规和行业标准，防止滥用个人隐私信息，规范科技企业的用户隐私权保护和数据安全措施。

(三)刑事处罚与预防措施的合理性

有效的刑事处罚是确保公民隐私信息刑法保护有效性的重要手段之一。 针对公民隐私信息的非法收集、使用和泄露行为，必须建立明确且具有威慑力的刑事处罚措施，以保护公民隐私权益和社会秩序。 例如，将严重的隐私侵犯行为纳入刑事犯罪范畴，确保涉及严重隐私侵犯行为的构成要

件和刑事责任规定明确清晰，对于严重侵犯公民隐私的行为适当增加刑事处罚力度，提高刑事法律对侵犯公民隐私行为的威慑力。

为了实现公民隐私信息刑法保护与科技发展的协调，优先考虑预防措施的合理性和有效性。行政部门应制定和完善相关的法律法规，明确个人信息的合法收集和使用范围，并规定违法行为的惩罚措施。法律法规应适应科技发展的新变化，及时对个人隐私保护的问题进行界定和规制。个人同意原则是个人隐私保护的核心原则之一，也是确保个人权益得到充分尊重的基础，确保企业和组织在收集、使用和存储个人信息时首先获得个人的知情同意。对于涉及高风险的数据处理活动，可以采取加密、脱敏等措施降低安全风险，确保个人信息的存储、传输和处理过程中的安全可控。

刑事处罚与预防措施在公民隐私信息刑法保护中需要相互配合和补充。刑事处罚主要针对已经发生的违法行为，起到惩罚作用，对于那些恶意侵害公民隐私信息的行为应该给予严厉的刑事处罚，以维护社会公正和秩序。预防措施则更侧重于避免违法行为发生，通过加强监管、提升个人隐私保护意识、完善技术手段等措施预防公民隐私信息的侵权行为。加强对违法行为的监督和打击力度，坚决依法查处侵犯公民隐私信息的刑事犯罪行为，确保公民的隐私权益得到充分保护，并促进科技与法律的协调发展。

四、结束语

随着信息技术的快速发展，个人信息保护已成为人们关注的热点。然而，法律保护与社会利益之间并非完全对立，法律保护也并非对社会利益的全盘否定。对个人隐私信息进行刑法保护，是在保护个人信息的同时兼顾社会公共利益。在大数据时代背景下，公民隐私信息在网络环境中的大量流动使得个人信息呈现出巨大的价值，而如何将这些价值进行合理保护是刑法需要面对和解决的问题。在个人信息刑法保护中，通过法律界限的明确性与适用性的考量，法律标准与科技发展的同步性的平衡，刑事处罚与预防措施的合理性等方面对侵犯公民隐私信息的行为进行刑法评价，使刑法达到公民隐私信息合理保护的目的。

参考文献：

[1]狄振鹏，姜士伟.大数据时代政府数据开放与公民隐私保护问题研究[J].情报杂志，2022，41(02)：155-159，118.

[2]娄宁.大数据时代公民个人信息法律保护存在的问题和对策[J].公民与法(综合版)，2021，13(02)：32-36.

[3]郭秉贵.大数据时代信息自由利用与隐私权保护的困境与出路——以“中国Cookie隐私第一案”为分析对象[J].深圳社会科学，2021，4(04)：110-119.

[4]付玉明.大数据时代个人信息的刑法保护——基于日本法的比较分析[J].国外社会科学，2022，45(05)：58-71，195.

[5]刘双阳，李川.大数据时代个人信息法益刑法保护的应然转向——以规制非法使用个人信息为重点[J].重庆大学学报(社会科学版)，2022，28(06)：231-242.

[6]从传锋，杨桢.基于大数据模式分解的隐私信息保护方法仿真[J].计算机仿真，2021，38(06)：251-254，433.

作者简介：

丁旋(1995－)，女，汉族，山东青岛人，硕士研究生，研究方向：法学、狱政管理。