Dispute Settlement 争议解决, 2025, 11(12), 18-26
Published Online December 2025 in Hans. https://www.hanspub.org/journal/ds
https://doi.org/10.12677/ds.2025.1112365

Hans汉斯

大数据背景下个人信息民法保护研究

王婷婷

北京林业大学人文社会科学学院，北京

收稿日期：2025年11月7日；录用日期：2025年11月26日；发布日期：2025年12月9日

摘　要

随着大数据技术的不断发展，个人信息的搜集和使用范围日益广泛，在便利人们日常生活的同时，现阶段个人信息保护仍面临诸多挑战。个人信息非法泄露，非法收集和买卖现象等频频发生，个人信息保护与大数据应用需求之间的矛盾仍然存在，相关法律保护制度也不够完善。我国目前没有设立相关的个人信息保护专门机构，人工智能、区块链等新兴技术的发展也使得新的问题不断涌现，与此同时个人信息的范围也不断扩展，但我国目前没有形成一个统一的个人信息的界定标准。此外，大数据控制者的权利义务和个人信息侵权案件的归责原则也都需要进一步的完善。本文研究的侧重点，主要在于深入探讨民法对于个人信息保护的规定和制度，以及个人信息保护实践中面临的现实问题和挑战，探讨个人信息保护与时代背景接轨发展的有效途径，希望能够为我国法律和制度的完善提供思路和建议。

关键词

大数据，个人信息，民法

Research on the Civil Law Protection of Personal Information in the Context of Big Data

Tingting Wang

School of Humanities and Social Sciences, Beijing Forestry University, Beijing

Received: November 7, 2025; accepted: November 26, 2025; published: December 9, 2025

Abstract

With the continuous development of big data technology, the collection and use of personal information is becoming more and more extensive, and while facilitating people's daily life, personal

文章引用: 王婷婷. 大数据背景下个人信息民法保护研究[J]. 争议解决, 2025, 11(12): 18-26.
DOI: 10.12677/ds.2025.1112365

information protection still facing many challenges such as the Illegal information leakage, illegal collection and trading also occur frequently, the contradiction between personal information protection and big data application still exists, but the relevant legal protection system is not perfect. China has not set up relevant personal information protection special institutions. The development of artificial intelligence, block chain and other emerging technologies has also made some new problems continue to emerge. At the same time, the scope of personal information is also expanding, but China has not formed a unified definition standard for personal information. In addition, the rights and obligations of big data controllers and the principle of attribution of personal information infringement cases also need further improvement. The focus of the research is mainly to deeply explore the provisions and systems of the Civil Law on personal information protection, as well as the practical problems and challenges faced in personal information protection practice. It explores effective ways for personal information protection to develop in line with the background of the times, hoping to provide some useful ideas and suggestions for China's laws and systems.

Keywords

Big Data, Personal Information, Civil Law

1. 引言

大数据背景下，电子产品的广泛应用和普及，使得数据的产生速度骤然增长，这些设备时刻记录着大量用户信息数据。对这些数据的合理的收集、分析和利用，一方面可以为人们生活带来极大便利，另一方面使得个人信息更加具有社会价值，甚至成为社会公共资源。但与此同时个人信息被无限度挖掘、非法滥用等案件日益增长，个人信息安全受到严峻挑战。大数据时代个人信息的范围如何界定?如何平衡大数据背景下的社会发展和个人信息的法律保护机制问题?如何规范大数据控制者的权利?这些问题值得我们深思。

2. 大数据背景下个人信息保护概述

2.1. 大数据背景下个人信息的界定

大数据背景下我国个人信息保护的界定主要有以下三种。

2.1.1. 识别说

识别说将个人信息定义为能够识别出特定个人的信息。具体来说，识别又分为“已识别”和“可识别”两种情况。更通俗一点的理解就如谢琳教授所说的[1]“已识别也称直接识别，指直接能识别出某一特定的人的信息，例如个人身份证号码。而‘可识别’则为间接识别，主要指存在识别信息的可能性。”由此可知，若几个信息相结合起来能够识别出特定个人，就属于间接识别。早期直接识别标准的支持者并不认同间接识别的方法，他们认为，不能直接识别特定的人的信息，不属于个人信息。

然而，在大数据时代，个人信息范围的扩展催生了间接识别标准的出现。大量高科技设备渗透进人们的生活，人们通过人工智能产品与外界联系时，难免产生大量数据。多个信息相结合便加大了识别出特定人的可能性。其次大数据后台通过对用户的画像分析，也加大了用户的可识别性。笔者认为可识别

标准与已识别标准相比较，把个人信息的范围进行扩大，更加与时俱进，更加适应社会发展。

2.1.2. 关联说

关联说将个人信息定义为与特定个人具有相关性的信息。学术界早期关联说观点认为，能够反映出特定人的身体，性格，社会评价等特征的信息属于个人信息[1]。但在大数据背景下，技术不断的迭代更新使得曾经不具有相关性的单个信息与其他信息整合起来可以形成更具体的用户画像，极大地增加了确定特定个人的可能性，这就使得个人信息的界定范围不断扩大，典型代表为大数据杀熟现象。目前学界的主流观点认为大数据时代的个人信息的界定应该采用最广泛的范围，如此才能与时俱进，更全面的保护公民的合法权益。

2.1.3. 识别说和关联说相结合的方式

《个人信息保护法》[1]颁布之前我国基本以“识别说”作为个人信息的界定标准，2021 年颁布的《个人信息保护法》第四条规定“个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息”。在强调信息的识别性同时也强调信息的相关性，这体现了识别说和关联说相结合的保护方式。这从侧面说明了用二者相结合的方式来界定个人信息符合我国的国情，也顺应时代的发展。但我国目前并没有明文规定用何种方式来界定个人信息，因此笔者建议把识别说与关联说相结合的方式规定为个人信息的判断标准。

2.2. 大数据背景下个人信息的特征

1) 以授权为基础：保护个人信息需要遵循个人意愿的原则，即在事先获得个人的自愿授权下进行信息的收集、存储、传输和使用。

2) 实时性：在互联网时代，信息流转的速度很快，个人信息的变化也非常快速，因此个人信息的变化实时性很高。

3) 多元化的保护方式：单一的保护模式已经不能完全解决所有问题，个人信息保护需要多元化的保护方式，如：技术手段、制度保障、法律规范等，来保障个人信息的安全。

4) 新的问题不断涌现：由于技术不断进步，新的问题不断涌现，如人脸识别、算法歧视和数据泄露等，也需要及时完善法律保护措施。

5) 跨地域传输和保护：大数据时代，信息的传输已经不再局限于一个国家或地区，因此信息的保护也需要跨越地域的限制，遵循国际通行的个人信息保护规范。

2.3. 个人信息保护的必要性

1) 加强个人信息保护能够更好地适应大数据时代的发展在大数据背景下，智能化的应用正在不断加速发展。大量的个人信息分布在各种 App、网络等平台、设备上，并且在很多情况下被收集、分析、利用，用于商业推销、行为跟踪和风险评估等方面。在这种时代背景下，加强个人信息保护变得十分重要。

2) 个人信息保护是维护公民权利的必然要求

大数据时代，不同机构和企业的数据管理和存储技术的水平和安全措施也各不相同，个人信息侵权案件频发，公民的隐私权、财产权、肖像权等公民权利面临严峻危险，加强法律保护是保障公民信息安全的必然要求。

3) 个人信息的保护也是维持市场秩序，促进公平交易的重要保障

如果企业通过非法获取用户信息而获取商业优势，那么就会对市场公平竞争造成不正当的影响。加

[1]《中华人民共和国个人信息保护法》网址：http://www.npc.gov.cn/npc/c2/c30834/202108/t20210820_313088.html。

强个人信息的保护有利于促进更加公平的市场竞争环境的形成。

3. 大数据下国内外个人信息保护原则和保护模式

3.1. 欧盟个人信息保护原则和保护模式

3.1.1. 欧盟个人信息保护原则：公民权利保护至上原则，设立个人数据权

欧盟各国的个人信息保护体现出浓厚的公民权利保护色彩，欧盟《通用数据保护条例》的颁布，使个人数据权与隐私权有了明确的界分。欧盟的个人数据权体现了强烈的公民权利保护属性[2]。相较于传统的隐私权个人数据权更能适应技术的快速发展，为欧盟公民提供更强有力的保护，尤其是对个人数据所体现出的隐私的保护。其次《欧盟基本权利宪章》中也规定了与个人信息有关的内容，宪章将个人信息权视为人的基本权利，是公民权利的重要组成部分，体现出强烈的保护色彩。

3.1.2. 欧盟个人信息保护模式：赋予权利同时设定义务，政府与个人共同主导

在大数据时代，欧盟采取了强有力的措施来保护个人信息。首先欧盟对个人数据权的权利内容做了详细的安排，具体来说包括权利人要被告知，可以接触数据的权利；请求修改的权利，以及信息主体的删除权和信息主体的拒绝权等内容。此外，还规定数据运营者应当承担对应的实质性义务等，但是欧盟并未采取简单的赋权模式将个人数据权赋予个人，而是强调国家或政府机关也要履行一定的保护个人数据的义务。

综上所述，欧盟在个人信息保护方面体现出两点特色，首先是欧盟设立了单独的个人数据权，形成了比较完备的保护体系，并从立法上理清了与隐私权的界限，其次是欧盟个人信息保护公民参与与国家调控相结合，很好的调动了公民的积极性，但我国目前并没有形成统一的个人信息保护体系，此外公民的个人信息保护意识淡薄，因此欧盟的举措对我国具有重要的借鉴意义。

3.2. 美国个人信息保护原则和保护模式

3.2.1. 美国个人信息保护原则：强调自由和限制政府权力原则

美国个人信息保护制度对政府机关收集个人信息的行为进行了严格限制。同时给公民最大程度的权利自由。例如美国法律规定了沉默权，赋予了美国公民审判时对涉及隐私的信息可以保持沉默的权利。美国法律还规定了正当程序原则来约束司法机关的司法行为，比如未经允许美国法院不能随意查看犯罪嫌疑人的手机，因为手机里面有大量个人隐私数据。此外美国的《隐私法案》对政府收集处理个人信息做了详细的规定，其中包括只有当事人同意的情况下政府才能进行信息公开、公民有权知道被收集的个人信息的用途等。这些规定体现出美国强调自由和限制机关权力的个人信息保护原则。

3.2.2. 美国个人信息保护模式：将个人信息定性为财产权，在不同领域分类治理

美国将个人信息定性为财产权，并允许公民将个人信息数据作为商品进行交易，并获取收益。由此可知，与欧盟的浓厚的保护色彩相比，美国采取的是完全相反的保护模式。并且美国个人信息保护呈现出分类治理的特点，美国虽然没有统一的法案，但是针对不同行业的不同特点，它有不同的个人数据保护规定，如《家庭教育权利与隐私法》规定了教育机构有义务确保其记录中任何可识别的个人信息不被泄露等教育领域的个人数据保护内容；如《联邦有线通讯政策法》规定了电讯公司必须遵守合理信息实践原则，未经本人同意不能收集其个人信息等有线通信领域的个人数据保护内容；此外，还有诸如《儿童网上隐私保护法》《视频隐私保护法》等法规都规定了对应主体收集利用个人数据应该遵守个人数据保护规定。

综上所述，美国在个人信息保护方面更加强调公民自由和限制政府机关，同时将个人信息定性为财

产权，在不同领域分类治理。这对我国具有重要的借鉴意义，大数据时代，我国单一的处理原则已经无法解决全部的侵权问题，美国的分类治理对我国具有重要的借鉴意义，并且关于如何更好地平衡个人信息保护与信息数据资源的合法利用这方面，美国已经进行了先行探索，我们应该充分吸收其中的经验和教训，促进个人信息法律保护的不断发展。

3.3. 我国个人信息保护原则和保护模式

3.3.1. 我国个人信息保护原则：知情同意原则 + 目的限制原则

关于我国处理个人信息的基本原则，学术界的主流观点为知情同意原则，然而，经过实践的验证，以“告知–同意”为核心的这种个人信息处理方式已经无法适应当下的需求，一来大数据时代技术不断革新，二来个人信息种类和数量不断增加。如果持续采用这种个人信息的处理模式，是无法完全解决个人信息侵权案件的问题的。在共享资源的大趋势下，盲目遵循“告知–同意”原则反而会变得教条主义，程序僵硬，这显然不利于数据的快速运转和流通。所以我们不得不承认我们已经陷入了“同意为王”的困境[3]。目前逐渐有学者提出不再笼统适用个人信息保护法，而是将它进行细化分类，在不同领域分类处置。

目的限制原则是个人信息处理的另一重要原则。目的指的是，任何个人和集体在收集个人信息之前，必须得明确自己的使用目的。限制指的是限制使用范围数据使用者对个人信息的使用不得超出法律规定的范围，不可胡乱使用。目前，我国对于使用限制的判定标准采取的是“关联性”。

但是，遗憾的是，关于“关联性”，它的具体内涵，表现形式，应用的范围，我国立法并没有给出明确的规定。我国《个人信息保护法》对于个人信息保护的保护范围主要集中在与特定个人具有“直接关联性”的信息上，对具有“间接关联性”的信息关注较少。然而，随着时代的发展，大数据的盛行，《个人信息保护法》出现了一丝局限性。

3.3.2. 我国个人信息保护模式：政府主导与技术防护相结合

我国个人信息保护模式：目前中国的个人信息保护模式为政府主导与技术手段相结合。政府设立了数据保护机构集中管理，如国家网信办，负责监管和管理个人信息的收集、使用和保护；另外，对公司企业的监管方面，各行业主管部门设立实名制、强制执行数据报告审查制度，要求企业和组织必须严格遵守，以促进个人信息保护的贯彻执行。我国还颁布了《数据安全法》[2]，明确要实施大数据战略，促进数据的开发利用。

在技术防护方面，政府、企业和组织采取一定的技术手段和措施，如信息加密、身份验证、数据备份和存储等，来防范个人信息泄露和滥用。同时还推进风险规制机制进行防护，通过对风险的评价和技术分析合理规避风险。

综上所述，通过对个人信息保护现状的研究可知，我国目前对个人信息还没有形成统一的界定标准。此外保护的范围不全面，主要集中在直接关联性信息上。在保护模式上以政府保护为主，政府采取了很多保护措施，管理较分散，并没有形成专门的保护机构集中管理。在技术防护上也没有形成统一的数据储存系统。

4. 我国个人信息民法保护存在的问题

4.1. 大数据背景下民法个人信息保护范围不全

大数据时代，现有的个人信息保护相关立法内容仍然不完善，笔者认为其存在以下两点问题。

[2]《中华人民共和国数据安全法》网址：http://www.npc.gov.cn/c2/c30834/202106/t20210610_311888.html。

4.1.1. 匿名化处理后仍能够通过技术手段识别的信息未纳入保护范围

《个人信息保护法》明确规定了“匿名化处理后的信息”不属于个人信息[3]，这是因为根据立法时的社会环境和技术水平，匿名化处理后的信息大多无法被识别，安全系数较高。

《个人信息保护法》自2021年11月1日起施行，随着时间的推移，法律逐渐出现一些新的漏洞，笔者认为基于目前的大数据分析技术，匿名化处理的信息已经不再是百分百的无法被识别，技术的革新和进步导致匿名处理逐渐失去绝对化意义，匿名的相对性成为趋势。此外，可以推断出随着识别技术的发展，现阶段不可识别的信息，未来并非不能识别，因此匿名化处理并不能够将信息被识别的风险降低为零。也就是说匿名化处理并不能彻底切断公开信息与特定个人的相关性，即匿名化无法完全消除可识别的风险，这使得我国法律在个人信息保护领域出现空白区域，因此将匿名化处理后仍能够通过技术手段识别的信息纳入保护范围具有现实意义。

4.1.2. 开源情报中仍然能够间接确定特定个人的碎片化信息未纳入保护范围

开源情报指的是公开发表，可公开访问下载的所有公开资源，最主要的作用是满足国家、政府、国际组织、执法部门等的工作需要。这些信息可以在线或离线、或者广泛存在开放式的无线电波和各类纸质资料上找到。包括但不限于：互联网论坛网站、GPS数据、数字认证信息、学术出版物、个人简历等。

但是开源情报并不会有选择的提取信息，而是全面的直接的挖掘所有可获取的信息，公开的信息虽然经过匿名化或者加密，脱敏，去标识化等技术处理而模糊其可识别性，但是并不能彻底切断公开信息与特定个人的相关性，仍然存在多个被模糊处理的信息进行拼凑能够识别出特定相关人员的现象。开源情报中可间接识别个人身份的信息属于开源情报的超范围收集，如果不加以保护就会导致个人信息保护出现真空。

4.2. 对大数据控制者的民法约束规范不完善

由于技术的发展，出现了大数据杀熟，大数据保险风控，滴滴泄露地图和用户数据为代表的大量个人信息侵权事件。这体现出我国对大数据控制者的的法律约束规范并不完善，主要存在以下两点问题。

第一个问题是数据主体在知情、同意、修改、删除等方面的权益得不到充分保护。大数据控制者对数据平台的后台操作痕迹在难以捕捉和取证的同时又缺乏相应的法律规范进行约束[4]。种种情况使得大数据控制者的违法行为达不到有效地打击力度。这无形中提高了对大数据控制者的道德期待，更加凸显出法律约束的缺位。

第二个问题是缺少科学合理的法律原则来规范数据的收集行为。由于大数据产业发展迅速，大数据控制者在获取数据时，通常会披上合法的外衣来进行远远超越此合法权限的数据收集行为。并且我国法律也没有对个人信息保护的监管责任和义务做出完善的规定，现实生活中的监管体系跟不上，监管手段和能力也相对较弱，难以对大数据控制者实时监管和约束，这就使得超过合理必要限度的数据收集行为得不到强有力的打击。

4.3. 现有立法无法满足区块链、人工智能等新兴业态的保护需求

2022年12月9日发布的《最高人民法院关于规范和加强人工智能司法应用的意见》[4]对我国人工智能、区块链等新领域的个人信息权利保护作出了相关规定，但这些规定依然是笼统而且概括性的，我国

[3]《个人信息保护法》第四条规定：“个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。”

[4]《最高人民法院关于规范和加强人工智能司法应用的意见》中规定：“禁止使用不符合法律法规的人工智能技术和产品，司法人工智能产品和服务必须依法研发、部署和运行，不得损害国家安全，不得侵犯合法权益，确保国家秘密、网络安全、数据安全和个人信息不受侵害，保护个人隐私，努力提供安全、合法、高效的智能化司法服务。

并没有专门且具体的法律来规范人工智能、区块链等新兴业态里收集、利用个人信息的行为。

笔者发现目前在人工智能、区块链领域依然存在以下两点问题：

第一，侵权主体难以明确，给权利救济造成阻碍。传统的数据管理方式往往是中心化的，数据往往存储在中心节点上[5]。而区块链和一些人工智能技术则是去中心化的存储方式，每个节点都存储了全部或部分的数据，并且在区块链、人工智能等技术里，数据往往是由多个参与者共同管理和维护，这就增加了确定侵权主体的难度。

第二，智能合约存在法律风险。智能合约是一种自动执行合约的方法，若合理的运用则会对研究个人信息的保护与合理利用之间的平衡关系产生有利的推动作用，但目前的现实情况是智能合约的编写者往往没有法律经验，因此智能合约运行过程中可能会存在一些法律风险。

4.4. 现有个人信息侵权案归责原则单一

我国法律采用过错(推定)原则对侵害个人信息的行为进行归责，即推定其有过错，如果不能证明自己没有过错，则需要承担侵权责任。但是在具体的侵犯个人信息的行为中，个人信息侵权主体众多，只单一的使用过错推定原则进行规则实际上并不能完全保护被侵权人的权益。当可以明确判断侵权事件过错方时，采用过错推定原则，推定其有过错显得毫无意义。就比如商家因差评擅自公布消费者个人信息时，商家的行为无需进行推定，可以直接认定侵权。此外政府等国家机关的工作人员的行为，代表国家意志，因此当发生侵犯个人信息行为的时候，采用过错推定原则不太妥当，由政府承担无过错责任显得更为合理。

5. 大数据背景下个人信息民法保护的建议

5.1. 完善个人信息立法保护

我国虽然已经相继出台了《民法典》《数据安全法》《个人信息保护法》等多部相关法律，但仍然不够完善，在立法上需要进一步提高。

5.1.1. 填补立法漏洞

笔者认为目前个人信息保护的完善立法内容不完善，主要针对大数据控制者和人工智能区块链等新兴业态两方面提出一点建议：

首先对大数据控制者，建议加强数据主体权益保护，明确数据主体的权益和责任，规定数据主体的知情、同意、修改、删除权等权利。加强对违法处理数据行为的处罚，明确数据控制者不得以任何形式获取和使用用户的数据，同时切实加强对数据的管理和监管。

其次对区块链和人工智能等新兴领域，建议采取分类治理的方法，具体问题具体分析。应按照实际标准判断义务主体，明确只有对信息处理的目的和方式产生实质影响，才能成为法律规定的义务主体。若信息主体选择区块链服务仅是为了单纯使用某项服务，如信息备份等，而并未作为节点参与到共识机制对其他信息处理产生实质影响，则不能苛责其承担安全保障、应急处理等义务。

5.1.2. 扩展个人信息保护范围

经前文论述，笔者认为当前个人信息的法律界定范围不全，随着大数据的发展，新的问题接踵而至，许多新的个人信息领域并未纳入保护范围。于是导致现实的问题和滞后的法律规范之间矛盾的出现。

《个人信息保护法》中规定个人信息不包括匿名化处理后的信息。笔者认为应当将不包括匿名化处理的信息分类讨论，将匿名化处理后仍能够通过技术手段识别的信息和开源情报中仍然能够间接确定特定个人的碎片化信息这两点排除在《个人信息保护法》第四条中的“匿名化处理的信息”范围之外。

5.1.3. 采用多元化个人信息侵权案件归责原则

在大数据时代，个人信息侵权类型多样。仅仅用过错推定原则来对侵犯个人信息的主体进行归责，并没有考虑到不同主体之间信息处理能力的差异。笔者建议不同类型的个人信息分开处理，采取不同的标准适用个人信息处理原则[6]。不断细化个人信息侵权救济制度，采用多元归责体系对个人信息主体进行归责，对一般信息主体侵犯他人个人信息权益时，采用一般过错原则进行归责。对于国家机关采用无过错责任原则，对于互联网平台等具有一定技术优势的主体，采用过错推定原则进行归责。

5.2. 设立专门法律机构

我国个人信息保护体系较为分散，个人信息的采集、存储、转移、利用等环节都没有相应的具体规范。设立专门的个人信息保护机构有利于更规范更全面更高效的处理个人信息侵权案件。日本与韩国与我国的历史文化背景更为相似，两国的个人信息保护举措对我国具有重要借鉴意义。日本设立了“个人信息保护委员会”这个独立监管机构，监管与个人信息处理相关的事项。韩国也设立保护委员会和调解委员会这样专门的机构，对有关个人信息案件进行权利救济或者是调解，同时也监督该领域相关法律的实施情况。

基于我国个人信息案件数量大，救济难等现状，以及日韩邻国的先行尝试，笔者认为设立专门的个人信息法律保护机构具有重要的现实意义。因此笔者建议在我国设立个人信息保护委员会作为个人信息保护的专门机关，监管全国的个人信息收集和处理等行为，同时赋予其启动民事诉讼的权力，以此加强对个人信息的保护。

5.3. 建立完善的大数据个人信息储存系统

随着大数据产业的迅速发展，个人信息侵权案件数量与日俱增。法律的缺位与监管的不到位等种种因素让违法犯罪分子有机可乘，因此建立完善的信息储存系统具有重要的现实意义。关于如何完善储存系统，笔者提出以下两点建议：

首先，对于个人信息的储存和共享，应该建立具有严格可控的安全管理机制[7]，确保数据归属明确、使用权限明确、使数据处理更加高效化，透明化。同时要保证数据安全可追溯，建议相关部门或者互联网平台等采用数据追踪技术伴随数据使用和处理的全过程中，明晰每一个数据的流向，确保数据的合法使用。

另外，笔者建议要完善数据共享权限机制。这有利于确定各数据管理权属及其使用范围，以保障数据合规流转。建议针对不同类型的个人信息采取针对性的管理措施，对一般的信息采用普通的权限进行把控就足以，但是对一些特殊的信息如精神问题、病史、财产状况等涉及个人隐私的敏感信息，应设立更高的访问权限，防止个人信息的泄露。

5.4. 加强宣传教育

目前我国公民的个人信息保护意识淡薄。笔者建议定期开展主题教育，通过互联网、报纸、公众号等各种渠道加强宣传教育，也可以定期组织司法工作人员进入学校，企业等进行宣讲，或整理发布一些典型案例。个人信息保护问题是一个严峻的挑战，不仅需要政府、企业和社会的努力，也需要每个公民加强保护意识，如此才能建立完善的个人信息保护法律体系。

6. 结语

大数据时代，个人信息不断凸显出其数据价值和社会属性，数据的分析和利用不仅关系到个人的权利，更是国家政策发布和科技发展的重要依据。随着新兴行业的不断涌现，互联网产品的不断发展，个

人信息的外缘边界不断扩展，我国虽然已经出台了《个人信息保护法》，但是在法律适用范围、违法行为的认定、惩罚力度等方面还存在诸多问题，现有的法律框架已经无法全面覆盖个人信息的保护范围。为此笔者认为可以将匿名化处理后仍能够通过技术手段识别的信息以及开源情报中仍可间接识别个人的信息纳入保护范围，此外，要完善大数据控制者的相关法律规范，使现有的法律体系更好地保护区块链、人工智能等新业态中的个人信息，减少违法犯罪事件的发生，同时社会方面可以采取加强宣传教育，规范政府部门和执法部门的工作等措施，切实保障公民的合法权益。

参考文献

[1] 谢琳. 大数据时代个人信息边界的界定[J]. 学术研究, 2019, 19(3): 3-6.

[2] 孙尧. 数字化时代我国个人信息保护制度研究[D]: [硕士学位论文]. 济南: 山东大学, 2022.

[3] 金善港. 数字经济时代个人信息保护中知情同意原则适用的研究[J]. 法学研究 2023, 23(3): 187-190.

[4] 魏晓彤. 个人信息保护机制中的平台“守门人”法律问题研究[D]: [硕士学位论文]. 上海: 华东师范大学, 2022: 25-35.

[5] 刘敏. 区块链技术下的个人信息保护路径[J]. 网络安全技术与应用, 2023, 23(3): 119-121.

[6] 李荣. 大数据下个人信息的民法保护[D]: [硕士学位论文]. 武汉: 湖北大学, 2022: 18-19.

[7] 王毓莹. 人脸识别中个人信息保护的思考[J]. 法律适用, 2023(2): 15-24.