E-Commerce Letters 电子商务评论, 2025, 14(7), 759-767
Published Online July 2025 in Hans. https://www.hanspub.org/journal/ecl
https://doi.org/10.12677/ecl.2025.1472232

Hans汉斯

电商发展下个人隐私保护的法治化保障

——以《个人信息保护法》为视角

桂明霞

贵州大学法学院，贵州 贵阳

收稿日期：2025年5月21日；录用日期：2025年6月6日；发布日期：2025年7月11日

摘　要

在电子商务快速发展的背景下，个人隐私保护的重要性日益凸显，个人信息保护法成为保障个人隐私的关键法律依据，本文以个人信息保护法为视角，深入探讨电子商务发展与个人的隐私保护的现实矛盾，如个人信息被无边界收集、数据共享导致个人隐私存在被滥用的风险；其次，对《个人信息保护法》在保护个人隐私方面的重要作用进行分析，包括构建全面的个人信息处理规则、保障个人权利以及规范了敏感信息，接下来对《个人信息保护法》在实施过程中存在的问题和困境进行剖析。最后基于上述分析提出相应的完善建议，旨在进一步加强电商环境下隐私保护的法治化保障，促进电商健康、有序发展。

关键词

电商，个人隐私，个人信息保护

Rule of Law-Based Protection for Personal Privacy under E-Commerce Environment

—Taking the Personal Information Protection Law as a Perspective

Mingxia Gui

The Law School of Guizhou University, Guiyang Guizhou

Received: May 21st, 2025; accepted: Jun. 6th, 2025; published: Jul. 11th, 2025

Abstract

Under the background of rapid development of e-commerce, the importance of personal privacy protection is becoming more and more prominent, and the Personal Information Protection Law has become the key legal basis for safeguarding personal privacy. This paper takes the perspective

文章引用: 桂明霞. 电商发展下个人隐私保护的法治化保障[J]. 电子商务评论, 2025, 14(7): 759-767.
DOI: 10.12677/ecl.2025.1472232

of the Personal Information Protection Law to discuss in depth the real contradiction between the development of e-commerce and the protection of personal privacy, such as the personal information being collected without boundaries, and the risk of abuse of personal privacy caused by data sharing; next, it analyses the important role of the Personal Information Law in protecting personal privacy, including the construction of comprehensive rules for handling personal information, the protection of individual rights and the regulation of sensitive information, followed by an analysis of the problems and dilemmas existing in the implementation of the Personal Information Protection Law. Finally, based on the above analysis, it puts forward corresponding suggestions for improvement, aiming to further strengthen the protection of personal privacy protection under the rule of law in the e-commerce environment and promote the healthy and orderly development of e-commerce.

Keywords

E-Commerce, Personal Privacy, Personal Information Protection

1. 电商发展与个人隐私保护的现实矛盾

随着互联网技术的迅猛发展，电子商务已经成为全球经济重要组成部分。越来越多的消费者倾向于通过电商平台购买商品和服务，电商平台的用户数据也在快速增加。这些数据中包括用户的个人基本信息、购买历史、支付信息、浏览记录等敏感信息，他们构成了用户隐私的重要组成部分[1]。这些数据对于电商发展来说尤为重要，但对于隐私而言存在被泄露、二次使用等风险，电商发展与个人隐私保护之间的矛盾日益凸显。

(一) 过度收集数据与隐私权保障的冲突

电子商务的运营对于数据的依赖性极高，海量的用户数据是电商平台实现精准营销、个性化推荐以及优化服务的基石。平台收取用户信息的方式有很多，这些信息除了基本的姓名、联系方式、收货地址等，还包括消费记录、浏览记录、地理位置等敏感信息。这些数据的收集都是为了能够在深入了解用户需求后，为用户提供更符合其喜好的商品和服务，从而提升用户体验和平台竞争力。

但是这种数据收集的行为时常引发与个人隐私保护的冲突。一方面，部分电商企业存在过度收集数据的现象，收集的信息远超过提供服务所需的范围。如，一部分电商软件在安装的时候要求获取过多不必要的权限，比如访问通讯录、麦克风、摄像头等权限，即便这些权限与核心购物功能并无直接关联。这种收集行为使得用户的大量隐私数据暴露在潜在风险当中。另一方面，用户在注册和使用电商平台时，往往处于劣势地位。电商平台的隐私政策和用户协议通常冗长复杂，还都是专业术语，普通用户很难真正地理解其中有关数据收集、适用和共享的具体条款。用户往往为了能够快速使用平台服务，不得不无奈勾选“同意”选项，导致个人隐私在不知情的情况下就被侵犯。

(二) 数据共享与滥用风险增大

数据共享为公共管理效能和数字产业链升级带来巨大提升的同时，也对隐私权的保护形成了新的挑战[2]。一方面，在电商生态环境中，数据共享是一种常见的商业行为，电商平台为了实现业务拓展和协同合作，往往会与第三方合作伙伴共享用户数据。例如为了完成订单的配送，电商平台需要将用户的联系方式、收货地址等信息提供给物流公司；为了能够实现广告的层层投放，会将用户的浏览和购买行为

数据分享给广告商。数字经济在给人们的生产生活带来极大便利的同时，也形成了“独立于人类的异化力量”[3]。另一方面，虽然数据共享促进了电商业务的发展，但是也带来了严重的个人隐私保护问题。首先，第三方合作伙伴的资质和信誉参差不齐，电商平台在数据共享过程中可能无法对其进行有效的监管，一些不良第三方可能会超过授权范围使用用户的数据，将数据用于其他非法目的或者转售给其他机构，导致用户隐私泄露的风险呈现几何级数增长。其次，用户对于自己的数据在第三方之间的流转情况往往缺乏足够的知情权和控制权。电商平台在进行数据共享时，通常不会详细告知用户数据将会被共享给哪些第三方、用于何种具体途径以及会采取哪些保护措施。从而导致用户在完全不知情的情况下，个人隐私就被扩散到了多个未知的领域，面临着更大的隐患。

(三) 数据存储与安全层面的矛盾

随着电子商务交易量的爆发式增长，电商平台积累了庞大的用户数据，这些数据都存储在服务器和云端数据库中，成为了黑客以及不法分子所觊觎的目标。保障数据储存安全，防止用户信息泄露，是电商企业的重要责任。然而，现实中数据存储安全面临着诸多的挑战。

尽管电商企业已经在保护数据安全方面投入了大量的资源，但黑客技术也在不断地进步，数据泄露事件仍然频频发生。一旦存储系统被攻破，用户的敏感信息就将面临着泄露风险。这些泄露的数据可能会被用于诈骗、恶意营销、身份盗用等非法活动，给用户带来巨大的经济损失和精神困扰。

此外，电商企业内部管理不善也可能导致数据安全问题。员工的失误操作、违规访问以及数据备份和回复机制的不完善等，都可能增加数据丢失或泄露的风险。而且，一些中小电商企业由于技术和资金限制，在数据安全防护方面相对薄弱，难以应对日益复杂的安全威胁，进一步加剧了个人隐私保护的难度。

电商平台发展与个人隐私保护之间的矛盾是多方面的，其中涉及到多个方面，包括数据收集、共享以及用户数据储存等。要想解决好这些矛盾，需要政府、企业和用户共同努力，构建一个既有利于电商健康发展，还能充分保护个人隐私的良好生态环境。

2. 《个人信息保护法》对于个人隐私保护的核心规定及积极作用

对于隐私和个人信息的关系，宪法上并没有明确的规定，对于个人信息这种新兴的人格利益，最初是由刑法和行政法对其进行规制的[4]。隐私与个人信息之间既相互联系又有所区别，两者在内容上有所联系，个人信息权益中可以含有隐私利益，但是两者的保护机制完全不同。我国《民法典》第一千零三十四条第二款对于两者的保护做了适用规定，个人信息中的私密信息，适用有权隐私权的规定；没有规定的，适用有关个人信息保护的规定。

《个人信息保护法》对于推动《民法典》的实施具有重要作用。《个人信息保护法》作为一部领域法，是一部全面保护个人信息的法律，性质上属于公、私法的混合[5]，其内容多以民事权利义务为主，对《民法典》具有补充、细化的作用，进一步加强了对隐私的保护。在《个人信息保护法》中有许多对于个人隐私保护的规定，主要体现在信息处理规则、个人权利保障、敏感信息处理等方面。

首先在信息处理规则方面，《个人信息保护法》强调了知情同意原则以及最小化和必要原则。知情同意原则即是处理个人信息应当在事先充分告知当事人的前提下取得其同意，并且当事人有权利随时取消该同意。这一原则有利于防止个人隐私的二次传播；最小化和必要原则则是要求信息处理者应当根据要实现的处理目的的最小范围和必要限度内收集、使用个人信息、不得过度收集个人信息，这一原则限制了信息处理的范围和方式，同时也要求信息处理者在保护个人信息时，应当积极地采取技术和管理措施，以防信息的泄露、篡改和丢失。

其次是个人权利保障方面。规定了当事人有权知道其个人信息的处理情况，包括是谁在处理其个人

信息、如何处理的等，并对自己个人信息的处理具有决定权，比如，是否同意他人对其个人信息进行收集、适用等；此外当事人有权利向信息处理者查阅、复制其个人信息，如果发现信息存在不准确或者是不完整的情况，有权向信息处理者提出更正、补充，在特殊情形下，如处理目的已经实现、处理期限已届满等，有权要求信息处理者立刻删除与自己有关的个人信息；最后是在针对自动化决策时，如果该决策对于个人权益存在重大影响的话，当事人可以要求信息处理者给予说明，并且有权拒绝仅通过自动化决策的方式作出的决定。

最后规范了敏感信息的保护规则。明确列举了敏感个人信息的概念和具体类型。从比较法上来看，对敏感个人信息存在具体的列举模式和综合考量模式[6]。《个人信息保护法》阐明了敏感信息的概念为“一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息”。另外对于敏感信息进行了具体的列举，包括生物信息、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等，以及不满十四周岁未成年人的个人信息。这也反映出了对于未成年人个人信息的保护进行了强化。对于不满十四周岁的未成年的个人信息在处理时必须要经过其父母或者监护人的同意。关于个人信息的处理构建了更为严格的规则：一是增强了更严格的处理前提；而是单独同意和依法取得书面同意；三是规定了特殊的告知义务[5]。

3. 电商环境下个人隐私保护存在的问题——基于《个人信息保护法》审视

(一) 法律适用模糊

在数字化时代，电子商务蓬勃发展，个人隐私保护的重要性日益凸显。《个人信息保护法》《电子商务法》《网络安全法》等多部法律从不同角度对电商环境下的个人隐私保护作出规定。然而，这些法律之间存在法条竞合、适用范围界定不清等问题，给法律的准确适用和个人隐私的有效保护带来挑战。

(1) 法条竞合

在相似规定方面导致的竞合。《个人信息保护法》《电子商务法》与《网络安全法》在部分条款上存在相似之处，都涉及对个人信息的保护。例如，三部法律均强调了对个人信息收集、使用应遵循合法、正当、必要的原则。《个人信息保护法》第 6 条规定处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式；《电子商务法》第 23 条要求电子商务经营者收集、使用其用户的个人信息，应当遵守法律、行政法规有关个人信息保护的规定；《网络安全法》第 41 条也指出网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则。这种相似规定在实践中可能导致同一行为同时触犯多部法律，出现法条竞合现象。当发生电商平台违规收集用户个人信息的案件时，执法机关可能面临选择哪部法律进行适用的困惑，不同法律的处罚力度和程序存在差异，这可能影响法律适用的准确性和公正性。

此外，在法律责任方面存在责任。三部法律也存在一定程度的重叠。对于电商平台泄露用户个人信息的行为，《个人信息保护法》第 66 条规定了处理者违反本法规定处理个人信息的相应处罚；《电子商务法》第 76 条对电子商务经营者泄露、出售或者非法向他人提供用户个人信息的行为设定了法律责任；《网络安全法》第 64 条同样针对网络运营者侵害个人信息依法得到保护权利的行为作出处罚规定。这种法律责任规定的竞合使得在具体案件中，确定对电商平台的处罚依据变得复杂。不同法律对同一违法行为的处罚幅度、方式不尽相同，可能导致执法的不一致性，也给电商企业准确把握自身法律责任带来困难。

(2) 适用范围界定不清

《个人信息保护法》《电子商务法》《网络安全法》在适用范围时存在主体、行为界定不清的问题。首先是主体范围界定模糊，《个人信息保护法》适用于处理自然人个人信息的活动，其主体范围较为宽

泛，涵盖各类个人信息处理者。《电子商务法》主要针对电子商务经营者，即通过互联网等信息网络从事销售商品或者提供服务的经营活动的自然人、法人和非法人组织。《网络安全法》则聚焦于网络运营者，即网络的所有者、管理者和网络服务提供者。在电商领域，一些主体身份具有多重属性，例如电商平台既属于电子商务经营者，又是网络运营者，同时也是个人信息处理者。当涉及某一具体行为时，难以明确究竟应依据哪部法律来界定其责任和义务。一些小型电商从业者，既是商品销售者，又自行搭建网站处理用户信息，在其出现个人信息保护问题时，三部法律的适用界限难以清晰划分。然后是行为方面的界定不清，三部法律对电商活动中涉及个人隐私保护的行为范围界定也存在不明确之处。《个人信息保护法》侧重于规范个人信息处理的全流程行为，包括收集、存储、使用、加工、传输、提供、公开等；《电子商务法》主要围绕电子商务交易过程中的个人信息保护行为进行规制；《网络安全法》则着重于网络环境下与网络安全相关的个人信息保护行为。然而，在实际电商场景中，很多行为相互交织。电商平台在进行促销活动时，通过网络收集用户信息用于精准营销，这一行为既涉及电子商务交易环节，又关乎网络环境下的信息处理以及个人信息的综合处理，这种行为范围界定的不明晰，使得在具体案件中难以确定应当优先适用哪部法律，容易出现法律适用的争议。

(二) 监管机制的不完善与执法力度不足

(1) 监管部门的职责分工不明确，存在监管重叠和空白的问题

电商领域个人信息保护涉及多个监管部门，如网信、工信、市场监督等，各部门的职责侧重点并不相同，网信部门侧重于在网络安全和信息化的宏观层面去进行把控，工信部门则是关注电信和互联网行业的规范运作，市场监督部门聚焦于市场竞争秩序和消费者的权益保护方面。三个部门虽然都有各自的职责，但是在处理某些问题时，不免会造成重复检查的情况，例如当需要收集网络平台上出现违规用户信息时，三个部门都可以依据自己的职责介入其中，这就会造成同一问题需要接受多个部门的重复检查、要求整改，容易给平台企业带来过重的负担，同时也造成行政资源的浪费。

目前，各部门之间缺乏完善、高效的协调机制。不同部门在监管目标、执法标准和工作流程等方面存在差异，难以形成监管合力。在信息共享方面，部门之间信息流通不畅，导致重复监管或监管空白。在联合执法行动中，由于缺乏统一指挥和协调，各部门行动难以同步，影响执法效果。面对复杂的电商个人隐私保护问题，需要多部门协同作战，但现有的协调机制无法满足实际需求，制约了监管工作的顺利开展。

(2) 监管手段的技术的落后，难以适应电商发展的监管需求

电商行业发展迅速，监管部门难免会面临着监管技术落后，难以适应时代变化需求的问题。电商高速发展用户数量急剧增加，平台所产生的个人信息数据量是尤其庞大的。这些个人信息当中就不免含有不想为他人所知悉的私密信息，监管部门就享有的数据检测技术是难以对这一海量的数据信息进行实时且全面的检测，更不用说对其中的信息进行分析，检测其是否属于个人隐私。除此之外，就现有技术而言，是可以从一些看似没有任何价值的数据中挖掘和分析出有价值的信息，许多不法分子就是利用这些技术从这些数据当中分析出可用信息。然而，监管部门在深挖数据分析技术方面仍存在不少缺陷，难以通过数据去分析出隐藏在复杂数据关系背后的个人信息记忆隐私的安全。

此外，对于新兴发展领域，监管部门的技术存在识别缓慢地问题，人工智能中人脸识别技术在广泛应用过程中存在数据泄露的风险，区块链技术的匿名性和去中心化特点则可能被用于非法交易个人信息中。监管部门对于这些新兴技术所带来的风险认识以及识别技术是跟不上其发展的，很难去及时地制定有效的监管策略。

(3) 惩罚力度不足

《个人信息保护法》第六十六条虽然规定对违法处理个人信息行为的罚款标准，但是在实际执法中，

罚款额度对于一些大型企业来说，可能是其巨大利润的一小部分，难以形成足够的威慑力。换句话说，对于大型电商企业而言，就算因违法规定侵犯他人隐私造成不良后果，但相较于巨大利润，这些罚款并未对企业的经营造成实质上的影响，导致企业很大概率上会继续冒险违规以追求商业利益。

除了罚款以外，第六十六条规定的其他惩处方式在实际执行中也存在局限性。例如，警告、责令整改等措施，对于一些蓄意违法的企业是没有什么效果的。企业可能只是表面上进行了整改，到实际上并未从根本去解决这些问题，整改之后仍然自我，继续是何时违法处理个人隐私的活动，而且对于违法企业责任人的惩处力度相对较轻，难以促成企业管理层真正地重视个人隐私保护工作。

(三) 公众隐私意识参差不齐

在电商迅猛发展的当下，公众隐私意识参差不齐成为一个突出问题，深刻影响着个人权益、电商行业生态乃至整个社会的稳定与发展。

不同群体的隐私意识在电商环境下呈现出显著差异。年龄层面，年轻一代生长于数字化浪潮中，对电商新事物接受快，但常因追求便捷而忽视隐私风险。比如青少年在注册各类电商应用时，鲜少仔细研读隐私政策便匆匆同意授权。中年群体虽逐渐意识到隐私保护的重要性，但面对复杂多变的电商技术，仍可能因知识局限而在隐私保护上力不从心。老年群体则由于对新兴技术的陌生，在电商操作中更容易泄露个人信息，成为隐私侵权的潜在受害者。地域方面，经济发达地区凭借良好的互联网基础和丰富的信息资源，公众对电商隐私问题关注度高，隐私意识相对较强；而欠发达地区受限于基础设施和信息传播，公众对隐私风险认识不足。文化程度也影响着隐私意识，高学历者凭借较强的信息分析能力和法律认知，在电商活动中更注重保护隐私；低学历者则因知识储备匮乏，容易在不经意间暴露个人信息。

这种参差不齐的隐私意识带来了多方面的影响。从个人角度看，隐私意识薄弱使公众极易陷入个人信息泄露的危机。一旦信息被不法分子获取，接踵而至的可能是诈骗电话、垃圾邮件的骚扰，甚至导致财产损失和个人名誉受损。对电商行业而言，参差不齐的隐私意识破坏了公平竞争的市场环境。部分不良平台利用公众的无知过度收集信息，而注重隐私保护的平台却可能因合规成本高而处于劣势，长此以往，将削弱消费者对整个电商行业的信任，阻碍行业的健康发展。从社会层面考量，大规模的个人信息泄露可能引发金融风险和社会秩序混乱，影响社会的稳定与和谐。提升公众在电商环境下的隐私意识迫在眉睫。

4. 以《个人信息保护法》为核心完善电商环境下个人隐私保护法治化路径

(一) 完善法律适用规则

(1) 细化《个人信息保护法》电商领域实施细则

鉴于电商行业的独特性质与复杂环境，为更有效地保障个人信息安全，迫切需要对《个人信息保护法》在电商领域的实施细则进行深度细化。

在个人信息收集“必要范围”方面，应依据不同电商业务类型进行明确界定。例如，对于仅提供商品展示与交易撮合服务的电商平台，收集用户的姓名、联系方式、收货地址以及支付相关信息通常属于必要范围，旨在确保交易顺利完成。而对于一些具有社交属性的电商平台，除上述基本信息外，若涉及用户发布内容、社交互动等功能，收集用户的头像、昵称、兴趣爱好等信息可视为满足平台特定功能需求的必要范畴，但需严格限制在实现功能所必需的最小限度内。同时，应明确禁止电商平台以任何理由收集与业务功能无关的敏感信息，如宗教信仰、政治倾向、基因数据等。

数据共享标准方面，需制定严格规范。电商平台在与第三方共享用户个人信息时，必须事先获得用户明确、清晰的授权同意。授权内容应详细说明共享的信息种类、共享目的、共享对象以及共享期限等关键信息。对于共享的数据，电商平台有责任确保第三方具备同等水平的信息保护能力，并通过签订书

面协议明确双方在数据保护方面的权利和义务。第三方在使用共享数据时，必须严格遵循约定的目的和范围，不得擅自将数据用于其他任何用途。若第三方出现数据安全问题，电商平台应承担相应的连带责任。

在侵权责任认定量化指标方面，应建立科学合理的评估体系。综合考虑侵权行为造成的损害后果，如用户个人信息泄露导致的经济损失、精神损害程度；侵权行为的主观恶意程度，包括故意或重大过失、一般过失等不同情形；以及侵权行为的持续时间、影响范围等因素。例如，若因电商平台故意泄露大量用户敏感信息，导致众多用户遭受严重经济损失和精神痛苦，应认定为严重侵权行为，加重其法律责任。通过明确这些量化指标，使侵权责任认定更加客观、准确，增强法律的可操作性和威慑力。

(2) 协调相关法律衔接

《个人信息保护法》虽为个人信息保护提供了基础性框架，但在电商领域，其需与其他众多相关法律协同发挥作用，以消除法律冲突，形成强大的协同保护合力。

首先，梳理《个人信息保护法》与《电子商务法》的交叉内容。两部法律在电商经营者对用户个人信息的保护义务方面均有涉及，但侧重点有所不同。《电子商务法》主要从电商经营活动规范的角度，强调电商经营者在交易过程中对用户信息的保护责任；而《个人信息保护法》则更侧重于从个人信息处理的一般性原则和规则出发，规范各类个人信息处理者的行为。应明确在电商场景下，当涉及具体交易环节中的信息保护问题时，优先适用《电子商务法》的相关规定；而对于个人信息处理的通用规则，如信息收集、存储、使用的基本原则等，则以《个人信息保护法》为准。同时，对两部法律中重复或冲突的条款进行统一和协调，避免出现法律适用的混乱。

其次，加强《个人信息保护法》与《网络安全法》的衔接。《网络安全法》主要聚焦于网络运行安全和网络信息安全，为个人信息在网络环境中的保护提供了技术和安全层面的保障；《个人信息保护法》则更关注个人信息处理过程中的权益保护。应明确在涉及网络安全事件导致个人信息泄露的情况下，如何综合运用两部法律进行责任认定和处罚。例如，若因网络运营者违反《网络安全法》规定的安全技术措施，导致用户个人信息泄露，同时违反《个人信息保护法》中关于个人信息保护的相关规定，应根据具体情况，分别依据两部法律的相应条款进行处罚，并明确处罚的合并或递进规则，确保对侵权行为的打击力度。

此外，对于其他与电商和个人信息保护相关的法律法规，如《消费者权益保护法》《民法典》等，也需进行系统性的协调。《消费者权益保护法》强调消费者在消费过程中的个人信息安全权，《民法典》则从民事权利保护的角度对个人信息权益进行了规定。应建立一套统一的法律适用指引，明确在不同法律诉求和场景下，如何综合运用这些法律，形成一个有机统一、相互补充的法律保护体系，为电商环境下的个人隐私保护提供全方位、无缝隙的法律保障。

(二) 完善监管机制、强化执法力度

目前，网信、工信、市场监管等读个部门均涉及个人信息保护监管工作，却因职责划分不清晰，出现监管重叠和空白的情况。对此，应当出台专门的监管职责划分细则，以法律条款形式准确界定各部门权力与责任范围。同时，构建高效的跨部门协调机制，设立常态化的联合办公小组，针对重大、复杂的个人信息侵权案件开展协同调查与处置。建立信息共享平台、实现各部门间线索移送、证据互换等工作的无缝衔接，打破信息壁垒，提升监管效率。

另外，随着电商经济的蓬勃发展，个人信息侵权手段日益隐蔽、复杂。传统的人工监管方式难以应对，需借助技术创新实现智能化监管。政府应当发挥引导作用，设立专项科技发展基金，每年投入专项资金用于个人信息保护技术研究。鼓励高校、科研机构与监管部门之间达成合作，培养专业人员，为技术创新提供智力支持。推动企业与科研力量合作。对于企业而言，要强化技术合规要求。企业在收集、

存储、传输个人信息时，必须采用加密传输技术，防止信息在传输过程中被窃取；运用去标识别化技术，将个人信息中的身份标识去除，降低信息泄露后的风险。最后，应加大对新兴技术检测设备和系统研发的投入，利用大数据、云计算等技术构建智能化检测平台。该平台能够做到实时收集、分析新兴技术应用过程中的数据，自动识别异常行为和潜在风险。

针对惩罚力度不足的问题。惩罚力度不足削弱了法律的威慑力。因此针对罚款额度，可以按照违法所得的一定比例处以罚款，且不设上限，并根据企业规模和违法所得制定差异化的罚款标准。对于多次违法或者造成严重后果的企业，实施高额顶格罚款。对于直接负责的主管人员和其他责任人员，依法追究刑事资格。建立全国统一的个人信息保护信用档案系统，将违法企业和个人的不良记录记录在其中，与金融信贷、政府采购等挂钩，形成全方位的信用约束。

(三) 提升电商发展环境下公众隐私意识的策略

电商平台收集个人数据、信息，建立庞大的数据库，记录着个人的对话、信息和轨迹，这些信息更容易被回溯或在未来被参考，或被不法分子利用实施盗窃和敲诈勒索。如果公众自己都不重视隐私是否泄露的问题，单凭国家和企业隐私权保护义务和责任的制度，是很难去防止隐私权的私密信息被滥用和泄露的任务。

政府应当培养电商发展环境下公民的隐私意识，通过多种渠道和方式大规模开展隐私保护宣传，在学校、社区、企业等场所开展专题讲座和培训，普及隐私保护知识和技能，提高全民的隐私保护意识和法律素养。此外政府要加大对数据安全技术研发的投入，鼓励科研机构和企业合作开展隐私保护技术攻关，如加密技术，匿名处理技术等，为企业和公民提供先进的隐私保护工具。

电商平台应当以清晰易懂的方式制定隐私政策，避免使用过于专业或晦涩的术语。在用户注册、使用服务等关键节点，以显著方式向用户告知数据收集的目的、范围，使用方式以及用户享有的权利等重要信息，确保用户充分知情并获得用户明确同意。同时，定期更新隐私政策，及时向用户传达隐私保护措施的变化。

公民自身要充分认识到个人隐私的重要性，主动学习隐私保护知识，了解常见的隐私侵权手段和防范方法。在日常生活中，保持警惕，不随意在不可信的电商平台透露自己个人敏感信息。另外在使用各类平台服务时，认真阅读隐私政策和用户协议，了解平台对个人数据收集、适用和共享规则。一旦发现个人隐私被侵犯，应当勇敢地拿起法律武器维护自己的合法权益。

5. 结语

在电商快速发展背景下，《个人信息保护法》为个人隐私保护构建了重要的法治防线，但在实施过程中不免遇到一些问题和挑战，如监管资源和执法力不足、公众隐私意识参差不齐等。面对技术更替带来的新型隐私风险，法律的实施仍需在实践中持续完善。

未来，强化个人隐私的法治化保障刻不容缓。立法层面需要紧跟技术变革，填补法律空白，明确模糊条款；监管上要加大资源投入、优化跨部门协作机制；同时，需要加强普法宣传，提高公众隐私意识与维权能力。只有各方齐心协力，形成合力，才能真正实现电商环境下个人隐私保护的法治化保障，营造一个既充满活力又安全可靠的电商生态环境。

参考文献

[1] 顾炜江. 基于序贯博弈模型分析技术保护电子商务中的网络隐私[J]. 山东农业大学学报(自然科学版), 2014, 45(4): 595-600.

[2] 任颖. 数字时代隐私权保护的法理构造与规则重塑[J]. 东方法学, 2022(2): 188-200.

[3] 王成. 个人信息民法保护的模式选择[J]. 中国社会科学, 2019(6): 124-146+207.

[4] 王苑. 数据权力视野下个人信息保护的趋向——以个人信息保护与隐私权的分立为中心[J]. 北京航空航天大学学报(社会科学版), 2022, 35(1): 45-57.

[5] 王利明, 丁晓东. 论《个人信息保护法》的亮点、特色与适用[J]. 法学家, 2021(6): 1-16+191.

[6] 胡文涛. 我国个人敏感信息界定之构想[J]. 中国法学, 2018(5): 235-254.