第1章
消费者隐私的演变及内涵

随着互联网和大数据技术的广泛应用，越来越多的企业认识到消费者数据的价值和重要性。从企业的角度来看，大数据在企业的生存与经营中占据着极为重要的位置。大数据不仅能够反映市场的发展走向和政策的扶持情况，还有助于企业判断消费者的需求及购买偏好，为企业创造经济价值。具体来说，大数据重要的意义如下：①大数据能够将消费者的反馈意见以及不同区域消费者对商品的需求信息有效地集中起来，通过进一步对数据进行加工、分析，对市场中的需求情况作出判断，如哪些产品为消费者所偏好、哪些产品无法满足消费者需求等，帮助企业改善产品与服务，制订更加详细的发展规划。②大数据有助于企业做好更精准的定位工作，如确定自己的目标市场、提供何种产品与服务、如何投放广告以及如何维持客户关系等。大数据不仅极大程度帮助企业节省运营成本，还大大提升企业管理效率。③大数据本身不仅是工具，还兼具产品性质。作为产品，它不单单限于各种数据间的买卖，还发挥着数据支撑的重大作用。例如，当前我们生活中所应用的各种智能穿戴设备，就是通过对人体的指标进行测量，积累产生人体大数据，反映人体的健康状况，进而为医疗服务提供依据。数据在其中则发挥着提供数据服务、给予数据支撑的功能。以各种直接或间接的方式收集、保存和使用消费者的隐私数据，逐渐成为企业一

项常规的营销行为（蒋玉石等，2015；Krafft 等，2017）。

从大数据视角，消费者隐私会转化为隐私数据。数据对于商家或其他组织而言代表着经济效益，这些隐私数据能够为其创造极大的商业价值。受经济利益的诱惑与驱使，服务商或其他主体非法获取、利用消费者的隐私，消费者被侵权行为所导致的伤害更多表现在经济层面。虽然国内部分相关法律对消费者的隐私予以保护，但是在具体的实践应用中仍然存在很多不完善的地方。大数据时代的来临，使得侵权的主体、消费者隐私权被侵犯的方式等层面都发生了变化。在对数据进行采集的阶段，侵犯消费者的隐私主要是通过非法收集或者黑客攻击来实现；而在数据的分析阶段则表现为深度挖掘消费者隐私。随着信息技术的发展和普及，消费者隐私问题日益受到重视。

为更好保护消费者隐私，本章将对消费者隐私的演变与内涵进行综述，探讨其在不同时期的变化和影响。隐私的演变历史是一个错综复杂且不断演变的过程，涉及多个推动因素，包括文化、社会、法律和科技等。通过梳理它产生的历史，在一定的程度上可能改变人们对于“隐私”固有的传统认知，并进一步使人们产生一个较为客观和全面的关于“隐私”的新时代认知。大数据背景下，厘清消费者隐私的演变与内涵对消费者的隐私保护具有十分重要的意义。

1.1 隐私的历史背景

1.1.1 隐私的东方文明历史背景

“隐私”一词最早出现于周朝初年，其含义等同为衣服，也就是把私处藏起来的东西。与现代含义不同，有没有“隐私”是文明人与野蛮人、人与野兽最明显的区别。“隐私”继承了部落文明时代抑制人类本能所产生的相关含义。周人在此基础上制定了与服饰相关的礼仪，并将它作为周礼的一部分向全社会推广并保留下来。在汉朝，“隐私”与男女两性关系联系起来，《汉书·张敞传》和《醒世姻缘传》中都出现了相关记载。宋代将剥夺隐私作为惩罚行为的一种

形态，即这一时期流行的在人犯脸上刻字的“黥刑”等（杨立新，2022）。而后的历史朝代均沿用这样的思想和刑法，一直持续到清朝。

总结周朝以来“隐私”一词含义的发展脉络，可以知道在封建朝代华夏文明认知中，“隐私”与家庭紧密相连，具有名分相当固定、非常明确而权利相对模糊的特点，个体“隐私”的地位被忽视。一般个体“隐私”都与恶的行为相关联。而我们在当今的文明体系下所讲的信息的价值和权利，由于儒家所代表的“宗族”主义思想的影响，在文明的进程和社会实践上，我们的祖先使其更多地代表了生产力层面的生产要素。可以说，华夏文明在表面上对于“隐私”的认知观念存在非常严重的二分现象与断代现象。但实际上由于儒家“宗族”主义思想的影响，不同朝代的界定范围或者实践层面会有所不同，究其根本则是保护相对小团体的相对“隐私”，而否定个体的“隐私”，这是华夏文明独有的文化特征。

在古代中国，隐私是与特权阶级紧密相连的。最高统治者拥有完全的隐私特权，如在秦朝，窥探皇宫者将被斩首，而议论皇室事务、损害皇室尊严的行为则被视为“大不敬”，列为“十恶”之一。《宋刑统》中也有规定，登高俯瞰皇宫者被判一年徒刑。相比之下，普通民众的隐私范围非常有限，仅涵盖基本的身体和性生活等方面。尽管儒家思想允许“亲亲相隐”，但历代各朝却鼓励告奸，即鼓励民众揭发个人家庭的隐秘事情。在这样的情况下，普通群众的隐私权无法得到根本的保护。

古代社会对女子隐私的重视尤为突出，特别是贵族女子。未出嫁的女子大多遵守深居简出的原则，甚至生病就医时也尽量避免与男性医生接触，规矩森严导致“大家闺秀”大门不出、二门不迈。明代《习医规格》规定，为女病人诊病时必须使用薄纱罩手，以确保医生不会触摸到女病人的肌肤。而对于宫中女子，明太祖朱元璋曾规定：“宫嫔以下有疾，医者不得入宫。”这意味着嫔妃生病时只能根据病情让医生开具药方。这种坚守贞节的观念实际上限制了女子真正享有隐私权的可能性，同时束缚了女性与外界交流的权利。

《礼记》是一部儒家经典，其中记录了许多古代的礼仪规范。在这部典籍

中，提到了一些关于拜访别人时的礼仪。在古代，人们非常重视隐私，认为拜访别人时应该尊重他人的隐私。因此，在进入别人的房间之前，一定要打招呼，避免突然闯入。当看到屋外有两双鞋子时，只有听到屋内的人说话的声音才能进去。进入别人房间时，一定不要东张西望，要保持安静并尊重别人的隐私。这些规矩可以避免不必要的尴尬和冒犯。此外，古人们还非常注重窗户的设计。为了不让屋外的人观察到屋内情况，且兼顾通风透气及抵御蚊虫，用纸糊的方式做窗户便成了当时的最优选。或许人们对窗户纸还停留在影视作品一捅即破的印象当中，但其实这是剧情需要导致被过分夸大的处理结果。古人们糊窗户所用的纸，其实是一种经过特殊加工的藤纸，不管是粗糙度还是硬度，都远大于普通纸张，窥视者把手戳肿也不能捅破。大户人家隐私防护做得更周全，材质都是使用昂贵的绢布。同时，府邸上下有着足够的人手进行全天巡逻护院，从大门到院子，一般人很难轻易进入，更不用提窥视了。总之，从这段记载中可以看出古人们非常重视隐私和礼仪规矩。这些规矩不仅体现了对别人的尊重，也有助于维护社会的秩序与和谐。

直到近代，我国隐私权的发展才有了重大突破。尽管《大清民律草案》和《民国民律草案》中没有明确规定隐私权，但它们对人格权的保护进行了笼统的规定。1929 年的《中华民国民法典》首次提及隐私的权利，但仅是简单列举，缺乏详尽的阐述。我国真正意义上的隐私权保护始于宪法对公民人格尊严的保护。新中国成立后，《中华人民共和国宪法》第 38 条规定：“中华人民共和国公民的人格尊严不受侵犯。禁止用任何方法对公民进行侮辱、诽谤和诬告陷害。”这是我国隐私权保护的基础，保护公民的人格尊严也意味着保护公民的隐私权。任何人都不得以揭露他人隐私的方式侵害公民的人格尊严。

我国民法对隐私权的法律保护经历了一个从无到有的过程。1986 年制定的民法通则并未使用隐私权的概念，但 1988 年的《关于贯彻执行〈中华人民共和国民法通则〉若干问题的意见（试行）》中首次使用了隐私概念。该意见第 140 条规定：“以书面、口头等形式宣扬他人的隐私，或者捏造事实公然丑化他人人格，以及用侮辱、诽谤等方式损害他人名誉，造成一定影响的，应当认定为侵

害公民名誉权的行为。”1993 年的《最高人民法院关于审理名誉权案件若干问题的解答》规定：“对未经他人同意，擅自公布他人的隐私材料或者以书面、口头形式宣扬他人隐私，致他人名誉受到损害的，按照侵害他人名誉权处理。”2001 年最高人民法院颁布的《最高人民法院关于确定民事侵权精神损害赔偿责任若干问题的解释》第 1 条第 2 款规定：“违反社会公共利益、社会公德侵害他人隐私或者其他人格利益，受害人以侵权为由向人民法院起诉请求赔偿精神损害的，人民法院应当依法予以受理。”

如今，隐私权纠纷作为一项独立的案由在民法层面保护着民众的隐私。《中华人民共和国刑法》第 245 条第 1 款规定：“非法搜查他人身体、住宅，或者非法侵入他人住宅的，处三年以下有期徒刑或者拘役。”这是宪法保护公民隐私权的精神在刑事领域的具体延伸，为保护公民隐私权提供了有力的法律保障。此外，我国法律确立了人民法院对涉及当事人个人隐私的案件进行不公开审理，在行政法规中也有众多关于隐私权保护的规定。

中国文化和历史背景深刻影响了民众有关隐私的态度，这可以从传统文化和现代社会有关隐私观的变化中看出。在中国的传统文化中，家庭和社区的权威被赋予更高的地位，个人权利往往要让位于家庭和社会的利益。个人的隐私在很大程度上被视为不重要，甚至是可以牺牲的。这种观念的形成，一方面是因为个人在社会中的地位和价值往往基于其对家庭与社会的贡献而确定，另一方面也是因为集体主义的观念在中国的社会中一直占据着主导地位。

然而，随着中国的现代化进程，虽然社会价值观发生了一些变化，但集体主义的观念仍然占据着重要的地位，这使得对个人权利的保护在中国社会中仍然面临困难。随着信息技术的广泛应用，企业和各类组织在数据收集与管理方面的需求日益增长，客观上对个人隐私保护提出了更高要求，也使隐私权利的落实面临新的挑战。近年来，中国的数字化进程加速，互联网技术的发展带来了更多的个人隐私泄露问题。在数字化快速发展的背景下，个人信息保护正成为一个备受关注的新议题。一方面，技术进步的速度较快，公众对隐私相关知识的了解仍在逐步加深；另一方面，相关法律法规也在持续完善，以更好地回

应时代需求。传统文化中“重集体、轻个人”的观念，曾使隐私话题较少被单独讨论，而今，随着社会价值观念的多元演进，越来越多的人开始主动关注自身信息的安全使用。未来，通过立法、企业与机构的自律，以及公众意识的共同提升，相信能够构建起更加平衡、可持续的数据治理环境，让技术红利与个人隐私在更高水平上实现良性互动。

1.1.2 隐私的西方文明历史背景

古埃及文明和两河流域的苏美尔文明，占据着西方文明历史舞台的主要位置。然而由于可考据的资料缺乏，尚未从上述两个文明遗留下来的文物中发现和现在“隐私”概念相关的记录。从目前对非洲大陆部落的相关研究中，反而可以窥见早期“隐私”的踪迹。有研究表明，由于社会形态处于原始社会阶段，人们主要的生存状态和获取生存资料的方式是采集渔猎。这个时候一个家庭往往生活在同一个空间内。在这一空间内，所有人并不存在现代意义上的“隐私”。在此阶段，“隐私”主要和男女之间的性行为联系起来。从这个角度看来，“隐私”实际上可能是人类的一种本能，其最根本的物质条件是拥有一个相对独立的空间。英国莱斯特大学的 Burke（2000）从考古学的角度，对希腊建筑的采光性和私密性的相关关系进行了研究，他发现古希腊建筑呈现出如下特点：每一个独立空间在暴露于公众视野最小化的前提下，同时最大化地利用可用光线，使得空间被光所照亮的效果最为明显。但由于奴隶制的存在，这一时期的“隐私”只属于古希腊文明中的公民。

在古希腊和古罗马时期，隐私观念尚未明确提出，这是由于当时的社会环境所致。城邦社会注重公共生活和集体利益，个人自由和隐私并未得到充分尊重。在这种社会背景下，个人的生活和事务往往被视为公共领域的一部分，而非私人领域。在古希腊城邦时期，私人领域和公共领域被严格区分。对应于私人领域的是家庭，其显著的特点是人们受生物本能的驱使而共同生活；对应于公共领域的则是城邦，摆脱了生存必然性控制的人们可以进入城邦，通过行动和言说参与政治生活。按照古希腊思想，政治生活是远远高于私人生活的。因

为私人生活存在于家庭领域之内，家长通过强力和暴力统治家庭成员及奴隶被看作正当的，是征服必然性和获得自由的手段；只有在政治领域中，所有人才是平等者或自由人，任何事情都取决于话语和说服，而不是取决于暴力和强迫。亚里士多德对人作为“政治动物”的定义表明，公民只有参与城邦的公共事务才是真正完整意义上的人。那些被排除在政治生活之外、仅存在于私人领域的奴隶和野蛮人“不是作为一个真正的人，而是作为动物种类的一个标本而存在于这个领域中。这正是古人对私人性表示极大蔑视的终极原因”。因此对希腊人来说，“私人领域”或者说“家庭内”就意味着被剥夺权利，是一种被剥夺了人的能力中最高级、最本质的东西的状态。

然而，这一时期的哲学家如亚里士多德和西塞罗，已经开始对个人自由和私生活进行思考。他们关注人类生活的各个方面，包括个人自由、权利和义务等，并对隐私观念进行了初步的探讨。例如，亚里士多德认为，个人应该拥有自己的空间和时间，以便自由地追求自己的目标。这种思想在一定程度上预示了现代隐私观念的出现。

在中世纪，私人领域和公共领域的鸿沟仍然存在，但已经失去了大部分意义，并且完全改变了位置。在罗马帝国覆灭之后，天主教堂为人们提供了一个公民资格的替代品，这曾经是市政府的特权。

中世纪社会实行严格区分社会阶级的等级制，人们被分为不同的阶层，每个阶层都有其特定的职责和权利。这种社会结构与古代的家庭领域相似，因为在那里，一切活动都以家庭为中心，并且仅仅具有一种私人的意义。

与此相对的是，古代的公共领域是切实存在于世俗领域之中的。希腊人在他们的伟大时代里，曾经在日常生活中发现了喜乐与美。他们只要走出狭隘的家庭领域，就可以进入城邦参与政治。这种公共领域的存在使得人们可以分享经验、参与决策、表达意见和行使权利。

到了中世纪，欧洲社会深受封建制度的影响。在这个时期，隐私在一定程度上得到了保护，尤其是在封建法中。封建法通过领主与封臣之间的契约关系，保护个人的一些权利和自由。

然而，这些法律保护的主要是贵族的利益，普通民众的隐私权并未得到充分关注。在封建社会中，普通民众的生活往往受到严格的限制和控制，他们的个人权利和自由受到了较大的限制。因此，在这个时期，普通民众的隐私权并未得到充分尊重和保护。

总的来说，古希腊和古罗马时期以及中世纪时期，隐私观念尚未明确提出或者未得到充分重视。然而，随着社会的发展和进步，人们越来越关注个人自由、权利和隐私问题。尤其是在现代社会中，随着科技的发展和信息化的加速，隐私问题变得更加重要，也更加需要得到重视和保护。

随着时间的推移，西方社会的隐私权观念在近代发生了深刻的变化。这主要源于资本主义的发展和民主制度的兴起。人们开始意识到，个人隐私和自由是基本的人权，需要得到法律的保护。

18 世纪末至 19 世纪初，美国和法国等国家开始在法律中明确保护隐私权。这是西方社会在隐私权观念上的重要转折点。具体来说，美国宪法第四修正案和法国《人权宣言》都规定了公民的私人住所和财产不受无理搜查与侵犯的权利。这些法律条文的出台，为公民的隐私权提供了坚实的法律保障。

然而，随着工业化和城市化的发展，以及国家对经济的干预增加，个人隐私与公共利益之间的冲突日益加剧。警察在调查犯罪时需要搜查个人住所和物品，但这往往会侵犯到公民的隐私权。为了平衡这种矛盾，20 世纪初，美国提出了“搜查令正当化”原则，为警察在调查犯罪时进行搜查提供了依据。这个原则在一定程度上缓解了隐私权和国家权力之间的紧张关系，但并没有完全解决问题。

进入 21 世纪，互联网技术的发展给西方社会的隐私权带来了前所未有的挑战。个人信息在网络上被大量收集、存储和分析，使得个人隐私遭受严重威胁。在这种情况下，西方国家开始通过立法和司法手段加强对隐私权的保护。例如，欧盟颁布了《通用数据保护条例》（GDPR），为公民提供更为严格的个人信息保护。这一法规的出台，标志着数据隐私保护已经成为全球性的关注焦点。

尽管法律有所进步，但网络时代的隐私问题仍然严峻。大型科技公司和政

府机构通过各种手段获取、分析和利用个人信息，使得个人隐私遭受持续威胁。这种状况引发了对数据隐私和数字身份的深入思考与激烈辩论。人们开始质疑大型科技公司和政府机构的透明度与问责制，同时也开始探讨如何在互联网时代更好地保护个人隐私权。

在这个过程中，公众意识不断提升，推动了隐私权观念的进一步发展。人们开始意识到，隐私不仅是个人权利，也是社会公正和民主的基础。因此，对于隐私权的保护，不仅是政府的责任，也是全社会的责任。在这个过程中，各种组织和机构开始参与隐私权的讨论与保护行动，形成了多元化的社会参与格局。

综上所述，西方社会自近代以来经历了对隐私权的深刻认识和保护实践。从法律条文的出台到互联网时代的挑战，隐私权观念在不断发展和演变。尽管仍存在许多挑战和争议，但公众意识的提升和社会参与的扩大为隐私权的保护提供了更强的支持与动力。

1.1.3 现代隐私的发展

隐私是一个多层次、多维度的概念，其定义随着时间的推移及文化和技术的发展而演变。我国法律规定隐私是自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息。自然人享有隐私权。任何组织或者个人不得以刺探、侵扰、泄露、公开等方式侵害他人的隐私权。隐私具有以下几层定义和解释。

（1）信息隐私。信息隐私通常涉及个人信息的收集、使用和分享。在数字时代，随着个人数据成为重要的商业资源，对信息隐私的保护成为社会关注的焦点。信息隐私的关键问题包括谁拥有个人数据、这些数据如何被使用，以及个人如何控制自己的信息。

（2）身体隐私。身体隐私指的是个体对自己身体和生理空间的控制权。这包括对个人健康信息的保护及在医疗和生殖权利方面的隐私。在某些文化和法律体系中，身体隐私被看作基本人权的一部分。

（3）空间隐私。空间隐私涉及个体对其居住环境和工作环境的控制，以及在这些空间中保持私密性和独立性的权利。随着监控技术的发展，如智能家居设备，空间隐私的概念和边界不断被重新定义。

（4）交流隐私。交流隐私指个体在进行交流时保持内容私密的权利，如电话通话、电子邮件和在线聊天。加密技术和安全通信协议在保护交流隐私方面起着关键作用。

（5）数据主体的自主权。在数据保护法律（如 GDPR）中，个人被视为其个人数据的“主体”，拥有对这些数据的控制权。这包括知情权（了解个人数据如何被使用）、访问权（查看收集的个人数据）和反对权（反对某些数据使用方式）。

（6）社会隐私。社会隐私涉及个人在社交互动中保持一定隐私水平的能力，如在社交媒体上进行信息分享。这涉及个人如何在公共生活和私人生活之间划定边界。

（7）心理隐私。心理隐私关注个人的内心思想、情感和欲望。这通常被视为最私密的隐私形式，但在某些情况下（如心理治疗）可能需要被适当地分享。

隐私的这些不同维度交织构成了一个复杂的概念体系。隐私的定义和理解也会根据技术进步、社会变迁和文化差异而发展变化。在数字时代，隐私的保护变得更加复杂和重要，特别是在全球化和网络化的环境下。然而，不同国家和地区在隐私保护方面的法律与文化具有显著差异，这些差异反映了各自的历史、文化价值观和社会政治背景。

工业革命的诞生，给人类的生存资料的获得带来了巨大的便利。工业革命的步伐飞速向前，社会的财富在不断增加，个人的独立空间领域不断扩大，让人们在意识层面上关于“隐私”的认知有所觉醒。随着邮政业务系统的诞生和发展，英国 1710 年的法案设置了一则条例：“邮政雇员不得私拆邮件，将邮件内容作为分类依据，进行分类整理以方便派送。”这则条例被视为关于“隐私”的第一条成文的具有法律约束力的条文。Warren 和 Brandeis（1890）发表《隐

私权》一文，标志着“隐私权”的诞生。他们主张隐私权是每个人的基本权利之一，它保护个人免受无端的干扰和侵犯，强调了隐私权在民主社会中的重要性，认为隐私权是保持个人自由和尊严的必要条件。然而他们的开创性文章并没有得到太多的关注。1902 年的“罗伯逊”一案中，一位年轻漂亮的女性控诉被告人未经许可就在有关面粉的广告中使用了她的肖像，导致她被人认出后遭到讥笑，并受到惊吓而卧病在床，要求法院下达禁令，禁止对方使用自己的肖像，并要求对方支付精神损失和身体损失 15 000 美元。虽然纽约州法院认为于法无据，没有支持，但这激起了社会公众的愤怒和舆论。1903 年，该州议会颁布了法律，规定为了广告或商业的目的，未经许可而使用他人的姓名和肖像，属于侵权和轻罪，这标志着美国第一部隐私法的诞生。此后，在 20 世纪中前期的大部分时间里，“隐私”在很大程度上被认为是为了维护男子对妻子公共生活和私人生活的所有权而诞生的一种全新社会意识，这与今天的“隐私”有很大的差别。但“隐私”逐渐在大部分文明社会的公民之中普及。自人类文明诞生之初，因“私有制”而引发的权益维护行为，使得“隐私”概念随之产生，并在后续的社会发展中，与私有财产形成了密不可分的联系。

这时在东方文明的社会中，依旧延续着传统农耕文明的相关观念。日本在社会意识层面上关于“隐私”的认知这一方面，全面学习西方。中国则截然不同，最开始只是在中华民国这段历史时期的民间艺术作品中发现了“隐私”的踪迹，而在当时中国关于“隐私”的认知主要是继承了传统的儒家文明的相关思想。两次世界大战中，政府当局监控着整个社会，“隐私”问题被搁置。

随着“隐私”与“私有制”的财产和利益紧密关联，它在现代法治框架中逐渐被确立为一种受保护的个人权益。第 40 任美国副总统杰拉尔德·福特（Gerald Ford）在其任期内向全美介绍了美国人在“隐私”领域的个人权利，并保证在他的政府中，不会有非法的窃听或闯入事件。在政府和私人活动中，将严格执行法律，以防止非法侵犯“隐私”。

随后，互联网的建立和广泛应用，使人们信息的交流变得顺畅、简单、便捷。随着网络终端的发展，网络终端不断地微小化、智能化及普及化。个体的

信息价值开始展现，警察可以利用这些信息有效地打击犯罪，医疗机构也可以通过这些信息来让患者得到及时的诊治，服务商可以利用这些信息为客户提供便利的服务。然而这也诱发了信息泄露、滥用问题，“隐私”问题变得空前重要。从20世纪末、21世纪初开始，国际上就逐渐涌现出一系列对互联网时代消费者隐私问题的研究。2015年，美国制定了《消费者隐私权法案》，该部法案重点强调大数据技术对消费者隐私造成的侵权问题。网络隐私的概念可以概括为互联网中的用户将涉及私人隐私的内容进行隐藏并控制个人信息被他人共享的权利（张军和熊枫，2005）。在互联网电子商务领域中，对用户个人隐私信息的保护逐渐成为热门的社会问题。越来越多隐私泄露纠纷的曝光也使对于这个问题的解决和预防程度影响电子商务平台的经营与推广。目前在消费者隐私领域，相关的研究已经扩展到许多关键层面，包括电子商务、市场营销、大数据以及消费者行为等（顾忠伟等，2015；梁晓丹等，2018；曾伏娥等，2018；吕巍等，2020）。在数字经济时代，数据成为关键生产要素和战略资源，其在推动科技创新、优化资源配置、改善人民生活等方面发挥着重要的作用。但与此同时，涉及用户身份、生物特征、行为习惯、宗教信仰、政治倾向等的海量数据，几乎全部聚集到数个大型数字平台上，引发了国内外反垄断领域对于数据垄断以及消费者数据隐私保护等系列问题的关切。

综上所述，“隐私”在某种程度上其实是人类历史发展阶段的特定产物，是人类为了生存更加便利所产生的“衍生物”。“隐私”始于人们意识到需要一定的私密空间，需要对私人事务保密，逐渐涉及个人道德和社会地位的问题、私有财产的保护，最后发展为对个人自由和权利的保护。从古代到现代，隐私观念的变迁和发展不仅反映了人类社会在不同历史时期的需求和价值观，也揭示了人们对于私人生活和信息保护的不断变化的态度。总的来说，隐私的历史背景是一个不断演变的过程。大数据背景下，网络在工作、生活中有着非常广泛的应用，这在一定程度上为违法者侵犯消费者的个人隐私提供了空间。无论是学习、工作还是生活涉及的各种隐私数据，都极有可能被侵权者进行不合理的收集、利用，致使消费者的隐私被侵害甚至达到无法控制的地步。尽管现代

科技给隐私带来了新的挑战，但人们也在不断探索和创新，以保护私人生活和信息。未来，随着技术的进一步发展和社会观念的变化，隐私的概念和保护方式也可能会继续演变。在更长的人类社会历史时期里，在人类的自然属性和社会属性中，透明的生存状态是占据大多数时间的。

1.2 新技术背景下的隐私定义

从人类文明的演化进程来看，“隐私”是植根于人类内心深处的一种本能。但它在历史上的特殊时段被人类所发掘、保留，成为人类历史上重要的社会意识。在现阶段的人类社会中，它仍旧有着重要的地位。它之所以重要，是因为我们过去在保护它的时候，是为了我们自身生活的方便、财富或名望。而现在大多数时候，我们同样非常愿意为了方便、财富或者名望去出卖“隐私”，将它作为一种筹码去实现自己的目标。那么，产生和保护以及出卖它的原因在这里已经明确显现了出来，即追求生活的便利。我们在过去300多年的时间内爆发的生产力，改变了世界的模样和自身生存的处境。在今天互联网和大数据的网络新时代，我们必然会获得更加强大的生产能力，这将进一步改变我们的生存状态。

2014—2024年是我国数字经济跃升的黄金时期，无论是数字经济的规模、发展速度还是影响力，都呈现出前所未有的态势。2024年，中国数据生产量达41.06泽字节（ZB），数字基础设施实现新跃升。我国已提前完成“十四五”规划关于5G（第五代移动通信技术）、千兆光网建设目标，实现县县通千兆、乡乡通5G、90%以上行政村通5G；算力规模达到280 EFLOPS（每秒百亿亿次浮点运算，FP32），位居全球前列。数据流通利用设施建设进入“快车道”。[①]但数字经济快速发展也带来了大量的数据安全和隐私保护方面的挑战，引发了人们对数据安全、数据隐私等话题的高度关注。侵害个人隐私、网络犯罪、数

① 国家数据局．数字中国发展报告（2024年）［R］．2025.

据泄露、算法滥用、平台垄断等问题不断涌现，网络安全及数据安全问题日益突出。数字经济宏观叙事背景下的数据安全、隐私泄露对个人、行业发展乃至国家经济安全的重要性不言而喻，如何加强对数字经济的规范与监管、保护消费者隐私成为重要议题。与此同时，隐私的定义也在这一过程中经历了一场深刻的变革。本小节将探讨在数字化和互联网技术背景下，隐私的新定义和内涵。

1.2.1 传统隐私观念的演变

“隐私”一词由来已久，我国传统上把隐私称为“阴私”，专指不可告人的信息，隐私是隐私权的客体，但隐私权是近代才有的提法。“隐私”一词通常出现在法律、哲学、心理学、社会学和信息科学中。然而，对于隐私究竟是什么，学者并没有达成广泛的共识。在操作上，隐私仍然是一个模糊的概念，人们很难给出明确的定义。例如，对于不同的人，隐私可能意味着不同的事情（Posner，1981；Acquisti et al.，2016）。

“隐私”一词可以追溯到1890年《哈佛法学评论》上发表的一篇题为《隐私权》的文章。Warren 和 Brandeis（1890）将隐私定义为“不受打扰的权利”，这被公认为隐私概念的首次出现。随后，关于隐私定义的哲学争论在20世纪下半叶变得异常突出，隐私的概念具有随着社会环境和技术的发展不断发展变化的特征。梳理现有文献，我们总结了以下几种隐私定义。

1. 控制观

基于个人信息控制理论，隐私被定义为一种控制个体环境的方式，个人控制领域即为隐私。更一般地说，个人信息控制理论将隐私视为一种“控制”对自身有价值的信息或空间的权利（Dinev 等，2013）。例如，Westin（1968）认为隐私是“对自我访问的选择性控制”。有的学者认为，隐私是有选择地控制他人接触自我的能力（Altman，1975）。Margulis（1977）认为，隐私是“对自己和其他人之间交互（transaction）的控制”，目的是强化“自治”的能力。Flaherty（1989）则明确地提出了将隐私作为信息控制的想法，并且将“数据保

护”发展为隐私的一个方面，这一概念为公平信息实践奠定了基础。杨立新（2003）认为，隐私是一种与公共利益、群体利益无关的，当事人不愿他人知道或他人不便知道的私人信息，当事人不愿他人干涉或他人不便干涉的私人活动，当事人不愿他人侵入或他人不便侵入的私人空间。Waldo 等（2010）认为，在家或者工作中的隐私，是指个人的决策免受政府干预、享有免受监控的自由的能力，或对电子通信和个人信息保密的能力。Smith 等（2011）则从同源的视角（cognate-based）将隐私定义为一种状态或一种控制力。信息隐私则是指：个体对自己的个人信息在何时、以怎样的方式以及在多大程度上被扩散给其他人的控制能力（Smith 等，1996；Hong 和 Thong，2013）。类似地，Acquisti 等（2016）认为隐私不是共享的对立面，而是对共享的控制。Culnan（1995）从消费者角度对隐私进行了定义，认为隐私是消费者对自己隐私信息的一种控制能力。

2. 权利观

限制接近学说认为隐私权旨在保护个人在其不愿意的情况下不被他人接近或者接触，无论是实际身体的接触，还是个人信息的接触（马特，2014）。隐私本身被视为一种内在权利，特别是作为“不受打扰的权利”（Warren & Brandeis，1890）。比如，Gavison（1984）将隐私定义为“隐藏一些关于自己的信息的权利”，以及“个体在参与社会活动时限制别的个体或者组织收集关于自己信息的权利”。她认为隐私是对个体秘密、匿名和独处三个关键领域的限制接近。当前，许多国家的法律将隐私视为一项必须受到保护的基本人权（Solove，2008），如《中华人民共和国民法典》（以下简称《民法典》）就明确规定了自然人享有隐私权。基于这种隐私概念，个人信息的处理必须受到限制。

3. 状态观

隐私还可以被视为一种能够实现自主的状态，这是一个与人格密切相关的概念。Westin（1968）通过孤独、亲密、匿名和保留四种状态来定义隐私，他认为隐私是“个人利用物理或心理的手段自愿地、暂时地将自己从社会化（过

程）中撤出”。类似地，Laufer 和 Wolfe（1977）将一般隐私概念化为一种情境概念（状态）。Margulis（2003）认为隐私指当事人有意保持的某种“状态”。王利明（2005）认为隐私是指自然人免于外界公开和干扰的私人秘密与私生活安宁的状态。需要指出的是，不同状态的隐私可能影响我们与他人的互动方式。

4. 利益观

利益观主张从保护隐私的利得出发，对隐私进行定义。例如，Milberg 等（2000）转引他人的文献，列举了 13 种与隐私有关的利益。Waldo 等（2010）认为隐私可以是一种价值或一种财产。在数字时代，个人信息被认为是一种新的商品（Spiekermann et al.，2015），具体而言，指用户可以将其个人信息作为无形资产进行交易（Xu & Gupta，2009）。一些学者认为隐私不仅是个人的一项重要权利，也是一种中间产品（Farrell，2012）或最终商品（Acquisti et al.，2016）。此外，Fairfield 和 Engel（2015）主张从公共品的视角来研究隐私。隐私的商品化为研究个人信息的价值提供了重要基础。

5. 集体规范观

Shaeffer 和 Keever（2021）认为个人数据在孤立的情况下并没有什么价值，只有与其他人所做、所说和喜欢的信息结合在一起时才变得有价值；个人数据汇总而成的大数据不是个人财产，而应被视为集体规范，因此他们提议从集体的角度对个人数据重新定义。

另外，也有学者将隐私划分为不同的维度来尝试澄清隐私的定义和范围。例如，Dienlin 和 Trepte（2015）将隐私区分为信息隐私、社会隐私和心理隐私三个维度，然后针对不同的隐私维度进行研究。

无论何种理解，隐私总是关乎自我与他人、私有（private）与公开（public）之间的边界（Acquisti 等，2016），因而总是与以下两个问题相关：控制他人对自我、自己的空间或自己的信息的接触，保持独处、免于打扰（Margulis，1977）。对于个人或者团体而言，隐私是一个主观的、宽泛的概念，它随着人或者团体的不同而不同，对于同一个人来说，隐私也随着时间的变化而变化。在

现实社会中，隐私往往是多维的、灵活的、动态的，随着生活的经验而变化，是机密、秘密、匿名、安全和伦理的概念重叠，同时依赖特殊的场景，如时间、地点、职业、文化、理由等。因此，很难给出一个明确的、公认的、通用的隐私概念和衡量标准。

具体到消费者隐私演变这一部分，消费者的隐私权指的是消费者的私人信息不被其他主体或组织者非法收集、复制、公开及利用，受法律保护的人格权；也指禁止通过网络平台泄露与消费者相关的交易信息，包括交易事实、交易记录及其他交易信息等。

在互联网技术时代，隐私的定义经历了重大的改变。传统上，隐私通常被理解为个人对于私人领域的控制权，即个人对于自己的身体、家庭、个人信息等私人信息的保护。然而，随着互联网技术的快速发展，隐私的范围已经扩展到了数字化世界中。在互联网技术背景下，隐私的定义和内涵可以从以下几个方面来理解。

（1）个人数据保护。在互联网上，个人数据的收集、存储和使用成为隐私问题的重要方面。隐私保护的关键是确保个人数据不被滥用、盗用或未经授权使用。个人数据包括但不限于个人身份信息、偏好、浏览历史、社交媒体活动等。

（2）信息安全和保密。隐私涉及个人信息的安全和保密。在互联网上，个人信息需要得到适当的加密和保护，以防止未经授权的访问或泄露。

（3）匿名性和身份保护。互联网技术允许人们以匿名或伪造身份进行活动，这也与隐私的保护相关。个人应该有权保持网络匿名状态，不被追踪或识别。

（4）权利和自主控制。隐私涉及个人对于自己个人信息的权利和自主控制。个人应该有权选择是否共享自己的个人信息，并有权决定将个人信息用于哪些目的。

（5）透明度和知情同意。在互联网技术的应用中，个人应该被告知收集和使用个人信息的目的，并在明确的知情同意下进行。

综上所述，互联网技术背景下隐私的定义已经从传统的私人空间扩展到了数字化世界。它包括个人数据保护、信息安全和保密、匿名性和身份保护、权利和自主控制以及透明度和知情同意等方面。在互联网时代，保护个人隐私成为一个重要的挑战，需要通过法律法规、技术保护和用户教育等多方面的努力来实现。

1.2.2 新技术背景下的消费者隐私定义

在数字化和互联网技术的背景下，隐私保护面临前所未有的挑战。一方面，新技术的发展使个人数据的收集和使用变得日益普遍和复杂；另一方面，现有的法律和道德框架在应对新技术带来的挑战时存在一定的局限性。在此背景下，对隐私进行重新定义具有重要意义，这关系到相关法律法规的执行。

1. 电子商务环境下的消费者隐私定义

互联网时代，网络隐私逐渐萌生、发展。在网络使用的过程中会产生大量与消费者有关的个人隐私信息：消费者进行网页浏览、购物、聊天、收发邮件等操作时，将会有相关的电脑 IP（互联网协议）、浏览网址、账号密码等信息。当前信息技术发展迅猛，这些个人信息能够被非常容易地收集和利用，这为消费者隐私的概念增添了技术色彩。

在互联网电子商务中，隐私可以作为一种能够给不同主体带来经济利益的有价商品，盗用、滥用的后果不堪设想。网络隐私权的概念开始进入公众视野，这个概念与普通的隐私权有所不同，网络隐私权更加关注对私人信息的保护，而随着信息化时代的到来，隐私保护开始由隐私内容保护向数据保护转化，这是电子商务时代消费者隐私保护的一个关键的变化趋势（王利明，2005）。在网络时代，消费者的隐私信息通常以网络作为载体，经过数字化的处理，具备匿名性、虚拟性及开放性等特点。在电子商务情境中，隐私概念又有了新的诠释。有学者认为，电子商务中的隐私可以概括为公民在从事电子商务活动时不愿被他人获知的信息或数据，即个人隐私信息（孟晓明，2010）。除了个人基本

资料信息、个人特质信息、个人信用信息、个人网络习惯和偏好等这些静态信息外，电子商务中的个人隐私信息还应包括在线交易信息、支付相关信息、浏览商品踪迹等一些动态隐私信息。

2. 大数据背景下的消费者隐私定义

在数字化和互联网技术的背景下，隐私的定义已经远远超出了传统的范畴。大数据时代的到来使传统隐私权受到了冲击，隐私权的概念也得到了新的发展，现在的隐私权不仅体现人格属性、还体现财产属性，而且更多地体现为在数据收集、处理中保护隐私权。因此，有必要将隐私权置于大数据的环境下重新定义。目前我国研究隐私权的学者大都集中于讨论网络隐私权的保护，但是很少有学者将隐私权置于大数据环境下进行探讨。比较典型的有：李德成指出在大数据环境中，公民个人的图片、言论、音频等私人信息数据均须依法予以保护，以免被非法窃取或泄露，任何个人隐私侵权的行为都将受到处罚。此外，学者蒋志培认为大数据时代的隐私权指的是，在大数据环境下公民数据信息不得任意获取，须经授权、批示才可分析或利用。从前述学者的观点可以看出，自然人享有的私人生活安宁和私人信息安全是隐私权的概念在学界达成共识的一种观点。隐私方面的文献认为，大多数用于营销目的的消费者个人信息包括以下五个方面：人口统计特征、生活方式特征、购买习惯、金融数据、个人识别信息（如姓名、住址、身份证号等）（Phelps 等，2000）。一些学者将网络和隐私结合起来，赋予消费者隐私权如下定义：大数据背景下的消费者隐私权不仅包括对自身新型数据或资料的控制权及支配权，还包括不受他人泄露、监听、刺探、公开自己隐私数据的权利。

总的来说，隐私的概念在演变过程中呈现出诸如模糊性、动态多边性、价值性和文化差异性等特点（Thomas，1992）。这给对隐私进行定义带来了诸多困难，学术界对隐私的定义也各种各样。因此对隐私进行定义时需要结合文化与社会背景。

例如，互联网广告，主要是指在线广告，包括搜索引擎广告、横幅广告、

电子邮件广告、定向广告、原生广告等。其中，搜索引擎广告是将广告内容显示在搜索引擎结果页面上的广告形式。当用户在搜索引擎中输入关键词时，与关键词相关的广告就会在搜索结果页面上显示。这种广告通常以付费的方式进行，广告主根据用户点击广告的次数支付费用。横幅广告是指在网页上以横幅形式显示的广告。横幅广告通常包括图像、文字和链接，吸引用户点击并访问广告主的网站或相关内容。这种广告形式在早期的互联网中很常见。电子邮件广告是通过发送广告信息到用户的电子邮箱中进行宣传的方式。这种广告通常采用邮件列表或个人电子邮件的方式，向用户推送与产品、服务或促销活动相关的广告内容。定向广告是根据用户的个人属性、行为或兴趣进行精准投放的广告形式。通过分析用户的浏览历史、搜索记录、兴趣标签等数据，广告平台可以根据用户的特征定向投放广告，提升广告的效果和转化率。原生广告是一种融入网页内容的广告形式，与网页的风格和布局相一致，更具有融入性和自然性。原生广告通常以文字、图片或视频的形式呈现，与网页内容相结合，以提高用户的接受度和点击率。

这些广告形式为广告主在互联网上进行产品推广和品牌营销提供了重要平台与机会。随着互联网技术的发展，互联网广告形式也在不断演变。在此基础上，隐私内涵也在不断发生变化。

（1）隐私侵犯范围由物理世界的私密空间向虚拟世界的行为信息扩大。搜索引擎的广泛使用，使得网站拥有了跟踪、记录用户行为的可能性。在中国第一例 Cookie 隐私权纠纷案件中，原告朱某发现自己利用百度搜索引擎搜索“减肥”等关键词信息，一些网站就会出现相应的广告，朱某指控百度跟踪、记录了自己搜索的关键词，并把其个人信息用于相应网站上的广告投放，这一系列行为侵犯了个人隐私权、选择权和知情权。该案件展现了搜索引擎虽然为用户检索信息提供便利，同时也带来了隐私的侵犯行为，而隐私的范围也由物理世界的私密空间向虚拟世界的行为信息不断扩大。除了 Cookie 跟踪技术外，还有电子监视、定位系统、黑客技术等为在线定向广告提供获取用户信息的手段，用户的隐私变得无处可藏。

（2）隐私侵犯形式从线上蔓延到线下。电子邮件广告营销是一种常见的广告隐私侵扰方式，由于用户无意间在不少购物网站、新闻网址上留下了自身的邮件地址，此后就会受到各种邮件直销广告的轰炸，其中涉及一些与用户私密有关的广告。部分购物网站获取了用户的个人地址信息后，不仅向用户虚拟地址（电子邮箱）发送广告，更有甚者还向用户现实地址（家庭住址）发送纸质版广告。因此，电子邮件广告隐私侵权行为已经从线上蔓延到线下，对民众生活造成严重困扰。

（3）隐私侵犯对象从广告内容向用户画像转变。隐私侵犯的行为透过广告似乎更加隐蔽、难以察觉。例如原生广告，原生广告将广告完全融入广告投放的场景中，与普通内容别无二致。原生广告由于其隐蔽性的特征，用户难以分清内容与广告的界限，同时让广告隐私侵权行为更加隐晦。与此同时，隐私侵权不再是传统媒体时代仅针对广告内容的隐私侵犯，而是转移到广告背后，通过技术这个非行动主体洞察用户画像，实现投放流程上的隐私侵犯。此外，广告隐私侵权的主体也呈现多样化，在互联网时代，每个社会主体都可能成为侵权者或是受害者。

总而言之，信息技术时代，技术构建的“眼睛”闪烁着窥伺光芒，逼近我们的隐私。我们每个人的隐私都被“盯梢”了，而隐私的内涵边界也不断扩大，由物理世界向网络世界拓宽，公、私领域边界开始融合，而广告隐私侵犯的主体则呈现多样化，侵权行为具有原生性和隐蔽性。

伴随着信息技术范式转向智能技术范式，人工智能（AI）技术作为第四次工业革命的核心驱动力，正在释放科技革命和社会变革积聚的巨大能量，将重构生产、分配、交换、消费等商业活动各环节，催生智能广告生态。智能广告的逻辑起点，主要是以人工智能、机器学习、自动化为基础的新技术。然而，智能技术也使隐私的定义和内涵变得更加复杂与多样化，带来对隐私保护的新挑战。

具体而言，隐私从道德领域转移到了市场领域，成为一种商品。隐私在人工智能时代不仅是人格权利的一种，而且成为智能社会必备的“数据养料”。其原因在于，用户隐私数据对于企业和机构而言，是培养和训练智能系统必需

的原材料。在企业人工智能技术的自动化分类、打包、聚合、标识、转移下，用户的隐私不再是固定的某一类信息，而是成为流动又宽泛的概念。在数字监控的注视下，除去固定私人信息范畴，隐私是涵盖用户 24 小时所有重点行为信息的聚合产物。在人工智能时代，平衡个人隐私权和智能社会的发展是一个重要的课题，需要企业、政府和个人共同努力来确保个人隐私得到恰当的保护，同时促进人工智能技术的创新与发展。

广告生态的变革也重构了对隐私的利用，智能广告与传统广告和互联网广告相比，最大的特点在于技术的进步和应用改变了广告的运作方式，重构了广告生态。这也导致了隐私的异化，以及人与机器之间关系的变革。在智能广告中，技术冲破了原来的限制，成为广告运作流程中的主导者。这种技术驱动的广告模式改变了传统广告运作机制，使隐私问题变得更加复杂。在这个新的环境中，隐私的现代性语境发生了根本性的改变。传统上，隐私的边界主要是公共领域和私人领域的界线。然而，随着智能广告技术的出现，人们的个人信息和数据不再局限于特定的领域，而是在流动的空间中被收集、分析和利用。可穿戴设备、算法监控、智能推荐等广告技术扩大了对人类社会隐私的时空侵犯。隐私的含义也与个人信息和数据不断融合，成为一个由个人定义的动态概念。

1）整合性

整合的隐私不是关于个人信息和数据的保护，而是将个人在不同环境中的行为和数据整合在一起，形成更全面的个人画像。首先，整合的隐私是碎片化的。随着科技的发展，个人的行为数据变得越来越分散，产生于不同的平台和设备。整合的隐私将这些碎片化的数据整合在一起，从而更好地理解个人的兴趣和行为模式。例如，通过整合个人在社交媒体上的发帖、购物平台上的购买记录和移动设备上的地理位置数据，可以得出更全面、准确的个人画像。其次，整合的隐私具有多样性。它不限于特定领域或平台上的个人数据，而是涵盖了个人在各个方面的行为和数据。这包括社交媒体活动、在线购物习惯、浏览历史、移动应用使用等。通过整合这些多样性的数据，可以更好地了解个人的兴趣偏好、消费倾向和行为模式。最后，整合的隐私是易变的。个人的行为和兴

趣可能随时间与环境的变化而变化。整合的隐私能够灵活地适应这些变化，并进行实时的数据整合和分析，从而确保个人画像的准确性和时效性，更好地满足个人需求和提供个性化的服务与推荐。

2）流动性

流动的隐私指的是将隐私概念置于流动的语境中进行审视。这是因为个人数据可以在跨平台环境中自由流动。在智能时代，隐私逐渐成为私人空间和公共领域不断交融、扩大的灰色地带，传统的“公共”和“私人”的二分法已不再存在。在智能广告平台经济的影响下，随着智能投放向跨平台流动和转移，隐私数据变得越来越“藏而不私”。换句话说，隐私不再是静态的信息，而是转变为流动的整合型隐私。在过去，隐私主要以个人信息的静态保护为目标，但现在随着不同平台和应用之间的数据交换与共享，个人数据的流动性大大提高。个人数据在不同平台之间流动，形成了更全面和综合的个人画像，并被新型广告技术用来进行更精确的投放。这种流动性导致隐私界限模糊，同时给个人数据保护带来了新的挑战。整合型隐私的流动性使个人数据变得更加复杂化、多样化和难以掌控。个人数据不再是孤立存在的片段，而是在不同平台和应用间相互关联和整合。这使个人隐私面临跨平台数据追踪、综合个人画像建模和系列隐私侵犯的风险。

3）可计算性

用户的认知具有隐蔽性和私密性，通常人类对于某一事物的观点与情感，连他们自身都难以觉察。然而，智能广告发展到高级阶段时，可以实现对用户认知进行计算分析，以实时监测用户在面对广告时的心理情绪状态。通过面部识别和智能传感等装置，可以收集和分析用户的身体行为数据，如微表情、心跳、血压等，从而推测用户的情绪、态度和喜好。这种情感分析技术可以帮助广告主更好地了解目标受众，调整广告内容和策略，以更精准地触达用户。然而，这种对用户认知的计算分析也引发了一些隐私和道德问题。监测和分析用户的情绪和个人喜好可能会侵犯个人隐私，让用户感到不舒服或被跟踪。此外，对用户情绪的准确判断也存在一定的挑战和局限性。人类的情绪和认知是非常

复杂和多样化的，仅通过技术手段来判断，可能存在误差和不准确性。因此，在进行用户情绪监测和洞察时，需要结合更广泛的信息和上下文考虑，以确保结果的准确性和可靠性。

综上所述，在人工智能时代，隐私已经成为一种商品，不仅拥有道德价值，还拥有经济价值。智能广告已经渗透到人们生活的方方面面，不仅时刻监视隐私，而且最大限度地侵犯隐私，跨越了时空限制。由于技术的特点，隐私伦理问题变得更加隐蔽，隐私保护也更加困难。人格尊严受损和自由意识受限都是隐私伦理保护所面临的典型问题。

随着人类社会进入信息高速时代，信息技术的快速发展引发的隐私伦理问题日益严重。在互联网技术范式下，隐私侵犯主体和领域都迅速扩大。隐私侵犯主体不再局限于个人或组织，而是涉及更广泛的广告主、数据收集者、数据分析者等。同时，隐私侵犯的领域也从个人生活扩展到了虚拟空间中的网络行为和数据传输过程中。在人工智能技术时代，智能广告利用技术的力量实现对用户的泛时空侵犯。由于智能技术的运用，广告的侵扰行为更加隐蔽和巧妙，很难被用户察觉。这导致隐私问题更为复杂，隐蔽性和危害性也不断增强。隐私伦理问题主要体现为个人人格尊严受损和自由意识受限。个人隐私被滥用和侵犯，会造成对人格尊严的伤害，个人失去对自己信息的掌控权，可能受到个人形象损害、个人选择受限等影响。此外，智能广告的个性化推送也可能限制用户的自由意识，让用户处于一个被操控和定向的信息环境中。综上所述，广告隐私伦理问题随着技术发展日益严重，隐蔽性和危害性不断增强。保护个人隐私和解决隐私伦理问题变得尤为重要，需要平衡广告商的商业利益与用户个人隐私权益之间的关系。

个人隐私的泄露和滥用已经成为一个关乎整个社会的问题，我们需要思考如何平衡广告技术发展与个人隐私保护之间的关系。随着技术的不断进步和广告生态的变化，隐私问题将持续存在并需要得到重视和解决。这需要社会各方共同努力，包括制定相关法律法规、推动隐私保护技术的发展、加强个人隐私意识教育等，以确保个人隐私得到充分的尊重和保护。

1.3 隐私的分类与特征

大数据时代的来临，使消费者的各种隐私信息都能够进行数字化处理，并作为新的数据被存储在网络当中，此时消费者的隐私不单纯包括自己的隐私信息，还包括隐私行为以及隐私空间等，它们之间是一种交叉融合的状态，而大数据本身具备的经济属性也使得消费者的隐私被贴上了人格属性与经济属性的标签。然而，一些企业或商家为了获得超额的利润，常常非法收集消费者的隐私信息，同自身所承担的责任和义务相违背，对消费者的隐私权更是置之不理。非正当地泄露消费者的隐私、非法交易消费者的信息等情况屡见不鲜。在这样的背景下，了解隐私的不同类型和主要特点，有助于更好地保护个人消费者隐私和权益。本部分将详细探讨隐私的分类与特征，帮助读者更深入地理解这一议题。隐私是指个体或组织在特定情况下拥有的私人信息和空间，不受他人干扰和侵犯。它是一个复杂而广泛的概念，涉及多个方面和领域。隐私可以分为多种不同类型，具有不同的特征。

1.3.1 隐私的分类

1. 根据隐私数据的获得来源分类

根据隐私数据的获得来源，消费者的隐私可分为三个类别。

1）监视隐私

监视隐私是指通过对他人的行踪及住宅、居所等进行监听、监视，安装窃听装置或者摄像设备等行为获取的隐私信息。除此之外，其还包括非法刺探调查他人的通信或其他私人文件的内容、非法刺探调查他人的性生活、非法刺探调查他人的财产状况等隐私资料的行为。如网站通过 Cookie 技术对用户上网痕迹进行跟踪，以此来监视和窥探用户网络行为；私自在他人笔记本电脑中安装远程控制软件，随即删除软件图标，之后通过远程控制软件，对他人笔记本电

脑进行录屏、摄像、浏览和下载电脑中的私人文件等操作，非法控制他人计算机信息系统，远程窥视他人日常生活的实时影像。此类隐私来源通常具有非法的特征。对于此种隐私遭到侵害的行为，可以借助问责系统和法律手段予以防护。

2）披露隐私

披露隐私是指消费者主动将其个人隐私信息提供给平台或者允许平台按照约定方式、范围和程度获取、收集、使用其个人隐私信息的行为。国内外学者对消费者隐私信息披露影响因素的研究主要通过成本收益视角，认为消费者进行隐私信息披露决策基于成本与收益的理性计算，以隐私计算理论为代表，认为消费者通过权衡感知收益与感知风险，来决策隐私披露行为（刘百灵等，2018）。感知收益对消费者隐私披露意愿具有正向影响，感知风险对隐私披露意愿具有负向影响（Dinev and Hart，2006），当隐私披露的收益大于风险时，消费者会倾向于披露隐私信息（Dienlin 等，2023）。Acquisti 等（2012）基于隐私计算理论指出，个人通过权衡隐私披露的成本与收益来决定是否披露个人隐私。比如，当对社交媒体平台信任程度较高时，消费者尽管存在积极的隐私保护态度和较高程度的隐私担忧，但为了在社交媒体上与他人互动、分享，或出于好奇、从众心理，仍然会主动披露个人信息（Zhang 等，2017）。

3）歧视隐私

大数据处理技术自身的不透明性，可能出现歧视问题，导致个人或团体的隐私泄露。例如，通过一串串反映我们基础生物学信息、人际交往关系、个人性格特征、日常行为偏好、文化审美品位的代码流，我们得以在数字空间存在并且被认识。在 2D（二维）数字时代，身份歧视主要以抽象的方式体现在具体情境中。此前备受关注的话题包括但不限于就业、阶层与种族，弱势群体的隐私泄露可能加剧统计歧视和失业（Agan 和 Starr，2018；Doleac 和 Hansen，2020）。如印度 Aadhaar 数据库的设计未将贫困考虑在内，无法识别长时间与石头、水泥、石灰为伴的工人，以及年龄在 60 岁以上的老人。黑人程序员杰基·阿尔辛（Jacky Alciné）曾被 Google 搜索引擎贴上大猩猩的标签，同时在 Google 浏览器上对“黑人”进行检索，更容易匹配到具有犯罪暗示的结果；

“家务劳动”往往与女性相关联，一名男子可以仅仅因为站在厨房中便被算法判定为女性等。身份认同以身份建构为基础，在客观身份、主观意识、社会交往的互动中结合为自身认同。在虚拟世界的身份歧视下，最为基础的客观身份反而可能构成身份认同的最大障碍，使主体产生认知层面的危机。

此外，对于消费者而言，企业越来越有动机获取消费者的私人信息，通过算法推荐、价格歧视等手段调整自身的营销方式，从而提升盈利水平，这在一定程度上损害了消费者利益。企业获得消费者个人信息后进行的价格歧视被称为基于行为的价格歧视（Fudenberg & Tirole，2000）。消费者在同一企业购买商品，企业会提供不同的价格来吸引消费者。保护隐私以制止价格歧视的效应取决于市场结构、商品数量、差异化竞争的方式和消费者对商品、隐私的偏好（Taylor 和 Wagman，2014）。

2. 根据不同对象分类

根据不同对象，消费者的隐私可分为四个类别。

1）通信隐私

国家标准《信息安全技术 即时通信服务数据安全要求》将即时通信服务数据划分为用户数据和业务数据，其中用户数据即为个人通信数据。考察即时通信服务数据的定义，个人通信数据可以被定义为通信服务提供者针对自然人使用主体所采集和制作的通信者个人信息。隐私是自然人对其隐私客体的敏感性认知（张凯亮和臧国全，2021），故个人通信数据隐私是通信服务使用者对其被采集个人数据的敏感程度认知，也是通信服务提供者对其用户通信数据在生命周期中被采集使用的个人隐私，简称通信隐私。通信技术进步推动通信业务快速扩展，产生海量具有较高价值的个人通信数据，这些数据不仅广泛应用于个性化通信服务以实现服务增值，也被其他领域大量使用以获取高额收益，导致泄露事件时有发生，严重威胁用户隐私安全。比如，2018 年圆通 10 亿条快递信息在暗网兜售，2022 年我国电信网络窃密数据传至境外等。目前在通信隐私保护方面已经从行业标准、立法、管理和技术等四个层面开展相关研究，建立

了通信数据分级分类的原则方法、通信数据生命周期隐私安全的保护规则，提升通信数据隐私风险管理水平，降低通信数据隐私风险概率。

2）位置隐私

位置隐私是指个人在物理或虚拟空间中的位置信息所享有的隐私权。随着全球定位系统（GPS）、移动网络、社交媒体等技术的发展，位置隐私保护问题变得越来越重要。

（1）在线位置服务被广泛应用于社交媒体、在线旅游、精准零售等场景中，有了海量精准位置信息的支持，其所提供的服务能更加契合用户需求，满足不同情境下的用户需求（Chellappa & Sin，2005），同时能为相关企业节省推送成本，提高利润和效率。然而用户在获取个性化位置服务时，向不可信的位置服务提供商主动提供自己的位置数据也产生了隐私风险。个人室内定位服务飞速发展带来了进一步的位置隐私问题。室内定位由用户智能手机上的传感器收集与位置相关的测量信息，并通过信息的交互计算来提供定位服务。与直接在智能手机上接收卫星导航信号并在本地进行定位的全球导航卫星系统（Global Navigation Satellite System，GNSS）不同，室内定位系统通过通信和交互计算实现定位的模式产生了特有的隐私泄露问题。用户的位置信息、移动轨迹等可能在交互计算的过程中泄露，从而造成与用户位置相关的隐私信息泄露，如生活习惯、收入水平、健康状况、宗教信仰等，给用户带来困扰，甚至危及生命财产安全。定位资源信息的泄露也将给定位服务商带来经济上的巨大损失。

（2）随着车联网的快速发展，越来越多的车辆用户连接到了车联网中，车联网给驾驶者带来了极大便利。基于位置的服务（LBS）就是其基本的应用之一，车辆日常行驶中已离不开 LBS 的支持，如实时导航和景点推荐等。但其因为开放式的网络特点，易遭受不法分子攻击，近年来黑客入侵车联网的新闻屡见不鲜。当用户使用 LBS 提供的服务时，车辆终端的定位设备向相应的 LBS 服务器提交用户此时的地理位置信息，LBS 服务器接收查询请求信息并返回结果。但是，在没有相应安全机制来保障位置查询请求安全可靠时，用户位置隐私将被轻易获取，导致敏感信息泄露，严重威胁用户生命财产安全。因此，位置隐

私泄露已成为定位服务亟待解决的瓶颈问题。

3）个人数据隐私

个人隐私数据被界定为个人不愿公开的、希望得到保护的以及经过数据分析处理仍不愿被识别公开的个人信息内容。这包括姓名、地址、电话号码、邮箱地址、银行卡号等个人信息。人类每天都会产生大量的数据，并不是所有的数据都涉及隐私，个人数据不等于个人隐私数据。个人数据是以数据载体呈现的、可以识别主体的信息。个人的私事及私生活、不愿表露的信息都属于个人的隐私，因此，只有个人数据中个人不愿公布的、希望得到保护的数据才属于隐私数据的范围。隐私数据也不等同于敏感数据，在大数据时代，原本不涉及隐私数据的敏感数据，在经过大数据技术的处理之后也有可能会侵犯个人的隐私。比如大数据的商业运用中，通过对用户海量数据的深度挖掘，分析还原用户的隐私特征（Dengler 和 Prüfer，2021）。因此，隐私数据的范围并不是简单界定、一成不变的，随着数据活动的进行，会不断产生新的隐私数据。

个人隐私数据具有三个新的特征：①隐私数据控制权受限。个人隐私数据的控制权虽然掌握在主体自己手里，但是当出于公共利益和自身利益出让自己的数据时，国家、企业就成为隐私数据的掌控者，个人没有办法直接控制个人数据。②隐私数据范围难以辨析。个人隐私数据的范围并不能简单界定出来，除了个人本身较为敏感在意的个人数据外，一些原本不涉及敏感信息的数据经过数据系统的算法分析也可能会变成敏感数据，侵犯到个人隐私；此外，每个人由于其个性特征、文化背景、生活环境的不同，对数据隐私接受程度不同，对于个人隐私范围的认知也不同。在一些人看来涉及隐私的信息，在其他人看来可能并不是很敏感，因此个人敏感数据的范围是较为复杂且不断变化的。③隐私数据泄露后果不可控。大数据时代，个人的任何社会交往都会留下痕迹，人的行为都被数据化，个人隐私数据一旦被不法分子利用，个人隐私就会暴露在公众视野之中，造成社会问题。正是由于大数据数量巨大，处理速度极快，其就具有了比传统隐私泄露更加不可估量、不可控制的破坏性。个人数据隐私

的核心是确保个人信息不被非法收集、存储、使用和泄露。

4）健康隐私

健康隐私是指个人在医疗保健领域所享有的隐私权。这包括病历记录、诊断结果、治疗方案等健康信息。《中华人民共和国个人信息保护法》（以下简称《个人信息保护法》）第 28 条通过“定义 + 列举”的方式将医疗健康信息纳入敏感个人信息范围内，因此类信息通常涉及个人身体数据、健康状况、医保支付情况，甚至家庭收入等个人不愿为他人知晓的隐私，一旦被泄露或不当利用，容易导致信息主体在日常生活和工作中遭受健康歧视、就业歧视等不公正对待。除了高敏感性，个人健康信息还具有一定的社会公益属性，在精准医疗、临床试验、基因检测等增进社会公共健康福祉的医学活动中，个人健康信息的汇聚、融合与应用将发挥必不可少的作用（高景宏等，2021）。个人健康信息的另一特点是信息主体的弱控制性，健康信息须经专业机构进行集成化处理方能充分发挥大数据价值（郭子菁等，2021），健康信息的生成、处理和利用过程，个人主体难以参与其中。实践中，个人除了在医疗机构、企业平台采集其健康信息时作出同意与否的表示之外，对自身健康信息后续利用的控制力度逐渐减弱，典型如生物样本库研究，传统的知情同意模式已不能完全满足样本提供者对自身样本用于何种研究的控制力之需。

3. 根据消费者的日常活动分类

根据消费者的日常活动，消费者的隐私可分为以下四个主要部分。

1）消费者的身份信息

该信息包括消费者在交易活动中用来反映自身身份的一切相关信息，如消费者的姓名、消费者的年龄、使用的电子邮箱、个人的身份证号以及家庭住址等。顾名思义，消费者的身份信息即为与其特定身份有关的个人信息，如一般意义上的姓名、住址、身份证号码等。其与一般意义上的个人信息相同，都以明显的可识别性为特征。身份信息与消费者的人格密切相关，因此应当完全处于消费者的控制之下，而其所蕴含的财产利益及商业价值，和其人身属性相比

居于从属地位，因此身份信息的财产利益应当完全归消费者所有。

2）消费者使用的账号信息

该信息包括消费者在所有网络活动中注册、使用的账号和密码，如社交账号及密码、通信账号及密码等。例如消费者在购物、支付等消费行为中所使用的账号，通常包括银行卡、支付宝、微信支付等。消费账号中可以记录消费记录、余额、积分等信息。消费账号的使用越来越普遍，尤其是随着移动支付的普及，越来越多的人开始使用消费账号进行支付。消费账号具有方便快捷、安全可靠，可以避免携带现金的风险，也可以方便地进行消费记录的管理和查询的优点。然而，在使用消费账号时也需要注意安全问题，一旦消费者使用的账号信息泄露，将对消费者的财产和人身安全造成严重威胁。

3）消费者财务金融状况方面的信息

该信息包括个人身份信息、财产信息、账户信息、信用信息、金融交易信息及其他与特定消费者购买、使用金融产品或服务相关的信息。例如消费者在多家网络银行以及各家金融机构中的消费记录、收支信息、交易账号、账户金额及银行卡密码等财务金融状况信息。具体而言，在个人金融信息方面，主要包括：个人身份信息，如姓名、身份证号、家庭状况等；个人财产信息，如收入情况；个人账户信息，如账号、余额等；个人信用信息，如信用卡还款情况、贷款偿还情况等。在个人金融交易信息方面，主要包括金融机构在中间业务过程中获取、保存、留存的个人信息以及衍生信息，如个人消费习惯、投资意愿等。

4）消费者在网络平台中的浏览信息

该信息即消费者在电子商务交易时以及使用或接受服务的过程中所产生的个人信息，具体内容包括浏览历史、交易记录、与电商经营者的沟通记录等。这类信息与身份信息相比并不具有强烈的可识别性，但其能够准确反映消费者在电商活动中的轨迹，通过技术手段深入挖掘和分析即可得知消费者的消费偏好和习惯、生活需求甚至是财产状况等。与身份信息相比，消费者行为信息的人格属性减弱，而财产属性增强，特别是随着经营者的产品营销模式向精准定向营销转变，分析消费者行为信息能够极大地提高营销效率、节约成本。因此

有必要将这类信息纳入消费者个人信息保护的范围，并将行为信息中的财产利益归属于消费者。

1.3.2 隐私的特征

隐私内涵丰富，根据不同的层面，可以从词义特征、消费者隐私内容特征和消费者隐私特征三个方面来分类总结隐私的特征。

1. 词义特征

从法律角度，再根据隐私的词义，可以总结隐私的两大特征：一是隐私的主体是自然人；二是隐私的客体是个人事务、个人信息和个人领域。从隐私的主体来看，隐私是自然人不愿告人或不愿公开的个人事务，是个人的自然权利，任何组织、机构、团体或他人都无权予以非法剥夺和侵犯。从隐私的客体来看，个人隐私属于私人领域，只为个人（自然人）所有，是现代文明社会中自然人的天赋财富，与公共利益、群体利益无关，不承担为公共利益、群体利益而予以公开的义务和责任，或者说，未经法律许可，无论出于何种理由，任何组织、机构、团体或他人都无权将某人的个人隐私予以公开。

2. 消费者隐私内容特征

根据消费者隐私内容的特征，可以总结出隐私具有自主性、有限披露性、可控性和敏感性等特征。

1）自主性

隐私的自主性是指个人有权自主决定何时、何地、以何种方式披露自己的隐私信息。这是个人自由意志的体现，也是维护个人权益的基础。在数字化和互联网时代，许多应用和服务都需要用户授权提供个人信息才能使用。软件供应方以此来收集用户的使用习惯，做大数据调查分析，才能为用户提供更加人性化的服务和功能。比如，零售商通过集成线上、线下以及销售目录数据库，可以获得更多消费者的个人描述信息、预测消费者的购物偏好等；GPS 服务商通过集成路网不同路段上的传感器数据，可以提供更好的道路规划与交通路线。

绝大多数消费者用户授权提供个人信息，是为了得到更高水平的服务。然而，这些服务往往在收集和使用用户信息时存在侵犯用户隐私的风险。比如，移动社交媒体中的定位功能设置，有可能暴露用户的位置和行踪，并据此推断用户的活动区域、生活习惯、兴趣爱好等个人隐私。再如，在众多的免费Wi-Fi中，不乏恶意的免费 Wi-Fi，用户一旦连接上这种 Wi-Fi，其大量的个人隐私便会在不知不觉中被迅速盗取。因此，用户应该拥有自主权来决定自己的信息是否被收集、使用或共享。

2）有限披露性

隐私的有限披露性是指个人应该在有限范围内披露自己的隐私信息。在社交媒体和其他数字化平台上，人们常常会分享自己的信息和经验，但这种分享应该是在有限范围内进行的。过度披露个人隐私可能会导致信息被滥用或侵犯他人的隐私权（Ichihashi，2020）。目前主要存在的是非正当地泄露消费者的隐私问题。非正当地泄露消费者的隐私，指的是没有明确经过消费者的允许或未获得消费者的授权，而将自己所掌握的消费者的隐私透露出去或故意允许他人进行泄露。所泄露的消费者隐私可能是正当合法收集的消费者信息，也可能是借助非法手段和非法途径获得的消费者信息。2015 年，《中国消费者报》对大数据背景下消费者的隐私保护状况进行网络调查。在涉及“大数据背景下消费者的隐私是否更加容易被非法泄露”这一问题时，76% 的网络使用者给予了肯定的回答。当被问及“最容易非法泄露消费者的隐私方式是什么”时，网络被排在第一的位置，占据了将近 14% 的比例；消费者使用的信息终端则排在第二的位置，占据了将近 13% 的比例；而相关的社交、通信等软件则占据了将近 11% 的比例。除此之外，有超过 50% 的网络使用者表示在网络消费中自己的隐私信息遭到非法泄露。因此，个人应该谨慎地选择披露隐私信息的对象和范围。权利主体有权依据自己的自由意志处置其隐私权，既可以将原来不愿意为人所知的个人秘密加以披露，也可以允许他人介入私人生活，甚至完全放弃对自己隐私权的享有，只要不违背法律规定和公序良俗即可。

3）可控性

隐私的可控性是指个人应该能够控制自己的隐私信息如何被收集、使用和共享。在数字化和互联网时代，许多应用和服务都会收集用户的个人信息（Belleflamme 等，2020）。然而，这些应用和服务在使用个人信息时存在侵犯用户隐私的风险。在大数据背景下，用户的电脑、手机以及一些社交平台无时无刻不在遭受着垃圾广告的植入和推送，而邮箱则是被大部分垃圾邮件所占据，各种推销短信、诈骗电话应接不暇。因此，用户应该能够控制自己的信息如何被使用和共享，可以通过修改个人账户设置、删除个人信息或要求服务提供商遵守隐私政策等方式实现。

（1）个人隐私的可控性是基于知情同意的原则。个人应该有权知道自己的个人信息将被收集、使用和共享的目的与方式。个人应该被告知他们的个人信息将如何被使用，以便作出知情的决策。知情同意原则确保了个人对于个人信息的控制权和决策权。

（2）个人隐私的可控性是基于透明度和可理解性的原则。个人应该能够理解自己的个人信息是如何被收集、使用和共享的，个人信息的处理过程应该是透明的。透明度和可理解性的原则确保了个人对于个人信息处理过程的可控性。

（3）个人隐私的可控性是基于访问和更正的权利。个人应该有权访问和更正他们的个人信息。如果个人发现自己的个人信息不准确或过时，他们有权要求进行更正。访问和更正的权利确保了个人对于个人信息的可控性与准确性。

（4）个人隐私的可控性是基于选择和限制的原则。个人应该有权选择是否提供他们的个人信息，以及选择他们个人信息的使用方式。个人应该能够限制其他人或组织对他们个人信息的访问和使用。选择和限制的原则确保了个人对于个人信息的自主权与控制权。

（5）个人隐私的可控性是基于安全和保护的原则。个人信息的安全和保护是确保个人隐私可控性的基础。个人信息的收集、传输和存储过程应该采取必要的安全措施，以保障个人信息的机密性和完整性。安全和保护的原则确保了个人对于个人信息的可控性与保密性。

4）敏感性

隐私的敏感性是指个人隐私信息的重要性和敏感性程度。有些隐私信息可能涉及个人的政治立场、宗教信仰、经济状况等敏感信息。这些信息一旦泄露或被滥用，可能会对个人造成严重的伤害或损失。个人信息泄露的危害包括：垃圾短信、骚扰电话、垃圾邮件源源不断；个人信息被非法买卖，复制消费者的身份证信息，在网上骗取银行的信用，在银行办理各种各样的信用卡；非法分子可能利用个人信息进行违法犯罪活动，导致消费者无辜被警察传唤或被法院传票通知出庭；丢失的银行账户或信用卡账户，重置密码后，提取账户钱款；被冒用信息，个人名誉无端受毁等。因此，这些信息应该得到特别的保护和管理。同时，一些普遍认为是敏感信息的类型，如姓名、身份证号码、电话号码等，也应该得到相应的保护和管理。

5）合法性

隐私的合法性是指个人隐私权在法律上的保护和认可。

（1）隐私的合法性是基于法律的授权和保护。大多数国家与地区都有相关的法律和法规来确保个人隐私的合法性。这些法律和法规规定了个人信息的收集和使用的条件与限制，要求数据控制者获得个人的同意和遵守数据保护原则。例如，欧盟的《通用数据保护条例》规定了个人数据收集和使用的条件，强调个人隐私和数据保护的重要性。

（2）隐私的合法性是基于个人权利的保护。个人隐私权是一种基本的人权，法律文件规定了个人对于其个人信息的控制权和保护的权利。个人有权决定自己的个人信息是否被收集，以及如何使用。个人隐私权的保护是为了维护个人的尊严、自由和自主权。

（3）隐私的合法性是基于公众利益和社会稳定的考虑。个人信息的滥用和泄露不仅对个人造成损害，也对整个社会造成负面影响。个人信息的滥用可能导致社会信任度下降、商业活动受到限制、创新能力受到抑制。因此，保护个人隐私对于维护社会公众利益和社会稳定是至关重要的。法律的制定和执行旨在平衡个人隐私与公众利益之间的关系。

（4）隐私的合法性是基于技术和安全的保护。随着科技的不断进步，个人信息被泄露和滥用的风险在增加。因此，保护个人隐私需要依赖技术手段和安全措施。例如，数据加密、访问控制和安全协议等技术可以有效保护个人信息的安全。

6）相对性

隐私是相对的，不同的人对隐私的界限和需求有所不同。个人对隐私的感知受到文化、社会环境、个人经验等因素的影响。例如，在某些文化中，个人信息的保护较受到重视，而在其他文化中，信息的公开和分享更为普遍。因此，隐私的特征是相对于个人和社会背景而言的。

（1）隐私的相对性体现在个体差异上。每个人对于隐私的需求和关注点可能有所不同。一些人可能更关注个人身体和健康信息的隐私，而另一些人则可能更关注社交媒体上的个人信息隐私。个体的价值观、生活经历和文化背景不同，其对于隐私保护的需求有所差异。

（2）隐私的相对性体现在文化差异上。不同的文化对于隐私的定义和重视程度有不同的观点。一些文化倾向于注重个人隐私和私人空间，而另一些文化则注重集体利益和公共事务，对于个人隐私的重视程度相对较低。例如，个人主义文化强调个体的权利和自由，对于个人隐私的保护较为重视；而集体主义文化强调集体的利益和社会的稳定，对于个人隐私的保护重视程度则相对较低。

（3）隐私的相对性体现在社会环境和技术进步上。随着社交媒体、大数据和物联网（IoT）等技术的发展，个人信息的收集和使用变得更加普遍与便捷。一些人可能更愿意分享个人信息，以获得更多的社交和商业机会，而另一些人则更关注个人信息的隐私和安全。社会环境和技术进步的不同，对隐私的相对性产生了影响。

（4）隐私的相对性体现在法律和政策的不同上。不同国家和地区对于隐私保护的法律与政策存在差异。一些国家和地区对于个人隐私的保护非常严格，制定了详细的法律和规定来保护个人信息的安全与隐私；而另一些国家和地区

则对个人隐私的保护相对宽松。这些法律和政策的不同导致了隐私的相对性。

7）个人性

隐私是个人的权利，是每个人作为独立个体的一部分。每个人都有不同的隐私需求和偏好，因此隐私的特征与个人的主观感受和价值观息息相关。个人性质使得隐私具有个体化、多样化和主观性的特征。作为个人，每个人都有权自由选择隐私信息的分享。

8）动态性

隐私是具有动态性的，随着技术和社会的变革，隐私的定义和范围也在不断演变。新兴技术的出现，如互联网、社交媒体、大数据等，给个人隐私带来了新的挑战。随着社会的发展和观念的变化，人们对隐私的看法和需求也在不断变化。因此，隐私的特征是不断变化和适应新环境的。

（1）隐私的动态性体现在技术的发展和应用上。随着科技的进步，个人信息的收集、存储和分析变得更加容易和全面。例如，社交媒体、智能手机、物联网等技术的普及使个人信息的生成和传输变得更加频繁和广泛。这些技术的应用和使用方式不断演变，对隐私的挑战也日益增加。因此，隐私的动态性需要与技术的发展和应用相适应。

（2）隐私的动态性体现在社会和文化的变化上。不同社会和文化对于隐私的定义和重视程度有所不同。随着社会的进步和文化的演变，个人对于隐私的需求和关注点也会发生变化。例如，在一些传统文化中，个人隐私的保护可能相对较弱，而在一些个人主义文化中，个人隐私的保护可能更加重要。因此，隐私的动态性需要考虑社会和文化的变化。

（3）隐私的动态性体现在法律和政策的不断修订与调整上。随着数字化时代的到来，各国和地区都制定了相关的隐私保护法律与政策。然而，随着技术和社会的变化，现有的法律和政策可能需要不断修订和调整，以适应新的隐私挑战和需求。

（4）隐私的动态性体现在个体意识和行为上。随着人们对于隐私权的认识和关注度逐渐提高，个体对于自己的隐私权的保护也会更加积极。个体意识的

提升将会对个人信息的共享和使用行为产生影响，从而使隐私的界限和保护机制发生变化。

消费者隐私保护的重要性日益凸显，由于互联网和大数据技术的发展，个人信息越来越容易被收集、使用和共享。因此，了解隐私的分类和特征对于制定有效的隐私保护策略至关重要。

3. 消费者隐私特征

消费者隐私具有与传统民法中的隐私所不同的特征。

1）主体是自然人

消费者隐私具有严格的人身性，主体可以是成年人，也可以是未成年人。只要是为生活需要而购买、使用商品和接受了服务的个人，都是消费者隐私权的主体。法人和其他社会组织没有自然人的精神活动，因而无隐私权，即便是有自己的秘密，也是商业秘密。隐私权为自然人专属享有，具有专属性，特定的自然人享有该项权利时不能将其转让给他人。

2）内容的不断扩展

传统的个人隐私包括姓名、出生年月、身份证号、婚姻状况、家庭情况、教育背景、收入、病历、职业、指纹、特征等数据。随着社会的发展，消费者的隐私还表现为电子邮箱、网络账号、电话号码、消费习惯、消费时间、购买的物品等。随着科技的发展，很多传统社会中不认为是隐私的内容都将成为名副其实的隐私。尤其是随着大数据的不断扩大、更新并产出新的数据，在网络触及、应用的地方，都会伴随着数据的活动，而这些数据的活动通常是在隐私主体不知情或无法控制的场合发生的。对于借助数据来获得非法收益的觊觎者，大数据实行开放是一件有利的事情，但是在实际开发、利用大数据的过程中，却容易出现过度挖掘数据隐私的情况，造成隐私权被侵犯。Risk Based Security（RBS）机构的数据泄露报告显示，2021 年度全球公开披露的数据泄露事件有 4 145 起，共导致 227.7 亿条数据被泄露。2021 年 1 月，2 亿多条中国公民信息被发现在暗网出售，其中包括 QQ 和微博的信息；同年 7 月，美国 LinkedIn 公司

7亿多条用户信息被泄露。[①] 从上述隐私信息频频被泄露的事件来看，隐私被泄露的范围、数量不断扩大，而用户的隐私被侵害的程度也在不断加重。因此，数据的开放性同消费者的隐私保护之间的矛盾也在不断被激化。

3）易侵害性

消费者在消费过程中处于弱势地位，极易泄露自己的隐私，经营者收集消费者的个人资料，以此作为商业活动的依据，可能会构成对消费者的侵权。在大数据时代下，公共领域同私人领域之间的信息不是彼此孤立的，而是呈现出交叉、融合的状态，这样就给消费者隐私侵权行为及侵权范围的界定带来了困难。消费者在进行网络购物时，常常借助智能工具将个人的相关数据转移到为自己提供服务的服务商手里，而数据在经历第三方媒介的介入以及多方交易以后，其信息的边界则会变得模糊不清，甚至面临逐渐消失的风险。令人熟悉的是，谷歌在2007年推出了一款街景服务，主要为顾客提供全方位的地图，但是街景车在拍摄的过程当中能够“无意”拍摄到一些私人画面，这在极大程度上增加了公众隐私被泄露的风险，致使街景地图饱受争议。此外，不同信息之间的交叉、融合增加了隐私侵权界定的难度。在一些公共服务的领域中，大数据智能分析及精准定位等功能会将消费者的消费偏好暴露无遗。特别是一些大型的互联网企业，借助大数据能够分析出消费者的购买记录以及浏览商品的信息，进而为目标消费者不定期推送一些商品信息。因而，大数据在为消费者提供所需商品信息的同时，也会给另一部分消费者带来苦恼，这些遭受广告骚扰的消费者却由于数据边界的模糊而无法维护自己的隐私权。

4）客观的限制性

消费者隐私具有客观的限制性，即为了维护国家安全或完成正当的法律程序，需要对消费者隐私权做必要的限制。个人信息具有促进创新（Goldfarb和Tucker，2012）、提高统计精确度（Abowd和Schmutte，2019）等作用，因此社

① 绿盟科技.《网络安全2022：守望高质量》报告之数据安全热点事件与趋势解读[R/OL].(2022-03-15). https://blog.nsfocus.net/rbs-data-security/.

会福利最优的隐私保护应该在一定限度内。适当的隐私保护本身并不阻碍反而促进个人信息的收集、共享和利用。在保护消费者隐私的同时，必须旗帜鲜明地反对“凡私必隐”。个人隐私应得到社会尊重与公民遵守国家法律并不矛盾。从政府的角度来看，相关的行政部门在掌控信息数据方面拥有绝对优势。行政部门通过对信息数据进行深度挖掘，可以获取信息数据的潜在价值，为其在提供服务过程中给予数据支撑。第一，大数据能够帮助行政部门对流通中的数据进行快速获取、高效处理及深度分析，促进不同部门之间的协同合作，从而更好地提高其行政效率。第二，通过大数据量的积累，行政部门能够分析国家的发展趋势及经济走向等相关信息，为政府进行决策提供更加科学的支持，进一步提升政府对突发状况的预警能力及应急能力。第三，大数据可以为政府收集民情、征询民意提供多重、可靠的网络渠道，推动政府公务朝着更加公开化与透明化的方向发展，便于民众参与到政府制定、执行决策中来，并给予及时的反馈与监督。大数据的开放性为社会的发展和经济的进步提供了强有力的帮助（Hughes – Cromwick 和 Coronado，2019；Abowd 和 Schmutte，2019），因此需要对消费者隐私权做必要的限制。

第 2 章
消费者隐私的重要性

在新技术背景下，消费者隐私的重要性逐渐成为众多研究领域关注的焦点。随着信息技术的迅速发展与数据驱动经济的兴起，个人隐私信息被更加广泛地收集、使用及交换，其中包括个人身份信息、消费习惯、位置数据等。这些信息的积累和分析为企业提供了前所未有的市场洞察力，同时也加强了服务个性化和客户体验的优化。然而，这种无处不在的数据收集活动也引发了隐私泄露的深刻担忧。一方面，消费者对个人信息被滥用的风险越来越敏感，如数据泄露、身份盗窃和个人信息被用于不正当营销。另一方面，当消费者意识到其隐私被侵犯时，可能会产生对企业的不信任，这可能损害企业的声誉并对企业造成经济损失。科技进步对隐私的影响是一把复杂的双刃剑。从积极的角度看，新技术如云计算、大数据分析和人工智能为个人隐私保护提供了新的技术手段与机制，如通过匿名化和差分隐私技术降低个人信息泄露的风险。从消极的角度看，这些技术也可能被用于更深入和更隐秘地监控和分析消费者行为，从根本上加剧了隐私侵犯的潜在威胁。在法律和道德层面，保护消费者隐私权成为构建健康数字经济的核心原则。例如，欧盟的《通用数据保护条例》正是为了更好地保护个人数据而设立的。企业和组织需要遵循这些规则来确保合理使用个人数据，同时保证消费者的知情权和控制权。在该背景下，本章重点探讨了

消费者隐私的重要性，主要包含个人权益、社会发展和经济发展三个方面。隐私对个人来说具有深远而重要的意义，涉及个体的自由、尊严和权益。在数字时代，隐私问题变得尤为突出，因为个人信息的收集、存储和处理变得更为便捷。

2.1 隐私与个人权益

2.1.1 隐私权是法律赋予公民的一项重要权利

“隐私”一词源于美国，用以指代与他人无关且不愿为他人知晓的私人生活领域。随着社会的进步，人们越来越重视其中的“独处性权利”。1890 年，Warren 与 Brandeis 发表了《隐私权》，将隐私权定义为个人权利，并具体表述为“个人独处的一般权利”，使得隐私权成为一项民事权利被广为人知。1960 年，Prosser 总结了数百个涉及个人隐私侵权的判例，归纳了隐私侵权的四种表现形式：盗用、侵扰、扭曲误导和公开私生活。这些行为包括：未经授权地使用他人的肖像、姓名等以获取利益；干扰他人的宁静生活、入侵他人的私密空间、扰乱私人事务等；通过歪曲事实、隐瞒真相等方式让他人受到侮辱；揭露他人的私人生活细节等。尽管 Prosser 的分类在当时引起了不同的看法，但至少有 28 个州采纳了他的分类建议，为隐私权的法律保护奠定了基础。

随着对隐私保护的广泛重视，世界各国也纷纷把隐私权作为一项基本的人权，制定相应的法律予以保护，如英国 1998 年通过的《人权法案》、日本宪法第 13 条，美国制定的《隐私权法》《财务隐私权利法》，以及针对现代信息技术侵权行为的《电子通信隐私法》等。

随着社交媒体、搜索引擎、云计算、大数据等信息传播技术的快速发展，个人隐私所面临的侵害和威胁被放大，这对个人隐私的保护构成了巨大的挑战。因此，2012 年初，欧盟发布了一项有关个人信息保护的改革计划。该改革计划赋予人们一项与个人信息相关的新权利——“被遗忘权”，即人们有权要求相

关机构删除他们的个人数据，并同时防止这些个人数据进一步传播。2014 年 5 月13 日，欧洲法院也通过了谷歌案的裁决，确认普通公民的个人隐私享有“被遗忘权”。

在我国法律中，隐私权的保护经历了不断完善和进步的过程。20 世纪 80 年代，根据《中华人民共和国民法通则》（以下简称《民法通则》）的相关规定，保护公民名誉权间接地发挥了保护公民隐私权的作用。1986 年，《民法通则》首次明确将精神性人格权规定在“人身权”中，但并未明确规定隐私权。1988 年，《关于贯彻执行〈中华人民共和国民法通则〉若干问题的意见（试行）》对《民法通则》中的名誉权进行了扩大解释，可以在侵害名誉权的制度下对隐私侵权者追究其侵权责任，以类推适用于名誉侵权的裁判方式对个人所受的隐私侵害实施司法救济。

2001 年，最高人民法院颁布了《最高人民法院关于确定民事侵权精神损害赔偿责任若干问题的解释》，通过这一司法解释，隐私权的间接保护得以转变为直接保护。但是，隐私权并未成为具体的人格权，而是一种具体的“人格权益”。2005 年通过的《中华人民共和国妇女权益保障法》修正案中首次明确规定了“隐私权”。直到 2009 年的《中华人民共和国侵权责任法》中，首次对隐私权作出规定。隐私权正式成为法律层面上的一项民事权利，并具有普遍性。至此，我国的立法已经完成了对隐私权的确认，但尚未明确界定隐私权的概念和保护范围。

2017 年 10 月 1 日施行的《中华人民共和国民法总则》（以下简称《民法总则》）对隐私权作出了积极规定。在《民法总则》中，明确规定了普通隐私权，并规定了一种特殊形式的隐私权，即信息隐私权，普通隐私权规定在第 110 条中，信息隐私权规定在第 111 条中，“自然人的个人信息受法律保护。任何组织和个人需要获取他人个人信息的，应当依法取得并确保信息安全，不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息”。《民法总则》的这一规定，是为了在互联网时代区分传统的信息权和隐私权。制定信息隐私权的规定，正是因为当时个人信息存在被非法收集、整理、

存储、泄露、买卖的风险。2021 年 1 月 1 日生效的《民法典》对隐私权的含义、效力和适用范围进行了相对详细的规定，明确“隐私是自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息”。

隐私权是消费者的一项重要权利，法律保障了消费者在数字时代能够享受安全、可靠的消费体验。消费者数据隐私具有鲜明的权利属性，具有人格权和财产权双重法律属性。一方面，消费者隐私具有人格权属性。从数据流通环节看，消费者是数据的产生主体。无论是消费者主动提供的个人信息，抑或是其在网络上的浏览行踪，都会被一一记录形成数据。这些数据不仅包含消费者姓名、性别等一般信息，还包括医疗信息、生物数据、家庭住址等隐私信息，此外还有通过收集、分析系统记录的浏览数据得到的用户偏好等私密信息。以上数据可以单独或者结合起来用于准确识别消费者个人信息，因此具有强烈的人格权属性，一旦泄露，会对消费者造成严重隐私侵害。另一方面，数据隐私具有财产权属性。学界对财产权的认定从三个方面进行：第一，以财产为客体；第二，具有经济价值；第三，具有可转让性。《民法典》第 127 条将“数据”和“虚拟财产”并列，从体系上可以认为数据和虚拟财产性质相同，均为财产。数据权利满足财产权的第一个要件。随着大数据技术产业以及平台经济的快速发展，互联网企业以用户数据的收集和使用为基础，利用算法分析进行用户画像，精准定位用户需求，吸引用户以及商户入驻，从而实现经济利益。除此之外，我国还成立多个数据交易平台以促进数据资源流通，互联网企业可以在平台上交易其控制的数据并获得对价。故数据不仅具有经济利益，还能流通交换，流通过程中数据附带的经济利益随之流向交易对象。

在现实生活中，消费者可以通过行使隐私权来确保个人信息的安全，要求企业或组织制定透明的隐私政策，并选择是否披露个人信息。如果消费者的个人信息被滥用或泄露，他们可以向相关机构投诉，并寻求法律救济，要求企业或组织承担相应的法律责任。隐私权是指个体对于其个人信息、行为和空间的控制权。这种控制权使个体能够决定自己的信息何时、何地、以何种方式被分

享、收集或使用。隐私权的核心是个体对自身信息的自主管理和控制。

2.1.2 隐私对个人权益的影响

1. 隐私影响消费者网络安全

随着信息化在人类社会中的纵深发展，以及大数据技术在各个领域的全面渗透，隐私不再局限于有形的“屋檐下的安宁”，其外延不断拓展，与个人数据交错、叠加。个人信息的保护可以被看作在大数据时代发展的隐私权的一种新维度。将个人信息和个人隐私视为一体，对消费者的保护更为有利。首先，在大数据时代，随着数据量的增加和技术的进步，利用数据叠加等方式可以很容易地识别消费者个人的身份信息。即使一开始被认为是“非私密信息”，在大数据分析的过程中，个人隐私可能也会被还原出来。因此，个人信息可以被视为一种“私密信息”或“个人隐私”。其次，个人隐私不仅包括个人账户，还包括其他敏感的个人信息。对于“账户”这一敏感信息，《个人信息保护法》要求采取特殊的处理规则。最后，信息技术的发展给传统的规范制度和行为习惯带来挑战，个人隐私权保护的存在感逐渐减弱。大规模的个人隐私泄露问题日益严重，这引发了人们对于“隐私已死”的担忧。

保护隐私能有效预防身份盗窃、虚假推销和其他潜在的个人信息滥用风险，确保消费者的经济生活和社交生活能够在安全与可靠的环境中展开。在数字时代，个人信息的收集和使用已成为商业活动中的常态。许多公司和组织使用消费者数据来观察、推断和控制消费者的利益。这种滥用可能包括：营销商试图操纵消费者的偏好，企业使用个人数据进行歧视性排序、提供有针对性的个性化宣传等。定向广告是互联网企业通过多种渠道来获取用户的个人信息、网络浏览行为及消费历史等数据，对收集来的数据进行处理和分析，形成用户画像并挖掘目标用户的个人偏好或需求，从而在用户访问移动应用或移动网页时实现精准投放的广告模式。定向广告是在收集和分析消费者个人信息的前提下提供个性化的广告服务，而收集和分析消费者个人信息的过程也是在不断“透

视”消费者的隐私。当消费者在享受定向广告快速发展带来的精准性、便利性等各种利好的同时，个人隐私信息被泄露、盗用甚至贩卖事件时有发生，骚扰、诈骗电话、诈骗邮件依然猖獗，成为全社会和广大消费者共同关注的问题。2016 年 12 月，京东被曝用户账户信息遭泄露，数据量高达 12 G，包括消费者的邮箱、电话号码、身份证号等多维度隐私信息。① 2018 年 3 月，Facebook 超过5 000万用户信息被泄露。2020 年 4 月，2.67 亿个 Facebook 账户信息在暗网和黑客论坛上以 500 英镑的价格出售，不仅包含用户的个人 ID（身份标识号）、账户名称，还包含用户姓名、电话号码、电子邮件、出生日期等多项敏感信息。②

隐私权保障了个人的自由。每个人都有权决定自己的思想观念、宗教信仰、行为活动和生活方式，而这些都是构成个体独特性的一部分。如果个人的隐私受到侵犯，就可能导致其自由受到限制，进而影响其个体发展的多样性。

2. 隐私影响消费者个人声誉和心理健康

消费者个人声誉受隐私披露和保护水平的直接影响。消费者的个人声誉通常在信息共享和交流的背景下构建与理解，隐私则作为个人信息流动的一个关键调节器（Acquisti et al., 2015）。当消费者的个人信息被收集、分析和共享时，其个人声誉便受到外界观感的影响。实体如企业、政府机构乃至个人，都可能基于这些信息对消费者作出评价或决定（Solove, 2007）。不必要的信息泄露可能导致与消费者利益不符的声誉构建，如个人信用评分的降低或在社交圈中负面舆论的形成（Boyd & Hargittai, 2010）。隐私的缺失可能引发背景信息不匹配的问题，意味着某些个人信息可能被剥离出其原始上下文，从而在新的上下文

① 网曝疑似京东 12G 用户数据遭泄漏[EB/OL].（2016 - 12 - 12）. https://news. cctv. com/2016/12/12/VIDEJEi0ZYTFRWxNWpKURD7Y161212. shtml;京东数据泄露门[EB/OL].（2023 - 04 - 08）. https://baike. baidu. com/item/% E4% BA% AC% E4% B8% 9C% E6% 95% B0% E6% 8D% AE% E6% B3% 84% E9% 9C% B2% E9% 97% A8/20278514？ fr = ge_ala.

② 杨露雅,蔡绍硕. 浅析公民隐私信息保护的伦理进路——从“Facebook”数据泄露事件谈起[J]. 记者摇篮,2023(2):36 - 38.

中被误解或误用（Nissenbaum，2009）。个人隐私泄露可能影响个人信用和社会评价，进而影响个人声誉（Taddicken，2014），尤其是当这些信息被恶意使用时。例如，个人信息被用来误导、诽谤或进行身份盗用时（Solove，2007）。信用评级机构能够通过个人消费数据预测其信用行为，一旦这些数据被错误运用或者泄露，即可能对个人声誉造成损害（Pasquale，2015）。消费者的声誉不仅与他们的社会地位和交际网络密切相关，还可能影响他们的信用评分和就业机会。

个人信息泄露可能涉及个人隐私方面的问题，这会给受害者带来一定的心理压力和困扰，严重时甚至可能导致心理健康问题。隐私侵犯可能导致消费者焦虑、不信任以及对技术的抵触。信息泄露导致的个人声誉问题累积，能够进一步引发消费者的心理压力，甚至导致长期的心理创伤（Acquisti et al.，2015）。消费者担忧个人信息的安全，可能会引发慢性压力反应，这些压力反应与抑郁症状有显著的相关性（Laufer & Wolfe，1977）。另外，个人信息的控制为消费者提供了一种自我表达的手段，而这种表达是自尊建立的重要组成部分（Burgoon，1982）。一旦消费者感觉到个人信息被泄露或滥用，他们的自尊心就会受损，长期会影响心理健康和幸福感（Hargittai & Marwick，2016）。根据 1973 年美国卫生、教育和福利部的一份有影响力的报告，“人们普遍认为，个人隐私对我们的身体、心理、社会和道德福祉至关重要”。爱因斯坦认为：“隐私是有价值的，因为它是一种手段，可以减轻在处理社会关系中产生的个人紧张关系。”对消费者而言，隐私是一种宝贵的资源，可以让个人在消费过程中减轻可能产生的压力和不安，使他们能够放松心情、充实内心，更好地处理和适应快节奏的消费生活。如果消费者担心他们的个人信息被过度收集和利用，他们可能会感到不安或受到影响，从而无法作出真实和理性的消费决策。隐私的保护可以增强消费者的信任感，使他们有更大的自由去作出符合自己需要和偏好的选择，而不受外部干预和操纵的影响。

由此可见，隐私对消费者的个人声誉和心理健康具有显著影响。在个人声誉方面，隐私泄露会导致消费者在社会中的信任度下降和信用评价不良。而在

心理健康领域，隐私侵犯感知与慢性压力、焦虑以及自尊心下降等负面心理状态关联紧密。在数字时代，保护消费者隐私不仅是法律和道德问题，也是公共健康问题。因而，亟须政府部门、企业和社会各界共同努力，形成有效的隐私保护机制。

隐私也与个体的尊严感和人格权息息相关。每个人都希望能够在某些情境下保持独立性和自尊，而这种保持需要一个私密的空间。当个人信息被滥用或未经允许地被揭示，可能伤害到这个人的尊严感和人格权。

3. 隐私影响消费者知情权

隐私权的保护程度往往与消费者获取信息的能力、数量以及质量直接相关。在互联网时代，消费者个人信息处理在现实中充满着挑战和矛盾，特别是在定制服务和个性化广告日益普及的背景下。

在线上交易的场景之下，消费者往往处于独自选购商品的状态，在进行消费时无法与他人就每一件商品的现时价格进行及时对比，自然也无从得知自己所选购的商品或服务的真实价格与他人可能支付的价格。消费者当前所看到以及最终支付的价格，由于大数据技术的干预而与商品的实际价格存在出入，这种出入并非由商品本身优惠或降价引起，而是算法基于对该消费者的相关数据分析从而为其“专门定制”，这种行为与消费者天然享有的知悉真情权相冲突，侵害了其正当权益。在进入平台时，消费者基于对平台政策和协议内容的不了解，对《用户协议》一般都会直接选择“同意”。同时，一些平台在用户未勾选“同意”之前是无法正常进入的。尽管表面上消费者同意了平台经营者对自身数据的收集行为，但平台只是获得用户的表面许可，消费者对于平台收集、利用自己的个人信息构建用户画像，以及后续对信息的使用和平台之间的信息共享等情况并不知悉。因此，平台所提供的《用户协议》实际上对于消费者的知情权并没有起到应有的保护作用。

消费者知情权范围包括差异化定价。《中华人民共和国消费者权益保护法》（以下简称《消费者权益保护法》）第 8 条规定，消费者享有知悉其购买、使用

的商品或者接受的服务的真实情况的权利。但第 28 条所规定经营者应当告知消费者有关产品或服务信息的义务则比第 8 条规定更为具体。由此看出，法律特别规定网络购物等特殊领域中的经营者应当主动告知消费者商品或服务的信息，而不是需要消费者来主动询问。这是因为网络购物等特殊领域的经营者与消费者之间的信息不对称，相较一般消费购物更加明显，消费者无法看到商品实物。另外，网络经营者具有实时改价的能力，因此对网络购物等特殊领域中的消费者的知情权保障力度应更大。

隐私权的保护与消费者知情权之间的关系是复杂的权衡和博弈。强化隐私权保护往往意味着限制企业对消费者个人信息的收集与使用，这可以避免消费者受到不当的市场影响和利益损害（Acquisti et al., 2015）。然而，隐私保护措施也可能限制消费者获取那些有助于其作出更加明智的购买决策的信息（Goldfarb & Tucker, 2011）。具体来说，提升消费者对隐私权及其影响的认识以及加强数据保护立法，如《通用数据保护条例》、《加利福尼亚州消费者隐私法案》（CCPA）等，有利于增强消费者关于个人数据如何被应用的知情权。消费者通过隐私权的行使也能够在事前得到适当信息，并在个人数据处理中享有决策权（Culnan & Armstrong, 1999；Cohen, 2018）。但是，过度的隐私保护可能导致信息的不对称，使消费者无法获得一些对他们潜在有益的信息，如基于偏好的折扣信息、个性化的产品推荐等（Hoofnagle, 2009）。此外，隐私权的强化同样可能增加企业的合规成本，这些成本可能转嫁到消费者身上，以价格提升的形式体现出来（Romanosky, 2016）。

因此，寻求隐私权与知情权之间的平衡点，鼓励政策制定者、企业和消费者之间的对话，并通过技术手段［比如隐私增强技术（PETs）］提升数据处理的透明度和控制性，以增强消费者的知情权且不对隐私权造成过度侵犯是需要解决的重要问题。

4. 隐私影响消费者自主选择权

消费者自主选择权（consumer autonomy）指的是消费者在完全信息和自由

意志的基础上作出选择的能力，其核心是消费者能够控制自己的消费行为，而不受外界不正当干预。无论是线上还是线下都存在海量商品和各种服务，哪种商品或服务能令消费者满意，只有消费者亲自甄别方能知晓。《消费者权益保护法》第 9 条规定赋予消费者对商品或服务的选择权，自愿性和自由性是该权利的最大特征。选择的自愿性体现为消费者在进行消费时不受任何外在因素的影响和干扰；选择的自由性是指消费者在消费时是自由的，经营者不得强行改变消费者意愿。

当消费者的个人隐私受到侵犯时，其自主选择权可能会受到制约。这不仅因为消费者的个人信息可能被用于商业行为目的，还因为信息的不对称性可能导致消费者的选择受限。隐私侵犯可能导致个人信息被滥用，产生消费者不愿意接受的后果，如价格歧视或欺诈。在大数据“杀熟”行为中，经营者在消费者不知情的情况下进行差异化定价，造成“千人千价”的情况。假设消费者明知对自己将要购买的商品或服务不是唯一定价，很有可能会作出不同选择。而消费者并不知道差异化定价的存在，对商品或服务的价格信息了解得不全面，因此无法真正做到自由选择。另外，市场上的某些机制以及隐私政策的不透明性可能限制消费者的选择。例如，通过复杂或模糊的隐私政策，公司可能会使消费者难以理解其个人信息如何被使用和共享，进而影响其真实的选择行为。

在数字时代，消费者隐私受到前所未有的挑战。大数据分析和人工智能技术的应用使企业能够基于消费者的个人数据进行精准营销，这进一步复杂化了隐私与自主选择权的关系。消费者可能会被“嵌入式选择”所影响，在某种程度上，他们的选择是由提供服务的平台预设的结果。个人数据的细粒度利用可能会导致消费者被操纵，甚至在不知情的情况下被推送可能并不符合他们真实需求和偏好的产品或服务。同时，这种嵌入式选择可能也会让消费者在不知情的情况下购买并不需要的产品或服务，从而增加了消费者的购买风险。

隐私和个体的自主权与自我决定权密切相关。每个人都应有权利决定自己的信息是否被公开，以及在何种程度上公开。这种自主权的存在使得个体能够更好地参与社会生活、政治生活和经济生活，同时也使社会显得更加多元和包