昆明学院学报　2022，44（1）：81～87　　ISSN 1674－5639　CN 53－1211/G4
Journal of Kunming University　　【法学】

个人信息双重属性的平衡

——基于“场景理论”的创新应用

魏嫱林，张然滔
（四川大学 法学院，四川 成都 610207）

摘要：我国现行法律以可识别性为标准，对所有个人信息实行无差别“知情－同意”原则的保护，这不仅使得同意原则在实践中流于形式、实施成本高，还导致个人信息的保护与利用之间的不平衡。引入场景理论，以个人信息类别以及信息的生命周期为要素构建类型化的场景，并对场景的风险进行评估，适用差异化的同意原则，通过约束个人信息处理者为其实施提供保障，以平衡个人信息的双重属性，兼顾个人信息的利用与保护。

关键词：个人信息；双重属性；同意原则；场景理论
中图分类号：D923　**文献标志码**：A　**文章编号**：1674－5639（2022）01－0081－07
DOI：10.14091/j.cnki.kmxyxb.2022.01.013

The Balance of the Dual Attributes of Personal Information:
Innovative Application Based on “Scene Theory”

WEI Qianglin, ZHANG Rantao
(Law School, Sichuan University, Chengdu, Sichuan, China　610207)

Abstract: Our country's current law adopts the standard of identifiability and implements the principle of undifferentiated “informed-consent” protection for all personal information. This not only makes the principle of consent a mere formality in practice and high implementation costs, but also leads to an imbalance between the protection and use of personal information. It is necessary to balance the dual attributes of personal information, take into account the use and protection of personal information, introduce scenario theory, construct typified scenarios based on personal information categories and information life cycle, evaluate the risks of scenarios, apply differentiated consent principles, and provide guarantees for their implementation by restricting personal information processors.
Key words: personal information; dual attributes; consent principle; scene theory

一、引言

大数据时代，信息成为当今社会发展的重要资源，个人信息保护也成了社会关注的热点问题。互联网技术的发展，使得个人信息的获取与流通更加便捷。然而，在对个人信息利用的过程中，存在大量滥用个人信息、侵害公民权利的行为，例如：因个人信息泄露导致犯罪分子通过非法获取个人信息进行精准的电信网络诈骗等行为。根据我国公安部发布的2020年全国打击治理电信网络诈骗违法犯罪的数据来看，全年共破获电信网络诈骗案件有32.2万起，累计挽回经济损失1 870余亿元[1]。由此可见，保护个人信息和利用个人信息之间存在一定的冲突。究其原因，是个人信息的个体属性与公共属性之间的矛盾。个人信息不仅承载个人利益，还与数字经济发展、政府治理等公共利益密切相关，企业和政府可以通过收集、分析个人信息实现精准预测，并据此做出决定或采取行动。基于个人

收稿日期：2021－08－09
作者简介：魏嫱林（1998—），女，四川巴中人，硕士研究生，主要从事民商法学研究；张然滔（1995—），男，四川眉山人，硕士研究生，主要从事宪法学、行政法学研究。

信息的个体属性，理应对个人信息进行保护，限制其流通和利用；然而，基于个人信息的公共属性，则应当鼓励个人信息的利用和流通。因此，如何平衡个人信息的双重属性，兼顾个人信息的利用与保护，成为探索大数据时代个人信息保护的重要课题之一。

《中华人民共和国民法典》（以下简称《民法典》）在人格权编中对个人信息的定义、处理原则、信息主体享有的权利等制定了基本性规则，奠定了个人信息的民法保护基础。但是，其对个人信息的保护是基于“主体自决”的，以“可识别性”为标准将所有个人信息都纳入保护的范围，并通过信息主体“知情—同意”的路径来保护公民的个人信息。此外，我国《个人信息保护法》已出台，这部针对个人信息保护的专项立法也规定了“同意原则”。中国是世界上唯一一个在立法上推进同意原则普遍化国家。[2]有学者认为，个人信息自决权理应受到个人信息价值的社会性限制，普遍同意的规则阻碍了个人信息价值的实现。[3]目前，我国法律对个人信息的保护以知情同意原则为基础，实行无差别的知情同意原则保护，实则是对个人信息中个体利益实行倾斜性保护，导致个人信息的双重属性之间的不平衡。因此，需要从个人信息的双重属性出发，运用场景理论，对现行的同意原则进行反思与重构。

二、个人信息的双重属性

（一）个人信息的个体属性

个人信息天然具有私权属性。个人与生俱来享有人格利益，与个人密切联系信息也承载着人格利益。[4]个人信息具备可识别性，往往对应特定的信息主体，公众可以通过个人信息来了解和评价所属的信息主体，使得个人信息与特定主体的人身产生了密切联系。《民法典》在人格权编中对个人信息做出规定是将个人信息纳入人格权范畴的重要体现。同时，《民法典》还明确规定了处理个人信息应当获得信息主体的同意，所以个人信息作为私益还表现为信息主体可以自主决定、处分其个人信息。此外，《民法典》还赋予了信息主体删除权、更正权等一系列信息权利，使得个人对自身信息掌握更多的控制权。另一方面，大数据时代互联网企业依赖用户信息进行精准推送，保证用户粘度，在这一过程中个人信息的人格利益被商业化，具有独立的经济价值，个人信息上也逐渐承载着财产利益。

（二）个人信息的公共属性

除了个体属性外，个人信息也逐渐成为大数据时代重要的社会资源，具有独特的公共价值。政府治理方式的创新、大数据和人工智能产业的发展依赖于个人信息的集合效应和规模化效应[5]个人信息作为社会交往中交流和表达的重要工具，从诞生之初就带有公共属性。此外，个人信息具有流动性和共享性，个人信息在传播过程中在人与人之间不断被共享，且这种传播过程是很难被控制的，体现了其公共属性。随着大数据技术的发展，个人信息被广泛利用于企业创新和政府治理创新，部分产业越来越依赖个人信息运行和技术创新。例如，“滴滴出行”软件只有靠获取用户的地理位置信息才能运营。政府通过掌握公民的个人信息做出正确的决策，提高行政效率，稳定社会公共秩序。

（三）个人信息双重属性的内在要求

个人信息兼具个体利益和公共利益，二者是辩证统一的关系。一方面，个人信息的双重属性之间存在冲突，个人信息的个体利益属性要求侧重于保护信息主体的利益，限制个人信息的流通和利用，而个人信息的公共利益属性则鼓励个人信息的积极利用。另一方面，个人信息的双重属性之间相互依存、不可分割，维护信息主体的人格尊严是实现个人信息公共利益的前提，而个人信息公共利益的实现也是信息主体个体利益实现的有力保证。因此，法律不能割裂个人信息的个体属性和公共属性来进行单边保护。个人信息的双重属性要求在个人信息的保护与利用之间找到平衡点，即在保护个人信息的基础上合理利用个人信息来实现社会公共利益。

三、无差别同意：个人信息保护与利用之不平衡

“知情同意原则”最早出现于医患关系中，医

生在做出诊疗前应当将风险充分告知患者或其家属，并征得患者或其家属对相关诊疗行为的同意。后来，个人信息保护领域也采用了此项原则。个人信息保护中“知情同意原则”是指信息处理者在处理个人信息之前都应当向信息主体告知法律规定的内容并征得其同意。[6] 目前，我国法律对个人信息的保护以知情同意规则为基础，实行无差别的知情同意规则保护，即除法律规定的特别情形外，对所有类别的个人信息在各个处理环节一律适用“知情－同意”原则。

（一）无差别同意的法律规定

个人信息的知情同意原则在学界虽然一直存在争议，但是在我国的法律上早已予以确认，其最早出现于 2012 年发布的《关于加强网络信息保护的决定》第 2 条。之后，在许多涉及个人信息的规范性法律文件中都对知情同意原则做出了规定。为进一步考察知情同意原则在法律规定上的具体情况，按照时间的先后顺序，对相关法律条文进行整理，具体规范见表 1。

表 1　知情同意原则的法律规定

颁布年份	法律条文	处理原则	告知范围	分类	例外情形
2012	《关于加强网络信息保护的决定》第 2 条	无规定	收集、使用信息的目的、方式和范围	无规定	无规定
2013	《消费者权益保护法》第 29 条	合法、正当、必要	收集、使用信息的目的、方式和范围	无规定	无规定
2016	《网络安全法》第 41 条	合法、正当、必要	收集、使用规则、目的、方式和范围	无规定	无规定
2020	《民法典》第 1034 条、第 1035 条、第 1036 条	合法、正当、必要；不得过度处理	处理信息的规则；处理目的、方式和范围	一般信息：个人信息保护规定；私密信息：隐私权规定	已经公开的信息；为维护公共利益或者该自然人合法权益
2021	《个人信息保护法》第 5 条、第 6 条、第 7 条、第 8 条、第 9 条、第 13 条、14 条、第 17 条、第 29 条、第 30 条	合法、正当、必要；诚信原则；明确、合理的目的；最小程度原则；公开、透明原则；安全保障原则	处理者的身份和联系方式；处理的个人信息种类、保存期限；个人行使权利的方式和程序；敏感信息还需告知处理的必要性和对个人的影响	一般信息：法律、行政法规规定单独或书面同意的从其规定；敏感信息：必须单独同意；法律、行政法规规定书面同意的从其规定	为订立、履行合同所必需；为履行法定职责所必需；为应对突发公共卫生事件、紧急情况下为保护自然人所必需；已公开的个人信息；为公共利益在合理的范围内处理个人信息

从表 1 可知，近些年最新的法律规范对“知情－同意”原则做出了细微调整，在处理原则、告知范围分类保护以及例外情形方面都予以补充和细化。在处理原则上，《个人信息保护法》在合法、正当、必要原则的基础上增加了 5 个新的原则；在告知范围方面，从《关于加强网络信息保护的决定》到《个人信息保护法》，将个人信息处理者需要告知的范围逐渐扩展，从收集、使用信息的目的、范围和方式到处理信息的规则，再扩展到处理者的身份、个人信息的保存期限甚至包括对个人的影响。此外，《民法典》和《个人信息保护法》在以往的法律规范基础上对个人信息的分类和例外情形做出了创新规定，《民法典》将个人信息分为一般信息和私密信息，指出私密信息适用隐私权的规定，《个人信息保护法》区分了一般个人信息和敏感个人信息，对信息主体同意的表达形式做出不同的规定，同时，两部法律均对不适用“知情－同意”规则的例外情形均做出了详细列举。

从《关于加强网络信息保护的决定》到《个人信息保护法》对“知情－同意”规则进行细化调整的趋势间接证明无差别同意规则在实践中仍面临问题，法律规定上的调整表明现行法律正尝试解决这些困难。但现行法律对同意规则的补充和细化均未触及关键点，即我国法律对于“知情－同意”的规定仍停留在概括的原则性规定上，实行所有个人信息无差别的同意规则保护，未予以细化。因此，从实质上来说，目前的“知情－同意”规则

仍然是无差别的同意，这也造成了同意原则在实践中长期遭遇的困境无法纾解。

（二）无差别同意的实践困境

1．同意机制流于形式。“知情—同意”机制虽然具有私法自治的精神，但这种同意机制在实践中往往流于形式。[7] 各类 APP 为执行“知情－同意”机制均会制定隐私声明，为了规避风险信息处理者将所有信息事无巨细地列入相关用户协议和隐私政策，造成信息主体的阅读困难，实际操作中用户一般没有耐心认真读完长篇的隐私声明。根据中国消费者协会 2018 年发布的《APP 个人信息泄露情况调查报告》显示，31.2% 的用户在使用手机 APP 时偶尔阅读用户协议或者隐私政策，26.2% 的用户从不阅读，在从不阅读的用户中，61.2% 的用户是因为不授权使用就无法使用 APP。[8] 通过以上数据可知，在实践中，用户往往没有拒绝的权利，隐私政策沦为数据企业处理信息正当化的“工具”。这点在司法实践中也得以体现，例如：抖音、微信读书等 APP 在并未授权的情况下便获取相关微信好友的信息并向用户推荐，这种行为明显侵犯了用户的个人信息和隐私权，而当被诉至法院时，相关隐私政策和用户协议就成了这些 APP 最好的开脱“工具”，他们往往会主张在隐私政策或用户协议中已告知用户会使用微信好友关系并获得了用户同意①。然而，事实上在用户登录过程中，如果不勾选“同意”或授权，则无法使用相关 APP 服务。

2．无差别同意的成本较高。无差别同意即除法律规定的特别情形外，对所有类别的个人信息在各个处理环节一律适用“知情－同意”原则。这意味着大量的个人信息的处理行为做出前都需要先由信息处理者向信息主体做出明确通知和说明，然后征得信息主体的同意，最终再反馈给信息处理者，这一过程将会耗费大量的金钱与时间成本。首先，对于信息主体来说，需要阅读大量冗长的隐私声明，并进行每一信息的授权，根据国外有关研究结果，信息主体每年需平均付出 244 hrs 来认真阅读所有可能遇到的隐私政策；如果只是粗略阅读，那么每年需平均付出 154 hrs。[9] 其次，对于信息处理者来说，需要投入资金进行隐私政策和告知界面程序的设计。信息收集者的成本与“知情－同意”原则的适用范围密切相关，正是因为现行的知情同意原则为无差别的同意，适用范围过大，因此导致其在适用过程中成本过高。

（三）个人信息的保护与利用之间的不平衡

我国的个人信息保护是建立在“主体自决”基础上的，以“可识别性”为标准将所有个人信息都纳入了保护的范围，并通过“知情－同意”的路径实现信息主体对个人信息的控制。一方面，大数据算法的兴起让许多本不具备“识别性”的信息也能够间接识别到特定自然人，如果仍然不区分类别地对所有个人信息都给予控制性保护，就会导致法律对个人信息的过度保护。另一方面，这种通过立法赋予信息主体对其个人信息无差别的控制权之方式，过度侧重于对个人信息的保护，导致信息处理者的收集和处理行为受到过多的限制，造成个人信息的保护与利用之间的失衡，最终不利于数字经济的发展和社会治理服务的提高。

综上所述，现行法律中利用知情同意原则对所有个人信息进行无差别的保护，不仅在实践中流于形式，且在操作层面的成本也过高，并且会造成对个人信息的过度保护，削弱个人信息的流通性，使得个人信息的保护与利用之间严重失衡，违背个人信息双重属性的利益平衡要求。

四、场景理论的创新应用

传统的知情同意机制已经无法满足个人信息双重属性平衡的保护需求，笔者认为，应当从平衡个人信息的双重属性入手，引入场景理论，结合个人信息的类别以及信息的生命周期，对现行的无差别同意原则进行重构。

（一）场景理论的引入

“场景理论”最早由尼森鲍姆教授提出，其是指个人信息的后续传播利用应受原初信息收集时的场景

①例如：（2019）京 0491 民初 16142 号、（2019）京 0491 民初 6694 号。

所限制。[10]之后，场景理论逐渐取得了各国学者们的共识，尤其是在欧美国家个人信息保护的相关法律中，场景理论得到了广泛的应用①，而在我国的个人信息保护制度中则缺乏场景理论运用，因此导致知情同意原则在实践中僵化，无法发挥其有效作用。

各国对于场景理论在个人信息保护领域的具体应用有所不同。欧盟的场景理论运用的目的是风险评估，即评估不同场景中个人信息处理的行为可能导致的风险，并对风险等级进行划分，以此来确定信息处理者的义务②。美国的场景理论运用的目的是对个人信息的合理利用进行界定，依据个人信息收集时的场景来对“合理性”进行判断，要求个人信息的使用，不论是商业目的，还是研究目的，均要与收集个人信息的场景相兼容③。通过对比可以看出，欧盟是以风险为导向确定对个人信息的保护，美国是以合理使用为导向。笔者认为，如果将这种场景理论应用于知情同意原则，完善我国现行的无差别同意的保护机制，可以考虑借鉴欧盟的风险导向的模式。通过构建具体的场景，并对在不同场景中个人信息处理行为带来的风险进行评估，根据风险程度适用差异化的同意原则，以此来平衡无差别同意原则带来的个体属性和公共属性的失衡。

（二）场景的设置

通过场景理论构建差异化同意原则的前提是对具体的场景进行预设。影响个人信息的保护程度与利用价值的主要因素是个人信息的类别和信息的生命周期。因此，本文在设置类型化的场景主要包括两个要素：一是个人信息的类别；二是信息的生命周期。

1．个人信息的类别。目前《个人信息保护法》对个人信息的分类采用“二分法”，将其分为敏感个人信息和一般个人信息两类。《刑事司法解释》的信息分类采用三分法：敏感信息、重要信息、一般信息，[11]并对敏感信息和重要信息进行了列举，还规定除此之外的其他信息均属于一般信息。《个人信息保护法》虽然对个人信息进行了分类保护，但是仍然实施的是无差别同意规则，并未体现差异化同意规则保护。所以可以考虑借鉴刑法上的“三分法”，对个人信息进一步细分。但是，由于不同部门法的规范目的不同，分类标准相较于刑法应当有所区别，构建差异化的同意原则是为了平衡个人信息的保护与利用之间的关系，而决定个人信息的保护和利用的关键性因素是个人信息的敏感度和流通价值。因此，在此种语境下的个人信息可以根据个人信息的敏感度和流通价值进行分类。

具体而言，根据个人信息的敏感度和流通价值的大小，可以将个人信息分为一般信息、重要信息以及敏感信息。一般信息是指与特定主体联系较弱，不具有直接识别性的个人信息，例如：网络交易记录、浏览记录等；重要信息是指能够识别到特定主体，具有一定隐秘性，但是该类具有较大的流通价值；敏感信息是指直接表现特定主体身份特质的信息，隐私性较强，与信息主体的人身或者财产具有紧密联系，例如：指纹、面部识别信息、银行账户等信息。

2．信息的生命周期。数据生命周期模型指从数据产生，到数据加工和发布，最终实现数据再利用的一个循环过程。[12]《民法典》第 1035 条第 2 款规定：“个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开等。”《个人信息保护法》对于个人信息的处理的定义基本沿用了该条规定，只是在此基础上增加了“删除”这一环节。由此可见，法律将个人信息的生命周期大致分为 6 个阶段：信息收集、信息存储、信息使用、信息加工、信息传输与提供④、信息公开。根

①例如：欧盟的《一般数据条例》、美国的《消费者隐私权利法案》等。

②欧盟 2018 年《一般数据保护条例》第 24 条规定：“在考虑了处理的性质、范围、语境与目的，以及考虑了处理对自然人权利与自由所带来的不同概率和程度的风险后，控制者应当采取恰当的技术与组织措施。”

③美国 2018 年《加州消费者隐私法案》第 1798．105 节中第（d）条项下第 9 款规定：“在内部以其他合法方式使用消费者的个人信息，该方式与消费者提供其信息的场景相匹配。”第 1798．140 节第（d）项规定：“‘商业目的’是指为商业或服务提供者的经营目的或其他通知目的使用个人信息，前提是个人信息的使用应是合理必要且成比例的，以实现个人信息被收集或处理，或用于与收集个人信息的情境得以兼容的另一个经营目的”，第（s）项下第 7 款规定：“仅用于与收集个人信息的场景相兼容的研究目的。”

④信息传输与信息提供都是将个人信息从一处送往特定另一处的行为，因此可以归于一个阶段。

据不同环节的保护程度和流通程度，可以将个人信息的生命周期从整体上分为 3 个部分，即收集阶段、使用阶段、传播阶段。

将个人信息的类别与信息的生命周期结合，可以构建出九大场景，分别是：一般信息的收集阶段、使用阶段、公开阶段，重要信息的收集阶段、使用阶段、公开阶段，敏感信息的收集阶段、使用阶段、公开阶段。设置完具体场景后，需要解决如何对这 9 个具体场景适用差异化同意原则的问题。

（三）无差别同意原则的重构

1. 制度设计。“个人信息处理是否必须经过权利主体明确同意，国际方面尚没有哪个国家制定非此即彼的规定，而是依据处理数据的类型、处理目的等区别对待。”[13] 根据个人信息处理的场景不同，可以将同意形态分为一般允许、相对同意与绝对同意。一般允许原则即无需信息主体的“知情 – 同意”即可允许其流通；相对同意原则是指信息主体未明确提出不反对即视为其同意；绝对同意原则是指在处理个人信息之前必须明确取得信息主体的知情同意。借鉴欧盟的风险导向模式，对于具体场景中的个人信息处理行为引发的风险进行评估，将风险分为“高、中、低”3 个等级，不同等级的风险适用不同形态的同意原则。低风险场景中适用一般允许原则，中风险的场景中适用相对同意原则，高风险的场景中适用绝对同意原则。

如表 2 所示，对于一般信息的收集和使用阶段，由于信息的识别性较弱且收集和使用阶段对个人信息泄露的危险性较小，属于低风险场景，因此应当倾向于保护信息的流通性，适用一般允许原则；对于一般信息传播阶段和重要信息的收集、使用阶段，由于传播阶段信息的泄露危险性较大和重要信息流通价值较大，属于中风险场景，因此适用相对同意原则；同理，对于重要信息的传播阶段，属于高风险场景，应当升格适用绝对同意原则。针对敏感信息，由于其较强的隐私性，必须予以严格保护，在每一阶段均应无差别的适用绝对同意原则。

表 2　不同信息在不同阶段同意原则的适用

信息类别	收集阶段	使用阶段	传播阶段
一般信息	一般允许原则	一般允许原则	相对同意原则
重要信息	相对同意原则	相对同意原则	绝对同意原则
敏感信息	绝对同意原则	绝对同意原则	绝对同意原则

2. 实践路径。差异化的同意规则将同意形态分为三种并在不同的场景中予以适用，其实质上促进了个人信息的流通和利用，以此来平衡无差别同意原则导致的个人信息过度保护。在实践中需要从约束个人信息处理者入手，推进信息主体的权利让渡和个人信息主体者的责任承担，实现个人信息双重属性的平衡。

“一般允许原则”与“相对同意原则”需要信息主体将其在个人信息上的部分权利让渡给信息处理者，这种权利让渡的正当性基础在于两个方面：一是部分权利的让渡并不会侵犯个人信息上所附有的个体利益；二是个人信息应用于政府公共服务和企业创新发展，能够为信息主体带来更好的服务。因此，实践中为保证差异化同意规则实施的正当性，在适用“一般允许原则”时，政府和企业应当证明其信息处理行为的必要性，并对相关个人信息进行妥善保管，在适用“相对同意原则”时，由于该原则的适用涉及一般信息的传播和重要信息的收集与利用，应当在“一般允许原则”的基础上，注重对个人信息进行匿名化处理，以避免被分析、追踪到具体的信息主体。除此之外，还要建立信息企业的负面清单制度，根据差异化同意规则适用的不同场景，判断企业的信息处理行为是否超出了必要范围，对于违法处理个人信息的行为，加大处罚力度。

五、结语

个人信息保护已经成为当下社会最关注的热点问题之一。平衡个人信息的保护与利用之间的关系是个人信息双重属性的内在要求。同意原则是我国个人信息保护制度的核心，传统的无差别同意原则已经无法满足个人信息双重属性平衡的需求。通过

场景理论的创新应用，以个人信息的类别和信息的生命周期为要素构建具体场景，对无差别同意原则进行重构，从而实现个人信息的个体利益与公共利益的平衡，满足公民对个人信息多层次保护的需要和大数据时代经济发展与政府治理创新的需要。

［参考文献］

［1］中华人民共和国公安部. 全国打击治理电信网络诈骗违法犯罪取得明显成效［EB/OL］.（2021 - 04 - 09）［2021 - 08 - 01］. https://www. mps. gov. cn/n2254314/n6409334/c7847027/content. html.

［2］高富平. 个人信息保护：从个人控制到社会控制［J］. 法学研究，2018（3）：84 - 101.

［3］任龙龙. 论同意不是个人信息处理的正当性基础［J］. 政治与法律，2016（1）：129 - 134.

［4］李晓辉. 信息权利研究［M］. 北京：知识产权出版社，2006：117.

［5］丁晓东. 个人信息的双重属性与行为主义规制［J］. 法学家，2020（1）：64 - 76.

［6］王利明，程啸，朱虎. 中华人民共和国民法典人格权编释义［M］. 北京：中国法制出版社，2020：419.

［7］姬蕾蕾. 个人信息保护立法路径比较研究［J］. 图书馆建设，2017（9）：19 - 25.

［8］中国消费者协会. APP 个人信息泄露情况调查报告［EB/OL］.（2018 - 08 - 29）［2021 - 07 - 20］. http://www. cca. org. cn/jmxf/detail/28180. html.

［9］ALEECIA M. MCDONALD，LORRIEFAITH C. The cost of reading privacy［J］. Journal of Law and Policy for the Information Society，2008（3）：543 - 568.

［10］范为. 大数据时代个人信息保护的路径重构［J］. 环球法律评论，2016（5）：92 - 115.

［11］周光权. 侵犯公民个人信息罪的行为对象［J］. 清华法学，2021（3）：25 - 40.

［12］武彤. 基于数据生命周期的美国研究图书馆科学数据开放共享服务研究［J］. 图书与情报，2019（1）：135 - 144.

［13］赵龙. 个人信息权法益确证及其场景化实践规则［J］. 北京理工大学学报，2021（1）：1 - 14.

（上接第 80 页）

但在对个人信息保护不断完善的背景下，个人信息的属性却是刑法学中争执不休的话题，个人法益与超个人法益之争互不相让。而对法益属性的不同理解，在某种程度上对入罪起到决定性的作用，同一可能触犯《刑法》的行为，在这两种观点下也可能会得出完全不同的结论。因此，法益属性的确定是本罪中亟待确定的难题。而我们认为，尽管大数据时代使得个人信息呈现出一定社会化的表象，但其实质仍然是以个人属性为支撑。虽然在某些犯罪中，我们承认超个人法益的存在，但在现代社会，对超个人法益的认定仍应当加以严格限制，以防止犯罪的无限扩张。

［参考文献］

［1］冀洋. 法益自决权与侵犯公民个人信息罪的司法边界［J］. 中国法学，2019（4）：66 - 83.

［2］曲新久. 论侵犯公民个人信息犯罪的超个人法益属性［J］. 人民检察，2015（11）：5 - 9.

［3］江海洋. 侵犯公民个人信息罪超个人法益之提倡［J］. 交大法学，2018（3）：139 - 155.

［4］于冲. 侵犯公民个人信息罪中“公民个人信息”的法益属性与入罪边界［J］. 政治与法律，2018（4）：15 - 25.

［5］张明楷. 刑法分则的解释原理［M］. 北京：中国人民大学出版社，2019：363 - 365.

［6］张明楷. 刑法格言的展开［M］. 北京：北京大学出版社，2019：3.

［7］凌萍萍，焦冶. 侵犯公民个人信息罪的刑法法益重析［J］. 苏州大学学报（哲学社会科学版），2017，38（6）：66 - 71.

［8］敬力嘉. 大数据环境下侵犯公民个人信息罪法益的应然转向［J］. 法学评论，2018，36（2）：119 - 120.

［9］王利明. 论个人信息权在人格权法中的地位［J］. 苏州大学学报（哲学社会科学版），2012，33（6）：68 - 75.

［10］高富平，王文祥. 出售或提供公民个人信息入罪的边界：以侵犯公民个人信息罪所保护的法益为视角［J］. 政治与法律，2017（2）：46 - 55.