第 3 章　有限实名网络环境中个人信息的内涵与监管面临的问题

有限实名网络区别匿名网络和实名网络，既兼具匿名网络、实名网络的特征，又有其自身的特点，是兼顾网络言论自由和互联网监管的中间方案。现阶段，对于互联网治理已经形成了普遍的共识，但就如何更好地实现互联网治理，不同利益相关方有着不同的利益诉求。因此，网络实名制的推进不可避免地进入了有限实名网络的发展阶段。有限实名网络在匿名性、实名性等方面有其自身的特征，其安全需求、实施难度与实名网络存在显著差异，因此需要更具针对性的互联网治理方案。

无论是网络实名制还是有限实名制，随着互联网应用的不断发展，尤其是电子商务、社交网络的不断发展，个人信息在网络环境的各个平台、应用程序中沉淀、累积，同样面临较高的安全风险。与此同时，大数据环境下，数据采集、分析技术不断发展，个人信息的经济价值、安全价值不断凸显，个人信息安全面临更为复杂的技术环境和政策环境。如何兼顾互联网发展、互联网治理以及个人信息安全保护，成为一个极为现实和迫切的需要。

围绕有限实名网络环境中个人信息的内涵与监管面临的问题，本章主要阐述了有限实名网络的基本特征以及有限实名网络中个人信息的内涵，并在此基础上，着重探讨、分析有限实名网络中监管面临的个人信息安全风险严重，个人信息侵犯隐蔽、监管权利边界不清晰、立法保护缺乏可操作性等主要问题。

3.1　有限实名网络的特征

按网络实名程度可以将网络环境划分为匿名网络、有限实名网络和实名网络三种。从用户实名程度这一角度看，有限实名是介于匿名与实名的一个中间状态。2012 年，全国人大常委会通过的《关于加强网络信息保护的决定》中不仅包括接入实名，也包括信息发布实名，但在实现方式上《关于加强网络信息保护的决定》并不排斥“前台匿名、后台实名”的“有限实名制”方式。因此，有限实名网络在当前和未来都是一种重要的网络形态。

电子工业出版社版权所有
盗版必究

一是面向网络社会的匿名性特征。

1993 年 7 月 5 日，彼得·施泰纳（Peter Steiner）创作的一幅关于互联网匿名性的漫画刊登在《纽约客》上，其标题为“在互联网上，没人知道你是一只狗”，广为流传、众所周知。这极为形象地描述了互联网最为显著的特征，即匿名性。自互联网诞生之日起，匿名性一直是互联网的一个重要特征，并在一定程度程度上促进了互联网虚拟社区的繁荣。网络较其他媒体介质具有不可比拟的虚拟性、开放性、互动性和隐匿性的特征。

互联网的匿名性，实际上是互联网行为主体身份的不可识别性。美国学者 Hayne 和 Rice 认为，互联网匿名性可分为两大类，一类是技术匿名性，另一类是社会匿名性。其中，技术匿名性主要是指在交流过程中移除所有和身份有关的信息。社会匿名性则指由于缺乏相关线索，而无法将一个身份与某个特定的个体相对应。从这一角度看，有限实名网络具有技术匿名性的特征，即面向网络社会的匿名性特征，这有利于减少对网络言论自由产生的冲击，保留网络本身的匿名性、虚拟性的特征。

二是面向监管者的实名性特征。

互联网可以应用于监管，同时也需要被合理有效地进行监管。互联网的匿名性使得互联网充斥着虚假信息、网络谣言、网络暴力等各类有害信息和行为。但是，互联网是社会生活的延伸，并不是法外之地，如何更好地对互联网进行监管，规范网络行为，营造风清气正的网络环境，成为当前互联网治理的重要内容。在此背景下，网络实名制应运而生。在有限实名网络环境中，用户的身份信息在互联网平台存储，以利于监管，是有限实名网络的基本特征。

国家互联网信息办公室于 2015 年 1 月 13 日宣布以“后台实名、前台自愿”为原则的网络实名制方案，该方案可以提升对互联网进行监督管理的能力。其中“后台实名”的核心意涵，在于互联网接入服务以及应用程序提供者应对注册用户进行基于移动电话号码等真实身份信息认证。因此，根据 Hayne 和 Rice 对网络匿名性的描述，有限实名网络并不具备社会匿名性的特征，网络行为主体的身份并不是不可识别的，有限实名网络具有面向监管者的实名特征。

三是实现形式的间接性特征。

从信息安全的角度看，有限实名网络中各互联网企业的信息安全能力参差不齐，完全的网络实名制无疑会带来很高的信息安全风险，也不利于互联网的繁荣发展。因此，采用间接的实名认证方式是一个广泛采用的替代方案。

“后台实名”有限实名网络分为两种情形，一种是后台注册是使用了真实的个人信息，可以直接实现网络虚拟角色与现实社会特定个体的对应，另一种是后台注册信息是可以间接实现与现实社会特定个体对应的个人相关信息，例如基于实名制的手机号。由此可见，有限实名网络区别于匿名网络和实名网络之处，还在于面向互联网应用程序提供者的实名形式可以是间接的，即可以通过实名的手机号、邮箱等间接信息来实现实名要求。这样在

电子工业出版社版权所有
盗版必究

一定程度上可以规避、减少应用程序提供者存储、使用、保护个人实名信息的压力，减少个人信息泄露的风险。

四是个人信息安全高风险性特征。

有限实名网络中的“后台实名”，使得后台使用了用户的直接或间接的实名信息，同样面临着信息泄露、信息滥用等风险。有限实名网络中个人信息安全风险客观存在于个人信息生命周期的各个阶段，并随着各种不确定因素的不断变化而呈现不确定性。随着大数据、云计算、数据挖掘[①]等信息技术的快速发展，个人信息的价值不断凸显，个人信息安全风险不断增加。这种风险主要表现为两个方面，一方面是因技术原因导致的信息泄露，例如安全漏洞、黑客窃取等，另一方面是应用程序提供者的管理漏洞导致的信息泄露，或应用程序提供者自身的滥用。因此，与匿名网络相比较而言，有限实名网络的个人信息面临较高的安全风险。

3.2 有限实名网络中个人信息的内涵

3.2.1 个人信息的界定

个人信息具有可识别性，通过个人信息能够把当事人直接或间接地从人群中辨认出来；个人信息具有时效性，大部分个人信息从产生之日起就处于不断变化和更新之中。个人信息如文化程度、工作履历、健康状况、财务状况、婚姻状况等都在变化中，过时的个人信息不能反映信息主体现时的真实情况；个人信息具有可共享性，同一内容的个人信息可以在同一时间被多个的信息用户获取和使用，而信息提供者不会因信息传递给他人而失去信息，依然拥有信息，这一特征大大增加了个人信息的保护成本与难度。

每个人的个人信息中都含有大量的属于个人隐私的个人资料，以此为标准，可以将个人信息分为敏感个人信息和一般个人信息。敏感信息能更强烈地体现信息主体的人格尊严，信息主体对其保护的心理因素会更迫切，如个人健康状况的记录（包括生理状况的记录）、个人婚姻状况的记录（包括个人婚姻变动状况的记录）、个人财产状况的记录（包括个人财产的数量、文件密码、资金账号等）。这些个人信息一旦违背信息主体个人意愿被泄露、被利用，对信息主体造成的精神损害、财产损失是巨大的。所以信息主体是绝对不愿意此类个人信息被收集、被利用的，如确实因特殊的需要对此类个人信息进行收集和利用，必须

① 数据挖掘是从大量的数据中通过算法搜索，发现隐藏于其中的信息和规律的过程。新技术的应用也给个人信息带来更大的安全风险。

电子工业出版社版权所有 盗版必究

经过法定的程序，并做好保密工作。除此以外的个人信息属于一般个人信息。

个人信息是可以直接或间接识别信息主体的信息，“识别性”是个人信息的重要特征。所谓“识别性”是指个人信息与信息主体之间一定存在着客观的、一一对应的关系，个人信息可以将信息主体从茫茫人海中直接或间接地指认出来。直接识别就是直接通过本人身份的个人信息来识别，如公民的身份证信息、人体自身的基因信息等；间接识别是指借助其他信息或者对信息进行综合分析，可以确定当事人的身份。在信息社会，个人信息几乎可以包含信息主体的所有自然属性和社会属性。个人信息可以准确地指向具体个人的特征，使其人格权的属性已为法学界逐步肯定。

个人信息已成为社会重要的基础资源。政府机构为履行行政职责可以收集公民个人信息，商业机构为经营和服务也可以收集公民个人信息。在国家行政管理机关的网站里，在银行、保险、电信、交通、医疗、电子商务等网站里，收集存储了大量的公民个人信息。

信息化推动了电子政务、电子商务的产生与发展。大数据时代，信息社会中个人信息是行政机关行使国家行政管理职能的重要资源，是商业机构决定经营计划的可靠保证。

在欧盟，《欧盟指令》将个人信息界定为：有关自然人的能被识别和可以识别的所有信息。由此将个人信息划分为可以直接识别和可以间接识别两大类，但究其核心主要是强调了个人信息的可识别属性。在美国，个人信息是指用来标识个人基本情况的资料。日本使用了“生活日志”的概念，将个人信息从静态的属性信息延伸到个人生活记录，例如网站浏览记录、电商网站的购买和支付记录、收集 GPS 位置信息等。

2013 年 2 月 1 日，我国首个个人信息保护国家标准《信息安全技术公共及商用服务信息系统个人信息保护指南》（以下简称《指南》）正式实施，《指南》中将个人信息界定为：可为信息系统所处理、与特定自然人相关、能够单独或通过与其他信息结合识别该特定自然人的计算机数据。同时，《指南》还将个人信息划分为个人敏感信息和个人一般信息两大类。其中个人敏感信息是指“一旦遭到泄露或修改，会对标识的个人信息主体造成不良影响的个人信息”，例如身份证号码、手机号码、种族、政治观点、宗教信仰、基因、指纹等。

综上所述，个人信息有狭义和广义之分，狭义的个人信息更多强调的是与特定自然人相关的属性信息，广义的个人信息则是与自然人相关并能够被识别的所有信息，即不仅包含相关自然人的属性信息，还包括其行为信息以及社会关系信息等。从这一角度看，厘清个人信息的范围和边界，是个人信息的保护以及实现有效监管的前提和基础。

3.2.2　有限实名网络中的个人信息

在网络环境中，个人信息存在的形式以“个人数据”为主。网络个人信息可以被界定为：在网络世界里具有识别个人特征的，而又可以通过互联网带来在现实世界中商业利益的个人信息。网络个人信息具有一定的财产性权利的特征，可以随着技术的进步不断衍生

电子工业出版社版权所有 盗版必究

新类型的数据。此外，根据前文阐述的有限实名网络的基本特征，存在于有限实名网络中的个人信息本质上是个人信息的子范畴，具有个人信息的共性特征；同时，源于有限实名网络自身的特征，相关的个人信息具有显著的模糊性等方面的特征。

1．有限实名网络中个人信息的财产权利特征

在个人信息权方面，以往相关研究及政策、法律更多地关注、保护的是涉及公民隐私权的个人信息。对于个人信息权的法律属性一直存在不同的理解和争议，主要表现在个人信息权的人格权、财产权属性及其关系。在互联网环境下，公民信息权的法律属性更为复杂且具有自身特殊之处，单纯的从人格权、财产权角度很难准确地体现互联网时代公民信息权的法律属性①。随着信息技术和互联网应用的不断发展，海量的个人信息存在于电子商务、电子政务、社交网络等网络平台，特别是一些大型的互联网企业或网络运营商。与此同时，网民自身作为其个人信息的权利主体，却无法有效控制存储在网络平台的个人信息。对此，《中华人民共和国民法典》就公民个人信息的收集、使用、加工、传输等行为进行了限定。这在一定程度上体现出，公民对个人信息权利的保护，可以转换为从立法角度对采集、加工、使用个人信息等行为进行约束②。

对于个人信息的财产权利特征，主要存在两种不同的观点。一是认为网络个人信息是当事人不愿他人知道或他人不便知道的个人信息，属于个人无形隐私，法律在进行保护时，应当将其作为一种隐私权看待，不能用金钱去衡量，只能用一定的观念对其作出评价，故不得转让、赠与、买卖。二是认为网络个人信息能为权利人带来财产利益，且客观上存在非法利用他人的网络信息谋取不法利益的大量犯罪违法行为，因而将其列入财产权的范畴。

随着网络实名制的推进，作为互联网的一个典型形态，有限实名网络环境加速了个人信息在网络平台的累积，同样具有相应的个人信息财产权利特征。对于个人信息的保护，其核心在于保护具有使用价值的个人信息或是个人隐私信息，并不是保护所有的个人数据。因此，进一步明确、强化有限实名网络中个人信息的财产权，是保护个人信息的前提和基础，对于保护公民的人格尊严，维护社会秩序具有显著的现实意义。

2．有限实名网络中个人信息的模糊性特征

有限实名网络中“后台实名”的个人信息，并非静态地存在于信息系统或应用程序中，也不是仅仅局限于相关自然人的属性信息。因此，有限实名网络中的个人信息具有显著的模糊性特征。

首先是有限实名网络个人信息内容的模糊性，既有姓名、电话、身份证、地址等明确

① 检察日报：个人信息权是公民的基本民事权利，2017-04-10。

② 《中华人民共和国民法典》第一百一十一条　自然人的个人信息受法律保护。任何组织或者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。

电子工业出版社版权所有 盗版必究

的信息，也有网络活动轨迹等模糊的信息，其内容边界很难完整、准确地给予界定。其次是有限实名网络中个人信息存在形式的模糊性。有限实名网络中个人信息的存在形式既有文本、图片、音视频，也包括数据库中的一些结构化的相关关系。这些信息散落在有限实名网络的各个应用程序中，但通过数据挖掘等信息技术又能够形成一些有价值的知识，并对个人的网络生活和社会生活产生影响。最后是个人信息权利的模糊性，个人信息具有财产权利的基本特征。然而，个人信息财产权利的归属是模糊的。例如，通过数据挖掘技术获得的个人相关信息或统计类信息，其权利属于相关自然人还是相关的互联网企业，仍然存在较大的不确定性。同时，从另一个角度看，个人信息在内容、形式及权利方面的模糊性也导致了关于个人信息保护在立法方面的模糊性。

3.3　有限实名网络中个人信息保护监管面临的主要困难

3.3.1　个人信息安全风险严重

1．个人信息的过度采集

以全国消协组织受理的消费者投诉数据统计为例，2018 年 1 月到 6 月，电子商务及网络社交等领域的网站、信息化系统、平台软件非法采集消费者个人信息现象成为消费投诉新热点，位居十大投诉榜榜首[①]。2018 年 7 月至 8 月，中国消费者协会专门开展了“App 个人信息泄露情况”的问卷调查，并发布了《App 个人信息泄露情况调查报告》。该报告中的相关调查数据显示，遇到过个人信息泄露情况的人数占比为 85.2%。而泄露的主要途径是，未经本人同意的个人信息收集和个人信息持有者的故意泄露、出售等。

基于个人信息潜在或直接的商业价值，个人信息的过度采集已经成为网络环境中一个较为普遍的现象。网络环境中的个人信息过度采集主要是指网络服务提供商超出所提供服务的业务需要，采集非必要或完全无关的个人信息的行为。例如，一些移动网络服务提供商借助 GPS 定位技术广泛采集用户的实时位置信息；一些电子商务企业或平台存储大量用户的银行账户信息；一些基于手机通信录的即时通信软件通过“云”端采集用户的通信录信息。此外，在大数据时代，数据挖掘技术为个人信息的获取、分析、处理带来极大的便利，同时也使得个人信息在获取、存储、转移等各个环节都呈现新的特点。而这些被过度采集的个人信息，在一定程度上增加了个人信息泄露的风险以及个人信息泄露后产生危害的程度。

① 人民日报：手机 App 过度采集，个人信息要多加几道保护锁，2018-10-10。

电子工业出版社版权所有 盗版必究

2．个人信息的滥用

个人信息滥用是个人信息安全中普遍存在的现象，这些滥用主要表现在从事违法犯罪或网络舆情的操控等活动。比如，2016 年“徐玉玉案”、精准的有害信息推送以及常见的垃圾短信、骚扰电话等[①]。以求职网站为例，求职者在网站注册的需要填写大量的个人信息，其中涉及较为具体的个人简历，在网站中可以较为方便的查看其年龄、头像、学历和毕业学校等个人信息，而通过使用爬虫软件等技术手段，有的机构和个人开始不断采集求职者注册的信息，并进行出售，从而为个人信息安全带来很大的隐患[②]。

目前，大数据及数据挖掘等相关信息技术，使得个人信息直接或潜在的商业价值不断凸显，这进一步刺激着互联网企业，甚至硬件设备商、应用程序开发商等都对用户个人信息进行过度的收集和滥用。有限实名网络中个人信息滥用主要表现为违规披露和违规共享两种情形，违规披露是网络服务提供商未获法律授权、未得到用户许可或者超出必要限度披露他人的个人信息；违规共享是网络服务提供商在未经法律授权或者用户许可的情况下，将所掌握的个人信息提供给其他机构。

3．个人信息的泄露

Risk Based Security（RBS）发布的《2018 年数据泄露快报》（*Data Breach QuickView Report*）中显示，2018 年，在公开披露的超过 6500 起数据泄露事件中，有大约 2/3 来自商业部门。同时，政府部门、医疗部门以及教育部门分别占比 13.9%、13.4%和 6.5%。2018 年 3 月，Facebook 5000 万用户信息泄露。同年 8 月，华住集团 1.3 亿个人信息数据被兜售。11 月，万豪集团客户预订数据库信息泄露[③]。

随着网络应用的不断延伸，以及信息技术不断发展，个人信息泄露不断规模化，产生的危害也日益严重。大数据应用的深入，在给社会生活带来极大便利的同时，也进一步为个人信息泄露推波助澜。中国互联网协会发布的《中国网民权益保护调查报告 2016》[④]显示，84%网民曾经遭受过因个人信息泄露带来的不良影响，个人信息泄露普遍性可见一斑。

从个人信息泄露的途径看，网络环境下，个人信息泄露的原因主要有技术原因和非技术原因（人为因素）两种。一是技术原因，主要表现为计算机病毒（手机病毒）通过传播在电子设备中获取个人信息，黑客利用系统漏洞等侵入计算机系统获取个人信息。二是人为因素，主要表现为互联网企业或企业内部人员有意或无意的泄露，既有商业因素驱动下的买卖，也有管理漏洞导致的泄露。

---

① 防止个人信息被滥用是关键，法制日报，2018-08-20。

② 58 同城被曝简历数据泄露：700 元可采集全国简历信息，21 世纪经济报道，2017-03-24。

③ 万豪旗下喜达屋酒店数据库遭入侵 5 亿顾客信息或泄露，央广网，2018-12-01。

④ 《中国网民权益保护调查报告 2016》由中国互联网协会和 12321 网络不良与垃圾信息举报受理中心联合发布，此后暂未再公开发布相应的年度调查报告。

电子工业出版社版权所有 盗版必究

3.3.2　个人信息侵犯的隐蔽性

互联网是实施公民个人信息的交易和侵犯的主要渠道。无论是技术手段、侵犯主体还是交易行为，互联网个人信息侵犯都具有显著的隐蔽性特征，这给公民个人信息的保护带来了极大的困难。

1．技术手段的隐蔽性

个人信息侵犯行为往往是隐蔽的，首先表现在通过技术手段实现的个人信息获取、存储等行为往往不易被个人信息的主体所察觉。无论是 Facebook 5000 万用户信息泄露还是万豪集团客户预订数据库信息泄露事件，保管个人信息的企业均未能及时察觉用户信息的泄露，更多的是在事件发生后的漏洞修补。在事件披露之前，被泄露信息的用户更加无法感知个人信息所面临的巨大风险。

信息技术手段的不断进步，使得个人信息的获取、存储和转移更为便利，同时也更为隐蔽。从获取的角度看，在系统存在漏洞的情况下，通过技术手段窃取个人信息具有较高的隐蔽性，即使事后察觉，也很难弥补已经发生的信息泄露和产生的危害。此外，通过数据挖掘技术获取更广泛的个人行为信息或统计信息等，更加无法抵御。

2．交易行为的隐蔽性

互联网应用的兴起，促进了电子商务的蓬勃发展，个人信息也逐渐成为重要的商业资源。互联网上非法买卖个人身份证信息、银行卡信息的问题日益凸显，出现了专门贩卖个人信息、电商账号（网络店铺）的 QQ“卡商交流群”和交易网站[①]，贩卖个人身份信息的黑色利益链日渐形成。“叫卖者”在这条黑色产业链中居于上游，通过“卡商交流群”、论坛社区、网站等渠道进行个人信息贩卖，进而个人信息被用于售假、诈骗等违法犯罪活动。

与传统的交易行为不同，由于个人信息通常以电子数据的形式存在，通过网络渠道，这些电子数据的能够非常便利地实现转移。个人信息的转移、买卖通过社交平台、即时通信软件、电子商务平台等，整个交易的过程从沟通、供货、支付都可以实现虚拟化和网络化。这使得目前个人信息的交易行为既隐蔽又十分迅速。互联网应用以及信息技术的快速发展，也使得个人信息的地下交易产业链更加隐蔽、难以追踪[②]。互联网环境下，对于个人信息的交易行为、侵犯行为，无论是事前、事中的感知和发现，还是事后的查处和追责都具有很大难度，而事后惩处的不足，也使得立法追责无法产生足够的威慑力。

3．侵犯主体的隐蔽性

互联网环境下，侵犯公民个人信息的不法主体关系错综复杂。由于犯罪行为大多依托

① 检察日报：经同意买卖个人信息也属违法犯罪，2018-08-15。

② 中国青年政治学院互联网法治研究中心于 2016 年 11 月《中国个人信息安全和隐私保护报告》。

电子工业出版社版权所有 盗版必究

互联网、移动电子设备，通过即时通信工具、电子邮件等多种方式实施，追踪实施不法侵犯的主体以及相应的调查取证难度都很大[①]。由于互联网的虚拟性特征，在互联网中对个人信息实施侵犯的侵权主体通常很难被发现和追踪。实施侵权的主体还可以利用多重身份来增加被发现和追踪的难度。

由于技术手段的隐蔽性、交易行为的隐蔽性，直接导致侵犯主体的隐蔽性。随着技术门槛的不断降低，无论是黑客个人还是互联网企业都可以借助相应的信息技术手段获取个人信息。这使得在个人信息泄露发生时，追踪侵犯主体存在明显的困难，这在一定程度上进一步刺激的个人信息窃取行为的发生，并使得监管和追责面临很大的障碍。

3.3.3 个人信息保护监管的权利边界不清晰

1．行业监管权利边界不清晰

中国互联网协会成立于 2001 年 5 月 25 日，是由中国互联网行业及与互联网相关的企事业单位、社会组织自愿结成的全国性、行业性、非营利性社会组织。该组织在其工作任务中明确提出："制订并实施互联网行业规范和自律公约，协调会员之间的关系，促进会员之间的沟通与协作，充分发挥行业自律作用，维护国家信息安全，维护行业整体利益和用户利益，促进行业服务质量的提高。"

作为互联网企业的重要监管力量，在立法相对滞后的情况下，行业协会的监管显得尤为重要。例如，中国互联网协会就先后发布了《中国互联网网络版权自律公约》《反网络病毒自律公约》《互联网搜索引擎服务自律公约》等行业自律制度，在互联网监管中扮演重要角色。然而由于网络边界的模糊性、个人信息边界的模糊性，行业协会的监管缺乏应有着力点和有效的针对性。行业监管针对互联网企业在个人信息采集、存储、使用、保护等方面的行为缺乏有效的评估能力、预警能力和追责能力。

2．行政监管的权利边界不清晰

网络环境中，对个人信息采集、存储、使用、保护等方面离不开行政监管。目前针对个人信息保护的行政监管主要存在两方面的问题。第一，虽然国内目前已经制定了一些互联网方面个人信息保护的法律法规，但这些法律法规较为分散且未成体系，这客观上导致监管工作呈现多头管理、交叉管理或无人管理的尴尬局面。第二，限于行政资源，目前并没有足够的行政资源参与个人信息保护。同时，由于网络技术的日新月异，监管什么、怎么监管都还有诸多不确定性。

电子工业出版社版权所有 盗版必究

① 最高人民法院、最高人民检察院、公安部《关于依法惩处侵害公民个人信息犯罪活动的通知》，2013-04-23。

3.3.4　立法保护缺乏可操作性

信息技术的不断发展，新技术的应用，对个人信息保护方面的立法工作提出了更高的要求。2018 年 9 月 10 日，中国人大网公布了《十三届全国人大常委会立法规划》，有近 69 件法律草案列入第一类项目，即条件比较成熟、任期内拟提请审议。其中，最令人关注的是个人信息保护法，这意味着个人信息保护将迎来专门立法。

无论是过去或是当前，关于个人信息的立法保护主要存在立法分散、立法滞后和立法空白等问题。首先是立法分散，个人信息保护的相关法律法规分散在多个法律条文中，且多为原则性要求，缺乏可操作性。其次是立法滞后，信息技术的快速发展，凸显出立法的欠缺，与发达国家相比，国内互联网发展更为迅速，但相关的个人信息立法则相对欠缺，例如在网络环境下，对个人隐私的界定还存在不确定性。最后是新技术的应用带来立法的空白，例如数据挖掘得到的个人信息的权利归属问题等。

3.4　本 章 小 结

有限实名网络作为一种典型的互联网形态，有其自身特点，这些特点又直接导致在有限实名网络中累积的个人信息无论在形态以及权利归属上具有差异性。这些特征、差异性使得有限实名网络环境中的个人信息安全问题需要进行新的研究和探索。

本章的研究内容主要包括三个部分。首先，归纳总结有限实名网络在“技术匿名性”、“社会实名性”、实现间接性、信息风险性等方面的基本特征。其次，在阐述个人信息内涵的基础上，结合有限实名网络的基本特征，分析有限实名网络中个人信息的特征。最后，以有限实名网络以及有限实名网络中个人信息的内涵特征分析为基础，探讨分析有限实名网络中个人信息安全风险严重、个人信息侵犯的隐蔽性、个人信息保护监管的权利边界不清晰、立法保护缺乏可操作性等关键问题。

电子工业出版社版权所有
盗版必究