我国网络信息化进程中新型个人信息的合理利用与法律规制

陶 盈

摘要：随着我国网络信息化的推进，蕴藏着巨大商业价值的个人消费信息、位置信息、医疗信息、网络浏览信息等得到广泛应用。此类信息有别于直接可识别个人的身份信息，但通过互联网或者移动通信技术等进行综合分析与核对后，还是可能识别出特定个人或特定群体。此类“间接可识别个人信息”具有财产利益和人格利益的双重属性，其法理基础是人格权中的个人信息权，需要从法律层面规制其收集、存储、加工、传播和删除等环节，建立信息自由与信息安全并举的个人信息保护模式。

关键词：间接可识别个人信息；个人信息权；隐私权

具有可识别性是个人信息的重要特征，而大数据时代的到来让个人信息的内容得到极大丰富。随着互联网定向广告、手机生活记录软件、GPS定位系统等技术得到广泛应用，个人消费信息、生活信息、行踪记录、网络浏览记录、上网时间记录、医疗信息等匿名化信息正创造出巨大的经济效益。这类信息虽然不同于姓名、出生日期、工作单位、联系方式、指纹、基因、犯罪记录、病历记录等能够较容易地识别和映射特定个体身份的“直接可识别个人信息”，但是如果利用新技术将这些信息结合其他信息进行比对分析，仍然能识别出特定个人或群体，故属于“间接可识别个人信息”。如何将这类信息与个人隐私进行区分，确定其概念内涵及合理使用的界限，平衡好信息自由与信息安全之间的关系，是我国推进网络信息化进程中的重要课题。

一、个人信息的传统分类方式与新发展

随着互联网技术的飞速发展，网络空间不断扩大渗透，已成为军事安全领域的第五大空间。由于中国目前正面临严重的网络空间安全威胁，维护网络安全被上升到国家战略高度，习近平总书记也反复强调没有网络安全就没有国家安全。而大数据时代个人信息的安全与国家网络安全密切相关，体现私人属性的个人信息在大量聚合之后以大数据的形式呈现出来，就有可能反映涉及国家安全的国民信息（如国民基因信息、国民健康信息、国民财富信息等）。对于这类信息的收集、利用、存储、加工和传播等都应当受到适当限制，而个体在享受着科技带来的便捷服务的同时，也应当对基于公共利益的信息收集与利用有一定的容忍义务。如何平衡好信息自由与信息安全之间的关系，保障互联网社会中自由与尊严、人性与科技的和谐统一，不但体现着法律对个人隐私权保护的立场和力度，也关系到国家信息网络安全的总体战略。

个人信息又称个人记录或者个人数据，是指与特定个人相关联的、反映个体特征的具有可识别性的符号系统，包括个人身份、工作、家庭、财产、健康等各方面的信息①。其对应个人信息权，即信息主体依法对其个人信息所享有的支配、控制并排除他人侵害的权利。王利明教授认为，个人信息注重的是身份识别性，只要此种信息与个人人格、个人身份有一定的联系，无论是直接指向个人，还是在信息组合

收稿日期：2015－09－27

基金项目：2016年北京市教委项目“互联网征信时代的个人信息权问题研究”（SM201610038006）、2014年教育部人文社会科学重点研究基地重大项目“民法总则重大疑难问题研究”（14JJD820005）。

作者简介：陶盈，首都经济贸易大学法学院讲师，法学博士（北京 100070）。

① 王利明：《论个人信息权的法律保护——以个人信息权与隐私权的界分为中心》，《现代法学》2013年第4期。

?1994-2016 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

之后指向个人，都可以认为其具有身份识别性①。这种观点符合我国以及世界人格权法上对个人信息的基本认识。与个人信息内涵相近的概念是个人隐私，其对应隐私权，保护个人自由决定何时、何地以何种方式与外界沟通。主流学说主张个人信息权与隐私权呈交叉关系，二者既有联系又有区别②。

从比较法上来看，对个人信息的定义都强调其具有可识别性。1974 年美国《隐私权法》规范了行政机关对公民“个人记录”的利用规则，涉及教育、经济活动、医疗史、工作履历等。加拿大《个人信息保护与电子文件法》明确了个人信息是指所有可识别的个人的信息，通过《隐私法》保护以任何形式记载的可识别的个人的信息，并明确列举其具体类型。欧盟于 1995 年制定了有关个人数据保护的指令，定义个人数据为任何与一个明确的自然人或可识别的自然人身份有关的信息，其中，“可识别的人”是指可以直接或间接识别的人，尤其是借助于身份证号码或其他一些有关身体、心理、精神、经济、文化或社会身份等特定因素可以直接或间接识别其身份的信息③。日本《个人信息保护法》第二条第一款将个人信息界定为“能识别特定个人的信息”，同时指明了“也包括能够较容易地与其他信息核对后，识别出特定个人的信息。”在我国台湾地区 2010 年修订后的有关个人资料保护的规定中，将个人资料限定为“得以直接或间接方式识别该个人之数据”④。较之修改前的电脑处理个人资料保护的有关规定中“足资识别该个人之资料”的定义方式，明确了能够以“间接方式识别该个人之数据”亦属个人资料的保护范围。

目前，各国和地区多通过区分个人信息类型以划定保护和利用程度的不同。本文根据个人信息是否可以被直接地识别，将其分为“直接可识别个人信息”与“间接可识别个人信息”。直接可识别个人信息是指能够较容易地识别特定个人的信息，主要包括姓名、性别、身高、体重、三围、身体缺陷、出生日期、住址、身份证号、护照号码、电话号码、邮箱地址、基因、指纹、财产状况、家庭情况、婚恋情况、犯罪记录、病历记录等。此类信息是单独或与其他信息简单结合后就可以指向特定个人的身份识别性信息，是传统的个人信息权理论研究的对象。间接可识别个人信息是指，通过互联网或移动通信技术手段等综合分析和核对相关个人信息内容后，可以间接识别该特定个人或者特定群体的信息。目前受到关注的主要包括个人消费信息、生活信息、行踪记录、网络浏览记录、上网时间记录、网络聊天记录等匿名化信息。这类信息的特点是，虽然不能直接体现具体的信息主体是谁，但可以反映出该信息主体何时何地以何种方式从事了何种行为，还可以由此分析其兴趣爱好、活动范围、消费能力、消费需求、行为方式等，并通过数据分析为个人提供个性化的服务，如互联网定向广告服务、个人生活记录服务、个人定位服务等。此类信息也具有身份识别属性，与个人人格、身份有一定的联系。

对于个人信息“可识别性”的分类标准，目前学理上的区分较为抽象。事实上二者之间并没有不可逾越的鸿沟，而是要依据信息内容加以具体判断。例如网络聊天记录，如果只是私人间的对话信息，则被视为个人私生活的体现，仅属于个人隐私，而不是个人信息。但如果这些对话中反映出了个人的姓名、单位、年龄、联系方式、财务状况等身份性信息，能够由此直接识别出具体的个人，则被视为直接可识别个人信息。如果这些对话中虽然没有直接体现个人的身份信息，但是通过数字化处理等科技手段，能由对话信息推测出其消费能力、交易习惯、交往范围、爱好特长等信息并间接识别出该个人或所属特定群体，就可以视其为间接可识别个人信息。随着科学技术的发展，间接可识别个人信息对个人生活的介入程度不断深入，对这一问题的讨论已经不能局限于技术方面，而是需要在法律层面上加以规范。

二、间接可识别个人信息的利用价值与法律属性

大数据时代的某些个人信息已经成为一种商业资本，能够创造出巨大的经济利益。这些个人信息属于有效数据，具有高速传播、可以反复利用等特点，数据中蕴藏的信息资产具有明显的财产利益

① 王利明：《个人信息权与隐私权有何区别》，《北京日报》2014 年 3 月 24 日，第 18 版。

② 王利明：《个人信息权与隐私权有何区别》，《北京日报》2014 年 3 月 24 日，第 18 版。

③ Directive 95/46/EC, Official Journal of the Europiean Communities, 281, 23.11.1995, pp.31-50.

④ 引自郭明龙：《个人信息权利的侵权法保护》，北京：中国法制出版社，2012 年，第 22 页。

?1994-2016 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

属性，也带动了商业运营方式的革新。例如根据美国一项报道，到 2012 年为止，Farecast 机票价格预测系统用了近十万亿条机票价格记录预测美国国内航班票价，使用该系统的旅客平均每张机票可省 50 美元①。但另一方面，个人信息的商业化利用也给用户带来了不安。例如广告商基于用户健康方面的敏感信息而投放的定向广告有可能对用户构成侵扰。可见，信息主体既在享受科技创新带来的便捷服务，又在担心自己的权利会被牺牲。由于个体对科技发展和权利让渡的态度存在差异，一刀切的法律规范标准也显得生硬，个人信息保护领域正面临着前所未有的机遇与挑战。

在当下，最典型的间接可识别个人信息表现为个人生活记录信息（Life log），即①特定自然人②关于特定活动③对特定信息④通过特定记录媒体的⑤自动的⑥作为数字化数据的⑦概括的或者连续的记录（存储），由此取得的⑧有关特定个人的个人信息（个人识别信息）以及⑨并非与个人相关的个人信息（非个人识别信息）的总称②。个人生活记录的主要信息内容包括：（1）位置信息、个人简介信息等；（2）与电子邮件、健康相关的电子财政数据信息等；（3）过去的检索、访问、购买历史等。

通过电脑或者手机软件收集用户的位置信息是个人信息应用的最新领域。移动通信经营者、网络服务商或者手机软件开发商等通过收集和传递用户发信、收信位置信息向用户提供定位、导航等服务。2011 年《华尔街日报》报道了苹果公司和谷歌公司的智能手机定期将手机位置信息、识别码等传回各自公司，引发广大用户焦虑③。2013 年 6 月 JR 东日本铁路公司被指未经用户同意，将约 4300 万张 Suica（IC 卡）的乘车履历信息贩卖给日立公司，该分析结果被作为市场资料提供给车站周边的经营者。JR 东日本铁路公司由于没有做出充分的说明和通知，收到大量用户的投诉，其在发文致歉后停止了对用户信息的销售。

上述 Suica 事件中用户的位置信息并不具有显著的私密性，网络服务提供者对此类信息的利用行为也未对用户造成生活上的困扰，不构成侵犯隐私权。但这类信息属于个人信息，具有一定的财产价值，通过大数据分析可以间接识别该身份群体，因此用户自身有一定的支配权和自主决定权，只不过用户在享受大数据时代个性化和精准化体验服务的同时，对此种利用行为有一定的容忍义务。JR 东日本铁路公司作为信息收集者虽然将信息做了一定的匿名化处理后提供给了信息分析、加工者日立公司，再由其提供给广告商，但其未尽到充分的通知说明义务。该事件引发轰动的原因，与其说是现实地侵犯了消费者的个人信息权利，不如说更主要的是引发了消费者对信息收集者未经通知、许可即擅自利用个人信息之行为的不安和反感。

网络服务提供者收集用户的检索、访问、购买历史，主要用于提供互联网定向广告服务。互联网定向广告也称“互联网精准广告”、“行为定向广告”（Behavioral Targeting Advertising），是指广告商通过收集一段时间内特定计算机或移动设备在互联网上的基本行踪和网络消费行为等数据，预测用户的兴趣爱好及未来的行为模式，再通过互联网对特定计算机或移动设备投放最接近用户需求的广告信息的行为。主要表现为通过搜集用户的网页浏览记录、电子商务中的购买历史、位置信息等行动履历，分析用户的性质，提示适合个别用户或者特定人群的广告技术。例如，Gmail 会根据用户邮件信息，利用自动算法推送最相关的广告，并通过用户对广告的浏览、点击、下载、转发等行为获得收益。互联网定向广告大大提升了广告的有效性和针对性，可以避免广告商随机投放广告造成的不必要浪费，也在一定程度上方便了用户的选择和利用。但是，网络服务商记录用户上网习惯、浏览记录、购物历史等信息是以盈利为目的的，频繁的广告推送行为、基于敏感信息做出的推送行为等也可能对部分用户造成侵扰。

2014 年 3 月，我国首个指导和规范互联网定向广告业务中对用户信息的收集、保存、使用和转移行为的行业标准《中国互联网定向广告用户信息保护行业框架标准》开始实施。2015 年 6 月南京市中级人民法院终审判决北京百度网讯公司的网络个性化推荐行为不构成侵犯用户的隐私权。该案作为国内有关 cookie 技术与隐私权纠纷的第一案，明确了互联网企业利用网络技术记录和跟踪用户所搜索的关键词，将其兴趣爱好、生活学习工作特点等显露在相关网站上，并利用记录的关键词，对其浏览

① 维克托·迈尔－舍恩伯格、肯尼思·库克耶：《大数据时代：生活、工作与思维的大变革》，盛杨燕、周涛译，杭州：浙江人民出版社，2012 年。

② 新保史生「ライフログの定義と法的責任」，『情報管理』2010 年 9 月，第 295-310 页。

③ 《iPhone 与 Android 手机涉嫌秘密记录用户位置信息》2011 年 04 月 22 日报道，引自 http://it.sohu.com/20110422/n280378363.shtml，2014 年 11 月 29 日访问。

?1994-2016 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

的网页进行广告投放的行为，只要是在依法明示告知用户，且未直接将数据向第三方或向公众展示的前提下，不构成侵犯隐私权，而网络用户对此有一定的容忍义务。

本文认为，间接可识别个人信息具有财产利益和人格利益的双重属性，其法理基础是人格权中的个人信息权，强调的是以人的人格性自主为核心内容的控制性和自我决定性权利，属于《侵权责任法》第 2 条规定的受法律保护的民事权益，当受到不法侵害时，侵权行为人应当承担侵权责任。利用个人信息推送定向广告、进行有针对性的电话或上门推销等行为也应当受到法律的规范和指引。出于营利目的，未经信息主体许可即收集、分析、保存、交易、传播其个人信息的，权利人有权请求行为人对信息的收集、利用的目的、方式进行说明告知，甚至是更改、删除、停止利用其个人信息等。

三、个人信息保护的比较法经验与新动向

目前已有 50 多个国家和地区制定了保护个人信息的相关法律，强调收集公众个人信息必须出于正当目的，收集行为须征得被收集人的同意，并应当对收集到的资料妥善保管。

欧盟国家主要是通过个人数据相关立法明确了收集方在获取个人信息时应当明示利用目的，在向第三人提供时须事前征得同意。例如 1995 年公布的欧盟有关个人数据保护的指令规定了使用个人信息时须征得本人同意的事前同意原则，并确立了本人对个人信息享有公开、修改、删除的权利。2010 年《欧盟范围内个人信息数据全面保护实施办法》进一步强调网络服务提供者须经用户明确授权才可编辑、利用其个人信息的规则。2012 年欧盟的 Cookie 指令明确了如果用 cookie 追踪用户的使用习惯，必须取得使用者的“明确同意”。近年来欧盟国家也开始探索政府规制与自主规制的结合。

美国虽没有统一的个人信息保护法规，但一方面借助业界团体行业自律标准进行规制，另一方面也在强化公共机关的干预，并通过《禁止利用电脑犯罪法》、《电脑犯罪法》、《通讯正当行为法》等 130 余部法规打击网络匿名环境下的谣言、中伤。以互联网定向广告为例，2012 年奥巴马政府提出了消费者隐私权利法案，旨在加强对消费者网络隐私的保护，限制互联网公司对消费者隐私数据的收集、保存、公开等行为；为了打击秘密追踪行为，要求谷歌、雅虎、微软和 AOL 在浏览器上安装“不追踪”按钮，使消费者能够更方便地决定是否接受上述公司的追踪行为。

JR 东日本铁路公司 Suica 事件引发了日本对个人信息保护的反思。2014 年 6 月日本政府公布《个人数据有效利用制度修订大纲》，为个人信息保护相关法令改正后的措施内容指明方向。9 月总务省修订《电信事业个人信息保护指南》，将电信业务经营者处理的位置信息分为：(1)移动通信中基站的位置信息；(2)GPS 位置信息；(3)Wi-Fi 位置信息。对这类信息的利用规则要求：(1)根据利用者的意思提供位置信息；(2)关于位置信息的提供要确保利用者的认识、预见可能性；(3)采取与位置信息有关的合理措施；(4)在与第三方联合提供服务时应当通过相关合同条款等体现对利用者隐私权的保护。

目前，各国和地区基本明确了信息收集者在对个人信息采集、分类、存储、传送、跟踪、删除、监督等各个环节中应负的义务。具体经验可以总结为：

第一，规制信息收集者对敏感性个人信息进行分类收集和使用，确保信息收集利用目的与手段的正当性、过程的透明性。世界最大的网络广告公司 Google 已经表示在基于用户兴趣投放定向广告时，将用户分为约 20 个大类和近 600 个小类，但并不以种族、宗教、性取向等敏感信息来归类①。

第二，要求网站赋予用户自主决定是否允许个人信息被利用的权利。网站收集用户个人信息应当进行充分的告知和说明，应当允许用户通过设置浏览器关闭 Cookie，在向第三方或向公众展示时须取得用户的事前同意。以互联网定向广告为例，在美国有观点认为可以在线以“opt-in”方式向用户发送定向广告，但应在采集信息前征得信息主体的同意。广告商可以奖励给选择“opt-in”的消费者现金或附加内容，从而更好地获取各种信息。这种做法虽然一定程度地增加了定向广告的成本，但可以大

① “Google 推出行为定向广告”，2009 年 3 月 11 日，http://it.sohu.com/20090311/n262745982.shtml。

?1994-2016 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

幅提高允许有偿利用个人信息的消费者的比例，解决了有可能侵犯隐私权的后顾之忧。

第三，在对个人信息的利用过程中，采取适当安全管理措施，对信息进行充分的匿名化处理。美国联邦贸易委员会在《在迅速变化的时代保护消费者隐私》的报告中提出了允许经营者进行匿名化信息处理的“三要件”，即(1)采取合理的不可识别化(de-identify)措施；(2)公开承诺不对该信息进行再识别化(re-identify)；(3)向第三方移交该信息时通过签约禁止对个人信息的再识别化①。经营者应当采取必要措施，保证信息匿名化为不可能合理地连接到特定顾客电脑及其他设备的信息。

匿名化处理是对个人信息合法利用的关键，虽然各国和地区已经明确了网络服务提供者的该项义务，但对匿名化处理应当达到何种程度并未做具体规定。在JR东日本铁路公司编制的《向公司外提供Suica相关数据中间报告》中，将通过技术对个人信息进行匿名化处理的方法大体分为两类：一是单纯匿名化(例如对可识别信息作化名、删除处理，将间接可识别信息暧昧化)，通过删除姓名、住址等可识别信息以及ID等间接可识别信息进行匿名化从而无法识别特定个人。但这种处理还是存在可以确定特定个人的情形(例如115岁以上的老人，则姓名基本可以特定)。二是集合匿名化(例如，对N人作匿名化处理)，基于各种描述汇聚信息也只能限定于分辨出N人，而不能识别特定个人的匿名化处理(例如，通过年龄搜索只能以10岁为单位进行检索等)。由此可见，单纯匿名化的处理并不能消除个人信息的可识别性，对于涉及隐私的个人信息，对网络服务提供者的匿名化处理应该有更高标准的要求。

第四，在间接可识别个人信息的利用过程中建立包括投诉、问询、监督、追踪等内容的综合应对机制。通过区分信息收集者的善意、恶意、重大过失等，保护基于公共利益和科学发展需要的信息利用行为，打击进行恶意营销和不正当竞争的行为。

四、我国个人信息保护的现状与立法展望

大数据赋予互联网卓越的思考能力，使其对海量、高速、多变的数据进行有针对性的分析，为监测人们的生活提供了便利，但也令法律对隐私权的保护受到挑战。大数据时代需要信息的流动和分享，但也不能牺牲对个人信息安全的保护。当90％以上的信息都是以数字形式呈现时，掌握了这些数据就可以轻易地对其进行存储、加工、操作和发送。网络用户既需要发送位置信息，又想阻止非法用户窃取该信息；既想合法利用便利的网络业务，又不想令他人知晓。立法不应当阻碍科技的发展，而应当致力于合理应对技术革新的风险，厘清信息的正常利用与个人信息保护之间的界限，树立法律规制的标准，在发挥个人信息最大社会价值的同时，兼顾信息自由、信息安全和消费者权益保护等诸多方面。

纵观我国立法进程，自1997年公安部的《计算机信息网络国际联网安全保护管理办法》就明确了网络违法行为的法律责任。2008年《个人信息保护法(草案)》提出信息保护的“八个一般原则”，2009年《刑法修正案(七)》增设“出售、非法提供公民个人信息罪”和“非法获取公民个人信息罪”。2012年《全国人民代表大会常务委员会关于加强网络信息保护的决定》明确了网络服务提供者和其他企业事业单位收集、使用公民个人电子信息的规范规则。2013年《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》明确了首个“个人信息保护”专项国家标准。2014年最高人民法院《关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》第12条明确了五种情形为网络用户或者网络服务提供者公开个人隐私和其他个人信息的免责事由。

2015年2月，国家互联网信息办发布《互联网用户账户名称管理规定》，确定推行网络实名制。这有利于遏制网络犯罪和侵权行为，防范网络倾泻和群体极化现象，提高合法有效信息的传播效率，但也引发人们对个人信息被不当利用或泄露的担忧。同年7月公布的《网络安全法(草案)》有8个条款针对侵犯公民个人信息权益的行为，同时加大了政府在访问、获取记录和阻断非法私人信息方面的权限。

结合当下的社会现状和立法背景，本文认为，对于间接可识别个人信息的收集、存储、加工和转让

① “云计算中的隐私保护”国际电联电信标准化局(ITU-T)技术观察报告，法国电信 斯特凡 吉约休 ITU－T 文卡特森 摩尔，张进京译，载于《中国信息界》2012年第10月，第74-81页。

?1994-2016 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

等应当明确以下法律规则：

第一，明确信息主体对其间接可识别个人信息享有知情权、利用权、修正权、控制权、删除权等基础权利，应尽快完善个人信息安全法律制度，整治个人信息混杂失真的乱象，打击利用个人信息恶意营销和不正当交易的侵权行为。

第二，信息主体对上述权利的行使，受到信息自由、公共利益和国家安全等正当目的的合理限制。以间接可识别个人信息的删除权为例，其有别于信息主体享有的要求信息控制者对其直接可识别的个人信息在合理时间内及时删除的积极性权利，而更多地体现为仅可要求信息控制者承担告知说明义务和安全合理使用义务的防御性权利。为防止信息主体滥用删除权，也应当赋予信息控制者或者第三方机构以审查核实的权利，保障信息控制者行为自由、言论自由和科学技术水平发展的合理要求。

第三，坚持信息业者的过错责任原则，通过立法健全其管理责任体制。信息业者对用户间接可识别个人信息在利用、存储、转让第三人的过程中负有安全保障义务。需要确立信息收集利用的事前同意原则，对用户公开信息收集者的名称和用途；允许信息收集者在通知信息主体和取得用户许可的前提下进行合理利用，但应当对收集到的信息进行充分的匿名化处理；及时更正陈旧信息，慎防信息保管中的漏洞；建立信息利用的监督和追踪机制，并可以通过许可协议和转让协议的方式明确双方权利义务。

第四，明确公权力机关、基础设施机构等对间接可识别个人信息收集、利用、保护的权限及政府主导下信息过滤的基本原则。徒法不能以自行，对间接可识别个人信息的保护还需进一步推动互联网行业规范、自净规则、行政体制等社会整体环境的完善。

随着有效用的间接可识别个人信息创造的社会价值急速增长，围绕网络用户个人信息权利的纠纷频频发生，到底什么样的信息权益值得保护，如何对同样的个人信息权进行同等合理的保护等问题困扰着审判实践，亟待立法和司法机关释明裁判规则。在我国网络信息化不断深入的背景下，对于间接可识别个人信息应当尽快明确其保护规则及权利边界，全面确认其个人信息权属性，秉承依法治国和依法治网的理念，兼顾信息自由与信息安全的基本价值，保障互联网社会中自由与尊严、人性与科技的和谐统一。

Rational Utilization and Legal Regulation of New Type Personal Information in the Process of Network Informatization

TAO Ying

(Law School, Capital University of Economics and Business, Beijing 100070, P. R. China)

Abstract: Along with the advancement of network informatization in our country, there is a huge commercial value of the individual consumer information, location information, medical information, web browsing information and so on, and that information is widely used. Such information is different from the personal identity information that can be identified directly, but some specific individual and specific groups can also be identified after comprehensive analysis and checking, through the Internet or mobile communication technology and so on. Such "personal information that can be identified indirectly" has both properties interests and personal interests properties, and its legal basis is the personal information right of personal right. It is necessary to regulate the collection, storage, processing, transmission, deleting of information and so on from the aspect of law, and to build a personal information protection mode that can make the freedom of information and the security of personal information simultaneous.

Keywords: Indirectly identified personal information; Personal information rights; Right of privacy

[责任编辑：林　舒]

?1994-2016 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net