doi:10.16060/j.cnki.issn2095-8072.2022.01.003

我国间接识别个人信息规制机制的检视与完善

孙其华

（中国社会科学院大学法学院，北京 102488）

摘　要：我国在多年的立法实践中将“可识别性”确立为个人信息的识别标准，并在个人信息的规制方面借鉴了欧盟《一般数据保护条例》，对直接识别个人信息与间接识别个人信息一体适用了较高标准。但我国现行立法并未对间接识别个人信息的内涵及外延作出明确阐释，从而给相关立法的适用带来了较大障碍，其成因在于法院相关认知能力的不足、既有信息处理秩序的限制与我国传统价值观念的制约。今后，我国个人信息保护立法应从间接识别个人信息的内涵与外延两个层面，对间接识别个人信息的识别与规制机制予以完善。

关键词：个人信息；间接识别个人信息；可识别性；法律规制；《个人信息保护法》

中图分类号：D922.16　　**文献标识码：**A　　**文章编号：**2095 － 8072(2022)01 － 0031 － 11

引言

自2005年中国人民银行《个人信用信息基础数据库管理暂行办法》第4条第2款首次将“可识别性”作为对身份信息的判定标准后，“可识别性”标准的使用逐渐扩展至对所有类型个人信息的认定中，并于2020年5月28日得到了《民法典》第1034条第2款的确认，成为我国认定个人信息的重要标准，2021年8月20日正式通过的《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4条第1款也将“可识别性”明确规定为个人信息的重要构成要件之一。而根据信息可识别程度的不同，以是否可依据相关个人信息直接识别特定自然人为标准，可以将个人信息分为直接识别个人信息与间接识别个人信息两大类（邓建鹏和石立坤，2020）。其中，能够单独用以识别自然人身份的信息即为直接识别个人信息，需要结合其他信息方可识别自然人身份的信息即为间接识别个人信息。相比直接识别个人信息而言，间接识别个人信息的范围更为广泛且不确定，现实中个人信息所具有的可识别性通常并非全有或全无，而是介于两者之间，仅呈现出程度上的差异，甚至连一部分经过匿名化处理后的信息事实上也残存一定的可识别性（齐英程，2021），从而进一步模糊了“间接识别个人信息”这一概念的内涵与外延。

长期以来，我国的个人信息保护立法在很大程度上受到了被称为“史上最严格个人信息保护立法”的欧盟《一般数据保护条例》（General Data Protection Regulation，GDPR）的影响，最典型的譬如《个人信息保护法》第4条第1

款即在“个人信息”概念的界定上借鉴了《一般数据条例》中“扩张主义”（expansionism）的立法进路（Schwartz，2011），将所有直接或间接可识别的个人信息均纳入其调整范围：“个人信息是以电子或其他方式记录的与已识别或可识别的自然人有关的各种信息，不包括匿名化处理后的信息。”综观整部法律，我国《个人信息保护法》对个人信息的保护力度与欧盟《一般数据条例》大体相当，但高标准的个人信息保护立法如何与我国其他相关法律法规有效衔接，并有效运用于我国司法实践？本文试图通过对当前间接识别个人信息在我国立法、司法与个人信息处理实践中的法律规制现状的分析，揭示间接识别个人信息保护在应然与实然、理论与实践间的差异，借以反思我国个人信息保护立法中立法目标与具体规则及司法实践间的背离，并在此基础上尝试对我国间接识别个人信息的识别与规制机制予以完善。

一、间接识别个人信息规制机制的立法检视

界定个人信息是前信息时代个人信息法律保护制度建构的起点。如前所述，我国学者在借鉴吸收欧美国家个人信息保护立法的基础上，提出了以“可识别性”定义个人信息的方法（齐爱民，2008）。但大数据技术的发展引发了可识别性操作的困境：一方面，可识别性个人信息的范围不断扩大；另一方面，个人信息权利受侵犯并不以可识别性为限（王秀哲，2018）。对于间接识别个人信息而言，其内涵的宽泛性与外延的模糊性不容忽视。

（一）间接识别个人信息内涵的宽泛性

在大数据时代，数据挖掘与分析技术的高度发达使得个人信息所蕴含的价值被榨取至极限，而与此同时随着越来越多的人、事物与信息在互联网的作用下实现“万物互联”，任何信息均可能在与其他来源的各种信息相结合，并进一步挖掘与分析的基础上识别出特定的信息主体（Purtova，2018）。在大数据时代，绝大多数与个人相关的信息都具有间接可识别性，这意味着间接识别个人信息的内涵实际上无比宽泛和不确定，也对个人信息保护立法的适用带来了严峻挑战。

为进一步限缩可识别个人信息的范围，欧盟曾于1995年颁布《关于涉及个人数据处理的保护以及此类数据自由流动的指令》，确立了判断个人信息范围的“合理识别的可能性”（reasonable likelihood of identification）标准。随后，欧盟委员会的内部咨询机构“第29条工作组”（Article 29 Working Party）则在其针对个人信息（数据）认定标准问题发布的《关于个人数据概念的第4/2007号意见》（Opinion 4/2007 on the Concept of Personal Data，以下简称《意见》）中进一步提出，在判定“合理识别可能性”标准时应当综合考虑识别成本、数据控制者的目的、数据处理的方式、数据关涉的个人利益、现有的识别技术及其可能发展，以及数据控制者所采取的组织或技术保护措施失灵的潜在风险等因素。但《意见》一方面并不具备强制效力，另一方面有关个人数据可识别性认定标准的表述仍然被学者们认为过于模糊不

清。譬如Schwartz & Solove（2014）指出，根据《意见》的相关表述，只要处理个人数据的目标暗含识别数据主体，即可认定数据控制者或第三方具有合理识别数据主体的可能。这意味着当数据处理的最终目的在于识别数据主体时，数据控制者所收集的所有信息都会被认定为个人数据，即便其中的部分数据可能并未被用作识别数据主体。又如Stalla-Bourdillon & Knight（2016）认为，根据《意见》中的相关表述，只要相关个人数据的原始控制者没有删除具有可识别性的原始数据，那些在原始数据基础上经过转换或匿名化处理的数据仍将被认定为个人数据，从而导致接受经过匿名化处理数据的继受者们仍然要受到个人数据保护规则的约束，这将对相关数据的流通和共享造成严重阻碍。

相比欧盟，我国在立法层面也并未对个人信息界定标准和可识别性判断标准作出权威阐释，而是将直接识别个人信息与间接识别个人信息均“一揽子”地界定为个人信息，但“能够与其他信息结合识别自然人个人身份的信息”的认定标准极为模糊（齐爱民和张哲，2018）。究竟何为“结合”？何种主体能够判定特定信息是否具有间接可识别性？“其他信息”是否应当仅限于无需经过特别调查或支付较高费用就可获取的信息？虽然2014年中国科学技术法学会与北京大学互联网法律中心共同制定的《互联网企业个人信息保护测评标准》（以下简称《测评标准》）将个人信息界定为“能够切实可行地单独或通过与其他信息结合识别特定用户身份的信息或信息集合”，在“可识别性”的基础上新设了“切实可行”标准，试图对可识别性的范围进行限定，但其并未对这一“切实可行”标准进行进一步的阐释，且该《测评标准》并不具有法律效力，无法在司法实践中被法院援引。

（二）间接识别个人信息外延的模糊性

借助大数据技术对海量个人信息进行挖掘分析能够有效获取包括特定主体或群体在内的在偏好、行为模式等方面的潜在规律，但在此过程中必须有效平衡处理个人信息可能获得的价值与可能造成的风险。为达到这一平衡，各国立法均引入“匿名化”或“去标识化”等技术手段，即允许信息处理者通过采取特定技术去除某些个人信息所具有的可识别性，并进而免除其在利用相关个人信息时所负有的相关义务。其中，欧盟《一般数据条例》第26条规定，经过匿名化处理以致不再能够识别数据主体的个人数据，即“匿名数据”（anonymous data）不再适用个人数据保护的原则和规则，且这一匿名化处理必须使个人数据达到任何数据控制者或第三方通过所有可能的方式均无法识别数据主体的程度。而美国的个人信息保护立法则主要采用了“去识别化”（de-identification）措施作为豁免适用个人信息保护规则的条件。1996年颁布的《健康保险携带和责任法案》（Health Insurance Portability and Accountability Act，简称HIPPA法案）规定了“专家决定法”（expert determination method）和“安全港法”（safe harbor）两种去识别化方法。具体而言，“专家决定法”是指经具备适当知识和经验的专家进行信息检查和去识别化措施，认定已将信息隐私泄漏的

风险降至最低，而“安全港法”则是指通过移除姓名、位置信息、邮政编码等一系列标识，从而使信息的可能接收者无法单独或者结合其他信息识别出该信息指向的具体信息主体，经过去识别化处理的信息不再属于个人信息。

我国个人信息保护立法主要借鉴了欧盟的相关规定，但不同法律规范之间仍存在较大分歧。譬如《网络安全法》第42条规定：“网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。”对此，立法者指出，“经过处理无法识别特定个人且不能复原”类似欧盟立法中的匿名化处理，强调处理结果必须使个人信息达到无法再识别信息主体且不能被复原的程度（杨合庆，2016）。但全国信息安全标准化技术委员会于2017年颁布的《个人信息安全规范》第8.2条则提出了如下要求：“向个人信息主体告知共享、转让个人信息的目的、数据接收方的类型，并实现征得个人信息主体的授权同意。共享、转让经去标识化处理的个人信息，且确保数据接收方无法重新识别个人信息主体的除外。”而根据《个人信息保护法》第73条第3项，“去标识化”是指“个人信息经过处理，使其在不借助额外信息的情况下无法识别特定自然人的过程”。换言之，将经过去标识化处理的个人信息与额外信息相结合，仍存在识别信息主体的可能，因而此处的“经过去标识化处理的个人信息”类似欧盟立法中的“假名化信息”（psedonymous data）而非已被匿名化处理的信息，本应属于间接识别个人信息的范畴，但《个人信息安全规范》将这类经过去标识化处理的信息认定为非个人信息，而最新的《个人信息保护法》对此则未置可否。此外，根据欧盟立法所确立的标准，经过假名化处理的个人信息应当达到任何数据控制者或第三方均无法识别的程度，但我国当前的“去标识化”个人信息显然远未达到此标准。上述规则的含混表述一定程度上阻碍了对间接识别个人信息与非个人信息的有效区分，表明我国立法机关至少在间接识别个人信息与非个人信息的区分问题上并未形成前后一致的统一认识。

由此可见，目前我国相关法律法规和司法解释均未对间接识别个人信息的判断标准作出具有可操作性的解释，且现有立法在对间接识别个人信息内涵与外延的界定问题上较为宽泛与模糊。这引发了两方面的风险：一方面，相对模糊的判断标准、高昂的调查成本与技术知识的欠缺在一定程度上限制了法院准确识别个人信息的能力，由此进一步导致了相关规则形同具文；另一方面，其为信息处理者通过设置隐私条款等方式随意缩减间接识别个人信息范围、逃避承担相应个人信息保护义务提供了潜在空间，从而使信息主体的隐私与安全面临更大的危机。

二、间接识别个人信息规制机制的实践难题

间接识别个人信息内涵的不确定性及其外延的模糊性在一定程度上影响了相关规则在司法实践中的适用。以全国首例大数据产品不正当竞争案——“安徽美景信息

科技有限公司与淘宝（中国）软件有限公司不正当竞争纠纷案”（以下简称“淘宝诉美景不正当竞争案”）为例，在本案中安徽美景信息科技有限公司（以下简称“美景”）主张，淘宝（中国）软件有限公司（以下简称“淘宝”）抓取并出售的用户浏览、搜索、收藏、加购、交易信息以及在此基础上推测出的用户性别、职业、区域、偏好等信息属于间接识别个人信息，其行为违反了我国有关个人信息保护立法。而“淘宝”则主张，其开发的“生意参谋”所处理的并非个人信息，不存在单独或与其他信息结合识别自然人个人身份的可能性，因而不适用我国个人信息保护立法中的相关规定。[①]

显然，该案的关键在于判断涉案信息是否属于间接识别个人信息，而法官在此问题上显然存在判定难度：一方面，法院否认相关涉案信息为个人信息，“这些行为痕迹信息与标签信息并不具备能够单独或者与其他信息结合识别自然人个人身份的可能性，故其不属于《网络安全法》中的网络用户个人信息”；[②]另一方面，法院又认为，由于网络用户行为痕迹信息“包含有涉及用户个人偏好或商户经营秘密等敏感信息”，因此“应当比照《网络安全法》第41条、第42条关于网络用户个人信息保护的相关规定予以规制”。这表明法院实际上认可网络用户行为痕迹信息与用户在网络中留下的个人身份信息或曾披露的其他信息相结合时，可能会识别出特定的信息主体，而作出这一判断的前提是相关行为痕迹信息属于个人信息，且符合“间接识别个人信息”的特点。此外，在该案中法院还提出：“涉案‘生意参谋’数据产品所使用的网络用户信息经过匿名化脱敏处理后已无法识别特定个人且不能复原，公开‘生意参谋’数据产品的数据内容，对网络用户信息提供者不会产生不利影响。”如前所述，“匿名脱敏化处理”是针对具有可识别性的个人信息所采取的技术手段，其目的在于消除个人信息原本所具有的可识别性。这亦表明法院已经意识到该案中淘宝收集的用户行为痕迹信息与标签信息等所具有的可识别性，属于间接识别个人信息的范畴。

法院判定间接识别个人信息能力的不足还体现在对同一种类的个人信息的“同案异判”。以手机号码为例，在“谭少慧侵犯公民个人信息案”中，[③]法院认为“单独的手机号码不能够单独识别特定自然人身份或者反映特定自然人活动情况”，因而不足以被认定为《刑法》所规定的“公民个人信息”。而在“庞慧敏、韩跃、秦钦、王玉、张丽侵犯公民个人信息案”中，[④]法院则认为“纯电话号码属于公民个人信息”，并指出“无论是否实名制，一个电话号码后面对应的一定是一个自然人”，因而电话号码显系个人信息。类似的情形还包括cookie记录的网络用户浏览、搜索记录等其他类型的信息。譬如在“北京百度网讯科技有限公司与朱烨隐私权纠纷案”中，一审法院认为百度网讯公司通过使用cookie技术收集的用户浏览、搜索记录信息展示

① 相关案件信息参见“安徽美景信息科技有限公司与淘宝（中国）软件有限公司不正当竞争纠纷案”，（2018）浙01民终7312号。
② 尽管事实上，2017年全国信息安全标准化技术委员会于该案发生之前颁布的《个人信息安全规范》已明确将“个人上网记录”，包括个人通过日志储存的用户操作记录、网站浏览记录、软件使用记录、点击记录等行为痕迹信息规定为个人信息。
③ 相关案件信息参见“谭少慧侵犯公民个人信息案”，（2018）皖0111刑初377号。
④ 相关案件信息参见“庞慧敏、韩跃、秦钦、王玉、张丽侵犯公民个人信息案”，（2018）川1302刑初6号。

了用户个人上网的偏好，反映了用户的个人兴趣与需求等私人信息，且能够标识用户个人的基本情况和个人生活情况，因此相关信息属于个人信息甚至隐私信息。而二审法院则认为cookie收集的用户浏览、搜索记录信息无法与特定的人相联系，也不包含《电信和互联网用户个人信息保护规定》第4条规定的个人身份识别信息，其收集到的仅是不可识别的网络行为碎片化信息，不可能与网络用户发生对应识别关系，因此不属于个人信息。[①]上述情况表明，在部分案件中法院对间接识别个人信息的把握失当，由此对相关个人信息保护立法规则的规制效果产生了不利影响，并已经引发了相当数量的“同案异判”。

三、间接识别个人信息规制机制的成因剖析

（一）法院相关认定能力的不足

如前所述，“间接可识别性”并非特定类型信息的静态属性，相反必须结合特定的信息处理场景与条件对其进行动态判定（Tene & Polonetsky，2013）。因此，迄今为止尚没有对间接识别个人信息概念的精准界定，而是需要综合考虑信息处理者的目的、信息处理方式、掌握的其他相关信息识别技术及其发展可能、信息的后续流转与使用等诸多因素予以综合判断（范为，2016），这对法院而言是相当严峻的挑战。法院通常缺乏了解上述信息的有效途径，譬如在前文“淘宝诉美景不正当竞争案”中，法院在判定涉案信息是否具备间接可识别性时，主要参考依据是淘宝所公开的《淘宝平台服务协议》与《隐私权政策》，并在此基础上作出判决，从而混淆了信息处理者所宣称采取的信息处理行为和其实际所采取的信息处理行为。

此外，法官囿于其知识结构并不具备衡量特定信息是否能够被用于识别信息主体的专业知识和技术经验，在此情况下法官更倾向于通过弱化涉案信息所具有的间接可识别性，免除信息主体的责任，从而避免其裁判结果对前述当前既有的信息处理实践产生冲击。而在信息处理者已经对特定个人信息采取一定程度的去标识化处理的情况下，法官还需对经过去标识化处理的信息是否已经转化为非个人信息进行判断。有学者指出，匿名信息与个人信息之间的界限并非一成不变，二者之间存在因具体环境变化而相互转化的可能（Stalla-Bourdillon & Knight，2016）。此种不确定状态使法院在判定信息可识别性方面的知识缺陷更加凸显。

（二）既有信息处理秩序的限制

目前，信息处理者往往通过利用立法规则在间接识别个人信息判断标准方面的粗疏性，以服务协议、信息保护政策等形式将部分间接识别个人信息排除在个人信息的范围之外，以减轻甚至免除自身在收集、利用和流转此类信息时所负有的通知、征

① 相关案件信息参见“北京百度网讯科技有限公司与朱烨隐私权纠纷案”，（2014）宁民终字第5028号。

询同意、采取处理措施等各类义务，回避上述义务履行不当所可能产生的责任。此种“行业惯例”事实上已经取代高度原则化的相应立法规则成为调整当前信息处理者个人信息处理实践的“潜规则”。

而法院在面对由此种“潜规则”塑造起的个人信息处理和流通秩序时，往往不可避免地表现出一定程度的保守和迁就。譬如在前述“淘宝诉美景不正当竞争案”中，法院并非没有意识到淘宝所收集的用户行为痕迹信息与标签信息所具有的间接可识别性，但其最终并未认定淘宝的行为构成对个人信息的不当收集和交易，这体现了法院在现实运作过程中的一种“另类”实践理性。一方面，面对业已形成且普遍存在的信息处理实践时，轻易否定乃至推翻此种信息处理惯例可能会对当前的个人信息收集、利用和流通秩序造成颠覆性影响，导致既有信息处理和流通秩序的不稳定。同时，可能因为对信息处理者的正常运作和利益需求所造成的不利影响而遭遇广泛、持久的反对。在缺乏法律明文规定的指引和支持的前提下，作出这样的认定无疑会给法院带来无法预测的风险，难以实现法律效果和社会效果的统一。另一方面，在“淘宝诉美景不正当竞争案”中，并无任何信息主体主张其个人信息遭到了淘宝的不当利用或侵犯，相比之下淘宝基于抓取和分析个人信息所形成的“生意参谋”数据产品能够为其带来可观的商业利益与市场竞争优势，在综合考量两种法益的基础上，通过将用户行为痕迹信息与标签信息解释为非个人信息，从而维持现有的信息处理实践亦是一种在个案场合下对法院而言最符合理性的选择。上述做法反映了一种“后果主义的裁判模式”，即法院基于对裁判后果的考量而在给定情况下调控裁判（雷磊，2019）。在此过程中，对各类后果因素的考虑可能会在相当程度上影响法官对法律问题本身的判断，从而在一定程度上牺牲立法规则对自然人个人信息安全期待的保护，为相关间接个人信息被不当利用留下隐患。

（三）我国传统价值观念的制约

本质上，法院与信息处理者对间接识别个人信息的规制实践与立法规定之间的反差源自当前个人信息保护立法所采纳的高标准与现阶段我国社会整体在个人信息隐私观念方面的发展水平与价值取向之间的差距。虽然我国目前的个人信息保护立法借鉴了欧盟《一般数据条例》中的相关规则，采取了较高的个人信息保护标准，但该制度借鉴的成功与否还取决于我国的社会现实以及全社会在个人信息保护方面的价值取向。

欧洲立法将信息隐私视为人格尊严的重要体现，认为对个人信息的不当收集和利用会阻碍自然人对其自我表现的自由构建，使其“本人人格塑造的结果偏离原来的预期”（谢远扬，2015），从而挫伤其人格尊严。因此，对信息隐私的保护被视为一种根本价值，在立法上享有优于其他权利的价值位阶。而与欧陆国家相比，我国并不具备高度重视信息隐私的传统，甚至在相当长的时间内隐私话语在我国始终处于缺失状态。譬如费孝通曾将西方社会的结构比喻为“团体格局”，在这一格局中，最重要

的就是界限的观念，个体被视为平等、独立的存在，而中国社会的结构是“差序格局”，群己的界限是相对的（费孝通，2007）。在传统中国社会中，个体彼此间界限的模糊导致隐私观念缺乏发育的土壤。一个明显的例证，在我国“隐私权”这一概念直到2009年才成为正式的立法表达，而针对信息隐私的一般保护规定则直到2012年的《关于加强网络信息保护的决定》中才首次出现。

社会结构、伦理观念以及相应的立法传统决定了我国社会在信息隐私保护方面的价值取向与欧洲国家存在显著差异。中国社会将信息隐私视为工具价值（instrumental good）而非本质价值（intrinsic good），强调信息隐私的“社会功能”和保护信息隐私对推进社会发展、维护社会秩序的作用，对信息隐私的保护必须受到社会和国家整体利益的限制（Lv，2005）。信息隐私在我国并非必然享有优先于其他法益的地位，其与其他法益一样需要被置于利益衡量的背景下决定何者应当在特定阶段、特定场合下享有更高的价值位阶（Schwartz & Peifer，2010），这一做法实际上与美国的个人信息保护制度而非GDPR的做法更为相似。利益衡量理论指出，权利的核心在于利益，而法律保护的本质在于保护更应当保护的利益（梁上上，2021）。因此，我国立法虽然借鉴了欧盟《一般数据条例》的做法，赋予信息主体对个人信息近乎绝对的控制权和受保护的权利，但在司法实践中，个人信息事实上仍需在与其他利益的博弈中获得自身的优势地位。

四、间接识别个人信息规制机制的完善路径

如前所述，我国信息处理者和司法机关在个人信息的利用与保护方面始终秉持利益平衡的理念，但当前立法将间接识别个人信息与直接识别个人信息等量齐观的做法并不利于利益平衡的顺利实现，因而这一理念在司法实践中难免被虚置甚至异化。此外，间接可识别性并非个人信息一成不变的固有属性，而是高度依赖于其所处的情境，同时取决于相关个人信息的利用主体与利用方式。因此，事前的、静态的间接识别个人信息规制难以发挥良好效果，当前对于间接识别个人信息的规制规则可从厘清内涵、扩大外延两方面加以完善，从而构建起动态的、全面的间接识别个人信息规制机制。

（一）厘清内涵

不同类型的个人信息与信息主体人格利益的关联程度以及蕴含的潜在风险并不相同，因而应当对其分别设置不同的规制规则。对于非敏感的间接识别个人信息无须予以与直接识别个人信息同样严格的事前控制，而应基于对此类信息的保护与利用的平衡，在适当放松对收集、利用和流转间接识别个人信息的事前控制的同时，赋予信息处理者对间接识别个人信息持续的保护义务，引导其自觉遵守相关规定。在此基础上，法院亦可对间接识别个人信息作出较为宽泛的解释，并以对信息处理者履行信息保护义务情况的判定取代对间接识别个人信息的判定来判断特定信息处理行为的合法性。

对间接识别个人信息的保护义务应覆盖整个信息处理的过程，其中的重要一环在于，如果要对间接识别个人信息进行合法处理，除特别情况外必须经过信息主体的同意。对此，欧盟《一般数据条例》第6条第1款列举了六种合法处理个人信息的情形：（1）经过信息主体的同意；（2）处理是为履行合同的必要或是因在签订合同前的请求而需要对个人信息进行处理；（3）为了履行法律义务；（4）为了维护自身或者第三方的切身利益；（5）为了维护公共利益；（6）信息控制者或第三方为了追求合理利益的对信息的必要处理（刘颖和谷佳琪，2020）。我国亦可借鉴此类规定，通过明确列举例外情形的方式，进一步明晰间接识别个人信息的内涵所在。此外，立法还可进一步明确间接识别性个人信息不受《个人信息保护法》以及《网络安全法》中关于个人信息查询权、删除权、更正权等规则的约束。上述规则事实上仅能规制直接识别个人信息，因为间接识别个人信息与直接识别个人信息的根本区别在于，其无法直接用于识别特定信息主体。因此，为真正实现间接识别个人信息的“间接可识别性”，应尽可能避免在间接识别个人信息与信息主体之间建立起直接的联系，否则不仅无益于对信息主体的保护，还会增加暴露信息主体身份和隐私的风险。

（二）扩大外延

从各国的尝试中不难发现，明确界定间接识别个人信息概念的外延十分困难。事实上，有学者也认为此种尝试未必具有预想的重要性，“不确定法律概念的出现，正是源于法律对一般性属性的需要”（Schwartz，2011；王贵松，2016）。正是个人信息处理实践的复杂性和个人信息类型和使用方式的多样性决定了个人信息保护立法在确定其适用范围和保护对象时，需要借助不确定概念以保有适度的宽松和弹性。因此，以间接识别个人信息这一具有弹性的不确定性概念实现对亟须保护的个人信息的尽可能全面的涵盖，有助于更好地预防和应对个人信息安全风险。因而有必要适度扩张间接识别个人信息这一概念的外延，将部分难以为《个人信息保护法》所涵盖的个人信息纳入其中。

与此同时，间接识别个人信息与非个人信息间界限的模糊导致现实中这一弹性概念往往被部分信息处理者用于逃避承担应负的信息保护义务。有鉴于此，笔者认为可以将间接识别个人信息作为个人信息保护立法的“兜底概念”，对其进行尽可能宽泛的解释，并将经过匿名化处理的非个人信息纳入间接识别个人信息的范围。因为随着数据分析和信息再识别技术的不断发展，间接识别个人信息与经过匿名化处理的非个人信息之间的区别正被不断消弭，传统的“个人信息—非个人信息”二分法也在逐渐丧失其原有的区分功能（FTC Staff，2011）。间接识别个人信息与经过匿名化处理的非个人信息均存在不同程度的可识别性风险，且两者间存在相互转化甚至相互混淆、同化的可能。譬如美国联邦贸易委员会（Federal Trade Comission）就曾注意到，美国企业普遍具有对匿名信息进行再识别的倾向，并时常能够成功实现对匿名信息的再识别（FTC Staff，2011）。与此同时，欧盟第29条工作组也承认，经过匿名

化处理的信息仍存在“剩余风险”（residual risks），因而信息处理者也仍需经常性地对这种“剩余风险”进行重新评估，并据以调整期采取的信息保护措施。[①]即便对于达到匿名化标准的信息，信息处理者在决定如何使用这些信息，尤其是与其他信息结合使用时，仍需充分考虑相关的可识别性因素，当相关因素导致此类信息的再识别风险超出其可接受的范围时，对该信息的处理可能需要再次被纳入个人信息保护法的调整范围。

结语

我国间接识别个人信息规制的应然与实然、理论与实践之间的差异表明，当前立法对间接识别个人信息处理行为的严格规制理念并未在立法层面得到一以贯之的全面落实，且在一定程度上脱离了我国当下的社会现实与司法实践。在大数据时代，个人信息的保护和利用应当被置于同等重要的位置，而非以牺牲一方为代价成就另一方（张新宝，2015）。当法院遇到相关案件时，更是应当在个人信息主体的法益保护与信息开发利用者的行为自由之间进行比较权衡，在平衡兼顾二元价值的基础上，合理划分个人信息的法益保护范围与信息开发利用之合法性边界（宋亚辉，2019）。对间接识别个人信息的保护必须与利用间接识别个人信息所能创造的价值相平衡，绝对保护这部分个人信息在现阶段的我国既无法实现，也并无必要，且这种“一刀切”的做法本身亦不符合大数据时代的社会发展趋势。我国今后对个人信息法律规制应摒弃对个人信息保护高标准的单一追求，转而探索符合我国国情的个人信息保护制度。当前，《个人信息保护法》已通过并正式施行，为我国个人信息保护提供了基本的、框架性的法律规范，但欲达致立法目的还需立法、执法和司法部门对该法的进一步理解与合理适用，否则“通过一部无法执行的法律就是一项有害的政策，因为如此法律将损及人们对于可执行法律的忠诚度”（保罗·戈斯汀，2008）。

参考文献

[1] 邓建鹏, 石立坤. 间接个人信息安全及法律保护[J]. 中国信息安全, 2020(1):107–110.
[2] 范为. 大数据时代个人信息保护的路径完善[J]. 环球法律评论, 2016(5):92–115.
[3] 费孝通. 乡土中国[M]. 上海：上海人民出版社, 2007.
[4] 保罗·戈斯汀. 版权之道：从古登堡到数字点播机[M]. 金海军, 译. 北京: 北京大学出版社, 2008.
[5] 雷磊. 反思司法裁判中的后果考量[J]. 法学家, 2019(4):17–32.
[6] 梁上上. 利益衡量论（第三版）[M]. 北京：北京大学出版社, 2021.
[7] 刘颖, 谷佳琪. 个人信息去身份化及其制度构建[J]. 学术研究, 2020(12):58–67.
[8] 齐爱民, 张哲. 识别与再识别：个人信息的概念界定与立法选择[J]. 重庆大学学报（社会科学版）, 2018(2):119–131.
[9] 齐爱民. 个人信息保护法研究[J]. 河北法学, 2008(4):15–33.
[10] 齐英程. 我国个人信息匿名化规则的检视与替代选择[J]. 环球法律评论, 2021(3):52–66.
[11] 宋亚辉. 个人信息的私法保护模式研究[J]. 比较法研究, 2019(2):86–103.
[12] 王贵松. 行政法上不确定法律概念的具体化[J]. 政治与法律, 2016(2):144–152.

① See Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymization Techniques (April 10 2014), p.44.

[13] 王秀哲. 大数据时代个人信息法律保护制度之重构[J]. 法学论坛, 2018(6):115–125.
[14] 谢远扬. 信息论视角下个人信息的价值——兼对隐私权保护模式的检讨[J]. 清华法学, 2015(3):94–110.
[15] 杨合庆. 中华人民共和国网络安全法释义[M]. 北京: 中国民主法制出版社, 2016.
[16] 杨楠. 个人信息“可识别性”扩张之反思与限缩[J]. 大连理工大学学报（社会科学版）, 2021(2):98–107.
[17] 张新宝. 从隐私到个人信息：利益再衡量的理论与制度安排[J]. 中国法学, 2015(3):38–59.
[18] FTC Staff,“Protecting Consumer Privacy in an Era of Rapid Change–A Proposed Framework for Businesses and Policymakers”, *Journal of Privacy and Confidentiality*, 2011:67–94.
[19] Lv, Yao–Huai,“Privacy and Data Privacy Issues in Contemporary China”, *Ethics and Information Technology*, 2005(7):11–13.
[20] Purtova, N.,“The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law”, *Law, Innovation and Technology*, 2018,40:40.
[21] Schwartz, P. M.,“The PII Problem: Privacy and a New Concept of Personally Identifiable Information”, *N.Y.U.L.Q. Rev*. 2011,86,1814–1877.
[22] Schwartz, P. M., and D. J. Solove,“Reconciling Personal Information in the United States and European Union”, *Calif. L. Rev*. 2014, 102:877–895.
[23] Schwartz, P. M., and K.–N. Peifer,“Prosser’s Privacy and the German Right of Personality”, *Calif. L. Rev*. 2010,98,1925–1954.
[24] Stalla–Bourdillon, S., and A. Knight,“Anonymous Data v. Personal Data–False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data”, *Wis. Int’l L. J*. 2016,34:284–318.
[25] Tene, O., and J. Polonetsky,“Big Data for All: Privacy and User Control in the Age of Analytics”, *Northwestern Journal of Technology and Intellectual Property*, 2013(11):239–258.

【作者简介】孙其华：中国社会科学院大学法学院博士研究生。研究方向：信息法。

Review and Perfection of the Regulation Mechanism of Indirect Identification of Personal Information in China

SUN Qi-hua

(School of Law, University of Chinese Academy of Social Sciences, Beijing 102488, China)

Abstract: China has established "identifiability" as the identification standard of personal information in years of legislative practice, and the regulation of personal information refers to the European Union "General Data Protection Regulations", and applies a higher standard to the direct identification of personal information and indirect identification of personal information. However, the current legislation of our country has not clearly explained the connotation and extension of indirect identification of personal information, which brings great obstacles to the application of relevant legislation. The reason lies in the deficiency of the court's cognitive ability, the limitation of the existing information processing order and the restriction of our traditional values. In the future, China's personal information protection legislation should improve the identification and regulation mechanism of indirect identification of personal information from two aspects of connotation and extension.

Keywords: personal information; inndirect identification of personal information; identifiability; legal regulation; Personal Information Protection Act

（责任编辑：马莹）