理论前沿

我国个人信息匿名化规则的检视与替代选择

齐英程

内容提要:个人信息匿名化规则试图通过彻底消除个人信息蕴含的可识别性以免除信息处理者负有的个人信息保护义务,但这一规则却面临着理论上的困境和适用上的障碍。“匿名化迷思”的根源在于,其试图通过对信息性质作出“非此即彼”的判定,以决定是否“一刀切”地斩断个人信息处理者所负义务。而现实情况是,个人信息具有的可识别性通常并非全有或全无,而是呈现出不同程度的识别能力,经过匿名化处理的信息仍可能残存一定的“可识别性”,将其彻底排除至个人信息保护立法的规制范围之外,事实上难以有效消解匿名信息具有的“剩余风险”。未来我国个人信息保护立法应从当前的一体规制模式转向基于信息识别能力类型化的区别规制模式,根据个人信息蕴含的识别能力而构建多层次的个人信息保护义务体系,并将匿名信息作为一种具有较低识别能力的个人信息纳入规制范围,实现个人信息保护与利用间的动态平衡。

关键词:个人信息　可识别性　识别能力　匿名化　去识别化

齐英程,吉林大学法学院博士后研究人员。

2020 年 10 月,我国首部个人信息保护立法草案提请全国人大常委会审议,标志着我国个人信息保护立法工作迈入了体系化阶段。《个人信息保护法(草案)》第 4 条将“个人信息”界定为“以电子或者其他方式记录的与已识别或者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”,从而将经过匿名化处理的信息完全排除至个人信息保护法的规制范围以外。其原理在于,个人信息保护规则仅适用于具有可识别性从而可能揭露与自然人相关之特定情况的信息,而经过匿名化的信息则丧失了识别特定自然人的能力,自然无须受到个人信息保护立法的约束。然而,何种程度的处理能够使个人信息转化为匿名信息?完全的匿名化能否实现?经过匿名化处理后的个人信息是否必然不再具有安全风险?对上述问题的轻松掠过可能导致我国个人信息保护立法因未能准确把握信息时代的现实风险,而难以承担充分保护公民个人信息安全的重要使命。

当前,匿名化处理的有效性及其应然标准等问题已在世界范围内引发了广泛的关注与讨论。欧姆(Paul Ohm)、施瓦茨(Paul M. Schwartz)和索罗夫(Daniel J. Solove)等学者均

主张,在大数据时代,匿名化乃注定是一种失败的尝试,立法应放弃当前“个人信息—匿名信息”的二分法,而应基于对具体信息风险的评估分别确立相应的个人信息保护标准。[1] 鲁宾斯坦(Ira S. Rubinstein)和哈佐格(Woodrow Hartzog)提出,匿名化规则乃是一种结果导向的规制规则,其效果难以保证和评估,个人信息保护立法应当将注意力转向通过对数据披露的程序性规制以实现数据安全风险的最小化。[2] 而鲍迪伦(Sophie Stalla-Bourdillon)和奈特(Alison Knight)则认为,虽然匿名化处理不可能达到完全消除匿名信息含有的再识别风险的效果,但其作为划定个人信息和非个人信息界限的标准,对于指导信息处理实践仍具有重要意义,只不过关键在于个人信息保护立法应改采一种更加动态的、场景化的匿名化标准,以实现对风险的灵活应对。[3] 既有研究主要着眼于欧盟和美国的个人信息匿名化(去标识化)规则所具有的缺陷及其完善途径,其研究结论对我国个人信息保护规则的构建具有一定借鉴价值。在此基础上,本文通过对当前我国个人信息匿名化规则的检视,明确这一规则的内在缺陷及其在实践中可能产生的实际效果,进而结合我国的立法进展和社会背景,寻求个人信息匿名化规则在我国立法语境下的替代方案,对未来我国个人信息保护立法规则的构建提出相应建议。

一 个人信息匿名化规则的内在缺陷及适用障碍

(一)个人信息匿名化规则的内在缺陷

立法规定个人信息匿名化规则的目的在于免除个人信息处理者在对特定信息进行后续处理和流转时负有的合规负担,这预设了经过匿名化处理的信息仍然具有继续留存和使用的价值。然而,这一规则要求匿名化处理必须达到彻底消除个人信息具有的可识别性且无法复原的程度,其在追求彻底消除信息安全风险之同时,亦将完全抹杀信息具有的后续利用价值。[4] 个人信息处理者对个人信息进行处理的目的主要在于通过对信息间相关关系的识别以发现个体或群体在行为、状态等方面的潜在模式,进而作出预测或决策。[5] 而匿名化规则在彻底斩断个人信息与信息主体的相关性之同时,也同时丧失对信息处理者的参考价值。

从我国当前的实践来看,各信息交易平台和信息处理者所交易的相关信息均只是经过一定程度的去标识化处理而无法单独识别出信息主体的间接识别性个人信息,比如某

〔1〕 See Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 *UCLA Law Review* 1701, 1744 (2010); Paul M. Schwartz & Daniel J. Solove, The PII Problem: Privacy and a New Concept of Personally Identifiable Information, 86 *New York University Law Review* 1814, 1894 (2011).

〔2〕 See Ira S. Rubinstein & Woodrow Hartzog, Anonymization and Risk, 91 *Washington Law Review* 703, 760 (2016).

〔3〕 See Sophie Stalla-Bourdillon & Alison Knight, Anonymous Data v. Personal Data - False Debate: An EU Perspective on Anonymization, Psyeudonymization and Personal Data, 34 *Wisconsin International Law Journal* 284, 322 (2016).

〔4〕 See Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 *UCLA Law Review* 1701, 1704 (2010); Sophie Stalla-Bourdillon & Alison Knight, Anonymous Data v. Personal Data - False Debate: An EU Perspective on Anonymization, Psyeudonymization and Personal Data, 34 *Wisconsin International Law Journal* 284, 285 (2016).

〔5〕 See Joshua A. T. Fairfield & Christoph Engel, Privacy as A Public Good, 65 *Duke Law Journal* 385, 389 (2015).

大数据交易中心交易的相关省份个人失信名单以及相关省市专业技术职务人员信息等。事实上,针对完全丧失可识别性的个人信息几乎不存在任何市场需求。同样,在自然科学研究领域,对具有相关性数据的获取和使用乃是开展符合科学伦理的社会科学研究的必要前提,〔6〕基于绝对的匿名化信息难以获得准确并具有意义的研究结论。〔7〕

欧洲网络与信息安全局在 2015 年发布的报告《大数据中的隐私设计:大数据时代的隐私增强技术概述》(*Privacy by Design in Big Data: An Overview of Privacy Enhancing Technologies in the Era of Big Data*)中提出"过强的匿名化"(too strong anonymization)概念,其认为此种信息匿名化的处理"能够防止将来自不同来源的数据与特定个体(或相似的个体)相关联,但同时亦抑制了大数据的许多潜在益处"。〔8〕 正如欧姆所言,"个人数据或者是有用的或者是被完全匿名化的,但绝不可能二者得兼。"〔9〕匿名化规则注定难以像立法者所期待的那样实现个人信息保护需求和信息利用价值间的有效平衡。

我国的个人信息匿名化规则的缺陷还在于,其意欲通过匿名化处理一刀切地斩断个人信息与信息主体间的所有关联,从而达到一劳永逸的效果。虽然此种想法在逻辑上可能会实现贯通,但实际上却忽视了个人信息处理实践的动态性和变化性特征,无法在信息的后续流转使用过程中实现对信息主体权益和信息安全的充分保护。既有立法均将匿名化处理作为免除信息处理者履行后续个人信息保护义务的法定条件,甚至在相关规范中将匿名化处理和删除信息某种程度上视为功能等同的处理措施。〔10〕 然而,经过匿名化处理的信息仍存在被使用和流转的需要,在此过程中,随着可结合信息来源的不断增加以及信息再识别技术的持续进步,现有的匿名化措施面临着被突破的可能性。个人信息和匿名信息的边界并非固定不变而是往往处于流变状态之中。〔11〕 将匿名化视为一种确定不变的状态,从而彻底免除对匿名信息的规制的做法必然难以充分应对信息处理实践的动态变化所带来的潜在风险。

(二)个人信息匿名化规则的适用障碍

对于何种程度的处理能够使个人信息转化为匿名信息,我国立法亦未形成明确的标准,从而阻碍了这一规则的有效适用和信息处理者对这一规则的严格遵守。最新提交审议的《个人信息保护法(草案)》(二审稿)第 72 条中规定,"匿名化"是指"个人信息经过

〔6〕 See Leslie Stevens, The Proposed Data Protection Regulation and its Potential Impact on Social Sciences Research in the UK, 1 *European Data Protection Law Review* 97, 99 (2015).

〔7〕 See Robert Gellman, The Deidentification Dilemma: A Legislative and Contractual Proposal, 21 *Fordham Intellectual Property, Media and Entertainment Law Journal* 33, 37 (2011).

〔8〕 参见 Giuseppe D' Acquisto et al., *Privacy by Design in Big Data: An Overview of Privacy Enhancing Technologies in the Era of Big Data*, European Union Agency for Cybersecurity (ENISA), 2015, https://www.enisa.europa.eu/news/enisa-news/privacy-by-design-in-big-data-an-overview-of-privacy-enhancing-technologies-in-the-era-of-big-data-analytics,最近访问时间[2021-05-19]。

〔9〕 See Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 *UCLA Law Review* 1701, 1704 (2010).

〔10〕 比如,《个人信息安全规范》中规定了在个人信息超出必要保存期限,或信息处理者停止运营其产品或服务、个人信息主体注销账户等情形下,亦应对信息主体的个人信息进行删除或做匿名化处理。参见《个人信息安全规范》(GB/T 35273—2020)第 6.1 条、第 6.4 条、第 8.5 条。

〔11〕 参见范为:《大数据时代个人信息保护的路径重构》,《环球法律评论》2016 年第 5 期,第 107 页。

处理无法识别特定自然人且不能复原的过程”。然而,其对“无法识别”的认定标准及其指向的主体范围却并未作出明确规定。[12] 根据我国《网络安全法》第76条之规定,“可识别”包括“能够单独或者与其他信息结合识别自然人个人身份”的情形,这一标准主要参考了欧盟《一般数据保护条例》(*General Data Protection Regulation*)中对可识别性个人信息的界定。[13] 《一般数据保护条例》“序言”部分提出,在认定特定信息是否具有可识别性时,应当考虑信息处理者或任何第三人在识别信息主体时可能使用的“所有具有合理可能性的方法”(all the means reasonably likely to be used)以及所有相关的客观因素。[14] 在此基础上,欧盟委员会内部咨询机构“第29条数据保护工作组”在其发布的《关于个人数据概念的意见》(*Article 29 Data Protection Working Party, Opinion 04/2007 on the Concept of Personal Data*)中进一步明确了“合理识别可能性”的判定标准,提出在判定“合理识别可能性”时要综合考虑进行识别的成本、信息处理的目的与具体方式、现有的识别技术及其可能发展,以及信息处理者所采取的组织或技术保护措施失灵的潜在风险等因素。[15] 可见,尽管世界范围内个人信息保护均以“可识别性”为“识别”个人身份的标准,但如何解释此种“可识别性”,却在不同法域的法体系脉络中存在差异,在其各自的实践中被纳入考量的影响因素亦不相同。因而,“可识别性”既是世界范围内讨论个人信息保护的基础,同时也是重要分歧所在。

相比之下,我国立法对“可识别性”并未作出任何具体解释,“无法识别”所应达到的标准也相应地处于较为模糊的状态。个人信息匿名化标准的模糊性为个人信息处理者策略性地适用这一规则以减轻、免除自身负有的个人信息保护义务留下了空隙。在实践中,个人信息处理者普遍在其隐私政策、个人信息保护政策中约定,仅需使个人信息达到令特定的信息接收者无法识别出信息主体的程度,即可在未经信息主体同意的情况下对其进行流转。比如,有的平台隐私政策中即约定:根据法律规定,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复原并重新识别个人信息主体的,不属于个人信息的对外共享、转让及公开披露行为,对此类数据的保存及处理将无需另行向您通知并征得您的同意。上述较为笼统地适用“去标识化”标准而使信息流动的做法,将导致经过处理的个人信息在蕴含较高再识别风险的情况下即可进入流转,进而对信息主体的信息安全造成较大威胁。不容忽视的是,不同信息处理者对匿名化规则所作的不同解释及其采取的不同程度的匿名化处理措施还将导致互联网产业陷入“柠檬市场”:有意遵循个人信息保护规则的企业需要投入昂贵的合规成本进行充分的匿名化处理;相反,游走于规则边缘的企业则无需受到此种束缚。长此以往,必然产生“劣币驱逐良币”的不良后果,引发信息产业的恶性竞争。

个人信息匿名化标准的模糊亦阻碍了司法实践中法院对匿名信息的准确界定。[16]

〔12〕 参见金耀:《个人信息去身份的法理基础与规范重塑》,《法学评论》2017年第3期,第123页。

〔13〕 Article 4 (1) of General Data Protection Regulation.

〔14〕 Recital 26 of General Data Protection Regulation.

〔15〕 See Article 29 Data Protection Working Party, Opinion 04/2007 on the Concept of Personal Data (June 20 2007), p. 13.

〔16〕 See Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 *UCLA Law Review* 1701, 1741 (2009).

比如,在安徽某信息科技有限公司与某(中国)软件有限公司不正当纠纷案〔17〕中,安徽某信息科技公司与某(中国)软件公司围绕某(中国)软件公司抓取并出售的用户浏览、搜索、收藏、加购、交易等行为痕迹信息是否构成个人信息发生了争议。对此,二审法院认定,某(中国)软件公司开发的某数据产品所使用和出售的用户行为痕迹信息经过匿名化处理已经无法识别特定个人且不能复原,公开上述信息不会对用户产生不利影响。而同时法院又指出:“网络用户行为痕迹信息不同于其他非个人信息,这些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。因部分网络用户在网络上留有个人身份信息,其敏感信息容易与特定主体发生对应联系,会暴露其个人隐私或经营秘密”,也即用户行为痕迹信息在与其他信息相结合的情况下仍然可能识别出特定的信息主体,其并未达到匿名化的标准。〔18〕 可见,法院在判定相关信息是否具有“可识别性”,进而判定相关信息以及经一定处理的信息是否属于个人信息等问题时亦比较犹豫,难以作出确定判断。

类似的纠结还体现在上诉人北京某网讯科技有限公司与被上诉人朱某隐私权纠纷案〔19〕中。该案中,朱某认为某网讯公司利用 cookie 技术记录收集其搜索关键词、网络浏览记录等个人信息,构成对其隐私权的侵犯。对此,二审法院认为:某公司在提供个性化推荐服务中运用网络技术收集利用的是未能与网络用户个人身份对应识别的信息,该信息的匿名化特征不符合“个人信息”的可识别性要求。其指出,网络用户通过使用搜索引擎形成的检索关键词一旦与网络用户身份相分离,便无法再确定具体的信息归属主体,并且,某网讯公司“在提供个性化推荐服务中没有且无必要将搜索关键词记录和朱某的个人身份信息联系起来”,因此其收集的信息并不具有可识别性而属于匿名信息。该案中,二审法院将某网讯公司“没有且无必要将搜索关键词记录和朱某的个人身份信息联系起来”作为认定其处理的信息构成匿名信息的依据,这一认识将在一定程度上放纵其对个人信息的不当处理和对个人信息保护义务的逃避。〔20〕 可见,立法上相关概念的不确定性将直接影响司法实践,并对个人信息权益保护存在较多“真空”之处,殊值重视。

二 个人信息匿名化规则的比较法考察

当前,各国立法均未有效破解“匿名化迷思”:个人信息匿名化标准或因过于严苛而难以实现,并产生过度抑制社会、市场对个人信息的利用需求与效率的负效用;或因过于宽松而难以达到充分保障个人信息安全的效果,均未能在个人信息的充分保护和信息资源的高效利用间达致完美平衡。

〔17〕 参见杭州市中级人民法院民事判决书(2018)浙 01 民终 7312 号民事判决书。

〔18〕 《个人信息安全规范》中已明确将“网站浏览记录、软件使用记录、点击记录、收藏列表等个人上网记录”界定为个人信息的类型之一。

〔19〕 参见南京市中级人民法院民事判决书(2014)宁民终字第 5028 号民事判决书。

〔20〕 美国《儿童在线隐私保护法》(*Children's Online Privacy Protection Act*)、欧盟《电子隐私指令》(*Privacy and Electronic Communicationg Directive*)中均明确将 cookie 信息认定为个人信息。

(一)欧盟立法中的个人信息匿名化规则之考察

欧盟基于高度重视人格尊严与人权保护的立法传统,为实现对自然人个人数据的充分保护,对匿名化处理设置了极为严苛的标准。根据“第 29 条数据保护工作组”发布的《关于匿名化技术的意见》(Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques),匿名化处理必须达到使信息处理者和任何第三方主体在使用“所有具有合理可能性的方法”后仍无法识别特定自然人的程度,并且此种处理是无法被撤销的。[21] 此种识别包括三种可能形式:(1)分选(single out),即能够将对应的主体从其所属的群体或种类中挑选出来;(2)联结(linkability),即能够在与同一主体相关的信息间构建起关联,即使无法知晓该主体的确切身份;(3)推断(inference),即能够较为准确地推断出与信息主体对应的相关属性。[22] 只要仍存在上述任何一种可能,即视为该信息并未达到匿名化的效果。在判断经过处理后的信息是否达到匿名化标准时,信息处理者必须考虑到所有可能被合理地使用以复原匿名信息的方法,并评估此种方法涉及的成本和相应知识产权问题,以衡量其被用于对匿名信息进行复原的可能性和所引发结果的严重性。在主体层面,欧盟立法要求信息处理者在进行匿名化处理时应考虑信息处理者本人和任何其他主体对匿名化信息进行复原的可能。[23] 此种规定将所有人均视为具有对匿名信息进行再识别意图的“积极侵权人”(motivated intruder),并要求信息处理者必须对每个潜在的“积极侵权人”所可能采用的再识别方法和结合的信息进行预判,当任何一位“积极侵权人”存在成功地再识别出信息主体的可能时,此种信息即被认定为未达到匿名化标准而仍需受到个人信息保护立法的约束。[24]

欧盟立法向匿名化处理者配置了一种持续性的评估义务,要求其对待匿名信息不得“释放并遗忘”(release and forget)。信息处理者必须经常性地识别新产生的风险,并对匿名信息的剩余识别风险进行再评估,从而衡量自身采取的控制措施是否足以应对新产生的风险,并及时进行必要的调整。[25] 信息处理者还需考虑匿名信息被用于与其他个人信息进行结合比对以实现再识别目的的可能,其必须时刻关注可能被用于结合以进行再识别的新的信息来源。上述要求导致信息处理者承担了极为严苛的合规负担,个人信息匿名化规则并未提供给其一劳永逸的护避风港,相反,悬挂在信息处理者头顶的“达摩克利斯之剑”随时可能落下。立法规定匿名化规则的本来目的在于免除信息处理者在使用、流转与自然人相关的信息时所受的限制,减轻其在信息处理方面的合规负担,然而其现实效果却是,信息处理者为确保信息的匿名化状态和应对再识别风险所需付出的成本和精

---

〔21〕 See Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques (April 10 2014), p. 5.

〔22〕 See Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques (April 10 2014), pp. 11 – 12.

〔23〕 See Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques (April 10 2014), pp. 9 – 10.

〔24〕 See Information. Commisioner's Office, Code of Practice for The sharing of Personal Information, https://ico. org. uk/media/1068/data – sharing code of practice. pdf. ,最近访问时间[2021 – 01 – 27]。

〔25〕 See Article 29 Data Protection Working Party, Opinion 04/2007 on the Concept of Personal Data (June 20 2007), pp. 24 – 25.

力可能已经超出其在履行个人信息保护义务方面原本承受的压力与责任。

为了防止信息处理者通过采取不完善的匿名化处理手段以逃避遵守《一般数据保护条例》等相关制度,欧盟立法还专门对“假名信息”与“匿名信息”的概念进行了区分。欧盟委员会副主席露丁(Viviane Reding)在公开发言时曾明确表示,欧盟应当警惕数据企业将“假名信息”概念作为逃避适用《一般数据保护条例》的“特洛伊木马”。[26] 但在现实中,“假名信息”和“匿名信息”的界限常常模糊不清。并且,将假名信息均视为个人信息还将对现有科学研究活动的正常开展造成严重阻碍。政府收集和开放的经过一定程度去标识化处理的公共数据(de-identified administrative data)一直是欧盟范围内学术研究工作者用以开展社会科学研究的重要原材料。在此基础上,政府部门和学术研究机构已经形成了极为规范、全面的信息利用机制。[27] 而《一般数据保护条例》关于假名信息处理仍需受到个人信息保护制度严格拘束的要求将直接打乱当前科研活动中形成的一系列制度、技术和组织安排,进而抑制欧盟范围内社会科学研究活动的效率。

(二)美国立法中的个人信息去标识化规则之考察

相比于欧盟,美国立法对个人信息流转持较为开放的态度。为促进信息流转,部分立法采纳了去标识化规则作为免除适用个人信息保护规则的条件,并对个人信息去标识化所需达到的标准作出了较为宽松的要求。这与美国立法对个人信息的限缩主义界定模式存在直接关系。不同于欧盟立法对个人信息进行尽可能宽泛的界定,以确保将所有与个人有关的信息均囊括进立法规制范畴,[28] 美国立法者和政府基于扶持和发展数据产业的战略目标以及对言论自由等价值的重视和考量,从不同角度对个人信息作出了较为限缩的界定。[29] 许多立法均对个人信息采取列举式定义,比如,美国《儿童在线隐私保护法案》(*Children's Online Privacy Protection Act of 1998*)中将个人信息界定为“在线收集的个人可识别性信息,包括姓名、家庭或其他地址、邮箱地址、电话号码、社会保障号码以及委员会决定的能够现实或在线上联络到特定个人的任何其他标识符”,[30] 从而将未经委员会决定的其他类型信息均排除至调整范围以外。部分立法还排除了对与个人有关的“公开可得信息(publicly available information)”的规制。[31] 与之相对,去标识化处理仅需达到使特定信息不再构成上述立法所规定的个人信息的程度即可。同时,美国的个人信息保护制度允许信息处理者在采取去标识化措施方面享有较大的裁量自由,只要信息处理者“并不实际知悉经过处理后的信息可以单独或与其他信息相结合用于识别信息主体”且“没有合理理由相信该信息可被用于识别特定个体”,即视为已满足去标识化要求,由此

〔26〕 See Press Release, Viviane Reding, Vice-President of the European Commission, EU Data Protection Rules: Better for Business, Better for Citizens, http://europa.eu/rapid/press-release_SPEECH-13-269_en.htm,最近访问时间[2021-01-30]。

〔27〕 See Leslie Stevens, The Proposed Data Protection Regulation and its Potential Impact on Social Sciences Research in the UK, 1 *European Data Protection Law Review* 97, 98 (2015).

〔28〕 See COM (92) 422 final, 28.10.1992, p.10.

〔29〕 See Danie J. Solove & Paul M. Schwartz, Reconciling Personal Information in the United States and European Union, 102 *California Law Review* 877, 887-891 (2014).

〔30〕 See Children's Online Privacy Protection Act of 1998, 15 U.S.C. §6501 (8) (2006).

〔31〕 See Gramm-Leach-Bliley Act of 1999, 15 U.S.C. §6809 (4) (a) (b) (2006).

使信息处理者不至背负过于沉重的合规负担。

此外,美国立法为信息处理者进行去标识化处理提供了一定规则指引。以美国《健康保险携带和问责法》(*Health Insurance portability and Accountability Act of 1996*)为例,其规定了两种用于确定去标识化信息的具体标准:一是统计法(statistical standard),即通过统计人员或具备合理知识和经验的专家进行判断,以确定信息处理者所采取的去标识化措施是否已达到使个人信息"不能识别并且没有合理理由相信可以被用于识别特定个体"的程度,从而决定其是否可以免除适用相关立法规定;二是安全港标准(safe harbor standard),《健康保险携带与问责法》中列举了姓名、地址、电话号码、电子邮箱地址、证件号码、银行账户号码等18项识别符,信息处理者在确保完全消除上述识别符且并不实际知悉该信息可以单独或与其他信息相结合用于识别信息主体时,即被视为已达到去标识化的效果。[32] 上述规则具有较强的可操作性,能够为信息处理者评估其对个人信息的处理合规提供明确、稳定的预期,但潜在缺陷在于,其对去标识化标准的要求难以达到充分消除信息安全风险的程度。事实上,统计法对去标识化处理所应达到的具体标准的规定缺失可能导致信息处理者与技术专家间形成寻租和共谋,进而影响相应决定的公平性和可信赖性;而安全港标准所列举的18种标识符并不构成对现实中存在的能够识别信息主体身份之信息的完全列举。已有实验证明,去除18种标识符后的个人信息在与美国选民登记记录进行交叉比对后即有0.04%的几率重新识别出其指向的信息主体,更遑论与更多信息结合后的效果。[33]

在意识到经过去标识化处理后的信息可能仍残存有一定安全风险的基础上,部分立法进一步规定了信息处理者及后续使用者负有的禁止再识别义务。比如,《消费者隐私权利保护法案》(*Consumer Privacy Bill of Rights Act*)中即规定,信息处理者在具有合理的依据相信经过去标识化处理的信息事实上已不能够再关联到特定的个人的情况下,还须公开承诺其不会对经过去标识化处理的信息进行再识别的尝试,并以合同或其他具有法律约束力的形式禁止信息接收方对此类信息进行再识别,同时要求第三方对此作出公开承诺,如此方可对经过去标识化的信息进行共享或转让。《健康保险携带与问责法》中还规定了在信息处理者与信息接收方签订具有约束力的协议要求其不得从事再识别行为的前提下,其可以使用或向他人提供仅删除16种标识符的有限数据集,[34] 其目的在于适度保留经过去标识化处理的信息所具有的应用价值。信息的本质是关于特定事物或个人之现象和本质的记录和表达,其通过作用于人类的认知使人们形成对特定事物或个人的理解,由此决定接受者对该事物或个人的态度及采取的行动。[35] 而去除所有标识符的信息在失去识别信息主体能力的同时也不再能够传达出任何具有意义的知识。

---

〔32〕 See 45 C. F. R. §164.514 (b) (1) (2009).

〔33〕 See National Committee on Vital and Healgh Statistics, Enhanced Protections for Uses of Health Data: A Stewardship Framework for "Secondary Uses" of Electronically Collected and Transmitted Health Data, http://www.ncvhs.hhs.gov/071221lt.pdf.,最近访问时间[2021-02-06]。

〔34〕 See 45 C. F. R. §164.514 (b) (2) (2009).

〔35〕 参见谢远扬:《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》,《清华法学》2015年第3期,第97-98页。

(三)小结

欧盟和美国立法对匿名化或去标识化标准的设定均未能够达到有效平衡信息保护和信息利用需求的效果。欧盟个人信息保护规则对匿名化处理所应达到的标准设置了过于严苛的要求,匿名化处理者不仅需要保证自身无法对匿名信息进行再识别,还需达到使任何第三方主体均无法对该信息进行再识别的程度,其中囊括了因遭受恶意攻击导致相关信息泄露的情形。此种制度设计导致匿名化处理者对匿名信息的安全负有一种严格责任,进而可能造成信息处理者弃用匿名化规则,最终可能会摧毁这一制度存在的必要性基础。同时,欧盟立法中规定的匿名化标准又极为模糊而欠缺可操作性,其对如何判定个人信息是否达到匿名化的程度规定了过多的考量因素,且这些因素必须置于个案中进行综合考量和判断,尤其是这些标准难以为信息处理者在从事个人信息处理活动时提供明确的事前行为指引,由此进一步加剧了匿名化规则的适用障碍。

与之相反,美国立法基于确保信息资源自由流通和高效利用的价值追求,对个人信息去标识化的标准作出了较宽松的规定,其规定的去标识化操作在去除个人信息识别能力方面较为孱弱,由此导致经过处理的个人信息仍存有较为显著的剩余风险。此外,美国立法中规定的禁止再识别义务仅能约束存在合同关系的信息转让者和信息接收者,却无法预防第三方主体对信息的再识别行为。上述问题导致美国立法在个人信息保护力度上有所不足,使其长期遭受欧盟数据保护机构的质疑,并影响了二者在个人信息流通方面合作的稳定。[36] 美国互联网企业近年来亦屡因未能充分履行个人信息保护义务而引发大规模信息泄露事件,从而遭到欧盟数据监管执法机构的严厉处罚。其均暴露出美国立法在个人信息去标识化规则标准的设置等问题上存在过度放纵个人信息安全风险的弊端。

欧美立法的上述问题曝光了个人信息匿名化(去标识化)规则所面临的尴尬处境,亦揭示出个人信息保护和信息资源利用间的内在抵牾。“匿名化迷思”的根源在于,其试图通过对理想的匿名化(去标识化)标准的事前界定以对信息性质作出“非此即彼”的判断,此种努力在信息智能时代注定难以实现。这督促我国立法应积极寻求更为可行的替代方案,以实现《个人信息保护法(草案)》(二审稿)第 1 条所规定的“保护个人信息权益”和“促进个人信息合理利用”的立法目标的兼顾。

三 个人信息匿名化规则的替代方案及体系调整

鉴于各国在确立能够充分保护个人信息权益并具有现实可操作性的匿名化(去标识化)标准方面的失败,有学者断言,匿名化已经沦为对个人信息保护的“破碎承诺”。[37] 个人信息匿名化规则的静态取向与个人信息处理实践的动态风格间的格格不入决定了其

〔36〕 See Paul M. Schwartz, The EU-U. S. Privacy Collision: A Turn to Institutions and Procedures, 126 *Harvard Law Review* 1966, 1967 – 1968 (2012).

〔37〕 See Paul M. Schwartz & Daniel J. Solove, The PII Problem: Privacy and a New Concept of Personally Identifiable Information, 86 *New York University Law Review* 1814, 1847 (2011).

难以达成立法者的愿景。在放弃这一注定难以实现的努力的同时，必须为其寻求更加妥适的替代方案，重塑个人信息保护与利用的平衡。目前，我国个人信息保护立法尚未形成对匿名化规则的高度倚赖，此时如果能够寻求更优的个人信息保护制度方案，有助于发挥我国立法在世界范围内个人信息保护立法的后发优势，并有效节约在个人信息保护立法方面的探索与试错成本。

（一）从“一体规制”到“区别规制”

当前，我国个人信息保护立法对所有个人信息均采取了同等程度的严格规制，[38]此种“一体主义”的规制模式对个人信息的收集、使用和流转设置了极为严格的限制，在一定程度上违背了利益平衡和比例原则的法理，亦有违我国社会在公民信息隐私保护方面的主流价值取向。事实上，我国的社会结构、伦理观念及立法传统等因素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明显差异。我国立法较为强调信息隐私的“社会功能”和保护个人信息隐私对推进社会发展、维护社会秩序的作用，对个人信息隐私的保护必须受到社会和国家整体利益的限制。信息隐私主要被视为一种工具价值而非本质价值予以保护，其必须被置于利益衡量的背景下决定能否受到保护以及所受保护的程度。而当前个人信息保护制度的“一体主义”规制模式有违利益衡量的法理，进而导致其在现实中未能得到严格遵循。[39] 此种“一体主义”的规制模式未能为信息处理者采取相应技术措施以降低个人信息具有的识别能力，从而减少因信息泄露或不当处理所造成的安全风险提供充分激励，结果不仅难以达到个人信息保护立法所追求的充分保护信息主体权益的效果，还可能导致实践中信息处理者为节省合规成本，而一味借助在形式上征得信息主体同意的方式以免除自身负有的责任。在当前信息主体“知情同意”流于形式的整体背景下，此种选择可能进一步降低对信息主体权益的保护水平。[40]

不同的个人信息所具有的识别能力不同，与信息主体的关联程度不同，当其被不当处理和流转时对信息主体个人权益产生的风险亦不相同。因此，对其相应的保护要求和信息收集、利用行为的限制程度亦应有所不同。近年来，各国立法者和学者均逐渐意识到个人信息在识别能力上的差异对相应个人信息规制规则设计具有的影响。

美国隐私法学者施瓦茨和索罗夫提出了所谓的“PII 2.0 方案”，主张应根据信息具有的不同识别能力分别决定对应的信息处理行为所需受到的法律限制。[41] 欧盟《一般数据保护条例》中也规定，在信息处理者不能直接识别自然人身份且无意于进行此种识别时，其可告知信息主体，并不再受到《一般数据保护条例》第 15－20 条规定的约束，除非信息主体通过提供额外的信息而使信息处理者能够对其身份进行直接识别。[42] 我国亦有学者主张，间接识别性个人信息只有在与其他个人信息相结合的情况下方可指向特定的信

〔38〕 参见齐爱民著：《拯救信息社会中的人格——个人信息保护法总论》，北京大学出版社 2009 年版，第 101－102 页。

〔39〕 参见齐英程：《论间接识别性个人信息规制规则的重构》，载梁慧星主编《民商法论丛》第 71 卷，第 295－297 页。

〔40〕 See Omer Tene and Jules Polonetsky, Big Data for All: Privacy and User Control in the Age of Analytics, 11 *Northwestern Journal of Technology and Intellectual Property* 239, 261 (2013).

〔41〕 See Paul M. Schwartz and Danie J. Solove, Reconciling Personal Information in the United States and European Union, 102 *California Law Review* 877, 904－912 (2014).

〔42〕 Article 11 (2) of General Data Protection Regulation.

息主体,对于此类信息的处理往往不会对信息主体造成明显的压迫和紧张感,即使其被不慎泄露,对信息主体人格、财产利益的威胁也明显较轻,[43] 因此,立法应适度放松对此类信息使用和流转的束缚。[44] 上述主张均认同对具有较低识别能力的个人信息应采取更加宽松的规制措施,并相应地降低甚至免除信息处理者负有的个人信息保护义务。基于此种考量,未来我国个人信息保护立法应从当前的一体规制模式转向基于信息识别能力类型化的区别规制模式,根据不同类型的个人信息具有的不同程度识别能力构建起层次化的个人信息保护义务规则体系,形成对既有个人信息匿名化规则的替代选择。

2021 年 4 月发布的《个人信息去标识化效果分级评估规范》(征求意见稿)对个人信息的分类问题作出了有益尝试。其基于个人信息的去识别化程度将其分为四类:(1)能直接识别信息主体的信息;(2)已消除直接标识符,但仍具有较高再识别风险的信息;(3)已消除直接标识符,且再识别风险可接受的信息,此类信息的再识别风险应低于 0.05 这一阈值;(4)聚合信息,即对个人信息进行汇总分析得出的整体层面的聚合数据。同时规定了在衡量针对特定信息的再识别风险时需要考虑的主要因素,包括信息类型、信息流转的范围、信息处理者采取的隐私和安全控制水平以及信息接收者的再识别动机与能力等。此种分类模式基于经过去标识化处理后的信息残留的识别能力和再识别风险对其进行层次化分类,为个人信息保护立法根据不同信息蕴含的安全风险对其采取相应的规制和保护措施提供了基础,有助于扭转当前一体规制模式过度限制信息流转与使用的弊端。

本文认为,未来我国个人信息保护立法可在一定程度上吸纳《个人信息去标识化效果分级评估规范》(征求意见稿)中确定的个人信息识别标准类型化的思路,根据个人信息具有的识别能力将其划分为直接识别性个人信息和间接识别性个人信息,并根据间接识别性个人信息具有的识别能力是否超过特定阈值将其进一步划分为识别能力高于阈值的间接识别性个人信息和识别能力低于阈值的间接识别性个人信息。在此基础上,采取“区别规制”的立法策略,针对不同类型个人信息蕴含的识别能力和安全风险,分别为其设置不同程度的个人信息保护义务,从而构建起层次化的个人信息保护义务体系。

(二)以信息识别能力为核心构建起层次化的个人信息保护义务体系

根据区别规制的立法策略,应对不同类型个人信息对应的个人信息保护义务作出差异化安排。其中,对于直接识别性个人信息,因其与信息主体间存在直接对应关系,立法仍应严格约束对此种信息的收集、分析、使用及流转,要求信息处理者全面履行各项个人信息保护义务。而对于已消除直接标识符的间接识别性个人信息,则应降低并部分免除

〔43〕 参见项定宜、申建平:《个人信息商业利用同意要件研究——以个人信息类型化为视角》,《北方法学》2017 年第 5 期,第 35 页。

〔44〕 还有学者提出,应当对“个人信息”和“个人数据”进行区分,个人信息强调可直接识别性,即可以直接识别出某一特定个人的信息;个人数据则泛指一切与个人有关的数据,不强调直接可识别性。间接识别性个人信息不属于个人信息而应属于个人数据。对于个人数据,商家可以自由收集且无需事先征得同意。参见邢会强:《大数据交易背景下个人信息财产权的分配与实现机制》,《法学评论》2019 年第 6 期,第 100 页,注释 12。

信息处理者对其负有的义务以及其在处理此类信息时受到的约束。比如,对于间接识别性个人信息的处理原则上无需受到目的限制原则、最小化原则等约束,且应免除适用个人信息保护立法关于个人信息查询权、更正权、删除权等规定。这不仅有助于减轻个人信息处理者的合规负担,促进信息资源的高效使用,同时亦有利于避免在信息主体和间接识别性个人信息间建立直接联系而增加暴露其身份和隐私的风险。[45] 同时,个人信息处理者虽然仍需对间接识别性个人信息承担其他法律规定的个人信息保护义务,但其在履行此种义务的过程中需要采取的具体技术措施和组织措施,以及应达到的审慎程度相比于直接识别性个人信息均应适度降低。

此外,对识别能力低于一定阈值的间接识别性个人信息,还应允许个人信息处理者在采取必要手段确保其不会被用于识别或关联信息主体的前提下对其进行流转,而无须征得信息主体的同意。目前,《个人信息保护法(草案)》(二审稿)第 24 条规定了个人信息处理者向第三方提供其处理的个人信息,必须通知并取得信息主体的单独同意。这一规定可能造成过度限制信息流转效率的结果。不同于"前信息时代"的传统经济形态,数字经济不再关注用于建立因果关系或内在逻辑的小样本数据,其关注的是海量信息汇集、整合、加工而成的"大数据"。而如若要求信息处理者在共享、转让蕴含海量信息的"大数据"前逐一征询相关主体的授权同意,必然会产生极为高昂的运作成本,当此种运作成本高于个人信息处理能够产生的收益时,原本有价值的信息处理行为就不会发生。并且,赋予自然人对其个人信息共享、转让的一般性决定权还可能诱发信息主体基于不合作策略而索取高价的行为。[46] 信息主体可能采取僵持策略以索取高价,从而显著增加交易成本并阻碍个人信息共享、转让的顺利进行。基于此,对于识别能力低于一定阈值的间接识别性个人信息,应允许信息处理者在未征得信息主体同意的情况下对其进行转让,同时为此种场合下的个人信息处理者设置持续性的个人信息保护义务和责任,以消弭此类信息在流转过程中对信息主体造成的潜在风险。

在此基础上,我国个人信息保护立法应放弃在确定匿名化标准方面的努力,规定经过去标识化处理使其识别能力低于特定阈值的信息仍属于个人信息的范畴,信息处理者仍应对其履行适当的个人信息保护义务。在大数据时代,数字技术的急速发展、信息来源的广泛分布决定了即使仅具有微小识别可能性的个人信息在与其他信息充分结合的情况下,仍可能重新识别出信息主体的身份,完全免除信息处理者对匿名化信息的保护义务并不合理。

同时,匿名化处理的结果具有极强的不确定性,其究竟是否达到使特定信息彻底丧失识别能力的程度通常难以判定。鉴于个人信息侵权行为通常具有的隐蔽性以及相关损失的非直接性、偶发性和累积性等特点,[47] 即使匿名信息事后被用于成功地对信息主体进

〔45〕 See Paul M. Schwartz and Danie J. Solove, Reconciling Personal Information in the United States and European Union, 102 *California Law Review* 877, 909 (2014).

〔46〕 See Christina Aperjis, Bernardo A. Huberman, A Market for Unbiased Private Data: Paying Individuals According to Their Privacy Attitudes, 17 *First Monday* 1, 1 - 5 (2012).

〔47〕 See Clara Kim, Granting Standing in Data Breach Cases: The Seventh Circuit Paves the Way Towards a Solution to the Increasingly Pervasive Data Breach Problem, 2 *Columbia Business Law Review* 544, 587 - 591 (2016).

行再识别,亦很难发现并证明侵权行为与匿名信息之间存在直接的因果关系,此种结果导向的个人信息保护规则在实现个人信息权益保护方面的效果难以评估。[48] 因此,相比于继续沉溺于对匿名化处理之应然标准的纠结,个人信息保护立法更应将注意力转移至对个人信息处理过程的规制,其必须抛弃对信息的绝对安全状态所持有的幻想,适度容忍因信息流动与使用所产生的风险,并通过规定个人信息处理者适当的后续保护义务,以将此类信息流转产生的风险持续控制在可接受的范围之内。

对于经过去标识化处理已达到使其识别能力低于阈值的个人信息,信息处理者仍应履行必要的程序性保护义务。个人信息处理者应建立相应的个人信息安全影响评估机制以评估对此类信息进行处理所存在的安全风险,如个人信息流转对信息主体合法权益的可能影响、信息接收者采取的个人信息安全保护措施的有效性、信息接收者违反约定对个人信息进行再识别的潜在可能及其识别能力等,从而采取与风险水平相匹配的信息安全控制和保护措施并及时进行必要调整。[49] 同时,其应对此类信息的流转情况进行记录,包括处理个人信息的具体类型、数量、来源,具体的信息处理操作,以确保当发生信息泄露或恶意攻击等情况时能够及时采取相应的应对措施,并对信息主体进行风险提示。此外,信息处理者还应对信息接收方存储、使用、流转个人信息的情况进行适当监督,并要求其提供不低于自身同等水平的个人信息保护措施。[50]

(三)引入不得从事再识别行为的法律义务

降低对识别能力低于阈值的间接识别性个人信息的流转限制意味着个人信息处理者无需使经过处理的个人信息达到使任何第三方主体在使用“所有具有合理可能性的方法”后仍无法识别特定自然人且不能复原的程度,即可对其进行流转。如若允许经过处理的个人信息保有一定的识别能力,必然将在一定程度上降低对个人信息权益的保护力度。对此,我国立法还应规定个人信息处理者不得从事再识别行为的法律义务,并明确规定个人信息处理者在相关情况下负有的法律责任,以补强对个人信息权益的保护力度。

再识别是指将经过去标识化处理的个人信息与其他信息相结合以重新识别信息主体的过程,这一过程因涉及对间接识别性个人信息的处理而当然构成个人信息处理行为,从而应当受到个人信息保护立法的规制。当前实践中,不少个人信息处理者存在未经信息主体同意而将经过去标识化处理的个人信息提供给有合作关系的第三方使用的情况,且并未禁止第三方将此种信息与其他合法获取的信息相结合。此种信息处理实践将给信息主体的合法权益带来较为显著的风险,第三方使用者在未经信息主体同意的情况下肆意对去标识化信息进行再识别,可能对信息主体形成密集的追踪,从而对其个人隐私与生活安宁造成严重侵扰。针对此种情况,个人信息保护立法应当明确在未经信息主体和信息处理者同意的情况下,下游信息使用者不得将经过去标识化处理的间接识别性个人信息用于对信息主体身份进行再识别,否则即构成对直接识别性个人信息的处理,并仍需遵循

〔48〕 See Ira S. Rubinstein, Woodrow Hartzog, Anonymization and Risk, 91 *Washington Law Review* 703, 730 (2016).

〔49〕 参见《个人信息安全影响评估指南》(GB/T 39335 - 2020)。

〔50〕 参见周汉华:《探索激励相容的个人数据治理之道——中国个人信息保护法的立法方向》,《法学研究》2018 年第 2 期,第 19 页。

个人信息保护法对直接识别性个人信息的规制规定。

信息处理者在未经信息主体同意而对识别能力低于阈值的间接识别性个人信息进行流转时，应告知信息主体信息接收方的身份、联系方式、处理目的、处理方式和其处理的个人信息的种类，以保证信息主体在遭受侵害时可以及时发现并主张权利。此外，其必须确保经过处理的信息已达到使特定信息接收方无法识别信息主体身份的程度，同时以协议等形式要求信息接收者承诺不会将个人信息用于识别信息主体的身份或联络信息主体，并约定相应的违约责任。由于信息处理者和信息接收者间的此种协议关系到所涉信息主体的权益，信息处理者应当以适宜的方式对此种协议进行公示，并接受相关信息主体和监管机构的监督。此种协议类似于个人信息保护政策，具有市场自律规则的性质，当信息接收者违反协议约定时，监管机构即可据此对其进行处罚。[51] 同样，当信息接收者基于其取得的间接识别性个人信息对信息主体真实身份进行再识别从而向其进行定向营销等行为时，信息主体亦可向信息处理者或监管机构进行投诉。信息处理者应对信息接收者的后续信息处理行为进行必要监督，其因怠于履行监督义务导致信息主体遭受侵害时，应与信息接收者共同承担责任。在信息处理者明知或应知信息接收者从事再识别行为而不予制止的情况下，二者构成《个人信息保护法（草案）》（二审稿）第 21 条规定的“共同处理个人信息”的情形，应对侵害个人信息权益所造成的损失承担连带责任。

上述措施只能约束与信息处理者具有直接联系的下游信息使用者的再识别行为，而无法有效应对第三方主体以恶意攻击、窃取等手段所从事的再识别行为。第三方主体从事再识别行为的目的往往在于破解自然人的相关信息以用于非法交易或从事违法犯罪活动等，对此，可通过刑法手段对此类行为予以制裁。比如，英国《数据保护法案》（*Data Protection HL Bill*）中即规定，在未经信息处理者同意的情况下对经过去标识化处理的信息进行再识别的行为构成刑事犯罪。[52] 鉴于第三方主体在实施个人信息再识别行为时，通常均需以恶意攻击计算机系统、非法获取计算机信息系统中存储的数据为前提，此种行为符合《刑法》第 285 条、第 286 条规定的“非法获取计算机信息系统数据罪”和“破坏计算机信息系统罪”的罪状；而通过购买等方式非法获取间接识别性个人信息以进行再识别的行为还可能触犯《刑法》关于“侵犯公民个人信息罪”的规定，因此，可以依托上述规定对恶意再识别行为进行必要规制，从而在风险来源层面遏制对个人信息权益的潜在威胁，在将信息处理者从确保任何第三方主体均无法重新识别信息主体这一不可能完成的任务中解脱出来的同时，实现对信息安全风险的必要控制。

四　结　语

个人信息匿名化规则假定通过匿名化处理这一技术手段可以彻底消除个人信息具有

〔51〕 参见王叶刚：《网络隐私政策法律调整与个人信息保护：美国实践及其启示》，《环球法律评论》2020 年第 2 期，第 152 页。

〔52〕 See Data Protection HL Bill (2017 - 19) 66, cl 162.

的识别能力。然而,在信息智能时代,绝对不具有识别能力的信息仅存在于想象之中,随着数据分析处理技术的发展,经过匿名化处理的个人信息在与其他来源信息充分结合的情况下可能再次识别出信息主体的身份。个人信息具有的识别能力往往并非处于全有或全无的状态,而更类似于一个连续的频谱:在识别能力最强的一端是具有直接识别性的个人信息,另一端则是几乎不具有任何识别能力的个人信息。〔53〕 同时,此种识别能力还将伴随个人信息处理实践的动态发展而不断发生变化。上述特点决定了个人信息保护立法不应过度追求对个人信息与非个人信息作出静态区分,而更应强调对特定信息蕴含的识别能力及安全风险的动态把握。未来的个人信息保护立法应区分不同个人信息在识别能力上的差异而对其采取区别规制的策略,激励信息处理者尽可能采取降低个人信息识别能力的措施以换取信息流通效率;同时,其应规定个人信息处理者应承担持续性的个人信息保护义务,并根据个人信息处理者是否履行了与信息风险相适应的信息保护义务决定其责任承担。相比于个人信息匿名化规则,此种过程导向的个人信息保护制度更加契合个人信息处理实践的动态性特征,且能为调控各方主体间的利益冲突提供更加富有弹性的制度空间,有望真正实现信息主体、信息处理者和下游信息使用者的利益平衡与合作共赢。

［**Abstract**］ The rule of anonymization tries to free information processors from their obligations of personal information protection by completely eliminating the possibility of identification contained in personal information. However, it is faced with difficulties in theory and obstacles in application. The root of the so-called the "myth of anonymization" lies in the fact that the rule aims to make an either-or judgment on the nature of information and a "one-size-fits-all" decision on whether to thoroughly cut off the obligations of personal information processors. In reality, however, the identifiability of personal information is usually not an all-or-nothing relationship, but shows different degrees of identifiability. Considering the remaining risks it contains, it is unreasonable to completely exclude the anonymized information from the application scope of personal information protection legislation. In the future, China should transform the personal information protection legislation from the current integral regulatory model to a differentiated regulatory model based on the categorization of identifiability of information, construct a multi-layered system of information protection obligations based on the identifiability contained in specific kinds of personal information, and treat the anonymized information as a kind of personal information with low level of identifiability, so as to achieve a dynamic balance between the protection and utilization of personal in formation.

（责任编辑:姚　佳）

〔53〕 See Paul M. Schwartz and Danie J. Solove, Reconciling Personal Information in the United States and European Union, 102 *California Law Review* 877, 905 (2014).