DOI: 10.16494/j.cnki.1002-3933.2020.09.004

个人信息保护中的“识别”要素研究

程德理,赵丽丽

(同济大学 上海国际知识产权学院,上海 200092)

摘 要: 个人信息的界定中多将“识别”要素纳入个人信息的构成要件。作为个人信息的核心要素,“识别”的内涵界定决定了个人信息立法的保护范围与强度,进而涉及多方利益的平衡,需要根据经济社会发展状况科学界定与解释。正确理解“识别”这一要素将对我国正在进行的个人信息保护立法及司法产生较大影响。目前我国在个人信息“识别”要素的解释方面仍具有不同的观点。在研究欧盟《通用数据保护条例》个人数据内涵的基础上,结合我国经济发展的实际情况,提出了用狭义解释界定“识别”要素及采用“与特定人事实上相连接”限定识别范围的建议。

关键词: 个人信息; 识别; 关联; 保护范围; 利益平衡

中图分类号: DF36 **文献标识码**: A **文章编号**: 1002-3933(2020)09-0044-11

The Research on the Identification Element of the Concept of Personal Information

CHENG De-li, ZHAO Li-li

(Shanghai International College of Intellectual Property, Tongji University, Shanghai 200092, China)

Abstract: In the definition of personal information, the “identification” element is often incorporated into the constituent elements of personal information. As the core element of personal information, the definition of the “identification” element

收稿日期: 2020-06-04 该文已由“中国知网”(www.cnki.net) 2020年7月21日数字出版,全球发行

基金项目: 教育部人文社会科学研究项目《我国知识产权密集型产业集群国际竞争力提升研究》(19YJA630012)阶段性研究成果

作者简介: 程德理(1972-),男,安徽阜南人,同济大学上海国际知识产权学院教授,研究方向: 知识产权与竞争法;

赵丽丽(1995-),女,安徽亳州人,同济大学上海国际知识产权学院研究生。

determines the scope and intensity of the protection of the personal information protection law, and thus involves the balance of interests of multiple parties. It needs to be scientifically defined and interpreted according to the economic and social development status. At present, China still has different views on the interpretation of the "identification" element. China is at a critical period of personal information legislation. Based on the study of the content of personal data in the EU's General Data Protection Regulation and the actual situation of China's economic development, the article proposes such suggestions as narrowing definition of "identification" elements and using "specifically associated with a specific person" element to delimit the identification element.

Key words: personal information; identification; association; protection scope; balance of interests

一、问题的提出

个人信息具有"识别"与"记录"两个要素,前者为实质要素,后者为形式要素[1]。在个人信息立法实践中,"识别"要素又有"直接识别"和"间接识别"之分。"直接识别"指无需借助其他信息就可以识别出特定个人的信息,如身份证号、指纹信息等;"间接识别"则需要与其他信息结合方能识别出特定个人,如血型、居住地址等。我国法律法规大多将"识别"要素作为个人信息的判断标准之一。如全国人民代表大会颁布的《中华人民共和国网络安全法》第76条第5款:"个人信息,是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息,包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。"工业和信息化部发布的《电信和互联网用户个人信息保护规定》、国家市场监督管理总局和中国国家标准化管理委员会发布的《信息安全技术个人信息安全规范》、全国信息安全标准化技术委员会发布的《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》、公安部颁布的《互联网个人信息安全保护指南》等都引入"识别"要素界定个人信息。对于用"识别"要素界定个人信息有不同的观点。一种观点认为,"识别"要素应作广义解释。他们认为,技术的发展使得"可识别"与"不可识别"的边界越来越狭窄,为了应对技术对个人信息的冲击,"识别"要素可以从信息内容、目的或者结果相关联情况来界定,即这三种情况任一因素与特定主体相关即可视为个人信息[2]。并指出,"宽进严控"是大数据时代定义个人信息的新趋势,应该对"识别"进行最宽泛的界定,如可以学习欧盟Breyer案件那样采用"识别"的绝对路径。即只要信息被世界上某机构所获得,无论该机构能否真正识别该信息,都视为"可识别"[3]。另一种观点认为个人信息应作狭义解释,认为如果过度仿照欧美国家的制度,对中小企业施以更加严格的义务,会加重中小企业的责任和义务,从而不利其发展[4]。"识别"要素的外延有多大?对"识别"要素采取广义解释还是狭义解释?目前学界尚无定论。

司法实践方面,国内外近年来不乏用"识别"来认定个人信息的案件。典型的案件如北

京百度网讯科技有限公司与朱烨隐私权纠纷上诉案，该案采用了个人信息的“直接识别”标准：百度公司搜集的信息仅识别到浏览器设备而非个人，故不属于个人信息①。该案判决与国内部分学者主张的对“识别”边界进行最宽泛认定观点相左。欧盟 *Patrick Breyer* 诉 *Federal Republic of Germany* 案件对“识别”要素的认定采用了与我国上述案件截然不同的做法：虽然动态 IP 地址不能直接识别到个人，但是其也可能通过其他渠道“识别”到个人从而构成个人信息②。未来我国个人信息保护的司法实践中，究竟是坚持百度与朱烨案件的“直接识别”标准，还是上述 Breyer 案件“绝对路径”的做法值得探讨。2020 年我国将制定个人信息保护法，个人信息保护将以单行法的形式步入一个新的台阶。“识别”要素边界的厘清关系到界定“个人信息”的内涵和外延，并对今后的法律适用产生较大影响。因此，需要对此进行进一步探讨。

二、国内外立法中个人信息的“识别”要素分析

（一）立法中的个人数据与个人信息的区别

“识别”的客体是个人信息还是个人数据，即个人数据与个人信息在概念上有什么不同，这是首先要明了的问题。越来越多的学者认为他们的实质内容是相同的，是一个可以等同的概念。个人数据是经过整理能够被检索到的内容，是个人信息的数据化。因此，个人信息与个人数据的关系是包含与被包含关系[5]。杨佶在肯定上述观点的基础上，进一步提出保护个人数据的目的在于保护个人信息，在立法上使用“个人信息”的概念更符合立法目的[6]。吕炳斌教授也更提倡使用“个人信息”这一术语，认为真正界分“个人数据”与“个人信息”的原因是数据是属于无形财产权需要保护的客体，而个人信息属于人身权所保护的客体，这样的区分更加符合《民法总则》的倾向[7]。梅绍祖认为信息不可能脱离数据而存在，并且数据的处理结果也会产生诸多信息，信息和数据有密切相关性。因此，个人信息保护的内涵与个人数据保护的内涵基本相一致，因此，没有区分二者的必要[8]。第 29 条工作组（WP29）③也没有澄清信息和数据之间的区别[9]。

不同国家和地区对个人信息保护立法过程中使用了不同的称谓，比如欧盟地区立法中多使用“个人数据”（personal data），北美多使用“个人识别信息”（personally identifying information，一般简称为 PII），澳大利亚、日本、韩国、美国加州等国家和地区多使用“个人信息”（personal information）。称谓的不同源于不同的法律传统和法律习惯，但是其实质内容却相同，其共同特征体现在以下两点：第一，法律保护对象是自然人；第二，法律所要实现的目标

① 参见南京市中级人民法院（2014）宁民终字第 5028 号民事判决书。

② 参见欧盟 Case C582/14 号判决书。

③ 第 29 条工作组（the Article 29 Data Protection Working Party），是欧盟在数据保护问题上的咨询机构。其根据 1995 年《数据保护指令》中第 29 条设立，由欧盟成员国、欧盟组织和欧盟委员会三方代表组成。GDPR 生效之后，其职责由欧盟数据保护委员会（European Data Protection Board）接替。

是使自然人的特定信息不被非法搜集、传播、处理从而保护个人权益免受侵犯①。故此,在本文中,“个人数据”和“个人信息”将做等同使用。

(二)域外个人信息保护立法中的“识别”要素界定

“识别”要素是个人信息概念的重要组成部分,识别性是界定个人信息的核心[10]。关于个人信息保护的国际规则方面,主要有经济合作与发展组织(OECD)于1980年发布的《隐私保护和个人数据跨境流通的指南》(以下简称“指南”)和欧盟委员会于1981年通过的《个人数据自动化处理中的个人保护公约》(以下简称“公约”)这两个文件。两个文件给“个人数据”规定了相同的定义,即“个人数据”是指与已识别或可识别的个人(数据主体)相关的任何信息②。在国际规则的指引下,自从20世纪90年代开始,各国先后制定国内个人信息保护法。根据联合国贸易和发展会议网站(UNCTAD)数据显示,截至目前,世界上总共有107个国家制定了个人信息或隐私保护法③。这些国家立法大多将“识别”要素作为“个人信息”的核心构成要件。美国于2020年1月1日正式实施的《加利福尼亚州消费者隐私保护法案》(CCPA)堪称美国史上“最严”的数据保护立法。该法案明确了个人信息的定义:个人信息是指能够直接或间接地识别、关系到、能够相关联或可合理地连接到特定消费者或家庭的信息[11]。该法案不仅承认“识别”要素,而且承认“关联”要素,即只要某一信息与特定人“有关”,那么该信息也属于个人信息。将“识别”要素和“关联”要素同时纳入“个人信息”概念构成的,除了美国加州的消费者隐私保护法,还有欧盟的《欧盟通用数据保护条例》(General Data Protection Regulation,以下简称GDPR),其相关内容将在后文详细阐述。日本2017年5月生效的《个人信息保护法》(Act on the Protection of Personal Information,简称APPI)第2条第一项对个人信息进行了界定:能够识别特定个人或者含有个人识别符号的信息。从日本个人信息立法历史来看,日本在个人信息立法与修改过程中对个人信息的界定不断优化。早在2005年的《个人信息保护法》中,其对个人信息的定义是:“与生存着的个人有关的信息中因包含有姓名、出生年月以及其他内容而可以识别出特定个人的部分(包含可以较容易地与其他信息相比照并可以借此识别出特定个人的信息)”。但是无论其定义如何变化,“识别”始终是界定“个人信息”的重要标准[12]。此外,加拿大早在2000年颁布了《个人信息保护和电子文件法》,该法对个人信息的界定简单明了:个人信息是指关于一个可识别的个人

① 参见周汉华《域外个人信息保护立法概况及主要立法模式》,http://www.iolaw.org.cn/%5Carticle%5C2009%5C7%5C28%5C663F517B149121517A079C76952FF18B.pdf,最后访问时间:2020年6月2日。

② 两个文件对“个人数据”定义的原文均是:“personal data” means any information relating to an identified or identifiable individual(“data subject”).

③ 联合国贸易和发展会议网站 https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx,最后访问时间:2020年3月12日。

的信息。该定义的核心也是“识别”①。

纵观域外立法,除了欧盟的 GDPR 和美国的 CCPA 之外,大多国家和地区均使用“识别”要素定义个人信息。我国目前虽然没有专门的个人信息保护法,在有关个人信息零散的法律规范中,“识别”要素仍然是“个人信息”概念的核心。

(三) 我国学界关于“识别”要素的讨论

近些年特别是 GDPR 实施以来,个人信息的保护问题逐渐成为学术界和实务界讨论的焦点,而如何认识“可识别”的内涵又是其中关键的一环。有学者指出,识别性是个人信息的首要特性,不具有识别性的信息不是个人信息[13]。王玉哲[14]、徐雄杰、叶丹枫[15]、汤擎[16]等学者也认为“识别”是判断“个人信息”的核心要件。从刑法角度来看,“识别”要素对个人信息的判断起着至关重要的作用,界定“识别”要素成了确定个人信息的必经环节[17]。从民法的角度看,侵害个人信息所承载的法益不是个人信息本身,而是不当使用个人信息所产生的“识别”风险以及“识别”之后所侵害的权利和法益[18]。以姓名为核心的身份识别体系是人在社会中不可或缺的一部分,法律需要保护身份识别所产生的精神利益和经济利益[19]。有些国家和地区将“关联”要素纳入“个人信息”保护范围,如美国加州的消费者隐私保护法和欧盟的 GDPR 等。有学者指出,引用“关联”要素会使个人信息的保护过于宽泛,过度的个人信息保护会损害国家和社会的利益[20]。而且,使用“关联”要素界定个人信息,有个人权利滥用的风险[21]。信息的“关联性”必然蕴含在“识别”要素中。信息具有“识别性”必然与个人具有“关联性”,但是信息具有“关联性”却不一定能“识别”到个人,即“关联”是界定个人信息的充分不必要条件而“识别”是界定个人信息的充分必要条件。个人信息立法目的在于保护自然人的权利而非信息本身。个人信息本身只是一个符号,但是当其可以“识别”到个人时则需要法律的介入并加以规范。引用“识别”要素界定个人信息符合个人信息保护立法的初衷。

三、GDPR 中“识别”要素的认定及评析

(一) GDPR 中“识别”要素的认定过程

在欧盟,“识别”要素最早见于 1995 年《数据保护指令》中关于“个人数据”的定义中,该指令第 2 款(a) 项目指出,“个人数据”是指已识别的或可识别的自然人(数据主体) 有关的任何信息。可识别的人是指可以直接或者间接识别的人,特别是通过参考识别号或一个或多个特定于自然人的身体、生理、心理、经济、文化或社会身份的因素②。该指令对“个人数

① 参见加拿大《个人信息保护和电子文件法》,https: //laws-lois. justice. gc. ca/ENG/ACTS/P-8. 6/page-1. html#h -416885,最后访问时间: 2020 年 1 月 9 日。

② 1995 年《数据保护指令》第 2 款第(a) 项:“‘personal data’ shall mean any information relating to an identified or identifiable natural person(‘data subject’) ; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

据”采用了“定义 + 列举”的方式进行界定。GDPR 虽对个人数据进行了重新定义，但大同小异，只是在列举方面增加了“生理、遗传”等识别因素。主要是因为随着技术的发展，遗传信息等与个体的密切性逐渐凸显出来，GDPR 中增加列举的这两个识别因素也是为了顺应社会发展的需要①。在 1995 年《数据保护指令》推出之后，第 29 条工作组意识到对个人信息概念深入分析的必要性，结合司法实践中遇到的对个人数据界定的具体情况，于 2007 年发布了《关于个人数据概念的意见》(Opinion 4/2007 on the concept of personal data) (以下简称“《意见》”) ②。该《意见》指出个人数据由四个构成要素组成，分别是: 任何信息(any information) ; 关联(relating to) ; 已识别的或可识别的(identified or identifiable) ; 自然人(natural person) 。“识别”要素中“已识别”并没有太大争议，争议的是“可识别”问题。故此，该《意见》第三章第 3 节对“可识别”进行了详细的解释。认为“识别”通常是通过特定的信息片段来实现，我们可以称“特定的信息片段”为“标识符”。姓名是识别特定人的最常用“标识符”。某些“标识符”是否足以达到“识别”的程度需要结合具体情境来定。例如，在全中国范围内，我们不能通过一个非常普通的姓氏辨认出某人，但是具体到特定的某个地点，例如教室，或许可以快速“识别”。第 29 条工作组认为可以采用“所有可能合理使用的手段”(all the means likely reasonably to be used) “识别”信息是否为个人信息。若通过“所有可能合理使用的手段”来识别某信息是否为个人信息的可能性不存在或者可以忽略不计，那么该信息是不可识别的，就不是个人信息。此外，第 29 条工作组阐述了防止身份被识别这一技术措施的重要性: 个人数据可以通过技术手段分别被加工为“假名数据”和“匿名数据”。数据假名化的目的是收集一个人除身份之外的其他数据。假名数据的收集主要和研究、统计相关，是一种可以通过技术措施逆向“识别”到个人的。数据也可以通过一种不可能重新识别的方式被加工为“匿名数据”，例如单项密码技术。欧盟已通过《一般数据保护条例》提出明确的匿名化标准，但该条例基于流程设置的标准适用于欧盟境内尚可，适用于我国或显得过于严苛，有碍数字经济的发展[22]。理论上讲，通过技术手段匿名化的数据不可能再通过“所有可能合理使用的手段”再次识别到个人，即匿名化的数据不可能再被识别了③。

(二) GDPR 中“识别”要素认定的评析

欧盟对个人数据中“识别”要素的边界采用广义解释。这一点无论从 GDPR 中个人数据

---

① GDPR 第 4 款第(1) 项: “‘personal data’ means any information relating to an identified or identifiable natural person(‘data subject’) ; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. ”

② 虽然自 2018 年 5 月 25 日起(即 GDPR 生效之日起) ，第 29 条工作组由欧盟数据委员会接任，但其之前发布的包括《关于个人数据概念的意见》在内的相关文件仍然有效。

③ Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, WP 136, pp. 12 - 20.

的定义、第29条工作组对“识别”要素的解释以及欧盟法院的司法实践都可以看出。欧盟注重包括隐私在内的自然人权力的保护,希望通过严格的数据保护政策能够加强数据存储安全和隐私保护。“识别”要素是个人数据的构成要素之一,其外延越大,个人数据保护外延范围也就越大,保护强度也越大。欧盟个人信息“识别”要素宽泛的界定使个人数据有了广泛的外延,法官在界定“个人数据”时有了较大的自由裁量空间。欧盟主流观点认为这样可以更好地保护个人数据权,减少因侵权或违法造成的损害。

但是,从衡量公共利益与个人利益的角度看,欧盟对于“识别”要素的外延界定过于宽泛。例如,在Patrick Breyer诉Federal Republic of Germany案件中,欧盟法院首次指出,动态IP地址本身没有办法识别到一个用户,这是与静态IP地址不同的地方。静态IP地址也称为固定IP地址,是不变的,是能够持续不断地识别网络设备的“标识符”。相反的是,在连接到因特网时动态IP地址会不断变化。而互联网服务提供者会随时保留这种变化了的IP地址的记录[23]。故动态IP地址无法直接识别到特定客户。但是,欧盟法院进一步指出,在运营网站的德国政府机构无法只通过动态IP地址识别用户的情况下,假若结合网络服务提供者(ISP)存储的其他数据后可以识别到Breyer,那么该动态IP地址则也是个人数据。在该案件中,法官的逻辑如图一所示,如果A公司所拥有的数据1不能单独识别出自然人,但是若A公司有合理且可能的渠道访问B公司的数据2,并且结合B公司的数据2之后可以识别自然人,那么A公司的数据1就属于个人信息①。

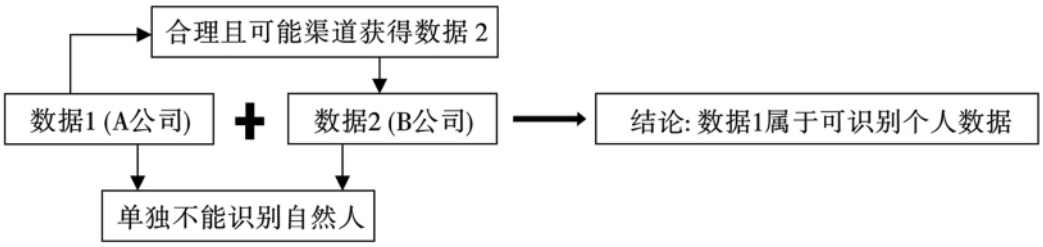

图1　欧盟个人信息“识别”认定关系图

欧盟在司法中始终坚持认为静态IP地址可以是个人信息。早在2011年的Scarlet Sabam案件中,欧盟法院已判定静态IP地址是可以构成个人信息的。原因是互联网提供商给顾客分配IP地址并且保留了分配记录②。但是Breyer案件在此基础上有了新的突破:将动态IP地址纳入个人信息保护范围。背后的原理是,该案件遵循了“可识别性”的客观方法(objective approach),即支持了GDPR立法说明(Recital)第26条:为了确定一个人是否可以被识别,应

① 参见APUS研究院《GDPR实战指南(七)并不简单的“个人数据”判断》,https://user.guancha.cn/main/content?id=27504&s=fwzwyzzwzbt,最后访问时间:2020年3月13日。

② 参见欧盟Joined Cases C468/10 and C469/10号判决书。

考虑数据控制者或者其他人使用的“所有可能的合理方法”识别的可能性。该案件同时也符合 Lindqvist 案件中欧盟法院寻求“个人数据在欧盟获得高水平保护”的司法期待①。

该案件的逻辑似乎给间接识别提供了新的思路，按照这个逻辑可继续类推，任何信息似乎都可以与个人相关。比如说，“背黑色双肩包的人”这个信息不能定位到某特定自然人，但是“某个场合”中“背黑色双肩包的人”或许可以定位到特定个人，那么我们可以说“背黑色双肩包的人”属于个人信息。依据该逻辑推导下的个人数据外延范围过于宽泛，这使得“个人数据隐私保护”与“数据利益”的天平更加倾向于前者。

国外学者将“识别路径”分为两种，一种是绝对路径，一种是相对路径。绝对路径是指数据控制者会穷尽所有可能的方法和手段来识别数据主体。相对路径是指为了识别个人，数据控制者只会采用必要的方法[24]。欧盟上述做法更倾向于绝对路径。由此观之，欧盟已将“已识别”数据与“可识别”数据视为同等类别。GDPR 的立法初衷之一是鼓励欧盟用户和企业充分利用数字经济，让欧盟公民拥有收集、分析和使用他们数据的选择权。在“数据利益”和“个人隐私”发生冲突时，欧盟宁可牺牲经济发展也要保护个人隐私。这植根于欧洲的人文传统、法律价值理念等因素[25]。正如前文所说，“识别”要素的范围决定了“个人数据”概念的范围，而“个人数据”概念的范围直接影响到个人数据的保护范围，GDPR 中“识别”要素宽泛的外延决定了其对个人信息给予非常充分的保护。有观点指出欧盟选择侧重保护个人数据权利，可能会阻碍技术与市场的发展。同时我们也应该注意到 GDPR 给经济带来的负面效应，如遏制了企业的创新，伤害中小企业从而破坏市场生态等[26]。学者们认为，GDPR 实质性的保护范围变得如此广泛，出发点是提供最全面的个人信息保护，但是在不久的将来可能产生事与愿违的结果[9]。非常全面的数据保护法反而破坏了个人数据保护，使之成为毫无意义的法律[27]。GDPR 对个人数据的实质性保护范围正在变得如此宽泛，以至于提供最全面数据保护的良好意愿可能在不久的将来无法实现，并且导致数据保护系统过载。

四、我国个人信息保护立法建议

我国即将出台个人信息保护法。基于我国与欧盟在文化传统、制度环境、产业发展状况等方面的差异，我国在制定个人信息保护法时不应完全向欧盟标准看齐，更不能照搬照抄 GDPR 中关于“识别”要素的界定。相反，我国应在基于国情的基础上，批判地借鉴 GDPR 中关于个人数据“识别”要素的外延，从而界定适合我国国情的个人信息“识别”标准。

(一) 明确界定“识别”要素的原则: 利益平衡原则

欧盟几乎将所有可能“识别”的信息都纳入 GDPR 保护的范围，其背后根本原因在于其人权至上的法律传统。鉴于我国目前正处于经济发展的关键时期，过于宽泛的个人信息界定可能不利于经济的发展。“本质上看，立法其实是一个利益识别、利益选择、利益整合及利

① 参见欧盟 Case C－101/01 号判决书。

益表达的交涉过程，在这一过程中立法者旨在追求实现利益平衡。”[28]个人信息承载了信息主体的人格利益。信息的控制者在处理个人信息时，应尊重信息主体的人格尊严和自由，避免对其人格利益造成侵犯。个人信息保护法在保护个人信息利益的同时，也要考虑个人信息的合法利用与流通。例如，对于企业而言，收集个人信息可以形成“大数据”从而为消费者提供更好的服务，推动企业的创新与发展；对于政府而言，收集和分析个人信息可以提供更好的公共服务；对于科研机构而言，收集个人信息可以推动科学的进步和发展，造福全人类。当个人利益与公共利益相冲突时，必要情况下可以牺牲个人利益以保护公共利益[29]。例如，在“新冠肺炎”爆发期间，政府、医院可以收集疑似患者和确诊患者的姓名、性别、家庭住址、近日行踪等信息，并且不需要得到疑似或确诊患者的同意。因此，个人信息不仅涉及到个人利益，而且涉及他人和公共利益。对个人信息的保护应注意平衡个人利益、他人利益和公共利益之间的关系。在大数据背景下，各种信息可以通过关联、结合从而识别出特定个人，但是对个人信息的保护应限定在合理的范围内，鼓励利用更多信息实现服务社会发展的目的[30]。

（二）对“识别”要素采用狭义解释

制定个人信息保护立法需要考虑到诸多因素：言论自由、政府信息公开等法律价值、数字经济的发展、数据主体的个人信息权利、数据保护领域国际上的“长臂管辖”等[31]。如果对“识别”进行过于狭隘的解释，个人信息不能被充分保护，个人隐私有暴露的风险；如果对“识别”采取像欧盟那样广义的解释，则有可能使所有的信息都变得“可识别”，个人信息保护法可能会变为一部不能很好实现的法律。从隐私的角度考量，个人信息保护法保护数据主体的隐私需要有一定的边界[32]。个人信息的“识别”具有动态性和场景性，也具有很强的时代特征。随着技术的发展，部分信息虽不属于现行法律下的个人信息，也可以精准识别到个人，这给“识别”要素的界定带来前所未有的挑战[33]。法律规范的形式确定性原则一般要求在不同的情况下对个人信息进行一致的解释。然而，现代技术的进步不断提供新的数据操作工具，例如，“识别”技术等[34]。技术的日新月异使立法很难对个人信息的“识别”要素做具体而固定的限定。

欧盟对个人信息界定源于其“人权至上”的法律传统。有学者称欧盟对个人信息的界定是“扩张主义”（expansionist view），美国对个人信息的界定是“简化主义”（reductionist view）。美国的“简化主义”认为，当数据事实上可与特定人相连接时才是个人信息[32]，它是平衡了经济因素与自然人权利的产物。技术的发展、大数据的整合使信息“识别”变得轻而易举。以前述 Breyer 案件为例，动态 IP 地址再结合其他信息之后可以“识别”到特定人，但是动态 IP 地址本身并未事实上与特定人相连接。即该案件中 IP 地址的与特定人相关性并不那么强。这种弱关联性是否能够成为界定个人信息范围的标准值得进一步探讨。

从民事法益的角度考量，个人信息属于民事法定利益，不是所有的民事法益都能当然地获得法律保护。只有合法的、确定的民事法益才能获得法律保护[35]。当个人信息具有的个

人利益与公共利益相冲突时，法律除了要考虑利益本身的正当性之外，还要考虑保护范围和保护成本。Breyer 案件中，将动态 IP 地址纳入个人信息保护范围会影响德国联邦政府的合理利益。且该动态 IP 地址的保护具有个案独特性，不具有普遍适用意义，不应成为需要法律保护的民事法益。若采用"与特定人事实上相连接"条件限定"识别"要素，该条件下"识别"的信息与个人相关度高，其背后承载的民事利益应该受到法律的保护。从利益平衡角度来说，并非所有可识别的个人信息都值得法律保护。在我国现阶段经济发展状况下，我国在个人信息立法过程中一方面要保护自然人的权利，另一方面仍然需要重视个人信息的公共价值，比如医疗价值、政府服务体系价值等，所以个人信息的范围不应过分宽泛。如果把所有可识别身份的信息都纳入保护范围，不仅会加重诉讼负担，而且会阻碍信息技术及信息产业的发展[36]。从法律效果角度来看，若适用广义解释界定"识别"，一方面使得法律保护范围过宽，法律保护上会力不从心。另一方面，该种个人信息保护方式看似充分保护公民的权利，但最终扩大公权力干预范围，从而剥夺公民的权利自由[22]。因此，界定"识别"要素应采取狭义解释，即不是所有的信息都应纳入"可识别"的范围，并且狭义解释的限定因素应是：与特定人事实上相连接。该限定因素不会使得个人信息保护范围过于广泛从而失去了可实施性，也不会使得企业合规成本过高而影响其发展。个人信息保护法的保护对象是自然人，当信息与特定人事实上相连接时，其承载的个人的民事法益具有保护价值。"识别"是保护个人信息的第一步，而"识别"的限定因素是将"可识别"的信息纳入个人信息保护的民事法益基础。

参考文献：

[1] 齐爱民. 个人信息保护法研究 [J]. 河北法学，2008，(4)：17.

[2] 韩旭至. 个人信息概念的法教义学分析 [J]. 重庆大学学报·社会科学版，2018，(2)：159－162.

[3] 谢琳. 大数据时代个人信息边界的界定 [J]. 学术研究，2019，(3)：71－75.

[4] 邓明理. 大数据背景下个人数据的监管保护 [J]. 北京邮电大学学报·社会科学版，2019，(2)：24.

[5] 李慧敏，王忠. 日本对个人数据权属的处理方式及启示 [J]. 科技与法律，2019，(4)：3－4.

[6] 杨佶. 论个人信息的法律保护 [J]. 吉首大学学报·社会科学版，2009，(1)：2.

[7] 吕炳斌. 个人信息权作为民事权利之证成：以知识产权为参照 [J]. 中国法学，2019，(4)：5.

[8] 梅绍祖. 个人信息保护的基础性问题研究 [J]. 苏州大学学报·哲学社会科学版，2005，(2)：3.

[9] Nadezhda Purtova. the Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law [J]. Law, Innovation and Technology，2018，(10)：3，49－53.

[10] 任龙龙. 个人信息民法保护的理论基础 [J]. 河北法学，2017，(4)：181－192.

[11] 谢业华，等. 美国加利福尼亚州《消费者隐私法案》研究 [J]. 征信，2018，(10)：1.

[12] 方禹.《日本个人信息保护法(2017)》解读 [J]. 网境纵横，2019，(5)：81.

[13] 韩旭至. 大数据时代下匿名信息的法律规制 [J]. 大连理工大学学报·社会科学版，2018，(4)：64.

[14] 王玉哲. 我国个人信息立法保护实证研究[J]. 东方法学,2016,(3):63.
[15] 徐雄杰,叶丹枫. 大数据视角下"公民个人信息"的界定[J]. 中国检察官,2018,(4):33-34.
[16] 汤擎. 试论个人数据与相关的法律关系[J]. 华东政法学院学报,2000,(5):41.
[17] 晋涛. 刑法中个人信息"识别性"的取舍[J]. 中国刑事法杂志,2019,(5):64.
[18] 苏今. 《民法总则》中个人信息的"可识别性"特征及其规范路径[J]. 大连理工大学学报·社会科学版,2020,(1):87.
[19] 高富平. 论个人信息保护的目的——以个人信息保护法益区分为核心[J]. 法学论坛,2019,(1):98.
[20] 刘占鑫. 基于民法总则的个人信息权概念界定[J]. 甘肃广播电视大学学报,2017,(6):66.
[21] 井慧宝,常秀娇. 个人信息概念的厘定[J]. 法律适用,2011,(3):90,91.
[22] 张建文,高悦. 我国个人信息匿名化的法律标准与规则重塑[J]. 河北法学,2020,(1):43-56.
[23] Frederik Zuiderveen Borgesius. The Breyer Case of the Court of Justice of the European Union: IP Addresses and the Personal Data Definition[J]. European Data Protection Law Review,2017,(3):2.
[24] Gerald Spindler, Philipp Schmechel. Personal Data and Encryption in the European General Data Protection Regulation[J]. Journal Of Intellectual Property, Information Technology And Electronic Commerce Law, 2016,(7):165-166.
[25] 张怀印. 欧盟制定 GDPR 最大的收获[J]. 中国中小企业,2018,(7):73.
[26] 吴韬. GDPR 阻碍中小企业创新 中国数字经济立法应优先考虑创新与发展[EB/OL]. http://finance.eastmoney.com/news/1350,20180706902252457.html,2020-03-22.
[27] Bert-Jaap Koops. The Trouble With European Data Protection Law[J]. International Data Privacy Law, 2014,(4):250.
[28] 张斌. 论现代立法中的利益平衡机制[J]. 清华大学学报·哲学社会科学版,2005,(2):1.
[29] 高富平. 个人信息使用的合法性基础——数据上利益分析视角[J]. 比较法研究,2019,(2):53-59.
[30] 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):94.
[31] 苏宇,高文英. 个人信息的身份识别标准:源流、实践与反思[J]. 交大法学,2019,(4):67.
[32] Paul M. Schwartz, Daniel J. Solove. The PII Problem: Privacy And A New Concept of Personality Identifiable Information[J]. New York University Law Revies,2011,(86):1817,1827.
[33] 何波. 试论个人信息概念之界定[J]. 信息通讯技术与政策,2018,(6):38.
[34] Vladislav Arkhipov, Victor Naumov. The Legal Definition of Personal Data in the Regulatory Environment of the Russian Federation: Between Formal Certainty and Technological Development[J]. Computer Law & Security Review,2016,(32):868.
[35] 阳雪雅. 论个人信息的界定、分类及流通体系——兼评《民法总则》第 111 条[J]. 东方法学,2019,(4):35.
[36] 岳林. 个人信息的身份识别标准[J]. 上海大学学报·社会科学版,2017,(34):8.

(全文共 11,277 字)