法商研究 Studies in Law and Business
Vol. 38 No. 2(2021)

网络与信息法

个人信息处理:我国个人信息保护法的规范对象

高 富 平*

摘要:个人信息保护法旨在保护个人信息处理中的个人权益不受侵犯。个人信息保护法需要界定个人信息处理中可能出现的个人权益侵害风险,以确立防范风险发生的个人信息处理规则。个人信息处理在个人信息保护法中具有界定规范对象和边界的双重价值。我国个人信息保护法的制定应当将个人信息处理作为规范对象,同时将个人信息处理限缩在以识别分析为核心的处理行为上,并将之划分为收集、控制、分享、分析和应用5种具体处理行为。

关键词:个人信息保护法 个人信息(个人数据) 个人信息处理 识别分析

一、引 言

个人信息(个人数据)保护法肇始于计算机应用,为解决个人信息电子化处理引发的个人权益保护问题,个人信息处理(数据处理)就成为个人信息保护法的基石性概念。自2012年全国人大常委会发布《关于加强网络信息保护的决定》(以下简称《决定》)起,我国即开始构建以个人控制为基础的个人信息保护制度,并散见于《中华人民共和国消费者权益保护法》(以下简称《消费者权益保护法》)、《中华人民共和国网络安全法》(以下简称《网络安全法》)、《中华人民共和国电子商务法》(以下简称《电子商务法》)等法律之中。2020年颁布的《中华人民共和国民法典》(以下简称《民法典》)开始使用"个人信息处理"替代之前的个人信息保护相关立法中"个人信息收集和使用"的表述。2020年10月21日发布的《中华人民共和国个人信息保护法(草案)》(以下简称《草案》)将该法定位于"规范个人信息处理活动",由此个人信息处理就成为基本概念。《草案》第4条以列举的方式将个人信息处理定义为"包括个人信息的收集、存储、使用、加工、传输、提供、公开等活动"。信息处理是计算机基本用语,但个人信息处理并没有得到法学研究者足够的

* 华东政法大学法律学院教授、博士生导师
基金项目:国家社会科学基金项目(18ZDA145)

关注。法律概念具有认识功能、构成功能和规范功能,其语义必须满足确定性,尽可能避免因歧义、模糊、开放等引发的语义不清给法律适用带来太大的解释空间。作为源自信息技术的技术概念,信息处理一定会随着技术的进步而变化并对社会产生不同的影响,因而我们应当从法律规范的目的——个人信息处理对个人权利的危害——出发对个人信息处理进行界定。个人信息处理的界定,既要使真正危害个人的行为得到规范,又要避免因信息处理概念的宽泛和模糊导致法律规范对象的泛化,产生对社会的过度干预甚或选择性执法的恶果。我国个人信息保护法在引入信息处理概念时还必须明确其内涵,使个人信息保护法的适用有明确的规范边界,同时利用处理行为的种属概念建立起清晰的个人信息处理规则,防范对个人权益的侵害。这是个人信息保护法需要解决的基础问题。

二、个人信息处理的规范价值

早在 40 年前,域外就兴起个人信息保护的立法。2012 年我国开始引入个人信息保护制度,《决定》明确宣布"国家保护能够识别公民个人身份和涉及公民个人隐私的电子信息",确立了个人信息收集和使用的基本原则和规则,这在我国个人信息保护制度发展史上具有里程碑意义。[①]《决定》确立的个人信息保护制度为《消费者权益保护法》(2013 年修正)、《网络安全法》(2016 年)、《中华人民共和国民法总则》(2017 年)、《电子商务法》(2018 年)等法律所吸收。由此,"个人信息收集和使用"成为我国个人信息保护法的基本术语。我国目前的个人信息保护制度的基本框架即构建在此术语之上,即个人信息的收集和使用应遵循合法、正当、必要原则,同时须经被收集者同意,且个人信息在收集和保存后应当依法或依约处理或使用。虽然目前分散的个人信息保护规范相当粗糙,但是"收集"和"使用"似乎可以涵盖所有对个人信息的操作行为。唯一需要明确界定的是"使用"。如果可以将"使用"细分为涵盖分析处理、披露、分享等行为,那么也就可以实现对个人信息处理的具体行为的规范。此方案是一种既可以实现对个人信息处理的具体行为进行规范又与现实法律对接的解决方案。当然,还可以不用"使用"一词,而直接用"分析""分享(披露、转移)""公开(含传播)",完全采取具体规范模式,实现对个人信息使用行为的规范。也就是说,单纯从个人信息利用规范的角度看,没有必要采取抽象信息处理的概念,而是直接规范收集、分享、分析、公开等行为以实现对个人信息处理行为的规范。

法律对社会生活的干预必须具有正当性。在个人信息处理的规范方面,存在一个基本假设,即个人信息是可以自由使用的,除非个人信息上存在明确可识别的个人权益,否则就不能赋予信息主体(信息指示或描述的对象)干预他人使用的自由。个人信息保护法之所以出现,就是因为计算机应用于个人信息处理引发了个人保护的新问题,需要法律干预个人信息使用行为。这是经济合作与发展组织(以下简称经合组织)于 1980 年发布具有软法性质的《隐私保护和个人数据

① 虽然《关于加强网络信息保护的决定》的名称中使用了"网络信息"的表达,但是其主要规范的是个人信息的保护。在我国,该决定第一次以法律的形式宣布保护个人信息,具有里程碑意义,只是以"决定"替代正式的法律具有应急性。笔者认为,2009 年《中华人民共和国刑法修正案(七)》在第 253 条增设侵犯公民个人信息罪是在我国还没有法律明确个人信息受法律保护的前提下从社会危害和公共秩序的立场上进行的一种规范,很难算作是个人信息保护制度的引入和确立。

跨境流通指南》(以下简称《指南》)[①]和欧盟于1981年发布具有国际公约性质的《个人数据自动处理中的个人保护公约》(以下简称《公约》)[②]在初创个人信息保护制度时定下的基调。《指南》旨在应对和规范计算机处理引发的隐私保护新问题。这里的隐私超出了传统隐私的范畴,是更复杂的利益合成体,更为准确地说其应当被称为"隐私和个人自由"。[③]《指南》第2部分(基本原则)提出了个人数据保护和利用的8项原则,即收集限制原则、数据质量原则、目的特定化原则、使用限制原则、安全保护原则、公开原则、个人参与原则、责任原则,适用于因处理方式或者因个人数据性质或场景而给隐私和个人自由带来危险的一切个人数据处理 。这些原则几乎影响了全世界的个人信息保护立法。从公约的名称看,《公约》旨在保护个人而非个人数据。个人数据事关个人,而个人是主体,因而处理个人数据就不能像对待客体那样随意,而需要对个人数据处理行为进行规范以捍卫"每个人的个人尊严和保护基本人权和基本自由"。虽然这种保护目的也被抽象为个人数据保护权,但是《公约》对个人数据保护权的保护仍然体现为通过一组个人数据处理的原则来保护个人的基本权益。《指南》与《公约》的差异在于:《指南》没有使用数据处理的概念,其原则性规范针对的是具体的处理行为("公开""获取"或"使用");而《公约》则使用了抽象的个人数据处理概念,并以此为基础构建了"一般+例外"的规范模式。然而,《指南》与《公约》对个人数据保护的目的和路径基本一致,即通过规范个人数据处理来保护个人权益不受侵犯。为此,应从技术和法律两个方面,对法律要干预的数据处理行为作出清晰的界定。由此,我们可以了解规范个人数据处理行为的必要性。

《指南》的起草者已经认识到,计算机和通信技术收集、组织、存储和分享信息构成数据处理的基本内涵,并指出:"《指南》适用于一般个人数据,或更准确地说,适用于因为个人数据处理方式或者因为个人数据的性质或场景,给隐私和个人自由带来危险的一切个人数据处理"。[④] 从技术方面看,有危害的数据处理方式是"建立和使用数据聚合以进行重复获取、作出决策、研究、调查和类似目的"。[⑤]《公约》起草者也已经注意到计算机技术与通信技术的融合,不仅可能实现分布式数据处理系统和数据传输,而且使广泛的远程信息服务成为可能。分布式、去中心的计算机

① 经济合作与发展组织《隐私保护和个人数据跨境流通指南》于2013年修订重新发布,鉴于2013年版本在基本术语和基本原则方面没有实质变化,本文不区分两个版本,引用以2013年的版本为基础。See Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (2013) [C(80)58/FINAL, as Amended on 11 July 2013 by C(2013)79], http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf,2015-11-23.

② See Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, CETS No.108, Strasbourg, 28/01/1981,http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108,2020-03-12.

③ OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data ,Explanatory Memorandum, https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm,2020-03-12.

④ OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Explantatory Memorandum, https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm, 2020-03-12.

⑤ OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Explantatory Memorandum, https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm, 2020-03-12.

系统具有超强的收集、处理和传递个人数据的能力,促使《指南》和《公约》的立法者们先检讨现有的法律是否能提供充分的保护,在否定的基础上再寻求新的保护制度。① 在当时,这些立法者已就风险源于"自动处理"达成共识,只是就是否在法律文件中使用"自动处理"的措辞存在分歧。同时,他们对计算机或信息技术给处理方式带来的新变化也达成了共识。当时,他们关注到 4 个方面的新变化:(1)可以不经个人知晓即可采集个人数据;②(2)可以存储个人数据并长期脱离数据主体对数据进行处理;③(3)可以运用数据的逻辑对获取的数据进行比较、联结、运算分析;④(4)计算机和通信技术的结合可以处理成千上万个位于不同地方的用户的信息,可以轻易实现跨境的数据处理。⑤ 这 4 个方面的变化将给个人权益带来新问题。因为个人数据是关于个人的,而个人是主体,个人数据的处理失去主体的控制,可能威胁个人的尊严、自由、平等。笔者认为,这 4 点是我们今天界定个人数据处理边界的主要依据。由此,影响个人权益的数据处理具有两个非常核心的要素,即电子存档和基于电子数据的分析。这两个要素改变了个人数据碎片化、随机性的使用,使之演变为全面、系统、持续性的使用,并且这样的数据处理方式要求数据控制者对个人有更深刻、全面和精确的观察和分析。此两个要素合在一起即为识别分析。这种利用个人数据的方式,彻底改变了纸质记录环境下的个人数据处理。在纸质记录环境下,个人数据即使被政府或企业组织收集,其保存和重复利用也非易事,进行研究分析则更不简单,因此不存在对个人数据使用干预的必要性。

从法律方面看,需要法律干预的数据处理应当是那些给个人尊严和自由带来威胁的数据处理。数据处理概念的核心是个人数据处理方式因计算机或信息技术的应用而发生变革。计算机技术的本质是数字化处理、网络化技术、智能化分析等应用数据的技术方法,其并不会改变个人信息的性质,也不能因为新的处理方式就使个人享有个人信息决定权,控制个人信息的使用。法律对个人信息处理行为的处理仍然应当恪守技术中立原则,避免妨碍信息自由和新技术应用。但是,新的处理方式的确给个人尊严和自由带来威胁,数据处理作为进入法律领域的术语就是界定危害主体权益的数据使用行为的工具。只有在数据处理行为危害个人隐私或自由(或法律保

① See New Technologies: A Challenge to Privacy Protection? https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent? documentId=0900001680684607, 2020-03-12.

② 在互联网应用之前,个人信息的收集以个人提供为主,很少像今天这样大规模网络跟踪、传感器远程监控。但是欧盟已经关注到遥测技术可以在没有个人参与的前提下远程收集个人信息,甚至已经预测到"个人完全被监控将成为可能"。See New Technologies: A Challenge to Privacy Protection? https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent? documentId=0900001680684607, 2020-03-02.

③ 不仅存在集中存储和处理的数据(被称为自动数据文档),而且在网络状态下的分散数据也因相互链接而被处理,个人无法或无力控制数据处理,透明度也无从谈起。See New Technologies: A Challenge to Privacy Protection, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent? documentId=0900001680684607, 2020-03-12.

④ 信息技术具有很强的分析个人数据、创设各种之前不可能有的联系的能力。就隐私而言,这被认为是最大的问题。See Michael Kirby, The History, Achievement and Future of the 1980 OECD Guidelines on Privacy, 1(1)International Data Privacy Law, 6-14(2011).

⑤ See Michael Kirby, The History, Achievement and Future of the 1980 OECD Guidelines on Privacy, 1(1) International Data Privacy Law, 6-14(2011); New Technologies: A Challenge to Privacy Protection? https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent? documentId=0900001680684607, 2020-03-12.

护的权益)、产生保护个人权益的必要时,法律对个人数据处理进行规范的条件和程序才具有正当性。个人数据处理必须限定在对主体权益带来风险的数据使用上,不能因为计算机处理有风险,就将所有利用计算机处理个人数据的数据使用行为均确定为数据处理,并以个人信息保护法规范之。对主体权益有实质性影响的数据处理才有必要进入法律,这是法律对个人数据处理的实质性限定。个人信息保护法旨在应对个人信息处理引发的问题,是否采用信息处理的概念只是立法技术问题。作为法律概念,个人信息处理具有确定个人信息保护法的规范对象和边界的作用。在个人信息保护制度创立之初,立法者就采取自动处理概念表明个人信息保护法特别的适用范围。其不规范所有的个人信息使用关系,只不过因为计算机应用导致个人信息处理方式发生变化,引发新的隐私保护问题而需要给予个人保护。也就是说,信息处理概念界分出个人信息保护法与传统法律的关系。

个人信息是与个人有关的个人信息,与个人有关的个人信息关涉个人权益,只要存在合法的个人权益,法律均予以保护;在法律形成和演变的过程中,不断发现和界定个人信息上可能存在的个人权益,设置相应的制度或规则予以保护,其中最基础的是人格权法对人格权益的保护。人格权保护也是通过规范个人信息的使用保护个人信息上的人格权益:自然人的姓名、肖像属于典型的个人信息,民法赋予个人以姓名权和肖像权就是对直接识别个人的信息上的人格权益进行保护;名誉权和隐私权则旨在制止他人不当使用个人信息的行为(传播虚假信息、擅自公开私密信息)以保护个人的名誉和隐私利益。除此以外,还有行业法律对各种服务关系中的个人敏感信息进行保护,如医疗服务、律师服务中的个人私密信息保护。《中华人民共和国居民身份证法》(以下简称《居民身份证法》)、《中华人民共和国刑法》(以下简称《刑法》)、《中华人民共和国行政监察法》(以下简称《行政监察法》)、《中华人民共和国选举法》(以下简称《选举法》)、《中华人民共和国统计法》(以下简称《统计法》)、《中华人民共和国税法》(以下简称《税法》)等法律,也对履行特定职务的工作人员施以安全保障义务,防范特定个人身份信息泄露,保护公民的民主权利、人身或财产安全。个人信息保护源自个人信息上存在需要保护的个人权益,其根植于我国法律保护的个人权益。要移植域外的个人信息保护法,在我国的法律体系中嵌入新的保护,就必须找到其区别于既有保护的特殊之处。如此,要保护的应该是计算机应用引发的新个人权益保护,概括新权益的基础概念便是信息处理,但决定是否要规范的是其对个人权益的危害。[①] 个人信息保护法旨在规范因新的信息使用方式而导致的个人信息滥用行为,以保护个人权益。处理的本质是使用,但是采用“信息处理”而非“信息使用”的措辞,其目的在于凸显利用计算机使用个人信息方式的独特性,着眼于对个人权益的新危害。

信息处理的规范价值除了可以将涉及个人信息的行为概括起来,建立个人信息保护法规范和适用的基本范畴之外,还在于可以界定个人信息保护法的边界。这样,在个人信息保护法中抽象意义上的信息处理就成为必要的概念,借助它可以支撑个人信息保护法基本原则的规定并界定个人信息保护法的规范边界。从我国现行的法律体系观之,我国的个人信息保护源自《中华人民共和国宪法》,并与《民法典》《刑法》《居民身份证法》《消费者保护法》《网络安全法》有交叉,与金融、健康、医疗、通信、律师等特殊行业或特殊关系的法之间有相互指引关系。任何一部法律都

① 个人信息保护的对象是由人的尊严所派生出的个人自治、身份利益、平等利益。参见高富平:《论个人信息保护的目的——以个人信息保护法益区分为核心》,《法商研究》2019 年第 1 期。

应当清晰界定它保护的个人信息处理涉及的个人基本权利,使法律不重复和不冲突地执行,避免个人信息保护陷入困局是制定个人信息保护法时应当考虑的问题。[①] 在笔者看来,个人信息保护与个人信息保护法并不能等同,个人信息保护是许多法律要解决的问题(尤其是对个人身份信息滥用、泄露的规范),而个人信息保护法解决的是其他法律不能解决的问题。个人信息保护法一定要有自己清晰的定位和边界,否则将导致个人信息保护法的适用模糊化和泛化,不利于法律的实施。

在明确个人信息处理的规范价值及其要解决的问题之后,关键是如何定义个人信息处理的概念。个人信息处理的概念关系着我国个人信息保护法的规范范围,关系着个人信息保护法与既有法律边界的划分。

三、个人信息处理的界定

在确定采纳信息处理的概念后,我们需要对个人信息处理作出明确的定位,使个人信息保护法有清晰的规范对象和范围。《草案》第 4 条将个人信息处理定义为"包括个人信息的收集、存储、使用、加工、传输、提供、公开等活动"。这一定义既无抽象表述,又采用开放式列举,很难看出个人信息处理的内涵与外延。例如,何谓使用,何谓提供,这些都需要解释。笔者认为,应当将个人信息处理定义为"以识别分析为目的对个人信息的收集、控制、分享、分析和应用行为"。

(一)个人信息处理的定义:《欧盟统一数据保护条例》的借鉴与超越

个人信息处理中的个人保护是一项源于域外的制度,并且已经演进 40 多年。我国在制定个人信息保护法时,需要借鉴这些域外立法经验和教训。但是,这种借鉴并非总结相关域外立法采取的定义然后求取最大公约数的简单移植,而应当回到 40 年前制度缔造者们的初衷来定义当今我国立法中的个人信息处理,沿着他们解决问题的思路,来解决我国面临的问题。尤其是在这 40 年中信息技术不断迭代发展,作为应对信息技术应用引发新问题的法律概念,个人信息处理的应用场景、对主体权利的威胁以及我们对它的认知均发生了变化,我们需要在新技术背景下重新定位我们要规范的个人信息处理。

欧盟是个人信息保护立法的推动者和探索者,2016 年颁布的《欧盟统一数据保护条例》(以下简称《条例》)是其在个人信息保护方面最新的法律成果。这里仅对《条例》中的相关定义及其面临的问题进行分析,为我国确定在个人信息保护法的基本范畴方面所应当采取的策略提供智识。

《条例》取代了 1995 年制定了《欧盟关于涉及个人数据处理的个人保护以及此类数据自由流通的第 95/46/EC/号指令》(以下简称《指令》)。从《指令》开始,数据处理即是贯穿于个人信息保护法的基石性概念。《条例》第 4 条对数据处理的定义几乎与《指令》第 2 条一致,采取"概括+列

① 数据保护其实也是一个困局。统一数据保护法并不排除特别法规范。任何一部法律都应当清晰界定它要保护的个人基本权利(如隐私权和个人数据保护),因此任何当前或未来的法律与该保护相冲突的,应当被视为无效。许多特别法都会涉及隐私权和个人数据处理,如通信监管、贸易、教育、电子政务、健康服务、金融和银行机构、消费者保护、网络安全和产品质量等方面的特别法。这些法律应当在尊重隐私权的同时,确保对个人数据加以保护。See Privacy International , A Guide for Policy Engagement on Data Protection, https://www.privacyinternational.org/sites/default/files/2018-09/Data%20Protection%20COMPLETE.pdf ,2020-02-22.

举”的方式,全面列举了数据处理的方式,既包括所有的技术手段,如记录、组织、结构化、存储、改编或修改、恢复、排列或组合、限制、清除或销毁,也包括收集、查询、使用、披露或者其他使个人数据可被他人获得的行为(相对于《指令》所列举的行为,《条例》仅多了“结构化”这一行为)。由此可见,欧盟的数据处理行为含义广泛,试图穷尽可能使用、接触或触碰个人数据的各种操作或行为,以提供一个在欧盟内可广泛适用的数据处理概念。《条例》对处理的定义相当广,你能想到的与个人数据相关的任何活动都构成处理。它不仅仅是计算机操作,也不一定使用计算机,你只要是从远程查阅一下数据就构成处理。①

《条例》将数据处理定义为“操作”表明其遵从《公约》的定位,用以规范利用计算机对个人数据的操作行为,但其对处理行为的定义过分注重技术内涵,而忽视这些行为对个人权益的影响,导致涵摄宽泛。加上计算机和网络应用在如今是一种普遍的现象,个人数据的处理像毛细血管一样渗入社会的每个组织和所有行为,这导致《条例》的实施面临很大的困难。数据处理涵盖所有动用个人数据的行为,贯穿于各种行业、领域和社会活动(行为)之中,这使得个人数据处理规范得以广泛适用,很难界定个人信息保护法适用的边界。一旦任何使用计算机处理个人数据的行为被纳入个人信息保护法的范畴,那么个人信息保护法就成为没有门槛的法律,不仅具有普遍适用性,而且适用无清晰边界。例如,某人未经他人同意上传他人的照片,或者转发内含可识别的他人个人信息,就会被认为构成个人信息的使用。这一方面会增加社会运行的成本,另一方面会增加法律适用的不确定性和混乱。无边界的个人数据、极大的数据处理概念将导致个人信息保护法的适用范围在无限扩张的同时,也与其他众多法律出现大量交叉;法律竞合的现象大量发生,使得数据主体可以利用这一现象,选择有利于自己的请求权基础,同时也导致选择性执法现象。这样无所不包的个人数据处理概念已经背离《公约》最初的立法目的和对数据处理的定义。② 欧盟的个人数据处理概念试图建构一个无所不包的信息处理概念,这将导致不设门槛和边界的个人信息保护法的适用,任何涉及个人信息的行为均受个人信息保护法的规范。这是《条例》本身存在的最大问题,《条例》实施两周年的评估也充分暴露了这一问题。③

《条例》之所以面临实施的困境是因为它坚持规范所有利用计算机处理个人数据的行为,而此类行为已经是所有社会活动开展的基础。在 40 年前计算机的应用仅涉及少数行业和少数主体,还没有普及到整个社会,那时还可以区分计算机(自动)与非计算机(非自动)处理,但今天以此区分信息处理的方式已经变得没有多少意义。在信息处理均已实现计算机化的今天,任何一

---

① See Personal Data: Getting It Right with GDPR——An Interview with Jay Exum, Privacy Counsel at SAS, https://www.sas.com/en_us/insights/articles/data-management/personal-data-getting-it-right-with-gdpr.html, 2020-02-29.

② 《个人数据自动处理中的个人保护公约》中的“处理”仅涉及运用计算机对个人数据进行存储和运算,并不涉及使用和披露(提供、传播、分发或移转等)行为。受《隐私保护和个人数据跨境流通指南》对数据处理内涵扩张的影响,2012 年修改后的《个人数据自动处理中的个人保护公约》中的“处理”涵盖所有使用个人数据的行为。See Sophie Kwasny, Convention 108+ and the GDPR, https://rm.coe.int/090000168093b851,2020-03-09.

③ See Eline Chivot, Two Years On, the GDPR's Flaws Show Why the EU Should Avoid Additional Rules, https://datainnovation.org/2020/06/two-years-on-the-gdprs-flaws-show-why-the-eu-should-avoid-additional-rules/,2020-12-01;Chris Preimesberger, Two Years In, IT Thought Leaders Judge GDPR's Impact, https://www.eweek.com/security/two-years-in-it-thought-leaders-evaluate-gdpr-s-impact, 2020-11-18.

个组织使用个人信息均落入个人信息处理的概念范畴,因而单纯从技术方面规范个人信息处理实际上使所有的个人信息使用行为都落入个人信息保护法的规范范畴,导致法律规范对象泛化。事实上,很难确定每一种个人信息处理行为都会给个人尊严或自由带来危害;否则,将导致"使用计算机处理个人信息就具有危害"的结论,而这显然是不切实际的。泛化的个人信息处理不仅使《条例》将所有个人信息使用行为纳入规范,而且导致对真正有危害的个人信息处理行为规范不足,没有真正应对个人信息处理中个人保护面临的真问题。在笔者看来,这样的定位背离了个人信息处理中的个人保护制度设计者的初衷。也许欧盟停留在基本权利层面的泛化保护法具有一定的可执行性,个人数据上的各种利益的平衡可以实现,但我国个人信息保护法的立法必须考虑可执行性、可适用性和可监管性,不能将个人信息保护法看成是承担一切个人信息保护的法律。

在人类进入到万物互联的网络化生存时代,人类信息产生的方式和相应的处理能力(算力、算法等)均发生了变化。今天,一切网络设备和终端都成为信息的生产源,在人类利用网络通信交流和从事各种社会活动、产生有价值的信息(包括科学文化成果)的同时,机器也每时每刻不断记录自然、机器、人类运行或行为的轨迹,形成大数据。这些大数据通过网络和各种设备可以关联其描述的对象(包括个人),对这些对象的运行规律和特性进行分析,并将分析结果运用到各种决策,这就是大数据、人工智能、云计算等新一代信息技术带给人类社会的新应用和新前景。在这样的时代,个人信息处理已经不再是 40 年前的个人提供数据的长期存储和重复分析使用的过程,而是利用泛在网络形成的大量与个人有关的信息进行深度挖掘分析,形成个性标签(用来鉴别个人偏好、倾向等个性),并在此基础上做出精准决定(如营销、信息推送等)的过程。这样的过程被概括为识别分析,它是进入到大数据时代对个人权益具有最显著影响的个人信息处理。

《条例》已经对识别分析下了定义,[①]并对自动的识别分析作出特殊规范。《条例》是建立在泛在的个人数据处理概念之上的,其目的并非在于应对数字时代新型的数据处理方式对个人的影响。在这样的时代,个人信息的产生方式、来源或渠道、表现形式、收集分析方式和能力以及应用场景和方式等都发生了巨大的变化。而《条例》确立的个人数据处理原则是建立在前网络时代"个人提供数据+计算机处理"这样一个基本模型上的,这些基本原则已经不适应泛在网络时代个人数据的产生和利用方式。泛在网络所生产的个人数据已成为社会重要的资源,基于个人数据的识别分析在于支持社会的智能决策。在这个时候,个人数据上的主体权益不仅要与资源价值进行平衡,而且这种平衡态势还会影响数据主体的权益范围、内容和保护方式。笔者认为,我国个人信息保护法的制定应当弥补泛化的个人信息处理这一缺陷,清晰界定出对个人有害的个人信息处理行为,唯此才能摆脱《条例》实施面临的困境。

(二)与时俱进的个人信息处理定义

作为因技术而生的信息处理概念也一定是随技术变化的,尤其是进入法律规范的信息处理一定要具有规范价值。正如《指南》起草专家组主席迈克尔·卡比在谈到《指南》草拟的经验时指出的那样,个人信息保护领域的政策和法律必须建立在对相关技术运行的正确和全面理解的基

① 识别分析(profiling),是指对个人数据采取的任何自动化处理的方式,包括评估某个自然人特定方面的情况,尤其是为了分析和预测该自然人的工作表现、经济状况、健康、个人喜好、兴趣、可信度、行为举止、所在位置或行迹。"Profiling"在我国多被译为"用户画像",实际上它并不一定针对用户,它可以针对任何个人或群体,在本质上是对特定个人或群体特征的一种分析和呈现行为。

础之上。正确的选择应确保技术的不断发展,以满足用户和社会的福祉。“法律的介入和有效的实践原则应当继续保护个人的基本权益,同时捍卫信息系统的完整性。”[①]在大数据时代,我们仍然应当从科技和法律这两个方面来准确界定个人信息保护法中的个人信息处理概念,将其限定为对个人权益可能带来危害的个人信息处理行为。

从技术方面看,个人信息处理已经从个人直接收集信息进行运算分析的阶段进入到大量依赖机器产生的数据和间接获取的数据对个人进行智能分析的阶段。利用数字技术收集个人信息,进行简单的计算机处理(存储、运算分析),满足任何的组织运营和对外交往需要,已经成为普遍的社会需求,同时也是个人进入到数字化生存时代不得不面对和接受的事实。对于这样的个人信息处理,法律只要施以安全保障义务,就可以防范个人信息使用带给个人的危害。随着大数据、人工智能等在个人信息处理方面的应用,对个人有危害的信息处理也升级迭代,利用泛在网络产生的数据关联性(大数据根本特征)对潜在个体进行分析成为对个人权益最大的威胁,我们应当以有规范价值的识别分析为核心来定义个人信息处理。

从某种意义上讲,以识别分析为核心来定义个人信息处理恰恰是回归到将个人信息处理纳入法律规范的本义。个人信息的基本功能和价值是识别,但是我们很难简单地根据单个信息或碎片化的信息来判断其是否具有可识别个人的属性,而只能根据信息处理者的信息处理能力(获取的信息数量、使用方法等)来判断其是否能够识别个人。因此,个人信息保护法在本质上应当是要规范利用个人信息识别分析个人的行为,而不是要规范个人信息的处理行为。仅处理不识别个人或者仅简单地认知和联络个人的行为不能仅因为使用计算机手段就受到法律的规范。个人信息的使用不能仅因为使用计算机而受到规范,最初的立法者们所担心的计算机处理给人们带来危害的行为并不是所有的利用计算机对个人信息处理的行为,而是那些建立个人电子文档并对其数据长期重复分析使用的行为。也就是说,分析使用是个人信息处理的核心。欧盟在立法中将个人数据处理泛化为覆盖数据生命周期的处理行为,是偏离了个人信息处理的核心并泛化了规范对象。今天,识别分析仍然是个人信息处理的基本面,只是所利用的数据量和分析的技术发生了巨大的变化。广泛收集个人信息形成个人数据集,并根据需要或目的对个体进行识别分析,然后应用于各种决策,既是当今个人信息最重要的应用,也是对个人权益最有影响的个人信息处理行为。

以识别分析为核心定义个人信息处理,可以将对主体权益有显著影响的个人信息处理行为纳入个人信息保护法,而将一般的个人信息使用行为留给其他法律或行业准则或社会习惯规范。这样,那些利用计算机存储客户个人数据、零散地使用个人信息的行为,如单独使用肖像或姓名或通讯方式等个人信息的使用行为,则无必要纳入个人信息保护法。例如,如果理发店存储的个人信息仅用于客户联系的服务,那么不受个人信息保护法规范;如果理发店老板以营利为目的出卖个人信息,那么应当由刑法规制。如果未经他人同意使用肖像,即使用于识别也应当由我国民法典人格权编来规范,而不是由个人信息保护法规范。这样的限缩有利于廓清个人信息保护法的适用边界,扼制对个人权益有实质危害的行为,而不是泛化个人信息保护法的适用。

之所以做这样的限定,是因为在泛在网络的环境下,个人信息收集、存储和使用极为常见,电

① Michael Kirby, The History, Achievement and Future of the 1980 OECD Guidelines on Privacy, 1(1) International Data Privacy Law, 6－14(2011).

子商务、共享经济、社交媒体、在线支付、智慧城市等不断创造联结和数据,网络化、数字化生存模式重构社会运行方式和对个人隐私的认知。人们已经不能再基于非网络时代的隐私观或自由观来设计网络时代的信息隐私或个人信息保护。在这样的时代,为个人提供再多的对自己数据的控制权,也很难避免泛在网络环境下个人数据使用对个人权益的侵害,最多只能是有限度的减轻。我们的隐私观也面临迭代升级:个人隐私控制的核心不是信息控制而是识别控制,只要不识别,个人数据就是可处理的;[①]只要识别性处理是正当的,个人数据的处理即是符合个人隐私期待可以接受的。因此,应当将个人信息处理限定于以识别分析为目的的个人信息处理,以此建立个人信息处理的程序和规则,保护个人信息处理中的合理个人权益。

这样的定位符合个人信息处理的实质标准。按照最初的立法者们的设想,只有对个人权益有实质影响的个人信息处理才宜纳入法律干预。在今天看来,并非所有的使用计算机处理个人数据的行为都会对个人权益产生影响,起码可以排除一些使用计算机处理个人数据的行为,如一次性使用个人数据的情形和非基于数据运算、加工分析而使用数据的情形。因为这些信息处理行为不存在长期和重复使用或运算处理的特性。甚至也可以排除基于法定的信赖或保密义务控制个人数据的情形,因为既有法律已经给予个人足够的保护。[②] 这样就可以将个人信息处理行为与个人信息的基本使用行为区分开来。个人信息使用是一个远大于个人信息处理的概念。个人信息的使用包括个人社交、公共事务执行、业务联络、具有保密义务关系下的个人信息的使用;而个人信息处理应当专指使用计算机等智能工具大规模、长期存储和多次使用个人信息,是一种必须汇集一定量的信息并对个人进行分析,然后再应用于决策的行为。如果能够构建狭义的个人信息处理概念,那么我们就可以避免个人信息保护法的泛化。

四、个人信息处理的内涵

将个人信息处理定义为为识别分析而使用个人信息的行为,以识别分析限定使用的内涵,从而使个人信息保护法规范的使用区别于一般意义上的使用。这样的定义有利于区别个人信息保护法的规范对象,将碎片化的使用、具有保密义务情形下的知悉甚或存储个人信息等行为排除在个人信息保护法的规范之外。

这一定义的关键在于识别分析。识别分析即是利用数据分析个人特征并做出影响个人或群体决定的行为。识别分析属于数据分析的范畴,属于从数据中获取行动知识的行为,识别分析的目的在于洞察个人并获得关于个人或群体的知识。识别分析通常采取描述性分析、预测性分析、处方性分析等方法对个人信息进行处理或运算,洞悉某人的特性(获取某个方面或全面的个性、特征、偏好等知识)或预测未来行为,并在此基础上决定是否要采取行动、采取什么行动。这里的行动包括推送信息、联络甚至发出要约,抑或是对犯罪嫌疑人的抓捕。这样的识别分析反映了个

① 《欧盟统一数据保护条例》第 11 条(无须识别数据主体的数据处理)确立了一个原则,即不识别或无须识别数据主体的数据处理不适用个人数据保护法。

② 金融机构、医院、医生、治疗专家、律师事务所、企业等都涉及采集、管理或使用客户个人信息,对于个人信息的保密或使用通常由行业准则或特别法律来规范。当然,如果超出原业务范围对用户进行识别分析,那么就属于个人信息保护法意义上的个人信息处理,就要适用个人信息保护法予以规范。

人信息处理技术的变化。如前所述,在40年前,个人信息处理的核心是收集和存储关于个人的数据,形成关于个人的电子文档,重复利用该文档作出关于个人的决定。今天,个人信息处理的核心是基于泛在网络产生的数据,运用大数据分析技术进行识别分析。这样的识别分析给个人尊严、隐私带来的危害是我们的法律应当关注的,也应当是个人信息保护法应当解决的核心问题。

当个人信息处理的概念进入法律后,就已经脱离技术意义上的具体处理行为(操作、运算)的含义,而抽象成为涵摄一切影响主体权益的个人数据使用行为。以识别分析为核心界定个人信息处理的目的仅在于明确个人信息保护法规范的范畴,为了实现对处理行为的规范,还应细分具体的处理行为。在这方面,《草案》对处理行为的列举已经摒弃《条例》无意义的广泛列举,并接近个人信息处理的实践。基于对识别分析的定位,我们应当围绕识别分析的实践来构建和区分具体的信息处理行为。为此,笔者建议将处理行为细分为收集(获取)、控制、分享(提供或披露行为)、分析和应用5种行为。识别分析意义上的处理是以分析为核心的数据活动,分析是对特定数据进行操作、运算的处理,形成关于某个人某个方面的描述、预测或结论;分析形成的结论要应用于决策,针对该人采取个性化商品推送或服务等行动。分析需要获取(收集)数据并持有(控制)数据,并且在这个过程中少不了信息分享行为,以涵盖信息在不同控制者之间的流动。因此,处理活动还应当包括收集、控制和分享3种行为。由此,将个人信息处理划分为信息收集、控制、分享、分析和应用5种行为,涵盖了个人信息利用的全过程。[①] 这5种子行为是从社会效果方面对处理行为的具体分类,既避免了《草案》从纯粹技术方面所下的定义(如存储、传输),又避免了有可能重合或模糊的"使用"概念。

收集是个人信息处理的起点。收集既包括从个人处直接收集(采集),也包括从特定信息控制者处间接收集和从公开渠道获取。最初的个人信息保护法只关注从个人处直接收集数据,但现在间接获取和从公共渠道获取已成为识别分析数据的主要来源。在这两种情形下,个人知情或同意几乎无法实施,如何防范这两种收集方式带来的风险是如今个人信息保护法必须关注的。这预示着我国个人信息保护法对个人权益保护的重点要从对收集进行控制转向对使用进行控制。

控制即实际控制和管理数据,在技术上表现为存储和管控数据。控制以存储为常态,也包括能够调用数据。按照立法者制定个人信息保护法的理念,保存和控制数据必须符合初始收集目的的需要,当该目的完成或实现,那么就不需要继续存储数据。在丧失法律基础的时候,须删除数据,删除数据可以解释为丧失控制。我们可以用更具有规范意义的控制来涵盖存储、删除这样的行为。在过去,收集和存储数据、形成电子文档或数据集是处理分析的前提,而在现代技术条件下,许多数据分析是即采即用(分析),不需要存储,许多数据分析工具(如联邦学习)可以实现仅运算分析而不获取和存储数据。这些都会改变对个人信息存储的认知,影响对控制(存储)行为的规范。

分享是信息控制者向他人提供数据,包括披露(向特定人提供)和公开(向不特定人提供)。这里的分享包括《草案》涉及的提供和公开两种行为。有分享才有个人信息的间接取得,但既有

① 笔者之所以没有将"使用"作为一种子行为,是因为任何子处理行为都是使用,并且处理本身也是使用;否则,将无法清晰地界定一种行为。

个人信息保护法多不涉及分享规范,甚至不承认信息控制者的分享权利。例如,依据《条例》序言第 50 条和第 2 章第 6 条的规定,数据控制者只能在初始目的(取决于收集时约定或法定目的)的必要范围内使用或再使用(包括提供给他人),超出该目的范围的再使用将丧失合法性基础。虽然《条例》旨在促进个人数据在欧盟境内的自由流通,但似乎仍然坚持个人"决定"流通,而不是数据控制者在确保主体安全前提下的主动提供或分享。单纯靠目的限定原则来限制数据的流动已经不符合当今个人数据利用的实践,①必须同时承认去标识后的个人信息是可分享利用的,但须通过个人信息保护法区分不同的场景,明确是否需要获得信息主体的同意。② 同时,信息控制者(处理者)应承担分享利用的责任,以建立确保个人信息安全的信息流通利用秩序,为个人信息间接取得(合法流通)提供合法路径,解决个人数据再利用的秩序问题。

分析是最为重要的信息处理行为。分析是对数据进行匹配、组合从而形成基于不同分析目的的数据集,并通过运行算法或分析工具的挖掘和预测揭示出个人行为、社会关系、个人偏好和身份特性等。人工智能系统是无限利用数据的分析方法,具有较强的预测和推算能力,给人的隐私或尊严带来新的威胁。算法本身具有不可解释性,算法的规制成为个人信息处理规范的重要内容。如何确保数据集的全面正确和算法的透明或可解释、防范算法歧视是规制分析行为的重点所在。

应用是基于分析结论(画像、预测、推论等知识)作出决策,该决策对个人、群体均会产生影响甚至产生社会后果。应用是依据分析结果进行行动,如向目标人群发送商业信息或者信息内容。需要指出的是,在人工智能应用中,大数据分析和应用是瞬间完成的,并不存在明确的分析和应用两个阶段。先进的数据分析治理必须考虑算法的迅速性和无缝隙迭代性。③

上述 5 种子处理行为既可以看作识别分析行为的 5 个步骤,也可以视为个人信息处理的 5 种行为。每一种行为均涉及技术应用,但我们不从技术方面,而从社会效果方面概括,使其具有规范价值。个人信息保护法需要分析这 5 种行为对个人权益的影响并从整个社会经济活动的需求出发来规范这 5 种行为,针对具体的个人信息处理行为设置条件和程序,建立正当的个人信息处理原则性规范。

---

① 目的限定原则包含两层具体的内涵:(1)数据控制者只能基于收集之初确定的具体、明确、合法的目的收集个人信息,(2)收集后不能再做基于与收集时所确定之目的不相兼容的其他目的的处理。这意味着,只要在初始确定的目的范围内或与初始目的相兼容,就可以对数据再使用甚至对外提供;如果基于初始目的以外的数据处理与初始目的相兼容,那么无需再获得新的合法性基础。个人信息保护法对个人主体权利保护的基本理念是:只要在主体同意的目的范围使用,个人数据的处理就被认为在个人意志控制之下,就可以避免个人信息被滥用的风险。但是,这种观点已被实践证明,个人没有办法判断和控制信息处理者的使用情况,并且与服务(或交易)捆绑的同意也无法反映主体的真实意愿,反而使所谓的个人控制流于形式。

② 当不需要识别身份时,则不需要同意;当需要识别身份时,则需要取得主体的同意。如果不区分应用场景,一律要求去标识化的个人信息处理仍需取得主体的同意,那么个人信息处理者就没有动机仅获取去标识化的个人信息,主体的个人信息被泄露、滥用的风险反而会增加。

③ See Advanced Data Analytic Processing－2019 UPDATE, Prepared by Paula Bruening for the Information Accountability Foundation, http://informationaccountability.org/wp－content/uploads/Advanced－Analytics－2019－004－1.pdf, 2020－11－18 .

五、结　语

个人信息处理是个人信息保护法的基石性概念,在个人信息保护法研究中占有重要的地位。从源头上看,个人信息保护法旨在保护个人信息处理中的个人权益不受侵犯,因而个人信息保护法应围绕个人信息处理的规范展开。个人信息处理成为个人信息保护法的基本范畴,同时对其本身的定义方式也关系到对个人信息处理的规范模式。《指南》的立法者没有把计算机应用于个人数据的行为概括为数据处理行为,从而建立了个人数据处理的一般规则。《公约》及其之后的欧盟个人信息保护法开启并引领了抽象规范模式,对计算机导致的个人数据使用行为进行概括和抽象,建立了个人数据处理的一般原则。这一传统为欧盟立法所继承和发展,形成无所不包的个人数据处理概念,将所有的可能触及数据和利用数据的行为包括在内,导致个人信息保护法的规范对象和适用范围泛化,背离了个人信息保护法防范个人信息处理可能引发的侵害个人权益风险的目的,最终导致法律对社会的过度干预。

作为源自信息技术应用的一个概念,个人信息处理进入法律范畴之后,承担着两项规范功能:一是界定个人信息保护法的适用边界。将对个人权益有实质影响的个人信息处理行为纳入法律规范,避免法律对一切个人信息使用行为的过度干预,也划分了个人信息保护法与其他法律之间的界线。二是规范行为。以信息处理术语体系为基础,构建个人信息处理的行为规范。在学习和移植欧盟个人数据保护法的过程中,个人信息保护法被简单地理解为个人数据保护法,而不是个人信息处理中的个人权益保护法,甚至将基本权利层面的主体自治、自决、自由简化为私法意义上的个人信息属于个人、由个人决定,导致个人信息私有化,更背离了个人信息保护法的宗旨。将个人信息保护法理解为为个人信息处理中的个人权益提供保护,并合理界定个人信息处理行为,是我国个人信息保护立法的基础工作。

《草案》第 1 条将“规范个人信息处理活动”作为法律规范的目标,表明我国个人信息保护法的定位是正确的。但是,《草案》关于个人信息处理的定义既没有反映个人信息处理规范的本义,又有对《条例》之个人数据处理定义的简单模仿之嫌疑。为此,笔者建议将个人信息处理定位于以识别分析为核心或目的的个人信息使用行为。这样的定位既坚持了个人信息保护法 40 年前的立法者确立的技术和法律两个标准,将个人信息处理定位于识别分析处理之上,又将一般的个人信息处理排除于个人信息保护法的规范范围,而只关注大数据时代的大数据分析、人工智能技术对个人权益有重大明显影响的个人信息处理行为。

在以识别分析为核心来界定个人信息处理边界的同时,笔者还希望以识别分析为核心构建个人信息收集、控制、分享、分析和应用这 5 种行为的规范。这 5 种行为是以信息生命周期为基础,从对个人权益影响的维度切分出的个人信息处理行为。这 5 种行为全面反映了现今个人信息使用的社会现实,但已经不再是技术语境下的信息处理概念,而是具有法律规范价值(对个人权益有影响)的法律术语。从个人数据的社会应用维度来定义个人信息处理的具体行为,不仅有利于个人信息保护法发展出具体的行为规范,而且能够回应时代对个人信息保护法的需求。

如果说 40 年前的立法者只是关注因信息技术带给个人信息的“被处理”而对个人权益产生的影响的话,那么今天的识别分析已经成为支撑各种决策智慧或知识的生产活动。数据应用在过去只是一种少量(或少数主体)应用的现象,但今天已经演绎为支撑经济、社会治理、学术研究

等的普遍应用。数据分析在过去是基于以个人提供为主的小数据分析,但今天已经演绎为基于大数据的分析活动。在数据成为资源的背景下,个人信息处理演变为一种经济活动。在这样的背景下,我们就不能再单纯地从对个人权益影响的维度来规范处理行为,而必须对合理切分出的具有社会后果和意义的行为加以规范,以使其具有规范效果。

如此制度设计的真正用意是,彻底地将个人信息保护法定位于个人信息利用的行为规范。在 40 年前,个人信息保护法关注的主要是个人提供给各种组织的个人信息在长期存储下因重复或长期积累使用给个人带来的危害,由此建立了以个人控制为主导思想的个人信息处理规则,其核心是在约定或法定目的的必要范围内使用数据,达到对个人数据利用进行控制的目的。如今,识别分析是基于泛在网络产生的数据展开的,间接甚至非接触取得数据已成为主流,以智能分析工具为工具,我们应将个人信息处理规制的重心置于识别分析行为和后果的规范上。

在这样的时代,识别个人信息的范围没有边界,能否识别一个人取决于用于识别的数据量和识别分析的方法,而不能事先判断。虽然在 40 年前个人信息处理给人带来的危害需要赋予个人对个人信息的一定控制,但现在可识别个人的信息已经沦为泛在的存在,无法判断其边界,个人也无能力实现对个人信息的控制。故通过赋予个人对个人信息的控制权来预防个人信息处理中对个人产生的危害已经证明无益于主体权益的保护。设置个人对泛在信息的控制不仅对个人信息保护不具有实际意义,并且信息收集者也将徒增合规成本。有效的个人控制实际上应当转向对个人信息识别行为的控制。在这样的思维下,拒绝被识别分析、拒绝识别分析约束在个人信息保护立法中就具有特别意义。既然个人信息保护法规范的对象是个人信息处理行为,那么个人信息保护法就应当围绕个人信息的利用行为构建信息处理者与信息主体之间的权利义务关系,防范个人信息处理行为侵害主体权益的风险,并在侵害行为发生时予以纠正和救济。个人信息保护法需要在此种意义之上理解和设计信息主体的权利和信息使用者(处理者)的义务,在限缩个人对个人信息的控制范围的同时,强化个人对个人信息处理行为和分析结果异议和拒绝的权利配置。

总之,我们应以当今信息技术应用对主体权益的影响为脉络概括个人信息处理的内涵,构建具有规范意义的处理行为,使我国个人信息保护法的制定能反映当今的信息技术水平和个人信息处理现状。这是基于个人信息保护制度创制的基本目的和基本理念出发,直面我国数字经济发展问题的一种制度设计,而不是直接移植域外制度和规则的结果。只有在精准科学的概念体系下,才能平衡个人信息上的个人权益与社会利益,建立公正有序的个人信息利用秩序,搭建个人信息治理框架,引领数字经济健康有序的发展。

责任编辑 何 艳