论个人信息保护的目的

——以个人信息保护法益区分为核心

高　富　平*

摘要:近年来,我国颁布了多部有关个人信息保护的法律,但相关立法的定位存在偏差。个人信息与个人(数据主体)的联系仅在于该信息可以识别某人或与某人存在联系,而这不足以使个人控制该信息或使其归属于个人支配。事实上,个人信息保护发端于个人基本权利(人权)保护,保护的是人的尊严所派生出的个人自治、身份利益、平等利益。个人信息不等于隐私,个人信息保护规范不等于隐私保护规范,但隐私保护是个人信息利用的前提,也是个人信息保护法的重要内容。个人信息安全有别于公法保护的安全利益,前者只是一种个人权益,由个人信息保护法调整;而后者属于公共利益,由刑法保护。只有区分需要保护的这些法益,才能正确地理解和移植源自西方社会的个人信息保护制度,正确地建构我国个人信息保护规范。

关键词:个人信息保护　　信息隐私　　信息安全　　人的尊严

伴随大数据时代的到来,个人信息(又称"个人数据",本文混同使用)保护问题成为热点话题。自2012年全国人民代表大会常务委员会发布《关于加强网络信息保护的决定》之后,个人信息保护逐渐成为许多法律保护的内容,如《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》)等。对个人信息保护,这些法律确立了一个基本规则:未经同意不得收集和使用个人信息。[①] 该规则暗含着个人对于个人信息具有支配权,其结果自然是:未经同意收集和使用个人信息即属于侵权。2014年6月,最高人民法院公布《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》(以下简称《信息网络侵权规定》),试图将侵犯个人信息作为独立的侵权类型,公开个人信息致人损害即构成侵权。[②] 以公开作为侵犯个人信息的加害行为,暗示着《信息网络侵权规定》将个人信息保护等同于隐私保护。个人信息保护是否独立于隐私保护,成为个人信息保护的基础性问题。在社会对个人信息保护的呼声日渐强烈的背景下,个人信息保护是否要明确为一种具体人格权成为《中华人民共和国民法总则》(以下简称《民法总则》)制定过程中的争议焦点。但最终颁

* 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(13&ZD178)、国家社会科学基金项目(18ZDA145)

① 《关于加强网络信息保护的决定》第2条第1款规定:"网络服务提供者和其他企业事业单位在业务活动中收集、使用公民个人电子信息,应当遵循合法、正当、必要的原则,明示收集、使用信息的目的、方式和范围,并经被收集者同意,不得违反法律、法规的规定和双方的约定收集、使用信息。"《中华人民共和国消费者权益保护法》第29条第1款规定:"经营者收集、使用消费者个人信息,应当遵循合法、正当、必要的原则,明示收集、使用信息的目的、方式和范围,并经消费者同意。"《中华人民共和国网络安全法》第41条第1款规定:"网络运营者收集、使用个人信息,应当遵循合法、正当、必要的原则,公开收集、使用规则,明示收集、使用信息的目的、方式和范围,并经被收集者同意。"

② 《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条规定:"网络用户或者网络服务提供者利用网络公开自然人基因信息、病历资料、健康检查资料、犯罪记录、家庭住址、私人活动等个人隐私和其他个人信息,造成他人损害,被侵权人请求其承担侵权责任的,人民法院应予支持。"

布的《民法总则》只是宣布个人信息应当受法律的保护,并未将个人信息明确为一种具体人格权。[①]

那么,个人信息保护与隐私保护是否为一回事,擅自公开个人信息或者未经同意使用个人信息是否都构成侵权?这涉及个人信息的法律定性以及个人信息上需要保护的法益问题,而回答这个问题又关系着对个人信息保护的理解和个人信息保护法的定位。本文首先从个人信息的社会功能角度分析个人信息的法律属性,然后检讨国际社会现有的个人信息保护立法,探寻个人信息之上法律所保护的法益,以准确理解个人信息保护及其立法目的。在此基础上,提出我国个人信息保护应有的法律定位。

一、个人信息及其法律属性

个人信息是指可识别具体个人(仅指自然人)的信息。个人信息概念强调"识别性",凡是能够识别特定个人的信息,无论是直接识别还是间接识别特定个人的信息,均为个人信息。在美国,个人信息被称为"个人可识别信息"(personal identifiable information,简称 PII)。[②] 欧盟立法对个人数据的定义也强调可识别个人,《统一数据保护条例》[③](以下简称《条例》)将个人数据定义为"与已识别或者可识别数据主体相关的任何数据"。

理解个人信息,关键是要弄清"识别"和"识别个人"。识别指的是根据与特定人有关的信息来认识、辨识或指认该特定个人,所依赖的信息通常是个人特有的或描述个人属性、特征的信息。识别的结果就是认出某人或者描述出某人的基本特征,英文统一表述为"identity"。Identity 既有个体身份的含义,也有个性特征的含义,表述一个人区别于另一个人的个性或"体征"。在汉语中,并没有准确的对应词语,一般译为"身份"。实际上汉语中的身份一词通常指不同社会地位或社会关系,而不包含个性特征的意思。然而,在研究个人数据保护法时,必须在广义上使用识别和识别的结果——个体(identity),否则就无法理解个人数据保护法规范的意义。

具体地说,个体本身有两层含义:一是个人身份,用来表示你是谁,最直接识别一个人身份的就是姓名,除此之外还包括与姓名直接联系起来的个人属性或标识符(如身份证号、工作单位、职称、职位等);二是个性特征,用来认知你是一个什么样的人,一般通过你的喜好、习惯、倾向来描述。[④] 在本文中,前者为识别身份,而后者为识别个体特征。个体特征的识别可以不识别身份(如只识别到一个设备 ID、IP 地址等),也可以与特定人的身份识别联系起来,对一个人进行完整识别。在社会交往中,身份识别是重要的。一个人如果没有确定身份,那其所确立的一切社会关系就变得极其不稳定;在弄清楚对方是谁之前,与一个身份不明的人打交道,也是危险的。在这个意义上,"识别"是以识别个人身份为核心的多信息维度个体识别体系,而姓名是身份识别的核心标识符。

在过去的社会环境中,我们是先识别一个人的身份(姓名)再进一步去了解某个人的特征;而在大数据环境下,我们可以通过了解一个人的个人属性(如职业、经历等)、网络浏览记录等数据来认识某个人的个性特征,然后再识别某个具体个人的身份(姓名),将个性特征联系到某个具体个人。例如,通过电脑或手机等终端设备可以识别使用该设备的用户,即使不知道用户的姓名,也可以达到认识该用户甚至与他(她)联系的目的。当然,在实名注册的情形下,识别用户实际上就是直接识别到该用户的身份。因此,在网络社会中,识别的基本含义就是通过分析关联数据以识别某个用户的个性特征(至于是否能识别用户的身

① 《中华人民共和国民法总则》第 109 条确立了一般人格权:"自然人的人身自由、人的尊严受法律保护。"第 111 条确立了具体人格权:"自然人的个人信息受法律保护。任何组织和个人需要获取他人个人信息的,应当依法取得并确保信息安全,不得非法收集、使用、加工、传输他人个人信息,不得非法买卖、提供或者公开他人个人信息。"

② Schwartz, Paul M. and Solove, Daniel J., Reconciling Personal Information in the United States and European Union, 102 California Law Review, 877 (2014).

③ 全称为《联盟议会与联盟理事会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 2016/679/EU 号条例》。该条例经过两年的过渡期,于 2018 年 5 月 25 日生效。

④ Identity 在英语语义中包含有个体特性、个人属性、身份、同一性等不同说法,在中国法律体系中,笔者以个人身份理解之,此身份既非身份法上的特殊身份概念,也非简单文意上的个人社会地位的象征,而是包含有个人特征和属性内容的身份概念。

份，则取决于所掌握的数据是否匹配或关联到某具体的个人）。

在一般意义上，“识别”与“通信”或“联络”无关。住址、电话、电子邮件、微信账号等在识别中所担任的角色，仍然是识别该用户是谁，识别本身并不导致与该用户通信、联络或对其进行推销甚至实施诈骗。联系被识别的人，不属于识别行为，而属于个人信息的利用行为，其本身不包含在识别范畴之内，也不是可识别个人身份的个人信息所导致的必然结果。

因此，个人信息就是任何能够认知、辨析、了解特定个人的信息。个人信息强调的是“可识别”，一切能够关联到某个人或了解某个人个性特征的数据都可以归入个人信息的范畴，并且这些信息在大多数情形下都要与其他信息结合起来才能识别出具体的某个人（即所谓的间接识别），而结合的信息越多，识别的结果就越准确和全面。①

个人信息是社会交往和社会运行的必要工具或媒介。工具性质决定了个人信息的社会性、公共性。个人需要运用一些信息标识其为某人，而社会也需要利用信息来识别某个特定个人。首先，个人需要利用可以识别自己的符号，向社会推介、展示自己，需要利用它来开展各种活动，将活动结果归属于其本人。在这一过程中，个人信息必然要被公开、外泄，为其他主体所掌握。其次，从社会的角度出发，社会也需要利用个人提供的个人信息和散落于各处的、可被搜集掌握到的有关个人信息来了解、判断某个人。前者是个人（数据主体）主动利用个人信息的过程，后者则是由社会主体（收集和使用个人数据的主体，称为数据控制人）对来源于个人（主动提供或散落于社会中的）的数据的利用。这两个方面构成个人信息应用的基本场景。

基于此，个人数据保护所面临的核心问题就是：这些可识别个人的数据是否归属于个人或者由个人控制，社会主体是否必须经过个人的同意才能对其进行识别？笔者认为，个人信息本身只是一种可以识别某个人的客观事实，这种客观事实并不当然地让个人拥有或控制个人信息。个人信息与个人的联结点是：这些信息指向或描述某个人，可以将之概括为该信息与某个人有联系、有关联。但是，纯粹与特定个人有联系不足以使个人对该数据具有支配利益。因为这种关联只在于信息所表达的意义、内涵，而不在于信息（这里使用数据更为恰当）本身。

自古以来，数据或信息本身一直是处于公共领域的公共素材或材料，是任何人均可以使用的资源，个人信息也不应当例外。② 当信息用来标识、记录、描述某个人时，并不因此而使该信息（数据）归属于该人，这些信息仍然可以用来标识、记录、描述其他人。数据或信息的公共性、可共享性，决定了个人数据本身的公共性。个人最多可以控制不联系或如何联系，但不能控制信息本身。例如，一个人购买了减肥霜，传递出的信息是他可能具有肥胖的体征，而购买减肥霜的消费记录虽然与个人有关，却不一定导致该人对该记录享有支配、控制的权利，也不一定导致别人不再使用减肥霜等字符的后果。因此，网络、传感器等记录的与个人有关的活动、浏览记录，只是与特定个人产生了联系，赋予该信息某种含义，而不足以使该个人对该记录信息拥有排他支配权。

即使直接可以标识个人身份的信息，个人也不享有支配权。以姓名为例，姓名是最直接标识自然人的标识符（文字），它具有等同于本人或代表本人的功能，虽然法律赋予个人以姓名权，③但并不包括对姓名信息（符号）的支配权。姓名权主要保护个人的两种利益：其一，个人有独立命名的自由，不受任何人干涉。它所保护的是人格独立和自由，而不是个人对自己姓名的垄断，阻止别人使用相同名字（文字）。其二，个人有使用自己姓名的权利。姓名的功能在于让一个人在社会活动中标识自己，将社会活动的结果归属于

① 参见王秀哲：《我国个人信息立法保护实证研究》，《东方法学》2016年第3期。

② 信息的产生和再生的成本很低，信息本质上不具有排他性，加上排除他人使用信息的成本过高，因此应将信息视为公共资源。See Joseph E. Stiglitz, The Contributions of the Economics of Information to Twentieth Century Economics, 115 The Quarterly Journal of Economics, 1441－1478(2000).

③ 《中华人民共和国民法通则》第99条规定：“公民享有姓名权，有权决定、使用和依照规定改变自己的姓名，禁止他人干涉、盗用、假冒。”

其本人,如在作品上署名、取得各种荣誉等。法律保护每个人正当使用自己姓名的人格利益。因此,姓名权本身并不是对特定文字符号的支配权,法律只是保护个人排除他人干涉、冒用、盗用姓名,但不能排除他人使用相同的姓名。简言之,姓名权本质上是对人格利益的保护,而不是对姓名本身的支配权。

相同的原理也适用于与特定个人有联系的信息。与特定个人有联系并不足以导致个人对该信息的垄断,法律没有理由赋予个人对个人信息的排他支配权。恰恰相反,一个人的联系方式、过往经历、性格习惯等一直被认为是认识和了解一个人的途径。在社会中,一个人没有权力阻止别人了解他,也没有权力阻止他人收集其个人信息,对其个人信息进行分析,最终对其作出评价。一个人无论是开展社交活动、商业往来,抑或是接受公共服务、升学就业,都要提供其基本的主体信息。离开个人信息,一个人不能标识自己,社会公众也无从判断和认知谁是谁。因此,个人信息本身具有社会性和公共性,不应当仅因某些信息可识别或联系某个人而赋予该人对其个人信息的某种支配权。个人信息的识别功能决定的是个人信息本身的社会属性而非个人属性,个人对个人信息并不当然地享有支配性权利。因此,对于个人信息保护而言,需要寻找其他的法益来奠定个人保护的正当性基础。

二、个人信息保护的基本目的:保护人的尊严

在寻求个人数据保护的法律理由方面,权威的国际立法文件和主要国家的立法均将个人数据保护定位于对人的尊严的保护,认为在个人数据上存在一个自然人最值得受法律保护、最重要的法益,即人的尊严。人的尊严被认为是最基本的人权,因而世界各国基本上都认为个人信息保护的目的在于对人权或基本权利的保护。

联合国 1948 年发布的《世界人权宣言》第 12 条被普遍视作保护个人信息的法律渊源。[①] 也就是说,个人信息保护源自对个人私生活的尊重和个人事务自决(自由)原则。欧洲委员会于 1981 年发布了《个人数据自动化处理中的个人保护公约》(以下简称《公约》),这是世界上唯一的个人数据保护公约。[②] 《公约》前言明确表示,其目的除了实现各缔约国法治统一外,还有“人权和基本自由”的统一;目的在于在个人数据跨境流通越来越频繁的情形下,“扩大对个人的权利与基本自由尤其是隐私权的保护”。《公约》2012 年修改后,取消了“尤其是隐私权”,表述为“捍卫每个人的个人尊严和保护基本人权和基本自由,尤其是通过对其数据及其处理的控制权来实现保护”,也就是借助“个人数据及其处理的控制权”手段,实现“保护基本人权和基本自由”的目的。这是关于个人数据保护目的最权威的表述。

《欧盟基本人权宪章》(以下简称《宪章》)明确地将“个人数据保护权”作为一项独立的基本权利加以保护。《宪章》第 8 条规定:“人人有权保护涉及自身的个人数据”。而欧盟也正是在人权保护层面上推动成员国落实《公约》,并于 1995 年发布了《数据保护指令》[③](以下简称《指令》)。经过 20 年左右的实践,为消除各国立法的不一致和保护水平的差异,欧盟 2016 年 5 月颁布《条例》,以替代 1995 年的《指令》,成为在全欧盟范围内具有直接效力的法律。《指令》和《条例》在立法目上的表述基本一致,均肯定“保护自然人的基本权利和自由”,只是“尤其”表述不一致,由“尤其保护有关个人数据处理中的隐私权”改为“尤其保护个人数据的权利”。[④]

由此可见,个人数据保护的目的是人权法或宪法意义上的“个人基本权利和自由”,它最终根源于对

① 该条规定:“任何人的隐私、家庭、住宅和通信不受任意干涉,对他的荣誉和名誉不得加以攻击。人人有权享受法律保护,以免受这种干涉或攻击。”

② 欧洲委员会(Council of Europe)于 1981 年在斯特拉斯堡通过了《个人数据自动化处理中的个人保护公约》;1999 年,该公约作过小幅修订,2012 年该公约进行更新修订,更名为《个人数据处理中的个人保护公约》(Convention for the Protection of Individuals with Regard to the Processing of Personal Data)。欧洲委员会共有 47 个成员国,该公约也邀请欧洲委员会以外的国家加入,目前有 45 个成员国已经批准该公约。

③ 全称为《欧盟议会与欧盟理事会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》。

④ 两个文本的对应条款为:《数据保护指令》第 1 条第 1 款:“成员国应当依据本指令保护自然人的基本权利和自由,特别是有关个人数据处理中的隐私权。”《统一数据保护条例》第 1 条第 2 款:“本条例旨在保护自然人的基本权利和自由,尤其保护个人数据的权利。”

“人的尊严”(human dignity)[①]的保护。[②] 在欧洲,“人的尊严不仅是一项基本权利,还是所有基本权利的基石”,“人的尊严是本宪章所赋予的各项权利本质的一部分”。[③] “个人数据保护权”便是“人的尊严”基本权利项下的一项子权利。

“人的尊严”源自人应当被独立、平等、有尊严地对待的普遍价值观。在法律上,我们往往将其具体化为特定法益,如“独立”“自由”“平等”。这些法益还会衍生出不同的表述,如“人格独立和自由”也被表述为“个人自治”。个人自治是指“对人的行为能力(成熟的或未成熟的)的一种复杂假设,该能力确保人可以发展并且按照高层次的行动规划,即严于律己的目标,来选择自己的人生及生活方式。”[④]个人自治蕴含着一个人能够自行做出决定并明确其内心意愿的能力,即个人行为自治,具体指个人能够在精神上自由地作出有意识的选择(内在自由),并且不受来自外界对其自由独立作出选择的限制。这就涉及自治的两个方面——选择自由和行为自由。由此可见,独立、自治、自由具有相同的含义,核心是个人意志自由。

人的尊严的另一重要含义是“平等”。平等的基本含义是每个人被视为独立人格而被同等对待。平等往往与不歧视联系在一起,平等和不歧视不仅是一项法律的基本原则还是人的一项基本权利。在国际法层面,平等主要强调不得因种族、肤色、性别、语言、宗教、民族等因素对公民进行区别对待;而在国内法层面,主要强调法律面前人人平等,确保人人能够平等地行使法律权利,防止公民在经济、政治、文化及生活各方面的权利受到歧视。

我们不能抽象地讲保护个人信息是保护个人基本权利、保护自由和平等,而是要找到个人信息与这些普遍价值的联系,寻找这些普遍价值与私人权益的联系。笔者通过检讨国际社会重要个人数据保护立法,将个人信息上存在的受法律保护的基本权益归类为以下三个方面:

1. 个人自治(自由)

个人虽然不能阻止他人使用其个人信息,但是,由于个人信息关涉到个人利益,因此其应当属于个人事务,属于个人独立自主决定的范畴。1983 年德国联邦宪法法院在“人口普查案”中确立的“信息自决权”,开启了个人有权决定个人数据如何被使用的先河。[⑤] 个人信息自决权的逻辑在于,个人信息属于个人事务,个人对于如何使用其个人信息享有自我决定的权利。个人信息自决权在美国也被演绎为个人信息控制权,以解决信息技术应用后所带来的个人对其个人信息的“失控”所引发的权利侵害问题,但这种演绎正在被纠正。[⑥]

个人信息自决权实际上是为了防止个人信息“被处理”。既然个人是独立主体,个人有权决定个人事务,那么就应当自主决定,而不是被决定。在个人数据保护立法中,一个普遍认可的规则是“个人享有不受自动化处理结果约束的权利”。[⑦] 之所以会特别肯定这一权利,是因为要保护个人免受“被决定”之侵害。自计算机投入使用,个人在社会交往过程中提供的个人信息被获取机构留存下来的,该机构可以不经过个人同意再次使用这些信息;尤其随着网络普及应用,个人行为可以随时随地全面地被记录、收集和再利用。

---

① 该术语通常译为“人格尊严”。笔者认为,在人权法语境中,应当表述为“人的尊严”更为准确和全面。

② 参见张新宝:《从隐私到个人信息:利益再衡量的理论与制度安排》,《中国法学》2015 年第 3 期。

③ Article Based Legal Explanation of the EU Charter of Fundamental Rights, http://www.eucharter.org/home.php? page_id=8, 2018-04-05.

④ Richards, D. A. J. , Rights and Autonomy, in John P. Christman ed. , The Inner Citadel: Essays on individual autonomy, Oxford University Press, 1989, p. 205.

⑤ 该案被认为以司法判例的方式确立了宪法上的“信息自决权”(德文 Recht auf informationelle Selbstbestimmung,英文 right to informational self-determination)。有学者指出该案是针对国家对于个体信息的收集和对于个体信息的威胁,德国联邦法院并没有将这种个人信息权或个人信息自决权扩大为一种私法权利。参见杨芳:《个人信息自决权理论及其检讨——兼论个人信息保护法之保护客体》,《比较法研究》2015 年第 6 期。

⑥ See Fred H. Cate, The Failure of Fair Information Practice Principles [from Consumer Protection in the Age of the Information Economy (2006)], http://ssrn.com/abstract=1156972, 2018-06-25 ; Amber Sinha and Scott Mason, A Critique of Consent in Informational Privacy, http://cis-india.org/internet-governance/blog/a-critique-of-consent-in-information-privacy, 2018-06-25.

⑦ 《个人数据处理中的个人保护公约》第 8 条 a 项赋予数据主体“不受仅基于数据自动化处理而不考虑其主观意识而作出的对其产生深刻影响的决定的制约”的权利。《数据保护指令》第 15 条和《统一数据保护条例》第 22 条都原则上肯定数据主体有权拒绝仅基于自动化处理行为得出的决定的制约。

如果这些机构随意自动地收集个人信息并对个人作出判断或决定,就等于将人(主体)作为被动的可“被处理”的东西,这是对人的独立自主的蔑视,是对人的尊严和自由的侵犯。这一认识正是德国哲学家康德“以人作为目的”观念上升为法律理念的结果。按照上述理念,人本身是目的,人应该自治、自决,凡是与人格形成、发展有关的情事,本人有权自己决定,并在此范围内排除他决、他律或他治。因此,保障数据主体对其个人数据的处理、使用、流通等一系列事务的自主、自治、自决是个人数据保护的应有之义。因此,个人信息自决并不意味着个人对与其有关的信息的排他控制,而是指在个人信息利用方面,个人不是处于被处理的地位,而是主动地知情、参与其中。① 尤其是,我们不能据此认为个人信息自决权是私权体系中的具体权利类型,更不是受侵权行为法保护的民事权利。②

2. 身份(识别)利益

由于身份(以姓名为核心的识别体系)是一个人开展社会活动的前提,也是社会将其活动结果归属于特定主体的工具,身份成为每个人的利益(及不利益)的载体,因此,保护身份实质上就是保护特定个体的利益,因这些利益负载于身份上,故可称之为身份利益。这种身份利益使得个人有权使用标识自己身份的符号开展社会活动并将其活动结果归属于其本人。这是每个人作为一个个体得到社会认可和尊重的基本条件,也是个人从社会获得认知的条件。此类利益包括但不限于:每个人对自己的智力成果署名以表明是其精神产物,有权将自己取得的成绩、资格、荣誉等归属于其本人。以姓名为核心的身份识别体系是一个人在社会中生存的根基,法律需要保护这种身份识别所产生的利益(包括精神利益和经济利益)。

过去一个人对另一个人的评价是建立在社会交往基础上的,所依据的材料和事实既可能源自个人的主动披露,也可能是其行为或生活事实不经意被记录或收集。随着网络、智能设备和数据的深度开发应用,一个人的行为过程、状态均可被记录下来,形成个人全“影像”。在网络环境下,广泛存在和使用的“用户画像”(profiling,或译为“用户文档”)就是企业根据用户网络行为轨迹和状态记录,对其身份、特性等进行描述。商家收集用户的过往记录,形成用户文档,通过文档中的各种信息对个人职业、喜好、性格特征、行为偏好等内容进行分析,形成对特定用户在经济、社会、文化、生理、心理等全方面的特性描述。至于这种描述有多全,取决于企业掌握的该用户的信息多少。这一过程往往发生在用户不知情的情形下,甚至完全是由计算机系统自动收集和分析完成的。这样,个人就会被动地被分析、被描述,并贴上各种“标签”。如果商家利用该自动化分析工具得出的结论不全面、不正确、不符合真实个体的现实情况,那么商家不仅会产生身份认知上的错误,还有可能损害相应个人的名誉,对其人格、信誉等方面产生负面影响。因此,通过利用散落于社会各处的与特定个人有关的信息对其进行错误识别或评价的行为有可能损害个人的身份利益。例如,收集的数据不完整或者已经过时了、分析程序不完善,那么其所得出的结论就不能正确反映数据主体的真实身份特性,导致数字化人格与现实人格不符。因此,数据控制人利用个人数据对特定个人进行识别分析和评价的过程应当要让数据主体知情并参与,给数据主体更正错误的机会,以保持“他知”与“自知”的一致性,以保护个人的尊严和身份利益。

3. 不歧视(平等)

在人权法中,平等要求每个人被一视同仁地对待,不因为个人的外在因素而被歧视。在个人数据保护立法中,平等对待或不歧视也被作为独立的一项法益来保护。这主要是因为,随着计算机的广泛应用,尤其是在网络和移动智能设备全覆盖的今天,收集个人信息的手段方式和个人信息的数量内容都比从前丰富得多,无论个人是否愿意,一切有关其个人生活的信息都有可能被他人掌握。也就是说,在网络环境下

① 国际社会关于个人数据保护立法都强调个人的知情和参与。譬如,2008 年美国国土安全部(DHS)隐私办公室颁布的正当信息通则[Fair Information Practice Principles (FIPPS)]第 1 项和第 2 项原则分别为“透明”和“个人参与”。2011 年美国白宫发布的由网络空间可信身份国家战略 (NSTIC)将“透明”与“个人参与”原则进一步推广至私人领域。《统一数据保护条例》第三章“数据主体的权利”规定了个人数据处理的透明、数据控制者收集信息时应向数据主体提供的信息、访问权、更正权、被遗忘权、限制处理权等保证数据主体对数据处理的知情和参与。

② 参见杨芳:《个人信息自决权理论及其检讨——兼论个人信息保护法之保护客体》,《比较法研究》2015 年第 6 期。

个人很难再有真正的隐私，每个人都变得透明。而这样一个透明的社会，更容易产生深层次的歧视。举例而言，在应聘岗位的情形中，应聘者被了解得越透彻、越全面，在应聘时就越有可能被企业拒之门外，因为即使与招聘要求无关，有些个人情况也会成为企业考量一个人的隐形标准，如性取向、政治倾向、宗教信仰、星座等。

同样的，通过对每个用户进行全面深度的了解，数据控制人还可以制定不同的交易价格。例如，在健康保险领域，根据精准的个人健康状态选择投保人和保险金；在汽车保险领域，根据驾车习惯制定不同的费率；在网络销售领域，根据用户的社会阶层制定不同价格。商品服务个性化定制的时代就是数据分析定价的时代，是基于数据的差异化时代。在数据带给人们精准决定权的同时，如何防止新型歧视也成为数据保护研究者所关注的领域。有学者就认为，个人数据保护法也适用于数据用于个性化定价的情形，此类商家必须遵守个人数据保护法的规则来处理个人信息。[①] 欧洲议会也强调，基于在数据处理的不同阶段进行评价和预测时所使用的数据集和算法存在差异，大数据利用不仅可能侵害个人的基本权利，还会导致具有相同特征的人群被区别对待或被间接歧视，尤其是在获取教育和就业机会方面。[②] 例如，最近热议的大数据“杀熟”，[③]就属于不合商业伦理的一种个人信息利用行为，要在个人信息保护法中增加算法或算法用途说明，满足消费者对个人信息使用及其可能的差异化定价的知情权。[④]

单纯从识别的角度看，个人数据保护立法的基本目的在于规范个人数据的利用行为，防止不当利用行为对个人自治（自由）、身份利益的侵害，同时也防范新型的个人歧视。相比于域外立法，我国立法并没有对个人数据保护的这三类权益进行明确阐释，至少现行个人信息保护立法缺少对这些法益的揭示，而隐私和安全利益反倒成为我国个人信息保护立法的关注焦点。因此，笔者认为个人信息保护与隐私保护以及安全利益之间的关系需要进一步澄清。

三、个人信息保护与隐私保护

个人信息保护与隐私保护有着复杂的联系，这主要是因为不同法域对隐私有着不同的理解，甚至在相同法域隐私规范也不尽相同。在美国，并没有与大陆法对应的人格权理论和制度，而是从个人自由发展出涵盖几乎所有个人权利的隐私概念，因而在隐私保护下讨论个人信息保护，形成美国特有的个人信息保护，即信息隐私（information privacy），[⑤]亦即个人信息保护与隐私保护是一回事。[⑥] 而在大陆法的语境下，隐私只是一种具体人格利益，隐私保护区别于个人信息保护。下文，笔者将结合我国对隐私保护的认知，在大陆法语境下讨论个人信息保护与隐私保护的关系。

在中文普通用语中，隐私指“隐蔽、不公开的私事”或者“不愿告人或不愿公开的个人的私事”。这一基本含义也被援引至法律中，以隐私表示受法律保护的“私事”。《中华人民共和国侵权责任法》（以下简称

① See Zuiderveen Borgesius, Frederik J., Online Price Discrimination and Data Protection Law, https://ssrn.com/abstract=2652665 or http://dx.doi.org/10.2139/ssrn.2652665, 2017－12－15.

② Motion for a European Parliament Resolution on Fundamental Rights Implications of Big Data: Privacy, Data Protection, Non－discrimination, Security and Law－enforcement[2016/2225(INI)], http://europal.europa.eu/sides/getDoc.do? pubRef=－//EP//TEXT＋REPORT＋A8－2017－0044＋0＋DOC＋XML＋VO//EN, 2019－01－07.

③ 有网友自述：其通过某旅行服务网站订特定酒店，自己账号与朋友账号显示的价格不一致，虽然同一天订房，但是相同的房间具有不同的价格；无独有偶，又有网友披露某打车软件对同一出发地和目的地针对不同的账号显示的价格不同，由此引发“大数据杀熟”的讨论。参见袁晗：《“大数据杀熟”真的存在吗？听听甲方乙方怎么说》，http://www.xinhuanet.com/talking/2018－03/30/c_129841126.htm，2018－04－05。

④ 参见高富平、王苑：《大数据何以“杀熟”？》，《上海法治报》2018年5月16日。

⑤ 美国学者艾伦·F.威汀在1967年出版的《隐私与自由》一书中认为隐私是“个人、群体或机构自主决定在何时以怎样方式在多大程度上将有关自身的信息披露给他人的权利”。See Alan F. Westin, Privacy and Freedom, Atheneum New York, 1967, p. 7。基于此，后人将威斯汀的贡献评价为从信息控制角度审视隐私的先驱，认为其提出了一种“新型隐私”。

⑥ 譬如，美国立法中就是将个人数据保护纳入隐私的范畴，1974年《美国隐私法》专门对个人记录（record）的保存和披露进行了规定。

《侵权责任法》)正式在法律层面使用“隐私权”一词,但是并没有明确其定义。[①] 因此,我国法律上的隐私概念是以学理解释为主导的,且还没有统一的认知。在这方面,对于隐私的定义比较经典的观点是:隐私指个人不愿公开或为他人知悉的秘密,这个秘密可能是文字记载事实、通信,也可以个人行为或活动过程。[②] 因而,隐私侵权行为可以类型化为两种:一是公开泄露个人不愿意让人知晓且不涉及公共利益的生活事实(私密信息);二是刺探他人私密活动(跟踪监视他人行踪、窥探私人活动或侵入私密空间等)。[③] 所有这些侵权行为都有一个共同的后果——个人私密事务被泄露或知晓,导致该个人精神痛苦。[④]

隐私保护本质上是保护人的尊严,我国最早将隐私纳入名誉权保护的立法实践即可证明这一观点。[⑤] 后来,人们逐渐认识到隐私也是一种独立的人格利益,有必要将其类型化为独立人格权。[⑥]《侵权责任法》首先将隐私权列举为侵权客体,如今《民法总则》也将隐私权单独列为一项具体人格权。[⑦] 作为独立的具体人格权,隐私权旨在对抗他人泄露私密信息或刺探他人私人生活的加害行为,赋予其停止侵害和损害赔偿的请求权。也就是说,隐私权是一种消极的、防御性的权利,在该权利遭受侵害之前,个人无法积极主动地行使权利,而只能在遭受侵害的情况下请求他人排除妨害、赔偿损失等。[⑧] 隐私侵权救济旨在保护公民的私密个人生活事实不被他人擅自泄露、公开,保护的是权利人的人格利益。

从概念上来看,个人信息与隐私具有明显区别,前者强调可识别性,后者强调私密性。[⑨] 但是,个人信息保护与隐私保护规范也存在交叉,主要体现在两个方面:

其一,个人信息中包含私密信息,而这是隐私权保护的重要内容。识别个人的信息并不一定都具有隐私利益,但是,越私密性的信息与特定个人的联系就越强,或者说该信息的个人属性就越强,其可识别性就越高,因而私密性信息均可落入个人信息范畴。这样,尚未披露也不愿意披露的私密性个人信息本身具有隐私利益,任何未经权利人同意就披露或使用其私密性个人信息的行为即构成隐私侵权。因此,在对个人信息的规范中,多数国家在个人信息中区分出敏感个人信息,[⑩]而敏感个人信息多具有私密性,落入隐私范畴。[⑪]

因此,一旦可识别个人的信息落入隐私范畴,就必须遵循隐私保护规范,必须按照保护隐私的方法保护此类个人信息,最为重要的是不得泄露,因为泄露即构成隐私侵权。这意味着对于落入隐私范畴的个人信息,需要赋予个人以控制权,使用属于隐私范畴的个人信息应当事先征得个人同意,且使用中应当保证

---

① 《中华人民共和国侵权责任法》首次将隐私权作为民事权益纳入法律文本之中。该法第 2 条第 2 款规定:“本法所称民事权益,包括生命权、健康权、姓名权、名誉权、荣誉权、肖像权、隐私权、婚姻自主权、监护权、所有权、用益物权、担保物权、著作权、专利权、商标专用权、发现权、股权、继承权等人身、财产权益。”

② 例如,杨立新教授认为,隐私中的信息,主要是一种私密性的信息或者私人活动,而且单个的私密信息或者私人活动并不直接指向自然人的主体身份。参见杨立新:《个人信息:法益抑或民事权利——对民法总则第 111 条规定的“个人信息”之解读》,《法学论坛》2018 年第 1 期。王利明教授认为,隐私是一种与公共利益、群体利益无关的,当事人不愿他人知道或他人不便知道的信息,当事人不愿他人干涉或他人不便干涉的个人私事和当事人不愿他人侵入或他人不便侵入的个人领域。它包括三种形态,一是个人信息,为无形隐私;二是个人私事,为动态的隐私;三是个人领域,为有形的隐私。参见王利明主编:《人格权法新论》,吉林人民出版社 1994 年版,第 480~482 页。

③ 这两类隐私侵权行为对应隐私的两个方面:一是个人未公开或不愿公开的事实或信息,二是个人私生活或行为空间的隐蔽状态。这两个方面形成个人隐私利益。参见高富平主编:《民法学》,法律出版社 2009 年第 2 版,第 94~95 页。

④ 侵害隐私权的损害后果主要表现为精神损害,即导致受害人精神痛苦,包括情绪低落、焦虑不安、羞愧等,虽然有时候也常常伴随着间接的财产损失,但不存在直接的财产损失。参见张新宝:《我国隐私权保护法律制度的发展》,《国家检察官学院学报》2010 年第 2 期。

⑤ 《最高人民法院关于贯彻执行〈中华人民共和国民法通则〉若干问题的意见(试行)》第 140 条规定:“以书面、口头等形式宣扬他人的隐私,或者捏造事实公然丑化他人人格,以及用侮辱、诽谤等方式损害他人名誉,造成一定影响的,应当认定为侵害公民名誉权的行为。”

⑥ 参见张新宝:《隐私权研究》,《法学研究》1990 年第 3 期。

⑦ 《中华人民共和国民法总则》第 110 条第 1 款规定:“自然人享有生命权、身体权、健康权、姓名权、肖像权、名誉权、荣誉权、隐私权、婚姻自主权等权利。”

⑧ 参见王利明:《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。

⑨ 参见王利明:《论个人信息权在人格权法中的地位》,《苏州大学学报》(法学版)2012 年第 6 期。

⑩ 欧盟以及欧洲各国在其立法中通常使用“特殊种类的个人数据”来指代敏感个人数据。例如,《统一数据保护条例》第 9 条“对特殊类型个人数据的处理”就涉及敏感个人数据的类型,包括但不限于种族、民族起源、政治观点、宗教信仰、哲学信仰、工会成员资格、基因数据、生物特征数据、健康数据、与性生活、性取向相关的数据等。2014 年修订的《法国数据处理、数据文档和个人自由法》第 8 条规定敏感个人信息包括“直接或间接暴露他人的种族本源,政治、哲学或者宗教主张,公会的归属以及他人的健康或性生活的个人信息”。《德国联邦数据法》第 3 条将“有关个人种族、民族、政见、宗教信仰、党派、健康或性生活的信息”作为敏感个人信息。

⑪ 参见王利明:《隐私权概念的再界定》,《法学家》2012 年第 1 期。

该信息不被泄露或公开。这就是《条例》在没有赋予数据主体同意权的前提下，仍然将同意作为处理某类个人信息合法性基础的原因。数据主体的“同意”和数据控制人的“不泄露义务”成为个人信息保护制度维护敏感信息（包括隐私）的两项重要制度。至于哪些个人信息落入敏感个人信息（或隐私）范畴，国际社会并没有统一的立法规则，需要各国根据国民一般认知和文化背景进行具体规定。

其二，个人信息的利用可能造成隐私侵权。隐私权的内容还包括个人独处或个人生活不被侵扰（即个人生活安宁权），个人信息的不正当使用也可能构成对此类隐私状态的侵犯。在过去，跟踪或刺探个人活动存在着技术障碍，但是在网络化、数据化时代，个人的一切行为过程、行为时间地点甚至目的都可能被收集和分析。这样，个人信息的收集和利用也有可能对个人行为隐私（私人生活免受打扰）造成侵犯。例如，个人行踪属于个人隐私，跟踪监控个人行踪轨迹、持续收集个人的位置信息既可能侵犯个人“独处”的隐私利益，也可能危害个人的安全利益，构成犯罪。[①] 因此，个人信息的收集和利用行为必须得到规范，以确保对个人隐私的保护，防范隐私侵权后果的产生。

因此，个人信息保护法涉及两方面的隐私利益保护，一是避免落入隐私范畴的敏感个人信息的泄露，二是防范个人信息利用过程中对私人生活的侵扰（个人生活安宁）。由于个人信息利用只有在保护个人权益的前提下才正当合法，因此个人信息保护规范当然包含隐私保护规范，隐私保护贯穿于个人数据保护的整个过程。只是隐私保护通过侵权救济来实现，是否侵犯隐私主要看个人信息的使用行为是否导致泄露、侵扰后果，导致数据主体精神痛苦，而不是事先通过立法来实现。

因此，在大陆法的语境下，我们不能将隐私保护作为个人数据保护法的目的。以欧盟立法为例，无论是各成员国国内的个人数据保护法还是最新的《条例》，总体上都属于公民基本权利（人权）法，而非私法，且隐私保护也只是作为人格尊严不可或缺的内容被放进法律规范中；在个人信息保护方面，并没有建立公开个人信息就构成侵权的规范，更没有建立未经同意不得使用个人信息的规范。[②] 因此，欧洲个人数据保护法内含隐私保护，但其规范体系不能对应到私法上的隐私权保护规范。

需要指出的是，在国际社会，隐私也被广义地理解为“要求尊重私人生活的权利”，而要求保护个人数据的权利也当然地属于隐私保护。在这个意义上，我们又可以将个人信息保护等同于隐私保护。因此，隐私与个信息保护的关系，关键在于如何定义隐私或隐私保护的范畴。

四、个人信息保护与个人安全利益

由于个人无法完全控制他人对个人信息的使用，因此个人信息的不当使用不仅可能侵害个人基本权利或精神利益，而且还可能危害个人的人身安全和财产安全，侵害个人的安全利益。

个人信息本身是社会交往的工具，其本身没有社会危害性。但是，这种识别和联系的功能被“不法分子”利用，用于违法犯罪活动，就会危害到个人安全。首先，个人信息收集越多，对于一个人的喜好、心理状态、社会关系等的掌握就越准确和全面，就有可能精准地实施恐吓、诈骗等犯罪活动。其次，如果可以轻易地获得包含特定个人联系方式（电话、微信、邮件等）的个人信息，这等于给犯罪分子提供了实施违法犯罪的工具。伴随电子通信的广泛应用，出现了新的犯罪类型，即“电信诈骗”。一些犯罪分子通过电话、网络和短信方式，编造虚假信息，设置骗局，甚至冒充电信局、公安局等机构的工作人员对受害人实施远程、非

① 最高人民法院、最高人民检察院《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》[法释(2017)10号]将“行踪轨迹”列为最具有危害性个人信息范畴，非法获取、出售或者提供行踪轨迹信息达50条以上的即可以视为情节严重，应承担相应的刑事责任。

② 无论是《数据保护指令》还是《统一数据保护条例》，抑或是欧盟各成员国（如德国、法国、意大利、荷兰等）的个人数据保护法规范，都没有将数据主体的同意作为数据控制者或处理者处理其个人数据的唯一合法性基础。例如，《统一数据保护条例》第6条规定：“只有符合以下情况之一的个人数据处理行为才是合法的：(a)数据主体已经对基于一个或多个具体目的而处理其个人数据的行为表示同意；(b)履行数据主体为一方当事人的合同或在订立合同前为实施数据主体要求的行为所必要的数据处理；(c)为履行数据控制者的法定义务所必要的数据处理；(d)为保护数据主体或另一自然人的重大利益所必要的数据处理；(e)为履行涉及公共利益的职责或实施已经授予数据控制者的职务权限所必要的数据处理；(f)数据控制者或第三方为追求合法利益目的而进行的必要数据处理，但当该利益与要求对个人数据进行保护的数据主体的基本权利和自由相冲突时，尤其是当该数据主体为儿童时，则不得进行数据处理”，该条列举了6种并列的合法性基础，只要择一即可。

接触式诈骗,诱使受害人给犯罪分子汇款或转账,或者盗取钱财。[①] 于是,如何减少和扼制个人信息的非法利用,消除个人对信息安全的担忧,就成了促进个人信息正当使用的必要条件,也成为法律规制的重要目标。

确保个人信息安全也是个人信息保护法的重要立法目标,因为个人信息不安全就会给"坏人"可乘之机,增加个人人身和财产方面的安全风险。个人信息的不安全因素主要来源于两个方面:一是在数据的正当使用、存储和传输过程中可能存在的泄露风险;二是来自外部的恶意攻击、盗取。如何加强个人信息存储和使用过程中的信息安全管理,防止泄露、盗用等风险也是个人信息保护法的重要内容。因此,"安全保护原则"是经济合作与发展组织在《隐私保护与个人数据跨境流通指南》中提出的个人信息保护 8 大基本原则之一,并将之表述为:"个人数据应当得到合理的安全保护,防止丢失或未经授权的访问、毁坏、使用、修改或泄露"。安全原则已经成为世界普遍接受的个人信息保护原则。[②]《条例》除了要求数据控制人在系统设计时即考虑个人数据保护以实现数据的系统保护和默认保护外,[③]还详细规定了数据控制人的安全保障义务(第 32、33、34 条)。实际上,除了从信息安全的角度保障个人信息安全外,要求数据控制人的数据处理行为合规合法也是确保个人信息安全的重要方面。在这个意义上,维护个人信息的安全也是个人数据保护法的基本宗旨。

但是,个人数据保护法所保护的安全是个人数据本身的安全,而不是针对利用个人数据从事违法犯罪的社会危害行为。这是因为个人数据保护法规范的是个人数据的正当使用行为,即在特定场景中为开展社会交往、实施社会活动(包括商业、公共管理等特定目的)而进行的收集和使用个人信息的行为。也就是说,个人数据保护法调整的是利用目的合法的个人数据处理行为,而不是利用目的非法的个人数据使用行为,后者只是将个人数据作为实施犯罪行为的一种手段而已。国际社会中有关个人数据保护的立法均是在行为目的合法的前提之下来规范个人信息利用行为,以确保个人信息利用行为不侵犯个人基本权利。在笔者看来,目的合法是默认的前提,基于非法目的的个人数据处理行为应当由其他法律调整,不在个人数据保护法的调整范围。因此,个人数据保护法中的合法性仅是指个人数据处理有法律依据(同意或符合法律规定的情形),而不是指个人数据使用的目的或用途合法。

因此,电信诈骗、恐吓等行为已经脱离了正常个人信息社会利用的范畴,构成违法犯罪行为,不属于个人信息保护法调整的对象,而是属于刑法的调整对象。针对个人信息被滥用、盗用、冒用所带来的危害,一些国家的刑法已经出现了专门针对身份冒用、盗用行为的明文规定。例如美国,1998 年美国国会通过了《身份盗用和假冒制止法》,确立了"身份盗用罪"。该法将身份盗用罪定义为:"没有合法授权,故意转移或使用他人的身份,意图从事或帮助或教唆任何构成违反联邦法律的不法活动,或者任何构成可适用的州或地方法律的重罪的行为。"可见,该罪名主要针对非法转移或使用某人的个人可识别信息,以冒用其身份从事欺诈等不法活动。该罪是目的犯,强调个人信息使用的目的是为"冒用身份"和从事"不法活动"。2012 年,美国破获了一起涉案人数与金额巨大的身份盗用案件,以至于被称为美国 2012 年以来最大且最典型的身份盗用案件。[④] 在该案中,某犯罪集团的成员通过不法手段获取了来自多个国家的公民的个人身份信息,获取信息后将该信息提供给其他成员伪造信用卡,最后利用伪造的信用卡进行无节制的奢侈消费。

美国的"身份盗用罪"对应到我国便是电信诈骗罪。由于该犯罪行为和方法复杂,侵害法益众多,因此《中华人民共和国刑法》(以下简称《刑法》)并没有单一条文和罪名(电信诈骗罪并不是一个具体罪名),而是适用诈骗罪(《刑法》第 226 条)、非法利用信息网络罪(《刑法》第 287 条)等条文。当他人利用个人信息

① 2016 年 8 月 19 日,准大学生徐玉玉被他人以发放助学金为由诈骗近万元人民币,因难以忍受该后果,其心脏骤停,不治身亡。此案在全国引起巨大反响。参见万晓岩:《"徐玉玉案"审判纪实》,《中国审判》2017 年第 21 期。

② 这些文件包括《个人数据处理中的个人保护公约》《联合国计算机处理的个人数据文档规范指南》《亚太经合组织隐私框架》《普遍接受的隐私原则》(GAPP)、《ISO29100 隐私框架》《美国正当信息通则》等。

③ 英文表达为"data protection by design and by default",又译为"隐私的设计保护"。参见《统一数据保护条例》第 25 条。

④ See 111 Individuals Charged in Massive International Identity Theft and Counterfelt Credit Card Operation Based in Queens, http://www.queensda.org/newpressreleases/2011/october/op%20swiper_credit%20card_id%20fraud_10_07_2011_ind.pdf, 2016-10-28.

实施诈骗等行为时，在这里个人信息只是犯罪的工具，直接侵害的是自然人的人身和财产利益，而不是人的尊严，因而并不是侵害个人信息犯罪。电信诈骗罪惩罚的是个人信息的非法利用，而个人信息犯罪（《刑法》第253条之一）惩罚的是个人信息获取行为和提供行为本身的违法性，二者不是一回事。

以上分析表明，个人信息涉及两类安全：个人信息安全与个人信息非法利用引发的安全。个人数据保护法仅规范个人信息安全问题，而利用个人信息实施非法行为侵害人身和财产安全的行为则应当由刑法来规范和惩治。《网络安全法》"网络信息安全"一章对个人信息安全的规范，显然属于针对网络运营者个人信息安全保障义务的立法规范，该规范主要是保护个人信息在存储、运营和利用过程中的安全，而非针对非法利用个人信息进行犯罪中的安全。由个人信息利用引发具有社会危害性的安全问题则应当受刑法规制。

不过，《刑法》通过两次修正案确立的"侵犯个人信息罪"（《刑法》第253条之一）是针对我国目前极其严重的个人信息买卖、盗用现象而设计的，该条文宣布"出售、非法提供公民个人信息"和"非法获取公民个人信息"违法，情节严重的可以入刑。这说明刑法隐性地确立了个人信息利用规范，并对严重侵害个人权益的个人信息违法利用行为予以刑事制裁。显然，它是将个人信息流通利用行为本身认定为犯罪行为（主要限定条件是违反法律规定），并没有将非法目的作为限定条件，因而是我国特有的对个人信息的保护方式。相对于其他国家而言，我国个人信息保护多了一层刑事保护。实际上，该保护旨在制止脱离具体应用场景的买卖、非法提供和盗用个人信息的行为，因为这样的利用行为本身即具有社会危害性。因此，笔者曾建议对刑法这一规定进行修改，将该罪修改为目的犯，即将"以从事违法活动或侵害个人权益活动为目的"作为该罪之构成要件之一，以符合刑法规范的目的。①

五、代结论：保护目的决定个人信息保护的定位

人们利用散落于社会中的个人信息（文史资料、档案记录等）识别个人是社会的常态，并非今天才有之事。之所以现在开始规范人们收集和利用个人信息的行为，主要是因为计算机应用导致收集和利用个人信息的方式发生巨大变化，个人对有关个人信息失去控制，导致个人刻画成什么样的人、被"处置"或"对待"存在不确定性。20世纪70年代，计算机刚刚应用不久，个人信息的保护问题即被提到议事日程，出现了个人数据保护法。例如，1974年美国颁布了《隐私权法》，规范政府机构的个人信息利用行为；1973年《瑞典数据保护法》和1978年《德国联邦数据保护法》分别开启了对公共领域和私人领域收集和利用个人信息的行为进行统一规范的先河。因此，个人信息保护成为一个法律问题肇始于个人信息电子化和自动化处理，而不断强化于网络日益普及和智能化的今天。在现今时代，一个人每时每刻的行为轨迹、甚至生理活动等均可以被电子化记录，形成一个生理、心理、习惯、行为、行踪等全息信息记录。这些全息性个人信息被自动处理和使用导致个人逐渐失去对其个人信息的控制，给个人的基本权利和自由带来前所未有的挑战。因此，个人信息保护成为这个时代各国立法必须要解决的问题。对于形成于西方社会的个人信息保护制度必须要有正确的理解和定位，只有这样才能移植和构筑适合于我国国情的个人信息保护法律体系。基于上述对个人信息上需要保护的法益论述，我们可以初步得出以下结论：

首先，个人信息是识别特定个人的信息，而识别个人是社会交往和运营的工具，因此个人信息并非属于个人所有，个人不享有排他支配的权利。个人信息保护旨在保护个人在信息上的利益，而这些利益保护不足以也不可能赋予个人对该信息的绝对控制。因此，目前我国立法规范中已经确立的"非经个人同意不得收集和使用个人信息"的规则，实际上隐性地赋予了个人对个人信息的支配权，这既与个人信息的社会地位不吻合，也不具有法律上的正当性。

其次，个人数据保护是在宪法层面对个人基本权利的保护，其保护人的尊严所派生出的个人自治（自

① 参见高富平，王文祥：《出售或提供公民个人信息入罪的边界——以侵犯公民个人信息罪所保护的法益为视角》，《政治与法律》2017年第2期。

由)、身份利益(正确识别)、不歧视(平等)利益。欧盟立法虽然将之抽象为个人数据保护权,但只是对个人数据受法律保护的简要表达,并不是一种单一权利保护,更不是一种私权保护。若要放入民法人格权编的话,应当作为一般人格权加以保护,而不宜直接视为一项具体人格权。也就是说,个人信息保护本质上还是法益保护,而不是赋予个人对个人信息享有某种权利来实现保护。

再次,在大陆法语境下,个人信息并不等于隐私,个人信息保护规范也不等同于隐私保护规范,至少欧盟的立法没有将个人信息保护置于人格权(尤其隐私权)意义上来设计保护规则。但是,保护隐私是个人信息利用的前提,因而,特定情形下征求数据主体的同意和防止个人信息泄露是个人信息保护法的重要内容。因此,隐私保护又贯穿于欧盟数据保护法的始终。

最后,个人信息本身并不具有危害性,但个人信息的不法利用具有危害性。这里应当区分两类不法和危害,一类是个人信息利用本身的违法,即为了实现正当合法的用途或目的,但没有遵循个人信息保护规范,侵害了个人基本权利(人的尊严);另一类是个人信息被用于不法行为,这种不法行为不仅侵害个人权益,而且具有社会危害性,因而需要法律制裁(最严厉的是刑事制裁)。前者是个人信息安全问题,属于个人信息保护法范畴;利用个人信息从事诈骗犯罪则属于后者,需由刑法调整,不是个人信息保护法的任务。而《刑法》规定的"侵犯个人信息罪"实质上是对个信息使用严重违法行为的惩治,使刑事保护成为我国特有的个人信息保护方式。

在人类社会进入网络化、数据化和智能化的时代,数据的应用已经无孔不入,成为经济和社会运行的"新能源",其中大多数数据都可以关联到个人,落入个人数据或个人信息范畴。可识别个人的数据既要能够为社会所利用,又必须确保该利用行为不侵犯个人权益。显然,这是一个相当复杂的法律问题。形成于 20 世纪 80 年代基于个人基本权利保护理念的个人数据保护法,试图构筑保护人权高度下的个人数据利用规范,为我们提供了可供参考的蓝本。为顺应大数据时代的到来,我国立法开始探索和建立我国的个人信息保护制度,但是并未真正地从源头上回答为什么要保护个人信息的问题,这导致我国个人信息保护法的定位存在偏差。我们必须正本清源,厘清个人信息上存在的值得法律保护的个人利益,这是准确定位个人信息保护立法目的的基础。

责任编辑 温世扬