

## 已公开个人信息保护和利用的规则建构

刘晓春

**内容提要:**已公开个人信息的保护和利用规则,虽已通过《民法典》和《个人信息保护法》确定下来,但其具体适用在实践中尚存争议。典型的争议场景包括处理政府信息公开、搜索引擎处理公开信息等。相对于欧盟和美国的立法模式,我国将已公开个人信息单独归类,并将个人决定权降格为“选择退出”的权利。在已公开个人信息保护和利用的规则建构中,应当针对合法公开的不同情形进行类型化处理。在确定信息处理者关于合法性认定的注意义务、信息处理行为的合理范围、是否对个人权益造成重大影响、拒绝权的行使及其例外各个要件时,应当充分考虑个人信息公开的类型、个人信息本身的敏感程度、信息处理行为的类型等要素,重视已公开个人信息中体现的公共利益价值与个人权益之间的平衡关系,通过为个人“拒绝权”创设例外等做法发展与完善我国已公开个人信息保护和利用规则体系。

**关键词:**已公开个人信息 选择退出 拒绝权 删除权

刘晓春,中国社会科学院大学法学院讲师。

已公开个人信息在我国立法中被作为个人信息的一个专门类别加以规定,《民法典》和《个人信息保护法》的相应条款整体上保持一致,措辞上略有区别。司法实践中,针对已公开个人信息的利用和保护,已经出现为数不少的判决,但对于具体规则适用尚未形成共识,而且对于最新立法条文及其构成要件,也尚未进行解释和适用。在现有法律规定的基础上,有必要探讨已公开个人信息规则建构中的利益冲突和价值取向,厘清现有条款构成要件的具体适用规则,梳理已公开个人信息相关规则与个人信息保护其他规则之间的关系,为已公开个人信息保护和利用提供规则建构的合理方案。

### 一 已公开个人信息保护的典型场景

实践中,已公开个人信息包罗万象,互联网的迅猛发展使得信息的检索和获取达到前所未有的便利程度,而大数据时代中各类主体对于数据收集、挖掘和利用的强烈需求,也

集中体现为对公开数据的抓取、加工等处理和利用。在司法实践中,围绕已公开个人信息的保护和利用,涌现出一系列具有代表性的纠纷,可以据此总结已公开个人信息规则适用的典型场景。

政府在行使公共职权过程中公开的各类信息,成为数据产业收集和挖掘的重要对象,也引发了众多的争议和纠纷。政府公开的企业工商登记信息、征信信息、司法裁判文书公开的信息等,都可能包含姓名、身份证号、手机号、任职、经历、行为记录、裁判结果等个人信息。行为人针对政府公开信息进行处理、利用、传播,例如将上述公开信息收入商业数据库,提供信息查询的收费或者免费服务,已较为普遍。但围绕此类数据的处理行为,也产生了一系列纠纷。

围绕“中国裁判文书网”公开的司法裁判文书,有企业将其下载并纳入商业数据库,进行再次传播和利用。两名原告分别在苏州和北京提起诉讼,要求被告移除载有其个人信息的裁判文书,在案件事实大体相同的情况下,苏州和北京的两个法院给出了截然不同的两个判决结果。前者倾向于保护个人对其个人信息控制的权利,后者则倾向于保护司法公开的价值以及公众知情权、监督权等公共利益,引起业内的广泛关注。<sup>[1]</sup>

针对政府公开信息作为源头的企业信息、征信信息的再次利用、加工和传播,在侵犯公民个人信息罪的刑事司法实践中也成为重要的案件类型,受到高度关注。在《民法典》通过之前,针对个人征信信息等的利用行为,曾在为数不少的案件中被认定为构成刑事犯罪。<sup>[2]</sup>但近期也有认定不构成犯罪的做法,特别是在《民法典》生效后,其中关于已公开个人信息的条款对刑事司法实践也产生了影响。<sup>[3]</sup>

搜索引擎对于公开信息的收集和展示,也成为实践中一类重要的争议类型。例如,针对用户自行上传到校友录作为用户头像的证件照,法院认定,在原告要求百度删除前,百度收集并存储原告证件照的行为并未违反作为搜索引擎的一般注意义务,但在原告提出删除请求后,百度应当删除该照片。<sup>[4]</sup>此外,针对百度等搜索引擎起诉的案件情形,还包括要求删除来源于已公开裁判文书的相关信息,包括违章行为、犯罪记录等。<sup>[5]</sup>

我国香港地区也出现了利用司法裁判文书、企业登记与破产信息建设商业数据库、在网页上设置已公开司法裁判文书链接的行政执法案例,行政机关认定这些再次利用行为超出了初始公开目的的范围,不符合信息主体的合理期待,从而构成侵害个人信息。<sup>[6]</sup>

[1] 参见伊某与苏州贝尔塔数据技术有限公司人格权纠纷案,江苏省苏州市中级人民法院(2019)苏05民终4745号民事判决书;梁某与北京汇法正信科技有限公司网络侵权责任纠纷案,北京市第四中级人民法院(2021)京04民终71号民事判决书。

[2] 参见江苏省徐州市铜山区人民法院(2018)苏0312刑初字第85号刑事判决书;江苏省徐州市铜山区人民检察院铜检诉刑诉(2018)425号起诉书。

[3] 参见卢志坚、白翼轩、田竞:《出卖公开的企业信息谋利:检察机关认定行为人不构成犯罪》,《检察日报》2021年1月20日第1版。

[4] 参见孙某与北京搜狐互联网信息服务等人人格权纠纷案,北京互联网法院(2019)京0491民初10989号民事判决书。

[5] 此外,被称为国内“被遗忘权第一案”的任某诉百度公司名誉权纠纷案也涉及公开个人信息利用问题,参见北京市第一中级人民法院(2015)一中民终字第09558号民事判决书。

[6] Office of the Privacy Commissioner for Personal Data Hong Kong, Report No. R13 - 9744, 13 August 2013.

在国外,针对搜索引擎展示已公开个人信息提起诉讼的“被遗忘权”案件,亦是为数不少。在欧盟,针对谷歌的被遗忘权案件涉及到政府信息公开,如刑事案件审判信息、企业登记信息,以及著名的“谷歌西班牙(Google Spain)”案中的原告破产拍卖记录等,<sup>[7]</sup>也包括公开报道和评论属性的文章、具有政治讽刺性的照片等。<sup>[8]</sup>法院在不同类型的案件中给出了不同的判决结果。

总结来看,实践中关于已公开个人信息保护和利用的纠纷出现多发态势,这一方面是因为对已公开个人信息的再次传播相对来说比较容易被观测到,由于其影响的广泛性对个人权益产生了较为明显的影响,个人提起诉讼寻求救济的积极性比较高。另一方面,典型领域的争议都涉及到不同主体的多重利益冲突,目前尚未建构起明确、统一的规范体系。从国内外的纠纷类型看,涉及到不同的“合法”公开类型;而需要回答的问题,则包括规则适用和建构的各个层面,如对于处理行为的“合理范围”及影响个人“重大权益”如何认定、个人拒绝处理其公开个人信息的权利如何行使以及是否存在例外、在具体案件场景中如何进行个人权益和公共利益的衡量等多个层次。

## 二 已公开个人信息保护的三种立法模式及其理论梳理

针对已公开个人信息的利用和保护,国际上存在不同的立法模式,体现了对于已公开个人信息制度定位和价值取向的不同选择路径。第一种模式以欧盟《一般数据保护条例》(*General Data Protection Regulation, GDPR*)为典型代表,没有将已公开个人信息作为单独类别进行特殊规定,对已公开个人信息的处理需要满足一般的原则和合法性基础规定;第二种模式以美国《加州消费者隐私法》(*California Consumer Privacy Act of 2018, CCPA*)和《加州隐私权法》(*California Privacy Rights and Enforcement Act, CPRA*)为代表,在“个人信息”的概念中将“公开可得信息”直接排除出去;第三种模式是在个人信息保护法中将“已公开个人信息”或“公开可得信息”作为一类单独列出,构成一种独立的合法性基础,亦即作为个人信息处理中获取“同意”义务的例外情形,我国《民法典》和《个人信息保护法》采用了此种模式,加拿大、新加坡、韩国等国家的立法也体现了这一特点。

### (一) 立法模式一:已公开个人信息适用一般规则

欧盟《一般数据保护条例》中,没有将已公开个人信息单独作为一类信息类型进行专门规定,而是适用其关于个人信息处理的一般性规定,并无专门的特殊例外。但是,已公开个人信息在一些具体规则的适用中,也会呈现其特殊性。

在欧盟《一般数据保护条例》关于个人数据处理原则(第5条)和处理合法性基础(第6条)的规定中,都没有专门规定已公开个人信息的类型。在关于“特殊类型的个人数据处理”(第9条)中,一方面该条第一款规定了禁止处理特定敏感类型的个人数据;另一方

[7] Case C-131/12 *Google Spain and Google* EU:C:2014:317.

[8] Case C-136/17 *GC and Others* EU:C:2019:773; Case C-398/15 *Commercio, Industria, Artigianato e Agricoltura di Lecce v. AEPD*, ECLI:EU:C:2017:197.

面,第二款规定了10种针对第一款的例外情形,其中(e)项规定的例外为:“处理被数据主体明确无疑公开的个人数据”。<sup>[9]</sup>亦即,对于数据主体自行以明确无疑的方式进行公开的情形,数据处理者对该公开信息的处理可以不受第9条第1款的限制。但是,需要特别指出的是,第9.2(e)条的例外规定,并不能构成个人数据处理的合法性基础,即使满足了自行公开这一例外情形,对于这些个人数据的处理依然需要满足第5条和第6条的规定,需要基于同意或者第6条规定的其他情形,才能获得处理行为的合法性。<sup>[10]</sup>这是欧盟《一般数据保护条例》与我国立法将已公开个人信息处理规定为同意的例外情形最重要的区别。

根据欧盟《一般数据保护条例》第6条第1款的规定,除了(a)项规定了同意作为合法性基础之外,(b)到(f)各项都可能构成处理已公开个人信息的合法性基础,其中,第(c)项履行法律义务之必要、第(e)项为了公共利益或公务职权行使之必要,以及第(f)项追求合法利益之必要,都有可能涉及处理已公开个人信息的情况。特别的,对于前述涉及的已公开个人信息利用的典型场景,如针对政府信息公开进行商业数据库形式的加工,或者通过搜索引擎、数据抓取对于公开信息的收集、利用和展示,通常落入第(f)项所规定之“合法利益”的可能性较大,也可能涉及到公共利益的情形。

个人对于已公开个人信息的处理行为,也拥有完整的权利体系,包括知情权、访问权、更正权、删除权、限制处理权、可携带权、反对权等。<sup>[11]</sup>涉及已公开个人信息处理的纠纷,目前为止多是围绕删除权(被遗忘权)的行使。在这类纠纷中,数据处理通常是基于第6.1(f)条规定的合法利益条款,而并非基于同意,在争议中通常会涉及至少两个层面的问题。第一个层面是合法利益作为合法性基础是否能够成立,这决定了处理行为本身是否合法;第二个层面是如果处理行为合法,原告是否可以有效行使删除权。在第二个层面,原告需要首先根据第21条主张反对权,并确保数据处理者的合法利益不能高于数据主体的利益、权利和自由。<sup>[12]</sup>此外,涉及政府信息公开、搜索引擎、数据抓取公开信息的场景时,数据主体通常还需要证明,自己要求删除信息或主张“被遗忘”的请求,不会构成第17条第3款所规定的删除权的例外情形,特别是不会妨碍到他人或公众“行使言论和信息自由的权利”、处理者执行公共利益或者官方职权的任务,以及基于“公共利益、科学、历史研究或者统计目的”的处理行为。<sup>[13]</sup>

欧盟《一般数据保护条例》第九章规定了一系列具体处理情形,可以由成员国自行制定法律规则,基于“言论和信息自由”的目的(第85条)、官方文件符合公共利益的情形(第86条)、为公共利益存档的目的、科学或历史研究目的、统计目的(第89条),设置个

[9] 欧盟《一般数据保护条例》第9.1,9.2(e)条。

[10] Edward S. Dove and Jiahong Chen, What Does It Mean for a Data Subject to Make Their Personal Data “Manifestly Public”? An Analysis of GDPR Article 9 (2) (e), 11 *International Data Privacy Law* 107, 108 (2021).

[11] 欧盟《一般数据保护条例》第12-22条。

[12] 关于欧盟《一般数据保护条例》合法利益条款的研究,参见商希雪:《超越私权属性的个人信息共享——基于〈欧盟一般数据保护条例〉正当利益条款的分析》,《法商研究》2020年第2期,第59-60页;谢琳:《大数据时代个人信息使用的合法利益豁免》,《政法论坛》2019年第1期,第74页。

[13] 欧盟《一般数据保护条例》第17.3条列举了删除权行使的五种例外情形。

人信息保护的豁免和例外。在以上这些情形中,已公开个人信息的处理都可能构成其中重要的典型场景,这也在司法判决中得到了印证。<sup>[14]</sup>

我国香港地区和日本也实行类似的立法选择。日本《个人信息保护法》采取了跟欧盟《一般数据保护条例》高度相似的立法逻辑,同样是在涉及敏感信息的条款中将“自行公开”作为禁止处理的例外,同时需要遵循个人信息处理的一般原则和合法性基础。<sup>[15]</sup>我国香港地区《个人资料(私隐)条例》也没有将公开个人信息进行单独规定,但是在第 8 部分“豁免”规定了个人信息保护的多项例外,其中涉及到执行司法职能、新闻、统计及研究等类型,皆有可能涉及已公开个人信息的利用。<sup>[16]</sup>

## (二) 立法模式二:个人信息概念中排除公开可得信息

美国的个人信息保护立法在联邦层面呈现“去中心化”态势,并没有形成统一的立法文件,而是分散于涉及个人信息处理的多个具体领域。由于美国的个人信息保护具有比较明显的“隐私权”保护传统,立法语言也经常使用“隐私”一词,因此隐含的前提即将公开可得信息排除在保护范围之外。例如,美国《健康保险携带与责任法案》(*Health Insurance Portability and Accountability Act, HIPAA*)就规定了个人医疗数据的保护对象是“非公开个人信息(nonpublic personal information)”。<sup>[17]</sup>

美国各州的隐私和个人信息保护立法沿袭了此种立法思路,其中影响力较大的是《加州消费者隐私法》和《加州隐私权法》,在“个人信息”的定义中皆规定不包括公开可得信息。“公开可得”指的是:合法可获得的联邦、州和地方政府的记录;企业有合理依据相信是由消费者合法披露给一般公众的信息;来源于广泛传播的媒体;来源于消费者自行公开且未限制特定受众类型。作为例外,公开可得数据不包括未经消费者同意而由企业收集的消费者的生物信息。<sup>[18]</sup>在加州之后通过的弗吉尼亚州的隐私权立法中,也采用了同样的模式,将“公开可得信息”从“个人信息”的概念中排除出去,不纳入立法保护的范畴。<sup>[19]</sup>

美国立法和执法中对于公开信息抱有的开放态度,与其强调宪法第一修正案的言论自由的价值理念高度相关,这一价值取向也体现在针对公开可得信息的个人“被遗忘权”在美国并未得到积极支持。<sup>[20]</sup>不过,针对未成年人自行发布的信息,加州制定专门的“橡皮擦法案”给予特殊保护,要求社交网站等允许未成年人行使删除权,删除自己上网时发布的各种信息;但同时又对删除权做出了众多限制,例如不能删除其他网站编辑过的信息,亦不能向搜索引擎提出删除请求。<sup>[21]</sup>

[14] See Case C-136/17 *GC and Others* EU:C:2019:773.

[15] 日本《个人信息保护法》第 17.2(v) 条规定了自行公开敏感个人信息的例外,第 15-16 条规定了个人信息处理的原则和合法性基础。

[16] 香港《个人资料(私隐)条例》第 51-63 条规定了 21 种个人信息保护的豁免情形。

[17] HIPAA, Section 509, Definition, (4) Nonpublic personal information.

[18] Californian Civil Code § 1798.140 (v) (2) (effective Jan. 1, 2023).

[19] Virginia Consumer Data Protection Act, Va. S. B. 1392 § 59.1-571 (2021 Session).

[20] 参见丁晓东:《被遗忘权的基本原理与场景化界定》,《清华法学》2018 年第 6 期,第 96 页。

[21] 参见陈钢:《美国“橡皮擦法案”的局限性解析》,《中国社会科学报》2021 年 1 月 4 日第 7 版。

### (三)立法模式三:已公开个人信息作为单独类别进行特殊规定

将已公开个人信息作为单独类别进行规定的模式,代表性立法是我国的《民法典》和《个人信息保护法》,以及加拿大、新加坡、韩国等国家的个人信息保护立法。

我国关于已公开个人信息的规定,体现在《民法典》第 1036 条和《个人信息保护法》第 13 条、第 27 条。<sup>[22]</sup> 对其的规定主要有三个层次,第一,个人自行公开或其他形式合法公开的个人信息,对其处理构成个人同意的例外,可以单独构成合法性基础;第二,要符合该条合法性基础,处理行为应在“合理范围”,且不能“侵害其重大利益”或“对个人权益有重大影响”,否则依然需要取得个人同意;第三,个人可以通过明确拒绝来反对个人信息处理行为。从现有规定看,已由个人自行公开或合法公开的个人信息,个人对其控制权能明显弱于未公开个人信息的情形,对应的个人信息处理行为也拥有更大的自由度。这集中体现在,处理行为不需要经过个人“同意”即具有合法性基础;也意味着基于“用户同意”的后续处理行为相关规则,例如“单独同意”“撤回同意”等规则,都不再适用。<sup>[23]</sup>

不过,用户虽然不能一般性地通过“事先同意”来控制已公开个人信息的处理,相关法条还是给予了用户“事后拒绝”的权利,这是类似于“默示同意”的“选择退出”机制,<sup>[24]</sup> 与《个人信息保护法》中规定的其他“拒绝权”相比,这是较为明显的差异。<sup>[25]</sup>

除了上述规定,《个人信息保护法》中关于个人信息处理规则(第二章)和个人权利(第四章)是否作为一般性规则适用于已公开个人信息处理的情形,例如告知义务、查阅、复制、更正等相关权利,虽然没有明确规定,但是在可适用情形下应当也具有约束力。需要指出的是,个人针对已公开个人信息处理的拒绝权利,尽管在表现形式上与《个人信息保护法》第 47 条规定的删除权比较接近,但应是一种独立的权利。与欧盟《一般数据保护条例》规定了删除权的多种例外情形不同,我国《个人信息保护法》无论是第 47 条关于删除权的规定,还是第 27 条关于拒绝权的规定,都没有规定基于公共利益、信息和言论自由等目的的例外情形,这有可能给规则具体适用带来一些潜在的问题。另一方面,在合法

[22] 《民法典》第 1036 条:处理个人信息,有下列情形之一的,行为人不承担民事责任:(一)在该自然人或者其监护人同意的范围内合理实施的行为;(二)合理处理该自然人自行公开的或者其他已经合法公开的信息,但是该自然人明确拒绝或者处理该信息侵害其重大利益的除外;(三)为维护公共利益或者该自然人合法权益,合理实施的其他行为。

《个人信息保护法》第 13 条:符合下列情形之一的,个人信息处理者方可处理个人信息:(一)取得个人的同意;(二)为订立、履行个人作为一方当事人的合同所必需,或者按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需;(三)为履行法定职责或者法定义务所必需;(四)为应对突发公共卫生事件,或者紧急情况下为保护自然人的生命健康和财产安全所必需;(五)为公共利益实施新闻报道、舆论监督等行为,在合理的范围内处理个人信息;(六)依照本法规定在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息;(七)法律、行政法规规定的其他情形。依照本法其他有关规定,处理个人信息应当取得个人同意,但是有前款第二项至第七项规定情形的,不需取得个人同意。第 27 条:个人信息处理者可以在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息;个人明确拒绝的除外。个人信息处理者处理已公开的个人信息,对个人权益有重大影响的,应当依照本法规定取得个人同意。

[23] 《个人信息保护法》第 23、25、26、29、39 条规定了单独同意的情形,第 15 条规定了撤回同意的内容。

[24] 关于个人信息“选择退出”机制的深入探讨和优缺点比较,参见冯恺:《个人信息“选择退出”机制的检视和反思》,《环球法律评论》2020 年第 4 期,第 148-165 页;冉高菁、范玉吉:《“选择退出”机制:重估我国网络个人信息保护》,《科技与法律》2017 年第 5 期,第 23-32 页。

[25] 《个人信息保护法》第 24、44 条规定了拒绝权。

性基础方面,已公开个人信息的处理有可能与第13条第1款第5项规定的“为公共利益实施新闻报道、舆论监督等行为,在合理的范围内处理个人信息”出现竞合。在具体规则适用中也有可能出现协调两种合法性基础之间关系的问题。

加拿大、新加坡、韩国等国家的个人信息保护立法也采取了将已公开个人信息单独规定的方式,例如,加拿大个人信息保护立法规定,针对公开可得的个人信息,处理行为可以不取得个人的事先同意,并制定了相关的法规对于“公开可得个人信息”的类型和范围做出了规定,包括公开的电话目录、行政和司法文件、公开媒体信息等。<sup>[26]</sup>新加坡和韩国也在“个人同意”的例外情形中列出了公开可得信息的类型。<sup>[27]</sup>

#### (四) 不同立法模式比较与理论梳理:已公开个人信息的制度定位与价值取向

##### 1. 立法模式比较

在三种立法模式中,欧盟《一般数据保护条例》没有针对已公开个人信息进行专门的例外规定,仅在敏感个人信息处理中规定了自行公开的情形,已公开个人信息适用一般性的例外规定。但是,由于其规定的例外层次较为丰富,包括“合法利益”“言论和信息自由”“公共利益”“科学、历史、统计目的”等,已公开个人信息可纳入例外的情形也较为丰富。

美国加州的立法模式则体现了对于公开可得个人信息的高度鼓励利用和流通的倾向,将特定类型的公开个人信息排除在法律适用范围之外,默认不予保护,仅在涉及未成年人保护时制定了特殊立法。当然,在加州的隐私权立法中,即使对于一般个人信息,也是采用“选择退出”机制,其保护强度大致相当于我国《个人信息保护法》对于已公开个人信息的保护程度。

中国的立法模式将已公开个人信息明确规定为获取同意的例外情形,体现了对其中公共利益和信息流通价值的重视。但是另一方面,“合理范围”“个人权益重大影响”等概念的范围边界尚不清楚,给信息处理者的义务范围带来不确定性,而且对“拒绝权”的行使也没有规定例外情形,在这点上反而不如适用一般规则的欧盟《一般数据保护条例》更有弹性空间。

##### 2. 理论梳理

已公开个人信息保护与利用的不同制度进路,体现出理论上的共识和分歧并存,可以总结为以下三个层次。

第一,已公开个人信息相对于未公开的个人信息应具有更强的公共性,以及更强的公共利益属性,这一属性在不同制度上具体表述为“公众知情权”“言论和信息自由”“公共利益”等。这一点可以认为已经达成共识,并可从两方面证成。其一,公开信息的自由利用是信息传播和知识进化的默认原则,这与同样处理信息产权问题的知识产权法中的“公有领域”概念具有相关性。<sup>[28]</sup>对于公开信息,公众的自由利用应为原则,而控制利用应为例外。其二,从成本收益分析,公开信息的利用过程中如须逐一甄别其中包含的个人

[26] Regulations Specifying Publicly Available Information, SOR/2001-7 (13 December, 2000), <https://www.canlii.org/en/ca/laws/regu/sor-2001-7/latest/sor-2001-7.html>, 最近访问时间[2021-10-10]。

[27] 参见李爱君、苏桂梅主编:《国际数据保护规则要览》,法律出版社2018年版,第401、446页。

[28] 参见吴汉东:《知识产权的多元属性及研究范式》,《中国社会科学》2011年第5期,第40页。

信息并赋予个人充分的控制权,会带来极高的成本,实质性阻碍公开信息的获取和利用。相比而言,要求在个人信息公开时进行更加严格的控制,而在公开后则通过推定或者选择退出等机制,来确保公开信息流动和利用可以在可控的成本范围内进行,应是更符合效率的做法,可节省巨额成本。

第二,已公开个人信息依然包含个人权益属性,但相对于未公开个人信息,这主要体现在一种受限的个人决定权。本质上已公开个人信息依然属于个人信息权益保护的范畴而并未完全进入公有领域。这种个人权益属性首先体现在其仅在“合法公开”的场景下受限,即使在美国法下,非法公开的个人信息也没有被完全排除保护。个人权益属性也体现在,合法公开情形下,仅仅是个人行使权利的条件发生了变化,但并没有否定实体权益的存在(美国模式是个例外),个人针对个人信息享有的其他权益也并未受到影响。在设置拒绝权的立法模式下,个人通过行使拒绝权即可以使得其权益不再受限,相对于其他立法路径实际上是对已公开个人信息给予了更强的保护。

第三,已公开个人信息的公共性和私权性之间的权衡,需要存在动态和弹性的调整空间。由于不同场景涉及的利益平衡状态的差异性,公共性和私权性之间的界分需要进行类型化调整。例如,涉及舆论监督、政府信息公开的情形,和个人自行公开个人信息的情形,就存在重要差异,前者应当更多考虑公众利益,而后者则可更尊重意思自治。具体到制度设计上,应有必要避免做出一刀切的规则设定,通过设置例外情形等方式,留出规则弹性适用的空间。

### 三 我国已公开个人信息处理规则的体系建构与适用

从我国已公开个人信息处理立法规则来看,一方面已经建立了较为清晰的界定层次,另一方面,其实践适用尚未得到具体检验,立法条文中规定的具体概念和规则尚存相当的不确定性,而从现有司法实践来看,法院对于一些基本问题的判断标准和价值取向亦尚未达成共识。因此,有必要借鉴国外立法和司法实践的经验得失,结合国内具体实践中出现的争议,对我国已公开个人信息处理相关的规则体系展开解释,并对需要补充的部分提出规则建构的建议。

#### (一) 个人信息的“合法公开”

##### 1. 合法公开的类型

我国立法体系中作为单独类别的已公开个人信息,需要具备一个重要前提,就是针对个人信息的公开行为应当是合法的,即“初始公开”合法。立法中规定了两类“公开”形式:一是个人“自行公开”,二是其他合法公开的形式。根据实践中典型的场景,他人“合法公开”的情形可能包括政府信息公开、媒体公开、其他个人或企业的公开等。<sup>[29]</sup>

[29] 《GB/T35273-2020 信息安全技术 个人信息安全规范》(“《个人信息安全规范》(2020)”)第5.6条规定收集使用个人信息的征得授权同意的例外,第9.5条规定共享、转让、公开披露个人信息时事先征得授权同意的例外。具体为以下情形:(1)个人信息主体自行向社会公众公开的个人信息以及(2)从合法公开披露的信息中收集个人信息的,如合法的新闻报道、政府信息公开等渠道。

第一,个人自行公开。这一情形属于个人对于其个人信息行使决定权的组成部分。具体的公开场景可能包括通过自己的社交媒体账号公开、通过其他媒介公开、通过参加公开场合的活动公开等,自行公开个人信息的目的可能包括社交分享、自我宣传、公共参与等。个人自行公开的情况可以类比于基于个人同意的信息处理,个人的自行公开个人信息行为可以产生一种“推定同意”,“意味着其在一定程度上同意他人对这些个人信息的处理”。<sup>[30]</sup>

对于个人自行公开的界定标准,在某些情况下可能引起争议。例如,“公开”需要指向不特定的人,在社交媒体上针对特定人的传播就有可能不构成“公开”,典型的如发布朋友圈、社交群内的传播、仅特定人群可见的微博内容发布等。

如何通过个人的行为或者表意确定是否“自行公开”,可以有不同的判断标准。欧盟《一般数据保护条例》第 9.2(e) 条下的个人“明确无疑”的“自行公开”界定,因其构成敏感个人信息处理禁止的例外,根据欧盟数据保护委员会(European Data Protection Board, EDPB)发布的相关指南,对其构成要件的要求十分严格,必须达到毫无疑义的程度,需要综合考量多个因素。以社交媒体上自行发布个人信息行为为例,需要考虑:(1)社交媒体平台的默认设置;(2)社交媒体平台的性质(熟人社交为主抑或陌生人社交);(3)发布信息页面的公开可访问性;(4)数据主体是否被明确告知他们发布的信息将被公开;(5)该信息是否是数据主体自行公布,或由第三方公布(例如,朋友发布的暴露敏感个人信息的照片)。<sup>[31]</sup>

美国《加州隐私权法》中所列的“公开可得信息”中,企业只要有合理依据相信相关个人信息是由消费者本人公开披露即可符合,采用了一种十分宽松的认定方法。<sup>[32]</sup>我国立法者对“自然人自行公开”的解释是“自然人主动将自己的某些个人信息向社会公开”。<sup>[33]</sup>由于与欧盟《一般数据保护条例》适用于敏感个人信息的第 9.2(e) 条在立法目的和定位上的不同,我国对于这一要件的认定可以不必过于严格,根据自然人的行为以及相关媒介(如社交媒体)的技术设置等特征,能够推断出其存在公开其个人信息的意图即可。

第二,经过个人同意的公开。这类公开通常由个人信息处理者做出,一定程度上可以认为是广义“自行公开”的一部分,但是由于在行为样态上与直接的个人“自行公开”具有比较明显的区别,实践中将其单独作为一种类别可以更方便规则适用。“公开”作为个人信息处理的一种对个人利益影响较大的特定情形,《个人信息保护法》对其合法性要求进行了强化的规定,“公开”个人信息的行为需要获取个人的“单独同意”,并进行个人信息保护影响的评估。<sup>[34]</sup>

[30] 黄薇主编:《中华人民共和国民法典人格权编解读》,中国法制出版社 2020 年第 1 版,第 220 - 221 页。

[31] European Data Protection Board, Guidelines 8/2020 on the Targeting of Social Media Users, adopted on 13 April 2021, paras 127 - 129.

[32] Californian Civil Code § 1798.140 (v) (2) (effective Jan. 1, 2023).

[33] 黄薇主编:《中华人民共和国民法典人格权编解读》,中国法制出版社 2020 年第 1 版,第 220 - 221 页。

[34] 参见《个人信息保护法》第 25 条。

第三,政府公开。政府公开的情形,还可以进一步细分为基于立法事务、行政职权的公开、司法公开等。实践中常见的根据政府公布的企业工商登记信息、征信信息、司法裁判文书等进行的数据挖掘和利用,都属于来源于政府的“初始公开”。政府在制定信息公开规则时,需要充分考虑各方主体及其利益的多元性,亦需要重点考虑公共利益,如公众知情权、民主政治、公众参与等价值,做出特定的利益衡量。<sup>[35]</sup>

第四,媒体和舆论公开。媒体和舆论公开属于合法公开的一种情形,但是与《个人信息保护法》第13条第1款(5)项的规定会出现竞合的情况,该项规定,“为公共利益实施新闻报道、舆论监督等行为,在合理的范围内处理个人信息”,也构成个人信息处理的一个独立的合法性基础。此外,《民法典》第990条也规定了人格权的“合理使用”情形:“为公共利益实施新闻报道、舆论监督等行为的,可以合理使用民事主体的姓名、名称、肖像、个人信息等”;根据立法者的解释,“舆论监督”的定义是“社会公众运用各种传播媒介对社会运行过程中出现的现象表达信念、意见和态度,从而进行监督的活动”,<sup>[36]</sup>从而其主体不限于新闻媒体机构,体现了对于公众言论自由等价值的维护。实践中,如出现为公共利益而实施新闻报道和舆论监督场景下的公开信息利用情形,则应当优先适用第(5)项的例外规定。

第五,其他个人或企业的公开。其他个人或企业未经个人同意而公开个人信息的情形,较有可能落入非法公开的范畴,但是实践中公开情形包罗万象,亦有可能存在其他具备合法性和合理性的公开情形,例如基于个人言论和信息自由、企业经营权行使等情形。由于公开个人信息呈现的是客观上的公开状态,追溯其初始公开的合法性往往具有较高难度,实践中可能最后转化为个案证明和举证责任分配的问题。<sup>[37]</sup>

个人信息合法公开的类型化区分,对于已公开个人信息相关规则的构建,颇为必要。合法公开不同类型及其背后体现的价值取向,会导致对于“合理范围”“重大利益损害”“拒绝权行使及其例外”等具体规则的不同适用倾向,此外,对于个人信息处理者的注意义务,也会产生不同的影响。

## 2. 对于公开“合法性”的注意义务

个人信息处理者需要根据不同情况承担“合法性”判断的注意义务。总体来说,为促进公开个人信息公共价值的实现,不应给主体施加过高的注意义务,否则,在大多数初始公开合法性难以判断的情形中,已公开个人信息的规定将形同虚设。

第一,根据初始公开的不同类型,其判断难度也各不相同,注意义务的认定标准也应有不同。政府公开是确定性较高的一类情形,尽管政府信息初始公开本身的合法性也有可能受到当事人的质疑和挑战,但是对于已公开个人信息的处理者来说,应可推定政府公开信息的合法性,不应就此负有更高的注意义务。新闻报道的公开情形亦属于较为容易判断合法性的情形。在个人自行公开、经过个人同意的公开、其他公开的情形,合法性判

[35] 参见王敬波:《政府信息公开中的公共利益衡量》,《中国社会科学》2014年第9期,第105页。

[36] 黄薇主编:《中华人民共和国民法典人格权编解读》,中国法制出版社2020年第1版,第52页。

[37] 对证明已公开个人信息合法性难度的探讨,参见周汉华:《平行还是交叉——个人信息保护与隐私权的关系》,《中外法学》2021年第5期,第1179页。

断难度相对较大,此时可借鉴美国《加州隐私权法》中关于处理者“有合理依据相信”的标准,处理者可以通过证明具体场景中存在合理依据的情形,例如有合理依据相信经过认证的社交媒体账号为其本人,来证明其履行了注意义务。

第二,根据个人信息的不同类型,适用不同的注意义务标准。对于敏感个人信息等可能给个人带来较高风险的已公开个人信息,以及未成年人等特殊群体的个人信息,处理者应当承担更高的注意义务。

第三,根据不同的个人信息处理行为模式,确定不同的注意义务标准。例如在搜索引擎的情形下,由于其原理在于对于全网公开信息进行检索并展示,需要处理海量数据,如要求其承担针对公开信息所涉个人信息初始公开合法性的全面审查义务,则会使其承担过高成本,损害其模式的正常运转,因此,在没有出现根据司法解释规定可以认定为较为明显的情形下,<sup>[38]</sup>应当要求搜索引擎承担较为有限的注意义务。此类情况也应当可以类推适用于从事公开信息合法抓取及从事数据挖掘的处理者。但对于特定领域个人信息进行垂直、深度处理和加工的处理者,则有可能承担比搜索引擎更高的注意义务。

在北京互联网法院判决的孙某诉百度案中,对于百度作为搜索引擎需要承担的注意义务,从涉案信息风险程度、搜索引擎处理模式的特点以及百度已经开通便捷维权渠道等理由出发,法院认定百度“作为全网信息搜索引擎服务提供者,需对海量互联网信息进行搜索、存储、归目等技术处理,不应苛求其对所有信息是否侵权进行逐条甄别和主动审查”,在原告提起删除请求前,已经尽到注意义务。<sup>[39]</sup>法院的论证过程一定程度上已经体现了上述类型化分析的思路。

在欧盟针对搜索引擎的案件判决中,欧洲法院也认为,搜索引擎不需要“事先”针对公开个人信息的合法性进行审查,或获取同意,而只需要在事后接收到数据主体的删除请求之后做出判断。<sup>[40]</sup>尽管已公开个人信息在欧盟《一般数据保护条例》并没有规定为同意的例外情形,但是如前文所述,基于“合法利益”条款以及信息与言论自由、公众知情权等公共利益的考量,法院针对搜索引擎的处理行为做出了与我国立法规定在效果上类似的决定。

## (二) 已公开个人信息处理行为的“合理范围”和“个人权益重大影响”

根据《个人信息保护法》第 27 条的规定,针对已公开个人信息应在“合理的范围”内处理,如果超出合理范围,或者处理行为对“个人权益有重大影响”,则需要取得个人同意。“合理范围”和“个人权益重大影响”两个概念,目前尚未在实践中得到解释和检验。

第一,需要厘清“合理范围”与个人信息初始公开目的的关系。在《个人信息保护法》一审和二审征求意见稿里,皆规定:“个人信息处理者处理已公开的个人信息,应当

[38] 最高人民法院《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(法释〔2014〕11号)》第9条。

[39] 孙某与北京搜狐互联网信息服务等人格权纠纷案,北京互联网法院(2019)京0491民初10989号民事判决书。

[40] Case C-136/17 *GC and Others* EU:C:2019:773.

符合该个人信息被公开时的用途；超出与该用途相关的合理范围的，应当取得个人同意。”<sup>[41]</sup> 二审征求意见稿中，改为与现行第 27 条相同的内容，并且与《民法典》相关规定保持一致。

从立法历史可见，立法者放弃了“符合初始公开用途”的限定标准，采用了更加宽泛的“合理范围”表述，一定程度上也是回应了确定初始公开用途难度过高的质疑。<sup>[41]</sup> 由此可见，现行立法中的“合理范围”应当不受初始公开用途和目的的限制。当然，符合初始公开用途和目的的处理行为，例如对于个人自行公开的商业推广信息进行进一步传播，一般应当被认定为属于“合理范围”。

有学者认为，若处理行为与该信息公开目的没有根本抵触，则属于合理范围，但如果明显违背初始公开目的、明显改变已公开个人信息的用途的情形，应当认为超出了合理范围，甚至有可能构成侵犯公民个人信息罪。<sup>[42]</sup> 另有学者认为，针对已公开个人信息的合理处理，应作相对宽泛的理解，原则上，只要法律法规没有明确禁止的处理行为，均可以认定为合理。例如，针对政府公开的企业登记信息，收集后进行商业利用，虽然可能超出初始公开的用途和目的，依然可以认为属于“合理范围”。<sup>[43]</sup> 这两种观点中，后一种虽然可能偏于宽泛，但应当更为接近立法原意。

第二，在确定“合理范围”时，或可参照欧盟《一般数据保护条例》中已公开个人信息利用的常见合法性基础“合法利益”原则的认定方法，将数据处理者或第三方的合法利益与数据主体的利益进行比较。<sup>[44]</sup> 但因为是已合法公开的个人信息，其中应当体现相当的信息和自由权利、公众知情权等公共利益，因此衡量的天平应当适当向数据处理者和公众倾斜。除非数据主体可以证明自己具有明显超越处理者和第三方利益的情形，否则应当认定处理行为属于“合理范围”。

第三，需要确定“个人权益重大影响”的认定标准并厘清其与“合理范围”的关系。《个人信息保护法》第 27 条规定的“对个人权益有重大影响”，与《民法典》第 1036 条规定的“侵害其重大利益”，措辞有区别，范围亦应有不同。从字面上看，“对个人权益有重大影响”的范围应当较大，包括了“侵害其重大利益”的情形。侵害利益的情形，可以包括“利用已公开个人信息实施可能危及公民人身或财产安全的违法犯罪行为”，<sup>[45]</sup> 典型的如侵害名誉权、<sup>[46]</sup> 实施电信诈骗等。当然，这些侵害行为其实通常不可能如第 27 条之规定去取得个人同意。

除了违法和侵权等法律禁止的行为，也可能存在其他处理行为对个人权益产生重大

[41] 参见周汉华：《平行还是交叉——个人信息保护与隐私权的关系》，《中外法学》2021 年第 5 期，第 1179 - 1180 页。

[42] 参见周光权：《侵犯公民个人信息罪的行为对象》，《清华法学》2021 年第 3 期，第 35 - 37 页。

[43] 参见喻海松：《民法典视域下侵犯公民个人信息罪的司法适用》，《北京航空航天大学（社会科学版）》2020 年第 6 期，第 7 - 8 页。

[44] 欧盟《一般数据保护条例》第 6.1(f) 条。

[45] 周光权：《侵犯公民个人信息罪的行为对象》，《清华法学》2021 年第 3 期，第 35 - 37 页。

[46] 恶意收集和利用有失偏颇的公开信息侵害名誉权的例子，可参见周大福与创客互动网络侵权责任纠纷案，北京互联网法院（2019）京 0491 民初 22797 号民事判决书。该案涉及的是针对企业的名誉侵权，但是类似的情况也可以适用于个人。

影响的情形。例如,处理行为涉及到基于个人信息加工而对主体做出评分和决策,且结果会对主体的人身和财产利益产生重大影响,如影响就业、信誉、贷款,形成具有约束力的征信结果甚至司法裁决等。<sup>[47]</sup> 但是,在确定已公开个人信息的处理行为是否需要经过个人同意时,还需要与其他因素和价值考量进行平衡,并不只是单向考察针对个人信息主体的利益影响。例如,在政府信息公开和搜索引擎两种情形下,应当更倾向于公共利益和信息、言论权利的考量,具体在本小节最后一点展开。

“个人权益重大影响”和“合理范围”之间,应是互斥的关系,如若能够符合“合理范围”的要件,则通常不会对个人权益造成重大影响;反之亦然,如果对个人权益业已造成重大影响,则处理行为通常不太可能落入“合理范围”。由于两个概念都具有抽象性,虽然立法条文中将两者分开规定,在实际规则应用中,较难想象会存在两者并存的情形。在这个意义上可以认为,不对个人权益造成重大影响,可以作为解释“合理范围”的认定情形之一。

第四,个人权益可以通过个人行使“拒绝权”机制得到保护,只要信息处理者提供了较为便捷的行使拒绝权的渠道,则并无必要基于“个人权益重大影响”和“合理范围”确立针对信息处理者过于严格的标准。通过将证明责任和拒绝权利分配给数据主体,来取得已公开个人信息上各方主体利益的相对平衡。

第五,针对政府信息公开与搜索引擎两种典型场景,“合理范围”的确定应当尽量宽泛。政府信息公开中承载了公共利益和公共职权的行使,对其进行收集、加工和利用,是政府信息公开制度功能的正常延伸和实现。例如,关于司法裁判文书的公开,如前文所述,苏州中院和北京四中院虽然在最后判决结果上存在差异,但是对于原告主张拒绝权之前数据库处理裁判文书信息的行为,两家法院皆认为属于合法范畴。<sup>[48]</sup>

搜索引擎是对公开信息进行全面的收集、检索、展示的行为模式,通常是对已公开信息的整理和再现,不会涉及进一步的加工行为,因此通常可以被认定属于“合理范围”。即使在欧洲涉及主体“被遗忘权”成功行使的案件中,搜索引擎也仅承担“事后”删除的义务,而一般不需要就其处理行为获得“事先”同意。<sup>[49]</sup>

### (三) 拒绝权的行使与例外

#### 1. 拒绝权及其行使

《民法典》和《个人信息保护法》中皆规定,个人“明确拒绝”情形下,已公开个人信息的处理者不得继续处理个人信息。拒绝权的规定表明,我国的已公开个人信息处理规则

[47] 此处可以参考欧盟《一般数据保护条例》第 22 条关于“自动化决策,包括用户画像”中关于“重大影响”的规定,其中就包括“自动化决策会对数据主体产生法律效力或对其造成类似的重大影响”。相关讨论参见张凌寒:《商业自动化决策的算法解释权研究》,《法律科学》2018 年第 3 期,第 65-74 页;张欣:《免受自动化决策约束权的制度逻辑与本土构建》,《华东政法大学学报》2021 年第 5 期,第 27-40 页;蔡星月:《算法决策权的异化及其矫正》,《政法论坛》2021 年第 5 期,第 25-37 页。

[48] 参见伊某与苏州贝尔塔数据技术有限公司人格权纠纷案,江苏省苏州市中级人民法院(2019)苏 05 民终 4745 号民事判决书;梁某与北京汇法正信科技有限公司网络侵权责任纠纷案,北京市第四中级人民法院(2021)京 04 民终 71 号民事判决书。

[49] Case C-131/12 *Google Spain and Google EU*; C:2014:317; Case C-136/17 *GC and Others EU*; C:2019:773.

并非一项完全的“同意豁免”规则或者“合理使用”制度,而是将个人的决定权从同意为基础的“选择进入”机制减损为一种“选择退出”机制,类似于知识产权法中的默示许可制度。<sup>[50]</sup>“选择退出”机制下,虽然也使得个人针对已公开个人信息掌握一定决定权,但是与“选择进入”机制不同,个人需要承担个人信息利用的调查和了解成本,控制风险的成本转移到个人信息主体身上,结果上导致个人信息控制权的弱化。<sup>[51]</sup>

不过,“选择退出”机制下,已公开个人信息的处理者依然需要承担《个人信息保护法》第17条规定的告知义务,这使其在一定程度上需要分担信息传递的成本。不过,由于缺乏取得个人同意的环节,已公开个人信息通常是批量处理,如果要求逐一联系信息主体进行告知,实质上会架空已公开个人信息基本规则,无法实现其立法目的。因此,可考虑允许处理者通过公示方式进行一揽子告知的方式,来履行其告知义务。欧盟《一般数据保护条例》第14.5条也规定,如果告知义务是不可能的,或者需要不成比例的工作量,特别是在出于公共利益、科学、历史研究或者统计目的的情况下,可以豁免处理者的告知义务。<sup>[52]</sup>

对于已公开个人信息主体控制权的弱化,其合理基础当然是建立在已公开个人信息本身所具有的公共价值基础之上。而当已公开个人信息是基于个人“自行公开”或基于个人同意的公开的情形下,这已经不能称之为一种弱化,而实际上是个人行使个人信息决定权的一种表现。在这两种情形下,个人行使“拒绝权”,有点类似于“撤回同意”,并可据此行使删除权。<sup>[53]</sup>

个人信息主体行使拒绝权的形式和要件,可以参照民法上关于网络侵权的“通知删除”机制。<sup>[54]</sup>根据有关司法解释,有效的通知需包含通知人的姓名和联系方式、侵权内容的准确定位信息、删除信息的理由等内容,并向网络服务提供者以书面形式或者其公示的方式发送。<sup>[55]</sup>在孙某诉百度公司人格权纠纷案中,双方就孙某发出的通知是否有效产生争议,法院认为原告“通过百度网站自行设定的用户问题反馈途径,提供了原告身份证明、要求删除信息的具体链接地址、要求删除的理由及初步证据,上述通知准确送达了被告,包含了有效通知所需的必要信息,构成有效的通知”。<sup>[56]</sup>不过,网络侵权领域的“通知删除”机制指向的网络服务提供者并非侵权行为的直接实施者,“通知删除”机制还有相应的反通知等程序;<sup>[57]</sup>而在已公开个人信息保护中,“拒绝权”行使的对象是个人信息的处理者,即直接行为人,一般也不会有转交通知和反通知等步骤。因此,行使“拒绝权”与

[50] 参见王国柱:《著作权“选择退出”默示许可的制度解析与立法构造》,《当代法学》2015年第3期,第108-109页。

[51] 参见冯恺:《个人信息“选择退出”机制的检视和反思》,《环球法律评论》2020年第4期,第153页。

[52] 欧盟《一般数据保护条例》第14.2(f)、14.5(b)条。

[53] 撤回同意和删除权,分别规定于《个人信息保护法》第15条和第47条。

[54] 参见《民法典》第1195条。

[55] 《最高人民法院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》(法释〔2014〕11号)第5条。

[56] 孙某与北京搜狐互联网信息服务有限公司等人格权纠纷案,北京互联网法院(2019)京0491民初10989号民事判决书。

[57] 《民法典》第1195-1196条规定了通知移交和反通知机制。关于《电子商务法》上知识产权通知删除机制的讨论,参见刘晓春:《〈电子商务法〉知识产权通知删除制度的反思与完善》,《中国社会科学院研究生院学报》2019年第2期,第124-136页。

“通知删除”规则虽然在形式和效果上存在相似之处,但依然是在原理和制度上彼此独立的权利行使机制。

## 2. 拒绝权的例外

《民法典》和《个人信息保护法》中规定的针对已公开个人信息的拒绝权,皆未规定例外情形。但是,已公开个人信息的不同公开类型下,是否可以毫无例外的全部行使拒绝权,尚存疑虑。对于个人自行公开、基于个人同意的公开这两种情形,个人行使拒绝权一般而言应无疑义。但是,对于政府信息公开、媒体和舆论公开的情形,个人行使拒绝权是否应当受到限制,是否应当考虑信息流通、言论价值、公众知情权、科学研究等公共利益,应有很大讨论空间。

在关于裁判文书公开信息利用的南北两份判决书中,其意见分歧的核心焦点即在此处。苏州中院认为个人应当可以行使拒绝权,而北京四中院则认为,裁判文书公开信息中的公共利益应当优于个人权益,此种情况下个人不能行使拒绝权。<sup>[58]</sup>

在欧盟关于被遗忘权的案件纠纷中,法院在有的判决中支持了原告的删除请求,如“谷歌西班牙”案;而在其他判决中支持了被告不删除链接的主张,即使在涉及政治观点等敏感个人信息的情况下,法院也强调信息流通和言论价值、科学历史研究等公共利益的重要性,认为谷歌可以不予删除,体现了较为开放的利益衡量思路,尤其是对公开信息中公共利益价值的重视。<sup>[59]</sup>

借鉴欧盟《一般数据保护条例》中规定的相关例外规定,例如,第 17 条第 3 款针对删除权也规定了基于公共利益的例外,<sup>[60]</sup>在我国关于已公开个人信息拒绝权的制度设计中,应当也创设例外规则。这些例外可以包括以下三种情形。

第一,政府信息公开作为初始公开的情形,对其的后续处理行为原则上不应允许个人行使拒绝权。此时也可能存在对个人信息主体造成不利影响的情形,例如,上述裁判文书公开信息的商业数据库利用,有可能影响到个人信息主体的声誉和后续就业机会,这在通过裁判文书公开犯罪记录的情况下尤其明显。但是,这种影响应当在政府信息初始公开的时候就进行充分考虑,将其与信息公开的公共利益进行充分权衡从而做出决定。例如,《政府信息公开条例》第 15 条规定,“涉及商业秘密、个人隐私等公开会对第三方合法权益造成损害的政府信息,行政机关不得公开。但是,第三方同意公开或者行政机关认为不公开会对公共利益造成重大影响的,予以公开。”《最高人民法院裁判文书公布管理办法》也对不宜公开的信息作了列举,其中包括涉及国家秘密、商业秘密、未成年人犯罪和个人隐私情况等。《最高人民法院关于人民法院在互联网公布裁判文书的规定》中,提出对特殊裁判文书隐名处理的要求,公布裁判文书应保留部分个人信息(包括自然人的姓名等)

[58] 参见伊某与苏州贝尔塔数据技术有限公司人格权纠纷案,江苏省苏州市中级人民法院(2019)苏05民终4745号民事判决书;梁某与北京汇法正信科技有限公司网络侵权责任纠纷案,北京市第四中级人民法院(2021)京04民终71号民事判决书。

[59] Case C-131/12 *Google Spain and Google EU*; C:2014:317; Case C-136/17 *GC and Others EU*; C:2019:773; Case C-398/15 *Commercio, Industria, Artigianato e Agricoltura di Lecce v. AEPD*, ECLI:EU:C:2017:197.

[60] 欧盟《一般数据保护条例》第 17.3(a)-(e)条。

等的要求。<sup>[61]</sup>就个人信息的匿名化、去标识化等措施,应依据这些规定,将其对个人权益可能造成的损害及其合比例性问题,在初始公开阶段即进行充分考虑。由此,在裁判文书公开信息利用的南北两份判决中,北京四中全会的判决认为个人信息主体的拒绝权应该受到限制,创设了司法公开信息处理情形下拒绝权的例外,应获肯定。

此外,个人信息主体如对初始公开中政府行为的合法性存疑,可以通过挑战该种初始公开行为的方式来实现权利的维护和救济。<sup>[62]</sup>如政府的初始公开行为被认定为超越了合法范围而侵害个人信息,后续个人信息处理者应有义务配合删除此类信息。<sup>[63]</sup>

第二,基于新闻报道和舆论公开信息的后续处理,原则上不应允许个人行使拒绝权。一方面,这是新闻报道和舆论监督的公共价值和功能所决定的,如果允许个人通过行使拒绝权删除相关信息,此类公开信息的功能在很大程度上就会落空。另一方面,《个人信息保护法》第13条规定的为公共利益实施的新闻报道和舆论监督行为,并未规定拒绝权,因此应当优先适用该条规定。

第三,其他由他人合法公开的情形,应视其具体情况,由执法机关或法官进行具体利益衡量,其中需要考虑的因素包括:初始合法公开的目的和范围;信息流通和言论价值;公众知情权;个人信息主体在特定情形下的个人权益;个人信息处理者和第三方的合法利益等,在此基础上做出个案的裁决,决定是否支持拒绝权的行使。

#### 四 结语

已公开个人信息的保护和利用中,立法条文层次并不复杂,但是实践适用场景较为丰富,且争议频发。应当在这个领域确立层次清晰的规则适用体系,划分自行公开和合法公开的不同类型,在确定信息处理者关于合法性认定的注意义务、信息处理行为的合理范围、是否对个人权益造成重大影响、拒绝权的行使及其例外时,应当充分考虑个人信息公开的类型、个人信息本身的敏感程度、信息处理行为的类型等要素,进行类型化的考察和规则适用。在已公开个人信息保护和利用的法律适用中进行利益衡量,应当充分考虑其中体现的公共利益价值,特别是针对政府信息公开和搜索引擎利用等典型场景,通过案例规则的探索和积累,形成指南、司法解释等规则,明确类型化的规则并通过列明考察要点清单的形式,为复杂的实践场景应用提供更强的确定性并指引方向。

[本文为作者参加的2020年度国家社会科学基金重大项目“网络空间政策法规的翻译、研究与数据库建设”(20&ZD179)的研究成果。]

[61] 《最高人民法院裁判文书公布管理办法》第4条;《最高人民法院关于人民法院在互联网公布裁判文书的规定》第8、10、11条。

[62] 例如,参见李世华与长沙市开福区人民政府行政纠纷案,湖南省高级人民法院(2015)湘高法行终字第10号判决书,该案即为挑战政府公开个人身份证号行为合法性而成功的案例。

[63] 《最高人民法院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》(法释[2014]11号)第9条。

[ **Abstract** ] Currently, there are three legislative models for publicly disclosed personal information around the world, reflecting different value orientations. The EU GDPR does not separately stipulate publicly disclosed personal information, but provides applicable space through principles such as “legitimate interest” and “public interest exception”. The United States excludes specific disclosed personal information from the scope of protection. In China, the rules for the protection and utilization of publicly disclosed personal information have been established in the Civil Code and the Personal Information Protection Law, but their application is still controversial in practice. Typical disputes include handling government public information, public information processing in search engines, etc. Compared with the EU and US legislative models, China’s model has its own unique features: it reduces the right of personal decision to the right of “opt-out”, but retains the right of individuals to refuse and set no exception to this right. From a theoretical point of view, on the one hand, publicly disclosed personal information has public feature, embodying public interests such as the public’s right to know, freedom of information, and freedom of speech. On the other hand, it is still the object of private rights protection in nature, only the exercise of these rights are subject to certain restrictions. A necessary flexibility of the boundary between public interests and private rights needs to be maintained to adapt to actual dynamic needs. In the establishment of rules for the protection and use of publicly disclosed personal information, situations of legal disclosure should be classified into five categories, namely direct disclosure by individuals on their own initiative, disclosure with individual consent, government disclosure, media and public opinion disclosure, and disclosure by other individuals or corporations, and full consideration should be taken of the type of personal information disclosure, the sensitivity of personal information itself, the type of information processing behavior and other factors in the determination of the standards on the application of the rules, including the information processor’s duty of care regarding legality determination, reasonable scope of information processing behavior, whether it has a significant impact on personal rights, the exercise of the right to refuse and its exceptions, etc. The determination of “reasonable scope” should not be limited to the scope of the purpose of the initial disclosure. In the case of government information disclosure, public opinion supervision, and search engines, exceptions should be created for the individual’s “right to refuse”, so as to ensure that the public interest embodied in publicly disclosed personal information is protected, prevent excessively high costs of using public information, and develop and improve the system of rules on the protection of publicly disclosed personal information.

---

---

(责任编辑:支振锋)