浙江理工大学学报，2020，44(2)：193-197
Journal of Zhejiang Sci-Tech University
DOI：10.3969/j.issn.1673－3851(s).2020.02.011

政府强制公开个人信息的技术区分保护的策略

邢益精，康建光
（浙江理工大学法政学院，杭州 310018）

摘　要：《中华人民共和国政府信息公开条例》第15条确定了行政机关基于公共利益的考量，违背信息主体意志而强制公开个人信息的合法性。而技术区分保护的策略成为平衡政府信息公开与个人隐私信息保护的重要途径。在分析技术区分保护的法律基础、内涵、价值与考量因素的基础上，提出了个人信息技术区分保护的策略。首先，行政机关应将政府持有的个人信息根据内容分为十一大类，并根据个人信息涉及隐私的程度分为高度、中度、轻度三个等级。其次，在此基础上运用失真、加密、匿名化等隐私保护技术对强制公开的个人信息进行区分处理。最后，经技术处理的个人信息被强制公开后，还应采取目的限制、禁止再识别等安全保障措施，降低个人信息被识别的风险，进一步保障信息主体的隐私权益。

关键词：政府信息公开；个人信息；隐私保护；技术区分保护；强制公开；策略
中图分类号：D924　　**文献标志码**：A　　**文章编号**：1673-3851 (2020) 04-0193-07

Technical differentiation protection strategy for mandatory disclosure of personal information by the government

XING Yijing, *KANG Jianguang*
(School of Law and Politics, Zhejiang Sci-Tech University, Hangzhou 310018, China)

Abstract: Article 15 of the Regulations on the Disclosure of Government Information of the People's Republic of China determines the legitimacy that the administrative organ can violate the will of the main body of information and force the disclosure of personal information in consideration of the public interest. The technical differentiation protection strategy has become an important way to balance government information disclosure and personal privacy information protection. Based on the analysis of the legal basis, connotation, value and consideration factor of technical differentiation protection, this paper puts forward the technical differentiation protection strategy of personal information. First of all, the administrative agency should classify the personal information held by the government into eleven categories according to the content, and divide it into three levels: high, medium and light according to the degree of privacy of personal information. Secondly, on this basis, privacy protection technologies such as distortion, encryption, and anonymization are used to differentiate the mandatory disclosure of personal information. Finally, after the personal information processed by the technology is forcibly disclosed, security measures such as restriction of purpose and prohibition of re-identification should be taken to reduce the identified risks and further protect the privacy rights of the information subject.

Key words: the government information publicity; personal information; privacy protection; technical differentiation protection; mandatory disclosure; strategy

收稿日期：2019－03－08　　**网络出版日期**：2019－07－18
作者简介：邢益精(1967－　)，男，浙江桐庐人，副教授，博士，主要从事宪法与行政法方面的研究。

政府强制公开个人信息指的是行政机关为避免对公共利益造成重大影响,在未经信息主体同意的情况下,强制公开涉及个人隐私的政府信息的行政行为[1]。《中华人民共和国政府信息公开条例》(以下简称《条例》)第15条对政府强制公开个人信息有所规定。通过利益衡量和比例原则,承认强制公开个人信息行政行为的合法性,这在司法实践中已有具体运用,如全国法院2013年度政府信息公开十大案例之四——杨政权诉山东省肥城市房产管理局案①。在该案中法院权衡了个人隐私利益和公共利益,最终认为应以享受保障性住房人让渡个人信息的方式优先保护较大利益的知情权、监督权,行政机关应强制公开保障性住房人的个人信息。这是依据《条例》第15条,由行政机关强制公开个人信息的典型案例。不可否认,个人隐私信息应让渡于涉及公共利益的知情权。王敬波等[2]认为,探讨信息公开的利益平衡蕴含着如何对公私权利进行取舍的思想,这需要坚持社会公共利益至上的原则。但个人信息在当今社会具有重要作用,尤其对个人而言,个人信息的意义更是举足轻重。章剑生[3]认为,计算机作为行政工具之一被广泛运用于记载、传播个人隐私方面的行政信息,使个人隐私权受到了前所未有的威胁。个人隐私权最早由美国学者提出,它被认为是"不受打扰之权",指个人私生活不受侵犯。随着社会信息化的发展,个人的数据信息已经承载了大部分个人隐私。个人隐私权也逐步从个人生活不受打扰的消极权利转变为积极控制隐私信息的权利,这些隐私信息包括被行政机关收集的有关个人的政府信息。在电子政务广泛应用的当下,个人信息隐私权与个人知情权存在一定的冲突。因此,值得思考的问题是:行政机关在作出强制公开个人信息的决定的同时,能否采取措施对被公开的个人信息中的隐私予以保护?在现代信息技术的支持下,尝试探索采用技术区分保护的方式对公开的个人信息进行保护便成为一个有意义的研究课题。采用这一方式能够在保障公民知情权的前提下,尽可能减少因公开个人信息对公民造成的损害,保护个人隐私权益。

本文将从技术区分保护的法律基础和内涵着手,结合技术区分保护方式对保护政府强制公开的个人信息的价值,剖析技术区分保护的重要因素以及对强制公开的个人信息进行技术区分保护的策略。

一、技术区分保护的法律基础和内涵

行政机关决定强制公开个人信息,应根据个人信息涉及个人隐私的程度、公共利益的权衡以及申请信息公开的目的等,对强制公开的个人信息进行区分并适度公开。这不仅能保障申请人的知情权,也能有效保护第三人的个人信息。要处理好强制公开个人信息的权利关系,关键在于准确理解信息的技术区分保护策略并加以实践运用。

(一)法律基础

技术区分保护的构想源于政府信息公开的"可分割性原则",即凡是可以从含有豁免公开的信息中分离出来的非保密信息,都应毫无保留地予以提供。根据这项原则,信息中可以合理分离的任何部分,在删除根据豁免条款应予保密的部分之后,应当提供给请求获取信息的任何人[4]。《条例》第37条明确规定了这一原则,这为技术区分保护提供了充分的法律基础。技术区分保护虽不同于可分割性原则,前者是在决定公开后通过技术手段对个人信息的保护,后者是在决定公开前通过行政机关的利益衡量对保密信息的保护,但两者都是对信息的区分性保护,都是为了在充分保障公民知情权的同时保护个人隐私。

(二)内 涵

技术区分保护包含两方面的内容,即"技术"和"区分"。其中,"技术"指的是隐私保护技术,顾名思义就是用于保护隐私的技术,它兼顾了信息公开和隐私保护,一般可以从隐私保护程度、数据缺失程度、算法性能等方面进行对隐私保护技术进行评价;而"区分"的重点在于对个人信息中是否存在个人隐私、涉及隐私程度的大小做区分。因此,技术区分保护指的是根据强制公开个人信息涉及的隐私程度等因素,区分采用不同技术方法对个人信息进行处理,从处理后的信息无法直接识别出特定个人的保护手段。技术区分保护目的在于通过不同技术手段的运用,隐匿个人信息中的识别符,使特定个人无法被识别,最终实现对个人信息的保护。

技术区分保护的重点主要有三个:一是区分信息。强制公开的个人信息中包含了不同类型的个人隐私,这些不同类型的个人隐私公开对个人产生的

① 山东省泰安市中级人民法院,行政判决书(2013)泰行终字第42号。本案中杨政权向肥城市房产管理局申请公开经济适用房、廉租房的分配信息和所有享受该住房住户的审查资料信息(包括户籍、家庭人均收入和家庭人均居住面积等)。肥城市房产管理局向申请人公开了前者,但后者因涉及个人隐私未予以公开。终审法院认为,当涉及公众利益的知情权和监督权与保障性住房申请人一定范围内的个人信息权相冲突时,应将保障房的公共属性放在首位,使获得这一公共资源的公民让渡部分个人信息,既符合比例原则,又利于社会的监督和保障房制度的健康发展。

不良影响是不同的。只有根据涉及的隐私程度等因素对个人信息进行详细区分，才能对不同类的个人信息进行有差异性的技术处理，尽可能降低隐私信息公开所带来的不良侵害。二是区分技术处理手段。行政机关既然决定强制公开个人信息，那么对该个人信息的技术处理不能影响申请人对该个人信息利用之目的实现，即不能对申请人所需要的个人信息进行过度技术处理。因此，在区分信息的前提下，还应结合申请信息公开的目的，将个人信息的技术处理方式进行区分，有针对性地根据目的对个人信息做技术处理，使隐私信息在最小范围内公开。三是对技术处理之个人信息的再识别风险控制。一般而言，技术处理并不能使处理后的信息完全不能被用于识别信息主体，而且随着科技的发展，绝对的“无法识别”的个人信息几乎不存在。人们可以通过技术还原识别符、其他信息的重叠识别等方法间接识别出特定个人。因此，对强制公开的个人信息进行技术处理后，还需要采取相应的措施以降低经处理后的个人信息被再识别的风险。

二、技术区分保护的价值与考量因素

(一)技术区分保护在政府强制公开个人信息中的价值

政府强制公开个人信息的行为是基于公共利益的考量，舍弃了部分个人隐私利益，保障了公民的知情权。但是，在大数据技术不断发展的当下，个人信息对于个人、信息企业和政府机关都具有重要价值。尤其是对于个人而言，个人信息能反映出其工作、生活等多方面的隐私内容，是个人人格的重要体现。行政机关强制公开个人信息后，个人人格被暴露下公众视野中，这对个人的损害是十分严重且不可逆转的。因此，行政机关应保护强制公开的个人隐私信息，积极运用技术区分处理的保护措施。

一方面，技术区分保护能控制个人信息再识别风险，保护个人隐私。行政机关强制公开个人信息势必将其中涉及的个人隐私也一并公开，而个人隐私恰是个人不愿让他人知悉的内容。那么，如何尽可能减少甚至不公开个人隐私？技术区分保护就能较好地解决这个问题。通过区分强制公开的个人信息涉及隐私的程度，对不同类型的个人信息在公开前进行隐私保护技术处理，尽可能降低公开后的个人信息被再识别的风险，从而达到保护个人隐私的效果[5]。

另一方面，技术区分保护可以减少行政机关对强制公开个人信息的顾忌，降低行政行为的法律风险。强制公开个人信息是政府对个人隐私权益和公共利益博弈衡量之后作出的行政行为，但由于《条例》中关于是否采取强制公开个人信息行政行为的判断依据(如个人隐私、公共利益等概念)相对模糊，导致行政机关在做强制公开个人信息决定时无法可依，只能采取僵化的行政行为，或者全部公开，或者统一保护。而技术区分保护能减少行政机关因立法不明确带来的顾忌，使其将重点转移至决定强制公开个人信息后对隐私信息的保护。这样可以在顾及公共利益的前提下，尽可能保护个人隐私，从而降低因申请人和信息主体对行政行为不满而带来的行政诉讼风险。

(二)技术区分保护个人信息的考量因素

行政机关在对个人隐私与公共利益的利益衡量决定强制公开个人信息后，基于技术区分保护的考虑，应当判断个人信息中涉及个人隐私的程度如何，能否对个人信息进行区分处理；如果能做区分处理，采用何种技术处理方式可以在满足申请人目的的情况下，尽可能地保护个人隐私。因此，技术区分保护个人信息的考量应从三个因素展开。

第一，能否区分。能够对个人信息中的隐私部分进行区分是技术区分保护的前提。“区分”指的是涉及个人隐私的个人信息可以区别于其他部分的个人信息，毕竟并非所有的个人信息都构成个人隐私，个人隐私仅指行政机关掌握的个人信息中涉及个人隐私权的内容[6]。但是，如果申请人申请公开的信息就是涉及个人隐私的个人信息，或者个人隐私与其他部分的个人信息必须结合使用才有公开的意义，又或者即使隐匿个人隐私的信息，通过其他任一部分的个人信息都可以推测出整个个人信息的内容，那么这些个人信息就应认定为无法进行区分。

第二，能否处理。能否对个人信息中的隐私部分进行技术处理是技术区分保护的核心。“处理”指的是通过技术手段对涉及个人隐私部分的个人信息进行隐匿。技术处理方式有很多，包括数据失真、匿名化、加密等等，这些方式大多是通过对数据的替换或隐匿实现个人信息的处理。因此一般而言，技术处理只适用于电子化的个人信息，原始纸质的个人信息无法实现技术处理。不过，在大数据时代，大量的政府信息通过数据化保存和利用，因此技术处理可以在大多数情况下实现。

第三，难易程度。一是区分处理的难易程度。如果强制公开的个人信息中个人隐私部分既可以被

区分,又可以被处理,但区分处理所需要的技术操作繁琐,或处理时间过长,或处理成本过大等,技术区分处理存在较大的困难,那么该个人信息就不宜进行技术区分保护。二是再识别的难易程度。对个人信息进行技术区分处理的目的在于最大程度去除或模糊识别符,从个人信息无法直接识别出特定的个人。所以,如果在现有技术下,耗费合理的时间和成本,他人能够从通过技术处理后的个人信息识别出特定个人,那么这种技术手段在保护个人信息上就没有任何作用。因此,对个人信息再识别的难易程度将影响技术区分处理的方式[7]。

三、个人信息技术区分保护的策略

(一)确立个人信息的分类和分级制度

对个人信息进行分类、分级是强制公开的个人信息得以区分保护的前提。目前大多数国家对于个人信息的定义都采用了概括式和列举式并用的方式,这其中就蕴含了信息分类的思维。《中华人民共和国网络安全法》中明确规定了个人信息的定义,同样采取了概括式和列举式并用的方式。同时在国家标准GB/T 35273—2017《信息安全技术 个人信息安全规范》的附录中,针对个人信息归纳总结出了个人基本资料、个人身份信息、个人生物识别信息、网络身份标识信息、个人健康生理信息、个人教育工作信息、个人财产信息、个人通信信息、联系人信息、个人上网记录、个人常用设备信息、个人位置信息、其他信息共十三种类型,并对十三种类型信息举出详细具体的例子。虽然这一列举并不全面,但反映了中国正逐步形成个人信息分类保护的意识。

基于中国行政机关行使多方面公共职能的现状,个人从出生到死亡或多或少都和政府有联系,比如户口登记、婚姻登记、注销户口等等,行政机关收集、处理和利用的个人信息涉及到个人的方方面面,因此要对政府持有的众多个人信息分类存在一定的难度。在此,可借鉴中国台湾地区"个人资料保护法之特定目的及个人资料之类别"对个人信息的分类方法[8],将个人信息分为识别类,特征类,家庭情形,社会情况,教育、考选、技术或其他专业,受雇情形,财务细节,商业资讯,健康与其他,其他各类资讯共十个大类,并在每个大类以下列出各小类,再对部分小类进行列举式的解释。比如,在特征类大类个人信息以下划分了身体描述、个人描述、习惯、个性四个小类,身体描述类又列举了身高、体重、血型等具体的个人信息。这一方法是通过分类和列举的方式,尽可能全面地将现有的个人信息纳入法律规范的范畴之内,差异化、全面化地保护政府持有的个人信息。因此,笔者类似地将中国政府持有的个人信息分为十一个大类,并将其详细分类,如表1所示[9]。

表1 中国政府持有的个人信息分类

大类	小类	列举说明
个人识别类	自然属性识别类	姓名、外貌、声音、基因、指纹
	社会属性识别类	身份证号、护照号、驾驶证号、银行账号、社会保障卡号
密码类	—	银行账号密码、手机密码、微信密码、各类网络服务帐号密码
个人特征类	自然属性识别类	性别、年龄、身高、体重
	社会属性识别类	户籍、国籍、民族
家庭类	—	配偶、子女、父母等家庭成员、婚姻状况、亲属关系
财产类	收支类	工资收入记录、纳税记录、个人经营生产收入、接受赔偿、赠与、继承等活动的收入记录
	资产类	房屋、有价证券、基金、存款、外汇、现金、珠宝首饰、黄金、车辆、船舶、飞机等有形资产;专利、商业营业权等无形资产的权属证书记录、交易记录、租赁记录、担保记录等
	福利类	社会保险、住房公积金、失业金领取、低保户补助、征地拆迁补偿安置、房屋拆迁补偿安置
医疗类	—	就医记录、诊断治疗记录、检验结果、体检报告、病历
人事类	—	职位、职称、政治面貌、公务员行政级别、学历、教育经历、考试成绩、奖惩情况
通讯类	通讯地址类	手机号、固定电话号码、家庭住址、工作地址、电子邮箱地址、微信号、微博号
	通讯内容类	邮件、快件、电子邮件、通话记录、网络社交媒体聊天记录、在社交媒体上传的个人信息和操作记录
行踪类	—	汽车、火车、飞机等交通工具的购票记录和乘坐记录、办理护照、签证以及出入境记录、个人地理定位记录、宾馆住宿记录
司法类	—	行政处罚记录、诉讼记录、犯罪记录
组织类	—	党派、党员档案、党纪处分记录

表 1 根据个人信息内容的不同将其分为十一个大类，并通过详细举例覆盖了政府持有的大部分类型的个人信息。那么如果行政机关强制公开以上某一类个人信息，是否都应得到同样的技术处理保护呢？并非如此。中国最高人民法院、最高人民检察院公布的《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》给出了区分保护的思路。该解释第 5 条的规定①根据个人信息的不同类型对入罪标准做了不同规定，是对个人信息区分处理的尝试。这种区分处理的主要依据在于个人信息的泄漏可能给个人的人身、财产造成不良影响的程度大小。鉴于此，根据个人信息能否直接识别特定个人来衡量个人对个人信息的敏感程度，并结合个人信息与个人人格、隐私之间的密切程度来衡量个人信息被强制公开后对个人的人格尊严的不良影响程度，笔者对中国政府持有的个人信息进行分级，可以分为三个等级：高度涉及隐私、中度涉及隐私、轻度涉及隐私。结合表 1，可以将个人信息的十一个大类涉及的隐私程度分别定级，具体见表 2。

表 2　各大类个人信息涉及隐私程度分级

个人信息涉及隐私程度	个人信息大类
高度涉及隐私	个人识别类
	密码类
	医疗类
	司法类
	家庭类
中度涉及隐私	财产类
	通讯类
	行踪类
	组织类
轻度涉及隐私	个人特征类
	人事类

虽然涉及个人隐私的程度并非仅仅根据个人信息的公开对人格尊严的不良影响程度所决定，但人格尊严作为个人信息所能反映的最基础也是最根本的价值，因个人信息公开对人格尊严造成的影响应该是判断个人信息涉及隐私程度的最重要因素。因此，通过一般理性人的价值判断，对十一大类个人信息的涉及隐私程度进行分级，可以有效地区分保护政府持有的个人信息。

(二)灵活运用隐私保护技术区分方式

对政府持有的个人信息进行合理分级之后，行政机关应根据个人信息的不同隐私级别，运用不同的隐私保护技术方式对强制公开的个人信息进行处理。目前，隐私保护技术的方式主要有三种：失真、加密和匿名化。

数据失真技术是通过修改原始数据，使真实的原始数据被隐匿，而修改后的数据只显示数据的统计性规律。即通过失真技术处理后的数据并非原始数据，且无法重构出原始数据，但失真数据的某些性质与原始数据相同，他人仍可以从失真数据中获得等同于原始数据的部分信息。

数据交换和数据随机化是失真技术的两种技术手段。失真技术操作相对简单，但由于采用的是数据的替换、随机化等手段，数据被再识别的可能性较大，因此对个人隐私的保护也相对较弱。

数据加密技术是通过加密设置使他人对原始数据不可见，达到隐私信息隐藏的目的。加密技术并未改变原始数据，而是将部分隐私数据设置密码，使他人无法看到这些信息。主要的加密技术手段有分组加密、公钥加密、循环编码加密等。加密技术需要对数据进行加密算法操作，因此操作相对复杂，而且数据的整体性会有所缺失，但其对个人隐私保护的能力较强。

数据匿名化技术指的是有选择的发布隐私数据，并将隐私数据识别个人的风险控制在一定的阀值范围之内的方法。数据匿名化的模型有 k-匿名模型、(a,k)匿名模型、l-多样性隐私匿名模型等等，但其基本算法主要是两种，一是抑制，即不发布隐私数据；二是泛化，即通过将原始数据的具体属性值用一般的值来表示，从而降低数据的精确度，使他人只能从模糊的数据中低概率地识别个人[10]。除了抑制和泛化之外，近年来提出的聚类算法，核心内容是根据不同数据的特点，将其分为不同的簇，同一簇中的数据相似，不同簇的数据有较大差别[11]，再对各个簇进行识别符处理，降低数据的可识别性。匿名化技术主要是对数据进行概括性、抽象性的处理，使数据精确度降低。其模型和算法多样，操作较为简单，能快速处理多样复杂的个人数据，能有效保护个人隐私，但也不能否认匿名化技术处理后的数据可用性较低，他人可以从其获取的信息会比较少[12]。

综合三种隐私保护技术的特点以及对个人隐私保护的强度，结合政府持有个人信息的涉及隐私级

① 非法获取、出售或者提供公民个人信息，具有下列情形之一的，应认定为“情节严重”：非法获取、出售或者提供行踪轨迹信息、通信内容、征信信息、财产信息五十条以上的；非法获取、出售或者提供住宿信息、通信记录、健康生理信息、交易信息等其他可能影响人身、财产安全的公民个人信息五百条以上的；非法获取、出售或者提供以上两个方面以外的公民个人信息五千条以上的。

别,采用不同的隐私保护技术区分方式。一般而言,行政机关在强制公开个人信息时,高度涉及隐私的个人信息应经过加密技术处理;中度涉及隐私的个人信息应经过匿名化技术处理;轻度涉及隐私的个人信息应经过失真技术处理。通过有针对性地对强制公开的个人信息进行技术区分处理,能在信息公开的基础上最大限度地保护个人隐私,维护个人的隐私权益。

当然,在行政机关强制公开个人信息的过程中,选用何种隐私保护技术不是固定的,也不是仅由个人信息涉及隐私的程度决定的,还可能受到其他多方面因素的影响。一是考虑信息公开申请人的目的。《条例》第1条明确政府信息公开的目的是发挥政府信息对人民群众生产、生活和经济社会活动的服务作用,因此申请公开的政府信息往往是有特殊目的的。那么,行政机关应该结合申请人的特殊目的,尽可能少地强制公开个人信息的内容。比如申请人出于对房屋拆迁补偿金额不满,以维权为目的,要求公开同一拆迁地域的拆迁户补偿安置的信息。拆迁户补偿安置信息涉及到户主姓名、户口人数、拆迁面积等众多隐私信息,应属于中度涉及个人隐私的信息。但考虑到申请人申请公开信息用于比较房屋拆迁补偿金额,维护自身的财产权益,因此仅需公开户口人数、拆迁面积等与拆迁补偿金有关的信息即可,其他涉及个人隐私的信息可以做简单的失真技术处理,而无须因其属于中度涉及隐私的个人信息而做精确度降低的匿名化处理。二是考虑技术处理后的信息再识别的可能性。经过不同隐私保护技术处理后的个人信息再次被识别的可能性存在差异,针对不同的个人信息要采用不同的技术处理方式。那么,个人信息被再识别的可能性该如何评估?英国信息专员办公室于2012年颁布的指引性文件《匿名化:针对实践的信息保护风险管理》[13]给出了答案。该文件提出了“蓄意入侵者”检验来测试信息再识别的可能性。“蓄意入侵者”指的是希望通过技术处理的信息识别特定个人的假想主体,其相较于普通大众有更高的再识别技术,但远不能达到专家标准。同时假设“蓄意入侵者”抱有识别个人的特定目的,且能在现有技术下运用资源的获取、技术的调查等手段获取信息主体的其他信息,进而分析“蓄意入侵者”能否识别特定个人就能为评估再识别可能性提供依据,如果处理后的信息不能被“蓄意入侵者”所识别,那么该信息被再识别的可能性就很小[14]。因此,技术处理后信息被再识别的可能性的大小,影响着不同技术处理方式的采用。如手机号和网络社交媒体聊天记录都属于个人信息的通讯类,根据涉及隐私程度的分级本都应采取匿名化技术处理。但由于手机号在人们生活中应用广泛,加之手机号码实名制的推广,他人可以通过其他信息轻而易举地将经过处理的手机号再次还原识别;而网络社交媒体聊天记录相对隐蔽,不为外人所知,而且其存储介质相对局限,不易传播,其再识别的可能性就很小。所以对手机号的技术处理需要采取比匿名化技术保密性更强的加密技术,尽量降低其被再识别的可能。

综上所述,对行政机关强制公开的个人信息应采取何种隐私保护技术方法,应结合个人信息涉及隐私程度、申请公开的目的、经处理后信息的再识别可能性等因素而决定。而在实际操作过程中,强制公开个人信息的情况要复杂得多,仅仅考虑以上三个因素也许无法很好地兼顾到信息公开和隐私保护,行政机关应结合实际灵活运用隐私保护技术。

(三)强制公开后对经过技术处理的个人信息采取安全保障措施

运用隐私保护技术处理后的个人信息,很大程度上降低了个人信息内容的可识别性。但是,隐私保护技术处理并不能做到绝对的“无法识别”,否则该个人信息也不存在利用的价值。因此,为进一步保护信息主体的隐私权益,强制公开的个人信息即使经过了隐私技术处理,仍应在强制公开后对其进行安全保障。英国信息专员办公室颁布的《匿名化:针对实践的信息保护风险管理》[13]关于针对信息控制者公开信息后的健全保护机制主要包括以下几点:第一,目的限制;第二,信息安全和最小化原则;第三,对获取信息者进行调查;第四,控制将其他信息转移至原始信息环境的可能;第五,信息只限于指定事项下使用;第六,限制再公开信息;第七,禁止再识别信息;第八,采取技术和组织层面的安全措施;第九,限制信息的复制;第十,目的完成后归还或销毁信息;第十一,制定惩罚措施。以上这些保护义务的规定针对的是信息控制者,行政机关无疑是信息控制者之一,针对其强制公开个人信息的行为,这些规定值得借鉴。

因此,经过隐私保护技术处理后的个人信息被强制公开后,行政机关仍需要施以强有力的措施对其进行保障。其中包括但不限于以下内容:第一,信息只限于申请公开之目的范围内使用,不得另为他用,这是信息利用的目的限制原则所要求的;第二,

限制申请人对公开信息的再公开；第三，禁止申请人通过技术手段对经过技术处理后的公开信息再识别；第四，申请人在申请公开之目的实现后应归还或销毁信息；第五，申请人在使用公开信息时应保护信息安全，并尽可能降低信息使用频率，减少信息使用内容。这是信息利用的安全原则和最小化原则所要求的；第六，必要时行政机关和申请人可签订合同，约定申请人使用公开信息的责任和义务。这些措施为经过隐私保护技术处理后的个人信息在强制公开后又增加了一道保护屏障，如果隐私保护技术处理是对信息的内部保护，那么这些保障措施就是对信息的外部保护[15]。

四、结　语

行政机关在经过公共利益衡量后，舍弃部分个人隐私利益，作出强制公开个人信息的决定，以保障公民知情权和社会利益。但是基于个人信息在大数据时代中的巨大价值以及信息公开对信息主体造成损害的不可逆性，行政机关应当注重对强制公开个人信息的保护，积极采用技术区分的方式进行个人信息保护。如杨政权诉山东省肥城市房产管理局案中，申请保障性住房人的户籍信息属于个人特征类，人均住房面积、家庭人均实际收入信息属于财产类，分别属于轻度和中度涉及隐私。行政机关依据判决对这些个人信息进行公开时，应当对前者进行失真技术处理，对后者进行匿名化处理，再向申请人公开。并向申请人声明该信息不得再传播公开，禁止对其再识别，要求申请人在达成公开之目的后归还或销毁信息。

行政机关运用技术区分保护的方式对强制公开的个人信息进行技术区分处理，将各类政府信息进行分级后，可以根据信息的隐私程度与敏感程度，区分使用失真、加密、匿名化等技术手段对政府强制公开的个人信息进行处理。这一保护策略可以在保障公民知情权和公共利益的前提下，尽可能减少对个人隐私的侵害，兼顾了个人信息的利用和保护，对行政机关正确运用强制公开政府信息制度有所裨益。当然，由于技术区分保护要基于政府信息的电子化以及相关的计算机算法技术，在实践中这一保护策略能否实现还有赖于行政机关的现实条件与工作人员的实践。但技术区分保护能在平衡个人隐私权、个人知情权与公共利益之间发挥效能，这对于行政机关解决强制公开个人信息的相关问题未来可期。

参考文献：

[1] 杨登峰.政府强制公开第三人信息程序之完善[J].法学，2015(10)：93-101.

[2] 王敬波，李帅.我国政府信息公开的问题、对策与前瞻[J].行政法学研究，2017(2)：77-93.

[3] 章剑生.知情权及其保障：以《政府信息公开条例》为例[J].中国法学，2008(4)：145-156.

[4] 杨寅，韩磊.政府信息公开中的可分割性原则及其司法运用：对赵某不服不予信息公开案的法律分析[J].行政法学研究，2010(1)：114-118.

[5] 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)，2018，39(4)：64-75.

[6] 李广宇.政府信息公开诉讼：理念、方法与案例.[M].北京：法律出版社，2009：98.

[7] 朱静. 困境与完善：信息可分割性原则的司法审查——以《政府信息公开条例》第 22 条为研究视角[C]// 最高人民法院.全国法院系统第二十二届学术讨论会论文集，2011.

[8] 中国台湾法务部：电脑处理个人资料保护法之特定目的及个人资料之类别[EB/OL].(2011-07-20)[2018-06-08].http://www.docin.com/p-234331032.html.

[9] 周庆山，王琪斯.政府信息公开中的个人信息分级保护问题初探[J].北京电子科技学院学报，2017，25(3)：1-10.

[10] 李晓晔，孙振龙，邓佳宾，等.隐私保护技术研究综述[J].计算机科学，2013，40(Z2)：199-202.

[11] 孔志伟，魏为民，杨朔，等.基于数据匿名化的隐私保护研究[J].上海电力学院学报，2017，33(6)：586-590.

[12] 李守威. 个性化隐私匿名方法的研究[D].哈尔滨：哈尔滨工程大学，2012：7-8.

[13] UK. Information Commissioner's Office. Anoymisation: Managing data protection risk code of practice[EB/OL].(2018-06-08)[2019-06-03]. https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf.

[14] 张晨原.数据匿名化处理的法律规制[J].重庆邮电大学学报(社会科学版)，2017，29(6)：52-58.

[15] 王融.数据匿名化的法律规制[J].信息通信技术，2016，10(4)：38-44.

(责任编辑：陈丽琼)