doi:10.13582/j.cnki.1672-7835.2023.05.018

敏感个人信息行政许可的公法效用、体系难题与法治完善

李熠

(广州大学 党内法规研究中心,广东 广州 510006)

摘　要:敏感个人信息的法律保护,正在成为法学界讨论的热点命题。而《个人信息保护法》第 32 条则为敏感个人信息的处理提供了一种全新的路径:行政许可。该路径体现出了明显的公法效用:补足了敏感个人信息的行政法保护,强化了敏感个人信息公共风险预防作用,拓宽了敏感个人信息的救济途径。然而,敏感个人信息的行政许可路径在我国也面临着一系列的体系性难题:告知同意规则与行政许可的形式冲突、充分必要规则与行政许可的价值冲突、意思自治规则与行政许可的程序冲突等。因此,为了完善敏感个人信息的法治保护,我国应当明确行政许可的敏感个人信息判断标准及其优先效力,创设行政许可的具体条件以及限制性措施,并以行政许可承诺制来抑制意思自治规则。

关键词:敏感个人信息;告知同意规则;安全保障义务;行政许可

中图分类号:D912.1　　**文献标志码**:A　　**文章编号**:1672-7835(2023)05-0143-07

一　问题的提出

数字时代,敏感个人信息的法律保护问题,已经成为法学界无法绕开的重要话题。特别是随着人脸识别技术、身联网技术等科技的广泛运用①,处理个人信息的方式也更加丰富,敏感个人信息逐渐成为一种具有市场价值、人身价值的“身份确认”方式②。对此,我国《个人信息保护法》第 32 条规定:“法律、行政法规对处理敏感个人信息规定应当取得相关行政许可或者作出其他限制的,从其规定。”这意味着,在敏感个人信息处理上,我国可以设定相应的“行政许可”,并将其作为个人“同意”规则的前置性程序。然而,在人脸识别技术、身联网技术不断作用于人身的当下,我国一方面正在面对敏感个人信息保护与人身保护的双重压力;另一方面又尚未建立明确的行政法保护机制,甚至行政机关尚未回应《个人信息保护法》的“行政许可”要求。有鉴于此,敏感个人信息的法治保护,亟须获得行政法的制度性回应,这无疑会补全敏感个人信息保护的公法保护缺陷,提高敏感个人信息的保护效果。

二　敏感个人信息行政许可的公法效用

(一)补足敏感个人信息的行政法保护

维护敏感个人信息的安全,不仅是个人信息处理者的一种私义务,同时也是行政机关的一项公共义务。对于后者而言,行政机关的公共义务,源自行政机关的公共安全保障职能,而非来自某项具体的法定职权。一旦侵犯敏感个人信息的行为危及了公共安全,那么行政机关便有义务施加国家保障。因此,相较于个人信息处理者的安全保障义务,行政机关承担出于保护公益及社会公众信息安全的特殊保护义务。例如欧盟《通用数据保护条例》就将种族或民族起源、政治观点、宗教和哲学信仰、工会资格、基因信息和生物信息等

收稿日期:2023-05-02

基金项目:广东省社科规划项目(GD22CFX06)

作者简介:李熠(1990—),女,广东惠州人,研究员,主要从事民商法学、数字法学研究。

①关于“身联网”法律问题的讨论,参见张玉洁:《身联网时代人身自由理论的数字法革新》,《浙江社会科学》2023 年第 5 期。

②马长山:《数字公民的身份确认及权利保障》,《法学研究》2023 年第 4 期。

作为特殊种类信息加以保护;日本《个人信息保护法》则将种族、信仰、社会地位、病史、犯罪记录、曾遭受犯罪侵害的事实列为需特殊保护的个人信息①。上述立法经验显示,对敏感个人信息和普通个人信息的处理,做出有区别的保护模式,也是为了更好地保护个人信息权益。这种义务分配模式,反映出科技发展、信息安全以及保护公益相平衡的行政法理念。这就要求敏感个人信息保护在遭遇公共利益诉求时,法律除了能够要求个人信息处理者履行安全保障义务外,还可以寄希望于行政机关公共安全保障职能。这样,无论是从公力保护还是私力保护上,敏感个人信息都能得到切实保障②。

随着数字技术同人身、财产关系的不断交叉,信息安全同人身安全、财产安全之间的界限愈加模糊。肆意收集和处理敏感个人信息,不仅会危害个人信息主体的财产安全,甚至会危及个人信息主体的生命安全。对于此类个人信息的收集处理,倘若只通过个人信息主体行使"同意权"就可获得权限,则有可能导致个人过度关注自身的利益,而有意放弃公序良俗、社会公益。因而,我国急需通过公权力的介入来限制敏感个人信息的市场化流通,并改变个人信息应用中的不公平关系。尤其是在个人信息处理者与个人信息主体处于网络服务协议地位不对等的情况下(如身联网技术的信息处理者对身联网技术的解释),由于信息主体的个体差异化、技术名词过于专业化等问题,个人信息主体的意思表示未必是完全自主的决策结果。尤其是在敏感个人信息"利己性"远弱于"利他性"的情况下,个人信息主体甚至会主动忽视"知情同意"的法律意义。而个人信息处理者与个人信息主体之间的不平等关系,则突显了公权力介入的必要性。为此,在敏感个人信息处置上,设置"行政许可"这一前置程序,是一种加强敏感个人信息保护的有效方式。相比采取事后罚款等强制性措施,或者由个人信息处理者承担安全保障责任而言,禁止未获得行政许可的主体收集和处理敏感个人信息,更能够有效地预防恶性个人权益损害的发生。

(二)强化敏感个人信息公共风险预防作用

在科学技术的催动下,风险预防原则正在成为行政法的一项重要原则。它要求行政机关必须审慎对待潜在的社会风险,以提前规划、制定预案、避免损害等方式来削减社会治理中的不确定性因素③。例如,世界各国在各个领域(如环境问题、食品安全、对消费者保护的政策与技术发展等)运用了风险预防原则④。具体而言,英国《数据保护法》和欧盟的《通用数据保护条例》要求处理敏感个人信息必须是为了保护数据主体本人或他人的重大利益,包括保护生命、健康和工作安全等。日本《个人信息保护法案》(Act on the Protection of Personal Information)则要求,敏感个人信息的处理活动,必须满足合法性、明确性以及正当性等要求,并且要采取足够的安全防范措施以保护敏感个人信息。而我国也坚持"风险防范+违法惩治"相结合的路径来推进敏感个人信息的保护。例如,我国《个人信息保护法》就采用"风险预防式"界定方式,将"敏感个人信息"界定为"一旦泄露或者非法使用,容易导致……危害的个人信息"。也就是说,某一个人信息是否属于敏感个人信息,并不单纯的依赖该信息的法律预先设定,还可以根据未来可能造成的损害后果,将"个人信息"转化为"敏感个人信息"。此即风险防范原则的一种典型例证。而《个人信息保护法》第32条对行政许可的相关规定,则体现了风险防范原则的具体化实施。这充分体现了我国法律对收集和处理敏感个人信息风险的防范态度,证明了风险防范的必要性。

上述国家对敏感个人信息的法治化保障措施表明,"风险预防"是当前敏感个人信息保护的主流策略。而且无论该风险是否发生,各国法律均采取了风险防范措施,以防备实际损害的发生。作为监管风险的公权力主体,行政机关在预防敏感个人信息的社会风险时,可以采取手段从技术

①宁园:《敏感个人信息的法律基准与范畴界定——以〈个人信息保护法〉第28条第1款为中心》,《比较法研究》2021年第5期。

②肖中华,邹雄智,聂加龙:《数字经济时代个人数据面临的风险、成因及防范策略》,《企业经济》2022年第10期。

③罗智敏:《论行政许可中保证金的设定问题》,《中国法学》2014年第5期。

④参见高秦伟:《论欧盟行政法上的预防原则》,《比较法研究》2010年第3期;陈海嵩:《风险预防原则理论与实践反思——兼论风险预防原则的核心问题》,《北方法学》2010年第3期。

源头和处理过程着手预防损害的发生。无论是采用风险评估机制还是技术规制,都可以有效抑制敏感个人信息的侵权风险。但行政许可机制的优势在于,它能够在事前进行全面规制,以防范损害后果的发生。换句话说,敏感个人信息的民法保护,属于事中事后保障和制裁的典型方式,而创设敏感个人信息的行政许可,则是对个人信息处理者实行事前审查,从而预防敏感个人信息损害后果的发生,降低人身损害风险和财产安全风险。

(三)拓宽敏感个人信息的救济途径

与个人信息保护措施有所不同,敏感个人信息的保护必须关注到信息侵权所带来的衍生性"实质损害",即侵犯人格尊严、人身损害或财产损失。为此,我国《个人信息保护法》专门增加了敏感个人信息"实质损害"的相关考量,从而将敏感个人信息的权益对象限定为自然人的人格尊严受到侵害;人身、财产安全;未成年人权益。具体而言,敏感个人信息的"实质损害"可以划分为三个方面。

一是"人格尊严受到侵害"所指向的人格尊严权。这里的"人格尊严"不仅是指宪法上的人格权益,还指向了民法上的一般人格权。一切对人格尊严的损害都可视为造成"实质损害"。有些个人信息的处理,看似不会对信息主体的人格尊严造成影响,但实质上,被列入敏感个人信息范畴的所有个人信息都与人格尊严的保护直接相关。例如个人医疗信息。一旦该医疗信息泄露或者被他人非法获取,则会对医疗信息主体的财产安全和人格尊严带来损害。因此对人格尊严的"实质损害"应当采取广义理解。

二是"人身、财产安全受到危害"所表明有关敏感个人信息处理的"实质损害",指向了人身、财产安全。所谓"人身、财产安全",包括了人身、财产权利的安全以及保护人身、财产权利不受侵害。这两者内容中的人身权利和财产权利包括了生命权、身体权、健康权、名誉权、债权等广泛的人格权和财产权权益①。

三是有关未成年人权益的"实质损害"。从《个人信息保护法》第 28 条的规定来看,该法对未成年人的权益保护极为严格。无论是否损害未成年人的人格尊严还是人身、财产安全,只要非法处理未成年人个人信息,就判定对未成年人造成了"实质损害"。因此,我国应当通过行政许可的方式,对未成年人个人信息的处理加以严格限制,以达到对未成年人严格保护的效果。

综观上述三种类型的敏感个人信息"实质损害",传统上会按照侵权纠纷加以处理,并由被侵权人开展私力救济。但考虑到数字时代侵权行为的单次性、被侵权人数的超大数量以及侵权后果的不可计量等特征,传统私力救济只能带来微小的损害赔偿,甚至让侵权人感觉到赔偿后的"有利可图"。值得注意的是,私力救济不足的问题同样也反映在公力救济模式之中。原因在于全体"被侵权人"无法从公力救济中获得完整的民事赔偿。为此,只有采取事前防范的方式,对可能造成"实质损害"的敏感个人信息处理者先行设定行政许可,从而借助行政机关的事前监管职能完成敏感个人信息的法律体系建设。

三　敏感个人信息行政许可的体系性难题

(一)告知同意规则与行政许可的形式冲突难题

作为个人信息处理的前置规则,"告知同意"规则的核心理论基础是个人信息自决理论与隐私自我管理理论。然而,"行政许可"作为处理敏感个人信息的前置程序,体现了国家对敏感个人信息主体和处理者的双重限制与约束。在两种前置规则共存时,若个人信息主体预行使同意权,同个人信息处理者约定排除"行政许可",那么,司法机关就可以援引《民法典》第 153 条的规定,认定该"同意"行为无效②。但在设立具有强制性的行政许可时,告知同意规则下赋予信息主体的信息隐私自决的意志自由空间便被削弱了③。

从"告知"角度出发,敏感个人信息的处理起点是个人信息处理主体告知行为的发生时间,以个人信息主体"知情"为终点。在现代数字技术

①韩旭至:《敏感个人信息的界定及其处理前提——以〈个人信息保护法〉第 28 条为中心》,《求是学刊》2022 年第 5 期。

②王轶:《行政许可的民法意义》,《中国社会科学》2020 年第 5 期。

③李运达:《〈民法典〉人格标识"许可使用"的规范解释——以第 993 条适用范围为重点》,《浙江工商大学学报》2021 年第 5 期。

的应用下,该“告知”行为虽然属于纯粹的民事行为,但单一告知行为所引发的事实变化确是普遍性的、公共性的。这也意味着,《个人信息保护法》第30条对个人信息处理者所附加的“告知义务”,实际上不是针对个体告知义务,而是一种群体告知义务。既然是群体性告知——单一决策或行为能够影响众多不确定的个人——那么,依然将个人信息处理者“告知义务”定性为民事行为,显然忽视了该行为的公共影响力。因而,《个人信息保护法》第32条要求设置敏感个人信息行政许可,就是对“告知”行为公共影响力的必要回应。

而从“同意”角度出发,《个人信息保护法》第29条分别规定了两种“同意”模式。其中,“单独同意”的法治意义在于明确个人信息主体“同意”意图的真实性、明确性。但法律或行政法规规定处理敏感个人信息需要获取“书面同意”的,应当按照法律或行政法规的规定。值得注意的是,这里的“书面同意”未做出主体的限定。其一方面可以指向个人信息主体本人,另一方面也给行政机关作为同意权的主体而预留了制度空间。倘若行政许可在“告知同意规则”之前,为个人信息处理者和个人信息主体设定了限制性条件,就能够防范个人信息处理者滥用市场支配地位,“胁迫”个人信息主体“同意”其要求。只是这一层面的讨论,尚未在实体法和法学理论层面得到重视。

(二)充分必要规则与行政许可的价值冲突难题

敏感个人信息处理的“充分的必要性”,给予个人信息处理者设定了两个层次的限制:第一层次是通过其他手段都无法实现特定的处理目的,方可对敏感个人信息进行处理;第二层是若特定的处理目的已经实现,就不应对敏感个人信息进行处理。虽然充分必要规则为个人信息主体减损个人利益换取便利提供了指引,但对于那些通过处理个人信息来增进个人信息主体利益的情况难以适用。换句话说,《个人信息保护法》将敏感个人信息的实际处理范围,是由个人信息处理者自行决定的。而公权力在此问题上“缺席”了。由此导致的后果就是敏感个人信息“充分必要”规则的肆意解读。这显然是有违规则化、规范化的法治进路的。恰是因此,当《个人信息保护法》第32条创设“行政许可”限制时,敏感个人信息保护便陷入充分必要规则与行政许可的价值冲突之下。

严格地讲,对敏感个人信息处理活动采用行政许可机制,属于一种事前行政监管程序,旨在保障和实现行政相对人的权利。这也是整个行政许可制度和治理逻辑的出发点。一般认为,行政许可的设置应当遵循适当性原则、必要性原则和均衡原则,仅基于这三项原则中的任何一项都无法授权个人信息处理者处理敏感个人信息。这意味着,敏感个人信息行政许可机制对所许可事项的必要性、适当性要求,都比《个人信息保护法》中充分必要规则的要求程度更高。无论个人信息处理者能否维护社会公共利益或他人的个人信息权益,都无法回避行政许可所要求的适当性原则、必要性原则。尤其是在均衡原则的影响下,国家必须平衡数字市场发展、个人权益保障和社会公共安全之间的关系,而不能只关注个人信息主体欲通过减损信息权益所换取的“便利”。

以上(潜在)价值冲突显示,行政许可才应当是我国敏感个人信息保护的制度起点与基石,而充分必要规则是在行政强制性保障基础之上、个人信息处理者所享有的有限“协议自由”。因此,在敏感个人信息行政许可设定时,充分必要规则与行政许可规定对于敏感个人信息的保护价值是有法定位序的,并且应当在现行敏感个人信息保护体系中率先明确。

(三)意思自治规则与行政许可的程序冲突难题

自然人对人格的自我决定和发展一直以来都是民事权利的价值内核①。在此理念下,民法上的意思自治规则也给个人信息主体提供了信息自决的可能。当前,无论是《民法典》还是《个人信息保护法》,均倾向于采用意思自治规则来处理敏感个人信息。其背后的治理逻辑是将敏感个人信息的处理活动,交由社会公众与网络平台来公平协商。二者基于平等民事法律关系来达成协议。该协议不受行政法、刑法的强制性制约,体现

①刘召成:《身体权的现代变革及其法典化设计》,《当代法学》2020年第2期。

了协议双方的意思自治。这样,在敏感个人信息的应用上,《个人信息保护法》实际上是通过意思自治规则垄断了敏感个人信息适用的私法决策权,即以“合意”来确定敏感个人信息的适用。然而,对个人信息的绝对控制已不具现实性。数字化进程的进行,使得信息处理技术多元化发展,对敏感个人信息的处理风险增加。这增加了个人信息主体保护自身权益的成本,也导致个人信息处理者与个人信息主体的地位失衡。因此,敏感个人信息的个人控制走向个人信息的社会控制就是符合趋势的。

意思自治规则的适用形成了平等化的技术适用关系,但在实践中却构成了个人信息主体“信息权益”的放弃。由于信息主体在放弃“个人信息权益”时更注重技术所带来的便利性,因此容易忽视敏感个人信息对人身的潜在损害风险。因此,意思自治规则的“合意”保护,不仅未能解决个人信息保护问题,还排除了公权力保护的制度空间。着眼于数字时代的敏感个人信息的保护,是否应当确立行政许可优先于个人意思自治的问题,以及如何实现人格的自我决定与社会公益保护的平衡,已经成为学界无可回避的命题。尤其是在敏感个人信息自决问题上,意思自治规则与行政许可的程序冲突实际是信息自由与信息安全的冲突。而行政许可的设立就是为意思自治规则之前设置了前置性限制,强调了信息安全优先于信息自由。在此意义上,敏感个人信息的行政许可机制虽然将在一定程度上限制了自然人对个人信息的自我决定权,却整体性提升了信息安全的保障水平。

四　敏感个人信息行政许可的法治完善

(一)明确行政许可的敏感个人信息判断标准及其优先效力

为了更为有效地保护敏感个人信息,我国《个人信息保护法》第 32 条已经明确规定行政许可优先于个人信息主体之间的“合意”。有鉴于此,我国就应当在行政法上明确何种个人信息属于敏感个人信息,从而落实行政许可对敏感个人信息判断的优先效力。具体而言,明确行政许可的信息对象,就需要审视该敏感个人受侵犯后,是否能够对个人信息主体造成“实质损害”。倘若能够带来“实质损害”,那么该个人信息就应当被视为“敏感个人信息”,进而明确行政许可的具体对象。

具体而言,敏感个人信息行政许可的具体对象判定应当从三个方面加以判断:一是以是否“侵犯人格尊严”为标准来判断敏感个人信息。虽然所有个人信息都涉及信息主体的人格尊严保护,但敏感个人信息与人格尊严的关联更为密切。一旦敏感个人信息被泄露或非法使用,信息主体的人格尊严将暴露在被非法侵害的高风险中。因此,认定敏感个人信息的标准,应当判断该信息同人格尊严的紧密程度。二是以是否具备(潜在)“损害人身和财产安全”为标准来判断敏感个人信息。敏感个人信息的泄露或非法使用不仅可能损害人格尊严,还会威胁信息主体的人身和财产安全。对于涉及人身安全的信息,如果某些个人信息与自然人的生命、身体、健康密切相关,一旦泄露将使个人的人身安全承受重大风险或严重损害,那么这类信息应被归结为“敏感个人信息”的范畴之内。因此,是否具备(潜在)“损害人身和财产安全”,可以被视为行政机关针对“敏感个人信息”做出行政许可的重要判断标准。三是以是否属于“未成年人”的个人信息为标准来判断敏感个人信息。由于未成年人对网络世界和现实社会诸多风险的认识不足,更容易因个人信息泄露、滥用而影响到自身的人身安全、财产安全,甚至是精神损害。因此,对于未成年人个人信息的敏感性界定,仅以未成年人的年龄为判断要件,而不考虑它是否存在被损害风险或者已经产生实质损害后果。

(二)明确行政许可条件以及限制性措施

为保障敏感个人信息,我国应当对敏感个人信息行政许可条件进行体系化的设定,并出台相应的限制性措施,以防备敏感个人信息行政许可的过度泛化。为此,我国应当从以下三个方面,逐步建立行政许可条件以及限制性措施。

第一,行政机关应当率先明确敏感个人信息创设行政许可的具体条件。从我国数字经济市场化发展趋势以及个人信息保护的紧迫性来看,敏感个人信息的行政许可应当采用普通许可模式,即允许符合条件的相关市场主体,在符合相应条

件的情况下,均可以向行政机关(可以是市场监管部门或工信行政部门)申请行政许可。但值得注意的是,市场主体处理他人敏感个人信息,应当具备如下基本条件:(1)具备企业法人条件;(2)建立健全敏感个人信息安全管理制度、操作规程;(3)有具备敏感个人信息安全知识和管理能力的专职安全管理人员;(4)具有与其敏感个人信息处理范围和服务种类相适应的安全保障设施和服务能力,并符合国家相关标准。符合以上条件的市场主体,可以向行政机关申请敏感个人信息行政许可。

第二,行政机关不得授权其他机关制定敏感个人信息行政许可的实施细则。行政机关应当严格限制行政性授权,以法律明确性规定为原则,以个别授权为例外。在许可信息处理者收集和处理敏感个人信息时,法律应当就行政许可的目的、事项、范围以及时限做出明确的规定。值得注意的是,行政机关不得针对该行政许可进行授权,否则就同《立法法》《行政许可法》的规定相违背①。

第三,要严格限定敏感个人信息行政许可中兜底条款的适用。设定兜底条款,是我国立法的一项重要特征。但在敏感个人信息行政许可的设定上,应当采用明确列举的方式来划定个人信息市场获得许可范围,不宜将敏感个人信息的范围做泛化处理。尤其是在数字时代,对个人信息处理者的行政许可条件设定中,其兜底性的许可依据范围不应包括国务院主管部门的部门规章和规范性文件、地方行政机关的地方政府规章和规范性文件。因为部门规章和各级地方政府及其工作部门不具有行政许可决定权,若将其列入敏感个人信息的行政许可兜底性条款,属于变相承认部门规章、行政规范性文件和地方政府规章和规范性文件设定行政许可的权限。

(三)以行政许可承诺制来抑制意思自治规则

从现代行政国家角度而言,行政许可承诺制是由市场主体的申请行为、行政机关的告知行为、市场主体的承诺行为乃至后续行政监管等行为所构成的一项约束机制②。尽管行政许可承诺制模糊了传统行政法律关系和民事法律关系的界限,有含混行政法律事项与民事法律事项的嫌疑。但在当前敏感个人信息的处理上,该机制符合数字经济的市场规律,降低敏感个人信息的侵权风险,提高了行政机关的监管效率。尤其是随着人脸识别技术、身联网技术、脑机接口技术的不断发展,通过行政许可承诺制去防范个人信息处理者滥用技术,符合时代要求的法治发展方向。因此,我国建立完善行政许可承诺制来完善敏感个人信息保护的时代需求,发挥行政机关与市场的多元约束机制。

在数字时代,行政许可承诺制在"行政许可"这一强制性约束基础之上,增加了个人信息处理者的自我约束机制。它分别以"行政规制"和"信用规制"为路径,拓宽了敏感个人信息保护的渠道和范围。前者采用"行政许可-行政处罚"的传统行政法范式,将敏感个人信息处理者的主体范围,限定于我国既有行政监管能力范围之内。同时通过"沙盒式监管",将敏感个人信息的泄露风险和侵权风险加以管控,再通过市场机制,实现敏感个人信息处理者的市场准入和准出。而在"信用规制"上,市场主体在获取"处理敏感个人信息行政许可"之前,应当就自身合法合规使用敏感个人信息做出相应的承诺。该承诺不仅具有民事意义,更具备管制意义。这对于高风险行业、高致损领域而言是必需的措施。一旦违反了获取行政许可的相关承诺,除了承担相应的侵权责任和行政责任(甚至是刑事责任)之外,还可以据此承诺收回敏感个人信息处理权限,退出相应级别的市场。

结语

数字时代的到来,不仅引发了技术的不断革新,也带来了新型社会关系的规制需求。目前,敏感个人信息通过告知同意规则对信息主体的权益进行保护,并不足以应对处理敏感个人信息可能带来的损害,个人信息处理者的安全保障义务也需要公权力加以监督。虽然行政许可制度与《个人信息保护法》对敏感个人信息的处理规则还存在冲突,但是两者的目的都是为了保护数字时代

①林华:《行政许可条件设定模式及其反思》,《中国法学》2022年第4期。

②宋烁:《论政府数据开放的基本原则》,《浙江工商大学学报》2021年第5期。

个人信息主体的权益。为此,当前我国个人信息保护体系的发展方向应当是二者的衔接和协调。既然行政许可是敏感个人信息民法保障机制的前置性措施,那么二者的衔接和协调就应当率先明确行政许可的对象和具体许可条件,再通过适用行政许可承诺制,对个人信息处理者处理敏感个人信息的前置程序进行调整。当然,敏感个人信息的行政许可机制的建构,不在于否认当前民法意义上个人信息保护的低效性,而在于打造一套不同于“民-刑”二元规制模式的全新模式:“行政法-民法-刑法”。或许法学界对行政权介入私权仍持保留态度,但在数字法治问题上,这种模式也许能够为民事法律问题提供更为高效的解决方案,也能为行政法发挥集中治理效能提供检验场域,从而为个人信息保护提供更为适恰的治理方案。

The Public Law Effectiveness, System Difficulties and The Improvement of the Rule of Law of Administrative Licensing for Sensitive Personal Information

LI Yi

(Party Law Research Center, Guangzhou University, Guangzhou 510006, China)

Abstract: The legal protection of sensitive personal information is becoming a hot topic in the legal community. Article 32 of *The Personal Information Protection Law* provides a new path for the processing of sensitive personal information, i.e. administrative licensing. This path reflects obvious public law effectiveness, complements the administrative law protection of sensitive personal information, strengthens the role of public risk prevention and expands the relief channels for sensitive personal information. However, the administrative licensing path for sensitive personal information in China also faces a series of systemic challenges: conflicts between the disclosure and consent rules and the form of administrative licensing, conflicts between the sufficient and necessary rules and the value of administrative licensing, and conflicts between the autonomy rules and the procedures of administrative licensing. Therefore, in order to improve the legal protection of sensitive personal information, China should clarify the criteria for judging sensitive personal information in administrative licensing and its priority effectiveness, create specific conditions and restrictive measures for administrative licensing, and use the administrative licensing commitment system to suppress the rule of autonomy.

Key words: sensitive personal information; inform consent rules; security obligations; administrative licensing

(责任校对　龙四清)