

告知同意原则在个人信息保护中的适用完善

刘子健

中南财经政法大学刑事司法学院，武汉

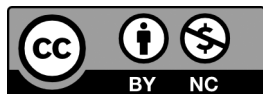
摘要 | 依据 2021 年 11 月 1 日正式施行的《个人信息保护法》规定，在处理个人信息时，个人信息处理者需遵循“告知同意”原则。通过了解“告知同意”原则的具体概念，以及分析现状，可以看出当前社会中对于“告知同意”原则的适用还存在许多现实问题，诸如隐私政策获取成本高、同意原则现实成效不大、“个人信息主体”的权利保障措施仍需改善等问题，就上述问题本文进行相关讨论，通过精简流程、优化“同意”与“告知”的衔接以及加强事前审查等优化措施或许可以对其提供现实保障。

关键词 | 个人信息保护；“告知同意”原则；个人信息处理；人脸识别

Copyright © 2022 by author (s) and SciScan Publishing Limited

This article is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

<https://creativecommons.org/licenses/by-nc/4.0/>



大数据时代，个人信息的安全问题和如何有效保护已成为一个突出的热点话题。我国于 2021 年 11 月 1 日正式施行《个人信息保护法》。在国际上，欧盟通过了《通用数据保护条例》（General Data Protection Regulation, GDPR）对欧盟内成员国公民给予个人信息保护在立法上的支撑；美国虽然在联邦层面目前暂时没有统一的法律规制，但是在人脸识别方面，美国多个州发布了适用于本州的法案通过限制人脸识别来体现与“告知同意”相类似的原则，例如华盛顿州颁布的《人脸识别服务法》和加利福尼亚州颁布的《人脸识别法》等。当今社会，个人信息保护意识的普及越来越广泛，告知同意原则的适用正面临告知有效性和用户同意确认难的新困境。告知同意原则在个人信息保护的适用中面临着许多困难，如典型的“隐私政策”没有人读、读而不懂等问题，个人信息主体被迫“强制”同意相

关隐私政策，使其难以行使同意的权利，因而个人的同意权利在数据处理环节很难取得有效成果。相关学者在此方面做出过一些研究，诸如对于 App 中告知同意原则适用的合理性的讨论，告知同意原则在现实实施中面临的相关问题，告知同意原则的“动态同意”机制的探讨等等。本文从告知同意原则的概念出发，探究告知同意原则的具体概念，从而明确立法机关对于告知同意原则适用的理论支持。通过现实层面的现状分析，本文发现告知同意原则虽然已经在立法层面得到了落实，但在原则实施落地上的具体细节面临着许多困境，例如信息处理方无法统一相关“告知”的政策标准，并且告知这一环节多以提供给用户“隐私政策”这一载体为主。笔者研究相关资料了解到“隐私政策”实为一种“尴尬”的存在，用户（即个人信息主体）难以完全了解政策相关内容，个人信息处理者却依旧修改、更

新相关隐私政策以应对国家相关政策要求，以上便是在“告知”这一环节出现了问题。同样，“同意”环节也存在类似的问题，总结而言就是个人信息主体在“告知同意”这一原则适用的环节总是处于“相对弱势”的一方，个人信息保护无法得到很好地落实，因此应通过告知方式和同意规则的优化与完善，做到事前严格监督、事中及时应对以及事后妥善处理三个方面，或许其在个人信息保护中的适用优化能够得到更好的体现。

一、“告知同意”原则的概念及其解释

（一）“告知同意”原则的法律依据

2020年10月21日，全国人大法工委公开就《中华人民共和国个人信息保护法（草案）》征求意见。在此之前，10月13日，全国人大常委会法制工作委员会副主任刘俊臣就《中华人民共和国个人信息保护法（草案）》（以下简称《草案》）做出了相关说明，其对于《草案》出台的必要性、主要内容、起草应注意的问题做出了相对客观准确的解释。在《草案》中，最重要的一项原则便是“告知同意”原则。刘俊臣在上述说明中提到，进入21世纪，中国的互联网发展迅速，截至2020年，中国的互联网用户已达9亿人口，占我国总人口的绝大多数，依托互联网为背景的数字经济影响着公民生活的方方面面，尤其是在信息时代下，由于没有专门法律的有效保护，公民的个人信息极易遭受不法分子非法侵害，造成财产损失、生命健康权受到侵犯，情况恶劣者甚至破坏社会正常运行秩序，危害国家安全等。而作为立法者，在关注到上述问题的现实状况后，通过立法将“告知同意”原则适用于个人信息保护领域，明确了个人信息保护的法律原则和法律依据。2021年8月20日，第十三届全国人民代表大会常务委员会第三十次会议通过了《中华人民共和国个人信息保护法》，个人信息保护法的通过具有重要的现实意义，该法是我国第一部明确具体规定了有关与公民个人信息相关的权利和义务以及其他有关规定，使得个人信息保护这一领域真正做到了有法可依。

（二）“告知同意”原则具体内涵

首先，明确“告知同意”原则的适用范围：个

人信息处理者与个人信息主体之间的信息处理环节及可能包含的其他操作。明确这一范围的前提，我们要先明确个人信息这一法律概念，个人信息来源于民法典中个人信息权^[1]这一民事权利，这是我国民法典明确规定的公民享有的个人权利，且个人信息权是指本人依法对其个人信息所享有的支配、控制并排除他人侵害的权利。其权利内容具体包括信息决定权、信息保密权、信息查询权、信息更正权、信息封锁权、信息删除权和报酬请求权。同样，在《个人信息保护法》中对个人信息的解释为“以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息”。^[2]

其次，“告知同意”原则的适用多被认为于个人信息处理环节得以体现，《个人信息保护法》中对于个人信息的处理的说明为“个人信息的收集、存储、使用、加工、传输、提供、公开、删除等”，^[3]并且该法第十四条规定了基于个人同意处理个人信息的，该同意应当由个人在充分知情的前提下自愿、明确作出。法律、行政法规规定处理个人信息应当取得个人单独同意或者书面同意的，也同样从其规定。

最后，“告知同意”原则还内在隐含了信息处理者“告知”的方式以及原则问题。可以看到，在处理个人信息遵循原则方面的改动上，原有《草案》中的合法、透明、诚信、公开等原则被合并为“合法、正当、必要和诚信原则”，^[4]并要求信息处理主体不得通过误导、欺诈、胁迫等方式处理个人信息，这是该草案自民法典颁布以来，又一新加的条款，

[1] 维基百科. 个人信息权 [DB/OL]. (2021-12-20). <https://wiki.mbalib.com/wiki/%E4%B8%AA%E4%BA%BA%E4%BF%A1%E6%81%AF%E6%9D%83>.

[2] 《个人信息保护法》第四条：个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

[3] 《个人信息保护法》第四条：个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。

[4] 《个人信息保护法》第五条：处理个人信息应当遵循合法、正当、必要和诚信原则，不得通过误导、欺诈、胁迫等方式处理个人信息。

之前在草案中,仅仅提及了不得通过误导、欺诈等方式处理个人信息,此次增加了“胁迫”一词,并且我们可以了解到,《民法典》第一百五十条规定了胁迫的法律定义为“一方或第三人以胁迫手段,使对方在违背真实意思的情况下实施的民事法律行为”,由于目前法律制度仍在不断完善,许多不法分子通过胁迫受害者的方式,故意使用AI技术将受害者的个人生物识别信息替换到淫秽色情视频中(即俗称的“换脸”),以此获取利益,此类违法行为在各类违规贷款活动中屡见不鲜,受害者总会出于个人名誉损失或诚信问题等被迫同意接受“换脸”,所以立法机关通过立法保护被胁迫的受害者这一目的,我们可以看到在立法层面立法者正逐渐将立法重心转移至人权保障,更加注重用立法的方式落实对个人权利的保障。

二、实现“告知同意”原则面临的现实问题

(一) 隐私政策获取成本高

首先,在现实生活中,大部分的个人信息主体在使用相关网站或者手机App时,几乎很少花时间阅读网站提供或手机应用程序所展示的隐私保护政策。有调查显示,2020年,中国手机网民对App隐私条款进行认真阅读的仅占到三成。^[1]况且,每人每天可能使用的应用程序和浏览的页面众多,期待每个用户都全面阅读所有涉及的应用程序和网站提供的个人信息保护政策并不切实际。换言之,即使用户愿意花部分时间阅读相关个人信息保护政策,绝大多数应用软件和网站所提供的隐私政策往往冗长繁杂,以腾讯公司腾讯隐私保护平台网站的《隐私政策》为例,单其隐私政策全文就有5000余字,政策中还包含了与其隐私政策有关的《腾讯服务协议》《Cookie政策说明》《儿童隐私保护声明》等其他未展示全文的服务条款和协议,且其中不乏法律术语,用户通常也难以在初次阅读时完全理解其中的含义。

在相关学术文章中,也有学者指出,以一份隐私政策为一万字为例,若一个人将自己一天时间内浏览的所有网站和应用程序的隐私政策阅读完毕将阅读近百万字,^[2]国外也有研究成果表明,如果信息主体要阅读提供给他们的所有隐私政策,那

么每年需平均付出近百小时。^[3]这不仅不现实,而且个人信息主体所消耗的时间成本过高而无法估量。再者,每个网站和应用程序提供的隐私政策并非一成不变,根据国家相关法律法规和政策的调整,其也会对相关政策予以更新和改动,这又存在个人在浏览网页或使用App时即使被告知了隐私政策的改动,也无法准确得知具体改动,因为我们并不完全清楚政策的原有规定和现行规定的区别,更无从谈及个人能够知悉政策的改动可能对其个人造成的影响。从以上现状,我们很容易得出一个结论:若个人信息保护告知体系没有完善,现实情况往往会变成信息处理方将个人数据在法律上的保护变成书面无效的保证。

(二) 同意原则现实成效不大

从提起草案到最后立法颁布,对比以往一些立法上的进步,我们不难看出,有关“告知同意”原则的相关问题,我们可以从《个人信息保护法》的具体规定中寻找原因。《个人信息保护法》第十七条规定了“个人信息处理者在处理个人信息前,应当以显著方式、清晰易懂的语言,真实、准确、完整地个人告知下列事项:(1)个人信息处理者的名称或者姓名和联系方式;(2)个人信息的处理目的、处理方式,处理的个人信息种类、保存期限;(3)个人行使本法规定权利的方式和程序;(4)法律、行政法规规定应当告知的其他事项”。^[4]

依据上述法律规定,我们也可以从中较为直接地提炼出,个人信息保护最重要的是个人信息主体“本人”的实际参与,而大数据时代背景下,个人生物识别信息在当今社会已然成为新一代的“ID密钥”,^[5]也就是说传统的法律保护能否全面地保

[1] 李彤. App个人信息保护中告知同意原则的适用研究[J]. 南方论刊, 2021(2): 75-78.

[2] 吕炳斌. 个人信息保护的“同意”困境及其出路[J]. 法商研究, 2021, 38(2): 87-101.

[3] McDonald Aleecia M. The Cost of Reading Privacy Policies 2008 Privacy Year in Review[J]. I/S: A Journal of Law and Policy for the Information Society, 2008(4): 543-569.

[4] 详见《个人信息保护法》第十七条。

[5] 林凌, 贺小石. 人脸识别的法规制路径[J]. 法学杂志, 2020, 41(7): 68-75.

护这一新兴的囊括社会生活方方面面的通行证,是我们较为关心的。依据数据处理的复杂性和连接紧密性,许多的数据保护制度的制定和实施变得越来越复杂,这使得个人信息主体与信息处理环节之间隔了一座“大山”,个人信息主体难以亲自参与个人信息的保护之中,现实状况往往是个人信息主体同意了其信息被处理后便没有了下文,也无从得知其同意的效力会延伸至何种范围。石佳友在其研究中指出现有人脸识别服务存在“使用即同意”的乱象^[1],同时在其对许多人脸识别机构的调研中,发现人脸识别服务协议中都规定了向“相关第三方”传输人脸图像用于识别,而在机构进行对相关第三方人脸图像传输处理时,绝大多数人脸图像本人并不知情,其人脸信息已经被进行了其他处理。

例如,在疫情期间,由于疫情防控的需要,加之人工智能应用的不断发展,越来越多的企事业单位选择通过收集用户人脸图像信息的方式来识别相关人员,随之诞生的网络人脸“黑市”就能够搜到众多人脸图像,而这些图像的来源我们并不知情,即使企业在收集人脸图像时告知了其用途和可能的去处,但是在实际操作中,被处理的人脸信息主体仅仅只了解收集其人脸信息的初始方,在此之后的其他环节经过了哪些渠道、是否在这些环节中被进行其他处理,信息主体并不知情,这就是我们要着重考虑完善的个人信息处理方对于处理个人信息时具有及时性的告知以及监管义务。

(三)“个人信息主体”的权利保障措施仍需改善

现有的法律对于个人信息权利的界定不清,易造成权利救济失效。《中华人民共和国数据安全法》^[2]第二十九条规定“开展数据处理活动应当加强风险监测,发现数据安全缺陷、漏洞等风险时,应当立即采取补救措施;发生数据安全事件时,应当立即采取处置措施,按照规定及时告知用户并向有关主管部门报告”,此规定仅包括了“发生数据安全事件”时告知用户,但依据大数据时代信息传输速度以及处理速度,当发生数据安全事件时,数据的传播以及利用可能存在已经传播并不断扩散的风险,并且此类情形对于数据主体造成的自然人权利或法人权利的侵害后果通常是发生即难以弥补。

然而,《个人信息保护法》在第四章第四十四

条又规定个人对其个人信息的处理享有的权利,其中包括享有知情权、自决权。^[3]

我们是否可以这样理解:上述法律中,前者仅要求紧急情况下对于个人信息主体个人数据的状态变更进行告知,而后者要求的是信息处理者在任何操作情况下的对于个人信息主体都应予以告知,因为个人信息既可以被视为一项常规数据可以被处理,又可以被视为是需要全程受到保护的个人信息,所以从个人信息主体录入个人信息到个人信息处理环节结束,对于信息处理者而言,这种情况会一直持续。出于减少信息处理环节的成本以及信息处理连贯性的考虑,信息处理者会在告知个人信息主体的问题上避重就轻,其往往不会第一时间告知个人信息主体其个人数据正处于何种环节、被进行何种处理,而是在事后告知或不告知,即使出现信息处理问题,因为隐私政策相关条款的规定,信息处理者很大概率会免于或受到很小处罚,承担信息处理问题后果的往往是信息主体自身。同样,《个人信息保护法》第五十七条又规定,个人信息处理者采取措施能够有效避免信息泄露、篡改、丢失造成危害的,个人信息处理者可以不通知个人;履行个人信息保护职责的部门认为可能造成危害的,有权要求个人信息处理者通知个人。这里我们比较担心的一点是信息处理者与监管者的身份对比,也就是其地位高低问题,若信息处理者处于绝对掌控信息处理环节的地位,则信息安全保护部门的存在可能仅仅是信息处理者的附庸,其安全保护的职能会大大削弱;若信息处理者地位低于安全监管部门,则也因此会产生过多繁琐的信息处理问题,降低信息处理的效率。因此我认为,这两者间最好的状态理应是互相监督、互相制约的,信息处理者在处理信息时及时透明地向安全监管部门公开,安全监管部门

[1] 石佳友,刘思齐.人脸识别技术中的个人信息保护:兼论动态同意模式的建构[J].财经法学,2021(2):60-78.

[2] 《中华人民共和国数据安全法》(2021年6月10日第十三届全国人民代表大会常务委员会第二十九次会议通过)。

[3] 《个人信息保护法》第四十四条:个人对其个人信息的处理享有知情权、决定权,有权限制或者拒绝他人对其个人信息进行处理;法律、行政法规另有规定的除外。

对其进行实时监控并进行实时风险评估,在存在任何可能的风险时,既告知信息处理方也告知用户,并在风险被消除,信息处理回归到正常状况时通知用户。在欧洲,网络和信息安全指南(NIS)就非常强调网络和信息对于构成国家的经济运行秩序和社会活动的功能的可靠性和安全性的重要性。^[1]该指南强调了数据安全和个人数据保护之间的必要联系,信息处理方需要优先提供个人数据保障,同时也要妥善处理信息和通信技术安全风险问题,后者往往比个人数据保护问题带来的国家和社会危害更加严重。这可以给我们未来的数据风险处理的发展道路提供一个现实方向上的参考。

三、“告知同意”原则适用之优化

(一) 精简流程提高告知效率

基于前文所述,在个人信息处理环节前,个人信息主体了解其信息被处理的相关操作和权利保护的政策大多呈现于信息处理者提供的隐私保护政策中,而现实情况是这些政策不仅冗长复杂,且个人很少会选择付出巨大的时间成本去阅读相关文字以完全掌握相关政策,以期在后续产生可能侵犯自身个人信息问题时保护自己的合法权益。因此,如何提高信息处理者的告知效率是当前仍需解决的一个问题。

根据美国心理学家洛钦斯的“首因效应”理论,^[2]首因效应,也称为第一印象作用,或先入为主效应。第一印象作用最强,持续的时间也长,比以后得到的信息对于事物整个印象产生的作用更强。首因,是指首次认知客体而在脑中留下的“第一印象”。通过“第一印象”最先输入的信息对客体以后的认知产生的显著的影响作用,它是由第一印象(首次印象)所引起的一种心理倾向,许多人习惯称之为“第一感”。首因效应本质上是一种优先效应,当不同的信息结合在一起的时候,人们总是倾向于重视前面的信息。即使人们同样重视了后面的信息,也会认为后面的信息是非本质的、偶然的,人们习惯于按照前面的信息解释后面的信息,即使后面的信息与前面的信息不一致,也会屈从于前面的信息,以形成整体一致的印象。例如有关隐私政策的制定和修改,当一项政策经过制定展现给用户阅读时,用户刚好在相关文本的开头部分就能够有效地阅读

所有内容且基本理解其中表达的含义,那么这个隐私政策就是合适的。但是,若在此基础上,信息处理者一直增加用户的阅读量,虽然文字所表达的内容仍与用户个人信息处理以及保护有关,甚至具体到相关信息处理的细节以及侵权责任认定等重要问题,但用户会随着阅读量的不断增加逐渐失去阅读的意愿,转而直接跳过中间环节至结尾部分,粗略地了解相关内容,并结合在开头阅读的文字自行猜测政策大致表达的含义。

基于上述观点,我们建议简化“告知”这一环节的形式以及内容,在用户阅读隐私政策时,信息处理者将相关政策处理得更加通俗易懂且突出重点,信息处理者提供相应政策可以实现简化其内容的同时也明确告知了用户相关政策,以达到提升数据处理的可预测性和透明性,使得用户可以在阅读相关隐私保护内容时生成一定的心理预期并对其做出相应的评估,从而了解整个数据处理过程会以怎样的形式、经历怎样的阶段,并在最初阶段的阶段明确自己的选择意愿。或者,由上级主管部门制定统一的隐私政策模板,对于当前个人信息保护涉及的内容做出大致框架的梳理,信息处理者在制定相关隐私政策时只需填充或增减有关内容即可。

(二) “同意”与“告知”应做到有效衔接

作为前提步骤的“告知”做到了有效处理,个人在对于信息处理者处理信息时的“同意”环节同样值得重视。《个人信息保护法》规定了在信息处理者处理信息个人信息时,若处理目的、处理方式和处理的个人信息种类发生变更,应当重新取得个人同意。具体解释其内涵,即个人对于个人信息处理的“同意”是一种非“契约式”的同意,也就是

[1] Tikk Eneken. Privacy online: up, close and personal [J]. Health and technology, 2017, 7(4).

[2] 首因效应(Primacy Effect),首因效应与近因效应是由美国心理学家洛钦斯首先提出的。它们反映了人际交往中主体信息出现的次序对印象形成所产生的影响,指的是在信息呈现顺序中,首先呈现的信息比后来呈现的信息在印象形成中有更大的权重。维基百科.“首因效应”:对社会知觉过程规律的研究[DB/OL].(2021-12-20).
<https://wiki.mbalib.com/wiki/%E9%A6%96%E5%9B%A0%E6%95%88%E5%BA%94>.

并非个人一旦表达了对“处理”的同意，在此之后的任何行为都被默认为是个人的同意，我们可以将其视为是一种“动态同意”，^[1]这种“同意”是视具体情况而发生改变的。

笔者了解到腾讯公司在履行“告知”义务方面的举措：腾讯公司的安全系统后台会在用户的个人密码被修改或处于异常登录状态时，及时地通过发送短信、发送电子邮件或依靠其他通讯方式告知用户其个人账户登录状态异常，需要个人进行输入验证码确认同意或登录相关网址、登录相关程序进行查询。这也就意味着，不仅个人信息处理者的“告知”具有实时性，个人主体行使权利时同样具有及时反馈性。依此，以人脸识别信息为例，个人信息处理方或监管部门是否可以将其作为参考，通过短信、电话或其他能够即时传递信息提示的方式，提醒用户其人脸信息曾在某设备（或虚拟环境）上正在被处理或被处理过，若非用户本人操作或授权同意的，可能是用户的个人信息泄漏导致，会产生相关不利影响。为了确保个人信息的安全，建议用户尽快联系对应的信息处理方或登录相应网站查询即时终止该行为等。

（三）加强事前审查

对于目前个人信息主体仍处于“相对弱势”一方的问题，笔者认为可能的原因为对于侵权责任的认定不清以及惩罚力度不够。以当前在年轻群体中较为流行的手机 App “哔哩哔哩”软件为例，若在搜索栏输入“换脸”搜索相关内容，可以搜到的“AI 换脸”视频多达 1000 余条（网站统计数据仅显示为 1000+，因此笔者无法明确得出具体统计数字），虽然多数人进行 AI 换脸的操作以娱乐搞笑为目的，但其中也不乏对于被换脸者个人名誉的侵害，被侵犯权利的个人因为公众“娱乐至死”的亚文化理念影响，以及个人维权遇到的种种现实障碍，诸如个人信息被散布于网上，如果信息主体没有强大的经济实力或人脉资源，很难在短时间内要求信息发布平台清除有关其个人信息的内容，亦或是个人信息已经被泄露或编撰成谣言，出于个人隐私保护的个人信息发布者或发布平台清除了有关内容，个人信息主体也无法要求已经获取该信息的用户清除记忆或停止通过其他方式（如朋友圈、微博、贴吧等）传播。个人信息主体也无法切实追究具体人员的相

关责任，仅仅能做到举报相关内容使其下架，但是相关内容一旦在公共场合曾经出现过，就已经对其个人形象及名誉造成了一定程度的影响，这种影响是不可逆的，一段时间内很难在人们的记忆中消失。在这种情境下，被侵害主体往往只能做到前文所说的，通过行使“个人信息删除权”，要求信息处理者删除相应内容或做出其他补救措施，但归根到底这都是一种事后补救措施，是事实处于“已然”发生状态，而要求接触过该信息的人遗忘该信息是不现实的，这种“已然”发生的事件很难在短时间内被个体自觉地遗忘。

因此，介于事后补救面临的各种难题，做好事前的审查理应成为个人信息保护的重中之重。当前即使处于个人信息保护的大环境下，我国对于个人信息的保护多出于对“事后”采取相关措施加以解决，即使有相关法律规定了未经同意信息处理者不得擅自处理个人信息，但是在衡量商业利益和面对法律处罚方面，只要违反信息保护相关法律所付出的成本低于所获利益，或者长期运营价值较大，信息处理者仍会选择通过各种手段处理个人信息，以达到规避法律惩罚，获取不法利益的目的。例如在日常使用手机购物 App 时，多数人会发现，只要用户选择了搜索某类商品或浏览过某类商品，甚至有人猜测手机 App 会“窃听”其在日常生活中的谈话从而获取其与商品数据库中匹配的商品从而进行推荐，这其实就是 App 通过设计内在的程序逻辑，将用户的个人信息经过处理得出“个人画像”，然后有针对性地对其实施营销策略，而这些在用户最初使用 App 时是不知情的，这就是我们强调为何在个人信息处理前也要强化监督管理。

举例而言，美国加利福尼亚州《加利福尼亚消费者隐私法案》（CCPA）在“个人信息和隐私保护”章节中通过立法的方式设立了隐私保护办公室，在加州消费者事务部（Department of Consumer Affairs）内行使职权。该办公室主要关注与涉及“身份盗窃”的通知有关的对于个人信息进行的干预活动，同时

———
[1] 石佳友，刘思齐．人脸识别技术中的个人信息保护：兼论动态同意模式的建构[J]．财经法学，2021（2）：60-78.

也涉及调查处理对于个人资料、消费者隐私及互联网个人资料库的具有侵犯性的商业利用手段等。^[1]此外,办公室还从事传播和教育公众有关个人信息保护相关内容的活动。以此为借鉴,通过设立相关部门,或设置对信息处理主体的信息处理行为规范和列举禁止性条例(或惩罚条例),规范信息处理主体对个人信息处理的前中后期操作,而不单单从事事中事后进行约束和管理,在这种情境下,根据《个人信息保护法》中提到的对于个人“同意”的“撤回”就至关重要,个人信息处理者可以给信息主体提供“个人画像”,但这种服务也同样需要提供“撤回”选项,即用户选择不需要信息处理主体处理其个人信息,并且在个人信息主体发现其个人信息可能会被强行处理时告知监管部门,对信息处理者进行调查,符合处罚条款的对其进行认定违规操作并

做出处罚,从而限制或减轻信息处理对个人信息主体的后续影响。

四、结语

当前个人信息保护法中对于“告知同意”原则的应用上,笔者认为仍有需要改进和完善细化的地方,个人信息主体在信息处理环节仍属于“相对弱势”的群体。信息处理者一旦处理不当就会造成个人信息的泄露等安全隐患,而其在进行信息处理操作时所承担的风险责任并不足以打击违法犯罪活动,依靠“告知同意”原则和侵权责任惩罚有效保障个人信息处理中的人脸识别信息安全问题,还有很长的路要走。

(责任编辑:李琼)

Application and Perfection of the Principle of Informing and Consent in Personal Information Protection

Liu Zijian

School of Criminal Justice, Zhongnan University of Economics and Law, Wuhan

Abstract: The Personal Information Protection Act stipulates that personal information is information recorded electronically or otherwise relating to an identified or identifiable natural person, and does not include anonymized information. This includes personal information such as face recognition information. When processing personal information, the personal information processor shall not process personal information in an illegal manner, while following the principle of “informed consent”. However, there are still some problems in the application of the principle of “informed consent” in the real society, such as the high cost of the subject of personal information, the lack of practical effect of the principle of consent, and the need to improve the protection measures of the rights of the subject of personal information.

Key words: Personal information protection; “Informed Consent” principle; Personal information processing; Face recognition

[1] Bartosz Marcinkowski. Can the United States provide a higher standard of personal data protection than the EU [J]. *Datenschutz und Datensicherheit—DuD*, 2017, 41 (6).