大数据时代个人信息风险与法律保护

黄　莹,刘佳音

(南京理工大学 紫金学院,江苏 南京 210046)

摘　要:大数据时代网络跟踪技术、隐蔽的个人信息收集行为以及告知同意原则的失灵等风险对公民个人信息安全造成了严重威胁。目前,我国个人信息保护框架仍存在不足,信息主体在信息知情、信息决定、信息删除的过程中对个人信息控制的权利有限,在很大程度上影响了用户的个人信息利益。因此,明晰个人信息的特征和属性,考察不同国家个人信息保护的立法经验,掌握风险应对的方法,才能保护我国公民个人信息的安全,最终促进信息技术产业的健康发展。

关键词:个人信息;风险来源;告知;同意;法律保护

中图分类号:F923　　**文献标识码:**A　　**文章编号:**1008-2638(2020)08-0085-03

Personal Information Risk and Legal Protection in Big Data Age

HUANG Ying, LIU Jia-yin

(Zijin College, Nanjing Institute of Technology, Nanjing Jiangsu 210046, China)

Abstract: In the era of big data, the risks of network tracking technology, hidden personal information collection behavior and failure of informing consent principle pose a serious threat to the personal information security of citizens. At present, there are still shortcomings in the framework of personal information protection in our country, and the information subject has limited rights to control personal information in the process of information knowledge, information decision and information deletion, which all affect the personal information interests of users to a great extent. Therefore, only clear the characteristics and attributes of personal information, inspect legislative experience in personal in formation protection in different countries, that we can promote the healthy development of information technology industry.

Key words: personal information; risk; sources inform; consent to legal protection

2014 年百度大数据案中,原告搜索的“隆胸、人流”等信息被跟踪记录,并在原告不知情的情况下进行商业广告利用。法院判决搜索记录关键词不属于原告隐私,仅是不可识别的网络化碎片信息,最终判决被告百度公司胜诉。当时个人信息还未写入民法,只能通过隐私权侵权起诉,现在法律对个人信息进行定义之后,再判断搜索记录是否属于个人信息时,不仅取决于该信息本身的人身指向性的强弱,更取决于信息收集利用者还掌握哪些相关联的信息。在平板电脑、智能手机普及的今天,信息收集者收集的个人信息越来越多,所以可以认定为个人信息的范围也可能越来越大。

一、大数据时代个人信息基础理论

(一)大数据时代个人信息的概念

美国加州隐私法(CCPA)对“个人信息”一词的定义是有关联、能描述、能够直接或间接与特定消费者及家庭关联的链接信息。CCPA 中也提供的许多个人信息示例,除了姓名等基本身份信息,还包括:商业信息(包括查询产品或服务的记录,消费历史或倾向的记录)、网络活动信息(包括搜索和浏览记录、应用程序使用记录),以及从其他信息中得出的推论,以创建识别身份,反映消费者的偏好、心理趋势、行为、态度、能力的个人档案信息。

我国大数据时代背景下,个人信息的概念应包含两个部分,能够单独识别自然人个人身份的信息以及透过其他信息结合可以识别个人的信息。直接可识别信息是指能够直接识别特定个人的信息,如姓名、身份证号、指纹等;间接可识别信息是指通过网络或通信技术综合分析和核对相关个人信息内容后,可以特定个人或者特定群体的身份识别信息,如消费信息、网络搜索浏览记录等。此类信息虽不能直接识别具体的主体是谁,但可以了解到信息主体的任意行为,并

收稿日期:2020-06-03

作者简介:黄莹(1988-),女,助教,在读硕士。主要从事民商法研究。刘佳音(1997-),女,在读学生。主要从事民商法研究。

由此分析出爱好、消费能力和需求、交往范围,从而逐渐与信息主体的身份搭建联系,推断出信息主体身份。

(二)大数据时代个人信息与个人隐私的区别

隐私信息主要是一种私密性的,私人活动信息。隐私信息的概念范围较窄,隐私信息具有的是人格尊严方面的利益,而且单个隐私信息并不直接指向自然人的主体身份。而个人信息是可以识别确定个人身份的信息或信息组合之后可以指向特定个人,反映自然人生活情况的各种信息,具有身份识别性。隐私信息和个人信息有区别,不能混为一谈采用同一种保护模式。个人信息已经超越隐私特性,具有特定公开性与共享性,若仍以隐私权保护模式保护个人信息,个人信息合法权益并不能得到应有的救济。

二、大数据时代个人信息保护风险来源

(一)Cookie 等新兴跟踪技术的发展

大数据时代下先进的跟踪技术,如记录网络用户日常上网活动的隐形录屏仪,能够对网民的网络活动进行全程记录,并成功收集到完整的个人信息。

Cookie 是一段不超过 4KB 的小型文本数据,用来记录人们浏览网页的内容和查阅过的信息。目前,Cookie 存在多种类别,如分析 Cookie、定位 Cookie、营销 Cookie 等。大部分网站都会使用各种 Cookie 来跟踪记录用户留下的信息,Cookie 技术在用户毫不知情的情况下,对网民的网络活动进行跟踪、记录。网站、广告商正是利用这种跟踪技术,能够源源不断地投放窗口广告,从而影响消费者和用户的选择权,给互联网数据隐私保护带来巨大威胁。因此,如何运用法律规制跟踪技术对人们进行追踪和记录,给予用户对于 cookie 等跟踪文件的控制,是大数据时代需要解决的难题。

(二)个人信息收集者对信息存留期限与存留地域的控制

隐私协议是有关账户注销后个人信息如何处置的条款,条款的内容为:如果停用账户,我们仍将使用您的部分账户信息,处理和分析现有的资料、访问记录和用户身份数据。显而易见的是,即使注销账户后,之前留下的账户信息、身份数据,用户也不能主动删除。个人信息存留期限不在用户的控制之下,我们无法知道网站、软件等信息收集者收集了哪些信息,更无法得知这些信息的保存期限。

对于个人信息的存留区域也在信息收集者的控制之中。许多隐私协议同意之后,就代表用户同意进行跨境传输,默认用户理解并同意:"将收集到的个人信息存储于中国或者其他国家的服务器上,并传送至关联控制公司或者跨境第三方服务供应商。"对于确定的信息存储地址及信息接收单位,用户却不知情。

(三)告知同意原则规制手段的失灵

告知同意原则是指收集、披露个人信息之前需要获得用户许可的原则,即收集处理个人信息,要么有法律明确允许处理,要么个人数据再被处理之前被告知处理的原因、背景和目的后得到同意。大数据时代的兴起,各类 APP 不断更新,互联网公司更迫切需要收集共享和处理用户信息,分析用户偏好,越来越多的授权同意成为大多数用户的负担。而互联网公司则以告知同意原则为收集任何信息的"挡箭牌",完成合规义务的"避风港",从而免除其大部分责任。告知同意原则这些挑战要求我们对隐私环境进行合理的重新评估,在大数据时代中,更需要找到保护信息隐私的机制的更优组合。

(四)数据收集范围的扩大化

最少信息(least information)是指保障某一服务类型正常运行所必需的个人信息,包括与服务类型直接相关,一旦缺少将导致该类型服务无法实现或无法正常运行的个人信息,这才是网络正确的个人信息收集范围。但现如今数据收集范围越来越大,浏览的网站、购物记录、使用的功能或者服务、语言、身体状况、手机或电脑内存储的照片,文件、本地缓存信息、所在的国家,地区精准地理位置等,过度的信息收集违背了最少信息使用原则的规定,也不利于用户对于个人信息的利益保护。值得关注的是,数据收集的范围也扩大到了生物识别信息。生物识别信息包括:指纹、声音、脸相等;人脸识别技术是生物识别技术的一项内容,根据《2019 计算机视觉人脸识别市场研究报告》显示,2018 年中国计算机人脸识别市场规模为 151.7 亿元,预计 2021 年将达 530 亿元。在我国,人脸识别的使用情况已经十分普遍。这种技术不仅用来抓取个人的面部生物信息,还可以与既有数据库中的数据进行比对。它能进一步追踪到个人的身份信息、日常的行踪轨迹、亲属关系的匹配等。与指纹、虹膜等其他生物信息识别技术相比,人脸识别具有非接触性的特点,这意味着很多人可能是在不知情的情况下,被抓取面部信息。当算法对人做出更多分析之后,成为"透明人"的可能性无疑存在。现有的人脸识别技术的应用仍然存在一些合法性层面的问题,需要完善立法,强化监管。

三、构建我国大数据时代个人信息法律保护制度

(一)制定和完善个人信息保护法规.

大数据时代应对个人信息风险需要相关法律规定的支撑。因此,制定《个人信息保护法》不仅可以为个人信息保护提供法律依据,也可以促进网络行业的经济健康发展,在保护个人信息的同时不阻碍信息技术的发展。

1. 明确个人信息存留期限

关于个人信息存留期限的风险,完善个人信息保护法中的信息主体删除权是很好的解决路径。赋予公民个人信息删除权,即在法定或约定事由出现后,用户即可请求网站删除其个人信息。信息主体删除权的使用情形,民法典一审稿草案曾做出明确规定,互联网与用户之间的隐私协议需要约定个人信息存留期限,存留期限已过,不可以继续存储公民个人信息。然而,民法典草案的终稿将删除权和法定事由的规定都删除了。删除有关信息主体删除权的内容,互联网行业等利益集团的施加的压力占了很大一部分原因。鉴于用户个人信息的保护,建议日后颁布的《个人信息保护法》应赋予用户自主的享有个人信息的删除权以及明确行使个人信息删除权的法定事由。《欧盟通用数据保护条例》对存留期限做出规定,即互联网信息收集者在收集信息时,应告知用户个人信息的存留期限。因此,我国可以此为鉴,规定个人信息存留期限达到一个固定年限后,在不损害公共利益的情况下,信息储存主体可以按照用户的要求删除其个人信

息。

2. 明确个人信息收集范围

《信息安全技术移动互联网应用(App)收集个人信息基本规范(草案)》中对最少信息做出了定义,即保障某一服务类型正常运行所必需的个人信息,一旦缺少将导致该类型服务无法实现或无法正常运行的个人信息。因 APP 种类的不同,每一种类别的 APP 的最少信息也是不同的,个人信息相关法律法规应明确个人信息的收集范围,依照最少信息原则,与最少信息没有紧密联系或与 APP 服务用途没有关联的个人信息则不会被强制收集。如规定网上支付应用程序可以收集身份证号码,家庭住址,理财资产信息,银行户名卡号等敏感信息,其他类别软件如视频软件等不强制要求使用微信等方式登录,从而读取联系人资料。

应对个人生物数据的收集的风险也需要通过完善立法来化解。严格限缩个人生物信息的收集主体,明确个人生物数据的使用规则等都有助于应对信息收集的风险。石佳友教授认为未来的个人信息保护法应规定:“在取得信息主体的明示同意的前提之下,才能收集、利用个人生物信息;收集主体严格遵守关于面部数据的利用、保存的法律要求;没有获得信息主体的明示同意,不得向第三方出售、交易个人生物信息。”对于面部信息滥用的类型、方式、主体都应该在法律上有所界定,从而进行相应的判定和处罚。对于生物信息而言,需要通过制定完善个人信息保护法规来让生物数据应用技术更加安全、恰当地得到利用,从而保护大数据时代下的公民个人信息。

(二)完善告知同意原则

1. 告知同意权的撤销与取消授权

美国加州隐私法案第 1798. 120. 规定:“消费者有权在任何时候指示向第三方出售消费者个人信息的企业停止出售消费者的个人信息。”这项权利可称为选择退出权,即消费者尽管事先同意了网站可以将收集的个人信息与第三方共享,但也可以重新选择不再授权网站这项权利,当用户撤回授权同意时也无需受到额外限制,告知同意权的撤销与取消授权意味着撤回同意与表达同意可以一样简单。

2. 有效规范信息主体的同意行为

欧盟规定小于 13 岁的未成年人,需要监护人为其做出明确同意。在美国为了保护未满 16 周岁的未成年,对告知同意加以年龄上的应用限制。法案规定如果企业实际知道消费者未满 16 岁,企业不得出售消费者的个人信息,除非消费者的父母或监护人已明确授权网站可以销售。我国可以欧美国家立法为参考,在与儿童相关的信息共享与产品营销方面的应当严格规范同意的方式以保护我国未成年的个人信息权益。

从比较法来看,告知同意原则具备三个前提条件:第一,同意必须明确。个人信息收集共享销售之前必须要披露告知用户,应该获得信息主体的明确同意。其中同意条款不可以非常模糊或过于复杂,如果同意条款不够清楚,即使获得了信息主体的同意,也不能认为是获得了真正的授权。第二,给予自由。如果拒绝,不得强迫用户同意或遭受任何损害。第三,严格限制概括同意授权,实践中,许多网站软件服务提供者往往采用拟定的概括授权条款,再此情形下用户对于信息收集者收集的信息内容,处理使用方式都不知晓。应该对告知同意原则作出合理限制,以避免其滥用而侵害个人合法权益,告知同意原则不能作为任何情况下不当收集个人信息的合法抗辩。

(三)运用技术化手段应对个人信息安全危机

数据去识别化本是美国医疗保健技术的重要组成部分,源于美国 HIPAA 联邦法案,目的是为了保护个人医疗信息,现在已经有更加广泛的应用了。根据 HIPAA 隐私规则规定,一旦数据被去识别,便可以使用或披露数据,不再受限制。例如,通过从共享列表中删除患者的姓名、社会保险号、出生日期和地址来实现匿名化,同时保留医学研究所需的重要组成部分,如年龄、疾病、身高、体重、性别、种族等。信息可用于研究、政策评估等领域,但不会侵犯公民个人隐私。

值得注意的是,匿名化与去标识化能够得到运用的前提是需要有法律的规制。GDPR、美国 HIPPA 法案中有严格的要求,规范实施主体,去标识化才会很好地得到应用,个人身份信息的匿名与去标识才能更好地得到安全保证。运用技术手段应对科技带来的调整,不仅有效而且必要。在保证数据价值得到充分运用的同时,也能保护个人身份信息被保护,匿名化与去标识化技术不失为大数据时代保护个人信息,促进信息流动利用的好方式。但其使用的前提还是需要法律的规制,否则泄露个人信息可能反而更加容易。

总之,有关个人信息的法律规定已经出现在了最新的《民法典》中,这加强了各行业对个人信息的保护力度。但从风险的角度以及司法实务来看,对于个人信息的保护仍远远不足。以告知同意原则需要满足的条件、“最少信息”作为评价个人信息收集范围等标准来看,收集者与用户之间的隐私协议还有许多可改进之处。用户对个人信息保护有更多的信赖,互联网经济也才能够更加健康的发展。想要完善个人信息的保护,需要发挥法律的规制功能,也需要配套相关技术化手段来阻止更隐蔽的信息收集方式。

参考文献:

[1]张新宝. 个人信息收集:告知同意原则适用的限制[J]. 比较法研究,2019,(06):1-20.
[2]石佳友. 人格权立法的进步与局限——评《民法典人格权编草案(三审稿)》[J]. 清华法学,2019,(05):93-110.
[3]宋亚辉. 个人信息的私法保护模式研究——《民法总则》第 111 条的解释论[J]. 比较法研究,2019,(02): 86-103.
[4]万方. 隐私政策中的告知同意原则及其异化[J]. 法律科学:西北政法大学学报,2019,(02):61-68.
[5]张茂月. 大数据时代个人信息数据安全的新威胁及其保护[J]. 中国科技论坛,2015,(07):117-122.

(责任编辑　李　维)