

国家安全视域下个人数据流动治理研究

李向阳

(山东科技大学 文法学院, 山东 青岛 266590)

【摘要】数据时代的来临给人类社会带来了深刻的变革,数据的治理成为了当前法律治理的热门。个人数据的不可控性、大规模聚集、缺乏监管使国家安全面临风险,通过对国家安全的界限、个人数据权属以及个人数据中利益的分析,寻求国家安全视域下个人数据治理的措施,提出厘清国家安全利益、根据利益相关的确权以及克减私主体权利,完善我国国家安全视域下个人数据治理方案。

【关键词】个人数据; 国家安全; 利益衡量

一、国家安全视域下个人数据流动治理

从2020年11月15日正式签署的《区域全面经济伙伴关系协定》(RECP)到2021年9月16日申请加入《全面与进步跨太平洋伙伴关系协定》(CPTPP)中表明:中国遵循“数据自由流动原则”,积极地加入各种数据自由流动的协定当中,促进数据自由流动。由于数据蕴含着多重法益,个人权利、经济利益与国家安全等利益,因此对数据进行治理的时当前学界研究的热点。

在数据治理需求中,承载个人信息的数据(以下简称“个人数据”)的治理具有重要地位,也是与人民群众密切相关的话题^[2]。当前学界对于个人数据的治理研究主要集中在对于个人数据权力的保护^[3]、个人数据确权^[4]与数据财产权的分配^[5]等角度。然而,个人数据不仅在私人和经济领域具有价值,也需要在国家安全维度进行考虑。

在习近平总书记提出的总体国家安全观中,国家安全的内涵就总体国家安全观涵盖政治、军事、国土、经济、金融、文化、社会、科技、网络、粮食、生态、资源、核、海外利益、太空、深海、极地、生物、人工智能、数据等诸多领域。随着数字技术的广泛应用,数据成为重要的生产要素和战略资源,数据安全已经上升到国家安全层面。

而在大数据时代的背景下,个人数据也与国家安全的关系越来越紧密。一方面,某些具有特定身份人员的个人数据泄露对国家安全有一定的影响,某些特定人员的个人数据直接关系到国家安全。例如,APP记录的军人行动路线,导致美国军事基地数据泄

露。另一方面,大规模的个人数据处理,对国家安全也具有一定的影响。据国外媒体报道,剑桥分析公司通过分析平台的用户政治倾向等数据,通过脸书进行广告投放诱导性新闻,影响脸书用户的投票行为,最终在美国大选与英国脱欧事件中发挥重要作用。

因此,对国家安全属于下个人数据进行研究有必要的,本位将从国家安全视域下个人数据治理的困境以及形成的原因进行分析,对我国个人数据治理提供一定的理论价值。

二、国家安全视域下个人数据治理的现实困境

(一)个人数据的不可控性导致国家安全风险增加

随着大数据、云计算、5G等技术的发展,使得个人数据传播得更加快速、广泛和隐蔽,这加剧了个人数据传播的不可控性。首先,新兴的技术降低了获取个人数据的难度。新兴的技术的运用降低了海量数据的处理难度,使得对数据处理花费的成本减少,降低还原个人数据的难度。其次,被获取个人数据的传播更加广泛和迅速。数据传播没有时间和地域的限制,一旦泄露将面临被传播的风险。最后,个人数据泄露损害多重法益。个人数据还会被新兴的技术进行深度计算,策划还原一国国家经济运用,关键设施等事关国家安全的数据。

(二)大规模个人数据的不当收集导致国家安全风险增加

大量收集用户个人数据广泛存在于各个数据平台,其目的是为了提供更好的商品或者服务。但是,这种收集在现实中往往存在一些问题。一方面,数据

平台在收集数据的过程中存在不合理收集、获取非必要个人数据的现象。当前，为给用户不同服务，数据平台收集个人数据时存在“越多越好、越细越好”的现象。另一方面，数据平台对于个人数据的处理和披露存在匿名化程度未达标的现象。《网络安全法》第四十二条规定，数据匿名化的标准是指经过加工无法识别且不能复原的个人信息，而在某些互联网平台存在非法披露未经允许披露的匿名化未达标的现象。而当越来越多、越来越细的数据被不合理收集以及不合法披露，都会对国家安全造成影响。

（三）个人数据的统一监管欠缺导致国家安全风险增加

国家安全在个人数据的传播与披露之下面临着巨大冲击，要想解决个人数据造成国家安全风险的问题，事前的防范与事后惩罚都极为重要，而我国想要建立一个完整的国家安全视域下个人数据治理体系面临着一个难题：没有对应的个人数据治理管理机构。在个人数据治理过程中，工业与电信部门只涉及电信与互联网管理，并不涉及对个人数据的治理，国家安全部门对于个人数据中国家安全风险的管理也存在一定的滞后性，同时也缺乏专业性。而在私主体权益受损时，其多以民事诉讼为主，国际安全方面也被忽略。

三、国家安全视域下我国个人数据治理困境的成因

（一）个人数据中国家安全法益的不确定性

个人数据的不可控性导致国家安全风险的来源，主要是由于个人数据中国家安全法益难以确定。当明确受到损害时，受害主体自会采取相应措施保护个人数据。从个人角度而言，当个人数据披露会对个人造成损害时，数据主体将会采取措施制止该种数据的披露，例如我国《个人信息保护法》中规定的知情同意原则以及相应的出发规定都赋予了数据主体相应的权利。与企业角度而言，数据的泄露会对企业造成损害时，该企业也会采取相应的挽救措施。同样，从国家角度而言，当个人数据披露会导致国家安全风险时，相关部门亦是采取相应举措，而在我国的个人数据治理体系中存在着一系列的国家安全保护条文。但是，由于个人数据的体量庞大繁杂，国家相关部门对于其中是否蕴含国家安全法益难以确定，同样，将保护国家安全的责任下放到个人或企业也难保其对个人数据中国家安全法益有明确的认识，且个人和

企业在遵循法律规制之外，对于国家安全利益并不具有明确的相关性。因此，个人数据的披露造成了国家安全面临风险。

（二）个人数据权属不清，利益相关者不明确

要想对个人数据治理形成从国家安全到个人合法权益的全面的保护，最重要的是确保该数据权属的主体是明确的，将责权进行具体明确的划分。目前，对于个人数据权属的划分有三种观点：第一种观点认为，个人数据的权属应当归于自然人，强调保护个体的权利；第二种观点认为，个人数据的权属也能够当归于数据处理者（此处包括数据收集者、存储者与控制者），强调数据的财产性质；第三种观点认为，个人数据应当归于国家，以国家为利益平衡者，平衡个人权益、数据财产与国家安全等法益的平衡。但无论第一种与第二种中关于个人数据权属的划分，都忽视了个人数据中的国家安全属性，过分强调私主体的权利。而第三种国家所有模式，能够很好地兼顾各方利益，但有很多学者指出，在国家控制下，资源配置和交易得不到优化，经济效率受到影响，不利于国家经济的发展。

（三）缺乏共性的利益衡量标准

个人数据治理是对个人对其个人权益的保护的要求，是对数据开发利用促进经济发展的需要，也是保障国家安全的体现。由于个人数据的多重法益，而且这些法益存在交叉竞合的范畴。由于个人数据的多重法益属性，导致个人数据中国家安全、个人权益与经济权益发生了交叉竞合。一方面，个人数据中多种法益保护存在一致性，保护一种法益的同时也能够保护另一种法益。例如，《个人信息保护法》中规定的个人敏感信息，对该种个人信息的保护不仅是对个人权益的保护也是对国家安全的保护。另一方面，个人数据中的法益保护存在矛盾，例如，当个人基于知情同意的基础上传输披露自己的个人数据时，与国家安全相关的数据有可能会随之披露，这是个人的权益与国家安全发生了冲突。而造成这种冲突的原因在于，无法明确个人数据中不同法益的利益，在缺乏利益衡量标准的情况下，无法实现对于国家安全视域下个人数据治理的全面保护。

四、国家安全视域下个人数据治理的对策

（一）厘清国家安全利益，细化数据分类分级

厘清个人数据中的国家安全信息，是在国家安

全视域下推动个人数据治理的前提和基础。首先,并非所有的个人数据都包含国家安全信息,如果对个人数据采取全面的国家安全保护,不利于我国法治资源的配置,也不利于我国个人数据开发和利用;其次,一般个人数据只有在数量上升到一定的程度,才有可能提炼出国家安全信息;最后,个人数据在国内国外呈现不同的表现态势,有些在国内并不会危害国家安全,例如敏感个人数据,但是当其出现在国外,可能会对我国国家安全造成危害。对于此类问题,我国《数据安全法》确立了数据分类分级制度,将数据进行分类与分级,根据数据的类别以及可能造成的危害进行分类和分级。根据数据分类分级制度,将个人数据进行分类和分级。对此,有必要根据个人数据是否直接蕴含国家安全信息以及其蕴含的国家安全信息的重要程度进行分级保护,对于集中的个人数据根据其数据的规模进行分级。并根据该数据处境与否进行区别审查,以保障国家安全。

(二) 以数据权属的利益相关度确定权属

明确个人数据的权属,是实现国家安全视域下个人数据治理的关键。在上文所提的三种权属中无论是自然人所有模式还是数据处理者所有模式,抑或国家所有模式,都存在一定的不足。首先,自然人所有模式过分强调个人权益,限制了企业对个人数据的获取,降低了数据利用效率;其次,数据处理者所有模式过分强调财产权益,不能很好地保障国家安全和自然人权益;最后,国家所有模式不利于数据市场的资源配置和发展,被大部分学者批判。因此,应该采取多元化模式,根据个人数据泄露造成的危害后果进行针对性适用,当个人数据泄露对个人权益造成极大危害时,采取自然人所有模式;当个人数据泄露损害企业财产利益时,采取数据处理者所有模式;当个人数据泄露导致国家安全问题时,采取国家所有模式。根据其数据的利益相关程度确定个人数据的权属,完善国家安全视域下个人数据治理的方案。

(三) 以有限度地克减私主体利益为利益衡量标准

当个人数据治理中多重法益产生矛盾时,确定不同利益的衡量标准就变得尤为重要。一方面,国家安全利益高于个人利益与企业利益。国家安全时

国家的最根本利益之一,其实现通常是以限制、牺牲与剥夺私主体利益为条件或代价。究其原因是国家安全高于私主体这一基本原则,国家安全是长远的、根本的更高层次的利益,其本身就是私主体权益让渡的结果。另一方面,国家安全实现的优先性应当受到正当程序的限定。国家安全不应一直占据优先和主导地位,否则不仅是对私主体的合法权益侵害,也违反了国家安全的正当性原则。在国家安全视域下个人数据治理体系中,对于国家安全与私主体权益产生矛盾之时,应当采取有限度的克减私主体权益为手段,明确国家安全保护的正当性与必要性,而非谈国家安全而色变,只要个人数据涉及国家安全就采取国家安全保护,削减私主体的权利。同时保护国家安全要合理、合法,个人数据治理涉及多个法律部门,甚至需要联合执法部门进行执法,为此应当明确数据治理权限,形成协调配合的执法体系。

结语

将个人数据治理置于国家安全视域下,是保障我国数字经济建设的稳定发展的重要需求。然而这一需求既要求我国保障个人数据的自由流动与开发利用,又要求我国保障国家安全。将个人数据治理的重心放在私主体的利益平衡显得更加施行,但是国家安全为其带来了更加复杂的利益平衡,国家安全优先使得个人数据治理面临新的挑战。解决这些挑战,首先要厘清个人数据中的国家安全范围,解决个人数据不可控风险;其次,根据利益相关度明确个人数据权属,应对大规模个人数据聚集时的不同风险;最后,有限克减私主体权益,遵循国家安全优先。

参考文献:

- [1] 赵鹏. 个人数据保护的合作治理模式研究[J]. 人民论坛·学术前沿, 2023(06):28-37
- [2] 郭海玲, 刘仲山. GDPR 对我国跨境数字贸易企业个人数据保护研究——基于数据生命周期理论[J/OL]. 情报杂志:1-8[2023-07-26].
- [3] 季良玉. 数据权属如何界定: 一个讨论[J]. 财会通讯, 2023(14):10-14.
- [4] 梅傲, 柯晨亮. 数据共享与数据财产化[J/OL]. 四川师范大学学报(社会科学版):1-10[2023-07-26].