国家参与视域下个人信息利用与保护的平衡之道

——以疫情期间公民涉疫信息全生命周期的处理为例

引言

在当今以物联网、“云”等要素为典型特征的大数据时代，信息以其生产力属性和技术支撑，一跃成为一种新兴商品。[①]个人信息隐私经收集与处理后，在社会的各方各面得到充分利用。“个人数据驱动”的社会也带来了一系列风险与治理挑战。[②]2021 年，我国个人信息保护法通过[③]，企业操作用户数据的行为被细化约束，信息隐私被纳入了国家的绝对监管之下。

在涉及个人隐私的问题上，国内已有的文献大多聚焦在如何协调个人与信息业者之间的信息边界。然而，一系列涉及国家与个人及信息业者的矛盾冲突表明[④]，国家不再是“超然物外”的审视者，而早已介入了信息的收集利用之中。但国家对自身的监管与立法可能或有阙如。国家对公民信息的保护承诺，才赋予其利用数据的合法性，国家数据权力边界国家也应限制在充分实现国家治理与安全的考量之内。

本文将围绕个人信息的价值利用与安全保护这对命题，从国家参与的视域切入，以公民涉疫信息全生命周期的处理为例，探究国家利用公民数据的权力边界、保护公民隐私的最低红线，亦即两者之间的平衡之道。

---

① 李海舰，赵丽：《数据成为生产要素：特征、机制与价值形态演进》，《上海经济研究》2021 年第 8 期，第 48-59 页。

② 孟小峰，慈祥：《大数据管理：概念、技术与挑战》，《计算机研究与发展》2013 年第 1 期，第 146-169 页。

③ 中华人民共和国全国人民代表大会常务委员会.（2021 年 8 月 20 日）. 中华人民共和国个人信息保护法. 中国人大网. http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

④ 例如，防疫过程中公民强制申报“健康码”，涉及国家与个人的隐私权衡；苹果公司与 FBI 的“法律攻防战”，则有关国家与信息业者对用户隐私的控制问题。*See* Burum, Sue, & Georgia Holmes, “Apple v. FBI: Privacy vs. security?”, *National Social Science*, 2017, pp. 9-22.

文献综述

（一）信息商品的“掘金”时代

信息社会(Information society)一词最早可追溯到上世纪七十年代。以信息的创造、使用、分发和整合为典型活动的信息社会，经数据存储、传输等技术大爆发的加持，逐渐演进为一个万物互联互通的智能社会。[①]“个人数据驱动”可以说是当下社会生活的代表面：小到个人生活，如刷脸消费与“大数据杀熟”；或是企业提供产品服务，如大型语言模型(LLM)的训练；大到国家治理、国家安全，如“最多跑一次”政务互通与犯罪罪证的追证。

上述种种，正说明了个人信息数据中蕴藏的巨大经济效益被渐加认识与充分发掘。早在1999 年，信息要素稍有萌芽之势，美国经济学家 Hal R. Varian 便已意识到信息商品的潜在市场。他在 *Markets for information goods* 一书中提到，信息商品具有高固定成本和低边际成本、网络外部性、捆绑和个性化等独特的特征，这些特征影响了它们的生产、分配与消费。他一并提供了一个分析这些特征，并将它们应用于网络经济中各种商业策略的框架。[②]之后的几十年直到如今，个人信息一直被政府和信息业者充分利用，带来了巨大的政治效益、经济效益与社会效益，形塑了我们所处的这样一个数字时代、信息时代。[③]

（二）国家/政府对信息业者的“监视”与对自己可能的“放任”

个人信息中可供发掘的价值，吸引了公司企业争相涉足信息业这块“宝地”。各款应用争相收集用户从个人信息到搜索喜好的各种数据，并通过背后的“信息高速公路”实现用户数据互通。[④]它们将一个个用户实体抽离为一个个信息点，实现了精准推送与个性化服务。然而，由于信息业领域的快速兴起，适配的行业规范尚未完全成熟，导致个人隐私安全问题频出：既出现了诸如“霸王条款”等事关信息收集的乱象，又有数据加密缺失、第三方信息出售等事关隐私泄露的危险。[⑤]

面对个人信息巨大的经济利益的“糖衣外壳”下同样巨大的安全隐患，各国都在逐步制定一系列的法律法规与行业准入规范，以期达到必要的保护效果。隐私保护技术主要有扰动

[①] 丁波涛：《从信息社会到智慧社会：智慧社会内涵的理论解读》，《电子政务》2019 年第 7 期，第 120-128 页。

[②] Hal R. Varian, *Markets for information goods*, Institute for Monetary and Economic Studies, Bank of Japan, 1999.

[③] Dufva, Tomi & Mikko Dufva, “Grasping the future of the digital society”, *Futures*, 2019, pp. 17-28.

[④] Aliya Ram et al., *How smartphone apps track users and share data*, October 23, 2018, https://ig.ft.com/mobile-app-data-trackers

[⑤] Alex Rolfe, *Invasive apps: which apps are sharing your personal data*, March 10, 2021, https://www.paymentscardsandmobile.com/invasive-apps-which-apps-are-sharing-your-personal-data

技术、加密技术和匿名化技术三类，而个人隐私数据涉及收集、储存、利用等过程，因此需要建立多级保护机制。[①]2021 年，《中华人民共和国个人信息保护法》审议通过，信息业者操作用户数据的行为受到严格约束。

但另一方面，在个人信息的保护和利用这个议题上，国家与其是监控个人与信息业者博弈的“在上者”，事实上已是参与到信息流通的各个环节中的主体之一。但不同于信息业者，国家在对公民信息的收集与利用过程中或有缺少自我监管的现象存在，相关自我立法可能也暂付阙如。美国政府一直致力于公民数据的“挖掘”(mining)，不惜以耗时的、昂贵的代价收集巨量的公民信息，用于国家治理、社会控制等目的，而无关这些数据的必要与否、侵犯公民隐私与否。[②]疫情初期，我国部分地区政府在推行“健康码”过程中乱象频出，个人信息安全问题受到极大威胁：用户知情权、同意权被架空，各类信息的录入成为强制要求；逾越最小必要原则，无助于防疫的公民信息被过度收集；监管缺失、保护疲软，个人隐私在网络“黑市”上高速流通。[③]

（三）国家的数据权力来源与权力边界

对于信息流通过程中国家主体的可能的不当行为，一些人开始思考国家的权力来源、权力边界等问题，特别是限定在数据权力上的合法性问题。黄明涛在讨论权力机关的权力边界时指出，“国家的……实际‘行动能力’决定了‘应当由其行使的职权’是有限的。”[④]进一步思考国家数据权力的合法性，张新宝认为 “政府不能无节制地肆意收集和利用个人信息……这是因为个人信息法律保护制度的构建……是为维护政府自身政权合法性所必须。”[⑤]国家（或政府）在收集公民数据前对其隐私性的保护的承诺，才赋予其利用数据的合法性。如果国家任意收集各种公民信息，无论其有助于治理与否，并对这些涉私数据缺乏监管、不予保护，那么它实际上已经丧失了这部分被赋予的数据权力。因此，国家的数据权力边界，应当限制在足以充分行使各项职能的范围之内，这是合理的也是唯一的红线。

宁园也对健康码数据收集权力与合法性进行回应。对于新冠肺炎疫情这一重大公共卫生事件，政府推广健康码是基于公共卫生安全至上、对公民最基本的生命健康权保护的考量。这是国家正当的、绝对的权力来源。因此，政府对健康码信息的收集使用只能以防疫目的的

---

① 刘雅辉等：《大数据时代的个人隐私保护》，《计算机研究与发展》2015 年第 1 期，第 229-247 页。
② Fred H. Cate, “Government data mining: The need for a legal framework”, *Harv. CR-CLL Rev*, 2008.
③ 宁园：《健康码运用中的个人信息保护规制》，《法学评论》2020 年第 6 期，第 111-121 页。
④ 黄明涛：《“最高国家权力机关”的权力边界》，《中国法学》2019 年第 1 期，第 104-121 页。
⑤ 张新宝：《从隐私到个人信息：利益再衡量的理论与制度安排》，《中国法学》2015 年第 3 期，第 38-59 页。

实现为唯一必要。然而，作者指出，

> 个人信息处理也存在超出必要之嫌。如北京市、上海市健康码生成以个人进行面部识别为必要，个人必须提交面部信息、虹膜信息，然而在同样担负防疫重任的其他城市（如武汉、长沙等），并不存在强制性的面部识别。

这一现象说明，防疫的目的完全可以在不依靠公民面部信息的情形下达成。[①]国家健康码数据的权力存在越界的可能。

（四）个人信息的价值利用与安全保护的冲突与平衡

上述种种现象突出了国家（或政府）在个人信息的价值利用与安全保护方面的冲突。2016年，美国联邦调查局(FBI)和苹果公司关于解锁嫌犯手机的冲突，引发了一场对隐私的大讨论。一方面，苹果公司拒绝解锁嫌犯手机，使得无法利用个人信息在案件侦破中的价值，直接影响了国家安全；另一方面，若苹果公司答应解锁手机，可能导致公众对自己信息安全的忧虑。[②]又例如，各国都在积极推动政务数据共享开放，这在充分利用公民数据的同时，也会存在隐私信息泄露的风险。[③]

国家也在积极促成两者之间的平衡。P. T. Jaeger 等人曾对数据要素刚起步的美国进行研究。当时的美国对个人信息管理分散，法律、政府、司法三者不统一，导致隐私保护效率低下、安全堪忧。作者提出了多种数据保护的国家结构模型，普遍采用一个高度独立、高度集权的隐私管理机构，以“中央集权”的方式统一个人信息的收集、管理与利用，在保护隐私安全的同时做到经济效率的提高。[④]同样，黄如花、刘龙在研究我国政府数据开放中个人隐私保护问题时也得出了相似的结论：一个国家级的数据开放平台、独立的权威监管机构、确切的立法与严格的审查，有助于保证隐私安全与利用数据价值。[⑤]由此可见，各国都在寻求如何在保护隐私的同时实现个人信息的效益最大化。

[①] 宁园：《健康码运用中的个人信息保护规制》，第 114 页。

[②] Michael Hack, “The implications of Apple's battle with the FBI”, *Network Security*, 2016, pp. 8-10.

[③] Noveck, B. S., “Rights-based and tech-driven: Open data, freedom of information, and the future of government transparency”, *Yale Hum. Rts. & Dev. LJ*, 2017.

[④] Jaeger, P. T., McClure, C. R., & Fraser, B. T., “The structures of centralized governmental privacy protection: approaches, models, and analysis”, *Government Information Quarterly*, 2002, pp. 317-336.

[⑤] 黄如花，刘龙：《我国政府数据开放中的个人隐私保护问题与对策》，《图书馆》2017 年第 10 期，第 1-5 页。