理论思考

文章编号：1001 - 2397(2019)03 - 0096 - 15

论个人信息法律保护的思想渊源与基本原理

——基于“公平信息实践”的分析

丁晓东

(中国人民大学 法学院，北京 100872)

摘 要：公平信息实践构成了全球个人信息保护的思想渊源与基本框架。对公平信息实践的演化和全球各个版本公平信息实践的原则进行总结，可以发现公平信息实践确立了以个人信息赋权与施加信息控制者责任的进路。但强化个人信息赋权却未必符合个人信息保护的基本原理，并不一定能够很好地保护个体的隐私权益。同时，对信息控制者施加某些责任也未必符合大数据的基本特征，不能恰当地利用与保护个人信息。本文提出大数据时代的公平信息实践版本，主张采取有限个体主义与动态化的个人信息保护。这一公平信息实践的版本强调平衡个人信息收集、处理和流通中的个体预期与社会预期，强调发挥个人信息的公共性价值与风险防范的个人信息保护进路。

关键词：公平信息实践；个人信息保护；大数据；个体主义；动态保护

中图分类号：DF49　　文献标志码：A
DOI：10.3969/j.issn.1001 - 2397.2019.03.07　开放科学(资源服务)标识码(OSID)：

个人信息保护研究已经成为法学界的热点。近年来，随着个人信息保护问题引起社会的日益关注，并且被列入国家的立法计划，各类个人信息保护研究的文献如雨后春笋般的兴起。但另一方面，在国内法学界的个人信息保护研究中，对于公平信息实践(fair information practices)的研究却基本处于空白状态，很少有学术文献对公平信息实践进行介绍，也几乎没有什么学术文献对不同版本的公平信息实践进行归纳总结，从原理上对其进行进一步分析①。

收稿日期：2019 - 01 - 15

基金项目：2018 年度国家社科基金一般项目“大数据背景下的个人信息保护与企业数据权属研究”(18BFX198)

作者简介：丁晓东(1982)，男，浙江淳安人，中国人民大学法学院、未来法治研究院副教授，中山大学电子与通信工程专业学士，北京大学、耶鲁大学法学博士，中国人民大学法学院博士后研究人员。

① 在中国期刊网上以“公平信息实践”为主题或关键词进行搜索，搜索结果只有一篇文献。(参见：黄缘缘，谢恩，张涛. 我国电子商务网站 FIPs 实施现状研究[J]. 管理学报，2011(8).)

对于我国的个人信息保护研究与个人信息立法而言,这不能不说是一个遗憾。从思想渊源与制度架构来说,公平信息实践提供了个人信息保护法或信息隐私法(information privacy)的思想渊源,奠定了现代信息隐私法的框架。隐私法研究的权威学者保罗·施瓦茨(Paul Schwartz)指出"公平信息实践是现代信息隐私法的基石"[1]1607-1614。长期关注隐私问题的专家保罗那·布鲁宁(Paula Bruening)也指出"公平信息实践的基本原则已经为世界各国、地区、公司和个人提供了关于数据保护和隐私的共同语言……当存在隐私或数据保护失败时,它们提供了测量遵守的工具和执行手段①。"一言以蔽之,公平信息实践"已经成为全球隐私保护的重要准则",得到了包括中国在内的全球各个国家的认可②。

本文对公平信息实践进行了介绍、总结和反思。通过对公平信息实践的介绍和总结,可以发现公平信息实践的不同版本都采取个体信息赋权与施加信息控制者责任的原则。但通过对公平信息实践的基本原理进行反思,可以发现过度强化个体信息赋权并不能有效保护公民个体的相关权益,某些施加于个人信息控制者的责任也并不合理。为了更有效地发挥公平信息实践的指引性作用,本文提出了新版本的公平信息实践。这一版本采取有限个体主义的立场与动态的个人信息保护进路,提出个人信息保护应当注重个人与社会对于个人信息流通的合理预期。同时,在大数据已经到来的时代,公平信息实践更应当注重发挥个人信息的流通价值与公共性价值,在此前提下采取措施防范相关风险。

一、公平信息实践的起源

公平信息实践诞生于1973年。二十世纪七十年代,美国政府用计算机数据库处理个人信息日益普遍,为了回应伴生的问题,美国政府在医疗、教育与福利部门成立了一个"关于个人数据自动系统的建议小组"(Advisory Committee on Automated Personal Data Systems)。这个小组在1973年首先发布了一份"公平信息实践准则"报告,确立了处理个人数据的五项原则③:

(1)必须禁止所有秘密的个人数据档案保存系统。

(2)必须确保个人了解其被收集的档案信息是什么,以及信息如何被使用。

(3)必须确保个人能够阻止未经同意而将其信息用于个人授权使用之外的目的,或者将其信息提供给他人,用作个人授权之外的目的。

(4)必须确保个人能够改正或修改关于个人可识别信息的档案。

(5)必须确保任何组织在计划使用数据时,其创建、维护、使用或传播可识别个人数据的档案中的数据都必须是可靠的,并且必须采取预防措施防止数据的滥用。

1973年的公平信息实践准则在1977年美国政府设立的"隐私保护学习委员会"报告中得到了进

① 参见:Paula Bruening. Rethink Privacy 2.0 and Fair Information Practice Principles: A Common Language for Privacy(2014)[EB/OL]. [2019-01-10]. http://blogs.intel.com/blog/rethink-privacy-2-0-and-fair-information-practice-principles-a-common-language-for-privacy/.

② 公平信息实践"不仅在美国扮演了关键性角色,而且已经成为全球隐私保护的重要国家准则"。参见:Marc Rotenberg. Fair Information Practices and the Architecture of Privacy: What Larry Doesn't Get[J]. Stan. Tech. L. Rev,2001:1-34.

③ 参见:Records. Computers and the Rights of Citizens Report of the Secretary's Advisory Committee on Automated Personal Data Systems[EB/OL]. [2019-01-15]. https://epic.org/privacy/hew1973report/Summary.htm.

一步发展。美国政府曾经在 1974 年设立“隐私保护学习委员会”(Privacy Protection Study Commission) ,对一系列隐私问题重新进行审查。1977 年,“隐私保护学习委员会”在提交给美国总统卡特的报告中,进一步发展了公平信息实践,设定了数据保护系统的三大目标[①]:

(1) 在个人对档案储存机构的期待和机构的实际做法之间保持平衡(最小化干涉性) 。

(2) 对于档案储存的操作,应尽可能减少个人的档案信息成为导致对其不公平的渊源(最大化公平性) 。

(3) 对于个人的档案信息的使用和披露,应当建立和界定有关责任(建立合法的、可执行的保密预期) 。

此外,“隐私保护学习委员会”报告还将公平信息实践的原则从五项扩展至八项[②]:

(1) 公开原则: 必须禁止所有秘密的个人数据档案保存系统,而且机构应当设立个人数据档案的保存政策、实践和系统的公开政策。

(2) 个人访问原则: 对于档案保存机构以个人可识别形式保存的有关信息,必须确保个人有权查看和复制。

(3) 个人参与原则: 对于档案保存机构,必须确保个人有权更正或修改实质性的其为档案储存机构所保存的信息。

(4) 收集限制原则: 对于一个机构可以收集的关于个人信息的类型,以及收集方法,应当存在某些限制。

(5) 使用限制原则: 在档案保存的机构内,对个人相关信息的使用应当有限制。

(6) 披露限制原则: 对于档案保存机构可能作出的对外披露个人信息,应予以限制。

(7) 信息管理原则: 档案保存机构应当制定合理、适当的信息管理政策和做法,保证收集、维护、使用、传播有关个人的信息是必要的、合法的,而且信息本身是最新和准确的。

(8) 问责原则: 档案保存机构应当对个人数据档案保存的政策、实践和系统承担责任。

总结而言,1973 年“关于个人数据自动系统的建议小组”和 1977 年“隐私保护学习委员会”所提供的两个版本的公平信息实践大致确立了个人信息保护的基本框架与原则。一方面,公平信息实践对个人进行了信息赋权,规定了个体所享有的一系列信息权利,例如个人的信息访问权、更正权与修改权等权利。另一方面,公平信息实践也对信息收集者或处理者施加了一系列义务,规定个人信息收集者或处理者应当承担相应义务,例如收集个人信息时的告知义务、使用个人信息的目的限制义务、个人信息安全保障义务等。

二、公平信息实践的影响与演化

公平信息实践的理论提出后,对美国、欧洲与国际组织的个人信息保护或信息隐私法产生了深远

① 参见: The Privacy Protection Study Commission, Personal Privacy in an Information Society (1977) , Introduction [EB/OL] . [2019 - 01 - 20] . https: //epic. org/privacy/ppsc1977report/c1. htm.

② 参见: The Privacy Protection Study Commission, Personal Privacy in an Information Society (1977) , Chapter 13 [EB/OL] . [2019 - 01 - 22] . http: //aspe. hhs. gov/datacncl/1977privacy/c13. htm.

的影响,这些国家和地区的法律或者明确接受公平信息实践,或者在其法律规定中体现公平信息实践的各项原则。

1. 美国

公平信息实践的原理极大地影响了美国的信息隐私立法。在联邦层面,1974 年美国隐私法案(The Privacy Act)直接采用了 1973 年公平信息实践的若干原则①。其后,在《家庭教育权利与隐私法》(Family Educational Rights and Privacy Act of 1974)②、《联邦有线通讯政策法案》(Cable Communications Policy Act)③、《视频隐私保护法》(Video Privacy Protection Act)④、《司机隐私保护法案》(Driver's Privacy Protection Act)⑤等法案中,公平信息实践的原理都得到了相应体现。在州政府层面,很多州开始根据公平信息实践原则来规范州政府收集个人信息的情形。例如马萨诸塞州制定了关于政府收集个人数据的一般性法律,将公平信息实践作为专门一章⑥;明尼苏达州制定的《政府数据实践法案》(Minnesota Government Data Practices Act),进一步具体化公平信息实践的原则⑦。

此外,一些规制机构和贸易委员会也采取或推行公平信息实践的若干原则[8]。如美国联邦贸易委员会(Federal Trade Commission)在其 2000 年报告中指出,当网站商业机构收集个人信息应当接受"四项广为接受的公平信息实践"⑧:

(1)告知:网站需要向消费者提供关于其信息实践的清晰和明显的告知,包括收集什么信息、如何收集信息(例如,直接或通过非显而易见的方式,如 cookie)、如何使用信息、如何向消费者提供选择、可访问性与安全、是否向其他实体披露收集的信息,以及其他实体是否正在通过网站收集信息。

(2)选择:网站除了在消费者提供信息以完成服务时(例如完成一项交易)给出选择之外,还需要向消费者提供关于如何使用他们的个人识别信息的选择。这种选择将包括内部二次使用(例如向消费者再次进行营销)和外部二次使用(如向其他实体公开数据)。

(3)可访问性:网站应向消费者提供对网站收集的关于他们的信息的合理访问,包括审查信息和纠正不准确或删除信息的合理机会。

(4)安全:网站需要采取合理步骤来保护所收集信息的安全性⑨。

2. 欧洲

欧洲立法对于公平信息实践的继受同样明显。1980 年,欧洲议会通过了有关个人数据保护的《保护自动化处理个人数据公约》(Convention for the Protection of Individuals with regard to the Automatic

① 参见:5 U.S.C. § 552a [EB/OL]. [2019-01-26]. http://www.law.cornell.edu/uscode/text/5/552a.

② 参见:20 U.S.C. § 1232g (2006).

③ 参见:47 U.S.C. ch. 5, subch. V-A (2006).

④ 参见:18 U.S.C. § 2710 (2006).

⑤ 参见:18 U.S.C. §§2721-2725 (2006).

⑥ 参见:Mass. Gen. Laws ch. 66A [EB/OL]. [2019-01-30]. https://malegislature.gov/Laws/GeneralLaws/PartI/TitleX/Chapter66A.

⑦ 参见:Minn. Stat. § 13.01 et seq [EB/OL]. [2019-02-02]. https://www.revisor.mn.gov/statutes/?id=13.01.

⑧ 参见:Federal Trade Commission, Privacy Online: Fair Information Practices in the Electronic Marketplace [EB/OL]. [2019-02-03]. http://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf.

⑨ 美国联邦贸易委员会曾经在 1998 年将公平信息实践归纳为五项原则,除了 2000 年的四项原则之外,还包括了"执行-救济"的原则。(参见:Federal Trade Commission, Privacy Online: A Report to Congress 7 (1998) [EB/OL]. [2019-02-10]. http://www.ftc.gov/sites/default/files/documents/public_events/exploring-privacy-roundtable-series/priv-23a_0.pdf.)

Processing of Personal Data)。这部公约规定,如果存在自动化处理个人数据,数据主体应当有权知晓,并且了解其主要目的;数据主体有权确认与数据主体有关的个人数据是否存储在文件中;有权查看、纠正或删除数据;有权获得未能遵守其他权利的救济。

其后,在 1995 年制定的《欧洲议会和理事会关于个人数据处理和自由流动的个人保护》的指令中,公平信息实践的一系列原则又得到了体现。根据工作小组的解释,这部指令至少体现了如下八项反映公平信息实践的原则①:

(1) 目的限定原则:数据应当只能因为某个目的而被处理,而且数据转移不应当与此目的相冲突。

(2) 数据质量与比例原则:数据应当准确,必要时应当及时更新。对于数据被转移或进一步处理,数据应当及时、相关且不超过一定的目的。

(3) 透明性原则:个体应当有权获取相关信息,比如处理的目的和数据控制者的身份,以及其他为了保证公平性的信息。

(4) 安全性原则:数据控制者应当采取恰当的技术与组织性措施来应对处理风险。

(5) 可访问性、纠正与反对的权利:数据主体应当有权获取其被处理的信息的备份,应当有权更正不正确的信息。在某些情形下,个体应当有权反对对其信息进行的处理。

(6) 对进一步转移的限制:对于进一步的个人数据转移,只有第二个接收者也受到同样恰当程度的保护,这种转移才能被允许。

(7) 敏感信息:对于涉及"敏感"类的数据,需要采取额外保护措施,比如要求得到数据主体对处理的明确同意。

(8) 自动化个人决策:当数据转移的目的是为了自动化决策,个体应当有权知晓决策的逻辑,而且必须采取其他措施来保证个体的正当利益。

欧盟于 2016 年制定并于 2018 年生效的《一般数据保护条例》可谓是公平信息实践在欧盟法中的最新体现。第 5 条规定,在处理个人数据时,应当遵循如下六项原则,并承担遵守责任和证明责任②:

(1) 合法性、合理性和透明性:对涉及到数据主体的个人数据,应当以合法的、合理的和透明的方式进行处理。

(2) 目的限制:个人数据的收集应当具有具体的、清晰的和正当的目的,对个人数据的处理不应当违反初始目的③。

(3) 数据最小化:个人数据的处理应当是为了实现数据处理目的而适当的、相关的和必要的。

(4) 准确性:个人数据应当是准确的,如有必要,必须及时更新;必须采取合理的措施确保个人数据的准确性,即违反初始目的的个人数据,及时得到擦除或更正。

(5) 限期储存:对于能够识别数据主体的个人数据,其储存时间不得超过实现其处理目的所必需

① Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (Eur. O. J. 95/L281).

② 欧洲《一般数据保护条例》[EB/OL]. [2019-02-11]. http://www.calaw.cn/article/default.asp?id=12864.

③ 根据《一般数据保护条例》第 5 条第 1 段(b)规定"因为公共利益、科学或历史研究或统计目的而进一步处理数据,不视为违反初始目的。"

的时间[①]。

(6)数据的完整性与保密性:处理过程中应确保个人数据的安全,采取合理的技术手段、组织措施,避免数据未经授权即被处理或遭到非法处理,避免数据发生意外毁损或灭失。

3. 国际组织

国际组织对于公平信息实践规定最为著名的当属经济合作与发展组织(OECD)。1980 年,OECD 制定了《隐私保护与个人数据跨境流通指南》,确定了个人数据保护的八项基本原则:

(1)收集限定性原则:个人数据的收集应当有限定性,而且任何此类数据都应当以合法和公平的手段获取,在合适情况下应当获取数据主体的了解或同意。

(2)数据质量原则:个人数据应当和它们将被使用的目的相关,应当是为了实现这些目的所必要的,而且应当准确、完整并且及时更新。

(3)目的说明原则:应当在数据收集之前说明收集个人数据的目的,使用收集的个人数据也应当只限于实现此类目的,或者和此类目的并不冲突而且在每次改变使用时都已进行说明的目的。

(4)使用限定性原则:除了以下情况,个人数据不应被披露、访问或使用:(a)数据主体已经同意;(b)法律要求。

(5)安全保障原则:应采取合理的安全保障措施,保护个人数据免受诸如丢失、未授权访问、销毁、使用、修改或公开数据的风险。

(6)公开原则:对于个人数据的发展、实践和政策的公开,应当有一般性政策。对于确定个人数据是否存在,个人数据的性质,使用个人数据的主要目的,以及数据控制者的身份和常住地,应当有现成的方式来确定。

(7)个人参与原则:个人应当有权:(a)从数据控制者那里得知数据控制者是否有和他们相关的数据;(b)以如下方式被告知:i. 在一定的合理期限内;ii. 如果收费的话,不超出合理限度;iii. 以合理的方式;iv. 以一种可理解的方式;(c)如果(a)项和(b)项中的请求被拒绝了,可以获得拒绝的理由,并且可以对拒绝提出质疑;(d)质疑关乎他们的数据,而且,如果质疑是成功的话,可以要求将数据擦除、改正或完善。

(8)可责性原则:数据控制者有责任采取措施,保证实现上面提到的原则。

2013 年,OECD 发布了一项名为《OECD 隐私框架》(The OECD Privacy Framework)的新隐私政策,对 1980 年的《隐私保护与个人数据跨境流通指南》进行了大幅修改。OECD 认为,由于社会、经济以及新技术的发展,原来的隐私保护框架已经不足以应对时代的变化。但值得注意的是,虽然 OECD 在新的隐私政策中对一些内容进行了删减,但对于公平信息实践的八项原则却未加以任何改变。

除了 OECD,亚太经济合作组织(APEC)也延续了公平信息实践的若干原则。2004 年制定的《APEC 隐私框架》规定了信息隐私的九项原则[②]:

(1)预防损害:基于个人对于隐私的正当期待,应当设计个人信息保护以避免对此类信息的滥用。此外,基于对滥用个人信息所带来的伤害风险,应当对此类风险施加特定的责任,而且,救济措施应当

① 根据《一般数据保护条例》第 5 条第 1 段(e)规定“超过此期限的数据处理只有在如下情况下才能被允许:为了实现公共利益、科学或历史研究目的或统计目的,为了保障数据主体的权利和自由,并采取了本条例第 89(1)条所规定的合理技术与组织措施。”

② Asia – Pacific Economic Cooperation, APEC Privacy Framework, 2004/AMM/014rev1 (Nov. 2004).

和因为收集、使用和转移个人信息所带来的可能性和严重性相称。

(2) 告知: 对于个人信息的操作与政策,个人信息的控制者应当提供清晰且容易访问的声明。为了保证在收集个人信息之前或收集个人信息时提供此类信息,必须确保所有合理的可操作措施都已经采用。

(3) 收集限定性: 个人信息的收集应当限定于和收集目的相关的信息,此类信息应当通过合法和公平的方式获取,而且在合适的情况下应当告知个人或获取个人的同意。

(4) 个人信息的使用: 收集的个人信息应当只用于完成收集的目标和其他相关目的,除非: (a) 个人信息的主体已经表达同意; (b) 对于个人请求的产品或服务是必要的; (c) 法律或其他具有法律效力的法律文书、声明所要求的。

(5) 选择: 在合适的情形下,应当为个人提供一种清晰、显著、容易理解、容易访问和可承担的机制,使得个人能够选择对所涉及的个人信息进行收集、使用和披露。对于收集可公开获取的信息,要求个人信息收集者提供此类机制可能并不合理。

(6) 个人信息的完整性: 个人信息应当准确、完整以及在使用目标所需的限度内保持更新。

(7) 安全措施: 个人信息的收集者应当采取恰当的措施,保护其收集的个人信息免受风险: 例如丢失或对个人信息的未授权访问,或未授权损害、使用、修改或披露信息或其他滥用。此类措施应当与损害的可能性和严重性、信息的敏感性和语境相称,而且应当接受间歇性的审查和重新评估。

(8) 访问和可更正: 个人应当可以: (a) 向个人信息控制者确认,个人信息控制者是否有关于其的个人信息; (b) 在提供关于其身份的足够证据的情形下,要求以如下方式告知他们: i. 在一定的合理时间内; ii. 如果收费的话,不超过合理费用; iii. 以一种合理的方式; iv. 以一种普遍能理解的方式; (c) 确保他们信息的准确性,而且在恰当情况下予以纠正、完善、修改或删除信息。

(9) 可责性: 个人信息控制者有责任采取措施,使得上述原则得以落实。当个人信息被转移给其他个人或组织,不论是国内转移还是跨国转移,个人信息的控制者都应当获取个人同意,或者应当采取合理注意义务,采取合理措施保证个人信息的接收者或组织也能以符合上述原则的方式保护信息。

比较 APEC 隐私框架所规定的九项原则与 OECD 的八项原则,可以发现 APEC 隐私框架很大程度上沿袭了 OECD 的若干项原则的规定。但比起 OECD,APEC 增添了一项"预防损害"的原则。

4. 小结: 公平信息实践各版本的异同

比较各个版本的公平信息实践,可以发现公平信息实践的一些共同点与不同点。如同上文所述,不同版本公平信息实践的相同之处在于对个体进行信息赋权和对个人信息的控制者(信息收集者与处理者)施加责任①。而各个版本的公平信息实践的不同之处在于它们对信息主体的赋权程度不同,以及对信息控制者施加的责任不同。

首先,就赋权程度而言,不同的公平信息实践版本采取了不同刚性程度的赋权②。例如在美国联邦贸易委员会的公平信息实践版本中,其对于个人信息的赋权就是推荐性的,这就意味着在美国联邦

① 其他一些学者还指出了公平信息实践在程序义务上的一些共同特征。(参见: Paul M. Schwartz. Privacy and Democracy in Cyberspace [J]. Vanderbilt Law Review, 1999, 52(6): 1607 - 1614.)

② 总体而言,美国联邦贸易委员会的版本处于信息赋权程度最低的一段,欧盟最新的《一般数据保护条例》则处于赋权程度最高的一段。

贸易委员会的执法机制中,个体并不具有对其个人信息的法定性权利。个体在多大程度上具有对其个人信息的权利,取决于不同网站或机构所设定的隐私政策。只要这些隐私政策不存在欺诈或显著不合理的情形,那么个体所拥有的信息权利就是网站所公示的权利[3]。相反,有的法律,例如欧盟《一般数据保护条例》所赋予信息主体的若干权利就具有法律强制性。网站或机构并不能通过和个人进行谈判或合约而宣称个体放弃了此类权利。一旦网站或机构违反了个体的某些法定性权利,这些网站或机构就可能面临巨额罚款①。

除了刚性程度不同之外,不同的公平信息实践所赋予个体的权利种类也不同。几乎所有的公平信息实践都赋予个人或信息主体某些种类的权利:例如个人在其信息被收集时的被告知权和选择权;个人对于其信息的访问权、更正权等权利②。但对于其他权利,不同的公平信息实践版本则有不同的规定。例如美国的若干公平信息实践版本主要赋予了个体以若干传统权利,而欧洲《一般数据保护条例》则在传统公平信息实践所赋予的若干权利之外,增添了个体对于个人数据的擦除权(“被遗忘权”)③、限制处理权④、数据携带权⑤等权利。根据这些规定,个人可以在一定情况下要求数据收集者与处理者删除个人数据,要求控制者对处理进行限制,以及要求数据控制者提供可以自由传输数据的便利。

其次,不同公平信息实践对于信息控制者所附加的责任不同。尽管不同版本的公平信息实践都提到了可责性原则,但它们对于信息控制者所施加的限制并不相同。例如对于信息的收集和使用,很多公平信息实践版本都设定了目的限定原则和信息最小化原则。根据目的限定原则,信息的收集者在收集个人信息时必须明确信息收集的目的,对于个人信息的收集只能是为了完成个体所需,或者基于个体的明确授权;而根据信息最小化原则,对个人信息的处理必须是为了实现信息处理目的而适当的、相关的和必要的,对于信息的处理不能超出个体初始的授权。但在美国联邦贸易委员会的公平信息实践版本中,此类限制则并不存在。

此外,在个人信息的管理义务方面,不同版本的公平信息实践也不同。在早期的公平信息实践版本中,例如美国 1973 年版本与 1977 年版本中,对于信息控制者的责任主要侧重于对于个人信息本身的管理,例如确保个人信息的可靠性,防止个人信息的滥用。但到了 1980 年 OECD 版本的公平信息实践,“安全保障原则”开始被作为单独的一条原则加以提出,对个人信息的管理义务成为了安全保障的一部分。其后,到了 1995 年的欧盟指令与 2016 年的《一般数据保护条例》,对于信息控制者的风险防范义务变得更为明显,1995 年指令与 2016 年条例的很多条文都规定了信息控制者的风险防范与安全管理义务。同理,APEC 于 2004 年制定的隐私框架将“预防损害”作为个人信息保护的首要原则,也凸显了信息控制者的风险防范责任。综合这些规定,可以看出比起早期版本,后期的各类信息实践版本对信息控制者施加了更多的风险防范与治理义务。

---

① 根据《一般数据保护条例》第 85 条第 5 款,一旦违反核心条款,违法者可能面临 20000000 欧元或上一年全球总营业额 4% 的金额的罚款。

② 以赋权个体对自身信息控制的方式来促进公民相关隐私权益保护,这起源于信息隐私法的奠基人阿兰·威斯丁(Alan Westin)的思想,威斯丁将首次将隐私界定为“个人、群体或机构对自身信息在何时、如何以及在什么程度与他人沟通的主张”。(参见:Alan Westin. Privacy and Freedom [M]. New York: Atheneum, 1967: 7.)

③ 参见《一般数据保护条例》第 17 条。

④ 参见《一般数据保护条例》第 18 条。

⑤ 参见《一般数据保护条例》第 20 条。

三、个体信息赋权的反思

公平信息实践的关键之一是赋予个体以隐私自我管理的权利,即让公民个体选择是否允许信息收集者收集其个人信息,经过几十年的发展,这一思想已经成为了很多个人信息立法和学术讨论的基本范式[1] 1607 - 1659。但从理论上我们如何看待这种对个人的信息赋权? 这种个人信息赋权是否是保护个人信息不可置疑的共识? 在个人信息保护愈来愈重要的当下,是否可以说,法律对个人信息赋权程度越高越好?

答案并非如此简单。首先,强化个体信息赋权,个体不一定能够合理地保护自身权益。就个体控制自身信息的手段而言,个体在面对信息收集者收集个人信息时经常遇到的就是"告知 - 选择(notice - choice) "框架,即面对网站等信息收集者的告知而选择同意或拒绝其个人信息被收集[4]。但大量研究已然指出,这一框架愈来愈面临形式主义和异化的困境。面对网站的隐私公告,个体往往难以理解网站的隐私公告的专业性①; 个体没有足够的时间阅读此类枯燥的隐私公告②; 个体对于隐私公告中的相关风险往往缺乏足够的辨识和警觉③。对于现实社会中人们阅读隐私公告的多种调查表明,人们几乎很少真正阅读隐私公告④。在这样的背景下,"告知 - 选择"框架虽然看似赋予了个体以选择的权利,但这种格式化的隐私公告其实并不能真正发挥公告或意思表示的功能,而所谓的选择其实也并非深思熟虑或有意义的选择。更多时候,公民个体对隐私公告的选择只是一种漫不经心或无可奈何的点击[5-6]。

值得指出的是,即使法律作出了进一步规定,要求网站所提供隐私公告清晰易懂,这种规定也不足以改变"告知 - 选择"框架异化的困境⑤。很多公平信息实践和法律都提出隐私公告应当尽可能清晰易懂⑥,避免过于专业化,但问题是信息收集者对于信息的收集与使用本身就是非常复杂的,隐私公告用语的一般化并不足以改变其信息使用政策的复杂性。如果强行要求网站的隐私公告以简单的政策来表述其复杂的实践,那么其结果只能是个体更不能有效地理解信息收集者的隐私政策[7]。

进一步赋予公民以限制处理权等权利也未必能很好地保护公民的权益。赋予公民被遗忘权、限制处理权等权利意在克服个体在行使初始同意后对其信息的进一步控制,但在实践中,这种对于信息收集后的进一步控制权常常难以行使。公民个体很难理解其信息如何被储存、使用和转移,从而也就很难对后续的种种信息处理行为进行控制。以 Facebook 的信息泄露事件为例,对于剑桥分析公司(Cambridge Analytica) 利用心理研究的旗号向社会大众收集资料,其后又利用注册者及其朋友圈的个

---

① 此类研究,参见: Kent Walker. The Costs of Privacy [J]. 25 Harvard Journal of Law & Public Policy,2001,(25) : 87 - 107.

② 此类研究,参见: Lorrie Faith Cranor. Necessary But Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice [J]. J. Telecomm. & High Tech. L,2012,10(2) : 273 - 274.

③ 此类研究,参见: Alessandro Acquisti & Jens Grossklags. What Can Behavioral Economics Teach Us About Privacy? in Digital Privacy: Theory, Technologies and Practices, Acquisti, De Capitani di Vimercati, Gritzalis, Lambrinoudakis [M]. Auerbach Publications,2007: 363.

④ 例如美国 2006 年的一项研究发现,只有 20% 的人在"大多数情况下会阅读隐私公告"。而另一项研究则发现,只有 4.5% 的被调查者说他们总是阅读隐私公告,只有 14.1% 的人说他们经常阅读隐私公告。(参见: Helen Nissenbaum. Privacy in Context: Technology, Policy, and the Integrity of Social Life [M]. Stanford University Press, 2009: 105.)

⑤ 对于这一问题的进一步探讨,参见: M. Ryan Calo, Against Notice Skepticism in Privacy (and Elsewhere) [J]. Notre Dame Law Review, 2012,87(3) : 1027 - 1033.

⑥ 例如《一般数据保护条例》第 12 条规定 "控制者应当以一种简洁、透明、易懂和容易获取的形式,以清晰和平白的语言来提供。"

人信息来进行政治等领域的分析,在此过程中公民个体很难进行察觉,而且即使察觉了也未必愿意以及有能力行使反对权。在 Facebook 的信息泄露事件中,我们看到也只是在 Facebook 卷入了美国政治并且经过新闻媒体的大规模曝光,此次事件才为大众所察觉①。总之,在信息收集已经极为隐蔽和复杂的今天,完全期待公民个体以行使权利的方式来维护自身的隐私权益,这并不是一条特别现实的道路。

从企业与政府等信息收集者与处理者的角度来看,强化个体赋权无疑会增加其成本,但重要的是,此类成本的增加可能对于真正保护公民的隐私权益并无帮助。在个人信息保护高度依赖"告知 - 选择"框架与其他权利的前提下,企业可能会将大量资源投入到隐私公告与其他形式主义的合规上。对于信息控制者来说,只要其通过隐私公告获取了个体同意,并且满足信息使用与处理过程中的个体投诉,那么信息控制者就可以规避法律的风险[8]。至于信息控制者在个人信息的收集、储存、使用与流转过程中是否真正考虑到了个人信息泄露与滥用的风险,并不一定能够成为信息控制者的首要关注点②。一个例子就是欧盟《一般数据保护条例》实施后所带来的合规压力。在欧盟《一般数据保护条例》实施后,很多网站都以弹框的形式来公告各自的隐私公告,以此来获取个体的同意。但是正如上文所述,个体不可能有能力、时间、兴趣来真正阅读和理解如此多的隐私公告。当过多的隐私公告不断出现,其对于个体来说与其说提供了选择的机会,毋宁说造成了极大的困扰③。

此外,强化个体赋权可能导致个体无法获取有效服务、制定良好公共政策、实现合理信息流通。就企业而言,在缺乏有效个人信息的情形下,企业就不可能有效地为个体提供可能满足其需求的供给,个体则可能会因为缺乏推荐而付出更高的价格④。就政府而言,个人信息的合理收集与使用一直是良好治理的关键,缺乏个人信息与相关数据的汇集,政府就很难制定有效的公共政策,甚至可能会因为相关数据的缺乏而导致治理的失败⑤。就社会而言,个人信息的合理流通是一个社会正常运转的关键,缺乏个人信息的合理流通,社会就不可能进行有效交流,形成合理有效的社会规范[9]。在所有这些情形中,无条件地强化个体信息赋权无疑会给企业、政府与社会带来信息障碍。尤其是在引进某些新型权利时,例如"被遗忘权"等权利时,如果允许将此类权利绝对化,赋予个人以主张对所有信息控制者以删除其"过时、不相关"个人信息的权利⑥,那么此类赋权将有可能导致公共空间中信息的漏洞,不利于信息的合理流通⑦。

---

① 对此事件的描述,参见 [EB/OL]. [2019 - 02 - 15]. https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal.

② 当然从隐私保护的重视程度上,企业可能会受到一些正面的影响。参见:Peter P. Swire. The Surprising Virtues of the New Financial Privacy Law [J]. Minnesota Law Review, 2002,86(6):1263 - 1316.

③ Jack Schofield. what should I Do about All the GDPR Pop-ups on Websites? [EB/OL]. (2018 - 07 - 05) [2019 - 02 - 20]. https://www.theguardian.com/technology/askjack/2018/jul/05/what - should - i - do - about - all - the - gdpr - pop - ups - on - websites.

④ Bill Pryor. Protecting Privacy: Some First Principles, Remarks at the American Council of Life Insurers Privacy Symposium, July 11,2000. Washington, DC, at 4.

⑤ 已经有很多研究指出了信息在国家治理中的关键性角色。例如孔飞力教授的《叫魂》、黄仁宇教授的《万历十五年》,都指出了因为国家信息收集能力或"大数据"收集能力低下而导致的国家治理的失败。(参见:黄仁宇.万历十五年[M].上海:三联出版社,1997;孔飞力.叫魂[M].陈兼,刘昶,译.上海:上海三联书店,2012.)

⑥ 例如在"西班牙谷歌案"中,欧洲正义法院确立了个体以针对搜索引擎的被遗忘权。(参见:Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González (2014).)

⑦ 本文并非完全反对被遗忘权在某些场景下的行使,对此的具体分析,参见:丁晓东.被遗忘权的基本原理与场景化界定[J].清华法学,2018(6):94 - 107.

从基本原理的角度思考，强化个体信息赋权之所以存在以上种种问题，关键在于信息与科技时代，相关机构对个人信息的收集、储存与流通已经大大超出了普通公民的个体预期，一个普通公民个体已经很难对伴随信息流通的风险进行预判[10]。在这种背景下，公民个体并不一定总能很好地行使相关信息权利，对自身的隐私权益进行有效管理，当公民个体行使各种信息权利时，可能同时产生个人信息与隐私权益保护不足与保护过度的情况。个体可能会轻率地放弃某些权利，从而使得自身的隐私权益受损，就像很多“公告－选择”框架中所出现的情形那样。同时，在有的情形中，个体又会过度行使自身的某些权利，从而妨碍个人信息的合理流通与使用①。

当然，本文上述分析并不意味着对个体进行信息赋权就是错误或无效的②，当某些种类的权利建立在公民对于相关风险的合理认知之上时，特别是当此类信息赋权不会影响国家的公共政策与社会的信息合理流通时，此类情形下的信息赋权将能够帮助公民个体更好地进行隐私权益的自我管理，预判和防范有关风险[11]。例如赋予个体以信息访问权，赋予个体以对被收集的非公开个人信息的纠正权和删除权，这将有利于个体对于其个人信息有更好的知情权和风险管理的权利，确保其个人信息不被不合理地收集与流转。总之，个体信息的赋权应当以确保信息的合理流通为目标，应当兼顾个体对于其信息流通的预期与社会对于信息流通的预期[12]。

四、信息控制者责任的反思

公平信息实践的另一核心是对信息控制者——或者说信息收集者与处理者——施加责任。对这些责任进行重新分析，会发现并非所有责任都是合理的，特别是在大数据已经广泛运用的今天，有的责任甚至不太符合信息合理运用与保护的基本原理。

以“目的限定”原则为例，目的限定原则的基本要求在于个人信息的收集应当具有具体的、清晰的和正当的目的，即只能在信息收集时明确其收集目的，并且获得个人的授权，个人信息收集不能超出此边界。“目的限定”原则的这一规定在前大数据时代有其较强的合理性，因为在前大数据时代，信息或数据往往是孤立的，对于数据价值的运用往往通过抽样或单项数据的分析来完成。在这样的背景下，要求信息或数据收集限定于某个目的，既可以实现对个人信息或数据的分析价值，又可以避免信息收集者收集过多的个人数据。但在大数据时代，信息或数据的打通使用价值已经非常明显，个人信息的价值可能并不仅仅局限于个人，当海量的个人信息价值汇合，就完全可能实现之前难以想象的公共价值[13]。在大数据时代，如果严格按照“目的限定”原则来要求收集数据，那么信息或数据就会成为一个个孤岛，并不能集合起来发挥大数据的价值。

存在类似困境的还有“数据最小化”原则和“限期存储”原则，“数据最小化”原则要求个人信息处理应当是为了实现数据处理目的而适当的、相关的和必要的；“限期储存”原则要求个人信息或数据的储存时间不得超过实现其处理目的所必需的时间。但在大数据时代，个人信息或数据的价值恰巧在于

① 对于个人信息过度赋权可能同时存在的保护不足与过度保护，参见：丁晓东. 个人信息传统私法保护的困境与出路[J]. 法学研究，2018(6)：194－206.

② 对于以“个人信息”概念为基础保护大数据时代公民的隐私权益是否合适，可以进一步参见：Paul Ohm. Broken Promises of Privacy[J]. UCLA L. REV，2010，57(6)：1701－1778；Paul M. Schwartz & Daniel J. Solove. The PII Problem，Privacy and a New Concept of Personally Identifiable Information[J]. New York University Law Review，2011，86(6)：1814－1894.

数据的二次甚至是多次挖掘,而数据的二次或多次挖掘又依赖于数据的海量汇集与沉淀。通过对海量沉淀的个人信息的二次或多次使用,大数据可以发现隐藏在这些孤立的数据背后的商业价值与公共性价值。商业机构可以通过此类分析为消费者提供更好的服务,政府或公共机构则可以通过此类数据处理而制定更好的公共政策或开展研究①。

个人信息或数据的聚合使用与二次使用在很多例子中都有体现。其中一个例子就是谷歌对于季节性流感的预测。2009 年,全球出现了甲型 H1N1 流感的大范围流行,这使得美国公共卫生部门大为紧张,美国的公共卫生部门通过医院等部门所登记的信息对个人信息进行分析,但结果却不尽如人意。相反,在甲型 H1N1 流行前两周,谷歌就准确地预测了 H1N1 流感爆发的范围与传播的趋势,并且其预测性精准到了州。正如谷歌工程师在《自然》杂志所发表的论文所显示的,谷歌之所以能比美国公共卫生福利部门更为准确地进行预测,就在于谷歌具有海量的信息收集能力,具备了海量的信息沉淀,通过对此类信息——其中很大一部分是个人信息——的分析与挖掘,谷歌最终完成了公共卫生福利部门难以完成的任务[14]。

针对大数据时代个人信息保护的此类困境,大数据专家与信息隐私专家舍恩伯格有过分析,舍恩伯格指出,"大数据的价值不再单纯来源于它的基本用途,而更多源于它的二次利用"。这首先"颠覆了当下隐私保护法以个人为中心的思想:数据收集者必须告知个人,他们收集了哪些数据、作何用途,也必须在收集工作开始之前征得个人的同意"[15]197。其次,在大数据时代,"很多数据在收集的时候并无意用作其他用途,但最终却产生了很多创新性的用途",这就使得政府或企业无法告知个人尚未预想到的用途,如果政府或企业严格按照"目的限定"或"数据最小化"原则来获取个人同意或处理数据,那么这就"限制了大数据潜在价值的挖掘"[15]197-198。

如何既合理地使用个人信息,发挥大数据的价值与潜力,又保护个人信息在大数据时代不被滥用?舍恩伯格在其著作中提出了若干范式转换,其中之一即是"从个人许可到让数据使用者承担责任"。对于这一转变,上文已经部分提及,因为个体难以对个人信息流通的风险进行预判,因此以个体许可或个体同意为框架的隐私保护常常难以奏效。这里需要补充的是,从信息控制者责任的角度来看,需要强化信息控制者的风险防范规则,确立基于风险防范的个人信息使用规则。"对于一些危险性较大的项目,管理者必须设立规章,规定数据使用者应如何评估风险、如何规避或者减轻潜在伤害。"在这种基于风险预防与避免伤害的指引下,数据使用者与公民个体都能得到最大的利益保护:数据的使用者将"无须再取得个人的明确同意,就可以对个人数据进行二次利用。相反地,数据使用者也要为敷衍了事的评测和不达标准的保护措施承担法律责任,诸如强制执行、罚款甚至刑事处罚"[15]220-221。

综观公平信息实践的发展以及相关信息隐私法的发展,可以发现预防损害与预防风险的原则逐渐受到重视。例如 2004 年的 APEC 隐私框架就将预防损害作为公平信息实践的首要原则,强调个人信息的收集、储存与流转都必须考虑相应的风险,采取相应的预防措施。而《一般数据保护条例》则在相

① 本文并不反对对个人信息或数据设置期限储存或"生命周期",因为此类个人信息"生命周期"的设置将有利于避免数字化记忆的问题,在此本文只是反对对个人信息进行即时删除的要求。对于大数据时代个人信息限期储存的必要,参见:维克托·迈尔-舍恩伯格,肯尼斯·库克耶. 删除:大数据取舍之道[M]. 袁杰,译. 杭州:浙江人民出版社,2013.

关条文中规定了与风险相称的技术与组织措施①; 风险评估②、以及监管机构的风险监管责任③,将风险预防放在了更为突出的位置④。

五、迈向大数据时代的公平信息实践

通过对公平信息实践的介绍、归纳与反思,本文的基本结论已经较为明显: 这就是公平信息实践总体上为个人信息保护奠定了良好的制度框架,但公平信息实践的某些版本和某些基于公平信息实践的立法也存在不符合个人信息保护原理的情形,尤其可能不符合大数据时代个人信息的合理利用与保护。究其原因,这在于某些版本的公平信息实践走向了形式主义与异化的道路,将个人信息保护中的个体信息自决逻辑推导至极端,而且忽视了个人信息可能具有的流通价值与公共性价值。从这种个体主义的、静态的观点来看待个人信息保护,那么公平信息实践就可能既无法保护公民个体的个人信息,又不能合理使用与发挥个人信息的公共价值。

为了避免公平信息实践走向异化,公平信息实践有必要把自身从强化个体信息自觉与对个体信息的静态化保护中解放出来,在认可个体信息流通价值与公共性价值的前提下保护个人隐私权益与相关利益,消除相关风险。一方面,公平信息实践应当建立在个体的合理预期基础之上,有限度地赋予公民以相关信息权利,避免信息权利的泛化与极端化。另一方面,公平信息实践应当以促进信息的合理流通与使用,促进包括公民个体在内的公共利益为最终目标。同时,伴随着个人信息的收集、使用与流转的风险日益剧增和难以察觉,信息的收集者与处理者也应当承担更多的风险预防责任,而非仅仅致力于形式主义的合规。

基于以上分析,本文在此尝试提出一个更为符合大数据时代特征的公平信息实践版本:

个体合理预期: 个人信息的收集、处理与流转应当符合个体的合理预期,尤其是在不涉及公共利益的情形下,当个人信息的收集、处理与流转超出一个社会中正常理性个体的合理预期时,个人信息的收集者或处理者必须对个体进行显著告知,确保个体理解伴随此类收集与处理的风险,并且在此类情形中获得个体的明确授权⑤。

访问权、纠正权与删除权: 对于未进入公共领域的信息和不涉及公共利益的个人信息,公民个体对其信息具有访问权、纠正权与删除权。对于进入公共领域的信息和涉及公共利益的个人信息,公民个

① 第 32 条规定 "在考虑了最新水平、实施成本、处理的性质、处理的范围、处理的语境与目的之后,以及处理给自然人权利与自由带来的伤害可能性与严重性之后,控制者和处理者应当采取包括但不限于如下的适当技术与组织措施,以便保证和风险相称的安全水平。"

② 第 35 条规定 "当某种类型的处理——特别是适用新技术进行的处理——很可能会对自然人的权利与自由带来高风险时,在考虑了处理的性质、范围、语境与目的后,控制者应当在处理之前评估计划的处理进程对个人数据保护的影响。"

③ 第 36 条规定: 当监管机构认为,某些"预期的处理将违反本条例,特别是当控制者无法识别或减小风险,监管机构应当在收到咨询请求的八个星期以内向控制者以及——在适用的情况下——处理者提供书面建议",而且可以运用相应的权力进行应对。

④ 参见: 丁晓东. 什么是数据权利? ——从欧洲《一般数据保护条例》看数据隐私的保护[J]. 华东政法大学学报,2018(4):39-53.

⑤ "合理预期"的标准目前主要在美国的宪法类案件中被使用,但本文认为可以在公平信息实践中加以移植和借鉴。在"Katz v. United States, 389 U.S. 347, 360-61 (1967) 案"中,美国联邦最高法院认为,政府是否在搜查中侵犯了公民隐私,这取决于这种搜查是否违反了社会上一般人的合理预期。

体的访问权、纠正权与删除权将受到相关限制①。

合理使用与流通:个人信息的收集不应当妨碍社会信息的合理使用与合理流通,当个人信息的收集与使用超出个体合理预期但符合社会公共利益时,应当优先考虑社会公共利益,在考虑社会公共利益的前提下限定个人信息的收集与使用。

消费者利益与公共利益优先:个人信息的收集与利用应当以促进社会的整体利益为基础。商业领域的个人信息应当以促进服务的提升和更好满足消费者为目的,避免利用个人信息来无限度榨取消费者剩余;政府对于个人信息的利用应当以促进服务公民与提升公共政策制定为目的。

风险预防:个人信息的收集者与处理者应当采取恰当的措施来防范伴随个人信息收集、储存、处理与流转的风险。此类措施应当包括但不限于风险评估、风险预警、分类保护、泄露告知等措施②。

毫无疑问,本文所提出的公平信息实践版本仅仅是尝试性的,远非完美。但本文相信,这一版本的公平信息实践至少具有极为重要的理论与现实意义。从理论上看,个人信息保护在大数据时代面临着前所未有的挑战,如何兼顾个人信息的合理利用与保护,这是摆在所有法学研究者面前的一个难题。从现实层面来看,我国的个人信息立法也基本继承了公平信息实践的若干基本原则③。例如我国《网络安全法》对于个人信息的规定基本上确立了“告知 - 选择”框架④、目的限定原则⑤、删除权与更正权⑥、风险防范⑦等原则。未来我国的个人信息法立法,必定会受到公平信息实践的极大影响——如果不是完全继承的话⑧。在这种情形下,反思并发展公平信息实践,或许正当其时。ML

参考文献:

[1] Paul M. Schwartz. Privacy and Democracy in Cyberspace [J]. Vanderbilt Law Review,1999,52(6).

[2] Paul M. Schwartz, Daniel J. Solove. Reconciling Personal Information in the United States and European Union [J]. 102 California Law Review,2014,102(4):877 - 916.

[3] Daniel J. Solove, Woodrow Hartzog. The FTC and the New Common Law of Privacy [J]. Social Science Electronic Publishing, 2014,114(3):583 - 586.

① 对于个人信息所涉及到的公共领域问题,可以参见:Robert Post. Data Privacy and Dignitary Privacy: Google Spain, The Right To be Forgotten, and the Construction of the Public Shpere [J]. Duke Law Journal,2018.

② 本文所提出的公平信息实践版本更接近于有的学者所提出的公平信息实践版本,参见:Fred H. Cate。Privacy in the Information Age [M]. Brookings Institution Press,1997:370 - 373.

③ 其他一些标准则更是全盘继承了公平信息实践的若干原则,例如全国信息安全标准化技术委员会组织制定和归口管理的国家标准《信息安全技术 个人信息安全规范》。参见 [EB/OL]. [2019 - 03 - 01]. https://wemedia.ifeng.com/46709905/wemedia.shtml.

④ 《网络安全法》41 条第 1 款规定 “网络运营者收集、使用个人信息,应当遵循合法、正当、必要的原则,公开收集、使用规则,明示收集、使用信息的目的、方式和范围,并经被收集者同意。”

⑤ 《网络安全法》41 条第 2 款规定 “网络运营者不得收集与其提供的服务无关的个人信息,不得违反法律、行政法规的规定和双方的约定收集、使用个人信息,并应当依照法律、行政法规的规定和与用户的约定,处理其保存的个人信息。”

⑥ 《网络安全法》第 43 条规定 “个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的,有权要求网络运营者删除其个人信息;发现网络运营者收集、存储的其个人信息有错误的,有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。”

⑦ 《网络安全法》第 42 条第 2 款规定 “网络运营者应当采取技术措施和其他必要措施,确保其收集的个人信息安全,防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时,应当立即采取补救措施,按照规定及时告知用户并向有关主管部门报告。”

⑧ 我国在此领域的权威学者的建议稿已经反应了此种趋势,参见:周汉华. 中华人民共和国个人信息保护法(专家建议稿)及立法研究报告 [S]. 北京:法律出版社,2006.

[4] Joel R. Reidenberg. Resolving Conflicting International Data Privacy Rules in Cyberspace [J]. Stanford Law Review, 2000,52(5):1315 - 1371.

[5] Omri Ben - Shahar, Carl E. Schneider. The Failure of Mandated Disclosure [J]. Actual Problems of Economics and Law, 2017(2):170 - 198.

[6] 万方. 隐私政策中的告知同意原则及其异化 [J]. 法律科学,2019(2):61 - 68.

[7] Kent Walker. The Costs of Privacy [J]. Harvard Journal of Law & Public Policy,2001(25):87 - 112.

[8] Omri Ben - Shahar. Contracting Over Privacy: Introduction [J]. Journal of Legal Studies, 2016,45(2):1 - 12.

[9] Robert C. Post. The Social Foundations of Privacy: Community and the Self in the Common Law Tort [J]. California Law Review, 1989,77(5):957 - 1010.

[10] Daniel J. Solove. Introduction: Privacy Self - Management and the Consent Dilemma [J]. HARV. L. REV, 2013,126(7):1880 - 1903.

[11] Ari Ezra Waldman. Privacy as Trust: Sharing Personal Information in a Networked World [J]. U. Miami L. Rev, 2015,69(3):559 - 630.

[12] Helen Nissenbaum. Privacy in Context: Technology, Policy, and the Integrity of Social Life [M]. Stanford University Press, 2009:140 - 160.

[13] Andrew McAfee, Erik Brynjolfsson. Big Data: The Management Revolution [J]. Harvard Business Review,2012,90(10):60 - 66.

[14] Jeremy Ginsberg, Matthew H. Mohebbi. Rajan S. Patel, Lynnette Brammer, Mark Smolinski, Larry Brilliant. Detecting Influenza Epidemics Using Search Engine Query Data [J]. Nature,2008:1012 - 1014.

[15] 维克托·迈尔—舍恩伯格,肯尼斯·库克耶. 大数据时代:生活、工作与思维的大变革 [M]. 盛杨燕,周涛,译. 杭州:浙江人民出版社,2013.

On the Ideological Origin and Basic Principles of Legal Protection of Personal Information: An Analysis Based on "Fair Information Practices Principles"

DING Xiao-dong

(Law School of Renmin University of China, Beijing 100872, China)

Abstract: Fair information practice constitutes the ideological origin and basic framework of global personal information protection. Summarizing the evolution of fair information practice and the principles of fair information practice in different versions around the world, we can find that fair information practice establishes the path of empowering personal information and imposing the responsibility of information controllers. But strengthening personal information empowerment does not necessarily conform to the basic principles of personal information protection, and does not necessarily well protect individual privacy rights and interests. At the same time, imposing certain responsibilities on information controllers may not conform to the basic characteristics of big data, and can not properly use and protect personal information. This paper proposes a practical version of fair information in the era of big data, and advocates the adoption of limited individualism and dynamic personal information protection. This version of fair information practice emphasizes balancing individual expectations and social expectations in the collection, processing and circulation of personal information, and emphasizing the way to protect personal information by giving full play to the public value of personal information and risk prevention.

Key Words: fair information practice; personal information protection; big data; individualism; dynamic protection

本文责任编辑:龙大轩