中外法学 Peking University Law Journal
Vol.34, No.5(2022)pp.1143－1162

诚信原则:个人信息保护与利用平衡的信任路径

许 可*

摘 要 如何平衡个人信息保护与利用,是数字时代的核心议题之一。《个人信息保护法》在“合法、正当、必要原则”外增设“诚信原则”,开辟了“基于诚信的平衡路径”。该路径有效融合“场景机制”,弥补“比例机制”和“风险机制”的立法缺憾,化解了数字信任困境。作为一般条款,诚信原则可具体化为三类次级机制:“补充处理者义务的诚信机制”对处理者苛以不得欺诈、操纵以及公平对待个体的概括义务;“限制信息主体权利的诚信机制”禁止个体滥用其在信息处理活动中的权利,损害他人合法权益;“平衡信息主体与处理者利益的诚信机制”一方面要求国家机关处理者承担忠实、勤勉的信义义务,另一方面引入正当利益条款,以调和私主体处理者和个体的利益冲突。作为授予自由裁量权的空白委任状,诚信原则亦要求执法者、司法者秉持诚信,以个人信息保护与利用平衡为宗旨,妥当解释法律规范、填补法律漏洞,最终铸就原则与规则相互融贯的个人信息柔性法治秩序。

关 键 词 个人信息 诚实信用 数字信任

引 言

《个人信息保护法》(下称“《个保法》”)第5条在《全国人民代表大会常务委员会关于加强网络信息保护的决定》第2条“合法、正当、必要原则”的基础上,增设“诚信原则”作为个人信息处理的新原则。将该原则理解为“秉持诚实、恪守信诺,不得通过误导、欺诈、胁迫等方式处理个人信息”,是目前的主流观点。不过,这种基于语义说的惯常认识可能小觑了“诚信”,也忽略

* 对外经济贸易大学法学院副教授。本文系国家社会科学基金重大项目“民法在建设职责明确、依法行政的政府治理体系中的作用研究”(项目编号:21ZDA050)的阶段性成果。

了“原则”的体系效用。就前者论，作为时代变迁之镜像，诚信的内涵历久弥新、日益丰赡，已由当事人的行为准则演化为各方利益平衡的一般条款；〔1〕就后者论，原则既承载了一部法律所追求的抽象精神，也是其内在体系的外显，并藉由具体化整合法律规则、标准和制度，以实现法律的融贯性和自创生性。出于这一理解，本文试图从《个保法》第 1 条“保护个人信息权益与促进个人信息合理利用”之立法宗旨出发，激活诚信原则所蕴含的利益平衡原理，提出富有价值追求和规则弹性的“基于诚信的平衡机制”。

作为对个人信息之上多元主体、多元利益的因应，个人信息保护与利用的平衡已成为各国念兹在兹的制度关切。在比较法视野中，相关机制可分为“基于比例的平衡”“基于风险的平衡”“基于场景的平衡”和“基于市场的平衡”。其中，“基于比例的平衡”系通过检验手段和目的之间合理性，适当限制个人权益，为个人信息利用留下空间；“基于风险的平衡”旨在识别和评估个人信息处理风险，设置与之相应的保护水平与规则；“基于场景的平衡”则打破了个人信息受个人控制的迷思，将关注点转向个人信息在不同场景中的合理流动；最后，“基于市场的平衡”以个人信息财产化和经济激励为基，推动个体和处理者共享个人信息收益，实现双方共赢。以此为棱镜，我国既有研究或多或少落入其间：王锡锌、彭錞和程啸等均主张“基于比例的平衡”；〔2〕倡导“基于风险的平衡”的如张新宝、梅夏英、周汉华等；〔3〕“基于场景的平衡”以丁晓东为代表；〔4〕刘德良等则支持“基于市场的平衡”。〔5〕

与意见纷呈的研究不同，《个保法》仅引入基于比例和基于风险的平衡机制。这是因为，我国沿袭从规范而非事实出发的整体规制理路，与场景机制难以兼容；同时，我国不承认个人信息的财产权益，〔6〕自然不采市场机制。其中，比例机制集中体现在《个保法》第 13 条，其融个人权益、当事人共同利益、公共利益于一炉，并通过“法律、行政法规规定”的兜底条款保持了平衡开放性。风险机制首先表现为“一般个人信息”和“敏感个人信息”区分保护；其次要求处理者根据处理目的、方式、个人信息种类以及对个人权益影响等，采取相应保障措施；最后，该机制还反映在对高风险处理活动的特别规制。尽管《个保法》总体上建立了个人信息保护与利用的平衡机制，但由于场景机制和市场机制的欠缺，相关规则仍不免失之刚性和僵化。况且，即便是比例机制和风险机制，其运用也未臻完善，可能引发保护过当或利用不足的问题。举其荦荦大者，第 13 条未规定“正当利

〔1〕 参见徐国栋：“诚实信用原则的概念及其历史沿革”，《法学研究》1989 年第 4 期，第 54 页。

〔2〕 参见王锡锌、彭錞：“个人信息保护法律体系的宪法基础”，《清华法学》2021 年第 3 期，第 23－24 页；程啸：“论我国民法典中的个人信息合理使用制度”，《中外法学》2020 年第 4 期，第 1008 页。

〔3〕 参见张新宝、葛鑫：《个人信息保护法（专家建议稿）及立法理由书》，中国人民大学出版社 2021 年版，第 6 页；梅夏英：“社会风险控制抑或个人权益保护——理解个人信息保护法的两个维度”，《环球法律评论》2022 年第 1 期，第 16 页；周汉华：“探索激励相容的个人数据治理之道——中国个人信息保护法的立法方向”，《法学研究》2018 年第 2 期，第 3－23 页。

〔4〕 参见丁晓东：《个人信息保护：原理与实践》，法律出版社 2021 年版，第 86－87 页。

〔5〕 参见刘德良：“个人信息的财产权保护”，《法学研究》2007 年第 3 期，第 80－91 页。

〔6〕 参见张新宝：“论个人信息权益的构造”，《中外法学》2021 年第 5 期，第 1144 页。

益”(legitimate interest)条款,不但使利益平衡遗漏关键一环,也令公开信息的合理使用缺乏规范基础和操作指引。又如,第 6 条要求处理个人信息应“采取对个人权益影响最小的方式”。显然,该条只考虑处理的负面损害,而没有将处理的正面收益一并衡量,实质上陷入了行政法比例原则必要性审查的误区,有悖于净收益最大、社会福祉最优的卡尔多—希克斯效率标准。〔7〕再如,在“个人信息—保护”和“匿名化信息—不保护”的二元格局下,“去标识化”仅被第 51 条视为一项安全措施,并未依风险变化而放松对去标识化信息的规制,不仅削弱了处理者去标识化和研发隐私计算的动力,更极大限制了个人信息共享的空间。

正因上述种种窒碍,诚信原则的意义才益发鲜明。放宽视野看,个人信息保护与利用的冲突潜藏着“数字信任危机”。信息流动的基石是信任,〔8〕保护与利用的失衡恰恰在于失去信任:个人恐惧其信息被处理者反过来侵害自身,处理者顾虑个人滥用其权利,国家则担忧个人和处理者罔顾公共利益。这一多边信任困境有待通过刚柔并济的机制来弥合。诚信原则在道德上以“信”为要素,在法律上以“衡平”为方法,是激励施信人与受信人合作互信,调和个人、企业、国家利益的重要信任机制。〔9〕一如诚信原则,“基于诚信的平衡机制”也应遵循“案例—案例群—类型化”的适用路径,〔10〕一方面立足于实际纠纷中原则具体化,汲取场景机制中打破统一保护、寻找“场景相关规范”的实用主义理念;另一方面坚持成文法传统,尽力嵌入、协调和弥合法律规范之间的罅隙,为司法者、执法者提供相对安定的法律规范,最终铸就以“规则—原则模式”为基的个人信息保护柔性法治秩序。〔11〕立基于此,下文将以《个保法》第五、四、二章为框架,以实务案例为素材,分别从“充实处理者义务”“限制个人信息主体权利”和“平衡个人信息处理中各方利益”三方面展开,以调适个人信息主体与处理者之权利义务,促成个人信息保护与利用的再平衡。

一、补充个人信息处理者义务的诚信机制

处理者是诚信原则的首要适用对象。除《个保法》第 5 条外,第 18 条第 2 款“及时告知义务”和第 47 条第 1 款“个人信息主动删除义务”,可谓处理者依诚信原则而生的附随义务。〔12〕然而,作为统领个人信息生命周期和各项处理活动的基本原则,处理者诚信义务尚缺乏全面梳理。在此,我们将其类型化为侧重于行为伦理的“内在诚信义务(善意与信守诺言)”和侧重于

〔7〕 参见戴昕、张永健:“比例原则还是成本收益分析——法学方法的批判性重构”,《中外法学》2018 年第 6 期,第 1529－1531 页。

〔8〕 参见谢尧雯:“网络平台差别化定价的规制路径选择”,《行政法学研究》2021 年第 5 期,第 27 页。

〔9〕 参见徐化耿:“论私法中的信任机制”,《法学家》2017 年第 4 期,第 35 页。

〔10〕 参见刘亚东:“民法概括条款适用的方法论”,《政治与法律》2019 年第 12 期,第 91 页。

〔11〕 参见雷磊:“适于法治的法律体系模式”,《法学研究》2015 年第 5 期,第 20 页。

〔12〕 参见张新宝:“个人信息处理的基本原则”,《中国法律评论》2021 年第 5 期,第 18－27 页。

客观评价的“外在诚信义务(合理与公平)”,通过更细致的“排除法”,〔13〕胪列种种不诚信行为,以便从反面划定其边界。

(一)处理者的内在诚信义务:不得欺诈和操纵

“守信不欺”是诚信的文义解释,也是其伦理性之所系。但法律诚信绝非道德诚信的翻版,如果说后者建立在对命令我们做好人之戒条的服从上,那么前者就建立在对未违反法律规范行事、未实施不义行为的确信上。〔14〕循此,处理者不得利用任何欺诈、误导、胁迫等方式致使个体陷入意志不自由状态,不得从事任何违反事先告知和承诺的处理活动。

1.违反个人信息保护承诺

处理者违反对信息主体的承诺是最典型的不诚信行为。这里的“承诺”不但包括了隐私政策或个人信息处理规则(合称“个人信息处理文件”),还包括了企业营销材料、操作手册、遵守自律性标准、最佳实践的声明以及网站 APP 的隐私设置、弹窗等技术设计。对承诺的宽泛界定,有助于从处理者义务施加而非个人权利赋予的角度强化保障,并化解了与处理者无关的第三方欺诈难题。〔15〕从美国判例观察,相关承诺包括但不限于:①承诺保密或避免向第三方披露信息;②承诺个人信息使用限于声明的目的;③承诺个人信息安全;④承诺个人信息保持匿名;⑤承诺个人信息不在破产程序中转移;⑥承诺维护和实施内部的保障措施和员工培训。〔16〕此外,“不作为”也可能构成欺诈,例如在个人信息处理文件中遗漏重要的或可能带来风险的处理场景。

2.个人信息处理的告知不充分

处理者的告知义务不止是知情权的当然之义,也是个人享有其他权利的前提。因此,《个保法》要求处理者真实、准确、完整地告知个人信息处理的各项事项(第 17 条),且只有在极其有限的情形下才能免于告知(第 18 条)。鉴于告知的关键地位,各国均将不充分告知作为重要的背信行为。在西尔斯案中,美国联邦贸易委员会(FTC)指出,尽管西尔斯公司在冗长的许可协议中披露了软件一直在后台运行并将跟踪信息,但其描述过于模糊并存在遗漏,具有欺骗性。在谷歌案中,法国国家信息技术和自由委员会认定,根据《通用数据保护条例》(General Data Protection Regulation,下称“GDPR”)第 12、13 条下的“透明度”义务,谷歌必须采用“简洁透明,易懂且易于获取的形式、清晰明了的语言”告知用户处理其数据的信息,但谷歌向用户提供的信息是“碎片化”的,不但分散在各个文件中,还必须额外激活按键和链接。〔17〕这种挤

〔13〕 See Robert Summers William McRoberts and Arthur Goodhart, “The Conceptualization of Good Faith in American Contract Law ,” *Essays in Legal Theory*, *Law and Philosophy Library*, Vol. 46, 2000, pp. 299－319.

〔14〕 参见徐国栋:“诚实信用原则二题”,《法学研究》2002 年第 4 期,第 76 页。

〔15〕 See FTC v. Accusearch Inc., 570 F.3d 1187, 1201 (10th Cir. 2009).

〔16〕 See Daniel J. Solove and Woodrow Hartzog, “The FTC and the New Common Law of Privacy,” *Columbia Law Review*, Vol. 114, 2014, pp. 629－630.

〔17〕 See Google Inc v. Commision nationale de l’informatique et des libertés (CNIL), C－507/17, 2019.

牙膏的设置,使用户必须多次点击后才能获得必要信息,并不得不再次整合、比较各项信息,方能理解处理内容及特定后果。在 WhatsApp 2.25 亿欧元处罚案中,爱尔兰数据保护局认定 WhatsApp 在隐私政策、服务协议、合法性基础告知、答问文档中用相似表述告知实则不同的内容,使用户难以发现其差异之处。〔18〕 无独有偶,中国企业的告知也常常隐藏在重重叠叠的文件之中。例如,为了找到关闭微信朋友圈个性化广告的信息,用户至少要经过 13 个步骤、点击 16 次,才能穿过"文山"找到按钮,不仅如此,即使用户选择关闭,其有效期也只有六个月。

3.其他一般性欺诈行为

除上列情形外,FTC 基于个人信息保护经验而发展出的"一般性欺诈行为规则",可作为查遗补漏的兜底条款。〔19〕 一般性欺诈行为的要素构成有三:一是存在可能误导用户的陈述、不作为或其他行为;二是从一个理性的用户角度出发去解释上述行为;三是上述行为对于用户权益产生了实质影响。〔20〕 显然,该行为类型难以穷尽,但至少包括了两种场景:其一,虚构身份或附属关系来获取个人信息。譬如,冒充账户持有人致电财务机构,从而诱导金融机构提供个人财务信息,或者虚构其与银行的关系,诱使用户提供信息,并声称用于验证。〔21〕 其二,虚构个人信息收集的必要性,如声称债务催收或反欺诈活动。在 Aaron 案中,FTC 认定在先租再买的电脑上弹出信息,要求拖欠费用的客户提供个人信息,亦构成欺诈。〔22〕

4. 操纵个人选择

《个保法》第 5 条将"误导、欺诈、胁迫"并列。其中,"误导"属于广义的欺诈,与此不同,"胁迫"是直接指向个人的强力干涉。质言之,胁迫系胁迫人采取非法方式或基于非法目的,告知被胁迫人将发生不利后果,被胁迫人因之心生恐惧,做出有悖真实意思的表示。〔23〕 但实践中,处理者以胁迫方式取得同意的情形甚为罕见。即使在被广泛诟病的"接受或离开"场景中,也因其手段不违法(提供合同条款)和目的不违法(处理个人信息),而无法归为胁迫。或出于这一考虑,《移动互联网应用程序信息服务管理规定》《移动互联网应用程序个人信息保护管理暂行规定(征求意见稿)》均舍"胁迫"而用"强制",要求处理者"不得以任何理由强制要求用户同意个人信息处理行为""不应强制要求用户一揽子同意打开多个系统权限""不得强制要求用户同意超范围或者与服务场景无关的个人信息处理行为"。然而,法律上强制一般限于"物理强制"(如暴力)或"公权力强制"(如执法),其核心是对当事人意思的彻底排除,这与移动 APP 收集个人信息的方式凿枘不投。其实,处理者令信息主体违背意愿而同意处理,并不限于胁迫或强制。本文尝试着从诚信原则出发,用"操纵"替代"胁迫和强制",以契合处理者基于"网络

〔18〕 See In the matter of WhatsApp Ireland Limited (DPC Inquiry Reference: IN－18－12－2), 2022.

〔19〕 See Solove and Hartzog, supra note 16, pp. 630－633.

〔20〕 See Chris Jay Hoofnagle, *Federal Trade Commission Privacy Law and Policy*, Cambridge: University Press, 2016, pp. 123－126.

〔21〕 See FTC v. Assail, Inc., No. W03CA007 (W.D. Tex. 2004).

〔22〕 See In the Matter of Aaron's, Inc., FTC File No. 122 3256, 2013.

〔23〕 参见张新宝:《中华人民共和国民法典总则·释义》,中国人民大学出版社 2020 年版,第 309－311 页。

架构”对个体行为能力和范围的影响力。〔24〕

这里的“操纵”,是指通过互联网界面设计影响和心理操纵个人行为,使其难以表达其实际偏好,进而导致其做出非意欲的、潜在有害的决定。在比较法上,“操纵”与“暗黑模式”(dark patterns)密不可分,后者意指处理者通过结构、功能或操作方式,有目的地颠覆、损害用户自主性、选择权或决定能力的交互界面设计。〔25〕由于其对用户的潜在威胁,暗黑模式被美国《加州消费者隐私法》《科罗拉多州隐私法》以及欧盟《数字服务法》和《数据法案》所禁止。暗黑模式日新月异,综合欧盟和美国的实证研究,〔26〕可将既有模式梳理如下:①超载:向用户提供大量信息、请求、选项和可能性,以阻止其在个人信息保护方面做出选择;②预设:向用户提供最具侵入性的个人信息处理配置,使用户总是更倾向于保留预先存在的设置。③阻碍:用户希望获取信息、以更严格方式决定其个人信息处理或者注销服务时遭遇技术阻碍,使其难以或不可能采取必要的行动来实现目标;④变化无常:通过故意不稳定和不一致的界面设计,使用户难以理解管理个人信息的设置或命令的确切用途;⑤强迫行动,如通过柔性的反复弹窗和刚性的强迫注册来实现其目标;⑥情绪操纵:激发用户情绪以影响其选择,例如使拒绝的确认框显得愚蠢;⑦视觉操纵:通过字体、大小、颜色、明暗等专门视觉设计诱导用户决策。总之,无论何种设计,暗黑模式都接近于“胁迫”,因为用户在有能力选择替代方案的情形下,将不会做出之前的决定。

(二)个人信息处理者的外在诚信义务:公平对待

“诚信就是公平交易。”〔27〕GDPR 第 5(1)(a)条将“公平”(Fair)作为个人信息处理的基本原则之一,强调处理者不得通过不公平手段处理个人信息。〔28〕有趣的是,德国、法国、西班牙将上述 Fair 翻译为“诚信”(Treu und Glaube)或“平等”(equitability),意大利、瑞典则翻译为“正确”(correctness),三者均根植于拉丁文“bona fide”,即“诚实信用”。〔29〕可见,各国殊途共归,违反诚信原则,多导致客观上显失公平的结果;而显失公平的行为,亦无不违背诚信原则。〔30〕据此,处理者的如下行为可视为有悖于外在诚信。

---

〔24〕 参见胡凌:“论赛博空间的架构及其法律意蕴”,《东方法学》2018 年第 3 期,第 89－90 页。

〔25〕 See The European Consumer Organisation, “Dark Patterns” and the EU Consumer Law Acquis Recommendations for Better Enforcement and Reform, 2022, pp. 4－5.

〔26〕 See The European Data Protection Board, Guidelines 3/2022 on Dark Patterns in Social Media Platform Interfaces: How To Recognise and Avoid Them, 2022; Jamie Luguri and Lior Jacob Strahilevitz, “Shining a Light on Dark Patterns,” *Journal of Legal Analysis*, Vol. 13, No. 1, 2021, pp. 43－109.

〔27〕 徐国栋:《民法基本原则解释:诚信原则的历史、实务、法理研究(再造版)》,北京大学出版社 2012 年版,第 211 页。

〔28〕 See Christopher Kuner, Lee A. Bygrave and Christopher Docksey (eds.), *The EU General Data Protection Regulation: A Commentary*, New York: Oxford University Press, 2020, p. 314.

〔29〕 See Gianclaudio Malgieri, “The Concept of Fairness in the GDPR: A Linguistic and Contextual Interpretation,” *In Proceedings of FAT* 20, 2020, p. 14.

〔30〕 参见邱聪智:《民法总则(下)》,台湾三民书局 2011 年版,第 475 页。

1.不公平的个人信息条款

GDPR 序言第 42 条明确规定个人信息处理规则不得包含“不公平条款”。何为“不公平条款”?作为处理者事先拟定、用户无从影响的格式条款,其公平与否可从《民法典》第 497 条来判断。一方面,如处理者不合理地免除、限制自身义务(如第五章下“个人信息安全保障法定义务”)和责任(如第 69 条下“个人信息损害赔偿责任”),令双方权利义务严重失衡,即构成不公平条款。进而言之,若处理者有意不作出安全承诺,也可能被认定为“不公平处理”。在 Rental Research Servs 案中,FTC 声称,尽管双方未就数据安全达成约定,但被告没有采用合理、适当的措施保护其收集的个人信息,未核实、验证个人信息接收方的身份和资格,即为“不公平行为”。〔31〕

另一方面,若处理者恣意追求一己之私,而自始未兼顾个人利益,甚至不合理地限制、剥夺个人的主要权利,也属典型的不公平条款。这里的“主要权利”限于《个保法》第 45 条到 48 条的诸权利。在 Slovakia 案中,欧洲人权法院指出,个人有权查阅、复制其医疗信息,对该权利的剥夺构成了“不公平处理”。〔32〕与上述权利有着微妙差异的是第 44 条下的决定权。鉴于这一抽象权利只能经由解释补充具体权利或转化为处理规则予以适用,其无需诉诸不公平条款的保护。同时,这里的“权利限制”应达到实质性、压迫性的程度,造成严重的利益减损,且无其他更重要利益予以权衡。作为相对性权利,基于市场的个人信息权益克减并非一概禁止,假设某一条款虽妨碍个人利益,但却因此带来其他较高或相等之利益,难谓不公平。〔33〕譬如,处理者发送的个性化广告,是发现和触达特定人群,满足细分领域消费需求的重要途径,不但降低了交易成本,而且加速了产品细分的创新与迭代,是互联网长尾经济的要义所在。就此而言,法律将不公平的个人信息处理定为非法,并不意味着处理者不能利用个人信息开展正当的商业活动。〔34〕

2.个人信息条款的恣意变更

诚信原则禁止反复无常的行为,防止当事人在其陈述或行为已经使他方产生合理信赖的情况下,单方实施改变他方法律地位的行为。实践中,个人权益的具体内容多由个人信息处理文件所形塑,处理者能否以及如何变更其中的个人信息条款成为关键问题。《个保法》最终稿将一审稿第 14 条“自愿、明确作出意思表示”中的“意思表示”删除,彰显了将“个人同意”排除在“法律行为”之外的立法意旨,〔35〕这亦被第 31 条第 1 款的“同意能力”和第 15 条第 1 款“同意撤回”所印证。因而,个人针对个人信息处理文件作出的同意,并非合同法下的承诺,个人信息条款的修改亦无需以《民法典》第 543 条下“双方协商一致”为前提,处理者可单方为之。但是,这并不意味着个人信息条款能被随意变更,相反,诚信原则对处理者施加了双重限制:在程

〔31〕 See United States v. Rental Research Servs.Inc., FTC File No. 072 3228 (D. Minn. Mar. 5, 2009).

〔32〕 See ECHR, K.H. and Others v. Slovakia, No.32881/04, 2009.

〔33〕 参见贺栩栩:“《合同法》第 40 条后段(格式条款效力审查)评注”,《法学家》2018 年第 6 期,第 183 页。

〔34〕 See Jack M. Balkin, “The Fiduciary Model of Privacy,” *Harvard Law Review Forum*, Vol. 134, No. 1, 2020, pp. 11—33.

〔35〕 参见杨合庆主编:《中华人民共和国个人信息保护法释义》,法律出版社 2022 年版,第 54 页。

序层面，对个人信息条款作出不利于个人的修改时，应在其官方网站面向社会公开征求意见，确保用户便捷、充分地表达意见，同时应以易于访问的方式公布意见采纳情况，说明未采纳理由；在实质层面，如处理者在之前个人信息处理文件中就特定处理方式作出过承诺（如不向第三方提供），则后续的变更将构成不公平处理，将修改后的个人信息条款溯及既往地适用于根据原有文件收集的个人信息，亦难言公平。〔36〕

3.不公平的自动化决策

从商品推荐到健康码赋码，基于个人信息的自动化决策被广泛应用在教育、就业、信用、贷款、保险、广告、医疗、治安、司法程序等领域，并对个人权益造成重大影响。《个保法》第24条第1款对自动化决策的规制主要体现为“决策透明度、结果公平和个人公平”上，而忽略了“过程公平和群组公平”，有待诚信原则填补。具体而言，在自动化决策算法设计阶段，处理者应秉持善意，贯彻多元化、公平公正及包容理念，辨识恶意偏见，并积极预防因数据挖掘、数据聚合而出现无意的歧视，禁止以区分、排斥、限制、偏向、隔离特定群体为目的的算法设计。当存在侵权之虞的算法部署实施时，处理者负有开展算法审计并向公众说明算法目的和基本逻辑的义务，并为可能受影响的社会群体、外部专家参与检测、审查提供渠道和便利。在自动化决策过程中，除取得个人单独同意并充分必要外，处理者不得使用对个人人格、身份至关重要的特性信息，如民族、宗教、国籍、社会出身、外貌、血统、性身份、性取向、年龄、残疾情况、健康状况等。鉴于自动化决策会系统性遗漏生活在大数据边缘的人群（如老人、低收入人士），处理者应适时调整算法策略、增加数据集矫正其程序的不公平。〔37〕

二、限制个人信息主体权利的诚信机制

尽管《个保法》第5条并未明确将个人信息主体纳入，但诚信原则君临各法域、适用于一切法律关系，个人作为民事主体，理应依据《民法典》第7条，在个人信息处理活动中遵循诚信原则，〔38〕这亦是《个保法》在民事关系领域作为《民法典》特别法的题中之意。不过，与作为义务承担者的处理者迥异，个人主要以“权利主体”的面貌出现，诚信原则因而具体化为《民法典》第132条的“禁止权利滥用”规范，即个人不得滥用其在信息处理活动中的权利，损害国家利益、公共利益或他人合法权益。《网络数据安全管理条例（征求意见稿）》第23条特别将“合理”作为个人提出各项权利请求的条件，可作佐证。

权利滥用的认定存在着主观标准和客观标准的分野。《最高人民法院关于适用〈中华人民共和国民法典〉总则编若干问题的解释》第3条采综合标准，以期回应现代社会日趋多样的权

〔36〕 See In re Gateway Learning Corp, 138 F.T.C. 443, 470, 2004.

〔37〕 See Solon Barocas and Andrew D. Selbst, “Big Data's Disparate Impact,” *California Law Review*, Vol. 104, N0. 3, 2016, pp. 715－720.

〔38〕 欧洲学者认为GDPR的“公平原则”亦适用于数据主体，See Daniel-Mihail Sandru, “The Fairness Principle in Personal Data Processing,” *Law Review*, Vol. X, No. 2, 2019, p. 66.

利滥用形态。基于此,本文将个人权利滥用类型化为:①权利行使有悖权利本旨:任何主观权利均体现着客观法的任务并最终实现其目的,若个人信息权利行使的对象、方式、内容、时间与权利设定的社会性功能相冲突,即构成权利滥用;〔39〕②恶意行使权利:以损害国家利益、公共利益、他人合法权益为主要目的行使个人信息权利,此为权利滥用之原初含义;③推定的权利恶意行使:在个人恶意难以确定时,可通过各方利益的比较推断其主观意图,〔40〕若"于己无益,于人有害"或"利己有限,损人甚大",可认定为恶意,此为权利社会化之基本内涵。鉴于权利滥用规范的适用有赖于"决疑法"的类案积累,这里将以《个保法》第四章为脉络,重点检视总括性权利"个人决定权"、基础性权利"个人信息查阅复制权"和创新性权利"个人信息可转移权"的行使边界。

(一)个人决定权的滥用

1.有悖于个人决定权本旨的权利行使

《个保法》第44条在《民法典》第1037条基础上抽象出"个人决定权",成为统领各项具体权利的概括性权利。论者多以"个人信息自决权"作为该权利的法理渊源,实属误把他乡作故乡。发轫于德国1983年"人口普查案"的"个人信息自决权",意指个人对信息拥有决定在何种范围内、于何时、向何人、以何种方式加以揭露或使用的自主权。这与我国个人决定权存在显著差异。就权利对象而言,自决权是指向"个人信息"的权利,而决定权则是指向"个人信息处理活动"的权利。个人信息之上的支配权是自决权的核心,但正如批评者所洞见,个人信息是人类行动的产物和前提,所谓对自己信息的支配,其实是对他人行为的支配,因而其无法归属于任何人。〔41〕恰恰是认识到自决权窒碍难行,立法者才将个人信息处理活动作为决定权的对象,其上承知情权,下启具体权利,维护人的主体地位和人格自由发展,避免个人沦为他人操纵的客体。就权利内容而言,自决权强调个人对其信息主动性管控,而决定权则强调个人对处理者处理活动的选择处理权、干预处理权、限制处理权、拒绝处理权。究其实质,其并非个人信息的管理机制,而是为矫正个人与处理者间关系扭曲,针对处理活动给其人格或财产带来危险的防御机制。〔42〕

从上述理解出发,以下情形可能构成个人决定权的滥用:①个人背离个人尊严、人身财产安全以及通信自由和通信秘密之目的而作出决定,〔43〕尤其是以金钱为对价出售、许可他人使用个人信息。《民法典》第993条将许可使用的客体限定在"姓名、名称、肖像"等人格要素,排除了个人信息的商业化使用,从而与个人信息权益奠基于人格权而非财产权的立法一脉相承。〔44〕当前,有观点主张个人以数据来源者的身份参与数据价值分配。其不但未把握个人

〔39〕 参见林诚二:《民法总则》(下册),法律出版社2008年版,第583页。

〔40〕 刘权:"权利滥用、权利边界与比例原则",《法制与社会发展》2021年第3期,第48页。

〔41〕 参见杨芳:"个人信息自决权理论及其检讨——兼论个人信息保护法之保护客体",《比较法研究》2015年第6期,第23-25页。

〔42〕 参见王锡锌:"国家保护视野中的个人信息权利束",《中国社会科学》2021年第11期,第132-133页。

〔43〕 参见张新宝,见前注〔6〕,第1149-1152页。

〔44〕 参见程啸:"论个人信息处理中的个人同意",《环球法律评论》2021年第6期,第46页。

信息权益(人格权)和数据权益(财产权)的区隔,更是对个人决定权的重大误读。②个人对其信息行使排他权和支配权,要求处理者按照其意志处理个人信息。《互联网信息服务算法推荐管理规定(征求意见稿)》第 15 条曾规定:"算法推荐服务提供者应当向用户提供选择、修改或者删除用于算法推荐服务的用户标签的功能",实质上赋予了用户对其信息的支配权,显然已超越决定权的边界。

2.恶意行使个人决定权

人是社会关系的总和,个人信息同样如此。个人就其信息的决定令他人、社会、国家遭至不利影响的情形多有。为避免过分限制个人权利,权利不得滥用规范并非一概是禁止个人信息主体损害其他各方,而是禁止其"故意损害"。

①出于故意损害他人的动机,就个人信息处理作出决定。"信息外部性"理论提醒我们,个人决定往往会给他人带来负外部性。这是因为,人们的信息将有助于处理者推断出他们朋友、同学或具有相近身份特征的人的信息。数据分析表明,同性恋男性的同性恋朋友比异性恋男性多出一定比例,处理者得以根据社交媒体用户朋友的性取向来预测本人的性取向。〔45〕一个更直接的例子是反映个人、血亲和种群生物特性的基因信息。〔46〕个人对其遗传疾病信息的披露使人联系到本人的后代、家族,甚或联系到其种族,以至于造成基因弱势群体。当个人明知其决定行为将直接导致他人受损,并有意促成时,则构成权利滥用。②出于故意损害社会、国家利益的动机,就个人信息处理作出决定。巨量敏感个人信息的汇聚可能转化为影响国家安全的重要数据,产生广泛的数据污染,〔47〕单一个人信息在特定条件下也能引发风险,"深度伪造"(deepfake)便是典型例证。作为"deep learning"和"fake"的合成词,深度伪造意指利用人工智能实现图像、视频、音频的生成或修改,达到信息内容以假乱真的效果。尽管深度伪造在教育、艺术、娱乐产业中潜力无限,但也侵蚀着公众对机构和媒体的信任,加剧社会分裂。深度伪造离不开个人信息的"饲喂",当个人决定将信息提供给深度伪造应用时,所威胁的并不是个人本身,而是社会系统,若个人有意使之生成虚假新闻,后果更不堪设想。对此,除《互联网信息服务深度合成管理规定(征求意见稿)》的公法规制外,私法上的权利滥用规范不失为更柔性的治理路径。

3.推定的恶意行使个人决定权

个人决定权恶意行使以"故意损害他人为目的"为主观要件,甚为严格,有必要通过利益衡量予以客观化。主观要件的放松应以客观对象的明确为代价,因而其适用应限定于攸关他人利益的"互赖个人信息"(interdependent personal information),即数人因某种关系或事件而

〔45〕 See Jay Pil Choi, Doh-Shin Jeon and Byung-Cheol Kim, "Privacy and Personal Data Collection with Information Externalities," *Journal of Public Economics*, Vol. 173, 2019, p. 116.

〔46〕 See Sheri Alpert, "Protecting Medical Privacy: Challenges in the Age of Genetic Information," *Journal of Social Issues*, Vol. 2, 2003, p. 98.

〔47〕 See Omri Ben-Shahar, "Data Pollution," *Journal of Legal Analysis*, Vol. 11, 2019, pp. 104—159.

形成、可识别或关联数人、不可分割的个人信息。〔48〕它具体表现为:①共同个人信息,即基于家族、血缘、婚姻以及特殊亲密关系(如情侣关系)等"共同关系"而形成的个人信息;②网络化个人信息:即基于个人与他人日常交往而形成的个人信息,如通信信息、社交平台互动信息(点赞、评论)、人际关系信息(如好友关系链)等;③群体个人信息,即数人基于时间、(虚拟)空间、事件的连接而形成的个人信息,如社交平台群组内信息、记录多人影像、声音的照片、视频和音频文件等。从钱钟书书信手稿拍卖案,到 Facebook 用户将 8000 多万名好友信息披露给剑桥分析公司,均揭示出互赖个人信息中权利冲突的普遍性。从决定权行使的角度,信息共生性使个人对互赖个人信息的决定,不可避免地影响到"被动"决定的相关方。面对争议,法律回应充满分歧:完全诉诸单一主体决定的立法如美国《搭线窃听法》第 2511(2)(c)条,其规定预先获得其中一方同意,就可窃听通讯双方的电话交谈内容;相反,要求各方一致决定的立法见于《加州消费者隐私法案实施条例》第 999.318 条,其规定只有家庭所有消费者共同请求知悉家庭某项信息或者删除家庭个人信息,企业才有义务回应。在互赖个人信息从线下"强共同"向线上"弱关联"转型的背景下,上述立法多执着于一端,不免左支右绌。其破解之道还应回归到权利滥用规范,当个人公开、提供、使用互赖个人信息,导致自己获利与相关人受损之间显失比例,可推定为恶意,其决定不生效力,构成侵权的,应承担侵权责任;除此以外的决定,单方有权为之。

(二)个人信息查阅复制权的滥用

1.有悖于查阅复制权本旨的权利行使

个人信息查阅复制权,意指个人有权向处理者请求查阅所处理个人信息的必要信息,并取得副本的权利。查阅复制权不但落实了《个保法》第 7 条"公开、透明原则"和个人知情权,还是个人信息可转移权、更正补充权、删除权的制度性前提,因而被称为"个人信息保护之大宪章""关键性之权利"。〔49〕就此而言,虽然第 45 条表述为"查阅、复制个人信息",但应通过体系解释将范围扩张到"信息处理活动的必要信息",包括第 17、23、24 条下各项信息,但不应扩展到"有助于审查个人信息处理合法性的所有信息"。这是因为,在《个保法》公私混合的架构下,处理者承担行政和民事双重义务,处理合法性的审查不仅需要个人权利行使,更有赖于行政履责;另一方面,处理活动高度复杂专业,普罗大众不太可能通过查阅信息就作出是否合法的实质判断。结合第 69 条第 1 款下归责原则,查阅复制权宜以"与处理者过错认定相关的处理活动信息"为限。此外尚待探究的是:查阅复制权指向的究竟"信息"还是"数据"?这绝非语义之争,而是关乎当事人利益侧重、诉求性质和救济方式的权利本旨问题。〔50〕

关于数据和信息的关系,向来聚讼纷纭。随着《个保法》第 4 条第 1 款及《数据安全法》第

〔48〕"互赖个人信息"借鉴并修正了亚历山大·米哈伊拉·奥尔特亚努(Alexandra-Mihaela Olteanu)等人提出的"互赖数据"和张新宝提出的"共同隐私"。See Olteanu A. M. et al. "Consensual and Privacy-preserving Sharing of Multi-subject and Interdependent Data," Proceedings of the 25th Network and Distributed System Security Symposium, *Internet Society*, 2018, pp. 1－16;张新宝:《隐私权的法律保护》(第二版),群众出版社 2004 年版,第 206 页。

〔49〕参见许文义:《个人资料保护法论》,台湾三民书局 2001 年版,第 121 页。

〔50〕参见梅夏英:"信息和数据概念区分的法律意义",《比较法研究》2020 年第 6 期,第 153－155 页。

3 条第 1 款等实定法出台，“数据和信息合一并区分”的观点逐渐取得共识，即数据是表现信息的形式与载体，信息则是数据所反映的内容。〔51〕 据此，个人信息保护所针对的恰是“有关个人的信息内容”，“信息”而非“数据”才是法律关注所在。尽管《个保法》一定程度上影响了数据利用，但其实质是纯粹信息问题。个人信息查阅复制权更是以满足个人知情权为目的，在个人提出请求时，处理者所提供的应是“为人所理解的信息”，而非“被机器理解的数据”。这一观点亦被欧盟法院所支持：数据控制者无需提供数据副本，只要以可理解的形式提供有关个人数据的完整摘要就可。〔52〕

基于上述，个人超越个人信息知情权和监督处理者的目的，查阅复制不必要的处理信息，或者要求提供机器可读的数据，均可能因有违查阅复制权本旨而视为权利滥用。

2.恶意行使查阅复制权

行使查阅复制权中的“恶意”可从 “正当目的之欠缺”来把握。综合英国信息专员委员会和欧洲数据保护委员会的操作指南，〔53〕如下情形可被视为“恶意”：①以谋取利益为目的行使权利，例如，提出查阅复制请求后表示可以撤回，企图迫使处理者支付金钱来换取该等撤回；②以扰乱处理者生产经营为目的行使权利；③出于私人恩怨，明显针对处理者或特定员工提出请求；④在提出请求时，明确表示是为了给处理者制造麻烦。毋庸讳言，主观恶意并不易判断，因此还要从行为入手，全面考量如下要素：①个人提出请求的背景以及该人与处理者之间的关系；②查阅复制信息的数量、范围和敏感程度；③查阅复制信息的电子或非电子形式；④拒绝提供信息对个人所造成的实质损害；⑤请求的频度和时间间隔；⑥请求是否跟其它请求存在重叠。在各种不正当行为中，反复提出请求、漫无目的请求以及请求微不足道事项等，将被视为纠缠请求和过度请求，处理者有权予以拒绝，但负拒绝理由的说明义务。

3.推定的恶意行使查阅复制权

查阅复制权同样关乎他方权益，正如 GDPR 第 15 条第 3 款所强调，复制权行使不得对他人的权利和自由产生不利影响。在推定权利人是否恶意时，需要重点考察其行为是否过分损害其他信息主体权益、侵害处理者或第三人的权利。就关涉他人信息的权利行使而言，权利边界因查阅复制信息的不同而有所差异：若请求信息包含着可分割的他人信息，则其主张应限于自身信息；若请求信息系互赖个人信息，则个人首先应尽力取得他人同意，当确实无法取得同意时，须向处理者证明享有合法、合理利益，且对相关人影响较小，例如个人已获知该信息、相关人之前提供过该信息或信息通常向公众公开。此外，当相关人因教育、医疗、社会工作、行政管理等职务行为与个人发生信息联系时，其行使查阅复制权一般应予支持。就关涉他人权利的权利行使而言，处

〔51〕 参见申卫星：“数字权利体系再造：迈向隐私、信息与数据的差序格局”，《政法论坛》2022 年第 3 期，第 97 页；许可：“数据权利：范式统合与规范分殊”，《政法论坛》2021 年第 4 期，第 94 页。

〔52〕 See YS v. Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v. M and S, Joined Cases C-141/12 and C-372/12, Court of Justice of the European Union, 2014.

〔53〕 See ICO, *Right of Access*, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/right-of-access/, last visited on 20 August 2022; European Data Protection Board, *Guidelines* 01/2022 *on Data Subject Rights-Right of Access*, 2022.

理者一般无需回应可能侵害商业秘密、著作权、专利权的请求,这在 GDPR 序言第 63 条已有明文。不容易回答的是:若查阅复制权给处理者造成重大负担,可否推定为"恶意"?

处理者一般不会把特定人的个人信息都汇聚成单一数据表单,而是以业务单元为架构,以结构化或非结构化格式,按需形成实时数据、存档数据和备份数据。庞大的数据量、在线的更迭、复杂的格式和多样化保存,使得处理者难以响应个人关于其"所有"信息的宽泛请求。具体来说,在传统结构化数据库中,每个人均有唯一标识符,得以快速定位和提取信息;而在当今非结构化数据集中,个体不仅会被不同符号标注,其信息还杂糅着各种内容,这使得无法通过自动化检索完成,必须仰赖人工审核和编辑。无疑,这是非常昂贵和繁重的工作。2017 年,英国护士和助产士协会为了一位父亲的查阅请求,花费了 24 万英镑。有鉴于此,英国法院认为处理者只有"合理和相称"信息检索与提供义务,而没有"不遗余力的义务"。〔54〕不过,考虑到我国个人信息保护的现状,不宜过分缩限访问复制权的行使,可考虑借鉴 2021 年英国个人信息保护改革建议文件《数据:新方向》第 2.3 条,对于费用不超过设定数额(如 1000 元人民币)的访问复制请求,处理者应及时提供;对于超支部分,除个人自行承担外,处理者可以拒绝。

(三)个人信息转移权的滥用

1.有悖于个人信息转移权本旨的权利行使

个人信息转移权,即信息主体在满足法定条件的情形下,有权请求处理者将个人信息转移至指定的其他处理者,原处理者应当提供转移途径。从制度渊源上,该权利移植于 GDPR"数据可携权",但在立法目的和规范结构上迥然有异,不可不察。

第 29 条工作组《个人数据可携权指南》开篇指出:与"访问权"(right of access)不同,数据可携权允许数据主体以结构化、通用性和机器可读的格式接收他们提供给数据控制者的个人数据,并将该数据传输给另一个数据控制者。其目的有二:强化个人对数据的控制,落实信息自决权;支持欧盟境内个人数据自由流动、促进控制者竞争,从而推动数字单一市场战略下的企业创新。〔55〕如前所述,包括转移权在内的个人信息权利均非奠基于个人信息自决权。同时,与 GDPR 第 1 条将"个人数据保护和自由流动"并置不同,《个保法》并未体现出"促进个人信息流动"意旨,相反,最终稿特别删除了一审稿第一条"保障个人信息依法有序自由流动"的表述,充分说明其无意于个人信息流动与市场竞争秩序建构。当然,我国并非没有考虑数据流通和公平竞争问题,而是将其交由《数据安全法》第 7、51 条处理。就规范结构而言,GDPR 第 20 条的数据可携权决非第 15 条下访问权的自然延伸,而是一种独立于《欧盟基本权利宪章》第 8 条的全新权利。正因如此,数据可携权在权利对象、行使方式和条件上均与访问权大相径庭。反观我国,无论是《民法典》第 1037 条,〔56〕还是《个保法》第 45 条,均表明个人信息转移

〔54〕 See Ittihadieh v. 5－11 Cheyne Gardens RTM Company Ltd and Others [2017] EWCA Civ 121, 2017.

〔55〕 See Article 29 Data Protection Working Party, *Guidelines on the Right to Data Portability*, 2017, p. 3.

〔56〕 最高法院认为移植个人信息属于《民法典》下复制权的内容,参见最高人民法院民法典贯彻实施工作领导小组编:《中华人民共和国民法典人格权编理解与适用》,人民法院出版社 2020 年版,第 390 页。

权系承接查阅复制权而来，权利对象与目的同一的“三位一体规范结构”由此成为与 GDPR 截然不同的特色。

基于上述，以下情形可能构成滥用个人信息转移权：其一，背离知情权的目的，为其他市场竞争者利益而行使权利。作为查阅复制权的强化，个人信息转移权旨在提供更充分、多样的个人权利保障渠道，而非商业利益的获取。为个人诊疗目的，在多家医院间转移健康医疗信息构成权利正当行使，相反，为其他医院研发新药而从原医院转移信息，难谓正当。其二，主张处理者为第三方设立开放接口，以传输电子化数据。个人信息转移权与查阅复制权共同指向“供人阅读的信息”而非“数据”，因而处理者有权自行决定电子邮件、页面下载等各种信息转移途径，而毋庸提供数据传输通道。

2.恶意行使个人信息转移权

个人信息转移权的恶意行使亦体现为“正当目的欠缺”。除与查阅复制权类似的情形外，个人信息转移权因牵连到其他处理者，更容易引起竞争对手以支付金钱为代价，蓄意诱导、组织用户行使转移权，不但对原处理者财产权益带来侵害，而且可能有损于其合同权利。〔57〕在“北京微梦创科公司与北京字节跳动公司不正当竞争纠纷案”[(2017)京 0108 民初 24530 号]中，被告抓取或以人工复制方式大规模获取新浪微博用户发布的内容，并紧随其后展示在今日头条中，严重削弱了原告的竞争优势。尽管被告宣称取得了用户同意，并诉诸数据可携权证明行为正当性，但法院明确指出：民事主体对其权利的处分不得超出自身所享有的权利范围，不得侵害他人合法权益，从被告移植内容看，明显超出了授权用户自身生成并享有权利的文字、图片范围，损害了原告基于经营新浪微博所享有的合法权益，被告获得授权的辩称不予支持。

3.推定的恶意行使个人信息转移权

辗转腾挪于三方之间的个人信息转移权，必然包含多元利益和价值之间的竞争。〔58〕其中，个人和他人的利益冲突主要体现在“互赖个人信息”的转移上。与查阅复制不同，“转移”属于《个保法》下高风险处理活动。对相关人而言，转移后的信息可能被泄露和滥用，还面临着后续难以向接收方主张权利的不利局面，因此，互赖个人信息转移的条件应比查阅复制更严苛，原则上应取得相关人同意。但是，若个人就转移享有正当、显著的利益，不会直接或者严重损害他人生命、身体、健康等人格权益，相关人已经被告知且未表示拒绝时，则不构成权利滥用。就个人和处理者的利益冲突论之，其不仅源于处理者因转移而生的成本以及商业秘密、知识产权的侵害，更是出于处理者对于接收方“不劳而获”的抵制。前者已在查阅复制权中论及，针对后者，GDPR 在可携带数据范围、处理方式和技术条件加以重重约束，《数据法案》第 4、6 条还特别禁止用户、第三方将转移数据用于开发与数据来源者竞争的产品。较诸欧盟大费周章的立法，我国早有了删繁就简的解决之道。具体而言，个人信息转移权以信息和数据、人格与财产、个体与市场二分为原则，让信息与人格归于个体，让数据与财产归于市场，实现了逻辑清明和功能简化，各方围绕数据的纠纷自然消弭。循此，除接收方业已构成侵权的恶意行使外，个

〔57〕 参见丁晓东：“论数据携带权的属性、影响与中国应用”，《法商研究》2020 年第 1 期，第 82 页。

〔58〕 参见王锡锌：“个人信息可携权与数据治理的分配正义”，《环球法律评论》2021 年第 6 期，第 14 页。

人信息转移权一般不会戕害原处理者,无认定“推定恶意”之虞。只有在第三方嗣后采取不正当手段大规模汇聚、加工转移后的个人信息,并实质上替代处理者产品或服务的情形下,才会引发不正当竞争。但此时,已非个人信息保护下的信息问题,而进入了数据领域。

三、平衡个人信息处理者与信息主体利益的诚信机制

补充义务、限制权利和利益平衡是诚信原则的三大机能。前两者已在上文详述,如何维持信息主体与处理者间的利益平衡自然成为本部分的重点所在。一切平衡都是关系性的,由于关系变动不居,利益平衡基准亦随物赋形。详言之,在债之关系、质押、相邻共同体、地役权等法律上“特别关系”(Sonderbeziehung)中,保护诚实与维护信用塑造了法律交往基础。〔59〕诚信原则据此要求当事人彼此信赖、相互合作,以“爱邻如己”的精神,用对待自己事务的注意对待他人,在追求自身利益的同时,不利用权力、能力损害他人,以实现各得其所。〔60〕与此不同,在代理人和被代理人、董事和公司、合伙人与合伙企业、医生与病人、特许人与被特许人、顾问与客户等“信义关系”(fiduciary relationship)中,受信人应确保委托人利益的至上性,凭专一忠诚为委托人利益行事,而不得将其自身或第三人的利益置于与委托人利益相冲突的位置。从特别关系到信义关系,利益平衡从信赖合作的互利向先人后己的他利转变,行为标准从“一般诚信义务”向“信义义务”转变,〔61〕展现出一条渐次上升的规则曲线。

(一)信义义务:因处理者而异的利益平衡机制

自杰克·巴尔金(Jack M. Balkin)力主将信义义务引入个人信息处理以来,〔62〕处理者应否承担信息信义义务,一时间聚讼纷纭。赞成者认为信义义务是个人信息保护的破解之道,反对者却质疑其模糊不清和自相矛盾,甚至可能将公共监管扼杀于摇篮中。面对正反两方针锋相对的意见,本文提出一个分而治之的思路:作为国家机关的处理者负有信义义务,而作为私主体的处理者则否。

信义义务以信义关系为前提。从制度功能出发,信义关系以化解经济学上“委托代理问题”和“不完全合同问题”为鹄的。〔63〕所谓委托代理问题,即委托人为自己事务之目的将财产或权力委托给受信人,在信息不对称、道德风险、逆向选择等固有缺陷的推动下,双方出现利益冲突;所谓不完全合同问题,即在复杂多变和交易成本高昂的世界中,凭借人的有限理性、语言能力以及可观察但不可证实的信息,为委托代理事项订立一个完全合同近乎不可能。由于合

〔59〕 参见于飞:“公序良俗原则与诚实信用原则的区分”,《中国社会科学》2015 年第 11 期,第 153 页。

〔60〕 参见沈达明:《衡平法初论》,对外经济贸易大学出版社 1997 年版,第 191 页。

〔61〕 诚信义务和信义义务当前已逐渐交融,参见朱圆:“论信义法的基本范畴及其在我国民法典中的引入”,《环球法律评论》2016 年第 2 期,第 94—95 页。

〔62〕 See Jack M. Balkin, “Information Fiduciaries and the First Amendment,” *U.C.Davis Law Review*, Vol. 49, No. 4, 2016, p. 1183.

〔63〕 See Robert Sitkoff, “The Economic Structure of Fiduciary Law,” *Boston University Law Review*, Vol. 91, 2011, p. 1041.

同漏洞不可避免，受信人获得可自由裁量的“剩余权力”，影响甚至决定了委托人权益，由此导致后者容易遭受损害的“脆弱性”。〔64〕

立足于信义关系，私主体处理者恐难成为受信人。一方面，个人和私主体处理者并非委托代理关系。实践中，个人不是处理活动发起人，处理者也不是向个人提供处理服务的受托方，恰恰相反，处理者是为了自己目的、自主决定处理目的和方式的人。除了为订立和履行合同之必要而进行的处理外，个人信息处理活动很难说与个人目的有关：就原始信息处理而言，它不过是履行合同的副产品，就衍生信息处理而言，它更多是为处理者目的而设。法律关系上或许看得更清楚。在个人信息非财产化和否定个人信息支配权的体系下，个人对处理活动的“同意”不是人格权商业化中权利人“许可”，不属于为他人创设使用某种财产或人格要素自由的“授权”，〔65〕其实质是侵权法上的违法阻却事由，其效力在于排除侵入个人信息权益的处理行为非法性。〔66〕另一方面，处理者对信息处理享有的权力决不是“开放性的”：其不仅受制于巨细靡遗的个人信息处理文件，还必须遵循“最小必要原则”，在明确、具体的处理目的下使用直接相关的信息类型。《常见类型移动互联网应用程序必要个人信息范围》等规范采取更严格的监管标准，进一步消解了剩余权力的空间。

与私主体处理者不同，国家机关处理者毋宁是典型的受信人。首先，如《宪法》所宣誓，国家机关的一切权力皆源于人民授予、系为人民福祉而行使的基于信托关系的权力。〔67〕其次，“个人信息国家保护义务”将国家机关置于尊重私人生活、防范“监控国家”和“监控资本主义”系统性侵害公民信息的首要位置上。〔68〕最后，国家机关在个人信息处理中天然地享有裁量权。作为现代行政权中最具共性的部分，裁量权是行政职能发挥所必需的权力。《个保法》充分尊重了行政裁量权：国家机关为履行法定职责而处理个人信息无需个人同意，“最小必要原则”也仅要求“不得超过履行法定职责所必需的范围和限度”（第 34 条）。但问题在于，这里的“法定”并无固定边界，除法律、法规外，还囊括了部门规章、地方性规章、规范性文件等形形色色的国家规定。〔69〕不惟如是，鉴于法律规范就如何处理个人信息鲜有明文，其处理的具体条件、种类、方式全然留给国家机关自行判断决定。例如，在“行政处罚决定公开”中，当事人姓名、性别、地域、职业、工作单位等林林种种的个人信息如何公开，仍无一定之规。〔70〕“李某迪因嫖娼被行政拘留”事件不啻为鲜活的一例。

（二）一般诚信义务：信息主体与私主体处理者的利益平衡

个人与私主体处理者的利益平衡系从“特别关系”出发，经由“一般诚信义务”而实现的。

---

〔64〕 参见许德风：“道德与合同之间的信义义务”，《中国法律评论》2021 年第 5 期，第 140－153 页。

〔65〕 参见高富平：“同意≠授权——个人信息处理的核心问题辨析”，《探索与争鸣》2021 年第 4 期，第 87－94 页。

〔66〕 参见程啸，见前注〔44〕，第 40－48 页。

〔67〕 参见（英）洛克：《政府论》（下篇），叶启芳、瞿菊农译，商务印书馆 1996 年版，第 92 页。

〔68〕 参见王锡锌：“个人信息国家保护义务及展开”，《中国法学》2021 年第 1 期，第 155－157 页。

〔69〕 程啸：《个人信息保护法理解与适用》，中国法制出版社 2021 年版，第 132 页。

〔70〕 参见孔祥稳：“行政处罚决定公开的功能与界限”，《中外法学》2021 年第 6 期，第 1631－1633 页。

一方面，在互动互联的网络社会和代码主宰的数字世界中，任何一方都不可能独存，永远在线的数字化生活和产业数字化转型已成为当代个体和企业的真实面貌。另一方面，两者相互依赖的特质，并未抹杀暗藏其间的不平等性。〔71〕故此，一般诚信义务蕴含了对特定情景中弱者加以保护和照顾的功能。在比较法上，GDPR 的正当利益条款，可谓落实该等利益平衡的重要经验。

遗憾的是，立法者出于对法律不确定性的担忧，《个保法》最终只将“实施人力资源管理所必需的个人信息处理”这一公认的正当利益事由纳入。职是之故，当个人信息处理涉及下述内容时：〔72〕①预防欺诈和犯罪：如了解你的客户、反洗钱可疑名单共享、打击网络黑灰产、披露威胁国家安全和公共安全的信息、公共区域视频监控等；②遵循行业自我规制要求：如恶意客户名单、客户信用信息、基于行业惯例的信息交流等；③维护网络安全：如安全事件调查、产品安全监测、监控对系统的访问和下载；打击盗版和病毒软件；④公司内部管理：如尽职调查、公司重组、为战略计划分析客户信息、管理第三方（供应商、媒体、合作伙伴）、企业集团内共享信息、保护知识产权和商业秘密等；⑤公司对外营销：如直接营销、收集市场情报、活动策划等；⑥提起诉讼和应诉；⑦历史、科学、统计等学术研究；⑧开展慈善活动；⑨遵守外国法律、执法机构和司法机关的强制性规定，《个保法》无法援引“正当利益条款”作出恰如其分地回应。此时，诚信原则作为克服成文法局限的法律原则，成为填补这一法律漏洞的最佳工具，而这也契合了正当利益条款的实质——提供一个灵活的平衡原则，而非局限于特定个案规则。〔73〕

GDPR 行之有效的“利益平衡测试”为诚信义务的个案适用提供了指引。〔74〕详言之，首先是“处理者利益测试”：其一，评估处理者正当利益的真实性，其利益是否现存、明确、具体、合法；其二，识别处理者正当利益的类型，是自身利益还是第三方利益，经济利益还是公共利益；其三，评估处理活动对正当利益实现之必要性，即从目的关联性和最小必要原则看，其处理是否不可或缺。在帕特里克·布雷耶诉德国联邦政府一案中，法院认为防止黑客攻击虽属合法利益，但记录原告 IP 地址未必是影响最低的使用方式，因而违反必要原则。〔75〕

其次是“信息主体利益测试”：其一，识别个人可能被影响的利益类型，是基本权利、其他权利还是法益，是财产性利益还是人格性利益；其二，评估对个人的影响程度。“影响”不限于“损害”，还指向了任何实际或潜在的后果，既有对个体人格权、财产权的直接侵害，还包括社会第

〔71〕 参见丁晓东：“法律如何调整不平等关系——论倾斜保护型法的法理基础与制度框架”，《中外法学》2022 年第 2 期，第 446 页。

〔72〕 See CLPI, *How the Legitimate Interest Ground for Processing for Processing Enables Responsible Data Use and Innovation*, 2021.

〔73〕 See European Data Protection Supervisor, *Additional EDPS Comments on the Data Protection Reform Package*, 2013.

〔74〕 See Article 29 Data Protection Working Party, *Opinion* 06/2014 *on the Notion of Legitimate Interests of the Data Controller Under Article 7 of Directive 95/46/EC*, 2014.

〔75〕 See Patrick Breyer v. Bundesrepublik Deutschland, judgment of 19 October 2016 (ECLI:EU:C:2016:779).

三方将来可能行为所引发的排除、歧视当事人的间接风险。为尽可能准确评估“影响”,应全面考虑个人信息的类型(公开还是非公开,敏感还是非敏感)、处理方式(高风险还是低风险)、处理者的身份(个人、小微企业还是大型公司)、危险的严重性及其发生概率、个人合理期待,等等。在容易引发争议的情景下,可使用“个人信息保护影响评估工具”,以国家标准《个人信息安全影响评估指南》为参考,细化相关影响程度。

再次是“暂定的权衡测试”,即凭借权衡思考和权衡法则,比较两者利益孰高孰低。在 Camera di Commercio 案中,欧盟法院认为,商会有权向第三方披露原告担任已破产公司管理人的信息,因为第三方可通过查明公司文件了解其个人情况,以确保合法公平交易,处理者和第三方的利益优先于原告利益。〔76〕 在另一个案例中,瑞典最高行政法院则认为:加油站安装摄像头自动读取车辆拍照号码,并与安全公司数据库中号码相匹配的处理活动,存在防范司机恶意逃费的正当利益,但其数据可能不准确、监控范围过于宽泛,从而给个体造成重大的隐私风险,因此其利益不被支持。这里的“权衡测试”之所以是暂定的,是因为处理者可另行采取措施,降低对信息主体的不利影响。

最后是“保护措施的测试”。除了遵循法定的个人信息保护义务外,对于暂时未通过权衡测试的处理活动,处理者还能利用去标识化、隐私设计、隐私计算等合规科技、赋能科技以及对个体增强赋权,〔77〕尽可能降低对个人的不利影响。例如,在智能出行的场景下,保证行车安全需要而采集车外个人信息构成正当利益,但应及时匿名化,删除含有能够识别自然人的画面,或对人脸信息进行局部轮廓化处理。再如,各医院为控制药品供应而共建药品瘾君子黑名单系正当利益,但由于该信息属于个人敏感信息,医院应采取额外措施,确保其不会被泄露和滥用。要之,若额外措施可行、合适,确保信息主体无条件地“选择退出”其处理活动,则处理者利益有可能最终优先。

(三)信义义务:信息主体与国家机关处理者的利益平衡

信息主体与国家机关处理者的利益平衡应遵循信义义务,而非一般诚信义务,GDPR 正当利益条款排除行政机关适用,可作佐证。通过事前预防和事后审查的双重限制,信义机制能够消解国家机关处理个人信息中的“合法要求”形式化、“正当目的”空洞化、“必要拘束”形骸化等痼疾,在合法、正当、必要原则力有不逮之时,规范自由裁量权,保护地位严重不对等的行政相对人。

信义义务由“忠实义务”和“谨慎义务”组成,从利益平衡的维度,忠实义务无疑是其核心。在抽象面向上,国家机关应向全体人民承担忠实义务,视公共利益、国家利益为唯一利益,不得将自己置于与其利益相冲突的位置,更不得通过个人信息处理谋求私利。公共选择理论业已证明:国家机关背后是自利的个人,其经常为了经济利益(如经济发展、财政收入或违法所得)、政治利益(地方保护、维稳或意识形态)而做出自身利益最大化,而非公共利益最大化的选择。

〔76〕 See Case C－398/15 Camera di Commercio, Industria, Aritigianato e Agricoltura di Lecce v. Salvatore Manni, judgment from 9 March 2017.

〔77〕 参见许可:“个人信息治理的科技之维”,《东方法学》2021 年第 5 期,第 60－65 页。

从跨地域逐利性执法，到不合理考核指标导致的部门利益滋生，均是例证。在具象面向上，除侦查犯罪、行政执法外，国家机关在针对特定人处理其信息时，不得采取可能有害于信息主体的处理方式。2016年日本行政机关个人资料法明确将“对本人或第三人权利、利益未造成不当损害之虞”作为自由裁量权的前提。就东京都教育委员会将某公立中学教师“服务事故报告书”提供给东京都议会议员一案，法院认为：相关信息在传播媒体上用作人身攻击之可能性极高，故提供个人信息的行为无法被认定为谋求公共利益之必要且正当者，属于裁量权滥用。〔78〕“禁止损害义务”构成了国家机关公开和共享个人信息的硬约束。就前者而言，政府信息公开不可避免地披露个人信息，但不得直接侵害相关信息主体的人格尊严、人身财产安全，若其能够预见第三方利用相关信息实施侵害行为时，亦同。为此，国家机关对个人私密信息和敏感信息一般禁止公开，对于一般个人信息应审慎公开。〔79〕就后者而言，在政府信息共享中，一方面坚持“被动共享模式”，即采取接收方依法定职权向他方调取个人信息，而非收集者主动向他方提供；另一方面坚持“禁止不当联结原则”，即接收方在行政裁量不得考虑与事件不相关的个人信息，尤其不得使用行政相对人近亲属的个人信息，以防不合理的“附第三人效应”。〔80〕

国家机关的忠实义务不会自我执行，其有赖于双重机制保障。一方面，忠实义务系为了保障弱势相对人而设，属于必备的、不容削减的法定义务，在国家机关和个人的特殊关系中更是如此。为防止前者利用公权力令后者陷入“表意不自由”的状态，应禁止通过个人同意机制豁免国家机关全部或部分忠实义务。另一方面，作为忠实义务的基础，国家机关负有“诚信的信息披露义务”。〔81〕有异于告知义务，该义务在披露对象上，强调攸关个人权益的所有事项；在披露时间上，强调事前、事中、事后的全流程披露；在披露方式上，强调在与个人的互动交流中说明、解释处理行为的合法性、正当性、必要性。总之，如果说告知义务来自一般诚信义务的话，那么信息披露义务有着更深刻的道德原则——它要求国家机关诚实、坦荡，在预见到个人因认知偏差、信息过载而无法理解信息时，承担积极的警告和解释职责。

四、结　语

个人信息保护与利用的平衡是数字时代核心议题之一。《个保法》创造性地引入了“基于诚信的平衡机制”，不仅弥补了既有平衡机制的缺憾，更有助数字信任困境的化解。但与此同

〔78〕 参见范姜真媺：“检视行政机关收集利用个资之问题及展望”，《法学丛刊》第63卷第2期（2018年），第40－60页。

〔79〕 参见张新宝、魏艳伟：“司法信息公开的隐私权和个人信息保护研究”，《比较法研究》2022年第2期，第114－118页。

〔80〕 参见沈岿：“社会信用惩戒的禁止不当联结”，《暨南学报（哲学社会科学版）》2021年第11期，第14页。

〔81〕 See Neil Richards and Woodrow Hartzog, “Taking Trust Seriously in Privacy Law,” *Stanford Technology Law Review*, Vol. 19, 2016, pp. 463－465.

时，诚信原则的提出亦引发了新的疑问：其如何与合法、正当、必要原则，尤其是“正当原则”分工协作？追本溯源，由民法公序良俗和行政法正当原则所发展的“正当原则”，〔82〕与诚信原则存在诸多差异：以制度宗旨论，前者以一般性公共秩序和社会利益为依归，后者以关系性权益及其平衡为依归；以调整对象论，前者不涉信息主体，后者涵盖多方主体；以规范内容论，前者侧重于处理者处理目的与程序的正当性，后者侧重于权利行使和义务履行的合理性；以行为标准论，前者是相对标准化和低要求的，后者是场景化和相对高要求的。当然毋庸讳言，正当原则和诚信原则同为一般条款，其内涵和外延均高度不确定，如何厘清各自边界仍有赖于未来解释论的努力。也正因如此，诚信原则必须经由更多个案的累积才能逐渐形成可预见的具体规则，而如何在复杂多变的环境下折中调和，依然路阻且长。我们期待着执法者和司法者亦能秉持诚信，在《个保法》执法与司法的实践中开辟出积极回应社会与经济真切需求的中国道路。

Abstract: One core topic in this digital age is how to balance between protection and utilization of personal information. The Personal Information Protection Law adds the principle of good faith to the principle of legality, legitimacy and necessity, creating a balanced path based on good faith. This path effectively integrates the “context-based approach” to make up for the shortcomings of the “proportionality-based approach” and “risk-based approach”, and solves the digital trust deficit. The principle of good faith can be categorized into the following three sub-mechanisms. First, “good faith mechanism to supplement the obligations of controllers” imposes a general obligation on controllers not to defraud, manipulate and treat individuals fairly. Second, “good faith mechanism to limit the rights of information subjects” prohibits individuals from abusing their rights in information processing activities to the detriment of rights of others. Third, “integrity mechanism to balance the interests of information subjects and processors” requires state organs to assume the fiduciary duty of faithfulness and diligence, and introduces a legitimate interest clause to reconcile the conflicting interests of private controllers and individuals. As a carte blanche of appointment granting discretion, the principle of good faith requires that law enforcers and judicial personnel should also uphold good faith, balance between personal information protection and utilization as the purpose, properly interpret legal rules, fill legal loopholes, and finally implement the flexible rule of law order for personal information protection based on the rules-principle model.

Key Words: Personal Information; Good Faith; Digital Trust

（责任编辑：彭 錞）

〔82〕 参见杨合庆，见前注〔35〕，第 25 页。