

个人信息保护中告知同意的困境与出路

——兼论《个人信息保护法（草案）》相关条款

韩旭至

摘要：以告知同意为原则的个人信息保护必然面临诸多困境，典型如“隐私政策”无人读、不可读、读不懂，信息主体被“胁迫同意”以致难以行使拒绝权，大数据处理实难取得有效的同意，问责机制难以发挥功效等。告知同意机制源自个人信息自决权与隐私权理论，但从私法上将同意等同于授权，实为对个人信息保护制度公法属性的误读。主流个人信息保护制度中，从未将告知同意规定为基本原则，它是个人信息保护中的一项具体规则。我国个人信息保护立法必须处理好告知同意与其他数据合法处理规则的关系。一方面，对告知同意规则进行进一步细化，并以格式合同规范约束“隐私政策”；另一方面，确立数据流通规则体系，引入个人信息保护设计。

关键词：个人信息保护；告知同意机制；个人信息自决权；数据流通规则；数据利用

[中图分类号] D923 [文献标识码] A [文章编号] 2096-6180 (2021) 01-0047-13

告知同意在个人信息保护中的法律地位存在较大理论争议。有学者认为，告知同意是个人信息保护的基础⁽¹⁾，属于个人信息保护的重要原则⁽²⁾。亦有学者认为，告知同意已经无法实现其原有功能，应弱化告知同意⁽³⁾，转为适用风险规则⁽⁴⁾。该争议已对我国个人信息保护立法产生了不容忽视的影响。2020年第十三届全国人民代表大会常务委员会第二十二次会议对《中华人民共和国个人信息保护法（草案）》（下称《草案》）进行了审议。《草案》虽未直接将告知同意规定为个人信息保护的原则，且第13条在告知同意以外列举了5类合法处理个人信息的情形，并扩充了《中华人民共和国民法典》（下称《民法典》）第1036条之规定，但其他合法的个人信息处理事由并未贯穿《草案》始终。“立法说明”仍然认为，告知同意是个人信息处理规则的核心，然而，告知同

【作者简介】韩旭至，法学博士，华东政法大学法律学院特聘副研究员，数字法治研究院副院长。

【基金项目】国家社会科学基金重大项目“数字社会的法律治理体系与立法变革研究”（项目批准号：20&ZD177）。

(1) 张勇：《APP个人信息的刑法保护：以知情同意为视角》，载《法学》2020年第8期，第113页。

(2) 张新宝：《个人信息收集：告知同意原则适用的限制》，载《比较法研究》2019年第6期，第1页。

(3) 梁泽宇：《个人信息保护中目的限制原则的解释与适用》，载《比较法研究》2018年第5期，第16页。

(4) 高富平：《个人信息使用的合法性基础——数据上利益分析视角》，载《比较法研究》2019年第2期，第72页。

意机制已不适应现代信息处理的发展，难以实现其原有功能。因此，必须从告知同意的适用困境出发，对告知同意机制的理论基础进行辨析，以正确处理告知同意与数据合法处理的关系，构建适应于时代发展的个人信息保护制度。

一、告知同意的内在缺陷

运用“法律—社群规范—市场—架构”的网络法基本分析框架⁽⁵⁾，告知同意应放在具体应用场景中进行分析，以判断这一机制是否与用户习惯、交易模式、数据处理技术相适应。分析可知，告知同意无论是作为一种授权机制抑或视为一种免责/问责机制，均面临困境，实难以成为个人信息保护的基点。

(一) 作为授权机制的失灵

第一，用户难以在获得有效信息的基础上作出同意的授权。为实现“告知—同意”，各类 App、网页都会展示相关“隐私政策”，常常需要用户去点击同意相关条款。为避免用户不经阅读就直接点击，不少条款还需要用户下拉至底端或等待若干秒以后才允许点击同意。即便如此，实际上也并没有多少用户真正阅读这些条款。如果一个人将其 1 年内遇到的所有“隐私政策”全部阅读完毕，不眠不休地进行也将需要花费数月时间。由此可见，“隐私政策”实际上也是不可读的。同时，若对“隐私政策”进行阅读便会发现，其条文充斥着各种“法言法语”，具有较强的专业性，对于普通群众而言，也是读不懂的。由此可见，“隐私政策”实际上无人读、不可读、读不懂，告知同意无法实现其应有功能，难以通过该机制保护个人信息。在这个意义上，告知同意也被称作“控制的幻象”。⁽⁶⁾

第二，由于用户习惯不经阅读即点击同意，告知同意机制存在被滥用的危险。企业常常在“隐私政策”中设置不合理、不公平、侵害个人信息权益的条款。最为典型的案例是，2019 年“ZAO”App 极其不规范的“隐私政策”即受到了广泛关注。该款“AI 换脸”App 在其“隐私政策”中约定，用户上传相关照片后，即视为同意授予“ZAO”及其关联公司以及“ZAO”用户在“全球范围内完全免费、不可撤销、永久、可转授权和可再许可的权利”。⁽⁷⁾事实上，即便是大型平台企业的“隐私政策”也存在众多对个人信息保护不利的约定。如百度规定，其可使用算法抓取用户信息。⁽⁸⁾支付宝也规定，其有权向关联方、合作伙伴提供所采集的用户个人信息。⁽⁹⁾显然，这些条款在披上告知同意的外衣后，将对个人信息保护形成更大威胁。

第三，用户对“隐私政策”难以真正行使拒绝权。虽然，理论上用户若不同意“隐私政策”

(5) [美] 劳伦斯·莱斯格：《代码 2.0：网络空间中的法律》，李旭、沈伟伟译，清华大学出版社 2018 年版，第 135 页。

(6) See Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies*, Harvard University Press, 2018, p. 75.

(7) 温婧：《国信办回应“ZAO”涉嫌违规：已制定多项法规并进行专项治理》，载中国日报中文网 2019 年 9 月 18 日，<http://cnews.chinadaily.com.cn/a/201909/18/WS5d82eb3da31099ab995e0d64.html?from=singlemessage>。

(8) 《百度隐私政策总则》，载百度网，<https://www.baidu.com/duty/yinsiquan-policy.html>，2020 年 12 月 20 日访问。

(9) 《支付宝服务协议》，载支付宝网，<https://render.alipay.com/p/f/iztow1fi/index.html>，2020 年 12 月 20 日访问。

即可拒绝。但实际上，网络服务提供商所提供的协议通常为一揽子安排的格式合同，并未提供菜单式选择，用户往往面临“要么同意，要么放弃”的困境。对于许多 App 的使用，实际上用户是无法拒绝的。例如，当今微信、钉钉、支付宝等 App 已经紧密嵌入人们生活之中，若无法使用这些产品，将严重影响工作和生活，甚至成为“数字弱势群体”而被边缘化。在这个意义上，也可以说用户的同意是“被胁迫”的。在“霸王条款”面前，告知同意形同虚设。

第四，告知同意机制偏重于数据收集环节，难以适应大数据处理的发展要求。大数据分析往往不限于数据收集目的，对海量数据的二次利用展现出复杂性、多元性与流动性的特征。信息处理者既难以在数据收集时要求信息主体给予广泛的授权，也难以在信息处理时获得信息主体的二次授权。^{〔10〕}此时，不仅告知同意的难度加大、成本上升，强调告知同意还可能会阻碍大数据产业的发展。^{〔11〕}此外，大数据时代中个人信息与群体数据密切相关。在标签化分类之下，一个人可能同时属于多个群组。其基于告知同意作出的某个决定，将同时对多个群组的数据分析产生影响。也就是说，针对个人的告知同意，将可能对群体利益产生影响。在这个意义上，技术伦理指出，“‘个人决定’将会转化成一种‘个人—集体决定’”。^{〔12〕}因此，已难以允许仅凭个人意志就作出涉及他人利益的同意。

（二）作为免责/问责机制的失效

当前，告知同意已从一种失灵的授权机制转变成为一种失效的免责/问责机制，无法全面回应实践中出现的数据利用问题。司法实践中，告知同意常被用于考察个人信息处理的合法性，成为企业处理个人信息的免责依据，或企业违反“隐私政策”处理个人信息时的问责依据。2016年，北京知识产权法院通过“新浪诉脉脉案”提出第三方获取个人信息须坚持“用户授权+平台授权+用户授权”的“三重授权”原则。^{〔13〕}《草案》第24条沿袭这一思路规定，个人信息处理者向第三方提供其处理的个人信息的，应当再次使用告知同意机制。然而，这一机制仍然存在忽视个人信息复合利益的问题。第三方只取得用户同意而未取得原信息处理者同意时，能否获取信息存在疑问。2017年华为公司未经微信同意，仅通过用户授权的方式采集微信记录，即曾经引发争议。根据告知同意的逻辑，似乎三重授权之中的“平台授权”并无必要，但这显然与数据权利保护内容不符。从数据权属的角度来看，告知同意之下企业似乎是基于继受取得获得数据权利，这又将与企业基于算法投入“劳动赋权”的原始取得逻辑相冲突。

此外，告知同意的授权范围存在局限。以通信录信息为例，记载的常常是其他人的个人信息，用户的授权无法指向相关内容，其授权合法性存疑，然而，众多社交软件关键的商业模式即为通

〔10〕 谢琳：《大数据时代个人信息使用的合法利益豁免》，载《政法论坛》2019年第1期，第129页。

〔11〕 田野：《大数据时代知情同意原则的困境与出路——以生物资料库的个人信息保护为例》，载《法制与社会发展》2018年第6期，第120页。

〔12〕 黄柏恒：《大数据时代下新的“个人决定”与“知情同意”》，载《哲学分析》2017年第6期，第110页。

〔13〕 北京微梦创科网络技术有限公司诉北京淘友天下技术有限公司、北京淘礴天下科技发展有限公司不正当竞争案，北京知识产权法院民事判决书（2016）京73民终588号。

过用户授权，获取通信录信息以进行推广。2020年“凌某某诉抖音案”实际上已经涉及这一问题。该案中，与一般意义的通讯录不同，凌某某在其通讯录中仅保留了其自身信息，但该平台在获取相应信息后，基于其他人通讯录中记载的关于凌某某的信息，对其推荐了“可能认识的人”。北京互联网法院认为，抖音未基于告知同意而收集凌某某手机上的个人信息属于侵权，但“可能认识的人”的推荐不构成侵权。⁽¹⁴⁾然而，该案中法院实际上并未对基于告知同意获取通讯录中第三方信息的行为作出分析，仅以该推送未侵害生活安宁为由否定了凌某某的第二项主张，事实上混淆了隐私侵权与个人信息侵权的区别。在域外或我国特别行政区的相关司法实践中，通讯录的授权需要所涉信息主体的同意已获得普遍认可。2016年我国香港法院在“梁竣杰案”中即认为，未经信息主体授权向他人展示第三人的名片，以供他人誊抄名片上的个人信息构成违法。⁽¹⁵⁾2017年德国“WhatsApp案”中，法院亦认为获取通信录信息需要获得所有联系人的书面同意。⁽¹⁶⁾然而，告知同意的这一要求，必将对众多社交软件的商业模式带来毁灭性的打击。由此可见，即便是作为一种免责/问责机制，告知同意也难以回应实践中产生的问题。

二、告知同意的理论误读

面对告知同意的困境，虽有学者提出场景化的且基于风险的分析路径，但实际仍未脱离告知同意的制度。⁽¹⁷⁾告知同意仍被部分学者奉为个人信息保护必须坚守的核心原则。⁽¹⁸⁾甚至有学者将告知同意称为“个人信息保护之魂”“个人信息保护大厦之基”⁽¹⁹⁾，或称“告知同意原则”是个人信息保护制度的“帝王条款”，如同意思自治在民法中的地位。⁽²⁰⁾事实上，无论是从个人信息保护理论体系还是制度规范体系来看，告知同意从来都不是个人信息保护的原则，而是一项具体规则。

（一）私法视角的误读

告知同意植根于个人信息保护的两大理论基础：一是欧盟个人信息保护体制中的个人信息自决权理论；二是美国法上的信息隐私权理论。从个人信息自决权来看，德国1983年“人口普查案”对现代个人信息保护的产生与发展具有重大意义。⁽²¹⁾在对该案判决的解读中，个人信息自决权的概念首次被提出。此后，个人信息自决成为域外个人信息立法的重要理论基础。从1995年欧盟《数据保护指令》（Data Protection Directive, DPD）到2018年《通用数据保护条例》（General Data

〔14〕 凌某某诉北京微播视界科技有限公司隐私权、个人信息权益网络侵权责任纠纷案，北京互联网法院民事判决书（2019）京0491民初6694号。

〔15〕 香港特别行政区诉梁竣杰，高等法院裁判法院上诉案件2016年第49号（HCMA 49/2016）。

〔16〕 Vgl. AG Bad Hersfeld, Beschluss vom 15. Mai 2017-F 120/17 EASO.

〔17〕 See Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 *Washington Law Review* 101, 119 (2004).

〔18〕 蔡培如、王锡铤：《论个人信息保护中的人格保护与经济激励机制》，载《比较法研究》2020年第1期，第108页。

〔19〕 田野：《大数据时代知情同意原则的困境与出路——以生物资料库的个人信息保护为例》，载《法制与社会发展》2018年第6期，第119页。

〔20〕 齐爱民：《信息法原论》，武汉大学出版社2010年版，第58页。

〔21〕 See Volkszählungsurteil, BVerfG 65, 1.

Protection Regulation, GDPR), 均受这一理论的影响。从信息隐私权来看, 美国 1977 年“惠伦案”确立了信息隐私权。⁽²²⁾ 隐私权被认为是个人对其个人信息披露的控制权。⁽²³⁾ 无论是个人信息控制权还是信息隐私权, 均强调信息主体对信息的控制力, 而告知同意被认为是个人信息控制力的核心。⁽²⁴⁾

基于上述逻辑, 有学者进一步认为, 信息主体的访问权、可携带权和收益权等积极权能, 以及更正权、限制或反对处理权和删除权(被遗忘权)等消极权能, 均源于告知同意。⁽²⁵⁾ 这一分析实际上是通过私法角度解读个人信息自决权与信息隐私权, 并在私法上强调个人自主决定的重要性。尤其是在混淆隐私与个人信息保护之时, 极为容易将隐私保护的同意原则套用于个人信息保护之中。此外, 部分学者将同意理解为授权, 通过授权机制又进一步塑造企业数据财产权。⁽²⁶⁾ 甚至有部分学者将个人信息保护中的告知同意与患者知情同意权进行比较。⁽²⁷⁾

同上述理解相左, 个人信息所涵盖的利益多种多样, 是人格利益、财产利益、公共利益的复合。个人信息保护经过数十年的历史发展, 已经与传统私法上的隐私保护相分离, 经过公法上的个人信息保护制度的构建, 最终形成了大数据时代个人信息的复合利益保护结构。无论在欧美还是在我国, 个人信息保护均为公法色彩浓郁的规范。“人口普查案”与“惠伦案”均是经典的宪法案例。我国《民法典》已经意识到, 单纯的私法保护路径较难在个人信息保护方面取得实效, 《民法典》第 1034~1039 条亦不是以任意性规范为主的纯粹私法规范。《草案》更是从新的技术时代出发, 制定于新的制度环境之下, 融合并兼顾了私法和公法的保护路径, 从体系性的角度对于重要的权利提供多维度的保护。

《草案》第 1 条即明确指出, 在保护个人信息权益外, 个人信息保护的至少还包括“规范个人信息处理活动, 保障个人信息依法有序自由流动, 促进个人信息合理利用”。《草案》中的个人信息控制权体系, 亦并不能直接等同于私法上的个人信息权。个人信息保护制度中的告知同意与传统私法上的同意不尽相同, 是一种植根于公法规范的个人信息处理的合法规则。在这个意义上, 方可理解《草案》第 15 条中, 为何立法者对独立作出告知同意的年龄标准采用了 14 周岁这一常见于刑事责任能力的标准, 而没有选择与民事行为能力标准相一致(该条规定有待商榷, 下文将作出分析)。从个人信息保护的多元利益出发, 告知同意能且只能是信息处理的合法情形之一。

(二) 数据保护制度的误读

在制度文本中, 告知同意从来就不是个人信息处理的原则。1980 年, 经济合作与发展组织“数

(22) See *Whalen v. Roe*, 429 U.S.589 (1977).

(23) 张民安:《场所隐私权研究》, 载张民安主编:《场所隐私权研究: 场所隐私权理论的产生、发展、确立和具体适用》, 中山大学出版社 2016 年版, 第 6 页。

(24) 张勇:《APP 个人信息的刑法保护: 以知情同意为视角》, 载《法学》2020 年第 8 期, 第 113 页。

(25) 叶名怡:《论个人信息权的基本范畴》, 载《清华法学》2018 年第 5 期, 第 143 页。

(26) 王雪乔:《论欧盟 GDPR 中个人数据保护与“同意”细分》, 载《政法论坛》2019 年第 4 期, 第 139 页。

(27) 万方:《隐私政策中的告知同意原则及其异化》, 载《法律科学》2019 年第 2 期, 第 62 页。

据保护指导原则”规定了收集限制原则、数据质量原则、目的特定化原则、使用限制原则、安全保护原则、公开原则、个人参与原则、责任原则。1995年，欧盟DPD规定了数据质量原则、数据处理合法原则、敏感数据处理原则、告知当事人原则。2018年，欧盟GDPR规定了合法、公平和透明原则、目的限制原则、最小范围原则、准确性原则、存储限制原则、完整性和保密性原则。这些主流的关于个人信息保护原则的规定中，从未有出现告知同意的原则，即便透明原则或告知当事人原则中涉及了告知的内容，但其并未强调同意，至少在欧盟法中，告知同意一直以来都只是个人信息合法处理的规范之一。

或许就美国法的“公平信息实践原则”(FIPPs)而言，“通知/知情”“选择/同意”“接近/参与”“信息整全/信息安全”“执行/救济”五项内容中，确有契合告知同意的要求，因此极易被误读。但相关要求应被解读为个人信息保护的具体规则而非原则。首先，美国法上的同意，采取的是择出(Opt-out)机制，与作为授权机制的择入(Opt-in)有本质区别。其次，这种同意只是公平信息实现的一种具体方式，且告知同意的要求也不是绝对化的。

从法律原则与法律规则的关系来看，告知同意也不具有原则地位。在内容上，规则是具体明确的，而原则是高度抽象和概括的。告知同意是一项典型的具体制度，其有强同意/弱同意、择入同意/择出同意、特别同意/概括同意的区分，还有动态同意、空白同意、推定同意、单独同意、书面同意等多种类型。在适用范围与适用方式上，告知同意不具有统摄个人信息保护法的地位，只能以“全有或全无”的方式适用，并受个人信息保护原则的约束。告知同意本身决不能称为个人信息保护的“帝王条款”。学界公认的个人信息保护“帝王条款”是“目的限制原则”。⁽²⁸⁾根据GDPR第5条第1款b项的规定，目的限制原则指“基于具体、明确、合法的目的收集个人信息，且随后不得与该目的相悖的方式进行处理”。我国《民法典》第1035条第1条第3项首次规定了目的限制原则的部分内涵，即处理个人信息必须“明示处理信息的目的”。《草案》第6条进一步拓展了《民法典》第1035条第1条第3项的规定，指出“处理个人信息应当具有明确、合理的目的，并应当限于实现处理目的的最小范围，不得进行与处理目的无关的个人信息处理”。这一规定实际上结合了目的限制与数据最小化原则。目的限制作为基础性原则，贯穿了个人信息保护制度始终。即便是主张告知同意具有原则地位的学者，亦无法否认告知同意受目的限制原则的限制。⁽²⁹⁾基于公共利益、履行法定义务、履行合同义务等无须告知同意的信息处理情形，也需要适用目的限制原则。

事实上，在我国的规范体系中，告知同意也只是个人信息处理的具体规则而非原则。《中华人民共和国网络安全法》第41条规定了“合法、正当、必要”的三原则，《民法典》第1035条在此三原则基础上，进一步明确了信息合法处理的要求。《民法典》第1036条更在告知同意以外列明了已公开信息、维护公共利益或信息主体的合法权益的免责情形。就个人信息保护规范体系而言，

(28) 李惠忠：《个人资料保护法上的帝王条款——目的拘束原则》，载《法令月刊》2013年第1期，第37页。

(29) 张新宝：《个人信息收集：告知同意原则适用的限制》，载《比较法研究》2019年第6期，第1页。

《民法典》第 1036 条存在的缺陷在于，一方面将个人信息合法处理情形规定为免责情形，另一方面未能周延地列举个人信息合法处理的具体情形，并将信息是否公开的隐私保护要件不当地引入了个人信息保护范畴。对此，《草案》第 13 条通过 6 项规定较为明确地规定了个人信息合法处理的具体要求，包括告知同意、缔约或履约之必需、履行法定职责或义务之必需、应对公共卫生事件或紧急情况之必需、公共利益实施新闻报道或舆论监督之必需、法律或行政法规所规定的其他情形。6 项规定之间是并列的关系，不能把告知同意与其他条款理解为一般与例外的关系。由此可见，告知同意规则与其他个人信息保护规则一起，在诸多个人信息保护原则的统领下，共同服务于个人信息保护制度体系。

三、告知同意与数据合法处理的规则构造

有学者将当前学界所提出的应对告知同意困境的方式概括为“放宽同意的要求和形式”“降低告知的约束力”“用风险规则置换同意规则”⁽³⁰⁾，然而，前两种路径，都是从告知同意本身出发所提出的，未能完全把握个人信息保护制度中告知同意与其他规则的互动关系。风险规则的路径，又试图完全脱离告知同意，从而出现了忽略个人人格尊严保护，并难以有效约束“隐私政策”野蛮生长的问题。因此，在明晰告知同意的法律地位后，告知同意困境的最佳应对策略应为：一方面，在告知同意机制的内部改造中细化告知同意规则，以格式合同规范约束“隐私政策”；另一方面，充分把握告知同意与其他规则互动的关系，确立数据流通规则体系，引入个人信息保护设计。

(一) 细化告知同意规则

就告知与同意的关系而言，我国应坚持择入机制。在择入机制中告知是前提和起点。在择出机制中，实际上没有告知也不存在同意，因此也被认为“以‘默示同意’为幌子，实际则背离了知情同意”。⁽³¹⁾同时，我国个人信息立法以移植欧盟相关规定为主，又对截然不同的美国制度进行交叉引入，必将导致体系性混乱。在择入机制的基本架构下，《草案》的告知同意规则应进行更为精细化的调整和完善。

第一，《草案》第 14 条规定了同意的实质要件为“特定、明确、自愿”，并在一般的同意规则外又指出了单独同意和书面同意的特殊规定，然而，几种同意形式在《草案》中体系混乱、关系不明。首先，书面同意可以删除。《草案》仅在第 30 条规定了“法律、行政法规规定处理敏感个人信息应当取得书面同意的，从其规定”。其实，仅在此处强调同意的要式并无必要。其次，应对单独同意与一般同意作进一步释义和区分。《草案》规定，向第三方提供个人信息时（第 24 条）、公开其处理的个人信息时（第 26 条）、处理敏感个人信息时（第 30 条）、个人信息跨境时（第 39 条）需要取得单独同意。由此可见，单独同意对应的特殊的个人信息处理情形，伴随有特殊的个

(30) 蔡培如、王锡铨：《论个人信息保护中的人格保护与经济激励机制》，载《比较法研究》2020 年第 1 期，第 107-108 页。

(31) 郑佳宁：《知情同意原则在信息采集中的适用与规则构建》，载《东方法学》2020 年第 2 期，第 202 页。

人信息告知要求。因此，单独同意实际上属于一种特别同意，即要求将一切信息和可能风险告知信息主体，在“特定、明确、自愿”的基础上，取得信息主体具体同意。而一般同意应理解为概括同意，虽然也要求“特定、明确、自愿”，但并不一定针对一个具体的事项，可以是针对将来信息处理行为概括的、一揽子的同意。

第二，《草案》第18条是对第7条透明原则的具体化。该条第1款规定了“个人信息处理者在处理个人信息前，应当以显著方式、清晰易懂的语言向个人告知”的4个事项。前3个事项详细列举了告知的一般内容，第4项兜底性规定链接到向合并分立时的告知要求（第23条）、第三方提供个人信息时的告知要求（第24条）、敏感信息处理的必要性及对个人影响的告知要求（第31条）、数据跨境时的告知要求（第39条）等。该条总体上对告知规则进行了较为完善的规定。值得注意的是，由于《草案》第15条将14周岁规定为作出同意的年龄要求，因此“显著方式、清晰易懂的语言”在针对未成年人之时应有更高的标准与要求。同时，《草案》第18条第2款仅规定“应当将变更部分告知个人”，实际上变更部分的告知方式也必须是“显著方式、清晰易懂的语言”（第1款）以及“便于查阅和保存”（第3款）。

第三，《草案》第25条规定了自动化决策权，同时隐含了算法解释权的内容，规定了“个人认为自动化决策对其权益造成重大影响的，有权要求个人信息处理者予以说明”。然而，信息处理者的说明义务对应的是客观的重大影响，而非信息主体主观认识的重大影响。实际上，《草案》在个人信息风险评估中的重大影响（第54条第1款第5项）、已公开的个人信息对个人的重大影响（第28条第2款）等规定中的“重大影响”均是客观的标准。因此，建议将“个人认为”删除，否则将造成说明义务适用前提不明；同时，对于“予以说明”的内容应进一步明确。此时的说明，并不要求公开自动化决策算法的内部机制，只应限于算法逻辑的说明。参照欧盟《监管目的的自动化个人决策和分析指南》规定，信息处理者只需要根据“若非A则无B”的反事实，以一个“没有受过教育的门外汉”能理解的标准，通过简洁、透明、易懂和容易取得的形式进行解释。

（二）以合同法进行解读

虽然个人信息保护法属于公法色彩浓郁的法律，但亦无可否认其在属性上兼具私法色彩，属于领域法的范畴。因此，私法规范，尤其是合同法的相关规范，应与个人信息保护制度有机互动。在告知同意上，《草案》第14条将同意界定为意思表示，也就是说，在私法的角度，“隐私政策”应认定为合同。虽然，平台规则的成立与生效受《中华人民共和国电子商务法》的特殊规制，但并不能否认“隐私政策”是平等主体之间通过意思表示一致达成的协议，经用户点击承诺后即成立。从合同法的角度，可对《草案》作进一步解读。

第一，《草案》第15条似乎有两种解释的可能：一是以14周岁为标准界定同意的年龄标准；二是强调了信息处理者注意相对方年龄的义务，在相对方未满14周岁时要求取得监护人同意。即便是采取后一种文义解释，也必将引申出同意年龄标准的问题。虽然，《草案》并非私法，但为了与《草案》第14条的规定相一致，同意的行为能力标准也应与民事行为能力标准相一致，也唯有

如此,《草案》才能与《民法典》相关个人信息保护规范相衔接。

第二,《草案》第16条规定了信息主体对同意具有撤回权,但此处的撤回不宜简单理解为意思表示的撤回,否则根据法律行为理论,意思表示合法撤回后,合意不复存在,合同自始无效,进而使得信息处理者对于撤回前信息处理的合法性基础不复存在,这显然不合常理。因此,此处的撤回应理解为赋予信息主体任意解除权。由于该条将撤回的前提限于基于告知同意的信息处理,其充分为了保护信息主体的人格利益,因此不应对任意解除附加以其他限制条件。对于信息主体撤回同意的法律后果而言,对应的是不得继续处理相关个人信息以及相关信息的删除,然而,根据《草案》第47条第1款第3项的规定,信息主体撤回同意只是信息主体申请删除个人信息的条件之一,也就是说,信息主体需要在撤回同意后另行申请才能行使删除权。这一规定并不符合撤回的法律属性。撤回后合法解除,信息处理者依法处理个人信息的基础已经不复存在,而存储也属于《草案》规定的个人信息处理行为,因此个人信息处理者必须主动删除相关信息,无须信息主体另行请求删除。

第三,《草案》第17条明确规定了企业不得以个人不同意或撤回同意为由拒绝提供产品或者服务,实际上这是对格式合同规则的落实。若收集处理个人信息与相关产品或服务并不相关,基于格式条款的个人信息收集就属于《民法典》第497条所规定的无效条款。例如,曾有一款手电筒App,试图通过“隐私政策”大量收集包括地理位置、通讯录、通话记录等信息,但其唯一功能就是打开手机闪光灯。显然这类格式条款因不合理、不公平、侵害个人信息权益而无效。同时,大量的App在人们日常生活中具有了越来越重要的影响,甚至与政府公共服务相捆绑。此时,就需要贯彻目的限制原则,探寻其信息收集的必要性。通过这一方式,该条确保了个人免于被“霸王条款”所绑架。

第四,《草案》第18条告知的内容在性质上属于“与对方有重大利害关系的条款”。根据格式条款规则,应从提示的时间与提示的方式两个方面进行判断相关告知是否达到《民法典》第496条第2款中所要求的“合理”程度,以及《中华人民共和国消费者权益保护法》第26条第1款所要求的“显著”程度。此外,应着重根据个人信息保护的相关规范,审查相关条款是否符合个人信息的保护原则与处理规则,并据以否定侵害个人权益条款的有效性,以此合同法手段,有效回应不合理、不公平、侵害个人信息权益的“霸王条款”问题。

(三) 确立数据流通规则体系

不少学者已经注意到,个人信息保护应采取激励相容的模式,不可“简单施加各种禁止性或者强制性规定”。^[32]在财产规则外,引入管制规则与责任规则,“以多种类的技术监督机制以消弭权利配置进路的负外部性”。^[33]事实上,无论是激励相容抑或法经济学规则菜单的理论,均基于

[32] 周汉华:《探索激励相容的个人信息治理之道——中国个人信息保护法的立法方向》,载《法学研究》2018年第2期,第3页。

[33] 丁晓强:《个人数据保护中同意规则的“扬”与“抑”——卡-梅框架视域下的规则配置研究》,载《法学评论》2020年第4期,第130页。

数据流通规则体系的构建，鼓励数据依法自由流动。就此而言，《草案》第13条在参考GDPR相关规定的基礎上，在告知同意外，规定了5种合法的个人信息处理情形，大大拓展了《民法典》第1036条告知同意外的两项免责事由，然而，这一规定仍有缺陷。一方面，数据流通规则未能贯穿《草案》始终，第13条往后的大量条文仍以告知同意为主。建议《草案》必须在坚持该条规定的基礎上，进一步明确承认信息处理者对数据的合法权益依法受到保护，并辅以相应的责任规则，构建从个人信息合法处理到数据合法利用的数据流通规则体系，发挥《个人信息保护法》在培育数据要素市场中的积极作用。另一方面，必须明确，数据流通规则必须受个人信息保护基本原则的约束。对于《草案》第13条第2~4项之中的“所必需”以及第5项之中的“合理的范围”应有一定的判定基准。欧盟“第29条工作组”即曾经提出数据流通规则的衡量标准，参照这一标准，对5种情形的解释必须考虑信息处理者的合法利益、对信息主体的影响、义务的平衡、额外的保障措施。⁽³⁴⁾

第一，《草案》第13条第2项规定了订立或者履行信息主体作为相对人一方的合同所必需的情形。首先，可以预计该项将成为绝大多数业务场景下收集信息的依据。因此，其必须受目的限制原则的约束，不得利用这一条款进行个性化营销。其次，从文本来看，该款对第三人不得适用，然而，涉及代理人时，虽然代理人是其所代理的合同关系中的第三人，但采集代理人的个人信息却又是必要的。此外，对个人信息处理者而言，也难以仅将其限缩至合同相对方的范畴。许多时候，关联方处理信息确实是履约所必需的。例如，某人在B平台办理了一张A品牌的会员卡，实际上每一个品牌分销商、加盟店都是独立的法人，若限于缔约主体的独立法人地位，将使得会员卡实际无法使用。因此，建议适当扩大该项范畴，涵盖代理人的信息，同时在确有必要时允许关联方使用相关信息。最后，必须解决《草案》其他条文与该项的矛盾与冲突。如《草案》第17条关于企业不得以个人不同意或撤回同意为由拒绝提供产品或者服务的規定中，指出“处理个人信息属于提供产品或者服务所必需的除外”。这一规定，在表述上容易得出提供服务所必需的情形也需要告知同意，仅仅是此时信息处理者可拒绝提供服务而已。然而，根据第13条第2项，此时已与同意无关。又如，《草案》第24条向第三方提供信息时单独同意的要求似乎是绝对的，但如前述在向关联方转移信息的事例中，确有为履行与信息主体作为相对人一方的合同之必要的情形。

第二，《草案》第13条第4项规定了应对公共卫生事件或紧急情况下为维护信息主体利益所必需的情形。或许有观点会认为，部分措施并非紧急，却与信息主体重大利益密切相关，如反欺诈措施、支付安全措施等。因此，不宜将维护信息主体利益所必需的情形限制在紧急情况之中。此观点实际上忽视了这些措施多已是信息处理者的法律职责或法定义务，可直接适用《草案》第13条第3项，无须在此处体现。紧急情况的限制确有必要。此条款与《草案》第19条相对应，必须有相应的回复机制。根据《草案》第19条第2款的规定，在紧急情况消除后，信息处理者必

(34) WP29, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP217 (2014).

须对信息主体履行告知义务。同时，应进一步明确由于紧急情况已经消除，应使用告知同意规则，在获得同意后方可继续处理相关信息。虽然公共卫生事件在此条文中予以单列，但实际上也属于特殊的紧急情况，事后亦应履行告知义务。

第三，《草案》第13条第5项规定了“为公共利益实施新闻报道、舆论监督等行为在合理的范围内处理个人信息”的情形。对该项的“等”的解释将直接决定该项的适用范围。若作“等内等”理解，则该项为针对新闻报道的规定；若作“等外等”的解释，该项可作公共利益的扩大解释。以公共利益的必要性作为考量，对个人信息进行处理的情形至少包括“监控疫情和人道主义救援、确保网络和信息安全、基于劳动和社会保障目的、维护公共健康、新闻和文学艺术创作自由、科学研究等”。^{〔35〕}为了与其他基于公共利益的信息流通规则相协调，该款中的等亦作“等外等”解释，同时建议进一步丰富列明公共利益的具体内容。在这个意义上，可进一步理解《草案》第27条关于公共场所监控的规定。该条规定，将公共场所监控限制在“为维护公共安全所必需”的情形，实际上已排除了告知同意规则的适用。因此，“设置显著的提示标识”的要求并不能简单理解为告知，亦无须信息主体同意才能进行信息处理。此外，回到《草案》第13条第5项，该项规定公共利益必须受“合理的范围”的约束。“合理的范围”并不等于“所必需”。以该项所指向的新闻报道为例，实难以说明信息处理是必须的，若以必须为逻辑，记者大可不报道相关信息。因此，对于涉及公共利益的信息利用而言，其适用的是比必要性更为宽松的合理性要件。新闻报道若涉及家庭地址、人肉搜索等便是超出了合理范围。

（四）引入个人信息保护设计

设计本身就是权力，设计通过代码决定了用户的行为。“程序员是一个宇宙的创造者，他自身也是其中唯一的立法者。无论是多么有权势的剧作家、舞台剧导演或皇帝，也不曾行使过如此绝对的权力来安排一个舞台或战场，并指挥如此坚定不移尽职尽责的演员或军队。”^{〔36〕}为了更有效地回应告知同意的困境，必须通过技术架构的挑战，以保护个人信息。根据助推理论，技术架构的设计可改变人们的行为。^{〔37〕}通过设计保护个人信息，将个人信息保护前置到产品设计环节，通过将个人信息保护融入默认设置、具体设计之中，以实现端对端的安全。这一概念的倡导者卡沃基安（Ann Cavoukian）提出，个人信息保护应自动而非被动、预防而非补偿；注重设计与默认设置；实现多方利益、价值共存，端对端安全，可见性和透明性，以用户个人信息为中心的产品设计。^{〔38〕}也就是说，个人信息保护设计是一种前置性的、预防性的保护手段，其不以告知同意为

〔35〕 丁晓强：《个人数据保护中同意规则的“扬”与“抑”——卡-梅框架视域下的规则配置研究》，载《法学评论》2020年第4期，第141页。

〔36〕 [德] 托马斯·威斯迈耶、[德] 蒂莫·拉德马赫编：《人工智能与法律的对话2》，韩旭至、李辉等译，上海人民出版社2020年版，第195-196页。

〔37〕 贾浩然：《助推及其对技术设计的启示》，载《自然辩证法研究》2018年第6期，第44页。

〔38〕 See Paolo Balboni & Milda Macenaite, *Privacy by Design and Anonymisation Techniques in Action: Case Study of Match Technology*, 29 Computer Law & Security Review 330 (2013).

基础。

遗憾的是,《草案》缺乏关于个人信息保护设计的规定。实际上,由于设计的重要性,法律对产品设计的关注并不少见。汽车设计中就有关于安全带、安全气囊、倒车镜等各种设计的标准,未满足相关标准的产品将不被允许上路。参照 GDPR 第 25 条的规定,个人信息保护设计应结合科技发展水平、标准实施成本以及个人信息处理行为的性质、范围、环境和目的进行规范,并确保在默认设置中,个人信息受到适当保护。在具体的措施上,可借鉴哈托格(Woodrow Hartzog)个人信息保护设计的回应模式,明确禁止欺骗性的设计与存在危险的设计,辅之以一定的设计标准和规范,对违反设计规范的企业作出一定处罚,以个人信息保护设计,回应告知同意的失灵。⁽³⁹⁾唯有将个人信息保护前置到产品设计之中,才能从根本上解决隐私政策的功能危机。

四、结语

当前,我国虽然尚未颁布《个人信息保护法》,但通过近年来《刑法》《网络安全法》《民法典》等法律中的相关制度,已经初步形成了具有中国特色、适应时代发展的个人信息保护制度体系。《个人信息保护法》的出台,应在我国既有的制度资源基础上,把握基础理论命题,回应数据时代的发展需要。其中,告知同意作为个人信息保护的一项具体规则,连接着公法与私法的相关规范,具有重要作用。明晰告知同意的规则地位,并非完全否定告知同意规则本身,而是应从个人信息保护规则体系出发,进一步理顺告知同意与其他个人信息合法处理规则的关系,正面回应告知同意的现实困境,更好地构建个人信息保护制度体系。

The Dilemma and Solution of Informed-consent Rule in Personal Information Protection—On the Relevant Provisions of the Personal Information Protection Law (Draft)

HAN Xuzhi

Abstract: Personal information protection based on the principle of informed-consent will inevitably face many difficulties. It is difficult for the data subject to read “privacy policy” and to exercise the right of rejection. It is difficult for the data processor to obtain effective consent in big data processing. As an accountability mechanism, informed-consent still cannot achieve its effectiveness. The informed-consent mechanism is derived from the theory of personal information

(39) See Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies*, Harvard University Press, 2018, p.157–193.

self-determination and privacy rights. However, from the perspective of private law, equating consent with authorization is a misunderstanding of the public law nature of the personal information protection system. In personal information protection system, informed-consent has never been a basic principle, but one of the specific rules. China's personal information protection legislation must properly manage the relationship between informed-consent and other data processing rules. On the one hand, the law needs to further refine the informed-consent rule, and restrict "privacy policy" with contract law. On the other hand, the law needs to establish data circulation rules, and introduce "Privacy by Design".

Keywords: Personal Information Protection; Informed-consent Mechanism; Right of Personal Information Self-determination; Data Circulation Rules; Data Utilization

(责任编辑: 张欣 汪友年)