

论反洗钱义务履行中的 个人信息处理*

许 可

【摘 要】为履行反洗钱义务而处理个人信息，是《个人信息保护法》第13条所规定的“为履行法定职责或者法定义务所必需”而处理个人信息的典型应用场景。反洗钱中的个人信息处理无需取得个人同意，但对个人信息的收集范围及处理活动应与反洗钱目的直接相关，并应最小化对个人权益的影响。为应对金融数字化转型的挑战，《反洗钱法》需适时修改，在强化保障个人知情权、查阅权、更正权和获得救济权的前提下，为以履行反洗钱义务为目的的个人信息共享提供便利，从而实现个人信息保护与合理利用的再平衡。

【关键词】法定义务 反洗钱 个人信息 共享

【作者简介】许可，法学博士，对外经济贸易大学法学院副教授。

【中图分类号】D923 **【文献标识码】**A

【文章编号】2097-1125 (2022) 05-0005-13

作为我国个人信息保护的专门立法，《中华人民共和国个人信息保护法》（以下简称《个人信息保护法》）突破了之前《中华人民共和国网络安全法》（以下简称《网络安全法》）和《中华人民共和国民法典》（以下简称《民法典》）中将“个人同意”作为唯一合法处理个人信息事由的基础法律框架，其第13条首次将“为履行法定职责或者法定义务所必需”列为个人信息处理的合法性事由之一，从而与“为订立、履行个人作为一方当事人的合同所必需，或者按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需”“为应对突发公共卫生事件，或者紧急情况下为保

* 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”（21ZDA050）、教育部哲学社会科学研究重大课题攻关项目“科学构建数据治理体系研究”（21JZD036）的阶段性成果。

护自然人的生命健康和财产安全所必需”“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”“依照本法规定在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息”等多种合法性事由一起，构成了我国个人信息合法使用的伞形架构。不过，如何理解“为履行法定义务所必需”的个人信息处理，理论界与实务界依然未臻明确。作为履行法定义务的典型情形，“反洗钱义务履行”不但事关金融安全，而且攸关个人信息权益。值此《中华人民共和国反洗钱法》（以下简称《反洗钱法》）修改的关键时刻，本文聚焦于反洗钱义务履行中的个人信息处理活动，以期厘清《个人信息保护法》相关规则的适用，并有裨于《反洗钱法》的完善。

一、反洗钱中个人信息处理的“法定性”

（一）“履行法定义务”的识别

准确界定“法定义务”之“法”的范围，是识别《个人信息保护法》中“为履行法定义务处理个人信息”的关键。对此，可从“任意性规定和强制性规定的语词分析”“公法规范和私法规范的公/私分析”“法律、法规、规章、规范性文件的位阶分析”三方面逐一展开。^①首先，这里的“法”是强制性地调整当事人之间的法律关系，当事人无法排除或变更的“强制性规范”。在文字表达上，强制性规范一般使用“应当”“必须”“不得”“禁止”等词语，但存在两种例外：一者含有相关词语的规范未必是强制性的，而仅是提倡和诱导当事人采用特定行为模式的“倡导性规范”；^②二者有些规范亦未必以上述词语来宣示，其强制性可通过揭示违反后果，或在一定条件下以许可的方式加以表达。^③因此，究竟是否系“强制性规范”，有必要从法律效果来判断。其次，从“义务违反、责任承担”的逻辑出发，只要能引发国家机关认定并归结于行为主体的、带有直接强制性责任的规范，即可属之。故此，这里的“法”来自公法规范，而非私法规范，更不是当事人对权利义务的“意定”。这是因为私法的强制性规范仅仅涉及个人信息处理者的权限和法律行为的效果，其内容已经被“为订立、履行个人作为一方当事人的合同所必需”的情形所吸收。最后，这里的“法”在位阶上是否限于“法律、行政法规”，仍待探明。在《民法典》第

^① 参见许可：《劳动合同的自治与规制——以“违反强制性规定的劳动合同”为中心》，《法学家》2017年第2期，第60~61页。

^② 参见王轶：《论倡导性规范——以合同法为背景的分析》，《清华法学》2007年第1期，第66页。

^③ 参见黄立：《民法总则》，中国政法大学出版社2002年版，第328~329页。

143 条第 3 项中，为避免公权力对当事人自由的不当干涉，充分尊重意思自治，可能导致法律行为无效的“法”之位阶被提升到“法律、行政法规”，排除了“地方性法规、部门规章和规范性文件”。与之异曲同工，《个人信息保护法》为避免个人信息权益被随意克减或个人信息处理者的义务被不当苛加，条文中也多次使用“法律、行政法规”的表述。然则，这里的“法”是否应采狭义解释？如欲回答这一问题，还有待进一步辨明“为履行法定义务所必需处理个人信息”的规范目的。

从体系视角观察，“履行法定义务”系个人信息处理的合法性事由之一，而非对个人信息权益的减损。在全球数字化转型的背景下，个人“数据人格”、企业“数据资产”和国家“数据资源”的重要意义与日俱增，《个人信息保护法》第 1 条开宗明义，将“保护个人信息权益”“促进个人信息合理利用”作为二元并置的立法目标。基于此，作为《个人信息保护法》“法眼”的第 13 条，在根本上改变了《民法典》“个人同意+特定免责”的个人信息使用模式，转向融知情同意在内的多元合理事由模式，以熨帖个人信息之上所承载的个人权益、企业利益、公共秩序、社会福祉、国家安全等多种价值追求。在多种价值追求中，“为履行法定义务所必需”系个人信息公共利益的具体化。个人信息并非个人所能“拥有”，作为非排他性和非竞争性之物，个体利益必须始终与公共利益相平衡。因此，《民法典》第 1036 条将“为维护公共利益或者该自然人合法权益，合理实施的其他行为”作为个人信息处理的免责事由。鉴于“公共利益”的含义过于宽泛，《个人信息保护法》第 13 条用列举的方式将之细化，分别是：（1）为履行法定职责或者法定义务所必需；（2）为应对突发公共卫生事件，或者紧急情况下为保护自然人的生命健康和财产安全所必需；（3）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。

基于上述体系定位及维护公共利益的目的，“履行法定义务”中“法”的范围应合理拓展，无须限定于“法律、行政法规”。循此，这里的“法”应采广义，不仅将法律、行政法规、地方性法规、部门规章、地方政府规章等规范性法律文件均囊括其中，^① 还包括国家机关在具体案件中作出的具有约束力的行政决定。^② 从比较法上看，该思路与欧盟《一般数据保护条例》（General Data Protection Regulation, GDPR）一脉相承。GDPR 第 6 条和第 23 条，将个人数据处理合法性基础规则与个人数据权利限制规则相互区隔，并

^① 参见程啸：《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。

^② Christopher Kuner, Lee A. Bygrave and Christopher Docksey et al., *The EU General Data Protection Regulation (GDPR): A Commentary*, New York: Oxford University Press, 2020, p. 333.

在“序言”第41条申明：法定义务的法律依据并不必须为一部议会通过的法律，但其适用对于相关主体来说应当是可预见的，并符合欧洲法院和欧洲人权法院判例法。此外，还需要说明的是，为了避免国家机关任意扩大个人信息处理的场景，规章和其他规范性文件应依法制定并已公开，其立法目的和规则还不得与上位法律、行政法规相抵触。

（二）作为“法定义务”的反洗钱

所谓洗钱，意指掩饰、隐瞒犯罪所得及其收益的来源和性质，并伪装成合法所得的行为。与之相反，反洗钱是指为了预防洗钱活动、遏制违法犯罪活动而采取相关措施的活动和过程。^①

反洗钱义务与公共利益密切相关，因而可归入《民法典》第1036条“为维护公共利益而处理个人信息”的情形。洗钱活动会对社会和经济造成显著的负面影响，包括但不限于：（1）洗钱使贩毒、抢劫等犯罪收入合法化，间接激励犯罪行为；（2）洗钱会损害金融机构自身声誉和客户信任，引发信用危机和支付危机；（3）洗钱活动中快速、异常、大额的资金转移，将危害资金的流动性和可偿付性，最终危及金融业安全；（4）洗钱会改变正常的货币行为，影响经济数据、宏观经济分析和政策制定；（5）洗钱会腐蚀经济和社会体系，带来巨大的社会和政治成本，削弱集体道德标准和民主制度。^②正因如此，打击洗钱已经成为世界各国的普遍共识。

同时，反洗钱义务亦是我国法律所明确的法定义务。从2003年中国人民银行发布《金融机构反洗钱规定》，到2006年《反洗钱法》和2015年《反恐怖主义法》的颁布，我国反洗钱规则的法律位阶不断提升，义务主体不断拓展，规范内容也日益丰富，以金融机构为核心、以非金融机构为辅助，贯穿支付结算业务全流程的反洗钱义务架构已初步建立。近年来，《金融机构大额交易和可疑交易报告管理办法》《支付机构反洗钱和反恐怖融资管理办法》《中国人民银行办公厅关于加强特定非金融机构反洗钱监管工作的通知》《互联网金融从业机构反洗钱和反恐怖融资管理办法（试行）》《法人金融机构洗钱和恐怖融资风险管理指引（试行）》《金融机构客户尽职调查和客户身份资料及交易记录保存管理办法》等部门规章和规范性文件的陆续出台，进一步扩展、细化了反洗钱义务的法律要求。

（三）反洗钱中个人信息处理的合法性

当前，反洗钱规制采取“双轨制”框架：一是洗钱定罪化和严厉处罚的“压制策略”（repressive measures）；二是基于金融信息调查的“预防措

① 本文中“反洗钱”是指“反洗钱”和“反恐怖主义融资”的统称。

② 参见 John McDowell and Gary Novis, *The Consequences of Money Laundering and Financial Crime, Economic Perspectives*, Vol. 6 (2), 2001, pp. 7-8。

施” (preventive measures)。^① 随着洗钱活动的复杂化和手段的多样化，通过金融信息来确定隐匿资产的位置、确定犯罪分子和犯罪组织的“反洗钱预防措施”日益重要。2003年《联合国反腐败公约》第14、52条列举出如下“反洗钱预防措施”：(1) 验证客户身份；(2) 视情况验证实际受益人身份；(3) 保持纪录；(4) 报告可疑交易；(5) 对正在或者曾经担任重要公职的个人及其家庭成员和与其关系密切的人或其代理人的账户强化审查。根据《个人信息保护法》第4条关于个人信息关联的认定标准，只要“反洗钱义务人”（金融机构和特定非金融机构）已经或可以识别特定自然人，那么与上述反洗钱预防措施相关的客户信息（不论是客户本人的信息，还是客户受益人信息；不论是身份信息，还是交易信息），均属于《个人信息保护法》中的“个人信息”。正是由于反洗钱预防措施与个人信息处理活动密不可分，履行反洗钱义务才成为处理个人信息的合法性基础。

基于“履行法定义务”的合法性事由，反洗钱义务人因履行反洗钱义务而处理个人信息时，不但无需获得个人同意，而且不应取得个人同意。这是因为，基于个人同意的个人信息处理须受制于个人的删除权以及自动化决策的拒绝权，由此可能引发个人恶意删除其不良信息和可疑交易信息，操纵其人物和交易画像 (profiling)，进而引发规避法律和危害公共秩序的不良后果。更重要的是，在各个合法性事由相互独立的架构下，反洗钱义务人不得在不同合法性事由之间随意转换，一旦个人撤回同意，则将无法另外以“履行法定义务”为由继续处理之前收集的个人信息，从而陷入两面违法的窘境。

二、反洗钱中个人信息处理的“必要原则”

(一) “必需”作为履行法定义务处理个人信息的限制

为履行法定义务而处理个人信息并非没有限制，《个人信息保护法》第13条特别将“所必需”作为其前提，以落实第5条所规定的“个人信息处理的必要原则”。自2012年《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》颁布以来，“必要性原则”一直是我国个人信息处理的核心原则之一。这里的“必要性”并不意味着“必不可少” (essential)，而是指“个人信息处理”应与“处理目的”之间具有合理关联。《个人信息保护法》第6条将之界定为：“处理个人信息应当具有明确、合理的目的，并应当与

^① 参见 Stefan D. Haigner, Friedrich Schneider and Florian Wakolbinger, Combating Money Laundering and the Financing of Terrorism: A Survey, https://www.econstor.eu/bitstream/10419/119391/1/diw_econsec0065.pdf, 2022年4月6日。

处理目的直接相关，采取对个人权益影响最小的方式。收集个人信息，应当限于实现处理目的的最小范围，不得过度收集个人信息。”据此，我们可以将“履行法定义务所必需”分解为三个环环相扣的内容：（1）个人信息收集范围与法定义务之目的直接相关；（2）个人信息处理活动与法定义务之目的直接相关；（3）个人信息处理活动应最小化对个人权益的影响。^①

（二）个人信息收集范围应与反洗钱目的直接相关

履行反洗钱义务的关键在于识别、评估、了解洗钱风险，以提升反洗钱的有效性。由此，“了解你的客户”（know your customer）构成了反洗钱“预防措施”的核心，反洗钱金融特别工作组（Financial Action Task Force, FATF）在《打击洗钱、恐怖融资、扩散融资国际标准：FATF 建议》进一步将其提升为“客户尽职调查”（customer due diligence）义务，旨在：（1）识别客户身份，并使用可靠且来源独立的文件、数据或信息核实客户身份；（2）识别受益所有人身份，并采取合理措施核实受益所有人身份，使金融机构确信其了解受益所有人；（3）了解并酌情获取关于建立业务关系的目的和真实意图的信息；（4）确保正在进行的交易与金融机构所掌握的客户资料、客户业务、风险状况（必要时，包括资金来源）等信息吻合。^②在我国法律中，履行反洗钱义务收集的个人信息包括如下内容。

其一，个人身份信息。根据《反洗钱法》第3、16条，反洗钱义务人需要依法识别客户身份并在法律规定的范围内留存相应的证明材料，例如客户的身份证明文件、客户代理人或被代理人的身份证明文件、保险或信托业务中合同受益人的身份证明文件等。

其二，个人交易信息。根据中国人民银行、中国银行保险监督管理委员会、中国证券监督管理委员会颁布的《金融机构客户尽职调查和客户身份资料及交易记录保存管理办法》第44条，交易信息包括但不限于：每笔交易的数据信息、业务凭证、账簿以及有关规定要求的反映交易真实情况的合同、业务凭证、单据、业务函件和其他资料。根据中国人民银行、国家外汇管理局颁布的《银行跨境业务反洗钱和反恐怖融资工作指引（试行）》第8条的规定，在办理跨境业务的准入和存续期间，金融机构还应收集客户在监管部门和银行的违规记录、不良信用记录等；客户经营状况、股东或实际控

^① 参见朱悦：《技术与市场之间——试论个人信息最小化原则的理解和适用》，《经贸法律评论》2021年第6期，第20页。

^② 参见 Financial Action Task Force on Money Laundering (FATF): International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, <https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf>, 2022年3月21日。

制人、受益所有人、主要关联企业与交易对手、信用记录、财务指标、资金来源和用途、建立业务关系的意图和性质、交易意图及逻辑、涉外经营和跨境收支行为、是否为政治人物等。根据《住房和城乡建设部、人民银行、银监会关于规范购房融资和加强反洗钱工作的通知》及《中国人民银行关于加强贵金属交易场所反洗钱和反恐怖融资工作的通知》的相关规定，在房地产交易、贵金属交易等非金融领域的交易中，金融机构还应当了解客户及其交易目的和交易性质、资金来源和性质以及实际控制客户的自然人和交易的实际受益人，同时还要保证留存资料能够完整准确重现每笔交易。^①

（二）个人信息处理活动应与反洗钱目的直接相关

在履行法定义务时，法定的“个人信息处理活动”是其必要性的当然之基。在我国法律中，基于反洗钱目的的个人信息处理包括如下内容。（1）个人信息收集：为了有效识别客户并做出风险评估，反洗钱义务人必须遵循“了解你的客户”原则，收集客户身份信息和交易信息。（2）个人信息保存和更新：反洗钱义务人应妥善保存客户身份资料和交易记录，保存期限不少于5年；在业务关系存续期间，反洗钱义务人应当及时更新客户身份资料并持续识别客户。（3）个人信息保密：反洗钱义务人对获得的客户身份资料和交易信息负有保密职责，非依法律规定不得对外提供。（4）个人信息报送：反洗钱义务人办理的单笔交易、在规定期限内的累计交易超过规定金额或者发现可疑交易的，应当及时向反洗钱信息中心报告。（5）个人信息共享：包括“集团内部信息共享”和“金融机构与非银行支付机构之间的信息共享”。一方面，根据2021年《银行跨境业务反洗钱和反恐怖融资工作指引（试行）》、2018年《法人金融机构洗钱和恐怖融资风险管理指引（试行）》的相关规定，金融机构应当建立内部信息共享制度和程序，对于高风险客户或高风险业务，银行可通过系统内部共享信息查证客户提供的真实性证明材料。另一方面，2018年《中国人民银行关于非银行支付机构开展大额交易报告工作有关要求的通知》要求，为履行大额交易报告义务，非银行支付机构与银行机构彼此应当提供完整、准确、及时的客户身份信息和交易信息，持续完善资金上下游链条信息。（6）个人信息移交：金融机构破产和解散时，应当将客户身份资料和客户交易信息以及包含上述信息的电子载体移交国务院有关部门指定的机构。

（三）反洗钱中个人信息处理应最小化对个人权益的影响

“最小化对个人权益的影响”意味着反洗钱义务人在个人信息的收集、存

^① 参见《住房和城乡建设部、人民银行、银监会关于规范购房融资和加强反洗钱工作的通知》第4条、《中国人民银行关于加强贵金属交易场所反洗钱和反恐怖融资工作的通知》第2条。

储、使用等具体行为中，应审慎评估其信息处理方式，并采取必要手段，尽可能降低信息处理风险，满足个人的合理预期。^①为此，在履行反洗钱义务处理个人信息时，应当贯彻“风险为本”进路（risk based approach），在治理科技的架构下，通过“合规科技”和“赋能科技”最小化对个人权益的可能侵害。^②

其一，“风险为本”作为反洗钱和个人信息保护的共通原则。自2006年沃尔夫斯堡集团（Wolfsberg Group）发布《风险为本的反洗钱方法指引》（Guidance on a Risk Based Approach for Managing Money Laundering Risks）确立“风险为本”的反洗钱原则以来，从“规则为本”转向“风险为本”已成为全球反洗钱体系发展方向，其要求反洗钱义务人科学、准确地评估洗钱风险，使洗钱风险程度与处置措施相称、处置成本与收益相称、处置方法和效率相称。^③与之类似，从国际经验观察，个人信息保护亦将“风险为本”的理念贯穿于个人信息处理全过程，从识别风险、评估风险到基于风险的应对措施，形成了持续性反馈循环。^④我国《个人信息保护法》总体上借鉴了“风险为本”进路的理念，^⑤并将其细化为个人信息分类、个人信息处理影响评估、个人信息安全义务等不同制度。“风险为本”在两大领域的耦合，使得反洗钱个人信息处理活动应综合考量客户洗钱风险、个人信息处理风险及其对个人权益损害的风险，采取三者相适应的法律规则。2022年颁布的《金融机构客户尽职调查和客户身份资料及交易记录保存管理办法》即以“风险为本”为准绳，结合客户特征、业务关系、交易目的和性质，采取与风险相匹配的一般尽职调查、简化尽职调查措施或强化尽职调查，以收集和处理不同范围的个人信息。

其二，“个人信息保护影响评估”作为合规科技的核心措施。鉴于反洗钱中的个人信息一般包含“金融账户、生物识别”等敏感个人信息，同时其处理结果可能引致实质性法律后果，反洗钱义务人应践行《个人信息保护法》第55条规定的“个人信息保护影响评估”义务，通过评估反洗钱中个人信息处理活动是否合法、正当、必要及其对个人权益的影响和安全风险，

① 参见刘忠炫：《个人信息处理的合理限度——基于必要性原则的场景化分析》，《上海政法学院学报（法治论丛）》2021年第5期，第154页。

② 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60~67页。

③ 参见陈垣桥、王连猛、边博旻：《风险为本原则与银行反洗钱资源配置研究》，《金融监管研究》2021年第7期，第1~16页。

④ 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7~8页。

⑤ 参见梅夏英：《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12页。

针对性地提出安全保护措施，最终达到动态优化式的权益保护效果。^① 实践中，反洗钱义务人或指定由内部评估、审计部门负责，或委托外部专业机构做出评估报告。根据《个人信息保护法》的规定，处理个人信息达到国家网信部门规定数量的反洗钱义务人，应当由指定的个人信息保护负责人领导和监督影响评估工作，并对最终的评估质量负责。作为一种事前评估机制，个人信息保护影响评估应在反洗钱个人信息处理之前做出，并随时机动调整。国家市场监督管理总局、国家标准化管理委员会发布的国家标准《信息安全技术 个人信息安全规范》即建议个人信息保护影响评估应定期（至少每年一次）开展，并根据业务现状、威胁环境、法律法规、标准要求等情况持续修正个人信息保护边界，改进安全控制措施。

其三，“隐私增强技术”作为赋能科技的重要工具。发轫于20世纪70年代的隐私增强技术近年来蓬勃发展。在强调个人信息保护的背景下，该技术试图在不提供原始数据的前提下进行分析计算，实现个人信息共享与融合过程中的“可用不可见”。就反洗钱的个人信息处理而言，隐私增强技术一方面体现为加密和去标识化处理，将明文个人信息转换为密文，提升信息安全保护等级；另一方面则体现为基于区块链和数字身份技术的匹配计算，实现彼此数据不可见和获取必要信息的双重目标。

三、反洗钱中个人信息共享与个人信息权益保护的再平衡

（一）反洗钱的挑战与个人信息的共享

随着数字金融的发展，不法分子开始利用跨机构、跨市场、跨行业的分散交易，形成层层复杂的交易链路，模糊资金来源和去向，切断资金链路，使不法交易更为隐蔽，难以追踪和监测。面对信息不充分难以识别可疑客户、特定行业场景单一甄别分析困难、反洗钱义务人无法联防联控和信息报送不完整等挑战，反洗钱义务人运用大数据、人工智能等信息技术，采集、分析客户信息，以期判断和预测复杂多变的新型洗钱活动。鉴于相关信息源自不同机构，个人信息在反洗钱义务主体之间的共享与汇聚成为有效协调各方资源、充分发挥协同效应、提升洗钱风险管理有效性的重要途径。

近年来，美国、新加坡、澳大利亚和加拿大等发达国家纷纷探索和建立

^① 参见张新宝主编：《〈中华人民共和国个人信息保护法〉释义》，人民出版社2021年版，第417页。

了符合自身特色的反洗钱个人信息共享机制。^①例如,美国《爱国者法》(USA PATRIOT Act)第314条允许反洗钱义务人按照下述条件进行个人信息共享:(1)信息共享是自愿性的;(2)信息共享用于协助确定可疑的洗钱行为是否存在,即仅在具体情形下共享信息;(3)监管机构知晓信息共享意图;(4)确保共享信息的安全性。2020年,美国《国防授权法案》(National Defense Authorization Act)全面更新《银行保密法》(Bank Secrecy Act)及其反洗钱监管框架,要求在金融机构、监管机构和执法机构间就打击金融犯罪和恐怖融资进行更多常规的系统性协调、沟通以及反馈。^②2021年,新加坡金融管理局发布立法文件,尝试为金融机构开发“洗钱和恐怖主义融资资料分享平台”(the Collaborative Sharing of ML/TF Information & Cases, COSMIC),以便金融机构能够在避免重大风险的前提下,安全地彼此共享客户或交易的信息,及其所展示的高风险行为信息和风险分析信息。金融管理局还要求对所有COSMIC参与者实施强有力的措施,防止未经授权使用和披露COSMIC信息。^③

(二) 反洗钱中个人信息共享的制度设计

“共享”并非《个人信息保护法》所列举的特定处理行为。在实践中,从个人信息原收集方和个人信息接收方两个维度,可以将个人信息共享分为如下两种类型:其一,由个人信息原收集方主动发起的共享。^④根据《个人信息保护法》第13、23条,“个人信息原收集方”作为“个人信息提供方”可以向第三方提供个人信息,但应当向个人告知接收方的名称、联系方式、处理目的、处理方式和个人信息的种类,对于基于个人同意而收集的个人信息,还应当取得个人的单独同意。接收方应当在原先处理目的、处理方式和个人信息的种类等范围内处理个人信息。其二,由个人信息接收方主动发起的共享。根据《个人信息保护法》第13、23条,个人信息接收方可依法向个人“直接收集”个人信息(包括个人主动提供、通过与个人交互或记录个人行为等方式),也

① 刘莹:《发达国家反洗钱信息共享经验及对我国的启示》,《甘肃金融》2019年第2期,第14页。

② Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act Of 2001, <https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf>, 2022年4月15日。

③ Monetary Authority of Singapore: *Consultation Paper on the FI-FI Information Sharing Platform for AML/CFT*, <https://www.mas.gov.sg/-/media/MAS/News-and-Publications/Consultation-Papers/1-Oct-2021-FI-FI-Information-Sharing-Platform-for-AML/CFT/Consultation-Paper-on-FI-FI-Information-Sharing-for-AML/CFT.pdf>, 2022年4月6日。

④ 根据《个人金融信息保护技术规范》第3.9条的规定,共享是个人金融信息控制者向其他控制者提供个人金融信息,且双方分别对个人金融信息拥有独立控制权的过程,即主要从个人信息提供方的维度作出的定义。

可以向第三方“间接收集”个人信息。此时，个人信息接收方应当向个人告知个人信息提供者的名称、收集目的、处理方式以及收集个人信息种类、保存期限，取得个人同意或者具备第13条规定的其他合法性事由。

以上述两种类型为基础，反洗钱中的信息共享也可采取两种形式。其一，反洗钱义务人作为个人信息原收集方，为履行反洗钱义务之目的，可在下述情形下主动提供客户信息：（1）向集团内关联企业提供高风险客户或高风险业务的相关信息；（2）向第三方提供大额交易相关的客户身份信息和交易信息，以协助他方履行大额交易报告义务；（3）向第三方提供客户的风险评价信息和高风险行为信息，以协助他方履行客户尽职调查义务。其二，反洗钱义务人作为个人信息接收方，可向个人信息原收集方间接收集信息。为履行反洗钱义务，反洗钱义务人应从各个途径，尽可能全面地收集与该义务直接关联的各种客户信息。基于此，在向客户履行告知义务的前提下，可以向个人信息原收集方请求提供必要的个人信息。根据《中华人民共和国反洗钱法（修订草案公开征求意见稿）》第35条，“任何单位和个人在与金融机构、特定非金融机构建立和维持业务关系过程中都有配合金融机构和特定非金融机构开展尽职调查的义务，都应当提供真实有效的身份证件或者身份证明文件，准确、完整填报有关身份信息，如实提供受益所有人相关信息和资料；根据金融机构和特定非金融机构的要求，如实提供与建立业务关系或者交易目的和性质、资金来源和用途有关的资料”。《金融机构客户尽职调查和客户身份资料及交易记录保存管理办法》第40条进一步要求，“金融机构应当在开展客户尽职调查中相互配合”。

（三）个人信息共享中的权益强化保护

毋庸讳言，个人信息共享和汇聚的过程中，可能因原始数据错误导致后续的错误匹配（mistaken identity）或错误认定（faulty inference），也可能因为接收方过错引发个人信息泄露与滥用的恶果。如何有效保障个人权益，由此成为反洗钱中个人信息共享与保护得以再平衡的关键。

一方面，应强化反洗钱义务人的告知义务。《个人信息保护法》第13条第2款明确因“履行法定义务处理个人信息”可豁免个人同意，但其并非对个人知情的排除。这是因为，知情权是所有个人信息权益的基础，若个人对个人信息处理活动一无所知，不但无法做出同意，后续的查阅、复制、更正以及救济权利均无所附着。正因如此，《个人信息保护法》区分了同意豁免和告知豁免，将免于告知的情形限定在“法律、行政法规规定应当保密或者不需要告知”以及“紧急情况下为保护自然人的生命健康和财产安全无法及时向个人告知”这两种情形，履行反洗钱义务显然不在其中。

遗憾的是，在一项对我国金融机构的调研中发现，被抽样调查的金融机构大多未能有效履行告知义务：41家抽样机构中，4家不会告知客户其个人信息的

用途,6家机构在客户询问时才会告知,23家机构会粗略告知客户其个人信息的可能用途,仅有8家机构会根据信息处理行为性质履行必要的告知义务。^①正因如此,反洗钱义务人亟待以显著的方式和清晰易懂的语言真实、准确、完整地告知客户下列事项:(1)个人信息处理者的名称和联系方式;(2)个人信息的处理目的、处理方式,处理的个人信息种类、保存期限;(3)个人行使本法规定权利的方式和程序;(4)信息处理对个人会造成何种影响尤其是不利后果;(5)采取的信息安全保护措施。鉴于反洗钱义务人一般以格式条款的方式进行上述告知,为充分提醒客户,在隐私政策、服务协议等法律文件中,还应通过加粗标记或单独列明关键条款的方式使之更易于被发现。

另一方面,应赋予个人查阅权、更正权和获得救济的权利。首先,《个人信息保护法》第45条规定的“查阅权”不但落实了第7条规定的“公开、透明原则”,也是个人信息知情权的重要内容。个人的知情权不仅体现在个人信息收集之时,也应延伸到后续的处理活动之中。一般在个人信息初始收集环节,个人往往因未能充分了解其个人信息处理的事项就点击同意,或即便有所了解,也不清楚个人信息处理在事实上究竟收集何种个人信息以及收集是否符合法律规定。据调查,金融机构依据反洗钱规定收集的个人信息不只用于反洗钱工作,还用于日常运营、客户管理和产品营销等途径。^②查阅权的设置,将大幅减少此类滥用行为的发生。其次,《个人信息保护法》第46条规定的“更正权”,赋予个人在其个人信息不准确、不完整之时,请求个人信息处理者更正、补充,以保障个人信息在其处理目的范围内的完整性和准确性的权利。在反洗钱的过程中,原始信息错误或者错误的自动化风险评估模型可能有损个人权益,尤其是在彼此分享信息的众多金融机构因“错误认定”一致拒绝为特定客户服务的情形下,将在事实上导致“金融抑制”。为落实更正权,可借鉴《征信业管理条例》《个人信用信息基础数据库管理暂行办法》相关规定,在客户就其异议提出证据材料后,个人信息处理者应在内部及时标注异议,并予核查和处理。经核查,确认相关信息确有错误或遗漏的,个人信息处理者应当予以更正或补充;经核查仍不能确认的,对核查情况和异议内容应当予以记载,对于已经更正的信息,个人信息处理者有必要告知其对外提供个人信息的第三方,以避免虚假信息的传播。最后,“无救济即无权利”,获得救济的权利是维护个人权益的最终工具。《个人信息保护法》为个人提供了较为完备的民事救济途径,^③包括:

① 侯建强、王喜梅:《反洗钱中的个人信息保护》,《财经科学》2013年第3期,第39页。
② 侯建强、王喜梅:《反洗钱中的个人信息保护》,《财经科学》2013年第3期,第39页。
③ 朱芸阳:《个人金融信息保护的逻辑与规则展开》,《环球法律评论》2021年第6期,第71页。

(1) 个人在查阅权、更正权遭受不合理拒绝时有权提起诉讼；(2) 个人在反洗钱义务人未履行或未完全履行信息安全保障义务时，有权主张其承担违约责任；(3) 因反洗钱义务履行导致个人财产损失，反洗钱义务人不能证明自己没有过错的，个人有权要求其承担损害赔偿等侵权责任。

四、结语：《反洗钱法》的修改与完善

反洗钱已经进入客户信息规模庞大 (Volume)、来源多样 (Variety)、高速流动 (Velocity) 的“3V”时代，为此，《反洗钱法》亦须顺应这一趋势，积极推动为履行反洗钱目的的客户信息共享，这不但是构建金融系统预防体系、完善洗钱风险管控制度的需要，也是扩大金融业双向开放、深度参与全球治理的必然要求。以此观之，《反洗钱法》第5条“对依法履行反洗钱职责或者义务获得的客户身份资料和交易信息，应当予以保密；非依法律规定，不得向任何单位和个人提供”，以及《中华人民共和国反洗钱法(修订草案公开征求意见稿)》第6条第1款“单位和个人对依法履行反洗钱义务获得的客户身份资料和交易信息以及反洗钱调查信息，应当予以保密；非依法律规定，不得向任何单位和个人提供”的规定，过度强调个人信息保护，却忽略了个人信息合理利用。

为化解《反洗钱法》第5条与个人信息共享的冲突，不妨采取“解释论”和“立法论”两种不同的进路。首先，就“解释论”而言，可将“客户身份资料和交易信息”解释为用于识别特定客户的“事实性信息”，将在此基础上通过标注、比对、分析、挖掘、推断而形成的“风险评价性信息”排除在外。根据《个人信息保护法》第13条，反洗钱义务人可向第三方即个人信息原收集方间接收集其客户涉洗钱风险的“评价性信息”，后者的提供行为不应被视为对《反洗钱法》的违反。其次，就“立法论”而言，建议将第5条修改为“单位和个人对依法履行反洗钱义务获得的客户身份资料和交易信息以及反洗钱调查信息，应当予以保密；非依法履行反洗钱义务或法律另有规定，不得向任何单位和个人提供”。修改后的条文为履行反洗钱义务的主动共享预留了空间，不但可避免“事实性信息”和“风险评价性信息”区隔难题，还能囊括反洗钱义务人为协助第三方履行反洗钱义务之目的而提供客户信息的场景。最后，为激励基于反洗钱目的的信息共享，可借鉴美国《爱国者法》第314条的“安全港”条款，对外提供其怀疑可能涉及特定非法活动收益相关信息的反洗钱义务人，以及接收此类信息并用于反洗钱工作的其他反洗钱义务人，均不因该等信息共享行为承担民事责任和行政责任。

(责任编辑：洪欣)