反电信网络诈骗中个人信息删除权的实现路径*

朱园伟

（北京大学粤港澳大湾区知识产权发展研究院，广东　广州　510000）

摘　要：《反电信网络诈骗法》是我国在数字社会中进行前端防控犯罪治理思路的典型转型，其中构建的信息监测共享机制成为政企多方协同治理的范例。该机制授予企业组织一定程度以个人信息工具化利用为特性的用户信息控制权，使得信息主体与信息处理者之间的关系更为紧张，其结果可能表现为个人信息删除权的被迫落空。在信息监测机制通体流程解构为“信息实名-信息留存-风险信息识别-风险信息核验-风险信息共享-中止服务”的程序链条中，包括安全义务主体、信息处理目的、信息留存时限都与删除权的权利场景不相协调。其疏解路径应当分别从《个人信息保护法》和《反电信网络诈骗法》两法规范体系内进行思考，明确在法理和规范性解释下法定个人信息利用行为对信息删除请求权抗辩的合理性，厘清信息监测共享机制中与义务主体、内容有关的模糊地带，同时对信息留存的时限与方式给予上限性规定，实现两法以个人信息保护为核心的共同意志。

关键词：反电信网络诈骗；个人信息删除；信息监测共享；个人信息留存

中图分类号：D99　　**文献标识码：**A　　**DOI：**10. 19358/j. issn. 2097-1788. 2023. 11. 013

引用格式：朱园伟. 反电信网络诈骗中个人信息删除权的实现路径［J］. 网络安全与数据治理，2023，42(11)：72-79.

The realization path of personal information deletion right in anti telecom network fraud

Zhu Yuanwei

(Intellectual Property Development Institute of GBA, Peking University, Guangzhou 510000, China)

Abstract: The Anti-Telecommunications Network Fraud Law is a typical transformation of China's approach to front-end crime prevention and control governance in the digital society, in which the information monitoring and sharing mechanism constructed therein serves as an example of collaborative governance between government and enterprises. The mechanism grants business organizations a certain degree of control over user information characterized by the instrumental use of personal information, making the relationship between the subject of information and the information processor more tense, and the result may be that the right to delete personal information is forced to fall through. In the process chain of the information monitoring mechanism, which is deconstructed into the information real name-information retention-risk information identification-risk information verification-risk information sharing-suspension of services, including the subject of the security obligation, the purpose of information processing, and the time limit of information retention are all incompatible with the scenario of the right of deletion. The path of resolution should be considered from within the normative system of the Personal Information Protection Law and the Anti-Telecommunications Network Fraud Law respectively, to clarify the reasonableness of the defense of the right to request for deletion of information under the jurisprudence and normative interpretation of statutory personal information utilization, to clarify the ambiguities related to the subject of the obligation, the scope and the content of the information monitoring and sharing mechanism, and at the same time to give the upper limit to the time limit and the way of information retention to realize the common will of the two laws centering on the protection of personal information.

Key words: combating telecom and online fraud; personal information deletion; personal information monitoring and sharing; personal information retention

* 基金项目：北京市法学会 2022 年市级法学研究课题“自动化决策算法治理中的平台责任研究”（BLS（2022）C008）

0 引言

2022 年 9 月 2 日正式通过的《反电信网络诈骗法》对近年泛滥的电信网络诈骗行为进行专门立法，其在参考域外主要国家的先进经验基础上[1]，进行了针对犯罪风险防控的创新型制度配置。在反电信网络诈骗法出台之前，对电信网络诈骗的规制主要体现为事后的责任追究和行为惩治，此次反电信网络诈骗法构建的诸如身份核验、监测预警以及信息共享等措施实现了前端防治转型。在整体治理逻辑上，反电信网络诈骗法强调对治理主体的广泛性和治理资源的丰富性予以体制性整合与重塑[2]，表现为《反电信网络诈骗法》第 6 条第 5 款中规定的电信业务经营者、银行业金融机构、非银行支付机构、互联网服务提供者四类主体，被要求构建反电信网络诈骗内部控制机制和安全责任的义务性规范，可视为授予了市场主体一定的行政管理职责。

《反电信网络诈骗法》中一系列的防治措施在实践中造就了以个人信息为核心的程序链条，即“信息实名-信息留存-风险信息识别-风险信息核验-风险信息共享-及时限制、暂停服务”以求规避风险。这一过程，经营者首先收集包括姓名、身份证件号、生物信息等个人敏感信息进行实名认证并留存，继而在业务经营中对用户活动和用户信息进行实时监测，将识别出的可能涉诈的用户信息进行实名核验，最后按照法定要求进行风险信息共享，最终目的在于及时停止提供渠道服务，中断诈骗行为的发生，同时为监管机关对诈骗案件侦查提供信息来源，见图 1。显然，个人信息的“实名 + 留存”是信息核验的必要前提，风险信息的确认共享是信息核验的行为目的，以实现对网络诈骗行为的即时识别、精准打击。不同于以保护性规范为本位的《个人信息保护法》，《反电信网络诈骗法》中个人信息成为了预防财产犯罪的工具，其中相关措施不免与个人信息权利束中许多主体权能产生矛盾交互，其中最为明显的是信息监测共享机制所勾勒出的个人敏感信息实时控制、频繁查验、信息留存、跨领域共享与个人信息删除权所映射的个人信息自决和信息利用最小化理念之间潜在的抵牾。虽然其背后反映出的个人信息保护和利用的权衡是个人信息法律保护中的永恒话题，但目前个人信息删除规则零散且廖少的状态使得公法性质的信息利用表现得过于强势，有待通过规则补正和优化实现缓和平衡。因此，厘清《反电信网络诈骗法》中个人信息工具性利用机制如何与现有个人信息保护规则实现和谐共生是本文的核心主题。

在电信网络诈骗的研究方面，目前学界多从刑事犯罪防控和罪名罪数认定两方面进行探讨，删除权的学术讨论主要集中在权利的构建以及与欧盟被遗忘权的对比中，鲜有研究将二者关联并关注到行政监管或者刑事防控而构建的工作机制对个人信息删除权形成的掣肘。本文试图通过对信息监测共享制度的特点及运行流程分析，结合目前学界已有的研究共识，梳理出个人信息删除权与反电信网络诈骗的信息监测共享制度之间的矛盾交互，为后续的制度运行及个人信息删除权的协同落实提供补充认识。

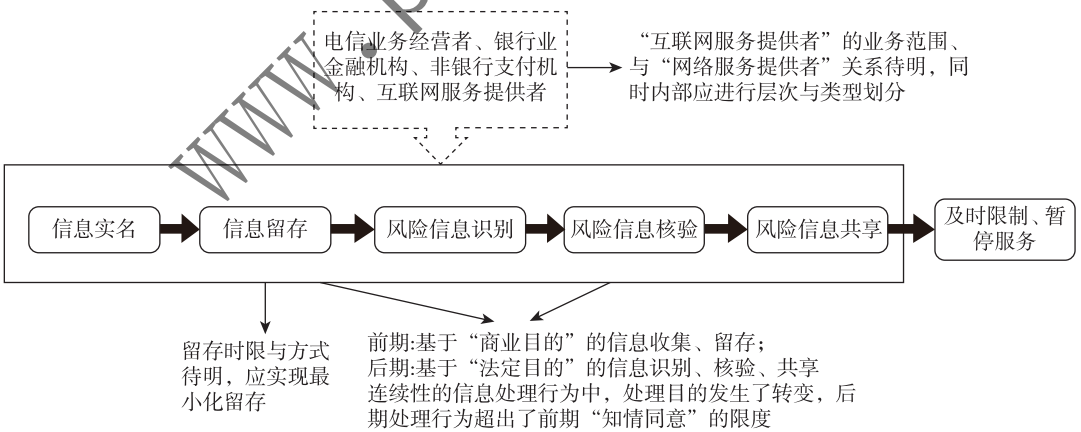

图 1 反电信网络诈骗中个人信息工具化流程

1 反电信网络诈骗中凸显的个人信息删除权实现问题

我国《个人信息保护法》第 47 条第一款列举出五项信息处理者应当主动删除个人信息的义务内容，并同时给予个人在信息未删除时请求删除的权利，意图形成对个人信息删除权的有效实践闭环。此制度架构下，删除权的多种实施场景与反电信网络诈骗法的信息监测共享制度存在安全保障落空、权利保护悬置、信息风险不明等问题。

1.1 义务主体范畴模糊

《反电信网络诈骗法》第 6 条第 5 款规定，承担风险

控制机制与安全责任制度的主体为电信业务经营者、银行业金融机构、非银行支付机构、互联网服务提供者。在这四类主体中，我国《电信条例》（第七条、第八条）与《电信业务分类目录》（2015 版）中对电信业务的概念、经营条件和范畴进行了限定和列举；我国《银行业监督管理法》（第二条、第十七条至第十九条、第二十一条）中对银行业金融机构的设立条件与经营规则进行了具体规定；非银行支付机构的范围、业务活动在《非银行支付机构分类评级管理办法》《非银行支付机构网络支付业务管理办法》等规章中同样有迹可循。但是，互联网服务提供者的内涵和外延在我国法律法规中并未得到明确，并且其与网络服务提供者这一主体概念的业务类型、层级关系较为模糊，处于定义不明、范畴不清的现状。

“网络服务提供者”的概念源于美国《数字千年版权法》中“Online Service Provider”，后出现在我国《侵权责任法》第 36 条用以针对性地规制网络活动主体，属于法律概念。在网络服务提供者的业务类型中，2013 年我国《信息网络传播权保护条例》中提及的网络服务提供者的业务包括网络自动接入、自动传输服务、信息存储服务和网络搜索、链接服务等。然而，在我国《工业和信息化部关于清理规范互联网网络接入服务市场的通知》的目标任务中，直接使用了“ISP”（Internet Service Provider，互联网服务提供者）的表述与“互联网接入服务”形成了等同关系。由此推断，接入服务应当是网络服务也是互联网服务，且互联网服务仅包括网络接入服务。但是，根据公安部 2005 年发布的《互联网安全保护技术措施规定》第 18 条规定，互联网服务提供者是指向用户提供互联网接入服务、互联网数据中心服务、互联网信息服务和互联网上网服务的单位。该规定认为互联网服务提供者并不限于接入服务，而是囊括多种业务的类似于网络服务提供者的概念。而且，另有观点认为《反电信网络诈骗法》中的互联网服务提供者应当包括接入服务、平台服务、内容及产品服务[2]。可见，二者的构成关系、指代的业务类型并未统一。

在概念层级上，对《美国数字千年版权法》（DMCA）解读中提到“网络著作权侵权责任限定法为在线服务提供商（OSP），其中包括互联网服务提供商（ISP）创建了安全港规则”，全国信息安全标准化技术委员会将二者认定为包含关系[3]。但是，有的学者认为互联网服务提供者是网络服务提供者可替换的概念，并且在我国最高人民法院 2000 年、2004 年和 2006 年的著作权司法解释中得到确认[4]。也有观点认为根据我国《网络安全法》第 76 条规定，公共电信服务提供者和互联网服务提供者可被合称为网络服务提供者[5]。可见，网络服务提供者与互联网服务提供者的概念关系同样难以辨析。

在对于互联网服务提供者概念界定的观点纷争中，难以言明是否所有的互联网服务提供者都有必要成为风险信息监测共享的义务主体。这是反电信网络诈骗机制建立的同时亟待明确的基础问题。

1.2 商业与法律目的交织

按照《个人信息保护法》第 47 条第 1 款要求，个人信息处理者处理目的已实现、无法实现或者实现处理目的不再必要时，应当对个人信息进行主动删除。这一规定的核心在于信息处理者的信息处理目的的界定和边界廓清，具体可归纳为当目的已达、目的不达以及目的不必要时，个人信息应当在法定期限内被删除[6]。关于“信息处理目的”，《个人信息保护法》将其明确要求在信息处理者的告知同意内容之中，旨在表明信息处理目的应是信息主体与处理者双方协商下的结果，从而使信息主体可对信息处理的界限和信息删除的时机进行把控。但在《反电信网络诈骗法》的信息监测共享机制中，电信业务经营者、银行业金融机构、非银行支付机构、互联网服务提供者等主体的信息处理行为实质上表现出商业目的和法定目的的交叉与混杂。一般情形下，处理者基于个人同意而处理个人信息，一旦个人信息处理者停止提供产品或者服务，个人信息的处理目的将不复存在，信息处理者留存的信息库中，非特定要求所必要的信息就不再具有合法基础，应当在法定期限内删除。但如果用户信息被信息处理者识别为风险信息，信息处理者则可按照法定要求对用户数据进行监测和收集并对信息主体的身份进行核验，当认定其具有涉诈可能性时，还需将信息传输共享至其他机关。此时，以同意为基础的信息处理行为则被法定目的下的信息处理收集行为所湮没，突破了原有的告知同意范围的处理目的。

个人信息删除权属于请求权范畴，其请求的对象为个人信息处理者，应当遵循民事法律体系中请求权的基本规范逻辑。当个人信息处理者以法定理由对个人信息进行必要留存或共享给第三方时，意味着此时信息成为刑事侦查机关的案件线索而脱离个人自决的空间范围。商业社会中，基于个人信息潜在的价值性，个人信息处理者原则上都企图对个人信息或者生成的数据集合尽可能地留存和利用，而在商业目的与法定目的交织下的个人信息处理行为有可能会成为信息处理者对个人信息继续留存的“合理化”借口。按照《反电信网络诈骗法》的规定，信息处理者对涉诈信息的监测、认定、核验等义务于一身，这无疑为个人信息删除权“法定原因”下的落空创设了更大的风险。

1.3 保存期限规定不明

根据《个人信息保护法》第47条第2款规定，个人信息保存期限届满时，信息处理者应当对个人信息进行主动删除。该款项中，“保存期限届满”成为了个人信息删除的法定理由。然而，各行业中对于数据信息的使用模式与存储方式并不相同，我国宏观层面的法律规范例如个人信息保护法或者国家标准当中，仅对个人信息留存最小化进行原则性要求。信息留存的具体期限多体现在特定行业规范或地方性法规之中。由此，我国关于信息留存时限的规则可分为三种类型，如图1所示。第一类为最低时限型规则，包括《电子商务法》《网络预约出租汽车经营服务管理暂行办法》《医疗机构管理条例实施细则》《证券法》《反洗钱法》《劳动合同法》在内都仅规定了信息留存的下限，即必须要保存的时长，其目的在于确保电子存档的可用性，使其有据可查。这些立法对于信息留存所带来的个人信息风险并未进行场景化类析，此情形下的信息处理者几乎可以基于特定目的或监管需要无限期对个人信息进行留存。第二类为业务区间型规则。例如《电信和互联网用户个人信息保护规定》第9条第4款、《信息安全技术 个人信息安全规范》6.4（3）项，将个人信息留存的合理区间设定为“提供业务/产品/服务时”，当服务停止时，信息应当删除。该类规则在反电信网络诈骗机制中难以发挥删除权的期间限定效用，原因在于服务结束时，其信息可随时被以反诈骗目的进行继续留存。第三类为特定期限型规则，例如《关于开展App违法违规收集使用个人信息专项治理的通知》第6项中，规定删除信息的日期不得超过用户提出请求权的15日；《南宁市个人信用信息征集使用管理办法》第17条规定，市信用信息系统对个人信用信息的保存期限为5年。该种类型的规定对信息留存给出了明确的期限，但在监测共享机制中其局限性与第二种相似，信息持续受监测的解释权由信息处理者掌握，反电信诈骗机制为用户的信息删除请求权设筑了壁垒。

事实上，信息留存目的与信息留存期限在个人信息的合规体系中是相互独立的部分，二者分别以目的限定和存储限定为基本原则。在欧盟法院公布的判例（Case C-77/21）中，Digi公司以程序测试、纠偏为理由将基于履行服务合同为目的收集的用户信息进行了持续留存和二次利用。最终欧盟法院在利用“目的兼容”原则判断Digi公司二次利用信息的目的与履行服务合同的初始目的具有关联性且满足信息主体的合理期待并不违法，但欧盟法院对于信息的留存同时作出了单独评价，认定其未满足存储限定原则而对Gigi公司处以罚款。以此案例为鉴，反电信诈骗为目的的信息监测预警尽管属于法定目的下的信息处理行为，但处理者在处理流程中仍应对信息留存满足最小期限承担注意义务。

表1 个人信息留存规则的类型及在监测机制下的风险表征

类型	规范	特征	风险
最低时限型规则	《电子商务法》第31条	仅进行了留存日期下限的规定	信息处理者几乎可以基于特定目的或监管需要无限期对个人信息进行留存
	《网络预约出租汽车经营服务管理暂行办法》第27条		
	《医疗机构管理条例实施细则》第53条		
	《证券法》第137条		
	《反洗钱法》第19条		
	《劳动合同法》第50条		
业务区间型规则	《电信和互联网用户个人信息保护规定》第9条第4款	信息留存区间为“提供业务/产品/服务时”	服务结束时，其信息可随时被以反诈骗目的进行继续留存
	《信息安全技术个人信息安全规范》6.4（3）项		
特定期限型规则	《关于开展App违法违规收集使用个人信息专项治理的通知》第6项	对信息留存确定了明确的期限	
	《南宁市个人信用信息征集使用管理办法》第17条		

此外，《反电信网络诈骗法》中所要求的监测共享信息类型十分广泛。在犯罪预防理论中，电信网络诈骗的监测预警主要利用大数据和算法等技术，对犯罪特征进行提炼，对犯罪规律进行建模，对犯罪嫌疑人和罪犯的特征进行精准画像，从而实现系统的自动识别[7]。其中，关键措施之一在于利用数据对规律和特征进行挖掘，仅针对被害人的特征研究中，就可细化为客观特征、主观特征、环境特征[8]、个人信息特征[9]等。该机制建立通常还需依托多方数据共享为前提，例如通过运营商数据、金融机构数据和政府数据的联合建模，有利于扩大名单覆盖率、提升欺诈识别精确度。这意味个人信息监测共享机制对类型广泛的个人信息的留存利用提出了急迫需求，却并未对各信息处理者的留存时间进行限制安排。个人信息权利的内容体现在对个人信息利用行为进行有限自主的控制和支配之上[10]，包括信息的收集、存储、使用、公开和删除等，而个人信息的存储则关系着个人信息权利的最终实现。同时，反电信网络诈骗监管机关

也可通过风险信息共享机制获取企业组织收集的信息，在多主体协同共治的政策指导下依法调取企业收集到的个人信息。这相当于确认了目前基于“预防犯罪”这一法定目的而进行几乎无限制的个人信息留存和流转，与保护个人信息理念与实践充满矛盾张力。

2 从规范价值对反电信网络诈骗中个人信息删除权实现的塑造

2.1 法定使用的价值优位

个人信息删除权指在法定或双方约定的情形下，信息主体请求信息处理者及时删除已收集的个人信息的权利[11]。在比较法上，欧盟的《一般数据保护条例》第17条第3款（b）项中规定了基于公共利益的目的可以对数据主体的删除权等一系列权利进行限制。我国台湾地区《个人资料保护法》中也有相关规定，在执行职务或业务所必须或经当事人书面同意情形下，无需对个人信息删除的请求进行处理。信息删除权在我国《民法典》和《个人信息保护法》中都有明确体现，但现有规定中对个人请求信息删除的例外仅限两种情形，即法律上不能（法律、法规规定的保存期限未届满）和事实上不能（技术上无法实现）[12]，并未将“基于公共利益目的”利用作为请求删除权例外的情形。对是否应当将公共利益考量纳入例外情形可以基于利益平衡视角和规范体系化视角进行分析。

以利益平衡视角分析，主要解决的问题是基于公共利益的限制诉求与个人信息主体自决行为之间张力的平衡。随着数字时代下个人信息处理行为的不断增加，催生出一系列个人信息保护领域特有的法律问题[13]。但是对个人信息的保护并不应当绝对化，正如知识产权的制度历程，同样是在技术氤氲发展下逐步验证了权利化的必要性，我国知识产权制度在价值构造上展现出一系列的利益平衡表征，例如基于公共利益考量的著作权合理使用和法定许可、基于公共卫生安全需求的专利强制许可、基于描述性或指向性为目标的商标合理使用等。事实上，由于我国《个人信息保护法》主要借鉴于欧盟《通用数据保护条例》，且我国《个人信息保护法》施行仅两周年，对于限缩个人信息受保护权的话题并没有得到理论和实践充分的验证，对多方利益的认知、识别及均衡对比都缺乏基本公式。但实践中，随着电子政务领域的迅速发展，个人信息在面对突发的公共危机事件或者常态化公共管理时，已经逐步实现了个人信息对于维护社会稳定、保障公共利益力量的重要作用。随着个人信息在新生的公法治理规则中占比越来越大，以安全、秩序、稳定为内核的重大公共利益维护，和涵盖知情同意、最小必要、目的限制等内容的基本权利保护之间的张力逐步拉大，个人信息自决的范畴应当与公共利益有着清晰的界限划分[14]，如此才能真正实现对基于公共利益目的的个人信息保护限制规则的完善塑造。

从规范体系视角分析，个人信息自决受限理论早在我国《个人信息保护法》出台之前，已有学者对其进行探讨，虽然个人信息自决属于对本人信息的支配，但个人信息常混杂于本人之外的随处可见、捉摸不定的信息之中，此种支配不应归属于绝对权，否则个人信息自决不仅促成个人对信息的支配，还导致对他人行为的支配[15]。在民法典出台后，有学者对其中的个人信息规则提出了“合理使用”的概念，即基于法定原因使用他人的个人信息[16]。该理论最终体现在《个人信息保护法中》第13条中，基于特定情形的信息处理可不以个人同意为前提：（1）合同或人力资源管理所必需；（2）法定职责或法定义务所必需；（3）紧急或突发情形所必需；（4）为公共利益的新闻报道。对于政府机关处理个人信息的有关规定同样散见于例如《政府信息公开条例》（第15条）《生物安全法》（第26条）等其他法律法规中。因此，无论是从法理分析，抑从《个人信息保护法》第13条的规范分析，以防范电信网络诈骗为目的信息处理行为可适当对抗个人信息删除的强制性义务，不应当直接对《反电信网络诈骗法》中信息利用行为进行根本否定。

2.2 最小损害的基本保障

必要性原则是我国公法治理中的“帝王原则”[17]，源于法国自由法治时期的必要性原则，尽管其内容仅包括手段必要和目的必要两要素，但是实际场景应用中，必要性原则常会表现出主观性过大的空洞性缺陷[18]，对基于目的和手段的必要限度的界定难以掂量。其后，1931年《普鲁士行政法》首次提出了最小损害原则，表述为“如果有多种手段可以实现对公共安全、公共秩序危机的消弭，或能有效地抵御危险，则应当尽可能地选择一种对相关人员与一般大众损害最小的手段。”此时，在必要性内涵的流变中，最小损害成为了必要性的评判标准之一。二者的关系可以理解为，如果某项手段在必须的情况下造成的损害没有最小化，那么这个手段就不是必要的。

倘若将个人信息删除置于信息监测共享机制中去分析其最小损害原则的应用，首先呈现的规范表达是个人信息收集的目的限制。目的限制原则要求信息处理者有明确且具体的处理目的，同时开展个人信息处理行为应当与处理目的直接相关，即目的明确、合理与使用限制。其中“合理”意涵的实质是要求信息处理的目的应当以

双方约定或者法律规定为前提，不得随意进行扩张。对于电信网络诈骗风险防范义务的主体而言，其信息收集、实名、监测、核验、共享主要目的在于为用户提供完整的经营业务以及实现必要的网络信息监管，此两种目标分别处于同意规则和同意豁免规则项下。对于以用户同意为基点的信息处理行为被明确限定在用户知情同意的范畴之内，且当个人信息的处理目的、处理方式和处理的个人信息种类发生变更时，法律要求重新取得个人同意。对于同意豁免规则项下的信息处理行为的目的限定规则却似乎被“例外情形”一词一言以蔽之，包括《反电信网络诈骗法》在内的涉信息处理的公法规范典型表现为忽视了以公共利益为前提的信息处理行为也应当符合目的限制原则，以明确告知用户信息处理的缘由、方式以及限度为基础，同时保证其处理行为都严格置于公共利益目的的框架之内，以在整体安全保障机制运转下推动风险防控主体“最小特权”的实现。

必要原则的实现还要求以国家名义进行的信息处理手段对个人信息的损害最小。个人信息保护与个人信息利用之间存在固有的此消彼长关系已是信息时代的基本理念，实现个人信息最大化保护的方式之一即是保证信息处理的有限化。反电信网络诈骗中，以往的商业主体在原来的信息处理者之上被赋予实行公共权力的身份，有利于协同治理违法犯罪的达成，但由此也为义务主体和监管部门提出更高的个人信息工具化的注意义务。另外，《反电信网络诈骗法》对诈骗犯罪“源头治理”的强调也映射出其对个人信息保护机制的落实要求，其内容可以理解为以信息保护为治理方向，同时又以信息利用为治理工具，但二者并非绝对的对立关系，依然存在统一的可能，前提在于相关主体对信息的利用秉持谦抑克制的态度。

2.3 协同共进的治理之纲

《个人信息保护法》为国家机关和私人机构的信息处理活动进行了“一体化调整”的模式，其中围绕私人机构处理个人信息的行为进行全方面的规制设计[19]。以此而形成的个人信息权利束的内容非常广泛，包括但不限于个人信息同意、更正权、删除权、可携带等。信息自决权源于1971年德国《个人信息保护法草案》[15]，其目标在于将个人信息置于人格尊严之下，构建起以个人控制为中心的保护体系，但将个人信息作为宪法性权益进行规则制度的配置也就决定个人信息自决权的完整落实将是缓慢而谨慎的进程。目前学界对个人信息权利的研究大多基于碎片化、独立化的思考，甚少去斟酌个人信息权利之间或个人信息权与传统的公私权力之间是否存在潜在的矛盾，是否需要进行必要的限缩而实现最大化福利。根据法律执行后的调查分析，在《民法典》《个人信息保护法》实施以来涉个人信息的司法案例中，民法典条款的引用次数达600余次，而个人信息保护法的条款引用次数仅为13次，并且引用条款集中于对个人信息定义和过错责任规则，并未涉及具体权利条款的引用[20]。由此可见包括信息删除权在内的个人信息权利于司法实践中并未得到明确适用，侧面反映出其权利的细化和配套规则在实践中并未得到有效验证。

《反电信网络诈骗法》中对个人信息工具性的利用机制将这种潜在的矛盾部分暴露出来，包括上述提及的义务主体模糊、处理目的混杂、留存期限不明等。其缘由既有反电信诈骗机制并未完全契合个人信息保护原则和理念，也存在个人信息保护制度本身的规定缺漏。因此本文所提出的矛盾疏解与治理方向应当由两部法律协同进行有关规范的健全，以实现法律规范之间的融贯性，而非仅仅强调某一方的作为与不作为义务。

3 信息共享监测中个人信息删除权的实现路径

3.1 扩张个人信息删除权的例外情形

我国《个人信息保护法》第47条第2款规定了个人信息删除的例外情形，即如果出现第1款所列举的五种情形，只有法律、行政法规明确规定的保存期限未届满或者信息删除在技术上无法实现之情形，信息处理者才有权继续对信息进行留存和采取安全保障措施。除以上情形之外，法律并未提出其他的删除权例外情形，也未进行兜底条款的保留。质言之，即便信息处理者是处于履行法定职责或者法定义务，当没有信息期限的明确规定时，个人信息主体可要求个人信息的删除或被遗忘。但如此以往，信息主体或称信息被监测主体随时有权要求退出业务并删除信息时，反电信网络诈骗的目的则将必然落空。例如，涉诈人员可利用虚假身份信息注册多个平台账号，并缩短每个账户的使用周期，在销号的同时要求平台方立即删除已留存的个人信息，并未给平台的犯罪监测模型保留足够的分析数据，则依靠信息监测分析来预防犯罪风险的机制则会陷入效率不彰的境地。

个人信息不仅附着信息主体的个人利益，还承载着信息处理者的正当利益和社会公共利益，故删除权的行使不能完全归依于个人，需要将信息主体的个人利益与信息处理者的正当利益、社会公共利益进行权衡比较[21]。欧盟在GDPR第17条第3款（b）项中明确规定“控制者执行或者为了执行基于公共利益的某项任务，或者基于被授予的官方权威而履行某项任务”属于删除权不得适用的情形。美国《加利福尼亚州隐私权法》中也规定了“检测安全事件，防止恶意的、欺骗的、虚假的或非

法活动”和“遵守法定义务”作为了删除权的例外情形。对比之下，我国目前《个人信息保护法》仅有删除权两种例外情形的规定似乎并未考量到《反电信网络诈骗法》这类以个人信息监测、留存、利用为手段以实现公共利益保护的运行机制会对教义学诠释下的个人信息删除权产生的影响。在个人信息删除权尽快落实的实践需求下，我国应当适当借鉴域外的模式，至少从固有窠臼中对基于群体利益考量的“保障公共安全与公共利益”作为删除权的例外情形进行正面列举。

3.2 细化监测共享主体、范围、标准

信息安全保障义务的主体根据《反电信网络诈骗法》的规定，包括电信业务经营者、银行业金融机构、非银行支付机构、互联网服务提供者。前三种类型的行业组织与国计民生密切关联，在我国准入门槛较高，在系列法律法规中受到较为严格的监管。但互联网服务提供者的范畴随着互联网技术的发展其范围不断扩充，表现出数量众多、类型复杂的特点。据中国互联网络信息中心数据统计，仅 2016 年～2021 年间，我国互联网企业的上市数量就已经达到 155 家，涉及短视频、游戏、直播、社交媒体等[22]。但值得思考的是，以上类型的组织业务是否全部为网络诈骗行为所介入。此外，依据市场份额与用户数量进行划分，社交媒体也可以分为不同的量级，针对不同量级的社交媒体平台应当秉持区分原则，对用户量和日活量进行区分，对有关媒体的信息检测共享机制和信息保护能力进行有效评估并施以不同程度和符合实践的监管措施，实现监管效果最优化。

各行业组织的主管机关对共享监测运行机制的监管应当细化到类型化的个人信息具体业务中。企业组织在实际业务中也应对特定类型的信息进行一定程度的监测共享。由于不同行业的企业组织收集到的信息呈现交叉相异的特点，监管要求的展开应当明确到是否涉及用户定位信息、通讯录信息，抑或是浏览记录、聊天记录信息等具象内容的颗粒化程度。此外，从《反电信网络诈骗法》第 12 条第 3 款规定来看，企业组织识别风险信息的标准应当是“不能排除合理怀疑”，如此才能解释采取的处置措施是限制、暂停而不是终止，但对于排除合理怀疑标准的界定，是否需要引入专门部门进行评估也需要进行成本和风险之间的权衡。现有信息监测共享机制给予了企业组织一定的“管理权限”，那主管机关对于权力的基准与界限势必要进行前置性规定。

3.3 明确留存时限、方式

共享监测机制下的个人信息表现出两种新型特点：一是即时共享性，即基于犯罪预防为目的，从企业组织的信息数据库流入共享数据库的信息频率只能是即时或者较短期限，但频繁地共享风险信息同时应当采取更为严格的信息校验技术和密码技术保证其完整性、可用性和保密性[23]。二是去标识化，根据《信息安全技术 个人信息安全规范》（GB/T 35273—2020）的规定，信息处理者在收集个人信息后，应当立即去标识化，并将可用于恢复识别个人的信息与去标识化后的信息分开存储。但在风险管理中，去标识化使得个人信息失去个人指向特征时，其中的信息预警价值也会有所减损，去标识化下的信息是否会影响犯罪监测目的的实现仍待实践验证，但在保证基本目的实现的前提下，即便要求不可完全去标识，对个人信息仍应持有量级保护的理念。

现有关于信息留存期限的规定体现出了根据行业性质和信息作用进行的有效区分。不同行业之间信息留存时限不一是否会影响风险信息的完整性和防控犯罪的价值性也需要进一步探讨。例如，金融机构与非银行支付机构对于客户身份资料、客户交易信息、网络支付业务操作记录、购卡人登记信息一般应当保存 5 年以上，证券行业的客户资料应当保存不低于 20 年。但对互联网企业而言，其信息存量大、更新速度快，信息存储期限的法定要求要远远低于金融、证券行业。另外，为实现个人信息删除权，其要求信息的留存时限不仅应当规定下限，也应当对上限有明确规定，且上限性规定要明确可以对抗信息处理者的信息监管权力。尽管以信息监测共享为目的的信息留存属于行业组织的新义务，应当充分考虑到犯罪预防下的信息留存时限要高于原来行业的一般要求，但仍应当以最小必要为原则进行上限的具体化规定，以此才能更优化对最小必要原则的实质解释。

4 结论

在真实案件中，电信网络诈骗的源头往往是个人信息的侵权行为，二者形成了紧密的利益链条，因此保证个人信息的稳定与安全是《反电信网络诈骗法》的立法目的之一。同时，《个人信息保护法》在完成对个人信息权益保障的各类强制性义务设立后，个人信息保护工作的重心也从损害救济转向为风险预防[24]。两部法律表现出了以个人信息保护为核心的共同意志。但作为反电信网络诈骗关键措施的信息监测共享机制，在现有法律规范体系下却与个人信息删除权的部分场景产生了矛盾交互。新型机制的运行对工作程序、规则的有机联系和有效运转中的信息审计、隐私治理和信息保护等要素应提出更加严格的周延保护要求。因此，疏解信息共享监测制度与个人信息删除权利之间的矛盾张力是进行法律融贯性有效解释的必然面向，扩张有关的删除权例外情形、细化监测共享内容和标准、明确留存时限和具体方式，

既是有效弥补法律间规则真空的有效方法，也是真正实现法律目的协同并进的实效措施。

参考文献

[1] 王玉环，崔现东，万晓玥，等. 国外电信网络诈骗治理经验及启示［J］. 通信世界，2021（18）：34.
[2] 陈伟. 中华人民共和国〈反电信网络诈骗法〉理解与适用［M］. 北京：中国法制出版社，2022：18.
[3] 献全国信息安全标准化技术委员会. 美国数字千年版权法［EB/OL］.（1998－10－29）［2023－01－06］. https://www.tc260.org.cn/front/postDetail.html?id=20141211132808.
[3] 鲁春雅. 论网络服务提供者的侵权责任［J］. 河南财经政法大学学报，2012（5）：58－68.
[4] 皮勇. 论网络服务提供者的管理义务及刑事责任［J］. 法商研究，2017（5）：14－25.
[5] 杨立新，赵鑫.《个人信息保护法》规定的本土被遗忘权及其保护［J］. 河南财经政法大学学报，2022（1）：60－71.
[6] 陈郝鹃，山丹，赵安晓宇. 电信网络诈骗犯罪预警实证研究［J］. 新疆警察学院学报，2020（4）：31－40.
[7] 刘鑫悦，范超云，李辉. 电信网络诈骗被害人群体特征及防范对策［J］. 云南警官学院学报，2022（4）：112－122.
[8] 赵知微. 供需模型视角下电信网络诈骗犯罪被害预防［J］. 网络安全技术与应用，2022（5）：153－156.
[9] 曹博. 个人信息权绝对权属性的规范依据与法理证成——从微信读书案切入［J］. 暨南学报（哲学社会科学版），2022（7）：16－28.
[10] 王利明. 论个人信息删除权［J］. 东方法学，2022（1）：38－52.
[11] 程啸. 论《个人信息保护法》中的删除权［J］. 社会科学辑刊，2022（1）：103－113.
[12] 孙玉荣，卢润佳. “场景完整性理论”的应用检视和功能再造——以个人信息保护司法裁判为视角［J］. 北京联合大学学报（人文社会科学版），2022（3）：70－79.
[13] 刘国. 个人信息保护的公法框架研究——以突发公共卫生事件为例［J］. 甘肃社会科学，2020（4）：156－162.
[14] 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［J］. 比较法研究，2015（6）：22－33.
[15] 程啸. 论我国民法典中的个人信息合理使用制度［J］. 中外法学，2020（4）：1001－1017.
[16] 范为. 大数据时代个人信息保护的路径重构［J］. 环球法律评论，2016（5）：92－115.
[17] 刘权. 论必要性原则的客观化［J］. 中国法学，2016（5）：178－195.
[18] 王锡锌. 行政机关处理个人信息活动的合法性分析框架［J］. 比较法研究，2022（3）：92－108.
[19] 张平.《中华人民共和国个人信息保护法》一周年观察［M］. 北京：法律出版社，2022.
[20] 郭春镇，王海洋. 个人信息保护中删除权的规范构造［J］. 学术月刊，2022（10）：92－106.
[21] 中国互联网络信息中心. 第49次中国互联网络发展状况统计报告［EB/OL］.（2022－02－25）［2023－01－13］. http://cnnic.cn/n4/2022/0401/c88－1131.html.
[22] 赵云，张笑笑. 基于等级保护的个人信息保护机制研究［C］//互联网安全与治理论坛论文集，2019：183.
[23] 辜凌云. 论数据泄露通知义务的制度构造［J］. 科技与法律（中英文），2023（3）：37－46，86.

（收稿日期：2023－07－04）

作者简介：

朱园伟（1998－），男，硕士研究生，主要研究方向：知识产权法、个人信息保护法。

（上接第63页）

[28] 孙晋，蓝澜. 数字垄断协议的反垄断法甄别及其规制［J］. 科技与法律（中英文），2023（1）：1－10.
[29] COMPETITION D. Finnish competition and consumer authority, Samkeppniseftirlitið, Norwegian competition authority, Swedish competition authority［J］. Joint Nordic Report. Online pharmacy markets in the Nordics, 2021.
[30] 叶明，朱佳佳. 算法共谋的竞争效应及其违法性认定研究［J］. 产业组织评论，2020，14（4）：1－17.
[31] POSNER R A. Oligopoly and the Antitrust Laws: a suggested approach 21 Stanford law review［J］. Journal of Reprints for Antitrust Law and Economics, 1969（1）：1575.

（收稿日期：2023－09－08）

作者简介：

刘奕麟（1995－），女，博士研究生，主要研究方向：反垄断法、国际竞争法。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部