非法获取个人征信数据的归责困境及疏解

孙梦龙 丁梦雨

摘　要：个人征信数据作为刑法中的公民个人信息、个人信息保护法中的敏感个人信息、征信领域法中的信用信息，导致非法获取个人征信数据的归责涉及民事、刑事及行政。在非法获取个人征信数据的场景中，立法的滞后与分散导致行政责任内部形成归责竞合；行、刑处罚标准的不贯通、行政处罚管辖权的割裂，阻隔行政责任与刑事责任的归责衔接；个人信息国家保护义务的构造，弱化民事归责中的个人诉权。为疏解这种困境，需修改征信领域等立法，将行政归责统一指向个人信息保护法；由网信部门会同其他部门协商确定行政裁量基准和双向的移送制度以建立归责的衔接；民事归责中，可通过司法解释确定关涉权益的范围，并修改个人信息保护法重构归责模式，以强化个人诉权。

关键词：个人信息；征信数据；归责；立法

中图分类号：D922.16　文献标识码：A　文章编号：1673-5706（2024）01-0106-08

非法获取个人征信数据的风险弥漫在征信机构等组织的内外部。中国人民银行曾通报个别商业银行员工利用职务便利，非法获取个人征信信息的问题[①]。司法实践中的刑事案件有迹可循，诸如方某甲、沈某原利用平安银行办公电脑系统非法查询个人征信报告出售[②]、颜某利用农村信用社内勤权限非法查询个人征信报告出售[③]等。内部工作人员亦存在非法获取个人征信数据的可能，例如，湖北某支行刘某某盗用账号非法查询个人征信报告出售[④]。征信机构亦具备非法行为的条件，据银罚决字【2023】71-73号，2023年8月，中国人民银行针对百行征信违反信用信息采集等的行为予以处罚[⑤]。外部风险更为严重，最高检检察机关依法惩治侵犯公民个人信息犯罪典型案例[⑥]、北京法院侵犯公民个人信息犯罪三起典型案例[⑦]，皆包括非法获取个人征信数据的案件。

基金项目：国家社科基金青年项目“司法区块链的制度体系、可能风险及应对策略研究”（20CFX005）。

① 参见2016年《中国人民银行关于加强征信合规管理工作的通知》。

② 参见（2015）甬慈刑初字第644号案。

③ 参见（2017）湘1382刑初422号案。

④ 参见（2016）鄂1221刑初125号案。

⑤ 参见中国人民银行官方网站行政处罚公示银罚决字【2023】71-73号。

⑥ 参见《关于印发检察机关依法惩治侵犯公民个人信息犯罪典型案例的通知》，载最高检官网。

⑦ 参见《北京高院召开北京法院侵犯公民个人信息犯罪案件审判情况新闻通报会》载中国法院网。

我国已出台若干保护个人征信数据的规范，如《征信业管理条例》（以下简称《条例》）、《征信机构管理办法》（以下《机构管理办法》）、《征信业务管理办法》（以下简称《业务管理办法》）等，这为个人征信数据的保护起到良好的作用。实践的需求推动《中华人民共和国网络安全法》（以下简称《网安法》）《中华人民共和国个人信息保护法》（以下简称《个保法》）《中华人民共和国数据安全法》（以下简称《数安法》）相继制定，造就个人征信数据的属性不断变得多元，呈现行政责任、刑事责任、民事责任并存的格局，同时造成若干归责困境。

一、个人征信数据的属性与归责

非法获取个人征信数据可触发刑事责任、行政责任、民事责任，三种责任具有不同的法律构造。

（一）个人征信数据的三元属性

首先，个人征信数据是征信相关法中的信用信息。个人征信数据最早为征信领域法所规制。1999 年中国人民银行《关于开展个人消费信贷的指导意见》出台，要求金融机构从银行信用记录做起，对每一位消费贷款客户建立个人档案，我国的个人征信数据库建设自始奠基。2005 年《个人信用信息基础数据库管理暂行办法》颁布，个人征信数据库的管理走上规范化道路。据《个人信用信息基础数据库管理暂行办法》[①]，个人征信数据的范围基本界定。2013 年颁布的《条例》《机构管理办法》未直接对个人征信数据予以界定。2021 年《业务管理办法》进一步明确个人征信数据的概念[②]。其次，个人征信数据是刑法中的公民个人信息。个人征信数据成为刑法的规制对象始自 2015 年《刑法修正案（九）》对刑法第二百五十三条的修改。随后，《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》（以下简称法释〔2017〕10 号）明确“征信信息”为侵犯公民个人信息罪的客体[③]。最后，个人征信数据为《个保法》中的敏感个人信息[④]。一是个人征信数据是《个保法》中的个人信息。从定义来看，个人征信数据不属匿名化处理后的信息，个人征信数据的识别性更加突出，其主要目的为判断个人在金融信贷领域的信用状况。从构成来看，个人征信数据包括个人基本信息、其他反映金融信贷情况的信息。《民法典》《个保法》《网安法》皆规定个人信息的概念，定义基本一致，核心要点在“识别性”。作为识别自然人信用状况的个人征信数据亦为规范意义中的个人信息。二是个人征信数据属于个人信息中的敏感个人信息。《个保法》规定“敏感个人信息是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息”。在最高检检察机关依法惩治侵犯公民个人信息犯罪典型案例中，涉个人征信案件在列，该案犯罪团伙非法获取并出售公民个人征信数据共计 31 万余条，违法所得钱款 450 余万元。以个人征信数据作为诈骗手段的犯罪案件亦不在少数，例如席某诈骗案中，席某谎称可消除不良征信，骗取他人巨额财物[⑤]。由此，个人征信数据的泄露与非法使用，不仅造成人格尊严的侵害，还会造成人身、财产的危害，个人征信数据应为敏感个人信息属实。

（二）非法获取个人征信数据的民事与刑事的归责模式

第一，刑事中的归责依据主要为《刑法》第二百五十三条。首先，从行为模式看，包括窃取、以其他方法非法获取两种，从语义上分析，窃取为非法获取的一种典型方式，以其他方法非法获取属于兜底条款。此外，法释〔2017〕10 号对以其他方法非法获取进行列举，主要包括“购买、收受、交换，在履行职责、提供服务过程中收集”。因此，

① 《个人信用信息基础数据库管理暂行办法》第四条规定个人信用信息的类型。
② 《征信业务管理办法》第三条规定信用信息的概念。
③ 法释〔2017〕10 号第五条，“征信信息”作为重点保护的客体被强调，个人征信数据当然为刑法中的“公民个人信息”。
④ 依据中国人民银行征信中心、百行征信、朴道征信公开的实际收集的数据类别，亦可得出此结论。
⑤ 参见（2019）内 0202 刑初 45 号案。

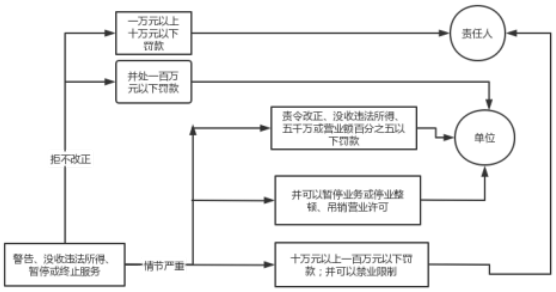
非法获取个人征信数据包括窃取，购买、收受、交换，在履行职责、提供服务中收集等方式。其次，以入罪情节来看，情节严重为入罪门槛，情节特别严重为量刑升格条件。据法释〔2017〕10号，情节严重具体包括“非法获取个人征信数据五十条以上的”等四种情形。情节特别严重指主要造成人身、财产的严重后果或数量特别大。

第二，民事中，非法获取个人征信数据的侵权责任涉及多部法律、行政法规和部门规章，但以引致条款为主。非法获取个人征信数据亦包括窃取、以其他方式非法获取两种，与刑事责任不同，对个人造成损失损害是成立民事责任的前提。基本的归责依据在《民法典》《个保法》。《民法典》明确宣示个人信息受法律保护，不得非法获取，并规定不承担民事责任的情形等规则，但未规定归责原则。《个保法》明确规定个人信息的归责原则、赔偿数额的确定方式，第六十九条规定，非法获取个人征信数据的归责原则为过错推定。

（三）非法获取个人征信数据的行政归责模式

第一，非法获取个人征信数据在征信领域法中的行政归责模式。《条例》第三十八条、《业务管理办法》第八条构建的非法获取个人征信数据的行政责任包括财产罚和行为罚。其中财产罚主要为罚款，没收违法所得的适用则可供裁量。罚款为“双罚制”，分别对单位、单位的直接责任人员处以罚款，幅度为单位五万至五十万元、个人一万至十万元。行为罚是指吊销征信机构的个人征信业务经营许可。在监管对象上，分为征信机构、金融信用信息基础数据库运行机构两类。

第二，非法获取个人征信数据在《个保法》中的行政归责模式。《个保法》未排除对征信机构、金融信用信息基础数据库运行机构的适用[①]，征信机构、金融信用信息基础数据库运行机构获取个人征信数据的行为是个人信息处理行为，在处理个人征信数据的场景中，征信机构等属个人信息处理者的范畴[②]。就征信机构、金融信用信息基础数据库运行机构而言，个人征信数据的监管主体仍是中国人民银行及其分支机构。《条例》《业务管理办法》规定信用信息的监管主体为中国人民银行及其分支机构，中国人民银行及其分支机构属《个保法》所规定的“在职责范围内”履行个人信息保护职责的部门。另外，在中国人民银行履职范围之外的部分，征信机构、金融信用信息基础数据库运行机构之外的组织、个人，非法获取个人征信数据的行为受网信部门、公安机关管理[③]。据《个保法》第六十六条，非法获取个人征信数据的行政处罚亦是“双罚制”，包括两种情形三个阶段（见下图）。



行政归责模式

二、非法获取个人征信数据的归责困境

多重责任叠加愈加放大归责困境。非法获取个人征信数据的行政责任具有执法依据多样、管辖主体多元的特点。同一行为可触犯不同规范，可由多个主体归责，导致不同的责任。行政责任与刑事责任裁量标准不同，导致案件移送不便，阻隔行刑归责的衔接。个人的归责能力畸弱是民事归责的突出问题。

① 《个人信息保护法》第十条规定：任何组织、个人不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息；不得从事危害国家安全、公共利益的个人信息处理活动。

② 《个人信息保护法》第四条规定：个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。第七十三条规定：个人信息处理者，是指在个人信息处理活动中自主决定处理目的、处理方式的组织、个人。

③ 《个人信息保护法》第六十条规定：国家网信部门负责统筹协调个人信息保护工作和相关监督管理工作。国务院有关部门依照本法和有关法律、行政法规的规定，在各自职责范围内负责个人信息保护和监督管理工作。

（一）行政归责存在多层次的竞合

首先，非法获取个人征信数据的行为者为征信机构、金融信用信息基础数据库运行机构时，根据《个保法》《条例》，监管主体皆为中国人民银行及其分支机构，但存在适用《条例》还是《个保法》予以处罚的疑问。非法获取个人征信数据的行为既符合《条例》，亦符合《个保法》，两者具有完全不同处罚条款、处罚思路、法律地位。一是非法获取个人征信数据的行政处罚规定不同。《条例》规定的比较简略，采用单位和个人皆处罚的“双罚制”，情节严重则可吊销经营许可。《个保法》规定的较为复杂，不仅规定警告、禁业限制等处罚，还区分出“拒不改正”和“情节严重”两种情况，情节严重的处罚额度也比较高，可上至五千万元。二是对非法获取个人征信数据的行为，《个保法》与《条例》的处罚思路完全不同。《条例》没有警告的阶段，直接对不法行为者处以罚款，《个保法》则规定有警告的阶段，只有在警告等处罚手段后“拒不改正”，才会上升到罚款层面。在“拒不改正”之前，《个保法》的处罚力度较小，在“拒不改正”之后，处罚力度比《条例》大许多。三是《个保法》与《条例》存在制定时间与法律位阶的错位。从法律位阶看，《条例》属行政法规，规则的适用限在征信信息领域；《个保法》为法律，具有适用的普遍性，关系所有的个人信息保护问题。以特别法优先一般法来看，《条例》作为征信领域法，规定的是征信领域的专门问题，应适用《条例》；以新法优先旧法来看，《个保法》是在《条例》生效之后制定的法律，包涵保护个人信息的普适性规则，应适用《个保法》。完全不同的两套行政处罚方式都具备执法依据，归责的竞合不可避免。此外，依据《网安法》第四十四和六十五条，公安机关也具备对征信机构、金融信用信息基础数据库运行机构的处罚权。在非法行为者是征信机构、金融信用信息基础数据库运行机构时，同一行为可触发三种行政归责模式。

其次，征信机构、金融信用信息基础数据库运营机构以外的组织、个人不属《条例》的规范对象。征信机构、金融信用信息基础数据库运营机构以外的组织、个人非法获取个人征信数据，虽不存在是否适用《条例》的问题，却也存在法律适用的竞合。依据《公安机关互联网安全监督检查规定》（以下简称《规定》）第二十五条规定，非法获取个人信息的，公安机关应按照《网安法》第六十四条的规定处罚。《个保法》亦规定非法获取个人信息的处罚，但《个保法》颁布在2021年，制定的时间比《网安法》和《规定》稍晚，在《个保法》制定时，公安机关已经具有处理非法获取个人信息的行政处罚权，结合《个保法》，履行个人信息保护职责的部门应包括网信部门、公安机关。征信机构、金融信用信息基础数据库运营机构以外的组织、个人非法获取个人征信数据的，网信部门、公安机关皆可依据《个保法》第六十六条予以行政处罚。公安机关作为《个保法》中的履行个人信息保护职责部门，同时具备适用《个保法》第六十六条、《网安法》第六十四条进行执法的依据。对非法获取个人征信数据的行为，公安机关可同时依据两套行政处罚制度予以处罚，归责的竞合也不可避免。故不法行为者是征信机构、金融信用信息基础数据库运营机构以外的组织、个人，可同时触发两种行政归责模式。

（二）刑事责任与行政责任的归责衔接存在多维度的阻隔

首先，刑事责任与行政责任归责标准不贯通。一是非法获取个人征信数据刑事责任的归责标准较明确。如前所述，刑法规定，侵犯公民个人信息罪的入罪标准为情节严重，法释〔2017〕10号解释情节严重的标准时，采用极为量化的指标[1]。综合入罪的若干项主要指标，从数量上看，非法获取个人征信数据五十条以上为情节严重，在刑事司法实践中，一般需核实侵犯公民个人征信数据的实际数量，据此作为定罪量刑的标准。从违法所得来看，以非法获取个人征信数据获利五千元以上为情节严重，在实践中，犯罪所得的数额是重要的量刑参照。据此，一般情况下，非法获取个人征信数据的入罪，有两条主要的、可混合适用的、直观且明确的平行标准，数量在五十条以上及犯罪所得在五千元以上。二是非法获取个人征信数据的行政责任归责标准不明确。非法获取个人征信数据的行为者是征信机构、金融信用

信息基础数据库运行机构时，依据《条例》，对单位和个人分别可处罚五万至五十万元、一万至十万元的罚款，情节严重的吊销经营许可，但归责门槛、处罚幅度都没有一个明确的量化指标，诸如何种情形应处罚何种罚款额度，“情节严重”如何判断，都没有具体的指标。中国人民银行及其分支机构，网信部门、公安机关适用《个保法》第六十六条处罚征信机构、金融信用信息基础数据库运行机构，其他组织、个人时，同样存在这一问题，“拒不改正”尚容易辨别，“情节严重”则缺少标准。

其次，行政归责的管辖权割裂。非法获取个人征信数据的行政归责涉及多个类别的主体。具有管辖权的行政主体为中国人民银行及其分支机构、网信部门、公安机关，行政行为的对象包括征信机构、金融信用信息基础数据库运行机构，其他组织、个人。不法行为者是征信机构、金融信用信息基础数据库运行机构时，管辖的主体既为中国人民银行及其分支机构又为公安机关；不法行为者是其他组织、个人时，管辖的主体既是网信部门又是公安机关。公安机关在办理案件中发现的涉嫌犯罪案件自然不必移送。中国人民银行及其分支机构移送的对象为征信机构、金融信用信息基础数据库，网信部门移送的对象为其他组织、个人。

最后，标准的不贯通、管辖权的割裂，共同造成行政责任与刑事责任归责移送的不衔接。行政责任与刑事责任归责标准的不贯通，是归责移送不衔接的基础原因。依据《中华人民共和国行政处罚法》第二十七条，违法行为涉嫌犯罪的，应先移送司法机关对犯罪行为进行处理。《个保法》第六十四条在个人信息保护领域对这一规定予以确认。在非法获取个人征信数据的归责中，行政责任裁量标准不明确、不量化，行政处罚的行政行为主体考虑非法获取个人征信数据的数量、违法所得的数额等量化内容成为不必要，行政行为的主体往往处在只知行政处罚不知是否涉嫌犯罪的境地，不自觉地以行政处罚代替刑事处罚，导致归责移送的不衔接。行政管辖的割裂，放大标准不贯通的弊端，固化归责移送不衔接的问题。征信机构经由中国人民银行审批获得经营资格，金融信用信息基础数据库运行机构属中国人民银行管理的事业单位，两者都与自身的监管机构存在千丝万缕的联系，行政处罚标准与刑事责任标准的不贯通，恰可为监管机构模糊被监管者不法行为的性质留下空间。依据《个保法》第六十四条，履行个人信息保护职责的部门发现涉嫌犯罪的不法行为，应移送公安机关处理，这是行政责任与刑事责任间的单向移送。《行政处罚法》规定的移送制度是双向的，对依法不需要追究刑事责任或者免予刑事处罚，但应当给予行政处罚的，司法机关应当及时将案件移送有关行政机关。行政管辖的割裂，放大这种单向移送的不衔接问题。公安机关具有对任何组织、个人非法获取个人征信数据的行政处罚权，在公安机关处理的涉嫌犯罪不法行为中，征信机构等最终被判定没有达到犯罪标准的，是否需要移送中国人民银行及其分支机构，便存在矛盾。

（三）民事归责中个人的诉权弱小

首先，民事归责中，个人诉权的实现存在权利范围不明的障碍。非法获取个人征信数据的民事责任以个人信息权益存在损害为前提。反之，非法获取个人征信数据，不存在个人信息权益的损害，应不承担民事责任。在刑事案件中，非法获取个人征信数据五十条以上为犯罪，例如，梁某侵犯公民个人信息罪一案中，梁某从其他不法份子手里购买个人征信报告 127 条，因而获刑①。此刑事案件中，个人征信数据被梁某非法获取的特定个人能否提起民事诉讼，需首先证明是否存在个人信息权益的损害。再如，在银罚决字【2023】71–73 号中，中国人民银行对百行征信予以警告、罚款 51.5 万元的处罚，理由包括非法获取信用信息等，虽行政监管不排斥民事诉讼，在行政处罚后，个人能否提起诉讼主张侵权责任，也存在个人信息权益是否遭受损害的认定前提[2]。一是《个保法》第六十九条所规定的“个人信息权益”具体内容，

① 参见（2019）苏 0321 刑初 639 号案。

实践中并无明确的规范性解释[3]。“个人信息权益”是财产权还是人格权，抑或同时具备财产权、人格权，没有清晰的界定[4]。另外，个人征信数据与其他个人信息不同，它是法律规定的需要强制收集的数据，又是敏感个人信息，以《个保法》构建的“告知—同意”为核心的个人信息自决权为基准，“个人信息权益”之于个人征信数据、一般个人信息，内涵并不完全一致。个人征信数据的特殊性质加重“个人信息权益”内容不明的诉讼难度。二是“个人信息权益”的内容不明使“造成损害”的数量计算落空。非法获取个人征信数据的行为模式具有特殊性，侵权者一般不会只获取特定个人的征信数据用以侵害特定个人的权益。不法行为者非法获取的个人征信数据存在一定的量级，特定个人的个人征信报告是确定、唯一的。即使非法行为者获取大量的个人征信数据，又通过出售等行为攫取不菲的违法所得，个人在其中的实际损害为何、不法者通过特定人的征信数据获取的违法所得为何，无论人格权益抑或财产权益，“损害”的量化相当困难。如此，个人的权利范围便不清晰，权利的行使走向真空。

其次，民事归责中，过错推定的归责模式削弱个人的诉讼权利。《个保法》规定，个人信息的侵权归责原则为过错推定[5]，行为者对个人信息权益造成损害，可证明没有过错时，将不承担民事责任。例如，在许某某侵权案中①，法院认为某公司确实损害许某某母亲的个人信息权益，但某公司可证明自己不存在过错，所以不应承担侵权责任。在个人信息国家保护的模式中[6]，个人要主张非法获取个人征信数据的侵权责任，在“个人信息权益”和“造成损害”范围不明时，除要举证个人信息权益遭受损害，还要期待行为者对自己无过错的证明不能。同等情形下的刑事责任、行政责任则容易证立。此外，《个保法》第七十条确立个人信息保护的公益诉讼制度，在刑事案件、行政案件中，检察院等法定主体可通过刑事附带民事公益诉讼等方式实现民事归责[7]。但对个人信息权益的保护也不能完全寄望利益中立、任务繁重的公共实体。个人不仅应在个人信息权益的保护中具备主体地位，还应具有相当的维权能力。侵权责任与刑事责任、行政责任的联系千丝万缕。非法获取个人征信数据可触发行政处罚、刑事犯罪，也可引发侵权责任，三者存在竞合也不等同个人需将自身权益的保护完全托付给国家。

三、非法获取个人征信数据归责困境的疏解进路

疏解个人征信数据的归责困境，可从解决行政归责竞合，行政责任、刑事责任归责衔接的阻隔，民事归责中个人诉权弱小三个方面着手。

（一）统一行政责任归责模式

首先，可考虑修改《条例》第三十八条，在征信领域法中，将非法获取个人征信数据的行政处罚指向《个保法》第六十六条。非法获取个人征信数据行政责任的多层次竞合，原因为立法的滞后性和分散性。任何法律都具有一定的滞后性，这是法律固有的特点。数字社会迅速发展，特定的事物往往短期内具有不同的立法需求，如此造成立法的分散无疑放大非法获取个人征信数据的立法滞后。《条例》颁布在 2013 年，彼时的网络社会发展还不充分，信息的载体以纸质文本为主，以数据作为载体的信息存储方式尚不普遍，非法获取个人征信的监管矛盾并不突出。其后，信息技术突飞猛进，《网安法》《个保法》《数安法》依次制定，个人征信数据的保护不仅涉及网络安全还涉及个人信息保护、数据安全。2021 年，部门规章《业务管理办法》出台，吸收《个保法》的若干精神，扩充个人征信信息的保护范围，但仍沿用 2013 年《条例》的处罚制度。《个保法》生效后，在对征信机构、金融信用信息基础数据库适用行政处罚方面，中国人民银行及其分支机构无论适用《条例》抑或《个保法》都具备执法基础，这种矛盾亟需解决。解决的最优路径是修改《条例》第三十八条，使其符合《个保法》第六十六条的规定。原因有三，一是《条例》已经

① 参见（2023）辽 03 民终 1358 号案。

制定十年，彼时对个人征信的保护并未涉及个人信息等问题，当下应对其修改以适用数字社会的实际需求。二是基于法律位阶[8]，《个保法》作为法律理应得到贯彻执行，修改《条例》适应《个保法》具有立法的法理基础。三是《个保法》的归责模式更优。罚金范围较《条例》的幅度更大，符合当下的经济社会发展；处罚梯度先柔和后严厉，能较好兼顾经济发展和个人权利保护。

其次，可考虑修改《网安法》第六十五条，由具体的处罚规定变为引致性条款，将对其他组织、个人非法获取个人征信数据的行政处罚指向《个保法》。原因有二，一是《网安法》颁布在2016年，主要目的为保障网络安全，彼时制定个人信息保护法的条件尚未成熟，《网安法》针对个人信息的保护也做一些规定，赋予公安机关非法获取个人信息的处罚权。2021年《个保法》制定，作为专门规范个人信息保护的法律，较《网安法》更为精细，《网安法》中涉及个人信息保护的规定已经完成历史使命，应调整为引致性条款，以方便涉及个人信息保护的行政处罚适用《个保法》。二是保证行政处罚的公平、统一。按照前述修改，对征信机构、金融信用信息基础数据库运行机构非法获取个人征信数据的处罚适应《个保法》第六十六条；其他组织、个人做出同样行为亦应得到相同行政处罚，否则将破坏法律适用的平等性。据此修改，结合《中华人民共和国行政处罚法》第二十五条，管辖的重叠将不是问题。无论网信部门、公安机关抑或中国人民银行及其分支机构，适用法律将具有统一性，法律适用的统一已经消弭管辖的重叠。

（二）完善行政责任、刑事责任归责的衔接制度

首先，应由网信部门会同有关部门商定非法获取个人征信数据的行政裁量基准。刑法严厉打击侵犯公民个人征信数据的行为，非法获取个人征信数据的行为较容易达到刑法的入罪标准，行政责任的适用反倒不紧迫。同时，对非法获取个人征信数据的行为者行使行政处罚权的管辖部门比较分散，并不是所有部门与司法机关的沟通、联系都如此密切，这容易造成以行政处罚代替刑事处罚的结果。基于非法获取个人征信数据的多方管辖特点，非法获取个人征信数据的行政责任的处罚裁量标准，应由网信部门会同中国人民银行、公安机关、检察机关、人民法院商定细则。网信部门作为个人信息保护的统筹协调机构，应承担规则制定的责任。中国人民银行、公检法机关都是个人征信数据保护场景中的职责部门，多方参与可将实践中的需求加入规则中。在行政裁量基准的制定中，应采用量化的方式，重点确定《个保法》的行政归责模式中，第一阶段情节未达严重、第三阶段“情节严重”的数额标准。

其次，应建立非法获取个人征信数据案件的双向移送机制。所谓双向移送制度，是指在非法获取个人征信数据的行政处罚中发现涉嫌犯罪的，中国人民银行及其分支机构、网信部门应将案件移送至公安机关；公安机关在处理涉嫌侵犯公民个人信息罪的过程中，发现达不到犯罪标准的，行为者如果是征信机构、金融信用信息基础数据库运行机构，应将案件移送给中国人民银行及其分支机构接受行政处罚。具体而言，双向案件移送制度的结构包括三个主体、两个方向。中国人民银行及其分支机构、网信部门将非法获取个人征信数据犯罪案件移送给公安机关，这是贯彻《个保法》第六十四条规定的基本要求；公安机关将达不到犯罪标准的案件移送给中国人民银行及其分支机构，依据在《中华人民共和国行政处罚法》第二十七条，即对不必追究刑事责任以及免于追究刑事责任的案件，应及时移送至行政机关。对公安机关处理的不涉嫌犯罪的非法获取个人征信数据案件，则不必移送，如前述修改，公安机关可直接依据《个保法》第六十六条处罚。

（三）强化民事归责中的个人诉权

首先，强化民事归责中的个人诉权可诉诸司法解释。对个人征信数据的“个人信息权益”的解释，应基于敏感个人信息的特点考虑，不应只局限在《个保法》以“告知—同意”为中心构建起来的个人信息自决权，还应包括《民法典》中的个人信息人格权。这些内容以侵权法为枢纽，可达到较好的联结。同时，对“造成损害”亦应做出扩大解释。非法获取个人征信数据的行为者

不可能只获取特定个人的数据，其违法所得、侵犯的征信数据造成的实际损害难以分离、量化到具体的个人。个人在论证非法获取个人征信数据具有损害方面具有操作的困难，“造成损害”应包括个人为维护个人信息权益而耗费的成本、被非法获取的个人征信数据暴露的范围等。[①]其次，强化民事归责中的个人诉权还需重新构造非法获取个人征信数据的归责原则。一是《个保法》中，个人信息的民事侵权归责原则为过错推定，这种模式有待优化，可考虑修改《个保法》第六十九条，增加无过错责任一项。基于业务经营等原因，在特定个人信息遭受非法获取时，持有特定个人信息、负有个人信息保护义务的企业等组织应承担无过错责任。具体而言，在其他组织、个人，非法获取个人征信数据的场景中，具有个人征信数据保护义务的组织应承担无过错责任。该种责任与非法获取个人征信数据的其他组织、个人连带承担。二是可考虑在《个保法》第六十九条中增加禁止非法获取个人信息一项。《个保法》中的“处理个人信息”应做限缩，理解为本身带着合法的权限、合理的目的处理行为，如此可与《民法典》的责任免除制度对接。如果本身带着非法的目的，自不应讨论过错的存在与否，不应适用《个保法》第六十九条的过错推定原则，而应直接按照损害承担侵权责任。只有本身带着合法的权限、合理的目的处理个人信息时造成损害的，才适用过错推定原则和《民法典》的责任免除制度。基于对此处的限缩解释，在《个保法》第六十九条，还应明确增加禁止非法获取个人信息的规定。

四、结语

非法获取个人征信数据的归责困境，亟需通过统一行政责任的归责模式，构建刑、行归责衔接制度，在民事归责中强化个人诉权来解决。前述归责困境，既是非法获取个人征信数据的专属困境，又是个人信息保护领域的普遍问题，对非法获取个人征信数据的归责困境的解决，本就带着解决个人信息保护领域的普遍归责问题的隐性审视。个人信息保护多主体多结构的归责模式，一方面表明在社会发展中，立法者一刻不停地紧盯个人信息保护，采取多种措施；另一方面也表明个人信息保护的全部核心问题并未完全揭开面纱，亟需在法律的不断适应中解决实际需求。

参考文献：

[1] 冯文杰．大数据时代个人征信信息的刑法保护机制创新 [J]. 征信，2022，（4）.

[2] 王锡锌．重思个人信息权利束的保障机制：行政监管还是民事诉讼 [J]. 法学研究，2022，（5）.

[3] 杨立新．个人信息处理者侵害个人信息权益的民事责任 [J]. 国家检察官学院学报，2021，（5）.

[4] 高富平，李群涛．“个人信息权益”的民法新定位 [J]. 东岳论丛，2023，（6）.

[5] 杨显滨，王秉昌．侵害个人信息权的民事责任——以《个人信息保护法》与《民法典》的解释为中心 [J]. 江苏社会科学，2022，（2）.

[6] 王锡锌．个人信息国家保护义务及展开 [J]. 中国法学，2021，（1）.

[7] 蒋红珍．个人信息保护的行政公益诉讼 [J]. 上海交通大学学报（哲学社会科学版），2022，（5）.

[8] 李爱君．个人征信信息法律规制研究 [J]. 中国应用法学，2023，（2）.

作者：孙梦龙，黑龙江大学法学院 2021 级民商法博士研究生

丁梦雨，郑州大学营商环境法治研究中心助理研究员

责任编辑：谭博文

① 我国台湾地区《个人资料保护法》的个人信息损害赔偿制度值得借鉴，其第二十八条规定“如被害人不易或不能证明其实际损害额时，得请求法院依侵害情节，以每人每一事件新台币五百元以上二万元以下计算”。