

违法处理个人信息的后果二分与责任衔接

贺 彤

中国社会科学院法学研究所, 北京 100009

摘 要: 我国个人信息保护呈现“刑先民行后”的立法进程, 违法处理个人信息的刑事责任与民事责任存在衔接问题。《中华人民共和国民法典》将个人信息分为私密信息和非私密信息, 违法处理私密信息构成隐私侵权; 而《中华人民共和国个人信息保护法》未规定私密信息, 违法处理非私密信息构成行政违法, 故两种个人信息的违法处理后果不同。违法处理个人信息的刑事责任认定, 需要先判断涉案个人信息是否私密, 以认定隐私侵权抑或行政违法, 继而以不同标准判断是否构成刑法中的情节严重, 从而实现违法处理个人信息的民刑、行刑责任衔接。既有规范中的情节严重标准存在不足, 应在区分私密和非私密信息基础上, 严格计算违法处理入罪的信息条数、违法所得金额。

关键词: 违法处理个人信息; 私密信息; 隐私侵权; 行刑衔接; 情节严重

中图分类号: D922.16

文献标识码: A

文章编号: 1672-3805(2026)04-0053-12

基金项目: 国家资助博士后研究人员计划“公共信用信息处理的法律规制研究”(GZC20241963); 2025年博士后第77批面上项目“侵害个人信息权益的法律责任衔接研究”(2025M770638)

作者简介: 贺彤, 中国社会科学院法学研究所助理研究员、博士后, 研究方向为数字法学。

一、问题的提出

我国的个人信息保护呈现“刑先民行后”的立法进程。个人信息保护的刑事立法始于2009年2月28日, 第十一届全国人大常委会第七次会议通过《中华人民共和国刑法修正案(七)》, 增加第253条之一“出售、非法提供公民个人信息罪”。2015年8月29日, 第十二届全国人大常委会第十六次会议通过《中华人民共和国刑法修正案(九)》, 将第253条之一改为“侵犯公民个人信息罪”, 增设从重处罚规定, 并将本罪的法定最高刑由有期徒刑3年提高至7年, 加大对侵犯公民个人信息行为的刑法打击力度。个人信息保护的行政立法则始于2016年颁布的《中华人民共和国网络安全法》。其后, 我国陆续出台《中华人民共和国民法总则》(2017年)、《中华人民共和国民法典》(2020年)(以下简称《民法典》)及《中华人民共和国个人信息保护法》(2021年)(以下简称《个人信息保护法》), 由此建立较为成熟的个人信息民行刑保护法律体系。此外, 个人信息保护的刑事司法也走在民法和行政法之前。2017年, 最高人民法院、最高人民检察院颁布《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《解释》), 相较于后续施行的《民法典》《个人信息保护法》, 将“特定自然人的活动情况”纳入规制范畴, 对个人信息的保护更加细致。可见, 刑法走在个人信息保护前列, 因而欠缺来自民法、行政法有关法益侵害的知识供给^[1]。

我国个人信息保护“刑法先行”的立法进程, 造成民行刑规范在个人信息保护法益与个人信息范围等方面存在立法脱节, 也带来违法处理个人信息入罪边界不清等民刑、行刑责任衔接不畅问题^[2]。根据《中华人民共和国刑法》(以下简称《刑法》)第253条之一可知, 向他人出售或者提供公民个人信息的行为在“违反国家有关规定”且“情节严重”的情况下构成侵犯公民个人信息罪, 而对于个人

信息保护的“国家有关规定”主要见诸《民法典》《个人信息保护法》，但不应包括地方性法规、地方政府规章，以避免犯罪成立条件上的混乱和不统一^[3]。这表明对于违法处理个人信息而言，只有在违反个人信息保护规范并构成情节严重时才成立犯罪，说明《民法典》《个人信息保护法》与《刑法》在个人信息保护的法益上具有实体性衔接。通过明确违法处理个人信息的不法后果及其侵害的法益，可完善侵犯公民个人信息罪的“情节严重”标准，实现民刑、行刑责任的规范、合理衔接。在轻罪立法呈现积极态势背景下，讨论违法处理个人信息的责任衔接问题，既有利于民行刑规范和民刑、行刑衔接的准确适用，避免过度刑法化和行刑双重处罚，确保过罚相当和一事不二罚，也有助于督促行政机关履职，解决个人信息保护前端治理失灵问题，实现个人信息的全周期保护。

二、个人信息及其违法处理后果的二分

《民法典》第1034条将个人信息分为私密信息与非私密信息，二者的违法处理将引发不同法律后果。刑法也应基于民法分类，分别评价私密信息与非私密信息的违法处理。

(一)违法处理私密信息的民事侵权后果

《民法典》将个人信息二分为私密信息与非私密信息。《民法典》第1033条将“除法律另有规定或者权利人明确同意外”的“处理私密信息”行为纳入隐私侵权范围，违法处理私密信息一旦发生，即被认为造成人格上的隐私损害，属于实害行为。关于违法处理私密信息的侵权损害认定问题，就被转换为私密信息的范围界定问题，易言之，权利人无需举证证明隐私侵害后果，只需证明行为人违法处理的个人信息是私密信息。

根据《民法典》第1032、1033条规定，与私密信息并列的还包括私密空间、私密身体部位和私密活动，具有“不愿为他人知晓”的共同特性。例如，卧室是典型的私密空间，性器官是主要的私密身体部位，其与办公室等工作或社交空间、四肢等一般身体部位相比显著不同。可见，隐私排斥不具亲密关系的他人，旨在营造高度信赖的环境，实现高度自主^[4]。

私密信息应以是否排斥他人作为判断标准——即只能由自己知晓或仅在亲密关系者之间产生和分享。例如，私人信件、日记、私聊信息、高度反映个性的查询访问记录等，其承载了信息主体基于高度信赖而产生的信息，体现高度自主性，故社会风俗和法律均禁止任何组织或者个人将之隐匿、毁弃或查阅。又如，个体在专属网络账号中的高度自主表达也属于私密信息，故盗号行为构成对他人私密信息的非法收集。以“张某侵犯公民个人信息罪案”为例。张某在其经营的移动营业厅内为顾客办理业务过程中，未取得顾客同意，私自将顾客的手机号码及其接收的验证码发送至“京东拉新”“淘宝拉新”等微信群，并指使店员赵某以同样方法发送至上述微信群，供他人用于注册京东、淘宝等软件账号，被法院判处侵犯公民个人信息罪^①。在此类案件中，手机号码是个体与外界联络的主要信息，故获取、提供手机号码不构成隐私侵权。但窃取密码(包含验证码)擅自登录账户或通过信息技术侵入账户，则构成窥探他人隐私。需要注意的是，账号密码不属于个人信息，不论密码设置是否与个体相关联，与个人信息没有必然关联，人们不会使用密码识别个体或被他人识别，因此窃取密码不属于非法收集个人信息。凭借密码登录的账户大多有“个人空间”“个人中心”或仅本人与选中好友可见的虚拟空间，是值得信赖的私密环境，个体通常会在其中收藏、记录或上传高度个性化的私密信息，自主决定是否将其公之于众。因此，未经信息主体同意，擅自获取密码，注册、登录其账户，损害信息主体对私密空间、私密信息的高度自主，构成隐私侵权。

此外，有学者认为电话号码、工作单位、身份证号码等属于私密信息，这些信息泄露引发的

① 江苏省连云港市连云区人民法院(2021)苏0703刑初205号刑事判决书。

电话骚扰与广告推销构成对生活安宁的严重侵害^[5]。但在面对电话骚扰、广告推销时，可以拒绝接听并予以标记和拦截，故其正常生活秩序不会因此受到明显侵扰，而往往只会心生厌烦（除非这些骚扰电话、短信传递出人身威胁内容），但这种厌烦一般不属于法律需要救济的精神损害，法院也不会将之认定为隐私侵权。如在“戎某与吕某隐私权纠纷案”中，原告认为被告将其姓名、住址、电话号码等信息通过业主群传播出去，导致其收到大量广告及诈骗电话骚扰，影响原告日常生活。而法院认为，公布上述信息一般情况下并不会造成人内心的强烈不安，原告亦无证据可证明其发生了相应损害结果，故不构成对隐私权的侵害^[6]。实际上，姓名、电话、身份证号码等信息属于与外界交流的必要信息，若不为人所知，个体将无法取得社会交往所需信任基础。因此，不能因为收到骚扰和推销信息，就将个人信息全部视为私密信息而禁止公开、交流。

（二）违法处理非私密信息不构成民事侵权

《民法典》第1034条规定，“个人信息中的私密信息，适用有关隐私权的规定”，而个人信息中的非私密信息则不适用。原因分析如下。首先，非私密信息可以被他人知晓，违法处理非私密信息不会直接造成侵权损害。法律上的因果关系认定通常采用相当因果关系说，该理论支持回溯禁止说，即在第三人的故意行为造成损害时，对该行为起到间接促成作用的行为不符合相应结果犯的构成要件^[6]。由此，侵犯非私密信息的行为不对被害人的后续损害负有法律上的责任。如在“陈某与上海瑞慈瑞兆门诊部有限公司隐私权纠纷案”中，被告将记录有原告会员号、真实姓名、出生年月、手机号码及家庭住址的申请表作为填写样板使用，造成个人信息泄露。法官认为这些信息“在社会交往和公共管理中必须在一定范围内为社会特定人或者不特定人所周知”，属于一般的个人信息^[3]，被告行为不构成侵权。显然，法官所说的“一般的个人信息”，是个人须向外界公开或自愿让他人获取的，否则他将无法开展正常的社会交往。《个人信息保护法》未区分私密和非私密信息，而区分敏感与不敏感个人信息。“敏感”是指一旦被泄露或违法处理就“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”，意味着敏感个人信息可以被他人依法合理处理，区别于排斥他人的私密信息，属于非私密信息。可见，即便对于受到普遍重视的敏感个人信息而言，违法处理只是带来受损的高风险，而非直接造成损害。如在“尹某侵犯公民个人信息罪案”中，法院认定被告人尹某在其家中注册账号登录暗网，向他人购买公民身份证、手持身份证照片、企业营业执照、公民护照等公民个人信息，下载并整理分类后上传至网盘，后将网盘链接发布至暗网销售，经清点共计39 017条，使得大量公民个人信息处于不安全环境^[4]，构成侵犯公民个人信息罪。但根据判决书可知，该侵权行为未使信息主体承受实际损害，本案尚未发生信息主体被冒用身份且人身财产权利受损之后果。有法官明确表示，有的案件没有非法获利或者具体被害人数量，无法确定损害赔偿，不少侵犯公民个人信息犯罪行为的损害对象较少、损害程度不明确^[7]。通常而言，我国民事裁判中认定因果关系采取的证明标准至少达到85%的“高度盖然性”，即法官虽不能排除其他盖然性，但已经能够得出待证事实十之八九是如此的结论^[8]。即便有学者认为该标准门槛过高而采用“明晰可信”标准，也要求待证事实的存在概率至少高于75%^[9]。显然，违法处理私密信息之后发生侵权的概率未达如此之高，如有学者计算得知，违法处理个人信息后诈骗风险的发生概率小于0.15%^[10]。因此，违法处理非私密信息不能认定为侵权。

其次，违法处理非私密信息不构成对信息自决权的侵权损害。我国不少民法、刑法学者将个人信息保护的权理论证为信息自决权^[11]，将之作为侵犯公民个人信息罪的法益，认为侵犯公民个人信息罪保护的是个人决定其信息是否公开、对谁公开、公开到何种程度的自主^[12]。然而，信息自决

② 上海市静安区人民法院(2021)沪0106民初51000号民事判决书。

③ 上海市普陀区人民法院(2020)沪0107民初5934号民事判决书。

④ 江苏省无锡市惠山区人民法院(2021)苏0206刑初741号刑事判决书。

权不完全适用于非私密信息。人们对大多数非私密信息无法控制和支配^[13]。如无法阻止他人了解自己的姓名、电话、邮箱、住址等基本信息,也无法阻止他人对个人信息的公开和不含侮辱、诽谤内容的评价。根据《民法典》第1025条,除捏造、歪曲事实,对他人提供的严重失实内容未尽到合理核实义务,以及使用侮辱性言辞等之外,这种公开和评价个人信息的行为不承担民事责任;根据《民法典》第1027条,发表以真人真事或者特定人为描述对象的文学、艺术作品,只要不含有侮辱、诽谤内容,亦不构成民事侵权。显然,上述对个人信息的公开和评价,若内容真实且未侮辱、诽谤,信息主体无法自主控制相关个人信息。如果坚持以“信息自决”作为个人信息保护的核心,试图将所有个人信息由个体控制和支配,则会导致知情同意规则失灵。可见,基于“个人自治”的私法保护路径无法满足个人信息保护要求^[14]。正如学者所言,个人信息保护最初的功能定位,便是国家主导的规制与治理策略,将个人对其信息的自决作为制度设计的基点与主线,不利于实现保护个人权益的效果^[15]。因此,违法处理非私密信息不构成对信息自决权的侵害。

最后,违法处理非私密信息之后引发的侵权损害不应直接归因于处理行为。如在“徐玉玉被电信诈骗案”中^⑤,法院认定陈某通过腾讯QQ、支付宝等工具从杜某处购买非法获取的山东省高考学生信息10万余条,并使用上述信息实施电信诈骗活动,冒充国家机关工作人员,通过拨打电话对不特定多数人实施诈骗,构成侵犯公民个人信息罪和诈骗罪,数罪并罚。此外,提供陈某个人信息的被告人杜某,利用技术专长非法侵入高等学校招生考试信息平台,窃取考生个人信息64万余条,出售考生个人信息10万余条,包含学生姓名、性别、出生年月、考籍号、身份证号码、家庭住址、所属学校、家长姓名和联系方式等,构成侵犯公民个人信息罪。尽管法院在判决书中认为,杜某非法获取和售卖个人信息行为“造成恶劣社会影响,情节特别严重”,但并未认定该行为与诈骗结果的因果关系,这就意味着侵犯非私密信息不会直接导致被害人的财产损害。同样,在诸多侵犯个人信息的民事公益诉讼案件中,检察机关认为违法处理个人信息“易引发犯罪”“威胁财产乃至生命安全”“具有危害财产安全的可能性”等,表明个人信息被违法处理后,诈骗等尚未发生,而是为侵权行为提供了有利条件,增加了损害发生的可能性。总之,违法处理个人信息与公民人身、财产权利损害呈间接因果关系,在此之后的侵权行为并不必然发生,故不能将损害结果归因于违法处理行为。正因如此,司法实践中不应将违法处理个人信息之后发生的损害直接归因于违法处理个人信息行为本身。

(三) 违法处理非私密信息的行政违法后果

违法处理非私密信息不适用侵权保护,但该行为违反个人信息保护规则。个人信息保护规则是以维护处理秩序为目的、以行政法义务为主要内容、以行政法责任为保障的规范,故违法处理非私密信息的后果是破坏行政法秩序。

首先,个人信息保护规则弱化私法属性,旨在构建个人信息处理的公共秩序。一方面,告知同意倾向于取得概括同意,弱化个人信息处理的私法属性。告知同意规则一定程度上延续私法中侵权保护的制度逻辑,意味着信息主体在处理者充分告知的前提下,既能够理解处理活动的全部内容,又能够对风险处理作出评估,由此依靠自由意志理性决定是否同意个人信息进入处理活动之中^[16]。个人信息处理海量且实时,信息主体的同意只能是概括的,否则,其日常生活与信息社会的发展进程将受到严重阻碍。这种概括的同意,无法构成信息主体的真实意思表示,故常见隐私政策协议难以构成平等主体基于真实意思表示而缔结的合同,违法处理难以成立民事违约。例如,用户在安装App时点击“同意”,并不能成为运营者在个人信息收集处理问题上恣意妄为的借口,易言之,概括

⑤ 徐日丹:《公诉人详解徐玉玉被电信诈骗致死案办案历程》,载最高人民检察院官网, https://www.spp.gov.cn/spp/zd gz/201706/t20170627_194085.shtml。山东省临沂市中级人民法院(2017)鲁13刑初26号刑事判决书,山东省临沂市罗庄区人民法院(2017)鲁1311刑初332号刑事判决书。

同意不能成为处理者超出法定限度处理个人信息的合法依据。显然，个人信息处理规则已跳脱单纯保护公民个人信息私权，具有强行法特点，不再以告知同意为核心，而是注重对公法义务的履行。个人信息保护的宗旨是追求个人信息资源的合理有序流动^[2]，故注重规制个人信息处理行为，应当定位于行为法^[17]。另一方面，合目的、最小范围、准确完整等处理规则旨在构建个人信息处理的公共秩序。合目的规则要求处理者在处理活动过程中只能执行与收集个人信息的目的相符的操作，而不得与其他目的不当关联。“直接相关”要求“间接相关”的处理活动也应被禁止。最小范围规则要求个人信息收集的范围和手段应在众多方案中选择损害最小实现方式。准确完整规则要求处理者确保其所处理的个人信息准确、完整，避免信息主体因个人信息篡改、失真而遭受权益损害。这些规则旨在划定个人信息处理的合理界限，为处理者设置公法上的义务，由国家网信部门和其他部门负责监督管理，构建和维护个人信息处理的公共秩序。根据《个人信息保护法》第1条的立法目的，这种公共秩序主要体现为处理者依法处理个人信息的安全秩序和个人信息合理利用的流通秩序，由于受到公法规制，故同时蕴含国家对个人信息处理活动的监管秩序。

其次，个人信息保护规则为处理者和有关行政主体设置了行政法义务。《个人信息保护法》设置处理者的行政法义务以保障个人信息处理的法秩序，要求处理者在处理个人信息前满足必要安全条件，预防信息风险；采取必要安全保障措施，如制定内部管理制度，采取安全技术措施，合理确定处理操作权限并定期开展安全教育和培训，制定并组织实施相关应急预案等^[4]。《个人信息保护法》还规定了个人信息保护行政主体的法定职责，通过规则制定、事中监管与事后处置等方式保障处理活动合法，实现信息风险防范^[18]。如《个人信息保护法》第62条规定有关部门制定个人信息保护具体规则、标准；第63条规定行政主体可采取检查、调查、询问、查阅等监管措施；第64条规定行政主体在发现较大风险或者发生个人信息安全事件之后，可要求处理者约谈或进行合规审计。即便是法律赋予信息主体的查阅、复制、更正、删除等权利，也是为个体化、全方位监督个人信息处理者的合规情况，以弥补行政监管在资源和信息上的不足^[19]。总之，个人信息保护规则以处理者和行政主体的行政法义务为主要内容，处理者侵犯公民个人信息的本质是违反其行政法义务和破坏公法秩序。

最后，个人信息保护规则设置对违法处理的行政处罚。《个人信息保护法》对信息处理者违法行为实施行政处罚，指向规避个人信息处理中的不特定风险，旨在建构一种稳定的公法秩序，以实现对个人信息处理活动的全过程监控^[20]。因违反个人信息处理规则而受到行政处罚的违法处理属于“单纯的不服从行为”，很大程度上承担的是一种不配合责任，即该行为的违法性在于不配合执法部门履行公法义务，而不在于行为的危害性。因此，违法处理非私密信息的后果是行政违法而非侵权损害。

综上可知，违法处理个人信息存在两种不法后果，一是违法处理私密信息的隐私侵权，二是违法处理非私密信息的行政违法。由此，《民法典》和《个人信息保护法》可以为侵犯公民个人信息罪提供民法和行政法上的法益侵害依据，进而通过规范解释衔接违法处理个人信息的法律责任。

三、两种违法处理后果的法律责任衔接

在既有个人信息保护的司法实践中，判决书往往不区分私密信息和非私密信息，而是直接列出个人信息种类，对涉案个人信息的私密性或敏感性等缺乏必要说明和论证，也未能提炼关于涉案个人信息的裁判规则。这表明司法机关在实践中尚未厘清民事或行政上的违法性就直接判处侵犯公民个人信息罪，不利于该罪的准确适用与公民权利保障。根据《刑法》第253条之一可知，构成侵犯公民个人信息罪须满足“违反国家有关规定”和“情节严重”。可见，对于本罪而言，刑事犯罪、民事侵权或行政违法的区别在于对相同法益不同程度的侵害，应当先适用《民法典》《个人信息保护法》判断行为违法性，在此基础上，分别判断私密信息和非私密信息违法处理是否“情节严

重”,由此实现民刑、行刑责任衔接。

实践中,司法机关对“情节严重”的认定也颇具争议,作为主要认定依据的《解释》存在诸多不足之处,如未区分私密与非私密信息、未规定违法处理私密信息的严重情形;虽区分不同种类个人信息在非法处理时构成犯罪的数量,但未形成较为合理的区分标准,且非法获取、出售或者提供个人信息数量的情节严重标准过低。由此,下文将在区分私密信息和非私密信息的基础上,根据两种违法处理行为的侵害法益,分别判断情节严重,以实现刑法与民法、个保法的有效衔接^[21]。

(一) 违法处理私密信息的民刑责任衔接

我国刑法未明文规定隐私犯罪,尚未确立隐私权独立的刑法地位^[22],目前关于披露他人身体隐私、私生活信息的刑事案例主要适用侮辱罪。根据《刑法》第246条可知,构成侮辱罪需要满足“情节严重”这一后果要件。在侵犯私密信息构成侮辱犯罪的案件中,法官对侵害后果达到严重情节的认定,蕴含对侵犯私密信息情节严重的判断标准。如在“王某甲、王某乙侮辱罪案”中,王某甲在与自诉人赵某恋爱期间,用手机拍摄含有自诉人正面表情及声音的隐私视频,后传给被告人王某乙,而被告人王某乙又通过微信平台公然传播自诉人隐私视频。法院认为,被告人王某甲对危害后果的发生持放任态度,具有侮辱自诉人的共同故意,对王某乙的行为客观上起到协作、帮助作用,二被告人的行为共同构成侮辱罪^⑥。本案中含有赵某身体隐私的视频属于私密信息,被告人的传播行为不仅构成侮辱罪,同时构成侵犯私密信息犯罪。法院认定王某乙行为情节严重而构成犯罪的理由,主要在于其通过微信平台公然传播自诉人隐私视频。该行为的严重情节主要有两方面:一是隐私视频内容极度私密,被害人的私密身体部位、私密活动及私密语言等本来仅可与伴侣分享的信息被公开;二是通过微信平台公然传播,其中,“微信平台”意味着该隐私视频在认识被害者的人之间传播,“公然”意味着传播范围较广,使被害人在其社交圈面临“社会性死亡”。信息内容越私密,可以分享的信赖范围就越小,社会观念越倾向于将该信息泄露行为认定为犯罪^[23]。此外,侵犯私密信息是否入罪,与和受害者有关联的知晓人数相关。在私密信息泄露后,和信息主体有关联的知晓人数越多,信息主体接收的负面评价就越多,受到的精神痛苦就越严重。

私密信息泄露后的实际影响,也是判断情节严重的重要依据。如在“王某侮辱案”中,王某在QQ空间及微信朋友圈里上传和发布袁某的裸照及其与唐某的私密照,在朋友圈、亲友圈等范围内传播。一审法院认为其行为对被害人人格、名誉造成一定影响,但尚未达到情节严重,不构成犯罪,而二审法院则认为该行为已对被害人的生活及声誉造成影响,情节严重,故改判有罪。显然,对被害人生活及声誉的实际影响也是判断情节严重的重要考量因素。不同私密信息的违法处理对被害人的实际影响有所不同。通常而言,记录私密身体部位等的信息高度私密,违法处理对被害人的实际影响极大。私聊记录、私人日记、私人账号空间等同样高度私密,有的人在这些私密信息被泄露后,因不堪其辱而轻生。因此,作为判断情节严重的重要依据,私密信息泄露后的实际影响因人而异,具有较强主观色彩,需在案件中具体认定。

综上所述,私密信息的可信赖范围、与信息主体关联的知晓人数以及私密信息泄露后的实际影响,是判断违法处理私密信息情节严重的重要依据。

此外,《解释》对违法处理非私密信息的“情节严重”设置了信息数量标准,但对于违法处理私密信息而言,信息数量对情节严重的认定影响不大。在上述泄露受害人私密视频、照片的刑事案件中,法院在认定“情节严重”时均未关注信息数量,而十分重视信息私密程度。违法处理大量私密程度较低的信息可能仅涉及隐私侵权,而违法处理单条私密程度较高的信息则可能构成“情节严重”。一定数量的同尺度私密信息在泄露后,外界会对受害者形成相对稳定的认识和评价,且这种

⑥ 山西省吕梁市离石区人民法院(2016)晋1102刑初91号刑事判决书。

认识和评价不会因私密信息数量而明显变化，只有在获取更大尺度的私密信息后，才会对受害者产生新的认识和不利评价。因此，违法处理私密信息的“情节严重”更关注信息的私密程度，而非信息数量。

（二）违法处理非私密信息的行刑责任衔接

违法处理非私密信息的后果是行政违法，其行刑责任衔接的核心在于对“情节严重”的判断。与违法处理私密信息“情节严重”关注的人格侵害程度不同，违法处理非私密信息的“情节严重”关注处理行为的违法程度，即超出合理处理范围或违背法定义务的严重程度。

不同个人信息的合理处理范围存在差异。与私密信息不同，非私密信息具有一定可公开性和可使用性，可在一定范围内被他人获取和处理。根据《个人信息保护法》第27条规定，“个人信息处理者可以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；个人明确拒绝的除外”。易言之，处理信息主体自行公开或虽非自愿但已被合法公开的个人信息，可默认为已取得同意，只要未超出合理范围，无论被处理到何种程度，均不构成违法，不宜定罪^[24]。而超出合理范围处理个人信息，则被认为是超过个人信息公开限度的违法处理，破坏了个人信息保护秩序^[25]。实际上，不同的非私密信息可公开范围不同。欧阳本祺按照“私密性”高低，将个人信息分为最核心层的隐私领域、中间层的私人领域、最外层的社会领域^[13]。隐私领域的个人信息属于私密信息，根据《个人信息保护法》中的敏感个人信息概念，可将非私密信息分为两类：广泛公开的不敏感个人信息与有限公开的敏感个人信息。

广泛公开的不敏感个人信息是个体为使更多人了解自己而必须或自愿公开的信息。姓名、国籍、民族、籍贯、邮箱账号等均在此列。生活中，他人通过获取姓名、相貌等个人信息，以便称呼和识别，这是人际交往的前提。他人要了解个体的基本信息，多数情况下无需征得其同意。在可以被称呼和识别的基础上，随着交往的不断深入和信任的逐渐建立，个体向他人提供更多不敏感与低度敏感的个人信息，以加深了解、产生和增进信任，进而缔结社会关系。缔结的社会关系又形成新的个人信息，使个体的人生阅历更丰富、社会形象更丰满^[26]，有助于更好地开展社交活动^⑦。可见，不敏感个人信息广泛公开，旨在使个体融入社群，开展交往。

敏感个人信息不是绝对不公开，也不是广泛公开，而是在特定范围内被有限公开。例如，经过技术处理并固定于载体之上的生物识别信息被用于支付软件等的身份认证；宗教信仰信息用于与尊重信仰之人或教中信徒间交流思想；医疗健康信息用于与医疗机构、病友、慈善组织等主体交流病情；金融账号信息用于与金融机构、交易对方及用人单位等主体经济往来；行踪轨迹信息被卫星通信或导航软件等收集并用于定位或导航。通常而言，敏感个人信息对正常社会交往而言不是必须的，个体参与法律关系的资格与在法律关系中的平等地位不会因宗教信仰、身体健康等因素而不同，个体也通常不会主动将其金融信息、行踪信息广而告之，故敏感个人信息不具有广泛公开性。这些信息具有特定功能，一旦超出特定目的收集、利用或在可公开范围之外提供敏感个人信息，则不具有合理性，违反个人信息处理规范。《个人信息保护法》明确列举敏感个人信息种类，将立法者对有限公开的个人信息的共识以法律形式确定下来。在具体案件中，司法机关应结合个人信息的特定功能和具体场景判断其敏感程度，并据此确定获取、提供行为是否超出个人信息的可公开范围，由此判断行为是否违法。

司法实践中，一些司法机关未区分私密信息、敏感个人信息和不敏感个人信息，只要存在个人信息的非法获取、买卖即判处侵犯公民个人信息罪。如在“李某侵犯公民个人信息罪案”中，李

^⑦ 社会交往的开展往往基于不敏感及低度敏感个人信息的使用和交流。例如，在校大学生为获得实习机会而提交个人简历，实习单位经过联络、面试后了解该生更多信息，综合判断后确定是否给予实习机会。该生经过实习，与同事、领导、客户等产生新的交往信息。这段经历作为个人信息被写入简历，将对其未来就业和发展提供帮助。

某通过在微信群中添加好友等方式,发布查询公民车牌信息(包含车牌、车主姓名、车主电话)广告,买入并出售公民车牌信息,从中赚取差价,其行为构成侵犯公民个人信息罪^⑧。该案中,车牌号、车主姓名、车主电话均属于可为人所知的个人信息,非私密信息,排除隐私侵权的可能;侵犯上述非私密信息,需根据违法情节严重程度判断是否入罪。

如前文所述,违法处理非私密信息的违法本质是对个人信息处理秩序的破坏,而违反个人信息处理秩序的严重程度,与非私密信息的可公开范围成反比,与非私密信息的处理数量成正比。《个人信息保护法》对敏感个人信息作出特别规定,多种国家技术标准也对个人信息及其违法处理后果分类分级,均可证明个人信息具有不同的可公开范围。可公开范围越大,违法处理造成的侵害越小。《解释》区分不同种类个人信息的入罪条数,如行踪轨迹信息、通信内容、征信信息、财产信息为50条,住宿信息、通信记录、健康生理信息、交易信息为500条,其他个人信息则为5000条。行踪轨迹等信息直接关乎人身安全、隐私、信用和财产等利益,故具有高度敏感性,可公开范围较小。在情节严重标准确定的情况下,可公开范围越小,违法处理的个人信息数量则越少,反之则越多。

此外,对信息主体的实际影响也是判断情节严重的重要依据。在“徐玉玉案”中,法院未认定非法获取和售卖个人信息行为与诈骗结果之间具有因果关系^⑨,即不认为违法处理者与加害人存在意思联络,未形成共同追求或放任损害结果发生的意志,故应当认定为“无共同故意”^[27]。但是,法院将被害人死亡作为认定违法处理个人信息的特别严重情节,表明对信息主体的实际影响属于法院判断情节严重的依据。

综上所述,非私密信息的可公开范围、处理数量及对信息主体的实际影响,是判断违法处理非私密信息情节严重的主要依据。

(三) 既有情节严重认定标准的不足与完善

由于《解释》比《民法典》出台更早,故未能依据《民法典》对个人信息及其违法处理后果的二分作出相应的解释和制度安排。私密信息和非私密信息的违法处理后果迥异,故《解释》中的既有规范应当依据《民法典》予以完善,对私密信息和非私密信息作出区分,在此基础上完善情节严重的认定标准。

有学者经过统计认为,目前侵犯公民个人信息罪在实践中的违法处理条数(以及相应的违法所得数额)均大幅高于《解释》中的违法处理数量^[28],即实践中的违法处理严重程度远大于法定的情节严重标准,呈现出立法较重、量刑畸轻状态。对此,一种合理的解释是,司法机关认为裁量规则设置的情节严重标准过低,如对于敏感和特别敏感的个人信息,侵犯数量分别达到500条和50条即可入罪,这与该罪社会危害性并不相当^[21],故审判实践倾向于趋轻判决。为缓和立法与司法之间的矛盾,应适当提高情节严重的法定标准。在非私密信息可公开范围不变的情况下,既可以增加构成情节严重的处理条数,提高入罪的情节严重标准,这需要对《解释》作出修改;也可以在情节严重标准不变的情况下,严格计算入罪的处理条数,达到实质出罪目的,由此弥合司法实践与法律规范之间的罅隙。

个人信息处理条数的计算,应当以可识别的特定身份作为计数依据。例如,一位大学教师,早晨从家里到学校办公(1),在办公室工作一小时(2),然后到达教学楼(3),上了三节课(4),下课后去教工餐厅吃饭(5),之后回到办公室(6),行为人向他人提供此行踪轨迹,应认定为提供了6条而非1条^[29]。这种认定方式按照信息片段计数,将导致数量急剧扩大。若按照此方式计数,个体的生活、上网信息均可拆分为无数信息片段,足以达到《解释》中的5000条标准,故这种计数方

⑧ 江苏省无锡市锡山区人民法院(2021)苏0205刑初584号刑事附带民事判决书。

式存在问题，应当回归个人信息的本质明确计算方法。个人信息的本质是识别，不可识别或匿名信息不属于个人信息，故一条个人信息须满足识别特定个体身份的要求。在该例子中，这6条信息如果脱离主体身份语境而单独呈现，将因无法识别特定主体而不属于个人信息。由此观之，个人信息条数应当根据个人身份信息计数，识别一个身份，成立一条个人信息，而不论该个人信息的片段多寡。在上述例子中，应当认定只有1条该教师的行踪信息。司法机关在实践中可能存在重复统计个人信息条数的情况，比如在非法售卖、提供个人信息的数据库中，与某一身份主体相关的姓名、电话号码、地址、行踪等信息被分别计数。而姓名因重名者甚多而无法被单独用来识别个体，电话号码可能因无法拨通而无法直接识别个体，地址、行踪等信息也可能识别为同乡或同行者，故这些信息均为信息片段，只有相互结合才能构成一条可识别特定主体的个人信息。因此，个人信息应根据特定身份计数。

此外，以违法所得数额作为情节严重的判断标准值得商榷。《解释》第5条规定，非法获取、出售或者提供公民个人信息，违法所得五千元以上的，属于情节严重。目前，大量侵犯公民个人信息刑事案件以或仅以被告人的违法所得金额判断情节是否严重，由此作为定罪依据。对此，有学者认为，违法所得数额与侵犯公民个人信息罪的法益侵害及其程度没有必然联系，不应作为情节严重的认定标准之一^[30]。在侵权法上，当被侵权人因过于困难或成本过高而无法精确证明损害数额时，可以按照侵权人违法所得的金额作为损害认定和赔偿的依据^[31]。由于违法处理个人信息不直接造成损害，而是带来不确定的风险，故立法者选择侵权法上这种以计算违法所得的方式来确定损害。但在刑事责任认定中，违法所得反映的主要是行为人的犯罪行为收益，其未必能够反映侵犯公民个人信息罪的法益侵害程度，故以计算违法所得方式判断法益侵害过于片面。不仅如此，违法所得反映的是被害人经济方面的损失，而侵犯公民个人信息罪是侵犯公民人身权利、民主权利的犯罪，以违法所得数额作为入罪的标准之一，实际上是“将经济犯罪的认定方法生搬硬套于侵犯公民人身权利、民主权利的犯罪”^[30]。由于实际发生的侵犯公民个人信息犯罪未必均为获利性犯罪，故以违法所得数额作为侵犯公民个人信息罪的定罪标准值得商榷。况且，《解释》将违法所得的定罪标准设置较低。实践中，许多司法机关在适用违法所得数额定罪标准时，并未考虑行为人支出的成本，故行为人即便未造成损害，也未取得较多金额，却被判定为情节严重，这也加剧了侵犯公民个人信息罪打击面过大的问题。

实际上，违法所得的范围如何界定、标准如何计算，在行政处罚领域一直具有争议，主要有违法所得收入论、违法所得收益论和违法所得折中论三种观点^[32]。违法所得收入论主张违法所得不扣除成本，故其确定的违法所得范围最大；违法所得收益论主张违法所得为行为人实施违法行为取得的收入扣除成本后的收益，范围较小；违法所得折中论主张综合考虑行为人的违法目的、主观意图、损害后果等决定是否扣除其成本。2021年修订后的《行政处罚法》规定，“当事人有违法所得，除依法应当退赔的外，应当予以没收”。就退赔份额的事实效果而言，已被行为人破坏的社会管理秩序在一定程度上得以修复，受害人得到相应补偿，违法行为危害性的影响范围、程度大幅缩减，故可以依据体系解释认为，在侵犯非私密信息的案件中，违法所得的计算应当将退赔程序前置化，扣除依法应当退赔和已经退赔的数额^[33]。如在“任某侵犯公民个人信息案”中，任某利用营业厅员工的身份，在用户不知情的情况下将用户手机号码收到的验证码发送给他人用于注册APP新用户。法院认定任某违法所得为4484元，因其符合《解释》第八项——在履行职责或者提供服务过程中获得的公民个人信息出售或者提供给他人，违法数额达到第七项规定标准（5000元）一半以上，判处侵犯公民个人信息罪^⑨。显然，法院并未扣除应当退赔给受害人的费用。若扣除退赔

⑨ 西安市鄠邑区人民法院(2023)陕0118刑初120号刑事判决书。

费用,被告人有可能不构成犯罪,而只需适用行政处罚。依据比例原则和过罚相当原则,侵犯非私密信息中行为人的主观恶性一般较轻,可以酌情考虑扣除合理的成本^[32]。如在“李某华、李某波侵犯公民个人信息案”中,被告人在微信群里以每个80元的价格收购42个微信白号,以每个260元的价格收购8个实名制微信号,后将微信白号、实名制微信号全部贩卖给孙某,法院认定其违法所得8620元^⑩。该案中,被告人并未造成实际损害,且自动到案并如实供述,主观恶性较轻,可以将收购费用5440元合理扣除,认定违法所得为3180元,小于5000元的情节严重标准。

总之,司法者需要优化违法处理非私密信息“情节严重”的判断标准。司法机关在实践中应不断总结不同私密信息的可信赖范围与非私密信息的可公开范围,进一步明确违法处理的严重程度。在此基础上,宜在本罪中增加个人信息的入罪条数,严格计算个人信息条数和违法所得金额,以弥合法定入罪门槛与司法裁判畸轻之间的缝隙,实现对违法处理行为的准确入罪,并使其与应承担的刑事责任相适应。

四、结语

根据我国刑法规定,构成侵犯公民个人信息罪的条件之一是“违反国家有关规定”。《民法典》在个人信息中划分出私密信息,规定违法处理私密信息构成隐私侵权,而违法处理非私密信息则不构成侵权。《个人信息保护法》规定个人信息处理规则和处理者义务,形成个人信息处理的公法秩序,故违法处理非私密信息构成行政违法。私密信息与非私密信息的违法处理后果截然不同,违法处理个人信息的法律责任应以个人信息及其违法处理后果的二分为基础。由此,私密信息的概念界定和认定,成为认定违法处理个人信息法律责任的首要环节。“私密”的核心特点是具备排斥他人在场的高度信赖环境以实现高度自主,故应当以同样的标准认定私密信息。

基于对私密信息的认定,违法处理个人信息的法律后果分为隐私侵权和行政违法。两种法律后果均以“情节严重”为判断标准,以实现与刑事责任衔接,但二者判断方式有所不同。对于隐私侵权的“情节严重”,应围绕人格损害的程度展开判断,重点考查三个维度:一是私密信息本身的可信赖范围,二是与信息主体相关联的知晓人数,三是私密信息泄露后对信息主体的实际影响。对于行政违法的“情节严重”,则应围绕背离规则的程度判断,重点考查三个维度:一是非私密信息的可公开范围,二是违法处理信息的数量,三是行为造成的实际影响。既有刑事规范中“情节严重”的认定标准存在不足,应当对私密信息和非私密信息的违法处理加以区分,在违法处理入罪的信息条数、违法所得的金额方面严格计算,从而实现民刑、行刑责任的合理、有效衔接。

参考文献

- [1] 李怀胜. 侵犯公民个人信息罪的刑法调适思路——以《公民个人信息保护法》为背景[J]. 中国政法大学学报, 2022(1): 138-148.
- [2] 石经海, 李鑫. 侵犯公民个人信息犯罪行刑衔接的困境与出路[J]. 吉林大学社会科学学报, 2023, 63(5): 78-90+237.
- [3] 张丽霞. 论侵犯公民个人信息罪的“违反国家有关规定”[J]. 河北法学, 2025, 43(9): 124-142.
- [4] 贺彤. 私密信息的概念构成与规则体系[J]. 华东政法大学学报, 2023, 26(3): 22-36.
- [5] 卢勤忠, 张宜培. 非法使用个人信息行为入刑的立法构思[J]. 河北法学, 2023, 41(1): 73-96.
- [6] 沃尔夫冈·弗里施, 陈璇. 客观归责理论的成就史及批判——兼论对犯罪论体系进行修正的必要性[J]. 国家检察官学院学报, 2020, 28(1): 35-56.
- [7] 周晓. 侵犯公民个人信息犯罪刑事附带民事公益诉讼案件的审理困境和规范应对[J]. 法律适用, 2023(2): 165-176.
- [8] 李浩. 民事诉讼证明标准的再思考[J]. 法商研究(中南政法学院学报), 1999, 16(5): 19-21.

⑩ 湖南省宜章县人民法院(2023)湘1022刑初313号刑事判决书。

- [9] 方程. 贝叶斯定理认定因果关系的逻辑展开——从个人信息侵权案切入[J]. 浙江工商大学学报, 2023(4): 142-156.
- [10] 贺彤. 安全作为个人信息保护的法益[J]. 财经法学, 2023(3): 110-125.
- [11] 孙鹏. 数据法益的阶层式还原路径与刑法适用[J]. 东北农业大学学报(社会科学版), 2024, 22(1): 78-89.
- [12] 刘艳红. 民法编纂背景下侵犯公民个人信息罪的保护法益: 信息自决权——以刑民一体化及《民法总则》第111条为视角[J]. 浙江工商大学学报, 2019(6): 20-32.
- [13] 欧阳本祺. 侵犯公民个人信息罪的法益重构: 从私法权利回归公法权利[J]. 比较法研究, 2021(3): 55-68.
- [14] 廖丽环, 俞程. 公共属性视角下个人信息保护的思路转变与制度完善[J]. 东北农业大学学报(社会科学版), 2023, 21(4): 18-28.
- [15] 王锡锌. 个人信息权益的三层构造及保护机制[J]. 现代法学, 2021, 43(5): 105-123.
- [16] 梅夏英. 在分享和控制之间 数据保护的私法局限和公共秩序构建[J]. 中外法学, 2019, 31(4): 845-870.
- [17] 高富平. 论个人信息处理中的个人权益保护——“个保法”立法定位[J]. 学术月刊, 2021, 53(2): 107-124.
- [18] 韩思阳. 公法介入私域: 平台中的个人信息保护[J]. 学术月刊, 2023, 55(5): 106-119.
- [19] 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, 44(5): 3-18.
- [20] 陈可翔. 个人信息保护中行政处罚的实施基础及制度逻辑[J]. 法学, 2023(11): 57-72.
- [21] 冯洋, 李珂, 张健. 侵犯公民个人信息罪司法裁量的实证研究[J]. 山东大学学报(哲学社会科学版), 2023(1): 92-102.
- [22] 徐翕明. “网络隐私权”刑法规制的应然选择——从“侵犯公民个人信息罪”切入[J]. 东方法学, 2018(5): 63-71.
- [23] 张小虎. 网络言辞侮辱的典型事实形态及其刑法定性[J]. 学术界, 2023(10): 26-36.
- [24] 周光权. 侵犯公民个人信息罪的行为对象[J]. 清华法学, 2021, 15(3): 25-40.
- [25] 黄陈辰. 论公开信息的刑法保护[J]. 大连理工大学学报(社会科学版), 2022, 43(3): 84-91.
- [26] 熊丙万. 私法的基础: 从个人主义走向合作主义[J]. 中国法学, 2014(3): 138-155.
- [27] 唐绍均, 李生银. 论客观关联共同侵权行为的理论辨正与立法回应——兼论《民法典》第1168条的解释[J]. 湖南大学学报(社会科学版), 2023, 37(4): 128-136.
- [28] 喻海松. 侵犯公民个人信息罪的司法适用态势与争议焦点探析[J]. 法律适用, 2018(7): 10-15.
- [29] 张明楷. 刑法学(下)[M]. 北京: 法律出版社, 2020.
- [30] 石聚航. 侵犯公民个人信息罪“情节严重”的法理重述[J]. 法学研究, 2018, 40(2): 62-75.
- [31] 程啸. 侵权责任法(第三版)[M]. 北京: 法律出版社, 2021.
- [32] 胡建森. 关于行政处罚“没收违法所得”的若干问题[J]. 中南大学学报(社会科学版), 2023, 29(5): 42-55.
- [33] 夏金莱. 行政处罚没收违法所得的认定与审查体系建构[J]. 行政法学研究, 2023(6): 75-85.

(责任编辑: 徐 源)

The Dichotomy of Consequences and Connection of Liabilities for Illegal Processing of Personal Information

HE Tong

Institute of Law, Chinese Academy of Social Sciences, Beijing 100009, China

Abstract: The legislative process for personal information protection has followed a sequence of "criminal law taking precedence, followed by civil and administrative laws", leading to connection issues between the criminal liability and civil/administrative liabilities for illegal processing of personal information. The Civil Code classifies personal information into confidential and non-confidential information, where illegal processing of confidential information constitutes an infringement of privacy. In contrast, the Personal Information Protection Law does not provide for confidential information, and illegal processing of non-confidential information constitutes an administrative violation. Consequently, the legal consequences for illegal processing of these two types of personal information differ. To determine criminal liability for illegal processing of personal information, it is first necessary to identify whether the personal information involved is confidential, so as to establish whether the act constitutes an infringement of privacy or an administrative violation. Subsequently, different standards are applied to judge whether the act meets the "serious circumstances" requirement under criminal law, thereby realizing the connection between civil-criminal liabilities and administrative-criminal liabilities for illegal processing of personal information. The existing standards for "serious circumstances" in relevant regulations are insufficient. On the basis of distinguishing between confidential and non-confidential information, strict calculations should be made regarding the number of information items involved in the illegal processing that constitutes a crime and the amount of illegal gains.

Key words: illegal processing of personal information; confidential information; infringement of privacy; connection between administrative law enforcement and criminal justice; serious circumstances