财经法学 No. 3，2023
pp. 110 - 125

安全作为个人信息保护的法益

贺　彤*

内容提要：法律创设的查阅、更正、删除等权利不是个人信息保护的目的。人格、财产权利损害非由违法处理个人信息直接、定然造成，而应归咎于后续独立的实害行为，故人格、财产权利非违法处理的侵害对象，亦非个人信息保护的直接目的。违法处理的直接后果是使权利被侵害的风险升高，其侵犯的利益是安全。安全减损引起注意义务的增加和法律资源的消耗等利益变动，但由于此等利益差额无法举证和计算，亦未产生可预见的危险，故无法适用侵权救济。与侵权保护相区别，《个人信息保护法》设置了处理规则、权利义务、职权和责任等规范，其目的并非弥补损失，而是保护和恢复安全法益。个人信息保护与侵权保护相对独立，《个人信息保护法》第69条是两种保护规范的衔接规定。

关键词：违法处理个人信息　实害行为　识别性　侵权保护　安全法益

一、问题的提出：个人信息保护到底保护什么？

自20世纪70年代始，国外便已探索个人信息保护模式，防范泄露、篡改或过度利用个人信息对个人利益的损害。2018年欧盟出台了严格保护个人信息的《通用数据保护条例》（以下简称GDPR），赋予信息主体知情、更正、数据移转和清除等8种权利，〔1〕使信息主体在一定情形和条件下对个人信息处理全过程进行控制或干预。〔2〕《中华人民共和国个人信息保护法》（以下简称《个保法》）也规定了查阅、复制、更正、删除等权利（束），信息主体得以请求的方式向信息处

*　贺彤，东南大学法学院博士研究生、东南大学人权研究基地研究人员。

本文为江苏高校项目“人格权重大疑难问题研究”（2020SJZDA091）、江苏省研究生科研创新计划项目“个人信息公法保护机制研究”（KYCX21_0072）的阶段性成果。

〔1〕 参见《通用数据保护条例》，载https://gdpr.eu/tag/gdpr/，最后访问时间：2021年12月26日。

〔2〕 参见高富平：《论个人信息处理中的个人权益保护——“个保法”立法定位》，载《学术月刊》2021年第2期。

理者行使之。但个人信息保护所保护的是这些请求权利吗？显然，它们本身没有分离或单独转让的价值，〔3〕非人身、财产等实体权利，而只是制定法所创设的、用以制衡信息处理者的工具。〔4〕假设这些请求权利未被设立，个人信息保护的利益依然存在。况且，个人信息保护更多依靠公权力来规制处理活动，无论是欧盟的GDPR、美国的信息隐私保护执法实践，还是我国个人信息保护制度，行政监管占据了主导地位。〔5〕可见，《个保法》中的请求权利，不是法律所保护的利益目的，而只是保护利益的一种工具。

根据《个保法》第1条“为了保护个人信息权益……制定本法”可知，保护个人信息的目的是保护“个人信息权益”。但这一答案仍不清晰。目前，我国学者对个人信息权益的属性和内涵已作了大量讨论，主要思路是将之定性为财产、人格等权利：或认为个人信息是有价值的商品，需给予财产权（主要是知识产权）保护；〔6〕或认为个人信息是人格尊严的体现，主张权利人对个人信息享有支配与自主决定的权利，依人格权获得救济；〔7〕或持人格权兼财产权的观点，认为个人信息兼具人格要素和财产要素。〔8〕

与其陷入理论争执，不如观察生活实践。法律所保护的“利益本身并不是立法者创造的，立法者只是在法律中确认和保护某种利益”〔9〕。《个保法》的制定是为了规制个人信息被不当处理而引发利益侵害的失序状态，故违法处理侵害的对象就等于《个保法》所保护的利益。因此，可以通过考察实践中违法处理“侵害了什么”，来解答“个人信息权益是什么”。如果个人信息权益是人格、财产权利，那么违法处理个人信息将会造成信息主体权利受损的结果；而若违法处理不会造成信息主体上述权利受损，那么个人信息权益的财产权说、人格权说则值得怀疑。在著名的“人脸识别第一案”中，原告在事实理由中表达了对被告强制收集和利用个人信息所产生的安全隐患的担忧，法院在判决中未判定被告存在欺诈等权利侵害行为。因此，有关个人信息权益是权利的学说尚且存疑，个人信息权益是什么的问题，有待进一步发现。

二、违法处理未必损害权利但直接减损安全

违法处理个人信息一般包括对个人信息的非法收集、利用、买卖与泄露、篡改、丢失等。实

〔3〕 参见叶名怡：《论个人信息权的基本范畴》，载《清华法学》2018年第5期。

〔4〕 参见王锡锌：《国家保护视野中的个人信息权利束》，载《中国社会科学》2021年第11期。

〔5〕 参见王锡锌：《重思个人信息权利束的保障机制：行政监管还是民事诉讼》，载《法学研究》2022年第5期。

〔6〕 参见谢立斌、李艺：《个人信息的宪法财产权保护》，载《江西财经大学学报》2021年第5期；任丹丽：《民法典框架下个人数据财产法益的体系构建》，载《法学论坛》2021年第2期。

〔7〕 参见程啸：《论个人信息权益》，载《华东政法大学学报》2023年第1期；张新宝：《论个人信息权益的构造》，载《中外法学》2021年第5期；程啸：《论我国民法典中个人信息权益的性质》，载《政治与法律》2020年第8期；程啸：《民法典编纂视野下的个人信息保护》，载《中国法学》2019年第4期；杨立新：《个人信息：法益抑或民事权利——对〈民法总则〉第111条规定的“个人信息”之解读》，载《法学论坛》2018年第1期；王利明：《论个人信息权的法律保护——以个人信息权与隐私权的界分为中心》，载《现代法学》2013年第4期。

〔8〕 参见彭诚信：《论个人信息的双重法律属性》，载《清华法学》2021年第6期；前引〔3〕，叶名怡文；任龙龙：《个人信息民法保护的理论基础》，载《河北法学》2017年第4期；刘德良：《个人信息的财产权保护》，载《法学研究》2007年第3期。

〔9〕 张明楷：《法益初论》（上），商务印书馆2021年版，第180页。

践中，违法处理并不直接、定然造成权利损害，二者之间隔着“风险的发生”这一条件。权利损害实际由违法处理之后的实害行为所致，而实害行为并不定然发生，违法处理只是为其提供了条件和可能性。故违法处理的直接后果是增加权利受损风险，易言之，减损安全。

（一）违法处理未必直接、定然造成权利损害

考察案例中“行为—损害”的因果关系可知，违法处理与权利损害之间并无直接因果关系。首先考察违法处理个人信息引发财产权利受损的情况，以“周裕婵诉广东快客电子商务有限公司、东莞市易得网络科技有限公司网络侵权责任纠纷案”为例。〔10〕该案中，法院在认定第三人诈骗的基础上，以侵权规则来解决该民事纠纷，认为个人信息处理者违反了《中华人民共和国网络安全法》第 40 条的“用户信息严格保密”义务，使第三人利用获得的个人信息实施诈骗，遂应承担侵权赔偿责任。这一判决看似是将周某被诈骗的财产损失结果直接归因于个人信息的泄露，实则非也。根据法院的事实认定和判决结果可知，法院认为泄露信息与财产损失之间具有“间接”的因果关系：（1）法院将泄露用户信息的举证责任倒置于快客公司，而快客公司因无法排除自己的责任而被推定存在泄露用户信息的事实；（2）网名为“售后楚楚”者利用从快客公司获取的用户信息，以快客公司“售后”的名义欺诈周某，这种表见的代理行为使周某有理由产生合理信赖并向其转账，故造成周某财产损害的直接原因是“售后楚楚”的诈骗行为，这是独立于泄露行为的、另一主体实施的实害行为；（3）法院在判决书中认定，“快客公司作为网络运营者未能履行保护用户信息的义务，对于因此给周裕婵造成的损失负有一定的过错”，可见，法院并未将周某财产损害的结果直接、完全归因于个人信息泄露，而是认为泄露行为与财产损失之间具有间接、“一定”的因果关系。由此可见，利用个人信息实施诈骗，使被害人遭受财产损失，这一结果的直接原因是诈骗行为而非泄露行为。将诈骗行为造成的财产损害完全归责于泄露个人信息的行为，有悖法院判决的本意。

其次考察违法处理个人信息引发人格权利受损的情况，以“蔡小燕与赵延安个人信息保护纠纷案”为例。〔11〕该案中，法院认为，被告未经原告同意将原告及其两子的户籍与二孩出生证明泄露，侵害了原告及其两子的隐私权。显然，法院在明确被告泄露原告个人信息的事实后，却以隐私规则裁判案件，其间的因果关系需补充说明。本案中，被告除了泄露原告及其子女的个人信息外，还张贴了“寻找原告之子蔡子明生父”的寻人启事，据此宣扬蔡某二孩非婚内所生，有损原告及二孩的名誉，也构成对原告隐私的泄露、刺探。可见，户籍登记与出生证明中的信息都是能够为人共享的个人信息，而真正带给原告精神痛苦的则是“寻人启事”的发布，人们据此对蔡某的私生活品头论足或猜测打听，造成对蔡某名誉和隐私权的侵害。因此，人格权受损与违法处理是间接而非直接的因果关系，两者之间还存在独立实施的人格侵权行为。

通过分析上述案例可知，在违法处理个人信息引发的财产、人格侵权案件中，还存在独立的实害行为。违法处理行为只是为后续实害行为提供条件，本身并非造成权利损害的直接原因，故不能将权利损害直接归咎于违法处理。

〔10〕 参见广东省深圳市中级人民法院（2019）粤 03 民终 3954 号民事判决书。

〔11〕 参见湖南省益阳市中级人民法院（2021）湘 09 民终 1585 号民事判决书。

此外，在现实生活中，大多数违法处理个人信息行为并未引发财产、人格权利致损的结果，这充分证明违法处理与权利损害之间不是直接、定然的因果关系。如在“陈瑜婷与上海瑞慈瑞兆门诊部有限公司隐私权纠纷案”〔12〕中，原告虽认为被告对其个人信息的泄露造成其在“信息安全及居住安全”方面的较大精神及心理压力，但没有表示有关隐私、名誉以及财产等权利受到损害。法院审理后认为，本案因所涉个人信息“难以归入隐私权的私密信息范畴”，故不构成隐私侵权；尽管“被告在处理原告个人信息的过程中确实存在不妥之处”，但并未造成权利损害结果，遂驳回其精神损害赔偿的诉讼请求；判决被告赔礼道歉，并非有充分事实、法律依据，只是因为“被告愿意”且“于法不悖”。可见，违法处理有时并不会造成人格、财产权利的损害，既然如此，个人信息权益并不等同于人格或财产权利。

有学者已注意到违法处理个人信息行为并不直接、定然造成权利损害，但仍将权利损害视为违法处理的危害后果，称作“下游损害”。〔13〕谢鸿飞教授表示：“当下游损害发生时，信息泄露本身造成的权益损害往往被司法实践忽视，它往往被下游损害所吸收。”〔14〕这一观点已认识到违法处理带来的权益侵害与权利损害有所区别，但仍将二者合一，将权利损害直接归责于违法处理行为。对违法处理侵害权益的忽视，导致个人信息保护与侵权保护难以界分。显然，这种认识不符合“行为—结果”一一对应的逻辑关系，也有悖于法治的基本精神，容易带来“连坐”之后果，即虽未实施欺诈等后续行为，却因具有一定关系而要连带承担欺诈等行为所对应的责任。

总之，在违法处理与权利损害之间，还有实害行为的介入，故须严格区分违法处理行为与后续实害行为。违法处理行为具有独立的侵害后果，不应将之与权利损害结果混为一谈，否则无法辨别个人信息上真正被侵害（或受保护）的对象。

（二）违法处理的直接后果是减损安全

既然违法处理个人信息实施了独立的侵害，那其直接后果是什么？违法处理在客观上为后续可能的实害行为提供了有利条件，使权利更容易、更可能受到损害，即“风险升高”。有学者认为，个人信息的暴露本身即为损害，无须再寻找其他的损害，〔15〕这种观点较为极端。个人信息暴露必然会带来风险，但人们早已习惯或需要被陌生人了解，若将个人信息的暴露当作损害而排除个人信息上的任何风险，那么人类交往将局限在熟人社会而无法进入开放市场，故不能直接将之当作损害。此外，更多学者认为应当对个人信息的无形损害实行损害的推定，〔16〕或将风险升高视为损害，〔17〕由此适用侵权救济。尽管这些观点有待推敲，但违法处理所致风险升高的不利益性，显然已被较多人接受。风险升高只是描述了不利益状态，与之相对应的利益应当是

〔12〕 参见上海市普陀区人民法院（2020）沪0107民初5934号民事判决书。

〔13〕 参见商希雪：《侵害公民个人信息民事归责路径的类型化分析——以信息安全与信息权利的“二分法”规范体系为视角》，载《法学论坛》2021年第4期。

〔14〕 谢鸿飞：《个人信息泄露侵权责任构成中的“损害”——兼论风险社会中损害的观念化》，载《国家检察官学院学报》2021年第5期，第29页。

〔15〕 See Maxwell E. Loos, *Exposure as Distortion: Deciphering “Substantial Injury” for FTC Data Security Actions*, 87 George Washington Law Review Arguendo 42 (2019).

〔16〕 参见徐明：《大数据时代的隐私危机及其侵权法应对》，载《中国法学》2017年第1期。

〔17〕 See Jennifer Wilt, *Cancelled Credit Cards: Substantial Risk of Future Injury as a Basis for Standing in Data Breach Cases*, 71 Southern Methodist University Law Review 615 (2018).

安全。

在 2021 年 4 月由最高人民检察院发布的个人信息相关公益诉讼典型案例〔18〕中，行为人违法收集、使用、出售或泄露个人信息，因牵涉的人数和个人信息数量较大，涉及公共利益，故引发检察机关提起公益诉讼。在数起典型案例中公民权利未遭受损害，但违法处理行为仍应受法律规制，这是因为该行为减损了公民所信赖的安全。典型案例中检察机关对侵害后果和履职活动的表述，可以验证这一观点。一方面，公民“合法权益”和社会“公共利益”是检察机关频繁用来描述侵害对象的用语，但也未能清晰展现被侵害对象的具体内涵。根据检察机关表述的“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”等用语可知，个人信息被违法处理后，诈骗等尚未发生，但这为侵权行为提供了有利条件，使不法者更易“趁虚而入”，增加了损害发生的可能性。因此，违法处理对公民合法权益和社会公共利益的侵害，实际上是对个人或群众人身、财产的安全造成减损。另一方面，“个人信息安全”是检察机关频繁用来描述保护目的的用语，其实质就是人身、财产权利的安全。安全是人所享有的利益或状态，作为工具和抓手的个人信息本身并不存在安全问题。〔19〕只有与信息主体利益相关时，信息安全才有保护的价值。检察机关打击个人信息违法犯罪的目的，是要消除违法处理给信息主体人身、财产权利带来的风险因素，使之恢复到合法安全状态。因此，“个人信息安全”就是信息主体的人身、财产安全。

综上，违法处理与公民人身、财产权利损害呈间接的因果关系，其间存在两个行为、两个结果、三层关系。如图 1 所示：违法处理直接造成安全减损结果；安全减损可能（而非定然）引发实害行为；违法处理后的实害行为是直接造成权利损失结果的原因。由于处理者造成了权利的高风险后果，且应当预见后续可能会发生权利侵害，故有义务采取妥当措施使信息主体脱离高风险状态，使之不会遭受后续实害行为的损害；若其放任风险发生，则应当对侵害结果承担一定的责任。〔20〕

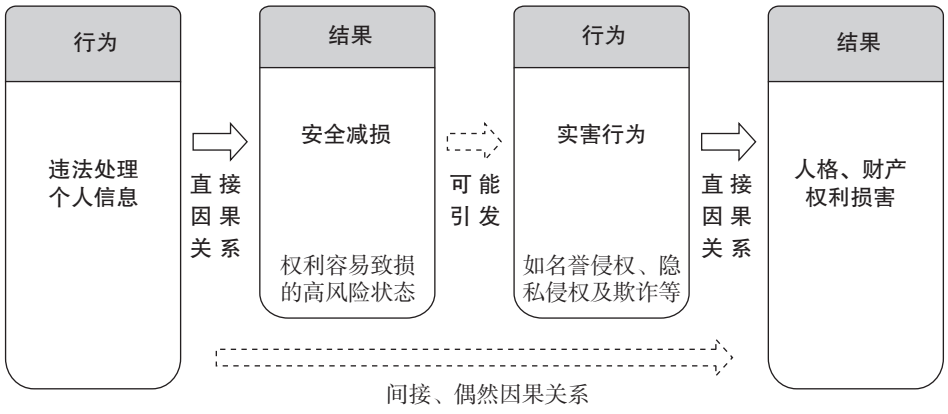

图 1　违法处理个人信息行为与权利损害结果关系示意图

〔18〕 参见《最高检发布检察机关个人信息保护公益诉讼典型案例——斩断个人信息侵权与电信网络诈骗之间的利益链条》，载 https://www.spp.gov.cn/spp/xwfbh/wsfbt/202104/t20210422_516357.shtml#1，最后访问时间：2021 年 11 月 26 日。

〔19〕 参见梅夏英：《在分享和控制之间——数据保护的私法局限和公共秩序构建》，载《中外法学》2019 年第 4 期；丁晓东：《个人信息的双重属性与行为主义规制》，载《法学家》2020 年第 1 期。

〔20〕 参见杨会：《浅论间接结合行为的界定》，载《法治研究》2013 年第 5 期。

三、安全减损源于个人信息识别特性

如前文所述，违法处理个人信息的直接后果是安全减损，而造成此种后果的根源就在于个人信息的“识别性”。他人识别个人信息的用途具有不确定性，故信息主体会因个人信息的不当处理而面临权利受损风险。如果无法识别个人，处理行为将不会引发针对个人的权利侵害。可见，不当处理个人信息减损安全的根源在于个人信息的识别本质，故个人信息识别性决定了个人信息保护的目的是安全。

（一）个人信息用于限缩范围以识别个人

国际标准化组织（ISO）将信息定义为“关于在特定语境下具有特定含义之客体——例如事实、事件、东西、过程或思想包括理念——的知识”〔21〕，这一定义凸显了信息对客体的“关联性”。作为信息的子项，“个人信息”增加了“个人”这一定语，故个人信息是与个人关联的信息。个人信息与个人的关联是“相关”还是“专属”，决定了个人信息的特性。

首先，个人信息不是专属于个人的信息，它向来为人们所共享。理由如下：其一，个人信息不是由个人生产出来的。记录个人信息的媒介往往由数据处理者提供，若没有记录媒介，个人信息难以存在，故个人和处理者均对个人信息的产生作出贡献，〔22〕个人信息不能单独为个人所有。其二，个人信息无法被自主控制，其价值在于交流。从古至今，无论是国家赋税还是社会活动，都需要每位成员提供个人信息以便管理，不提供个人信息的人通常是社会不安定因素。不同于有形、有限的物质，个人信息一旦为他人所知，便“一传十十传百”，不再受个人控制；个人信息可以被获得者同等、充分利用，再利用也不会使之贬值。故无论出于公共管理的目的还是社会生活的需要，信息主体必然会与他人分享个人信息而不将之独占。其三，个人信息由人共享。比如，每个人与亲朋共享自己的姓名以便相互称呼；熟人之间共享住址、联络方式等信息。显然，个人信息不专属于个人，且无论从伦理还是技术方面，我们都无法从与他人共享的信息中摘取专属个人的信息片段。而那些只有自己知道并不愿为他人所知的信息，是自己的隐私、秘密，而非用于交流的个人信息。

其次，个人信息不是泛指所有与个人有关的信息，而是在具体场景下对识别个人起到实质作用的信息。根据事物普遍联系的特性，一切信息都与个人具有千丝万缕的关联，若如此，个人信息将漫无边际。既然个人信息凸显的是与特定主体的关联性，故应当将其限定在有助于识别个人的信息范围内。一方面，个人信息是能够实质限缩识别范围的信息。前文案例中，行为人不当处理姓名、住址、电话号码、指纹和人脸信息等个人信息，减损信息主体的安全，这是因为以上个人信息能够反映个人特征、锁定个人并与之取得联系。其中，有的信息能够单独锁定个人，如指纹、虹膜和人脸信息（但需要相关技术支持）；而有的需结合其他信息，如姓名、住址、电话号

〔21〕 该定义原文为“Information：knowledge concerning objects，such as facts，events，things，processes，or ideas，including concepts，that within a certain context has a particular meaning”，载 https://www.iso.org/obp/ui/#iso：std：iso-iec：2382：ed-1：v1：en. 最后访问时间：2021 年 12 月 13 日。

〔22〕 参见前引〔8〕，彭诚信文。

码等需结合识别，从重名者或同一地区的人中锁定个人。尽管存在识别效率高低之分，但毋庸置疑，个人信息能够实际限缩识别范围。另一方面，个人信息是场景主义下的动态概念。识别是“根据特点辨别，做出判断，以便找出或认定某一对象”〔23〕的活动，是从不特定多数中辨认特定个体的过程，故那些不能反映个人特征、无法与他人区别的关联信息不属于个人信息。与集体成员共同的身份信息，相对于其他集体而言，能够反映一定的个人特征，属于个人信息；但在集体内部，则不具有缩小识别范围的作用，不属于个人信息。由此观之，个人信息的特性在于识别。

最后，个人信息处理活动正是利用了个人信息识别特性。在数字社会（尤其是数字经济）中，个人信息因作为商业分析的重要资源而具有商业价值，商家可运用个人信息形成的数据产品获得巨大商业利润。〔24〕而个人信息之所以能被分析和运用，正是因为它与个人稳定联系，据此得以把从真实的人身上得来的信息预测结果，再运用回真实的人身上，比如个性化推送抑或诈骗电话。如果个人信息处理针对的是抽象的或匿名的人，那么这种信息分析结果的利用将不具有针对性，只能依照所揭示的一般大众需要来开展商业活动，无法发挥个人信息的真正价值，如个性化推送和服务。因此，处理个人信息活动本质上是利用个人信息的识别特性开展后续的利益撷取。

有学者否定个人信息的识别本质，认为“随着大数据分析技术深度嵌入社会生活以及信息共享技术的广泛运用，大量不具有可识别性的信息能够按照特定的算法被关联、融合，进而能够将相关信息与特定的个人相联系”〔25〕。这种观点令人困惑，若不识别个人，将如何对抽象的分析结果进行具体运用呢？那些通过多重数据融合与交叉验证来确定信息主体的信息，〔26〕看似去除了个性化特征，但既然能够通过算法联系到个人，则说明这种“数据＋算法”具有限缩识别范围、辨别个人特征的作用。实际上，只要是从不特定多数中指向特定个人，则必然需要某些具备个性化因素的条件。

个人信息的识别本质，还可以由与其功能相反的“匿名”信息得出。根据《个保法》第 73 条可知，匿名的功能在于消除个性，使信息在客观上无法用于识别、锁定个人，并且，由于该信息不具有能够辨认个性化的内容，信息主体不会认为该信息与自己相关，即便发生违法处理也不会产生权利可能受到侵害的不安心理。因此，个人信息和匿名信息的根本区别就在于可识别性。《个保法》第 4 条第 1 款规定“个人信息……不包括匿名化处理后的信息”，将匿名化的信息排除在个人信息之外，这也意味着匿名信息不具有个人信息保护的利益。毋庸置疑，“识别”是个人信息的本质特征。

（二）可识别性决定个人信息保护的目的是安全

在利用个人信息识别特定主体的活动中，被识别者是具体、确定的，但识别者是谁、是否可被信任，以及识别后是否行为、行为对被识别者是否有害，这些问题在通信高度便利、违法成本极低的陌生人社会充满了不确定性。故识别活动本身具有风险，这决定了个人信息保护的目的是

〔23〕 中国社会科学院语言研究所词典编辑室编：《现代汉语词典》（第 7 版），商务印书馆 2016 年版，第 83、1185 页。

〔24〕 参见前引〔8〕，彭诚信文。

〔25〕 郑晓剑：《个人信息的民法定位及保护模式》，载《法学》2021 年第 3 期，第 120 页。

〔26〕 参见刘迎霜：《大数据时代个人信息保护再思考——以大数据产业发展之公共福利为视角》，载《社会科学》2019 年第 3 期。

风险控制，即保障安全。

首先，非自主选择的识别者的可信任程度较低。在所有识别活动中，最明确且最值得信任的识别者就是自己，而社会交往的需要使得个人信息不为个人所私有，〔27〕必须被他人识别。在多数情况下，人们分享个人信息并被他人识别，不能完全依据自己意愿作出决定。出于顺利开展社会交往的需要，人们不得不与软件平台、服务机构、所在单位、政府部门等分享能够识别自己的信息。由于这些组织中的识别者难以确定且不为人知，而被识别者通常缺乏技术且精力不足，因而无法对其充分监督，故这些识别者的可信任程度较低，无法保证其在获取个人信息后不对被识别者实施侵害。实践中，违法处理个人信息的往往是那些有信息处理能力又隐藏在幕后的识别者。

其次，他人在识别后实施违法行为的成本较低。在信息时代，个人信息被电子或者其他方式记录，并通常被上传至网络空间。具备一定信息处理能力的识别者，能够通过搜索、购买等方式获取那些被电子化记录的个人信息。识别者掌握的信息技术越发达，则越隐蔽，其被发现、追究的可能性越低，故实施后续违法犯罪行为的成本也就越低。可见，识别者通过处理个人信息而具有实施后续实害行为的可能，并因行踪、身份隐蔽而具备实施侵害的有利条件。故被识别者在他人识别其个人信息后，便处于被动的不安全状态。

最后，他人在识别后可能造成不确定的损害。被识别者是确定的，识别者可以利用个人信息将之准确锁定，但识别者是不确定的，其在识别之后将在何时、何地以及如何行为，这对被识别者而言充满了不确定性，因此，他人尤其是缺乏信赖关系的人识别个人信息，就像是一颗“不定时炸弹”，给个人权利带来诸多不确定因素。有学者将风险进行量化，试图将风险解释为损害而囊括到侵权法体系之中。〔28〕风险若可被量化、确定，则可以准确预防利益侵害，也可以适用侵权救济。但风险的可怕之处正在于无法估计和预测，其辐射范围亦不可确定。正因如此，才需要强调国家履行保护义务，防范违法处理带来不可挽回的后果。

综上可知，处理者能够利用个人信息创造效益，并在不当处理后造成个人安全的减损，根源在于个人信息具有“识别”特性。正因如此，规制个人信息的违法处理，防范处理者对主体的任意识别，就是为了保障主体的安全。

四、安全利益区别于侵权法益

在法经济学的视角下，各种权利义务充当法律行为的成本因素和收益因素，〔29〕而减损他人安全在客观上将增设防范风险的个人注意义务，并消耗国家预防违法犯罪的法律资源，这些在安全减损前后出现的利益变动表明，安全是一种包含人格、财产与公共利益的复合型利益。在违法处理个人信息引发权利损害的“事后环节”，权利损害能够“激活相关民事实体权益的救济机制”〔30〕，适用侵权法救济；但违法处理直接造成的安全减损，是一种理念上的抽象不利益，

〔27〕 参见欧阳本祺：《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》，载《比较法研究》2021 年第 3 期。

〔28〕 参见田野：《风险作为损害：大数据时代侵权“损害”概念的革新》，载《政治与法律》2021 年第 10 期。

〔29〕 参见冯玉军：《法经济学范式》，清华大学出版社 2009 年版，第 231 页。

〔30〕 王锡锌：《个人信息权益的三层构造及保护机制》，载《现代法学》2021 年第 5 期，第 115 页。

不具有“已发生或迫近”与“具体”等侵权特点，且实践中风险防范支出要么不存在，要么因具有假设性或推测性而难以证明，〔31〕故亦不具有需要“填补”的利益损害。〔32〕因此，安全减损无法被视作侵权损害，安全利益区别于侵权责任保护的利益。

（一）安全是抽象的复合型利益

在现代化进程中，生产力的指数式增长，使风险和潜在自我威胁的释放达到了前所未有的程度，现代风险以系统的方式引发普遍甚至全球性的危险和不安。〔33〕贝克在提出风险社会的时候，人类还没有进入数字时代。时至今日，信息技术的威胁迫近。不当处理个人信息可能引发的权利损害，或许是大范围的甚至跨国性的。面对此等风险，国家积极采取保护措施，通过建构和运行一套关于个人信息处理的法律制度来履行保护义务，帮助个人对抗大规模、持续化信息处理中权利减损的风险，〔34〕“使风险处于社会观念可容忍的水准之下”〔35〕。是以在国家保护之下，违法处理个人信息将有损可信赖的安全秩序，引起个人和国家利益的变动。

一方面，违法处理个人信息为信息主体增设注意义务。数字背景下，个人信息与储蓄、不动产等私有财产以及人们重视的名誉、肖像等人格要素有着高度关联，而违法处理将突破国家对公民权利的基本安全保护，破坏被识别者对自身权利的安全预期，从而增加被识别者对自身权利的注意义务，即处理者将社会交往中应尽的控制或降低风险的危害防免义务转移给了被识别者。〔36〕注意义务的增设，迫使被识别者要么选择积极防御，以恢复至（令其感觉）安全的状态，由此承担实际支出和机会成本，即信息主体将有限资源用于防范风险而丧失其他用途的可能收益；〔37〕要么选择节省支出而忍受风险，由此承受可能出现的损害。可见，个人利益在违法处理前后产生变动，故安全是关乎信息主体权利的一项利益。

另一方面，违法处理个人信息将消耗国家机关的法律资源。由于违法处理个人信息为利用个人信息违法犯罪带来可能，而事后追究法律责任往往难以挽回受损利益，且难度大、耗时长，故国家机关出于正义和效率价值之考虑而倾向于采取事前预防，即通过规制违法处理个人信息活动，打击侵犯个人信息犯罪，以防范利用个人信息所实施的其他违法犯罪。正如检察机关所言：“打击利用互联网出售、提供、非法获取公民个人信息等侵犯公民个人信息犯罪，切断其与电信网络诈骗等犯罪的犯罪链条，从源头上预防和减少犯罪发生。”〔38〕显然，对违法处理行为的治理会增加国家机关的法律负担，消耗国家有限的司法资源，故检察机关常用“公共利益”来概括违法处理行为所侵害的对象。因此，保持权利处于安全状态，能节省国家机关在预防违法犯罪、维

〔31〕 See Emily Schmidt, *Article III Standing in Data-Breach Litigation: Does a Heightened Risk of Identity Theft Constitute an Injury-in-Fact?*, 49 Cumberland Law Review 389 (2019).

〔32〕 参见王泽鉴：《侵权行为》，北京大学出版社 2009 年版，第 175－176 页；王利明：《侵权责任法研究》（上卷），中国人民大学出版社 2010 年版，第 302 页。

〔33〕 参见〔德〕乌尔里希·贝克：《风险社会：新的现代化之路》，张文杰、何博闻译，译林出版社 2018 年版，第 3－7 页。

〔34〕 参见王锡锌：《个人信息保护的国家义务及展开》，载《中国法学》2021 年第 1 期。

〔35〕 王贵松：《论法治国家的安全观》，载《清华法学》2021 年第 2 期，第 24 页。

〔36〕 参见张新宝、唐青林：《经营者对服务场所的安全保障义务》，载《法学研究》2003 年第 3 期。

〔37〕 机会成本是指把一定的资源在用于某种用途时放弃其他用途所丧失的潜在利益。参见汪金锋、祁雄编：《西方经济学（微观部分）》，北京理工大学出版社 2018 年版，第 69 页。

〔38〕 2017 年 5 月 16 日《最高检发布六起侵犯公民个人信息犯罪典型案例》典型案例 3：“章某某等诈骗、侵犯公民个人信息案”，载 https://www.spp.gov.cn/xwfbh/wsfbt/201705/t20170516_190645.shtml#2. 最后访问时间：2021 年 12 月 13 日。

护法律秩序上的治理成本，故安全也包含公共利益。

综上可知，安全不仅是个人信息所蕴含的一种价值理念，〔39〕还是一种能够保障人们合理预期且客观存在的“人的生活利益”（menschliche Lebensinteressen）或“生活条件”（Lebensbedingung），〔40〕是一项包含人格、财产与公共利益的复合型利益。安全作为利益的成本收益分析，如图 2 所示。

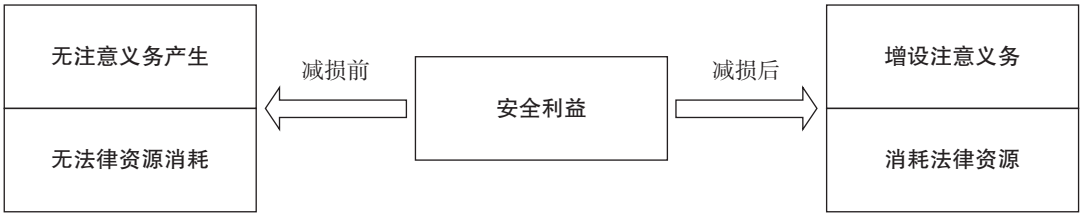

图 2　“安全”的利益分析

（二）风险不属于侵权损害

为化解个人信息保护中信息处理者责任无从追究的困境，有学者尝试把违法处理个人信息造成的“风险”解释为具有确定性的“损害”，由此将个人信息权益纳入侵权保护的范围，对处理者追究侵权责任。为满足成立侵权责任之要求，田野教授依靠证明风险的“高发性”和“利益差额”的可计算性，来解决风险作为“损害”的认定问题。〔41〕尽管违法处理所造成的权利风险升高客观存在，但由于风险发生的几率极低，且无法对风险升高前后的利益进行客观比较以确定损害，故风险升高作为“损害”的观点难以成立。此外，违法处理个人信息造成的风险，与侵权责任法中防御性请求权所对抗的危险有显著区别。后者是已着手的侵权行为所带来的紧迫且可被证明的妨害，前者是指发生侵权行为可能性的提升，二者所保护的利益并不相同。因此，安全利益区别于侵权法益。

1. 对风险“高发”的质疑

风险不具有高度盖然性和损害紧迫性。正如前文所述，违法处理个人信息并不定然带来人身、财产权利致损之结果，风险的发生属于偶然事件。在生活中，泄露或不当处理个人信息的行为大量存在，很多人身上都发生过接到推销房产、培训、保险等的本地、外地甚至境外陌生电话的情况，不少推销者清楚地知道接听者的姓名等个人信息，但实际上，由此发生电信诈骗、隐私刺探、恐吓骚扰、冒名顶替等情况的概率极小。“腾讯守护者计划”发布的《2017 年第四季度反电信网络诈骗大数据报告》显示，全国“第四季度诈骗电话拨打 1.6 亿次，收到诈骗短信人数为 467 万……诈骗案件共 23.9 万件”，即月均泄露和违法利用个人信息 0.55 亿条以上，而每月发生诈骗案件为 8 万件，故违法处理个人信息后诈骗风险的发生几率为≤0.15％。〔42〕综合这些数据

〔39〕 参见凌霞：《安全价值优先：大数据时代个人信息保护的法律路径》，载《湖南社会科学》2021 年第 6 期。

〔40〕 参见前引〔9〕，张明楷书，第 42 页。

〔41〕 参见前引〔28〕，田野文。

〔42〕 月均泄露和违法利用个人信息数量：(1.6＋0.0467)亿条/3 月≈0.55 亿条/月；违法处理个人信息后诈骗风险的发生几率：8 万件/0.55 亿条＝0.15％。参见《反电信网络诈骗大数据报告》，载 https://tg110.qq.com/newspage/report_center_20180208page1.html，最后访问时间：2021 年 11 月 17 日。

来看，在通信高度发达的数字时代，泄露、非法利用个人信息的行为在广泛、频繁地发生着，但是，利用个人信息实施诈骗等违法犯罪并造成实际损害的情况，相较于信息泄露等不当处理而言，少得多。因此，违法处理个人信息的风险“高发”实际指的是发生数量较多，而非发生几率较高。可见，个人信息处理致损的风险不具有高度盖然性。正因风险大概率不会暴发，且无法被预见何时何地暴发，故亦不具有紧迫性。

2. 对风险“损害”可计算的质疑

除不具有高发性外，风险还不具有确定性。田野教授尝试用三种“利益差额”来甄别、计算风险的“损害”，包括“个人信息暴露导致的风险升高”“预防风险的支出”“风险引发的焦虑”，但因缺乏可操作性与客观标准而无法用作“损害”的确定方法。

首先，“个人信息暴露导致风险升高”的利益差额无法证明。田野教授认为，风险在成为现实损害之前看起来风平浪静，实则暗流涌动，一旦暴发，想要补救为时已晚，因此，有必要在悲剧发生之前认可风险本身即是一种可获赔偿的损害。〔43〕但是，风险施加有害作用是“多么飘忽不定和不可捉摸”〔44〕。一方面，由于尚未出现实害行为，人身、财产权利在个人信息暴露前后不具明显差异，信息主体虽表示担忧，却仍能够正常行使权利。另一方面，风险升高是抽象的侵害，因不具有客观表现形态而不可预见，无从估算，无法举证，通常由主观感觉来认知，猜测权利在个人信息暴露后更易发生危害，而猜测性不符合侵权损害的确定性特征，故无法采取侵权救济。〔45〕

其次，预防风险的支出无法客观确定。基于理性经济人的理论假设，〔46〕面对权利风险，人们通常会在防御的支出与可能的损害之间进行利益对比，由此在忍受和防范之间进行选择。由于风险是否发生、何时何地发生以及发生的范围、程度等均无法预测，无法对风险升高前后的利益差额进行估计，遂无法作出理性选择。故在生活中，尽管违法处理个人信息案件频发，但多数人因无从对比而忍受权利风险，只有在侵害发生、权利受损后才选择维权，此时法院支持的诉讼请求是赔偿权利损害而非预防成本。田野教授以“沈晴与上海容蓁汽车用品有限公司姓名权纠纷案”为例，认为法院判令被告赔偿原告的 2500 元中，有部分属于预防风险的成本。但据判决书所述，“原告沈晴作为具有会计从业资格的财务工作人员，在正常的执业中受到了影响，产生了一定的财产损失”〔47〕，法院综合被告所得收益（即“减少必要用工成本”）和原告必要维权成本等因素，确定赔偿金额。可见，法院计算得出的赔偿金额是用于恢复原告财产损失的，而预防风险的支出在其中并未体现。在美国司法判决中，法院同样以无法确定损害（lack of a cognizable harm）为由，驳回信息主体的侵权赔偿请求。〔48〕因此，在违法处理个人信息致损的案件中，适用侵权救济的是权利损害，而非安全减损。

---

〔43〕 参见前引〔28〕，田野文。

〔44〕 前引〔33〕，乌尔里希·贝克书，第 15－16 页。

〔45〕 See Filippo Lancieri, *Narrowing Data Protection's Enforcement Gap*, 74 Maine Law Review 15 (2022); Steven Shavell, *Liability for Harm versus Regulation of Safety*, 13 Journal of Legal Studies 357, 357－363 (1984).

〔46〕 参见周林彬、董淳锷：《法律经济学》，湖南人民出版社 2008 年版，第 86 页。

〔47〕 上海市闵行区人民法院（2019）沪 0112 民初 26438 号民事判决书。

〔48〕 See Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 Texas Law Reriew 737, 737－739 (2018).

少数人具有较强的风险防范意识，在权利损害发生前积极防范风险，但无法通过侵权救济途径填补有关防范风险的支出。在“人脸识别第一案”中，原告为了防范权利风险而向法院提起诉讼，最终得到“合同利益损失及部分交通费”的赔偿与部分诉讼费的承担。其中，交通费的赔偿是基于违约责任而非侵权责任，诉讼费的支出亦未弥补。同样地，在“陈瑜婷与上海瑞慈瑞兆门诊部有限公司隐私权纠纷案”中，作为胜诉方的原告不仅没有获得维权支出的赔偿，还要承担主要的诉讼费用。可见，信息主体试图以侵权救济来恢复安全，但实际上并未由此填补防范风险的诉讼支出。此外，为防范风险而购买的风险监控和管理等商业服务（如保险、信用状况监督），其实际支出和机会成本具有较强的主观性。这是因为，风险无法被准确预见，信息主体遂无法采取针对性的防范措施，故其为恢复安全所做的实际支出均为猜测而非必需；此外，机会成本是一种假计成本，没有实际支出且不可计量。〔49〕因此，把猜测的预防支出和抽象的机会成本归责于违法处理行为，这将突破“过错责任”“过错与责任相适应”等侵权法原则。由此观之，采用“预防风险的支出”来确定风险造成的“利益差额”不具有可行性。

最后，风险引发的焦虑不应属于侵权法中的精神损害。一方面，依据《中华人民共和国民法典》（以下简称《民法典》）第1183条，侵权法的精神损害赔偿须以侵害“人身权益”或“具有人身意义的特定物”为基础，“只能对人格权受到侵害导致的精神痛苦、生理疼痛以及其他不良情绪提供补偿”〔50〕，故安全减损因缺乏人格权利损害而不能主张精神损害赔偿。另一方面，将焦虑这一主观感觉认定为精神损害，将造成法律秩序的混乱。如在陈瑜婷案中，信息主体虽表达了对安全的焦虑和担忧，但只停留在模糊的感觉上，对后续实害是否发生、何时何地发生、多大范围内发生以及造成何种程度的损失均不清楚。与这种焦虑相比，生活中因恋爱、婚姻、工作、学业等产生的诸般焦虑可能严重百倍，如果承认风险引发的焦虑为精神损害，那么将有无数伴侣、家人、单位、学校会出现在精神损害赔偿案件的被告席，造成滥诉。因此，将“风险引发的焦虑”解释为“利益差额”不具有可行性且将有害于法律秩序。

3. 与“危及人身、财产安全”之区别

《民法典》第1167条规定：“侵权行为危及他人人身、财产安全的，被侵权人有权请求侵权人承担停止侵害、排除妨碍、消除危险等侵权责任。”显然，该条作为防御型侵权责任的一般规定，也提到了“安全”。但是，这里的“安全”对应的是侵权行为带来的现实妨害和可预期危险，与个人信息保护的安全利益有显著不同。

根据民法学界通说，停止侵害、排除妨碍、消除危险可归结为妨害排除和妨害防止两个方面。〔51〕妨害排除适用于侵害行为已经发生或正在进行的情况，即以“因现存的妨害源而产生的妨害在持续”为要件。〔52〕在该情况下，人身、财产权利已实际受到妨害，亟需去除妨害权利行

〔49〕 参见李欣隆：《机会成本与道德的关系探微》，载《道德与文明》2018年第1期；毛洪涛：《西方经济学成本基本范畴研究》，载《会计研究》2000年第10期。

〔50〕 许中缘、崔雪炜：《论合同中的人格利益损害赔偿》，载《法律科学（西北政法大学学报）》2018年第3期，第129页；张新宝主编：《精神损害赔偿制度研究》，法律出版社2012年版，第57页。

〔51〕 参见杨彪：《非损害赔偿侵权责任方式的法理与实践》，载《法制与社会发展》2011年第3期；茅少伟：《防御性请求权相关语词使用辨析》，载《法学》2016年第4期。

〔52〕 参见前引〔51〕，茅少伟文。

使的“瑕疵”以恢复至完满状态。故妨害排除请求权所保障的，实为人身、财产权利本身。

妨害防止请求权以存在重复发生之危险为要件，行使于侵权行为发生之前，目的是使行为人不再从事威胁他人的特定行为。〔53〕其中，“危险”的概念决定了防御性请求权的边界。根据人格权法和物权法，防御性请求权所针对的危险应当是现实且可被证明的。《民法典》第 997 条的人格权禁令制度，是为更好实现《民法典》第 1167 条中有关人身利益安全的程序保障。〔54〕该条规定了权利人主张人格禁令的基本条件：行为人应当即将或正在实施侵害人格权的违法行为；且民事主体应就侵害行为以及可能造成的损害后果提交必要的证据等。〔55〕简言之，行使人格权妨害防止请求权，须能够证明存在紧迫或至少是可预见的现实威胁，而不能基于无法确定的、推测性的风险。〔56〕同样地，物权的妨害防止请求权并非请求权人主观上一感受到危险即可行使，〔57〕亦须满足对物的支配存在明确威胁之条件，即“根据一般的基准（标准）或情形，妨害（侵害）发生的危险性或可能性系明确、清楚”〔58〕。因此，妨害防止请求权所防范的是可预见、明确的现实威胁，且能够证明其权益受到的妨害存在着为社会所认可的确实可能性，而不能是无法预见、无法证明的风险。

总之，《民法典》第 1167 条规定的防御性请求权虽然涉及“安全”，但这与个人信息保护的安全并不相同。前者对应的是正在发生的妨害或可预见的现实危险，而后者对应的是无法预见和证明的风险，即相较于无违法处理时发生侵害行为的更大可能性。故个人信息保护的安全利益不是《民法典》第 1167 条中的“安全”，与侵权法益相互独立。

综上，个人信息保护的安全利益包含了人身、财产利益与公共利益，区别于侵权保护的法益。个人信息保护的安全利益是违法处理行为发生前，信息主体人身、财产保持原有低风险状态，以及公共法律资源未被增加使用的复合型利益。而侵权保护则主要是在侵权行为发生后对损害的填补，以及对正在发生的妨害和可预见的现实威胁的制止。有学者认为：“将个人信息权益理解为权益集合的观点会对整个侵权法的归责体系造成毁灭性破坏。”〔59〕但实际上，个人信息保护的利益目的和适用领域与侵权保护有着显著区别，前者并不会对后者取而代之。

五、《个保法》中安全法益的规范证成

违法处理造成的安全减损，因无法计算并证明损害结果而无法适用侵权法救济。但这并不意味着法律对该不利益状态的放任。通过规范分析可知，《个保法》正是用于防范和化解这种不利益，保护和恢复安全。

（一）《个保法》对违法处理的防范是为了保护安全法益

《个保法》规定了个人信息处理规则、处理者义务以及对处理活动的监督机制等，用来预防

〔53〕 参见曹险峰：《防御性请求权论纲》，载《四川大学学报（哲学社会科学版）》2018 年第 5 期。
〔54〕 参见程啸：《论我国民法典中的人格权禁令制度》，载《比较法研究》2021 年第 3 期。
〔55〕 参见张红：《论〈民法典〉之人格权请求权体系》，载《广东社会科学》2021 年第 3 期。
〔56〕 参见毕潇潇、房绍坤：《美国法上临时禁令的适用及借鉴》，载《苏州大学学报（哲学社会科学版）》2017 年第2 期。
〔57〕 参见范雪飞：《请求权的一种新的类型化方法：攻击性请求权与防御性请求权》，载《学海》2020 年第 1 期。
〔58〕 陈华彬：《论所有权人的物上请求权》，载《比较法研究》2020 年第 1 期，第 88 页。
〔59〕 前引〔7〕，程啸文，第 9 页。

违法处理行为的发生，规避信息主体的权利风险，保障信息主体的权利处于安全状态，即保护安全利益。

首先，《个保法》设置了规范个人信息处理的规则，约束处理活动以保护安全法益。一方面，“知情同意”是个人信息处理的合法基础与核心规则，〔60〕据此，信息主体依靠自身意愿与风险评估，来理性地选择是否进入信息处理活动之中。〔61〕另一方面，《个保法》要求处理活动符合必要（最小）原则，在有助于目的实现的必要范围内运用对个人权益影响最小的手段，包括收集最少够用的个人信息、个人信息不得用于其他目的、在授权目的与合理期限内合理使用或存储个人信息。可见，知情同意与必要原则的设置用于规制个人信息处理活动，使处理活动被限制在可容忍、可控的限度内，从而尽可能降低不当处理个人信息所引发的权利侵害可能，故其保障的是安全法益。

其次，《个保法》规定了处理者的义务，以保护安全法益。处理者采取必要措施最大程度保障个人信息安全，是个人信息处理必要原则的重要内涵。〔62〕为防止对个人信息进行未经授权的访问或违法处理，法律规定个人信息处理者应当依据“可能存在的安全风险”采取系列措施，包括：制定内部管理制度和操作规程，对个人信息实行分级分类管理，采取相应的加密、去标识化等安全技术措施，合理确定个人信息处理的操作权限，并定期对从业人员进行安全教育和培训，制定并组织实施个人信息安全事件应急预案（《个保法》第51条）。《个保法》为处理者设置的管理和组织等义务，防范的是“可能存在的安全风险”而非权利危险或损害，即保障信息主体的安全法益。

最后，《个保法》对个人信息处理活动设立了监督机制以保护安全法益，包括自我监督、国家监督和公民监督。在自我监督方面，法律要求“处理个人信息达到国家网信部门规定数量”的个人信息处理者，安排专人或设立专门机构，负责个人信息保护事务，并公布责任人姓名和联系方式，还要求个人信息处理者对其开展的处理活动与保护措施进行定期的合法、合规审计，对信息处理活动产生的风险进行动态监督、风险评估、报告发布等（《个保法》第52—56、58条）。在国家监督方面，法律规定了国家网信部门及有关部门对处理活动的监管职责，包括询问、查阅、复制、检查和调查等（《个保法》第60—63条）。在公民监督方面，法律赋予信息主体查询、复制等监督权利，赋予组织、个人投诉、举报的权利（《个保法》第45、65条）。这些机制的设置均用于对个人信息处理活动的常态化监督，对可能的侵权风险进行监控，以避免违法处理个人信息的发生，对安全法益予以保护。

由此可见，《个保法》通过设置处理规则、处理者义务以及监督机制，防范违法处理的发生，规避权利受损风险，使处理活动按照法定轨道开展，使潜藏于其中的权利风险保持在人们普遍接受和可控的限度内，使权利处于可信赖的安全状态，〔63〕即保护安全法益。

---

〔60〕 参见《关于〈中华人民共和国个人信息保护法（草案）〉的说明——2020年10月13日在第十三届全国人民代表大会常务委员会第二十二次会议上》，载 http://www.npc.gov.cn/npc/c30834/202108/fbc9ba044c2449c9bc6b6317b94694be.shtml，最后访问时间：2021年12月26日；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；万方：《隐私政策中的告知同意原则及其异化》，载《法律科学（西北政法大学学报）》2019年第2期。

〔61〕 参见前引〔19〕，梅夏英文；丁晓东：《个人信息保护：原理与实践》，法律出版社2021年版，第67页。

〔62〕 参见刘权：《论个人信息处理的合法、正当、必要原则》，载《法学家》2021年第5期。

〔63〕 参见周学峰：《个人信息保护立法中的基础问题探讨》，载《北京航空航天大学学报（社会科学版）》2020年第3期。

（二）《个保法》对违法处理的规制是为了恢复安全法益

《个保法》规定了违法处理发生之后的规制，主要从处理者的义务履行、网信等部门的职责履行和信息主体的权利行使三个维度展开。分析可知，这些规制措施用于化解违法处理所升高的风险，对安全法益予以恢复。

首先，《个保法》要求处理者在违法处理后及时履行补救和通知义务，以降低风险，并使信息主体自主评估和控制风险。根据《个保法》第 57 条第 1 款，个人信息处理者采取补救措施的条件是“发生或可能发生个人信息泄露、篡改、丢失”，这表明此时尚未出现对信息主体权利的损害或威胁，故补救义务的内容是个人信息的不当处理状态而非权利损失。结合《个保法》第 57 条第 2 款可知，通知义务履行的条件是“履行个人信息保护职责的部门认为可能造成危害的”，其目的是使个人在知晓风险的基础上做好风险应对。若风险不可避免，及时告知个人泄露、篡改、丢失的信息种类、原因和可能造成的危害，已采取的补救措施和个人可以采取的减轻危害的措施，以及处理者的联系方式，亦是规避风险的必要之举。故《个保法》设置处理者在违法处理后的补救和通知义务，是出于恢复安全法益之目的。

其次，《个保法》设置了网信等部门对违法处理行为的惩治规则，为安全法益的恢复提供强制力保障。依据《个保法》第 64 条之规定，在监督过程中发现个人信息处理活动存在较大风险或者发生个人信息安全事件后，有关部门通过履行约谈、合规审计等职权，要求处理者“采取措施，进行整改，消除隐患”。从中可知，消除隐患是采取措施和进行整改的目的。“隐患”意指潜藏的祸患，即产生危害的可能，故对违法处理者的约谈、合规审计等是为了消除违法处理所带来的危害可能，即恢复安全。若处理者拒不改正，则依据《个保法》第 66—67 条之规定，有关部门有权对其处以罚款、没收违法所得等行政处罚。这正是《个保法》为安全法益的恢复所提供的强制力保障。

最后，《个保法》赋予公民“个人信息权利束”，目的是能够更高效地规制个人信息处理活动，〔64〕及时恢复安全法益。依据《个保法》第 46—50 条，信息主体通过行使更正、补充权利，使个人信息完整、正确；通过行使删除权利，使个人信息被最小化利用；在处理者拒绝个人行使权利请求之后，个人有权向法院提起诉讼。而保证个人信息的完整、正确和最小化利用，目的并非救济财产、人格损害，而是及时发现和纠正个人信息的违法处理行为，避免发生个人信息被违法利用并致其权利受损的情况。并且，这些“个人信息权利束”是在国家规制框架中对个人进行的赋权，是国家为保障安全法益而设置的监管机制的组成部分。〔65〕故《个保法》赋予工具性权利，亦是为了恢复安全法益。

综上，“个人信息权益”就是安全法益。《个保法》着重对违法处理行为本身进行规制，设置多种机制来保护和恢复安全。“安全”在我国《宪法》中以概括性的形式出现。《个保法》中的“根据宪法”条款表明，国家在个人信息保护制度中为个人安全提供保障，〔66〕故个人信息保护的

〔64〕 参见前引〔5〕，王锡锌文。

〔65〕 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》，载《环球法律评论》2022 年第 1 期。

〔66〕 参见前引〔35〕，王贵松文。

安全法益具有宪法基础。

六、结　语

个人信息权益不是财产、人格权利，而是安全法益，故个人信息保护与侵权保护是相互独立的两种制度。《个保法》第69条涉及违法处理个人信息致损的侵权责任，容易发生个人信息保护与侵权保护的混淆，需要予以说明。如前所述，“处理个人信息侵害个人信息权益造成损害”存在两个行为，即违法处理和实际侵害。违法处理不直接造成损害，故在损害发生前适用个人信息保护规则。在损害发生后的侵权救济中，由于处理者具有保障信息安全的严格的注意义务，并掌握证据资料和调查取证的技术优势，〔67〕更具有实施侵害的便利条件，故《个保法》第69条的侵权规则要求其承担过错推定责任。易言之，处理者若不能证明自己没有过错，则应当推定其对实害行为发挥积极作用，应承担损害赔偿等侵权责任。可见，《个保法》第69条不是个人信息保护与侵权保护的混淆，而是权利损害发生后两种保护规则的衔接。

Abstract: The rights of access, correction and deletion created by law are not the purpose of personal information protection. The damage to personality and property rights is not directly and inevitably caused by the illegal handling of personal information, but should be attributed to the subsequent independent infringement. Therefore, personality and property rights are not the object of illegal handling, nor the direct purpose of personal information protection. The direct consequence of illegal handling is to increase the risk of infringement to rights. Thus the interest of the nuisance is security. Security derogation causes the increase of duty of care and the consumption of legal resources. However, since the difference of interests cannot be proved and calculated, nor did foreseeable danger occur, tort remedy cannot be applied. Different from tort protection, the Personal Information Protection Act sets up norms of handling rules, rights and obligations, powers and responsibilities, and the purpose of which is not to compensate for damage, but to protect and restore safety. Personal information protection and infringement protection are relatively independent. Article 69 of the Personal Information Protection Act is a convergence of the two protections.

Key Words: illegally handling personal information, harmfully infringing, identifiability, tort protection, security legal interest

（责任编辑：殷秋实　赵建蕊）

〔67〕 参见孔祥稳：《论个人信息保护的行政规制路径》，载《行政法学研究》2022年第1期。