中外法学 Peking University Law Journal
Vol. 36, No. 2(2024)pp. 366－385

个人信息保护法与侵犯公民个人信息罪的衔接机制

童云峰*

摘 要 《个人信息保护法》是数字时代的前沿性法律，具有前置法、不完整领域法、不真正附属刑法的特征，与《刑法》中侵犯公民个人信息罪的规定存在时差。为了有效融通规范之间的衔接鸿沟，需要将《个人信息保护法》嵌入侵犯公民个人信息罪的出入罪适用流程。在入罪衔接机制上，将两法中的个人信息范围作统一理解，避免犯罪圈的扩张化；将前置法关于个人信息的类型划分和处理设置，作为解释侵犯公民个人信息罪构成要件的方向，以实现罪刑均衡和法律衔接。在出罪衔接机制上，《个人信息保护法》上的“同意”因法益阙如而阻却刑事违法，其余《个人信息保护法》上的正当化事由均因法益衡量原理阻却刑事违法，相应正当化事由可分别归入刑法教义学上的正当业务行为、紧急避险、法令行为，而合理处理已公开个人信息应成为数字时代独立的新型违法阻却事由，前述事由可在个人信息分类场景下为相关行为出罪。

关 键 词 个人信息保护法 侵犯公民个人信息罪 同意 法益衡量

进入数字时代，我国陆续创设诸如《中华人民共和国数据安全法》(以下简称《数据安全法》)和《中华人民共和国个人信息保护法》(以下简称《个保法》)等数字法律。基于此，我国政策与理论层面形成了具有领域法属性的数字法学。比较来看，德国、日本遵循二元刑法模式，诸多特定领域的犯罪被规定在附属刑法中，无需考察刑法典；自 1997 年《中华人民共和国刑法》(以下简称《刑法》)颁行后，我国即采纳统一刑法典模式。然而，以侵犯公民个人信息罪为代表的数字犯罪具有明显的法定犯属性，构成要件的补足需要依赖前置法。因此，寻找新兴数字法律与相对滞后的刑法典的妥当衔接方案，已成为数字时代法学研究者的使命。本文主要探讨《个保法》与《刑法》中侵犯公民个人信息罪的衔接适用机制，以期通过“以点带面”的方式

* 华东政法大学中国法治战略研究院副研究员。本文系上海市哲学社会科学规划课题青年项目“数字时代个人信息权益的全生命周期刑法保护研究”(项目编号：2023EFX010)的阶段性研究成果。

为新兴数字法律与刑法的精准衔接提供参考。

一、个人信息保护法与侵犯公民个人信息罪的关系

在《个保法》颁行之后，我国关于个人信息保护的系统性法律格局已形成。在寻找《个保法》与侵犯公民个人信息罪的衔接机制之前，需先厘清二者之间的关系。

（一）个人信息保护法是适用侵犯公民个人信息罪的前置法

域外立法所创设的个人信息保护法律，均包括私法、公法和刑法的规范内容，强调无论民法、行政法亦或刑法都应保护个人信息。〔1〕我国关于《个保法》属性界定的研究成果已经较多，主要包括私法说、公法说、交叉混合说和领域法说等。〔2〕既有研究均试图界定《个保法》属性，但大多忽视了它与《刑法》的关系。我国《个保法》除了有诸多调整平等主体之间关系的规范外，其第二章第三节“国家机关处理个人信息的特别规定”、第六章“履行个人信息保护职责的部门”、第七章“法律责任”，均是关涉行政法规范的整体性布局。我国《个保法》中的私法条文是民法的特别法，而公法条文则是行政法的特别法。

一方面，欠缺保护个人信息罪名与法定刑规范的《个保法》是不完整的领域法。所谓“领域法”是以解决问题为导向，不受传统部门法逻辑束缚，调整某一特定领域的法律规范集合，如教育法、卫生法等。〔3〕领域法学是以领域法为研究对象的学科体系，研究领域法的发展规律和现实问题。为了应对个人信息领域层出不穷的新式社会问题，立法者要打破公私对立、部门法分立的传统僵化思维，采纳公私融合与部门法协同的新思维去勾勒个人信息保护制度，推动个人信息之上多元利益的兼容与协调。可见，《个保法》是调整个人信息关系的法律规范集合，具有强烈的领域法属性。因此，侵犯个人信息权益行为承担的法律责任具有递进性，不法行为按照情节轻重依次适用侵权责任、行政责任和刑事责任。德国《联邦数据保护法》和日本《个人信息保护法》等域外个人信息法律，均直接设置了保护个人信息的具体罪名与法定刑。与此迥异，我国遵循统一刑法典模式，《个保法》第71条只规定“构成犯罪的，依法追究刑事责任”。可见，此处的“依法”显然是依据《刑法》追究刑事责任。换言之，德日的“个人信息保护法律”可以完整容纳民事责任、行政责任和刑事责任，属于完整的领域法。而我国《个保法》只能涵盖民事责任和行政责任，没有刑事责任，属于不完整的领域法。《个保法》加上《刑法》中保护个人信息的罪状与法定刑，才能组成完整的保护个人信息的领域法。

另一方面，《个保法》是判断侵犯公民个人信息罪的前置依据。我国《个保法》与《刑法》中

---

〔1〕 See Murat Volkan Dülger, “Protection of Personal Data with Criminal Norms in the Context of Protection of Personal Data Law and Turkish Criminal Code,” *Istanbul Medipol Universitesi Hukuk Fakultesi Dergisi*, Vol. 101, No. 3, 2016, pp. 104-105.

〔2〕 See Tong Yunfeng, “The Influence of the Personal Information Protection Law on Crime Evaluation under the Principle of Law Unity,” *China Legal Science*, Vol. 11, No. 5, 2023, pp. 111-112.

〔3〕 参见薛刚凌：“行政法法典化之基本问题研究——以行政法体系建构为视角”，《现代法学》2020年第6期，第89页。

的侵犯公民个人信息罪虽有共同的立法目的和价值旨趣，但两部法律的规制功能和调适方法并不相同。《个保法》作为前置法具有敏捷性，而《刑法》属于保障法具有谦抑性，这就决定了两部法律追究行为人法律责任的力度存在明显差异。《个保法》无法调控已经触刑的侵犯个人信息行为，《刑法》中侵犯公民个人信息罪的构成要件和违法性的判断，尚需从《个保法》中寻找依据，只有将《个保法》嵌入《刑法》中才能准确适用侵犯公民个人信息罪。司法者在判断刑事责任时，应将二者有效衔接。要言之，欠缺刑事责任条款的《个保法》是个人信息领域的前置法，而《刑法》中的侵犯公民个人信息罪是个人信息领域的保障法。

（二）个人信息保护法中的涉刑条款是“不真正附属刑法”

所谓附属刑法是指，关涉刑罚的规定附属在刑法典之外的非刑法中，例如，破产法、公司法等。〔4〕这些法律本身不是刑法，但其中隐藏着几个刑罚的制裁规定。需要思考的是，《个保法》第 71 条涉刑条款能否理解为附属刑法？

首先，我国不存在附属刑法与核心刑法的区别。我国与域外关于附属刑法概念的理解存在区别，在德国，附属刑法较为丰富，与附属刑法相对应的是核心刑法（一般是指刑法典），例如《德国刑法典》制定于 1871 年，之后经过多次修订。德国存在附属刑法与核心刑法区分的难题，理论上形成了立法技术观、法益性质理论、规制对象理论和秩序属性理论等界分标准论。〔5〕《法国刑法典》之外的附属刑法也较为丰富；《意大利刑法典》只规定传统犯罪，如杀人、抢劫、诈骗等，其他犯罪则散布在其他法律中；《日本刑法典》之外的单行刑法与附属刑法也难计其数，它们可以直接规定犯罪与刑罚。〔6〕可见，域外的附属刑法直接规定犯罪与法定刑，是刑法的重要渊源。而我国奉行统一刑法典模式，尚无附属刑法与核心刑法区分的难题。我国学者所认为的我国刑法中的附属刑法，与域外的附属刑法不能等同，它并不包含罪名与法定刑。

其次，《个保法》中的涉刑条款应是“不真正附属刑法”。本文提倡将我国附属刑法概念分为“真正附属刑法”和“不真正附属刑法”，前者是在非刑法法律中直接设置罪状与法定刑的规范；后者是在非刑法规范中仅概括描述需要承担刑事责任的规范。这一概念区分借鉴了刑法教义学上“真正不作为犯——不真正不作为犯”“真正身份犯——不真正身份犯”的区隔，且我国刑法学者也有过类似的区分表达。〔7〕按照“真正的附属刑法——不真正附属刑法”的区分逻辑，我国刑法上的附属刑法应是不真正附属刑法。1979 年《刑法》颁布后，从 1981 年至 1997 年我国开展大规模刑法修订，全国人大常委会先后颁布了 25 部单行刑法和在 107 部法律中附设了 130 多个专门的罪刑条款，附属刑法受到青睐。〔8〕我国自 1997 年采纳统一刑法典模式

〔4〕 参见林东茂：《刑法纵览》，一品文化出版社 2016 年版，第 4 页。

〔5〕 参见柏浪涛：“德国附属刑法的立法述评与启示”，《比较法研究》2022 年第 4 期，第 101—104 页。

〔6〕 参见张明楷：“网络时代的刑事立法”，《法律科学》2017 年第 3 期，第 75 页。

〔7〕 我国早有学者关注到这一区分，将二者定名为独立性的散在型附属刑法立法模式和依附性的散在型附属刑法立法模式。参见柳忠卫：“刑法立法模式的刑事政策考察”，《现代法学》2010 年第 3 期，第 49—50 页。

〔8〕 参见周光权：“我国应当坚持统一刑法典立法模式”，《比较法研究》2022 年第 4 期，第 58 页。

后，单行刑法模式被废弃，而所谓的附属刑法也只是在其他法律中设置诸如“依照刑法有关规定追究刑事责任”之类的规定。至此，我国刑法学领域便一直不存在真正意义上的附属刑法。与德国、日本的行政刑法相比，我国的附属刑法名不副实。我国所谓的附属刑法几乎均可归为“不真正附属刑法”，《个保法》第71条涉刑条款亦是如此。“不真正附属刑法”是我国刑法的特色，它能够阐明前置法与刑法的关系，这一概念对于构建中国自主刑法教义学话语体系具有一定的意义。

最后，不真正附属刑法与刑法中的空白罪状相互呼应。《刑法》第253条之一为侵犯公民个人信息罪设置了空白罪状，即以“违反国家有关规定”为前提。立法者为了实现刑法与前置法的沟通，推动刑法的开放与发展，故意将相关构成要件要素委任于前置法。为了填充该罪的空白罪状，《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《个人信息刑案解释》）将“违反国家有关规定”的范围界定为“法律、行政法规、部门规章”。2017年的《个人信息刑案解释》在生效之时，我国尚无保护个人信息的专项法律。因此，司法解释对侵犯公民个人信息罪空白罪状的范围划定较广。2021年生效的《个保法》统合了个人信息领域的法律规范，此后侵犯公民个人信息罪中的空白罪状主要指“违反《个保法》中的规定”。可见，《个保法》中不真正附属刑法与侵犯公民个人信息罪中的违反性规定应相互呼应。一方面，《个保法》中不真正附属刑法指明，对于比较严重的侵犯个人信息行为，应适用《刑法》进行定罪量刑。另一方面，侵犯公民个人信息罪中的违反性规定指明，需要从《个保法》中寻找规范以补足构成要件。

（三）个人信息保护法与侵犯公民个人信息罪需要充分沟通

在2009年至2021年间，我国关涉个人信息的刑事立法已相对完善，但系统性前置立法尚未启动。然而，刑法上侵犯公民个人信息罪以“违反国家有关规定”为前置条件，这就表明在之前很长一段时间内，司法实践中侵犯公民个人信息行为的入罪，欠缺《个保法》作为一道前置防线，诸多不法行为可能跳跃前置法而直接进入犯罪评价圈，使得“违反国家有关规定”的功能无法施展，刑法难免存在处罚早期化的情形。按照法学一般常理，在法秩序体系内无论立法抑或司法，均应警惕“先刑后民”或“先刑后行”的法治风险。〔9〕为了避免这一风险，近年来我国关涉个人信息保护的前置立法不断完善，《民法典》《数据安全法》和《个保法》相继生效，创设了诸多新规则、新制度。与此相对，《刑法》中的相关制度则呈现出相对滞后的特征，由“刑法先行”转向“刑法滞后”的规范格局。因此，为了避免侵犯公民个人信息罪适用的早期化，应将《个保法》嵌入该罪的适用流程，《个保法》与侵犯公民个人信息罪的有效衔接是以二者充分沟通为前提。

首先，《个保法》与侵犯公民个人信息罪的沟通需要摆正二者适用的位阶。符合法理的立法规制位阶是，先由前置法立法规制相关行为，其中较为严重的不法行为才需启动刑事立法调控。然而，个人信息立法是先设置侵犯公民个人信息罪后制定《个保法》，这种立法倒置现象会促使侵犯公民个人信息罪适用的早期化。同时，当前刑法学上形成了两大趋势：一是刑法的工

〔9〕 参见王锡锌：“个人信息权益的三层构造及保护机制”，《现代法学》2021年第5期，第122页。

具化;二是刑法“去枷锁化”,去除传统法治国对刑法的各种限制,推动刑法灵活化。〔10〕 如此趋势可能使侵犯公民个人信息罪脱逸前置法的限制,直接作用于具体个案继而加剧刑法适用的早期化。为此,在《个保法》生效之后,应将大部分侵犯个人信息行为交由《个保法》调适,发挥《个保法》承担避免刑法提前适用的功能,警惕《个保法》规制功能成为“马奇诺防线”,只有严重侵害法益的行为才应由刑法调控。

其次,《个保法》与侵犯公民个人信息罪的沟通需坚守法定犯的从属性。侵犯公民个人信息罪以“违反国家有关规定”为前置要件,体现其对前置法的从属性,集中呈现为三个维度:①概念的依附性,例如,在《个保法》生效后,侵犯公民个人信息罪中个人信息范围的划定应与《个保法》保持一致;②空白罪状的依附性,侵犯公民个人信息罪中构成要件不明确的事项需要在《个保法》中寻找依据;③违法阻却事由的依附性,在《个保法》中属于正当化的行为,在刑法中也不应被惩罚。〔11〕 法定犯的从属性包括消极的从属性和积极的从属性,前者是出罪从属性,即如果行为没有违反前置法,那么构成犯罪的基础也就不存在;后者是入罪从属性,即构成要件的判断对前置法违反的依赖性。〔12〕 为坚守这种从属性,在进行刑事违法性判断时,先进行前置法层面的实质判断,得出违法结论后再进行刑事违法判断。换言之,前置法违法性是断定刑事违法性的必要不充分条件。

最后,《个保法》与侵犯公民个人信息罪的沟通应遵循“缓和的违法一元论”。按照法秩序统一性原理的理解,各个部门法关于同一事项的处理应彼此和谐,不应相互抵触。至于刑法与前置法在违法性判断上如何协调,存在三种理论:①违法相对论,不同部门法关于违法性的判断应相互独立,刑法违法性与前置法违法性的判断并不勾连;②严格的违法性一元论,即不同部门法关于违法性的判断应完全一致;③缓和的违法一元论,即不同部门法的违法性在总体上是一致的,但彼此之间存在程度上的差异,前置法上的违法行为可能因为情节轻微而未达到刑事违法性程度,刑法不予评价但不意味着在刑法上是合法行为。〔13〕 若遵循违法相对论,则《个保法》与侵犯公民个人信息罪也就没有沟通之必要;若遵循严格的违法性一元论,不仅无法划分违法性的程度,也无法厘清《个保法》与侵犯公民个人信息罪适用的先后顺序。本文提倡缓和的违法一元论,它能够在践行法秩序统一性原理的基础上,说明前置法违法性与刑法违法性的程度差异,也是《个保法》与侵犯公民个人信息罪能够有效沟通的前提。

二、个人信息保护法与侵犯公民个人信息行为入罪的衔接机制

在入罪衔接机制方面,需以《个保法》确立的新型规则为方向,对侵犯公民个人信息罪的构

〔10〕 参见(德)希尔根多夫:《德国刑法学:从传统到现代》,江溯等译,北京大学出版社 2015 年版,第 249 页。

〔11〕 参见刘艳红、周佑勇:《行政刑法的一般理论》(第 2 版),北京大学出版社 2020 年版,第 9—10 页。

〔12〕 参见陈兴良:“法定犯的性质和界定”,《中外法学》2020 年第 6 期,第 1482—1483 页。

〔13〕 参见张明楷:《外国刑法纲要》(第 3 版),法律出版社 2020 年版,第 114—115 页。

成要件进行合理解释。

(一)个人信息保护法关于个人信息的识别与侵犯公民个人信息罪衔接

关于个人信息含义的立法例有如下类型:①定义描述立法例;[14]②“抽象定义+具体列举”立法例。[15] 关于个人信息的内涵应采纳何种标准,理论与实践中存在不同方案:①隐私性标准,美国即采纳这一标准,个人信息可以被隐私涵摄;②识别性标准,通过分析特定信息可以甄别具体的自然人,那么该则信息即为个人信息;③关联性标准,知道特定自然人之后,那么所有与之相关的信息均为个人信息。[16] 本文认为,在我国的整体法秩序下对个人信息含义的界定应遵循识别性标准。

其一,在《个保法》颁行之前我国诸多规范已确立个人信息的识别性标准。在前置法层面,2016 年的《中华人民共和国网络安全法》第 76 条第 5 项、2020 年《民法典》第 1034 条均界定了个人信息的内涵。在刑法领域,2017 年《个人信息刑案解释》第 1 条也界定了“公民个人信息”。上述规范共同组成前《个保法》时代我国个人信息保护的基本法律秩序,不同规范均坚持“识别性”标准。

其二,纵然《个保法》关于个人信息内涵的规定与既有规范不同,但仍可被解释为对识别性标准的坚守。《个保法》第 4 条规定,“个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息,不包括匿名化处理后的信息。”其与前述法律规范关于个人信息定义的区别有两点:①对个人信息适用的是定义描述法,并未举例说明。②该条特别强调“有关”二字。有观点认为,“有关”是在阐述关联性,表明《个保法》在承继既有识别性标准的基础上已转向关联性标准。[17] 还有学者认为,我国《个保法》已吸收欧盟《一般数据保护条例》的“关联性”标准。[18] 由此产生疑问,《个保法》关涉个人信息范围的划定是否已抛弃“识别性”标准?侵犯公民个人信息罪入罪的“个人信息”要件的判定是否要改变?

首先,《个保法》关于个人信息定义的补充说明揭示了对“识别性”标准的坚守。《个保法》第 4 条第 1 款从正反两方面界定了个人信息,正面是直接对“个人信息”下定义;反面是特别说明“不包括匿名化处理后的信息”。可以从中推导出两层含义:①通过反向推理可以得出《个保法》仍采纳“识别性”标准。若《个保法》已采纳关联性标准,则经匿名化处理后的信息虽无识别性但仍有关联性,应属于个人信息。然而,《个保法》通过反面说明,旨为将有相关性但无识别

〔14〕 即在规范条文中对个人信息含义予以纯粹说明,遍览域外各国,这种模式总体相对较少,以英国的《数据保护法案》为主要代表,美国有关州的最新立法《弗吉尼亚州消费者数据保护法》(Virginia Consumer Data Protection Act,VCDPA)也采纳这一立法例。

〔15〕 即在对个人信息进行抽象定义后,通过列举典型个人信息以阐明个人信息的基本属性,这种立法例是当前国际社会的主流做法,比如欧盟的《一般数据保护条例》。

〔16〕 参见张平主编:《中华人民共和国个人信息保护法理解适用与案例解读》,中国法制出版社 2021 年版,第 10 页。

〔17〕 同上注。

〔18〕 参见王利明、丁晓东:“论《个人信息保护法》的亮点、特色与适用”,《法学家》2021 年第 6 期,第 2 页。

性的数据驱逐出个人信息范畴,可见《个保法》仍在坚守识别性标准。②“有关”不应理解为“关联”,而应理解为对“识别”的重申。特定信息一旦具备识别性,必然会与特定的自然人相关。域外有的国家或地区已采纳关联性标准,例如,德国《联邦数据保护法》与欧盟《一般数据保护条例》。与我国不同的是,域外立法例均未从反面说明“不包括匿名化处理后的信息”,说明前述域外立法例已采纳关联性标准。若我国也采纳关联性标准会使个人信息的保护范围过宽,不利于个人数据的流通利用。我国应采纳“识别性”标准,并将之贯彻在侵犯公民个人信息罪的适用流程中。

其次,《个保法》关于个人信息定义不能与《民法典》的设计相左。《民法典》将“识别性”作为划定个人信息范围的核心标准,有观点认为《民法典》与《个保法》分别采用的是识别性标准和关联性标准,但两种标准所界定个人信息的范围基本相同。〔19〕这一论断值得商榷,前述两种标准得出的结论并不相同。例如,在“朱某诉百度公司案”中,朱某利用百度搜索引擎检索关键词的相关记录能否理解为个人信息?如果遵守“关联性”标准,朱某的网络检索纪录应是个人信息,但法院指出,在线活动轨迹信息若不能识别或定位特定自然人的身份,就不能理解为个人信息。〔20〕可见,法院采纳的是识别性标准。本文认为,我国《个保法》与《民法典》均是在坚守识别性标准。两法之所以对个人信息的定义方式存在差异,是因为《民法典》生效在前而《个保法》颁行在后,立法者在制定后者时为了节约立法资源,故而采取抽象简约的定义模型。若采用“关联性”标准可能会明显扩充个人信息的范围,继而导致侵犯公民个人信息罪的泛化适用。总之,《个保法》的法律位阶低于《民法典》,其对个人信息的界定不能颠覆《民法典》的规定。

最后,《个保法》坚守“识别性”标准可避免侵犯公民个人信息罪的扩张适用。2017 年的《个人信息刑案解释》第 1 条已将个人信息区分为“身份识别信息”和“活动轨迹信息”,但二者均是以“识别性”为核心要件。若认为《个保法》已采关联性标准,则意味着刑法司法解释关于个人信息的“识别性”标准将被废弃,侵犯公民个人信息罪的适用范围将会扩大;若认为《个保法》仍采“识别性”标准,则与其采用相同标准的刑法司法解释仍然有效,可避免侵犯公民个人信息罪的扩张适用。显然后者更具合理性,也符合法秩序统一性原理。在坚守“识别性”标准的基础上还要准确理解识别性,个人信息中的“识别”,是通过特定信息或一组信息“认出”具体的自然人。〔21〕在规范上,个人信息识别包括身份识别和特征识别,前者要求认出信息主体具体是什么身份的人,后者要求辨别信息主体是什么样的人,二者的共同目标均是要知道信息主体是何人。至于个人信息的识别性如何判断,理论上存在“客观说”“主观说”等不同观点。〔22〕本文提倡“任一主体说”,即任何主体针对特定信息或信息集,采取合理且常用的方法即可认出

〔19〕 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 57 页。

〔20〕 参见北京百度网讯科技有限公司与朱某隐私权纠纷案,南京市中级人民法院民事判决书,(2014)宁民终 5028 号。

〔21〕 参见齐爱民:《大数据时代个人信息保护法国际比较研究》,法律出版社 2015 年版,第 136 页。

〔22〕 参见韩旭至:“个人信息概念的法教义学分析——以《网络安全法》第 76 条第 5 款为中心”,《重庆大学学报(社会科学版)》2018 年第 2 期,第 159 页。

特定自然人，那么这一信息便是个人信息，这一标准可以使个人信息的认定相对准确。此外，信息识别包括直接识别和间接识别，前者是通过单一信息即可认出信息主体，后者是需结合多种信息才能识别信息主体。信息处理者的“识别”能力会随着数字技术的发展而增强，对于个人信息识别性的判断需立足具体的技术场景。

（二）个人信息保护法关于个人信息的分类与侵犯公民个人信息罪衔接

欧盟《一般数据保护条例》总体上将个人数据划分为三大种类：①一般个人数据；②敏感个人数据；③私密个人数据。域外的立法例对我国个人信息分类的实践、理论与规范均产生影响：①实践层面，在黄某诉腾讯微信读书案中，法院将个人信息区分为私密信息、不具有私密性的一般个人信息、兼具防御性和期待性的信息，并对三类信息适用不同的裁判规则。〔23〕②理论层面，有学者梳理了个人信息分类的五种观点。〔24〕在刑法领域，有学者将个人信息区隔为一般信息、重要信息、敏感信息。〔25〕③规范层面，在《个保法》颁布之前，国家指南和国家标准已进行个人信息的分类。《信息安全技术公共及商用服务信息系统个人信息保护指南》第3.2条，将个人信息划分为敏感个人信息和一般个人信息。《信息安全技术 个人信息安全规范》第3条区分了敏感个人信息和一般个人信息。《个保法》从法律层面对个人信息进行分类，其第51条第2项要求对个人信息实行分类管理。本文认为，我国《个保法》已将个人信息划分为“私密个人信息、敏感个人信息、一般个人信息”。

其一，私密个人信息可从《个保法》与《民法典》的关系中推演出来。可以发现，我国《民法典》第1034条第3款已明确了个人信息与隐私的关系。本文讨论的私密个人信息就是《民法典》上的“私密信息”，是隐私和个人信息的交叉部分，是以信息呈现的个人隐私，《民法典》第1032条第2款也指出私密信息是隐私的一部分。换言之，私密信息既是个人信息也是隐私。原本私密信息应由《个保法》规定，但因《民法典》制定在前，《个保法》立法者为了节约立法资源就未在规范中重复描述私密信息。但基于《民法典》第1034条第3款后半句可知，当私密信息在《民法典》中没有保护规范时，就适用“有关个人信息保护的规定”，而所谓的“有关个人信息保护的规定”主要指《个保法》。换言之，通过《民法典》的指引，可以得出《个保法》中应包含私密信息这一类型。

其二，敏感个人信息由《个保法》明确规定。《个保法》第28条界定了敏感个人信息的概念，且第二节专门规定了“敏感个人信息的处理规则”。英国学者边沁曾指出，敏感就是自然人感受到某一定量的苦乐的倾向，体现敏感存在程度差异。〔26〕敏感虽是自然人的感受，但不能完全理解为个人的主观体验感，而应从客观上界定对自然人利益影响的程度。对于敏感度的界定，当前研究成果多从形式和实质两个维度来判断，前者以信息与自然人权益的勾连度、多

〔23〕 参见北京互联网法院民事判决书，(2019)京0491民初16142号。

〔24〕 参见邢会强：“大数据交易背景下个人信息财产权的分配与实现机制”，《法学评论》2019年第6期，第99—100页。

〔25〕 参见周光权：“侵犯公民个人信息罪的行为对象”，《清华法学》2021年第3期，第32页。

〔26〕 参见(英)边沁：《道德与立法原理导论》，时殷弘译，商务印书馆2020年版，第99页。

数人的体验度为方向，后者以法益遭受侵害及其危险的程度为标尺。实际上，“敏感”虽来源于自然人的主观感受，但应采用主客观相结合的方法界定。在客观层面，敏感是与自然人核心权益的关联度；在主观层面，敏感与自然人的人格直接勾连，直接影响自然人的主观感受。我国《个保法》在界定敏感个人信息时已采纳这一标准，强调敏感个人信息一旦被非法处理即会对信息主体的人身权益或财产权益造成极其严重的影响。

其三，一般个人信息在《个保法》中通过“定义＋排除两步法”确定。与私密信息、敏感个人信息不同，一般个人信息的判定并非一蹴而就。本文提倡“定义＋排除两步法”：①第一步，通过个人信息的定义判断法，确定相关信息是否为个人信息；②第二步，适用排除法，特定信息若属于个人信息但又不是私密信息和敏感个人信息，则应是一般个人信息。可见，一般个人信息的规范依据是《个保法》关于个人信息的定义，它的范围应通过“排除法”确定。

从法理上看，前述规范分类符合领域理论（Sphärentheorie）的旨趣。〔27〕领域理论强调个人生活领域由内向外呈现出多层“回”字形结构，即依次为隐私领域（Intimsphäre）→私人领域（Privatsphäre）→社会领域（Sozialsphäre）。〔28〕三类信息之间的关系如下图所示（见图 1），前述三大领域依次对应着私密信息→敏感个人信息→一般个人信息。由内向外，法律保护的力度逐渐递减。三大领域、三大信息内部彼此之间的界限不是泾渭分明的边界线，而是表现为过渡带，处于过渡带的个人信息优先适用更高强度的保护方案。

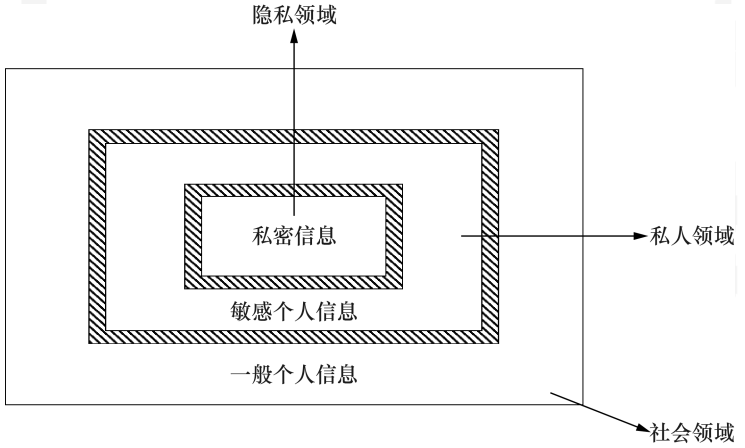

图 1　公民个人信息的领域区分图

在立法者创设侵犯公民个人信息罪时尚无《民法典》和《个保法》，所以该罪的规范未体现个人信息分类分级保护的理念。之后，《个人信息刑案解释》为回应司法实践的分类需求，在解释侵犯公民个人信息罪入罪标准（情节严重）时，为三类个人信息设置不同的入罪标准。本文

〔27〕 参见张千帆：《西方宪政体系（下册·欧洲宪法）》，中国政法大学出版社 2001 年版，第 372 页。

〔28〕 参见童云峰：“侵犯读者信息行为的刑法分层规制模式”，《图书馆论坛》2022 年第 5 期，第 61 页。

认为,《个人信息刑案解释》中的三类信息应与《个保法》的分类相衔接。

首先,第5条第3项的规定是对私密信息的阐述。私密信息需要刑法采用更强的保护方式,所以侵害行为的入罪标准理应更低。第5条第3项只具体规定了"行踪轨迹信息、通信内容、征信信息和财产信息",前述四则信息都应理解为自然人的私密信息。按照规范表达的惯例,列举条款一般会以"等"字收尾,以应对社会发展中出现的新情况。吊诡的是,该项规定却是封闭列举。本文认为,司法机关在制定司法解释时,数字技术还没有如今发达,人们对私密信息的理解与认识较为局限,所以制定者只能有限列举。对此,可通过补正解释将"等"镶嵌在第3项中,如此不仅能与第4、5项保持一致,亦可全面涵摄所有类型的私密信息。

其次,第5条第4项的规定是对敏感个人信息的陈叙。该项通过"列举+兜底概括"的方法,旨在阐释对该类信息的非法处理会侵害信息主体的人身安全或财产安全。该项规定与《个保法》第28条对敏感个人信息内涵的界定基本吻合,可以《个人信息刑案解释》第5条第4项中的"等"字为界分点。"等"之前关涉具体信息类型的列举,是对典型敏感个人信息的描绘;"等"之后实质是对敏感个人信息的抽象定义。《个人信息刑案解释》早于《个保法》,其对典型敏感个人信息的列举可能并不准确,这就决定了对列举的信息类型不能进行形式理解。换言之,不应认为只要能归入列举的类型即是敏感个人信息,应以敏感度作为判断标准。例如,有的通信记录和交易信息具有明显的私密性,则应归入第3项的私密信息之中;再如,有的住宿信息只能体现信息主体所入住的酒店,则至多只能解释为敏感个人信息;但有的住宿信息能反映自然人与同性或异性在一起的开房记录,则代表着自然人的隐私权,应归入第3项的私密信息。

最后,第5条第5项的规定是对一般个人信息的表达。前文已述,一般个人信息是通过"定义+排除两步法"确定,第5条第5项规定是在表达这一方法。所谓第3项(私密信息)、第4项(敏感个人信息)规定以外的公民个人信息,应是一般个人信息。私密信息关涉隐私权,原则上不能处理否则可能会违背公序良俗原则;敏感个人信息与自然人的人格权益更为紧密;一般个人信息与自然人人格权益的关联相对松散。因此,法律对三类信息背后的个人权益的保护力度逐渐递减,对其中的社会价值的关注依次递增。因此,刑法司法解释对侵犯三类信息行为设置的入罪标准依次为50条、500条和5000条。如上将《个保法》的分类表达嵌入侵犯公民个人信息罪的入罪标准,会产生诸多积极价值:①能够坚守法秩序统一性原理。具言之,能够将《民法典》《个保法》关于个人信息分类的民事责任、行政责任与《刑法》中的刑事责任有效衔接。②推动信息保护与利用的平衡。私密信息原则上不能利用,敏感个人信息重保护而轻利用,一般个人信息重利用而轻保护,通过上述解释能够将保护与利用的平衡理念贯彻至刑法层面。③有利于贯彻罪责刑相适应原则。侵犯三类信息的违法性及有责性存在显著差异,如果适用相同的入罪标准则无法体现责任刑,上述理解有助于实现罪刑均衡和刑事归责的精细化。

(三)个人信息保护法关于个人信息的处理与侵犯公民个人信息罪衔接

《民法典》第111条和第1035条第2款均在阐述处理的含义,前述规定被《个保法》第4条第2款承继并续造。但后生效的《个保法》多列举了一个"删除",是为了体现对被遗忘权的保

护。侵犯公民个人信息犯罪始创于《刑法修正案(七)》,当时创设的行为类型已是“窃取”“非法获取”“出售”“提供”。《刑法修正案(九)》只是将两罪合并并进行一定程度的修改,但并未扩充行为方式。如此立法与时代背景密不可分,前数字时代,立法者对个人信息的利用价值缺乏充分认识,只关注其中的个人权益,所设置的上述四种行为方式均是为了防止个人信息被非法转移。换言之,《个保法》上的“处理”与侵犯公民个人信息罪中“侵犯行为”的表述存在差异。为了实现法法衔接,应将二者贯通。

首先,《个保法》上“收集”与侵犯公民个人信息罪中的“窃取”“非法获取”衔接。收集环节是个人信息离开信息主体的第一个阶段,除符合合理处理的情形外,大多收集行为都需要经过信息主体的同意才有合法性。我国《刑法》第 253 条之一第 3 款规定了“窃取”或“以其他方式非法获取”,这一表述是非法收集行为在《刑法》上的表达。非法收集的表现形式呈现多种样貌,除“窃取”外,还包括骗取、购买、交换、抢取等类型。换言之,在《个保法》上被评价为非法收集的行为,需承担民事责任或行政责任。情节严重时,可能会被评价为“窃取”或“以其他方式非法获取”,继而构成侵犯公民个人信息罪。

其次,《个保法》上“传输、提供、公开”与侵犯公民个人信息罪中的“出售”“提供”衔接。“提供”的本质是个人信息在不同主体之间流转,包括有偿提供和无偿提供。有偿提供就是“出售”,出售实乃提供的子概念。应对侵犯公民个人信息罪中的“提供”作扩大解释,使之等价于流转,继而足以涵摄实践中可能出现的各种新型流转行为。本文认为,《个保法》上的“传输、提供、公开”均可解释为《刑法》上的“出售”“提供”,是因为传输、提供、公开均发生了个人信息的流转。其中传输、提供可能发生在“一对一”的提供场景中,而“公开”的本质是信息持有者向不特定对象提供,如果发生在有偿的情形中便是“出售”,出售是一种有偿提供行为,赠送则是无偿提供行为。因此,传输、公开等关涉个人信息转移的行为,皆可被侵犯公民个人信息罪中的“提供”涵摄。

最后,使用、删除等《个保法》规定的其余处理行为无法被侵犯公民个人信息罪涵摄。面对刑法的打击盲区,实践中不乏强行适用侵犯公民个人信息罪的情形;理论上大多主张完善侵犯公民个人信息罪或增设新的罪名。对此问题本文认为可能有两种方案:①司法上,适用其他罪名间接规制非法处理行为。其一,通过其他罪名规制部分非法处理行为。例如,对于非法删除个人信息行为,可以适用破坏计算机信息系统罪。以柴某某破坏计算机信息系统罪案为例,被告人柴某某与被害人是同学,高考结束后二人填报志愿时均报考了同一所高校的同一个专业,被告人因自己的成绩不如被害人,担心自己不能被录取,便利用之前记下的被害人的相关信息登录高考志愿填报系统,删除被害人所填报的志愿信息,使被害人未能被该高校录取。法院裁决,被告人构成破坏计算机信息系统罪。〔29〕 其二,将非法处理行为视为其他罪名的量刑情节。以滥用个人信息实施电信诈骗为例,单纯的滥用行为无法构成诈骗罪,但滥用个人信息是实施电信诈骗的手段行为,基于其对个人信息法益的侵害,可在诈骗罪的量刑阶段酌重考量。②立法上,可将侵犯公民个人信息罪修正为“非法处理公民个人信息罪”。毋庸置疑,教义学可

〔29〕 参见河北省大名县人民法院刑事判决书,(2020)冀 0425 刑初 231 号。

以解决的问题勿需求助立法论。〔30〕然而，直接适用侵犯公民个人信息罪规制存储、使用、加工和删除等行为会违背罪刑法定原则，适用其他罪名可能无法精准保护法益。对此，最为彻底的方案是修正侵犯公民个人信息罪。为推动法律衔接，未来刑事立法应将侵犯公民个人信息罪修正为“非法处理公民个人信息罪”。其中，非法处理的内涵应与《个保法》第4条第2款作同义理解。

三、个人信息保护法与侵犯公民个人信息行为出罪的衔接机制

在出罪衔接机制方面，主要探讨《个保法》中的正当化事由与刑法违法阻却事由如何衔接。需要思考的是，《个保法》上确立的正当化事由在刑法教义学上如何定性？它们如何运作才能为侵犯个人信息行为出罪？刑法教义学上的违法阻却事由，可划分为“基于法益阙如阻却违法的事由”和“基于法益衡量阻却违法的事由”。〔31〕基于此，本文将《个保法》上七项正当化事由分别归入相应类别，继而阐述它们阻却违法性的运作流程。

（一）个人信息保护法上正当化事由与刑法中法益阙如原理衔接

刑法理论一般将被害人承诺、推定的承诺、自损行为等归为因法益阙如而阻却违法性的事由，其中被害人同意是典型的法益不存在情形。〔32〕本文认为，《个保法》第13条第1项的同意规则进入刑法领域，应被理解为“承诺”，是因法益阙如而阻却违法性的事由。

一方面，《个保法》上的同意应与刑法教义学上的承诺衔接。愿者不受害（Volenti non fit injuria）是一句古老的罗马谚语，其在现代法律体系中仍扮演着重要角色。〔33〕英美法系的“知情同意”起源并兴盛于美国的卫生健康领域，强调医生未经病人同意实施手术是一种伤害行为。〔34〕大陆法系的“知情同意”集中表现为刑法上的被害人承诺理论，强调被害人在犯罪过程中也需要承担一定的法律责任。〔35〕在被害人同意理论内部，存在是否区分同意和承诺的争论：①不区分说，强调既然否定犯罪成立的根据是一样的（被害人同意），那么对成立条件或有关故意和错误的不同处理就并不妥当，也就没有必要区分；〔36〕②区分说，一般情况下同意能够阻却构成要件该当性，经同意的行为因法益阙如而无法益侵害性；对于身体、名誉等本身就有价值的法益，即使被害人同意也只能阻却违法性，此时同意就是承诺。〔37〕本文当前认

〔30〕 参见车浩：“立法论与解释论的顺位之争——以收买被拐卖的妇女罪为例”，《现代法学》2023年第2期，第175页。

〔31〕 参见张明楷：《刑法学》（第6版），法律出版社2021年版，第254页。

〔32〕 参见（日）松宫孝明：《刑法总论讲义》，钱叶六译，中国人民大学出版社2013年版，第77页。

〔33〕 参见（美）乔尔·范伯格：《刑法的道德界限（第一卷）》，方泉译，商务印书馆2013年版，第126页。

〔34〕 参见中国信息通信研究院互联网法律研究中心编著：《个人信息保护立法研究》，中国法制出版社2021年版，第175页。

〔35〕 参见申柳华：《德国刑法被害人信条学研究》，中国人民公安大学出版社2011年版，第278页。

〔36〕 参见（日）山口厚：《刑法总论》，付立庆译，中国人民大学出版社2018年版，第162页。

〔37〕 松原芳博『刑法総論』（日本評論社，2017年）123—125頁参照。

为,没有必要区分同意与承诺,构成要件符合性和违法性的判断不应决然分裂,只不过前者是从正面积极判断行为是否契合构成要件,而后者是从反面判断哪些行为不具有违法性。没有必要在构成要件阶段讨论被害人同意与承诺,应统一在违法性阶层讨论被害人承诺。至于同意为什么能够阻却违法性?对于这一问题理论上存在四种答案:①目的说,因符合特定目的且手段正当的承诺可阻却违法性;②社会相当性说,依承诺所为之行为,乃属于社会相当性范围内之行为;③保护法益阙如说,被害人承诺是对特定法益的抛弃,因要保护的法益已不存在而阻却违法;④法益衡量说,因被害人自我决定的价值优于所放弃的法益而阻却违法。〔38〕本文认为,法益阙如说更具有合理性,得到同意的个人信息处理行为,因为信息主体放弃法律保护而使法益不存在,继而阻却违法性。

另一方面,针对私密信息、敏感个人信息、一般个人信息,同意阻却违法性的流程存在差异。侵犯公民个人信息罪保护的法益总体上可以概括为人格权,但针对不同类型个人信息,保护法益的具体类型也有差异。私密信息、敏感个人信息和一般个人信息背后对应的法益分别是,隐私权、人格尊严和人格自由。

首先,经过同意的私密信息也只能有限处理。私密信息由于关涉自然人的隐私权,原则上不允许处理,只有符合特殊要件时才能有限处理。①必须有信息主体的"明确"同意。按照《民法典》第 1033 条规定,除法律另有规定或权利人明确同意外,任何组织或个人不得处理他人私密信息。即信息主体同意的内容必须明确和具体,信息处理者在处理私密信息时,应严格遵守同意的内容和范围要求。例如,信息主体要求信息处理者对私密信息进行保密处理,信息处理者则不得公开私密信息;信息主体要求在指定日期前删除,信息处理者必须删除。②符合公序良俗原则。即使经过信息主体同意也只有在不违反公序良俗原则的情况下,信息处理者才能合理处理。例如,信息主体虽然同意处理者公开处理其在私密空间中的裸照、裸体视频等信息内容,信息处理者也不能公开处理。换言之,信息主体明确同意后,信息处理者可以获得处理的合法依据,但是也不能侵犯公共法益或善良风俗。

其次,经过同意的敏感个人信息可以适当处理。对于敏感个人信息,经过信息主体同意后,信息处理者可以合法处理,但信息处理者的处理也要取得个人的单独同意。《个保法》第 29 条规定,处理敏感个人信息应当取得个人的单独同意,法律、行政法规规定处理敏感个人信息应当取得书面同意的,从其规定。"单独同意"虽相较于"明确同意"要求稍低,但也必须是"一对一同意"且内容相对具体。在非单独同意的情况下,处理敏感个人信息行为不能阻却违法性。

最后,经过同意的一般个人信息可以合法处理。一般个人信息背后的法益是一般人格权(人格自由),一般个人信息是自然人与社会交往的媒介,法律鼓励合理利用以促进信息社会的构建。相对于前两类个人信息,法律对一般个人信息同意处理的要求较低。《民法典》第 1035 条要求处理自然人个人信息,征得该自然人或者其监护人"同意"即可。《个保法》第 14 条规定,"基于个人同意处理个人信息的,该同意应当由个人在充分知情的前提下自愿、明确作出。

〔38〕 参见陈子平:《刑法总论》,中国人民大学出版社 2009 年版,第 200 页。

法律、行政法规规定处理个人信息应当取得个人单独同意或者书面同意的，从其规定”。后一句是对同意处理敏感个人信息的要求，前一句则是对同意处理一般个人信息的要求。可见，对于一般个人信息的处理，只要信息主体自愿明确做出即可，不要求单独做出，对内容的明确性程度也没有敏感个人信息要求高。

（二）个人信息保护法上正当化事由与刑法中法益衡量原理衔接

本文认为，我国《个保法》第13条第2至7项规定的正当化事由进入刑法后，均为基于法益衡量原理而阻却违法性。

1.个人信息保护法上正当化事由与刑法上的“正当业务行为”衔接

《个保法》第13条第2项规定，“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，个人信息处理者方可处理个人信息”。本文将前半句简称为“基于合同当事人事由”，后半句简称为“基于实施人力资源管理需要事由”，将二者统合简称为“合同与人力资源事由”。同时，《个保法》第13条第5项前半句规定，若为公共利益实施新闻报道，在合理的范围内处理个人信息，无需信息主体同意即具有正当性。对于这一事由，本文将之概括为“新闻报道事由”。前述事由能够阻却违法性的本质是法益衡量的结果，可归为刑法上的“正当业务行为”。正当业务行为是指，刑法虽没有直接规定，但在社会生活中被认为是正当的业务上的行为，不应成为刑法上的犯罪行为。〔39〕

其一，“合同与人力资源事由”本质上是“正当业务行为”。一方面，法益衡量型目的说可以说明“合同与人力资源事由”阻却违法性的本质。目的说认为，若行为人为了实现国家认可的共同生活的目的而采取适当的手段，则具有正当性。法益衡量型目的说是目的说的重要内容，强调对目的的客观价值与所产生的法益损害之间进行比较衡量（本质上属于法益衡量）。例如，为了实现劳动者的权利之目的，何种程度的争议行为是正当的？对此，应将劳动者所获得的权益与被害法益进行比较衡量。〔40〕只要以提高劳动者地位为主要目的，就具有正当性。〔41〕这一示例刚好能解释说明，“合同与人力资源事由”可以阻却违法性是法益衡量的结果，即为了实现签订、履行合同目的与实现人力资源管理目的所取得的利益，明显大于自然人在此过程中受损害的个人信息法益。另一方面，“正当业务行为”可以涵摄“合同与人力资源事由”。为完成订立、履行合同事项，双方当事人都需要提供或处理当事人的个人信息，这是完成合同目的的必经程序。正当业务行为没有固定的种类，职业性的体育比赛、律师辩护行为等是典型代表，它强调业务是社会生活中反复实施的行为，且行为是为了维持或保持正当利益。对于私密信息，原则上不能合理处理，只有在与合同事项、人力资源事项密切相关时，数据处理者在遵循公序良俗原则的基础上可进行内部处理，但不得公开处理；针对敏感个人信息，只有在符合实现合同事项、人力资源事项的特定目的且有充分的必要性，并采取严格保护措施的情形

〔39〕 参见黄荣坚：《基础刑法学（上）》，元照出版有限公司2012年版，第225页。

〔40〕 参见张明楷，见前注〔13〕，第117页。

〔41〕 参见（日）高桥则夫：《刑法总论》，李世阳译，中国政法大学出版社2020年版，第235页。

下,处理者方可处理;对于一般个人信息,作为合同相对人和人力资源管理者的信息处理者可以正当处理。

其二,为公共利益的“新闻报道事由”本质上也是“正当业务行为”。实施新闻报道而合理处理个人信息,必须是为了实现公共利益目的。首先,为公共利益实施新闻报道行为,也不能处理私密信息。这是因为私密信息反映着隐私权,而新闻报道又是一种广而告之行为,不能基于公共利益对个人私密信息进行新闻报道,否则会违背公序良俗原则。新闻记者的部分报道行为可能是为了公共利益,即使如此也不能在个人信息处理过程中损害他人隐私权。例如,在日本的外务省泄密案中,新闻记者要求外务省公务员告知其有关“返还”冲绳的秘密电文,否则就泄露二人存在不正当男女关系的隐私信息。日本最高裁判所在判决中指出,行为人的手段不具有正当性,基于法益衡量原理而否认正当化。〔42〕 其次,为公共利益实施新闻报道行为,一般情况下也不能处理敏感个人信息。《个保法》第 28、29 条为敏感个人信息的处理设置了严格的条件,对基于合理处理事由而处理敏感个人信息的情形应适用更严格的条件。敏感个人信息原则上只有获得信息主体的同意与授权才能处理,适用合理处理必须要经过利益衡量测试,即合理处理所获取的利益必须要明显大于因信息处理而被损害的法益。如此才能在一定范围内实施新闻报道,且需采取匿名化、去识别化和事后删除等相对严格的保护措施。最后,一般个人信息具有明显的社会利用价值,可基于公共利益目的实施采访报道而处理。如果实施新闻报道而处理一般个人信息是为了实现公共利益,自然人的个人利益应适当让渡于公共利益,法益衡量的结论是可以进行新闻报道,但亦需采用适当的保护措施。

2.个人信息保护法上正当化事由与刑法上的“紧急避险”衔接

《个保法》第 13 条第 4 项规定,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,信息处理者可以合理处理个人信息。这一事由进入刑法后,应理解为我国《刑法》第 21 条规定的紧急避险。紧急避险制度是功利主义刑法观在刑事立法上的彰显,功利主义刑法观以“成本—收益分析”(cost-benefit analysis)作为分析的逻辑和思路,如果适用刑罚能够增进社会福祉,则刑罚具有正当性,否则刑罚不具有正当性。〔43〕 紧急避险制度要求司法者应在功利主义刑法观的指导下进行法益衡量,即法律所要保护的法益必须明显大于被牺牲的法益。

应当明确,《个保法》第 13 条第 4 项的规定符合紧急避险的基本要求。首先,“突发公共卫生事件”和“紧急情况”均是对紧急避险中“正在发生的危险”的描述。其次,为了在公共卫生事件或紧急情况下保护自然人的生命健康法益、财产法益,不得已处理公民个人信息,即被迫损害自然人的个人信息权益。再次,信息处理者作为避险人的避险意识是为了应对突发公共卫生事件或紧急情况等风险。最后,被牺牲的个人信息权益明显次于需要保护的生命健康法益、财产安全法益等。基于紧急避险处理公民个人信息,只能在风险正在进行中才能处理,事前避

〔42〕 参见(日)前田雅英:《刑法总论讲义》,曾文科译,北京大学出版社 2017 年版,第 215 页。

〔43〕 参见(英)威廉姆·威尔逊:《刑法理论的核心问题》,谢望原、罗灿、王波译,中国人民大学出版社 2014 年版,第 51 页。

险或事后避险都不能阻却违法性。避险行为也不应超过限度，避免给信息主体造成不必要的损失。因紧急避险而阻却违法性的情况，个人信息处理者应提供证据证明其存在紧急避险的事由。紧急避险是包容人性自私而设，对其有种种设限，不可轻易主张。〔44〕

对于私密信息，信息处理者可基于紧急避险而进行内部处理，不得对外公开。例如，在疫情防控期间，为了对感染病例进行溯源追踪以遏制疫情蔓延，可以调查相关感染人员的开房记录，了解与其相关的密切接触者，继而精准采取隔离防控措施。但是，不能将感染者的开房记录对外公开。对于敏感个人信息，信息处理者可以基于紧急避险而合理处理，但应对敏感个人信息采取适当的保护措施，在风险解除后应及时删除敏感个人信息。对于一般个人信息，信息处理者可以基于紧急避险而合理处理，法律对此项合理处理的容忍度较高，只要不超过合理限度均可合理处理。

3.个人信息保护法上正当化事由与刑法上的“法令行为”衔接

《个保法》第13条第3项规定，信息处理者为履行法定职责或者法定义务所必需，可以合理处理个人信息；第5项后半句规定，信息处理者为公共利益实施舆论监督行为，可以合理处理个人信息。本文认为，该两项正当化事由在刑法中可界定为法令行为。所谓法令行为，是在形式上具有法益侵害性，但实质上是法律、命令和法规允许的行使权利或承担义务的行为，本质上是基于法益衡量原理而阻却违法性。〔45〕法令行为主要包含四种类型：①法律有意明示了合法性条件的行为，即某类行为本来具有犯罪性，但法律又特别规定符合一定条件时阻却违法，例如，对有堕胎罪的国家而言，优生法会允许一定条件下的堕胎行为；②职务行为，例如，执法者对死刑犯执行死刑；③权利（义务）行为，例如，公民将正在行凶者扭送至公安机关；④基于政策的行为，例如，购买彩票行为。〔46〕

一方面，履行法定职责或者法定义务而合理处理个人信息行为，可归为职务行为。因为有法律的明确背书，使处理个人信息行为阻却违法性。例如，网络警察为了维护网络安全，可以适度处理自然人的微信聊天记录、网页浏览记录等，约谈发表违法言论信息的行为人。对于私密信息，信息处理者可因履行法定职责或者法定义务而合理处理，但仅限于信息处理者内部相关人员知悉，不得对外公开。同时处理必须与公务活动密切相关，不得将私密信息另作他用。例如，网络警察不得将所掌握的相关自然人的开房记录信息，泄露给他人，不得收受贿赂提供代查私密信息的“服务”。对于敏感个人信息，信息处理者可因履行法定职责或者法定义务而合理处理，但需遵循《个保法》第28条第2款的要求，采取严格保护措施。对于一般个人信息，信息处理者不仅可因履行法定职责或者法定义务而合理处理，且处理的程序和要求均比私密信息和敏感个人信息宽松。

另一方面，信息处理者为公共利益实施舆论监督行为，可归为权利（义务）行为。该项事由的前设条件是“为公共利益”，以公共利益目的为底色的各类合理处理事由已被域外个人信息

〔44〕 参见林东茂：《刑法总则》，一品文化出版社2021年版，第159页。

〔45〕 小林憲太郎『刑法総論』（新世社，2020年）89頁参照。

〔46〕 参见（日）大谷实：《刑法总论》，黎宏译，中国人民大学出版社2008年版，第228—229页。

保护立法所采用。我国《个保法》第 13 条第 5 项内容均是以保护公共利益为目的，只不过新闻报道应被评价为正当业务行为，而舆论监督应被评价为法令行为下的权利（义务）行为。在舆论监督场景下，监督主体是公民，而被监督主体是国家机关及其工作人员。例如，企业、单位或个人为监督某国家机关工作人员，向纪检监察机关提供其与贪污贿赂犯罪有关的个人信息。此时举报者提供个人信息实乃检举揭发行为，因《中华人民共和国宪法》第 41 条赋予公民的申诉、控告或者检举的权利而阻却违法性。可见，为公共利益实施舆论监督是公民的一项宪法权利。基于此而合理处理个人信息，可因权利（义务）行为而阻却违法性。进入数字时代，普通网络用户已经成为舆论监督的主体，基于公共利益的舆论监督阻却违法性应在具体场景下贯彻。对于私密信息，基于公共利益目的的舆论监督可以合理处理，但原则上只应向纪检监察机关提供。例如，对于某已婚官员与下属的开房记录，可以向纪检监察机关提供，但不宜在网络上大肆宣传。除非在举报无果的情况下，才可借助网络舆论予以监督。对于敏感个人信息，在符合严格条件的情况下可基于公共利益目的的舆论监督而合理处理，如将某官员违法的收入（银行转账记录）向纪检监察机关提供。至于一般个人信息，在符合基本条件时，可基于公共利益目的的舆论监督而合理处理。

4. 已公开个人信息合理处理是刑法上法益衡量原理下的独立事由

对于已经合法程序公开的个人信息，社会公众能否自由处理？在《个保法》颁行之前理论与实践中曾有过争论。《个保法》第 13 条第 6 项和第 27 条明确规定，处理已合法公开的个人信息是正当化事由。《个保法》上的已合法公开的个人信息包括两大种类：①主动公开型，信息主体自愿主动公开自己的个人信息，使社会公众可以知悉其个人信息；②被动公开型，即虽非经信息主体主动公开，但按照法律规定应公开的个人信息。例如，因政府信息公开或法院司法公开而公开的个人信息。处理非经合法途径公开的个人信息，不能阻却违法性。

一方面，“处理已合法公开个人信息”是数字时代法益衡量原理下的新型违法阻却事由。有不少学者认为，处理主动公开型的个人信息和被动公开型的个人信息，阻却违法性的法理事由存在差异。〔47〕本文则认为，处理两类已公开个人信息皆因法益衡量原理而阻却违法性。

其一，优越利益胜出论可以从法理上解释合理处理已公开个人信息阻却违法性的因由。无论个人信息是主动公开还是被动公开，只要被合法公开，就表明个人信息的保密性价值即消失，还表明个人信息已进入社会流通利用领域，具备了更大的社会利用价值。此时个人信息之上会缠附信息主体个人法益之外的公众知情权和公共利益等法益。与未公开的个人信息相比，已合法公开的个人信息之上的公共法益量增加而个人法益量下降，其上的社会利用法益已超过个人法益，此时法律更加倾向保护已合法公开个人信息之上的社会利用法益。因此，立法者在《个保法》第 13 条第 6 项和第 27 条中将已合法公开的个人信息设置为合理处理的对象。

其二，刑事司法实践对处理已合法公开个人信息作为违法阻却事由，已由拒绝走向接纳。

〔47〕 参见刘双阳：“‘合理处理’与侵犯公民个人信息罪的出罪机制”，《华东政法大学学报》2021 年第 6 期，第 64—68 页。

早些年，对未经信息主体同意而处理已公开个人信息的行为，大多法院判定构成犯罪。〔48〕在《民法典》《个保法》相继颁行后，对于类似案件在进入审判阶段之前，就已被检察院不起诉或被公安机关作撤案处理。〔49〕主动公开型个人信息上的自然人人格法益仍然存在，只是因保密性不在而使个人法益量降低。因此，试图以法益阙如原理来解释合理处理主动公开型个人信息的违法阻却性并不科学。处理两类已合法公开个人信息之所以能够出罪，均是法益衡量的结果。但是，传统法益衡量原理下的法令行为、正当业务行为、行政许可和义务冲突等事由，均无法解释处理已公开个人信息的违法阻却性。况且，处理已公开个人信息能够阻却违法，是立法者为了呼应实践需求和促进数字经济发展，才创设的新型违法阻却事由。

另一方面，处理已合法公开个人信息阻却刑事违法性应符合限度要件。应以何种标准作为判断处理已合法公开个人信息阻却刑事违法性的标尺，存在不同学说：①公开目的考察说。若个人信息合法公开的目的被改变，则处理行为可能会构成犯罪。例如，行为人在网络上广泛收集已合法公开的个人信息，继而将之打包或加工，然后提供给电信诈骗组织，导致信息主体被电信诈骗而遭受重大损失。此时，个人信息原本合法公开的目的被改变，此种处理行为需要刑法规制。〔50〕②客观开放程度标准说。以个人信息的开放程度为方向，勘定相关处理是否具有违法性。对于已完全开放的个人信息，无需刑法保护。对于有限开放的个人信息，擅自处理行为具有违法性。对于被非法公开的个人信息，如果行为人误认为是合法公开的个人信息而处理，则属于过失行为，不构成侵犯公民个人信息罪；如果行为人明知个人信息处于非法公开的状态仍然处理，则不应阻却违法性。〔51〕本文认为，前述学说均有一定的局限性。

其一，公开目的考察说存在一定的主观恣意性。对于主动公开型个人信息的公开目的存在于信息主体公开时的脑海中，随着时间的推移自然人可能会更改公开的目的，导致公开目的具有易变性；对于被动公开型个人信息，因为法律的强制性规定而被动公开，这类信息的公开目的的判断相对客观。然而，对于被动公开型个人信息的公开目的，需在要求公开的法律中探知，最终的结果可能要探求立法原意，而立法原意并不客观且会被时代发展所更替。

其二，客观开放程度标准说在我国欠缺规范依据。如前所述，客观开放程度标准说以数据的开放程度为判断方向。然而，我国没有专门的数据开放法律，我国既有法律也没有对数据开放程度予以明确划分。同时，数据开放不等于信息公开，前者表明权利人放弃对数据的垄断权，允许社会公众抓取和使用底层数据；后者只是表明信息内容可以被社会公众知悉，但并不代表信息的底层数据可以被任意抓取。〔52〕因此，我们既不能照搬与我国规范不符的域外标准，亦不能用数据开放程度标准来解释信息公开的问题。本文提倡个人信息分类场景下的法

〔48〕 参见田某侵犯公民个人信息罪案，徐州市铜山区人民法院刑事判决书，(2018)苏0312刑初85号。

〔49〕 参见卢志坚、白翼轩、田竞："出卖公开的企业信息谋利：检察机关认定行为人不构成犯罪"，载《检察日报》2021年1月20日，第1版。

〔50〕 参见周光权，见前注〔25〕，第39页。

〔51〕 参见王华伟："已公开个人信息的刑法保护"，《法学研究》2022年第2期，第197—206页。

〔52〕 参见童云峰："大数据时代网络爬虫行为刑法规制限度研究"，《大连理工大学学报(社会科学版)》2022年第2期，第93页。

律标准说,即不同类型个人信息存在不同情况。

第一,对于私密信息不允许公开。私密信息背后的法益是自然人的隐私权,自然人若自愿主动公开虽可因同意而阻却违法,但私密信息的公开会违背公序良俗原则故仍存在违法性;若私密信息被非法公开,不仅侵犯自然人的隐私权,也会违背公序良俗原则,具有双重法益侵害性。换言之,对于私密信息无论主动公开抑或被动公开,均可能存在违法性。既然私密信息的公开状态已是非法,那么对已公开私密信息的各种处理行为便难以阻却违法性。

第二,对于敏感个人信息可以有限度地公开与处理。《个保法》第 27 条设置了处理已合法公开个人信息的禁止性规定;第 28 条规定了敏感个人信息的含义。对该两条进行对比分析可知,前条中的"对个人权益有重大影响"和后条的"容易导致自然人权益受到危害",应作相同解释。已公开个人信息与敏感个人信息的耦合体是已公开的敏感个人信息,处理该种信息会对自然人的权益产生重大影响,应取得自然人的单独同意。与私密信息相比,敏感个人信息可以主动公开亦可被动公开;与一般个人信息相比,对于已公开的敏感个人信息需采取更严格的保护措施。同时,对于已公开敏感个人信息只有获得自然人的单独同意才能处理,未经同意的处理行为不能排除违法性。

第三,对于一般个人信息的公开与合理处理相对宽松。对于已合法公开的一般个人信息,原则上均可合理处理,按照《个保法》第 27 条规定只有两个例外情形,分别是"自然人明确拒绝"和"对自然人个人权益有重大影响"。"自然人明确拒绝"是指,信息主体对他人即将、正在或嗣后处理其已合法公开个人信息的行为表示反对。可以处理行为的发生时间为界分点,将"自然人明确拒绝"划分为事前拒绝、事中拒绝和事后拒绝。①事前拒绝,即自然人在他人处理其已合法公开个人信息之前,就已借助多元方式明确表达对他人处理行为的反对。对此,信息处理者的处理行为将无法阻却违法性;但若确有证据证明信息处理者并不知情,则能阻却故意,继而无法构成作为故意犯罪的侵犯公民个人信息罪。②事中拒绝,信息处理正在进行的过程中,信息处理者虽未征求信息主体的同意,但信息主体向信息处理者明确表示反对,此时信息处理者应立即停止正在进行的处理行为,并补偿对信息主体可能造成的损失,否则无法阻却违法性。③事后拒绝,信息处理者在完成信息处理行为后,信息主体才向其表达反对的意见。对已处理完成的行为,不因事后拒绝而具有违法性,否则会严重损害信息处理者合理处理信息的积极性,不利于数据的有效流通和利用。换言之,事后拒绝没有追溯效力。"对个人权益有重大影响"是指,对已合法公开个人信息的处理,将会对自然人的生命健康和重大财产等核心法益产生损害或带来危险。法律为了规避这种风险,明确要求此类处理行为需获得自然人的同意。

四、结 语

实现个人信息保护与利用的平衡,是《个保法》和侵犯公民个人信息罪的共同目标。立足当下,只有将《个保法》与侵犯公民个人信息罪有效结合,才能组成相对完整的个人信息保护领域法。在整体法秩序视野下,有效衔接《个保法》与《刑法》,才能准确回应个人信息领域的法律

需求和精准解决个案难题。在入罪衔接层面，应将个人信息的范围、类型与处理等要件与侵犯公民个人信息罪无缝衔接。在出罪衔接层面，《个保法》所确立的法定正当化事由，进入刑法后可因法益阙如或法益衡量原理而阻却违法性。展望未来，可以考虑将侵犯公民个人信息罪修正为“非法处理公民个人信息罪”，扩容后的罪名可以充分涵摄《个保法》所列举的处理行为。可以将未来实践中可能出现的新的正当化事由归入《个保法》第 13 条第 7 项的兜底条款，并解释为刑法上的超法规的违法阻却事由。面对新兴的数字法律，刑法应保持适度开放以实现入罪与出罪的与时俱进。

Abstract: The Personal Information Protection Law is a cutting-edge law in the digital age. It has the characteristics of pre-emptive law, incomplete field law, and no real subsidiary criminal law. There is a time lag with the provisions of the criminal law on the crime of infringing on citizens' personal information. In order to effectively bridge the gap between norms, it is necessary to embed the Personal Information Protection Law into the application process of the crime of infringement of citizens' personal information. In terms of the criminalization linkage mechanism, the scope of personal information in the two laws should be understood uniformly to avoid the expansion of the criminal circle; the classification and processing settings of personal information in the pre-position law should be used to explain the constitutive elements of the crime of infringement of citizens' personal information, direction to achieve balance between crimes and punishments and legal coherence. In terms of the connection mechanism between crimes, “consent” in the Personal Information Protection Law prevents criminal violations due to the lack of legal interests, and other legitimate reasons in the Personal Information Protection Law prevent criminal violations due to the principle of weighing legal interests. The corresponding legitimate reasons can be classified into legitimate business behavior, emergency avoidance, and legal behavior in the criminal law doctrine, and the reasonable handling of disclosed personal information should become an independent new illegal obstacle in the digital era. The aforementioned reasons can decriminalize related behaviors in the context of personal information classification.

Key Words: Personal Information Protection Law; Crime of Infringing on the Personal Information of Citizens; Consent; Legal Interest Measurement

(责任编辑:车　浩)