Open Journal of Legal Science 法学, 2026, 14(8), 127-138
Published Online August 2026 in Hans. https://www.hanspub.org/journal/ojls
https://doi.org/10.12677/ojls.2026.148240

Hans汉斯

侵犯公民个人信息罪分层法益构造

——以制度信赖为核心

董树华

武汉科技大学法学与经济学院，湖北 武汉

收稿日期：2026年7月13日；录用日期：2026年7月23日；发布日期：2026年8月24日

摘　要

侵犯公民个人信息罪的保护法益之争长期困于个人法益与超个人法益的二元对立，传统混合法益说未能厘清二者位阶关系。文章认为，该罪法益应厘定为一种“分层构造”：个人信息自决权为一阶基础法益，公共信息安全为二阶派生法益，后者内核为“制度信赖”。一阶法益的正当性源于其作为信息处理合法性制度起点的规范功能与不可替代的出罪检验任务；二阶法益通过“人身附随性”划定边界，虽派生自一阶法益但具备不可还原为个人权利的独立价值。二者并非平行保护对象，而是同一制度信赖在不同层面的差异表达，二阶法益的适用须受启动前提、评价位序与出罪路径三重限制。

关键词

侵犯公民个人信息罪，法益分层构造，制度信赖，个人信息自决权，公共信息安全

Hierarchical Structure of Legal Interests of the Crime of Infringing upon Citizens' Personal Information

—Centered on Institutional Trust

Shuhua Dong

School of Law and Economics, Wuhan University of Science and Technology, Wuhan Hubei

Received: July 13, 2026; accepted: July 23, 2026; published: August 24, 2026

Abstract

The debate over the protected legal interests of the crime of infringing upon citizens' personal

文章引用: 董树华. 侵犯公民个人信息罪分层法益构造[J]. 法学, 2026, 14(8): 127-138.
DOI: 10.12677/ojls.2026.148240

information has long been trapped in the binary opposition between individual legal interests and trans-individual legal interests, and the traditional mixed legal interest theory fails to clarify the hierarchical relationship between them. This article argues that the legal interests of this crime can be constructed in a "hierarchical structure": the right to self-determination over personal information serves as the first-order basic legal interest, and public information security acts as the second-order derivative legal interest, whose core connotation is "institutional trust". The legitimacy of the first-order interest derives from its normative function as the starting point of the legitimacy system for information processing and its irreplaceable role in decriminalization tests. The second-order interest demarcates its boundaries through "personal dependency"; although it is derived from the first-order interest, it possesses independent value that cannot be reduced to individual rights. The two are not parallel objects of protection, but rather differential expressions of the same institutional trust at different levels. The application of the second-order interest is subject to threefold constraints: activation prerequisites, evaluative order, and exoneration pathways.

Keywords

Crime of Infringing upon Citizens' Personal Information, Hierarchical Structure of Legal Interests, Institutional Trust, Right to Self-Determination over Personal Information, Public Information Security

1. 引言

当行为人泄露海量信息却未造成可查证的具体个人损害时，法院仍以“情节严重”(信息数量达标)定罪。这一裁判逻辑引发根本追问：本罪保护法益仅为个人信息自决权吗？若存在超越个体的“公共信息安全”，与个人法益是何关系？

侵犯公民个人信息罪的保护法益之争已持续多年而未获共识。个人法益说将本罪法益界定为个人信息自决权，其内部衍生出隐私权说、信息自决权说与新型权利说三大分支，正如论者所指出，该说并未认识到个人信息自决权的集合性延伸价值，难以回应海量信息泄露对公共法益所造成的系统性威胁[1]。超个人法益说则走向另一极，契合了数字时代集体性侵害的规制逻辑。但其对“公共信息安全”的界定模糊，若过度强调公共法益而忽视个体权益的实际损害，将与本罪在刑法分则第四章的立法定位相冲突，亦有不当扩张之虞。混合法益说虽意图调和，却始终未完成对公共信息安全独立地位的论证。多数研究止步于“同时保护双重法益”的原则性构想，未明确二者的位阶关系，更未正面回应“公共信息安全究竟是不是一个独立于个人信息自决权的规范概念？”

近年来，学界新兴的“场景化法益观”为克服传统学说的平面化缺陷提供了重要启发[2]。其主张个人信息法益的判断应置于具体的信息处理场景中，以消解统一法益标准在复杂实践中的适用困难。然而，若将此逻辑推向极致，缺乏一个统一、稳定的法益内核作为支点，恐导致“一案一标准”的裁判碎片化，使法益概念丧失其构成要件解释指导机能。

为回应该困境，本文提出分层法益构造。以“制度信赖”为统一内核，为不同场景下的法益判断提供稳定价值基点，同时通过一阶法益(个人信息自决权)中的“同意边界”与“场景一致”原则检验，充分吸纳场景化判断的合理性，从而在裁判的可预测性与个案公正性之间寻求平衡。

2. 一阶法益的规范证成

分层法益构造的起点是一阶法益。若个人信息自决权本身不具有作为基础法益的正当性，则整个分层结构将失去根基。而学界对个人信息自决权说的质疑集中于立法论、效力论与还原论三个维度，本文将从以下方面回应并完成一阶法益的正当性论证。

2.1. 体系定位：分则第四章的规范约束

本罪被置于刑法分则第四章“侵犯公民人身权利、民主权利罪”中，明确了对本罪核心侵害指向是公民个人的信息权益，而非抽象的社会管理秩序。

立法论质疑者可能主张，既然大数据时代个人信息侵害已呈现集体性特征，就应将本罪移出第四章、归入第六章“妨害社会管理秩序罪”。本文对此的回应是：第一，移出第四章并不能解决法益界定问题，反而可能使本罪脱离个人法益的约束，导致打击范围不当扩张；第二，法益解释应优先在既有框架内完成，而非动辄诉诸立法修正。张明楷教授明确指出，“法条的体系地位是确定具体犯罪保护法益的最重要依据，对于规定在刑法分则第四章与第五章的犯罪，只要与构成要件内容没有明显冲突，就不能将其中的具体犯罪的保护法益确定为公共法益[3]。”在解释论上寻找容纳公共法益的空间，同时坚守个人法益基础地位，比推倒重来更具方法论上的审慎性，如有学者指出，公民个人信息应当作为独立的新型权利受到刑法保护，其兼具人身属性与财产属性，不应附属于其他法益[4]。

2.2. 制度性保障：对效力论质疑的回应

超个人法益论者最有力的批评是：在数字环境下，信息主体无从具备真正“自决”的能力，知情同意沦为形式，信息自决权作为法益已经“空转”。对此已有印证。多数裁判文书对“知情同意”的论述极为简略，知情、自愿、明确三要素在司法实践中难以同时满足[5]。可见，同意规则在实践中已不可避免地形化，信息主体极少作出实质同意决策。如果自决权在事实层面已经无法有效行使，其能否承担起刑法法益的功能？

本文看来，此批评精准地揭示了“自决权 = 事实性支配”这一传统理解的局限，但并不构成否定自决权作为一阶法益的充分理由。现代基本权利理论早已区分了“权利的事实行使可能性”与“权利的制度性保障功能”。正如公法学者在论述基本权利的客观法功能时所揭示的，某些基本权利不仅保障个人在事实层面的行为自由，更在制度层面为整个法秩序设定规范起点[6]。即使个人在事实上难以充分行使该权利，其作为制度起点的规范功能也并未消解。

法律秩序将“个人自主决定”设定为信息处理合法性的制度起点，正是《中华人民共和国个人信息保护法》(后文简称《个人信息保护法》)第十三条将“取得个人同意”设为首要合法性基础的法理深意。这并不意味着法律期待每个信息主体在事实上都能做出理性自主的决定——这确不可能，本文也从不否认。同意作为合法性基础，不是对个人事实能力的描述，而是对信息处理者义务的规范设定。个人信息权利束本质上是国家为制衡信息处理者而赋予个人的工具性权利，知情同意规则的功能不在于描述个人的事实能力，而在于为信息处理秩序设定规范性起点[7]。

退一步讲，若因“个人事实上无力自决”就否定自决权的一阶法益地位，将导致一个危险的逻辑滑坡：凡是现实中难以充分实现的权利，都应被移出刑法保护？生命权在面对系统性风险时同样脆弱，但没有人会因此否认生命权是杀人罪的基础法益。一项法益是否具有基础地位，取决于法秩序是否将其设定为制度的出发点，而非取决于个人在事实上能否完美地行使它。事实上，正是因为个人在数字时代面临自决能力的结构性削弱，刑法才更有必要将自决权锚定为一阶法益，而非放弃这一支点。

2.3. 出罪检验：对还原论质疑的回应

持还原论立场的学者可能承认本罪保护自决权，但主张真正支撑入罪的是公共法益。毕竟，在绝大多数案件中，入罪的关键是信息数量，而非是否侵犯了某个具体个人的自决权。

对此，本文认为如果自决权仅为名义上的基础，那么所有侵害公共信息安全的行为，无论是否侵犯了具体的个人自决权，都应构成犯罪。这显然不符合常理。本罪以“违反国家有关规定”为前置要件，具有入罪和出罪的双重功能，而违反的核心标志之一就是欠缺有效同意(或欠缺其他合法性事由)。这表明，即使在公共场景中，一阶法益也发挥着不可逾越的出罪检验功能。如果信息处理行为没有侵犯任何信息主体的自决权——例如获取已彻底匿名化、不可还原为特定自然人的信息，或者信息主体做出了符合“目的限定与场景一致”原则的有效同意就不能构成本罪。

一阶法益不是“名义上的基础”，而是“功能上的出罪阀门”。在刑法教义学中，出罪功能与入罪功能同等重要，而本罪的出罪检验“是否存在有效同意或合法事由”不可能由公共信息安全这一二阶法益来承担，其无从回答“这个特定的信息主体是否同意”这一核心问题。换言之，一阶法益之所以不可被二阶法益吸收或替代，根本原因就在于它承担着二阶法益无法承担的出罪检验任务。在现行刑法已明确将公民个人信息作为独立保护对象的规范框架下，本罪的法益构造应以个人法益为基础，同时兼顾超个人法益的保护维度。

然而，仅有一阶法益尚不足以解释批量入罪的规范实践。这要求我们追问：公共信息安全是否具备独立规范依据？

3. 二阶法益的规范依据

二阶法益的公共信息安全并非纯粹理论推演，本部分从刑法规范、前置法目的与司法解释三个层面，逐一检视二阶法益的规范根基。

3.1. 《刑法》第二百五十三条之一的规范构造

侵犯公民个人信息罪被规定于《中华人民共和国刑法》(后文简称《刑法》)分则第四章，这一体系定位固然是本罪首先保护个人法益的有力论据，但仅凭体系定位并不能穷尽本罪法益构造的全部内涵。《刑法》分则第四章中的罪名并不都是纯粹的个人法益犯罪。以同章的侵犯通信自由罪为例，该罪所保护的法益固然首先是公民个人的通信自由权，但其同时承载着保障社会信息流转秩序的公共功能[8]。本罪同样如此。以公民个人信息权益为基础保护对象，但这并不排斥信息权益在规模化聚集后形成的公共信息安全，同样值得刑法保护。

更为关键的规范特征在于，《刑法》第二百五十三条之一并未将“造成具体个人损害”列为入罪要件，而是以“情节严重”作为入罪门槛。最高人民法院、最高人民检察院司法解释将“情节严重”的核心标准锚定于信息数量：行踪轨迹信息 50 条以上、住宿信息等 500 条以上、其他信息 5000 条以上[1]。以数量为入罪标准，意味着立法和司法解释在此关注的不仅是某一个公民是否遭受了具体损害，而是信息侵害行为在数量维度上达到的规模化程度本身。为何是 50 条、500 条、5000 条？逻辑在于，当信息侵害达到一定数量级时，其不法内涵就不再局限于对个体权益的侵害，而是形成了对不特定多数人信息安全的系统性威胁。这种系统性威胁正是二阶法益所要保护的对象。

[1]参见最高人民法院、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》第 5 条。http://gongbao.court.gov.cn/Details/f9bbdd79e39de33c7b3417fa4061ff.html?sw=%e4%be%b5%e7%8a%af%e5%85%ac%e6%b0%91%e4%b8%aa%e4%ba%ba%e4%bf%a1%e6%81%af%e7%bd%aa

司法解释在侵犯公民个人信息罪的定罪量刑标准上采取立法定量模式，这一规范特征即表明该罪所保护的法益不限于个人法益，还包含公共信息安全维度。司法解释的起草者对此亦有清晰认识：“侵犯公民个人信息的危害性不在于该信息对于使用者是否有用，而在于公民个人信息被泄露而产生的相关危害及影响[9]。”这里的“相关危害及影响”，显然不限于特定个体的损害，而是包含着信息大规模失控后对整个社会信息流转秩序的冲击。

3.2. 《个人信息保护法》的双元目的

《个人信息保护法》第一条完整表述了立法目的：“为了保护个人信息权益，规范个人信息处理活动，促进个人信息合理利用，根据宪法，制定本法。”这一表述呈现出清晰的“双元结构”。一端是“保护个人信息权益”，另一端是“促进个人信息合理利用”。二者并非主从关系，而是并列设置。须知，促进利用的前提是信息流转秩序的可信赖，这正是二阶法益独立规范价值的前置法依据[2]。

从法秩序统一性的视角审视，刑法作为后置法，理当与前置法的保护目的相衔接。如果《个人信息保护法》的立法目的仅仅在于保护个人的信息自决权，那么刑法确实只需保护个人法益即可。但该法将“促进个人信息合理利用”与“保护个人信息权益”并列，本身就表明立法者对个人信息所承载的公共利益有着清晰认识。个人信息不仅是个人权益的客体，也是数字经济社会运行的基础资源，其中既包含个人对信息的控制权能，也包含国家对信息处理秩序的维护职责[7]。

基于此，公共信息安全作为二阶法益确立了独立价值根基。

3.3. 司法解释的间接印证

最高人民法院、最高人民检察院2017年《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》为本罪法益的层次构造提供了进一步的规范印证。该解释第五条不仅以信息数量作为“情节严重”的核心标准，更在“情节特别严重”的认定中引入了“造成重大经济损失”、“造成恶劣社会影响”、“引发群体性事件”等实质性危害后果。这种从“数量”到“后果”的梯度递进，实际上对应着法益侵害程度的升层。当信息侵害行为不仅逾越了数量门槛，而且导致了现实的社会后果时，不法程度也随之升级。

更为直观地印证来自检察公益诉讼的实践。在最高人民法院指导性案例第192号李开祥案[3]中，法院不仅追究了被告人的刑事责任，还支持了检察机关提起的刑事附带民事公益诉讼。公益诉讼的性质决定了其修复对象不是某个具体被害人的损害，而是被侵害行为所破坏的公共信息安全秩序。如果公共信息安全仅仅是个人法益的量的累积，公益诉讼就没有独立存在的必要，民事诉讼足以解决个体权益的救济问题。公益诉讼之所以被启动，正是因为侵害行为所触动的，是一种不能由个体私益诉讼来修复的公共利益。

4. 二阶法益的独立结构

我国侵犯公民个人信息罪的二阶法益构造，是在《刑法》分则体系定位与司法解释的规范实践之下，形成的本土化分层理论，并非域外理论的简单移植[4]。

4.1. “公共信息安全”的内涵边界

在展开二阶法益的规范结构之前，须先厘清“公共信息安全”的内涵边界，使其形成范围符合一般

[2]此处“并列设置”系对立法目的文本关系的客观描述，与本文主张法益“分层构造”处于不同层面——前者描述前置法的立法目的结构，后者建构刑法的法益位阶关系。
[3]参见李开祥侵犯公民个人信息刑事附带民事公益诉讼案，最高人民法院指导案例192号(2022年)。
[4]域外讨论如欧盟《通用数据保护条例》(https://gdpr-info.eu/)的双重目标与德国“人口普查案”的信息自决权，多在宪法或行政法层面展开，与本罪刑法教义学分层构造语境有实质性差异，故本文不展开比较。

人期待。

正面界定：制度信赖。公共信息安全是指，不特定多数信息主体对“个人信息将被依法处理、信息流转秩序将得到有效维护”这一制度承诺的无差别信赖。有三层规范内涵：其一，它不是对某一特定信息处理者的个别信赖，而是对整个信息处理制度的一般信赖。人们之所以愿意在日常交往中提供个人信息，不是因为相信每一个处理者都可靠，而是因为相信有一套制度在维护信息处理的基本秩序；其二，不是对“个人信息不会被泄露”的绝对保证，而是对“信息流转存在有效规则、违法行为将被追责”的合理预期；其三，不要求识别出具体被害人，但其受损必然降低社会整体的制度信心，从而破坏个人信息合理利用的社会基础。

负面排除：三条边界。第一，不等于纯粹的行政管理秩序。仅仅是违反了信息处理的行政备案要求、未按规定提交风险评估报告等程序性违规，虽然可能构成行政处罚，但不能认定为侵犯了作为二阶法益的“公共信息安全”。第二，不等于技术系统的数据安全。计算机信息系统被非法侵入导致数据泄露，首先触犯的是计算机犯罪所保护的系统安全法益，而非本罪的公共信息安全。除非泄露的数据包含可识别的公民个人信息。第三，不等于数据跨境流动的监管秩序。数据出境未依法进行安全评估，违反的是国家数据安全监管制度，其法益属性更接近国家安全层面，不应混同于本罪所保护的、与公民人身权利紧密关联的公共信息安全。

综上可见，本罪二阶法益具有“人身附随性”[5]。即公共信息安全始终以“可识别的公民个人信息”为事实载体，以不特定多数信息主体的信息权益受威胁为实质内容。离开“公民个人信息”这一载体，就不再属于本罪的保护范畴。例如，依据《个人信息保护法》第七十三条，经过不可逆匿名化处理、无法识别特定自然人的数据集(如仅保留统计分类特征的医疗研究数据)，因丧失人身附随性，对其的侵害不构成本罪；反之，技术上仅作可逆的假名化处理，仍可通过关联分析还原为特定自然人的数据集(如包含网络行为轨迹与设备指纹的用户画像数据)，则依然具有人身附随性，仍为本罪的保护对象。这是二阶法益区别于其他公共法益的本质特征，也是防止其适用泛化的底线规则。

4.2. 派生性：二阶法益的生成逻辑

二阶法益不是凭空产生的独立价值，其生成以无数个体信息权益的事实存在为前提。这种“派生性”是二阶法益区别于纯粹集体法益的本质特征，也是本文坚持“分层”而非“分立”的深层原因。

公共信息安全并非自发产生的制度性利益，而是由无数信息主体的自主决定汇聚而成的集合性秩序形态。当且仅当特定信息集合能够追溯至具体的个人信息主体时，制度信赖才不致沦为脱离个体权益的空洞宣示。刘艳红教授指出，本罪属于“自然犯的法定犯化”，其根本性质仍是自然犯——“如果仅仅侵犯了超个人集体法益，并不能确定犯罪的成立”[11]。这一论述从犯罪性质的维度印证了派生性的逻辑起点：公共信息安全的规范概念之成立，以个人信息自决权的事实存在为前提。

个体信息自决权经由制度中介转化为不特定多数信息主体对信息处理秩序的制度信赖。《个人信息保护法》第十三条将“取得个人同意”设为首要合法性基础，其法理深意正在于此：同意的制度功能不在于确保每个主体作出理性自主的决定，而在于为信息处理的合法性提供规范性起点。当无数主体在具体场景中持续行使自决权能时，不仅是在维护自身权益，更是在向整个社会传递“信息处理规则有效运行”的信号。

当个人信息自决权从单一个体的孤立行使上升为不特定多数人对信息处理秩序的普遍信赖时，这种信赖便不再是个体自决权的简单叠加。个体自决权的损害可以经由删除信息、赔偿损失、停止侵害等个

[5]有学者将集体法益界定为累积犯侵犯的法益，具有不可分配性(参见[10])。本文主张的“制度信赖”虽也具有不可分配性，但其核心特征在于“人身附随性”，与一般集体法益有所不同。

体救济来修复，但制度信赖的动摇，并不能通过任何一个个体权益的救济来平复。如同司法公正、货币信用一般，它已转化为一种不可分割的公共产品，由全体社会成员共享。

4.3. 独立性：不可还原的规范价值

二阶法益的独立性，是本文与既有混合法益说的根本分歧所在，也是本文的核心理论主张。既有混合法益说之所以止步于“同时保护双重法益”的原则宣告，根本原因在于对公共信息安全的理解停留在“若干个人法益的集合”这一量的维度上[12]。在这种理解下，公共信息安全没有独立的规范内涵，其只是“很多个人信息自决权”的简称，理论上可完全还原为前者。

二阶法益具备不可完全还原为一阶法益的独立规范价值。对此命题，混同法益理论已有成熟论述，认为集体法益具有使用上的包容性、消耗上的非竞争性和不可分配性，已获得独立于个人法益的地位，二者不再仅是量的区别[13]。本文看来，当公共法益在满足特定条件后，亦可具备与集体法益相似的不可还原属性。个人法益在规模化聚集后形成了不可分割的公共产品属性时，其价值内涵便不能由个体权益的加总来完全替代。这并非否定其个人法益的生成基础，而是承认个人法益的规模化聚集产生了一种超越个体权益的新属性。制度信赖正是这样一种不可分割的公共产品。

制度信赖的不可还原性可以从两个层面来理解：

第一，制度信赖是不可分割的公共产品。个体信息权益的损害可以经由个体救济来修复，如删除信息、赔偿损失、停止侵害。但如果大规模信息侵害行为动摇了公众对信息处理秩序的整体信赖，人们不再相信其信息在数字空间中会被依法处理，开始拒绝提供信息或提供虚假信息，这种信赖的损失无法通过任何一个个体权益的救济来修复。

第二，制度信赖具有不可替代的规范功能。在公共场景下，当海量信息面临系统性风险却尚未造成具体个体损害时，如果仅有个人法益，刑法将无法介入。因为没有具体被害人，无法认定具体损害。但正是在这种情形下，公共信息安全受到的威胁最为紧迫。黑产交易链条中的海量信息流转，虽然尚未“变现”为具体个体的损害，但对制度信赖的侵蚀已经发生。二阶法益的引入，为刑法在这种场景中提供了正当的介入根据。

敬力嘉教授早已洞见到，本罪法益保护取向应从私法上的个人权利转向公法上的信息安全秩序[14]。本文在此基础上将这一秩序的内核进一步精确化为“制度信赖”，由此完成从宏观方向判定到微观教义学结构的理论推进。

4.4. 一阶与二阶的深层关系

完成一阶法益与二阶法益的独立证成之后，需回应一个对分层结构的前提性质疑：如果二阶法益具有不可还原的独立性，那它与一阶法益是否只是本罪内部的两个平行保护对象？如果二者仅属于并列法益，则本文所谓“分层构造”便与近年来混合法益说所主张的双重法益保护并无本质区别，其规范功能亦可借助传统想象竞合理论加以解释，由此便无须另行建构分层结构，何必创造一个“分层”结构？

本文的回答是：想象竞合逻辑之所以无法替代分层构造，根本原因在于其所预设的两个法益是“并列”关系，想象竞合的成立“完全取决于偶然的案件事实‘激活’法条之间的关系”，其本质是“法益侵害事实(结果)的叠加”；同时，想象竞合成立的前提为案情事实“溢出”一罪构成要件范围，需以数罪才能完全包容评价[15] [16]。而这恰恰是一阶法益与二阶法益间不存在的前提关系。故本文主张，其为同一制度安排在两个层次上的规范表达，二者共享一个理论内核——制度信赖。

制度信赖具有一种独特的“双侧性”。其在“个体侧”表现为个人信息自决权的制度保障。每个信息主体都有权要求信息处理者依法取得同意、履行告知义务。在“秩序侧”则表现为公共信息安全的制

度预期。不特定多数信息主体对信息处理秩序的整体信赖。这一结构亦可从王锡锌教授提出的“个人信息权利束”理论中获得一定启发，在个人信息保护的权利束中，同时包含个人对信息的控制权能和国家对信息处理秩序的维护职责，二者并非相互排斥的两种权利，而是同一规范整体的两个维度。

正是这种“同一内核、双侧表达”的结构，决定了想象竞合逻辑在此力有不逮。想象竞合适用的前提是两个法益相互独立、有可能分别被不同的行为侵害，只不过在本案中偶然地被同一行为同时触发。但一阶法益与二阶法益之间不存在这种独立性，不可能存在一种情境，其中二阶法益受到侵害而一阶法益毫无关联，正如不可能存在“经络受损而肌肤完好”的状况。二者不是“两个法益被一个行为同时侵害”，而是“同一制度信赖在两个评价层次上被同一侵害行为所触动”。想象竞合描述的是法益之间的横的并列，分层构造揭示的是法益之间纵的生成。

必须明确的是，所谓“分层”，并非个人法益与公共法益间存在高低价值之分，而是二者在法益生成、规范评价与司法适用上的位阶差异。一阶法益决定刑法介入之正当，二阶法益则决定介入之必要，前者构成评价起点，后者体现评价深化。正因如此，分层构造不仅能够解释本罪法益保护对象为何兼具个体权益与公共利益，亦能够避免混合法益说在法益评价中容易出现的重复评价与评价位序不明的问题，从而为犯罪成立条件及司法适用提供更为清晰的规范指引。

5. 二阶法益的教义学功能

二阶法益的教义学功能体现在多个层面：一为划定入罪边界，为刑法提前介入提供正当根据；二为整合体系解释，使信息数量分级、下游犯罪加重、公益诉讼等规范现象获得统一说明；三为重述不法内涵，揭示公共场景中本罪特有的规范非难内容。

5.1. 入罪边界的划定功能

当海量信息面临严峻系统性风险却尚未造成具体个体损害时，二阶法益为刑法提前介入提供了正当根据。行为人将海量个人信息扩散至公共空间，虽未造成可查证的具体损害，但法院仍以侵犯公民个人信息罪定罪[6]。在二阶法益框架下，这种裁判逻辑获得了完整的教义学解释——行为人虽未侵害某个具体个人的自决权，但其行为已实质性危及公共信息安全，动摇了制度信赖。这种“制度信赖的动摇”并非某个具体被害人能够感知的个体损害，而是弥漫于整个社会信息流转秩序中的系统性危险，这正是二阶法益所要保护的核心内容。

熊昌恒案从另一个方向印证了这一功能[7]。该案中，行为人通过购买空白微信号并批量添加好友后转售，还批量购买他人求职信息后转售牟利。求职者在特定场景中自愿提供了个人信息，但信息被转移至完全不同的商业流转场景。法院认定，虽然信息系被害人自行公开，但行为人“改变了公民公开个人信息的范围、目的和用途，不属于法律规定的合理处理”。该裁判规则在二阶法益的框架下获得了新的解释维度。信息主体在求职场景中的同意，在一阶法益层面排除该特定处理行为的违法性；但当行为人将信息从封闭的求职场景转移至开放的大规模转售场景时，同意的效力边界已被超越，新的处理行为不仅侵害了一阶法益(超出同意范围)，更因行为的批量性和扩散性对二阶法益构成了独立的系统性威胁。

需注意的是，功能主义刑法立法观虽能适应风险社会的规范性需求，但也要警惕积极介入的立法导向可能制造新的风险。抽象危险虽然不以实害为要件，但须以“法所不容许的危险达到紧迫程度”为前提。对于数量不大、范围可控、滥用风险低的情形，民事或行政手段足以应对，无需刑事规制[17]。

[6]参见同前注李开祥侵犯公民个人信息刑事附带民事公益诉讼案。
[7]参见熊昌恒等侵犯公民个人信息案，最高人民法院指导案例 194 号(2022 年)。

5.2. 体系解释的整合功能

二阶法益的引入，可以使本罪中若干难以用一阶法益单独解释的规范现象，获得体系化的说明。

信息数量的分级标准得以在法益层次上获得合理解释。司法解释以个人信息数量来界定抽象危险的成立标准，对于敏感个人信息与一般个人信息应有所区别，这正是分级保护的法理基础[18]。这实质上是根据信息所承载法益的重要性程度形成的“分类–分级”双层次保护结构[19]。行踪轨迹信息 50 条即构成“情节严重”，而普通信息需 5000 条，正是因为前者一旦失控，对不特定多数人信息安全的威胁更为紧迫、更易被下游犯罪利用。其背后，是二阶法益在不同信息类型中受损的紧迫性差异，即信息越敏感，其规模化泄露对制度信赖的冲击就越大。

“引发下游犯罪”作为加重情节同样可以在二阶法益框架下获得解释。信息泄露后，如果信息被查证属实用于实施诈骗、敲诈勒索等犯罪，说明二阶法益受到的威胁已从抽象危险转化为现实侵害，公共信息安全遭受了实质性破坏，不法程度因此升级。

刑事附带民事公益诉讼在二阶法益框架下获得了完整的理论解释。李开祥案中公益诉讼的启动，其修复对象正是被破坏的制度信赖。这种信赖的修复不可能通过个体私益诉讼来完成，因为不存在具体的被害人。检察机关之所以有权提起这类诉讼，正是因为大规模信息侵害行为触动的是一种不能由个体私益诉讼来修复的公共利益，这也印证了二阶法益的公共产品属性。

5.3. 不法内涵的说明功能

在一阶法益视角下，本罪的不法内涵被理解为“侵犯个人的信息自决权”。此种理解在个人场景中完全成立，但在公共场景则难以自圆其说。当被害人不特定、损害不确定时，这一不法描述就失去了具体的指向对象。

在二阶法益的补充视角下，公共场景中的不法内涵可被重新表述。即行为人未经许可地处理海量公民个人信息，制造信息被后续滥用、关联识别、非透明决策所支配的系统性风险，动摇了数字社会信息流转的制度信赖。该侵害越过个体，直指所有信息主体对信息处理秩序的制度预期。

这种不法内涵的重述，更契合本罪法定犯的性质。本罪以“违反国家有关规定”为前置要件，本身就表明其不法判断高度依赖实定法规范，而非诉诸在先的伦理非难。二阶法益作为制度信赖的载体，正是这种实定法规绕的核心对象，它保护的不是先在的自然权利，而是法律所建构的信息处理秩序本身。

6. 二阶法益的适用限度

二阶法益的独立性是“受限的独立性”。若不加限制，其可能反向挤压一阶法益的评价空间，甚至导致处罚范围不当扩张。因此，必须明确其适用限度。也即，承认二阶法益的独立性，不意味着其可以不受限制地扩张适用。

6.1. 积极要件之一：二阶法益的启动前提

二阶法益的启动以涉案信息承载着“可识别的公民个人信息”为前提。若涉案信息与具体公民个人信息无关，或已做匿名化处理而无法识别特定自然人[20]，则一阶法益已失去评价对象，二阶法益亦无从启动。

换言之，二阶法益并非随着个人信息权益受到侵害而必然启动，其作为超越个体利益的制度法益，应以个人信息处理行为已超出个体侵害范围并形成制度性风险为基础。只有当行为足以突破个体损害评价，进而可能影响社会公众对个人信息处理规则的整体信赖时，刑法才有必要进入二阶法益评价阶段。也即，二阶法益的介入具有补充性，而非当然性。

这一限制的法理基础则在于前文反复论证的“人身附随性”判准。本罪的二阶法益以公民个人信息为唯一载体，离开这一载体，就不再属于本罪保护范畴。纯粹的数据安全、信息系统的技术安全、数据跨境流动的行政管理秩序等，即便值得刑法保护，也应通过其他如计算机犯罪、拒不履行信息网络安全管理义务罪等实现，不能通过扩张本罪二阶法益来“搭便车”。

在此基础上，二阶法益评价尚须进一步满足系统性风险达到刑法规制程度，并保留充分的出罪审查空间。

6.2. 积极要件之二：系统性风险达刑法规制程度

系统性风险并非单纯取决于个人信息数量，而应结合信息敏感程度、处理规模、流转范围以及是否可能诱发下游违法犯罪等因素综合判断。上述因素共同反映行为对于个人信息处理制度运行及社会信赖基础的影响程度，从而决定是否进入二阶法益评价。而所谓系统性风险，并非风险已经现实发生，而是行为足以持续削弱公众对个人信息依法收集、处理和利用机制的制度信赖，并因此具有突破个体法益评价范围的现实可能。

例如，在有具体被害人的个人场景中，一阶法益处于评价核心地位，二阶法益作为补充性评价要素。当行为已造成特定个体人身损害、财产损失或人格权益侵害时，应以一阶法益的实质损害为定罪量刑的核心依据，二阶法益的抽象危险不得重复叠加为入罪标准，至多在量刑时作为从重情节参酌。

吴某慧、陈某强案为此提供了实证支撑[8]。该案中，被告人非法获取公民住宿、行程、社交关系等敏感个人信息，通过网络“开盒”方式恶意公开曝光，并配以煽动性言论引导网民围观、辱骂，相关信息在网络平台快速扩散。上述裁判实际上体现了先以一阶法益完成犯罪成立评价，再以二阶法益完成社会危害程度评价的分层思路，法院裁判呈现出清晰的分层评价结构。定罪层面，以特定被害人生活安宁被破坏、人格尊严遭受侮辱的具体损害作为认定“情节严重”的基础要件；在社会危害性评价层面，则将信息扩散对网络公共秩序的破坏程度纳入量刑考量。

需注意的是，“补充而非替代”。即便在公共场景中，二阶法益的评价权重也不能完全挤压一阶法益的评价空间，公共场景中的“推定侵害”仅是一种因证明困难而设置的规范技术，其功能是降低控方的证明难度，而非封闭被告人的出罪途径。因此，系统性风险之认定始终服务于二阶法益评价，而不能反向替代一阶法益的成立判断。

6.3. 出罪路径的限制

二阶法益的评价不能反向限制被告人的出罪权利。在经由推定认定抽象危险成立后，必须为被告人保留反证出罪的通道。本罪的规范目的在于规制上游信息侵害行为以防范下游犯罪引发的安全风险；若侵犯行为不足以造成公众人身伤害或财产重大损失，应予以出罪；已公开的个人信息因欠缺实质法益侵害风险，不应作为本罪的规制对象[21]。例如被告人能够证明抽象危险已经消除或者不存在持续扩散可能的，抽象危险即告丧失，不得仅凭信息数量继续追究刑事责任。即使二阶法益评价已经启动，也并不意味着犯罪当然成立。对于依法履行法定义务、基于公共利益处理个人信息、行为整体风险已被有效控制等情形，应充分发挥违法阻却及构成要件限缩解释功能，避免二阶法益评价突破罪刑法定原则和刑法谦抑原则。二阶法益的引入，应当强化刑法介入之正当性，而非扩张刑法处罚范围。

出罪路径的限制与一阶法益的出罪检验功能形成呼应。一阶法益在构成要件层面检验“是否存在有效同意或合法事由”；二阶法益的出罪路径则在公共场景中检验“抽象危险是否已被消除”。两者共同构成一个完整的出罪保障体系，确保分层法益构造在入罪功能与出罪功能之间保持平衡。当然，该出罪

[8]参见吴某慧、陈某强侵犯公民个人信息案，江苏省苏州市姑苏区人民法院(2020)苏 0508 刑初 714 号刑事判决书。

路径的适用须严格限缩，若批量处理已公开信息并形成新的画像或关联分析，对个体安全造成超出原始公开范围的系统性威胁时，仍可能重新激活本罪保护。由此，二阶法益既构成犯罪成立后的进一步评价依据，也同时构成限制刑法过度介入的重要保障机制。

7. 结语

个人信息自决权之所以成为一阶法益，不仅源于本罪在刑法分则的体系定位，更在于其承担着信息处理合法性制度起点的规范功能与不可替代的出罪检验任务。即使个人在数字时代面临自决能力的结构性削弱，但自决权的制度性保障功能并未消解，其依然是划定信息处理合法边界的出发点，亦为检验是否存在“违反国家有关规定”的核心标尺。公共信息安全作为二阶法益，其本质内核是“制度信赖”。它是所有信息主体对数字社会信息流转秩序的无差别依赖，承载着不可完全还原为个人权利的独立规范价值。

一阶法益与二阶法益并非平行保护对象，而是同一制度信赖在不同维度上的规范表达。这既是对已有研究成果的继承与发展，也是对单一法益观局限性的有力克服。本文的理论框架既回应了个人法益说在海量信息侵害面前的解释力不足，也吸纳了超个人法益说对系统性风险的洞察，克服了传统混合法益说内部结构不明、位阶不清的缺陷。在数字时代，本罪法益亟须一种能同时兼顾个人权利保护和公共信息安全的理论框架。分层构造的法益观，正是在个体保护与公共秩序之间寻找精妙平衡的一次尝试。而不同信息类型(如敏感信息与一般信息)在分层构造中的具体适用标准，仍有待后续研究进一步细化。

参考文献

[1] 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.

[2] 郑泽星. 论侵犯公民个人信息罪的保护法益——场景化法益观的理论构造与实践立场[J]. 清华法学, 2023, 17(3): 92-108.

[3] 张明楷. 具体犯罪保护法益的确定依据[J]. 法律科学(西北政法大学学报), 2023, 41(6): 43-57.

[4] 于冲. 侵犯公民个人信息罪中“公民个人信息”的法益属性与入罪边界[J]. 政治与法律, 2018(4): 20-31.

[5] 李雨桐. 明理之辨丨知情同意原则对侵犯公民个人信息罪司法裁判的校准[EB/OL]. 北京市第二中级人民法院官网, 2023-10-13. https://bj2zy.bjcourt.gov.cn/article/detail/2023/10/id/7574453.shtml, 2026-07-16.

[6] 张翔. 个人信息权的宪法(学)证成——基于对区分保护论和支配权论的反思[J]. 环球法律评论, 2022, 44(1): 53-68.

[7] 王锡锌. 国家保护视野中的个人信息权利束[J]. 中国社会科学, 2021(11): 115-134.

[8] 秦小建. 新通信时代公民通信权的实践争议与宪法回应[J]. 中国法律评论, 2020(7): 85-97.

[9] 周加海, 邹涛, 喻海松.《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》的理解与适用[J]. 人民司法(应用), 2017(19): 31-37.

[10] 张明楷. 集体法益的刑法保护[J]. 法学评论, 2023, 41(1): 43-57.

[11] 刘艳红. 侵犯公民个人信息罪法益: 个人法益及新型权利之确证——以《个人信息保护法(草案)》为视角之分析[J]. 中国刑事法杂志, 2019, 5(5): 19-33.

[12] 何群, 胡宗媛. 法益二元论视野下侵犯公民个人信息罪之法益内涵与规制路径[J]. 宁夏大学学报(社会科学版), 2024, 46(2): 107-117.

[13] 王永茜. 论集体法益的刑法保护[J]. 环球法律评论, 2013, 35(4): 67-80.

[14] 敬力嘉. 大数据环境下侵犯公民个人信息罪法益的应然转向[J]. 法学评论, 2018, 36(2): 116-127.

[15] 陈洪兵. 竞合处断原则探究——兼与周光权、张明楷二位教授商榷[J]. 中外法学, 2016, 28(3): 817-839.

[16] 方鹏. 刑法适用方法视角下的法条竞合与想象竞合关系论[J]. 刑事法评论, 2018, 42(1): 441-475.

[17] 劳东燕. 风险社会与功能主义的刑法立法观[J]. 法学评论, 2017, 35(6): 12-27.

[18] 刘浩. 侵犯公民个人信息罪的法益构造及其规范解释[J]. 环球法律评论, 2023, 45(3): 163-179.

[19] 王德政. 从分类到分级: 我国公民个人信息的刑法保护[J]. 湖南社会科学, 2023(5): 122-131.
[20] 杨凯. 以公法法益观理解侵犯公民个人信息罪[N]. 检察日报, 2021-12-10(03).
[21] 曹岚欣. 侵犯公民个人信息罪的规范目的与出罪路径[J]. 西南政法大学学报, 2025, 27(1): 117-128.