论数据权益的刑法保护

——民刑交错视角下的法益保护论探讨

郑军男*

目次

摘要 关于“数据权益的刑法保护”问题，在理论层面上，可从“刑法解释论”和“刑法立法论”两种路径进行探讨。“刑法解释论”探讨路径以现行《刑法》罪名体系为出发点，主要任务是揭示哪些罪名的犯罪构成之设置是以“数据权益”为规范保护目的；“刑法立法论”探讨路径是在刑法立法层面上探讨立法者为在刑法政策上实现数据权益的刑法保护这一目的，动用刑罚禁止何种行为类型才具正当性的问题。然而，两种探讨路径都将依赖于“数据权益”的内涵确定以及法益格的认定问题，换言之，是刑法法益理论在数据权益刑法保护问题上的具体运用。《民法典》第127条并非是关于数据的确权性规定，且在民法理论界关于数据权益的法律属性存在诸多争议的状况下，“数据权益”内涵不明、法律属性不清导致其并不具备作为刑法保护客体的“法益”格。当前刑法理论界存在的关于“数据权益”的刑法类法益保护模式探讨路径，是对刑法法益保护方式的误读，并未触及“数据权益刑法保护”之规范层面问题的实质。“数据安全”法益观的探讨路径则不仅混淆了现象层面与规范层面上的“数据犯罪”概念的界分，也由于没有论证“数据安全”如何能够构成刑法的保护法益，而导致结论过于武断。在理论探讨上，应该明确作为行为客体的物理层面上的“数据”概念与作为保护客体的法益层面上的“数据权益”概念之间的区别，据此明确“数据权益的刑法保护”在规范层面上是否构成新问题。

关键词 数据 数据权益 法益保护 数据犯罪 数据安全

* 吉林大学法学院教授、法学博士。

一、问题的提出

首先需要明确的是,“数据权益的刑法保护”这一论题与刑法的任务或刑法的目的问题密切相关,即当我们谈论刑法的任务是法益保护〔1〕或者刑法的目的是法益保护〔2〕时,实际上意味着我们需要在刑法的保护客体即法益层面上来讨论数据权益的刑法保护问题。其具体涉及如下几个问题:1.什么是数据权益?其是刑法保护客体之法益吗?2.现行刑法在如何保护数据权益?3.刑法应当如何保护数据权益?

因此,数据权益的刑法保护问题,大体存在两种基本理论探讨路径:第一种是与上述第二设问相关联的“刑法解释论”探讨路径,即在现行实定刑法中,有无具体的犯罪类型是直接将数据权益作为保护客体的,或者用通说的理论用语来讲,哪一具体罪名犯罪构成中的犯罪客体要件是以“数据权益”为内容。此种理论探讨路径以现行刑法罪刑法规为出发点,通过运用刑法解释方法,揭示现有罪名体系中可供“数据权益”刑法保护的具体罪名有哪些,探讨这些现有罪名能否满足“数据权益”刑法保护的现实需求等问题,因此这是从实然层面对“数据权益刑法保护”问题的探讨。第二种是与上述第三设问相关联的“刑法立法论”探讨路径,即在刑法立法层面上,立法者为在(刑)法政策上实现数据权益的刑法保护这一目的,动用刑罚禁止何种行为类型,才是正当合理的。因此,这是关于“刑法立法正当性”问题的探讨。如果说,刑法立法的正当性必然要求犯罪类型的设置与法益保护这一刑法目的相关联,一切与法益保护内容无关的行为类型的刑罚制裁法律,都将构成欠缺立法上的正当性而归于无效。〔3〕那么,我们首先要思考的是,“数据权益”能否作为新兴法益为刑事立法上处罚某种行为提供正当性根据?这是从应然层面上探讨数据权益的刑法保护问题。

然而,需要进一步指明的是,无论是上述“刑法解释论”探讨路径还是“刑法立法论”探讨路径,都无法回避第一设问——“数据权益”的内涵为何?其是刑法的保护法益吗?——这一基本问题的解答。换言之,第一设问的探讨,将构成后两个设问探讨的前提和基础。因为,只有事先明确“数据权益”这一法益内涵,才能在“刑法解释论”的层面上发挥“法益的体系内解释机能”,为具体犯罪类型的实质解释提供方法论上的指导;同时,在立法论探讨中发挥“体系外立法批判功能”,为通过刑法保护“数据权益”的刑事立法提供正当性根据。因此,上述三个问题可抽象概括为刑法法益理论在数据权益刑法保护问题上的具体运用,而法益概念及其相关理论问题将构成本论题探讨的基点。

二、问题探讨的理论基点:作为刑法保护客体之“法益”概念的理解

众所周知,“法益概念”自近代刑法学发展以来,目前已然成为构建现代刑法学的理论基石。

〔1〕 参见[韩]金日秀、许辅鹤:《韩国刑法总论》(第11版),郑军男译,武汉大学出版社2008年版,第25页以下;高橋則夫『刑法総論〔第2版〕』(成文堂,2013年)11頁以下;古承宗:《刑法的象征化规制理性》,元照出版有限公司2017年版,第5页以下。

〔2〕 参见张明楷:《刑法学(上)》,法律出版社2021年版,第25页以下;林幹人『刑法総論』(東京大学出版会,2004年)24頁以下。

〔3〕 上田正基『その行為、本当に処罰しますか——憲法的刑事立法論序説』(弘文堂,2016年)25頁、36頁以下参照。

“法益保护原则”更是作为现代刑法中的三大原则之一,〔4〕在刑法立法与刑法解释适用上发挥着重要作用。具体而言,法益理论在关于刑罚效力界限的讨论中,从刑法立法目的在于保护法益这一基本认识出发,不仅为刑法立法提供合理性的处罚根据,也要求在实质犯罪概念的解释上,将“法益之侵害或危险”作为核心内容,主张不法构成要件实质内涵之探讨必须与“法益”相关联(法益关联性)。〔5〕 据此,“法益概念”成功联结起“立法论”(法益保护目的)视角与“解释论”(法益侵害说)视角,“违法判断的内容及违法要素的范围,将受到该当刑罚法规所预设之规制目的或保护目的的限定”这一认识的普遍化正是法益论的功绩。〔6〕

尽管如此,“法益”概念也因其内涵的不确定而饱受诟病。甚至有学者直言,由于内涵不清,“不能清楚地区辨什么应该是刑法上保护的对象”,“在这种情况下,要讨论犯罪构成要件的正当性问题就欠缺客观的标准,只能借由主观的、片面的论述堆砌恣意地肯定或否定保护对象的资格。到最后形成的结论,充其量只能反映出论述者个人所持的特定价值立场”。〔7〕 确实,在我们常见的法益概念如“法益是法所保护利益”〔8〕或“法益是法所保护的抽象的、社会秩序价值”抑或“法益是法所保护的利益或价值”〔9〕等表述中,“利益”“价值”等抽象性表述究竟具体指何种实体内容并不明确。虽然本文的主题并非构建明晰的法益概念内涵,但至少应该明确法益概念的基本构造,这也是判断某种具体的利益或价值是否符合“法益”概念或者判断其是否为刑法保护客体的最低基准。这同时也是为探讨“数据权益”是否具备法益资格问题提供理论基础。

(一) 作为刑法保护客体之“法益”概念的基本构造

本文认为,刑法中法益概念的基本构造由三个要素组成,即:1. 价值实体性;2. 法的评价性以及 3. 法的实践性。

1. 价值实体性,是指法益概念必须以社会的事实性利益或价值为基础。只有这样,其作为价值实体,才能够成为法的评价对象。法益,作为关系性概念,是社会性“存在(is)”与法律上诸种原理及理念的规范性“当为(ought)”的综合。〔10〕 因此,法益不外乎是从法的视角将社会性事实利益评价为“有价值”而已。在这里,法益的构成必须要具有实定法的个人、社会或国家的事实性利益作为价值的实体,并获得法的评价和承认。

2. 法的评价性,是指社会的事实性利益只有经过法的价值或理念的评价才能成为法所保护的利益,即法益。因此,法的评价性是使社会的事实性利益上升为法所认可利益的必经程序,也是法益概念的必备要素。构成法益之价值实体的社会事实性利益或价值,在未经法的评价或承认之前,尽管对于社会或个人而言是有价值的、具有“有用性”的,但不能由此直接推导出其是(刑)法中的“法益”,受(刑)法保护。只有当从(刑)法的立场认定其为值得保护的利益,此法益才具有法秩

〔4〕 张明楷教授认为,刑法基本原则包括“罪刑法定原则”“法益保护原则”和“责任原则”,见前注〔2〕,张明楷书,第 52 页以下。但是,也有学者将“法益保护”视为刑法的任务,将“行为主义”“罪刑法定主义”和“责任主义”等视为刑法基本原则,井田良『刑法総論[第 2 版]』(有斐閣,2019 年)16 頁、30 頁以下参照。

〔5〕 嘉門優『法益論—刑法における意義と役割—』(成文堂,2018 年)9 頁参照。

〔6〕 井田良「犯罪論と刑事法学のあゆみ」法学教室 179 号(1995 年)20 頁。

〔7〕 周漾沂:《从实质法概念重新定义法益:以法主体性论述为基础》,载《台大法学论丛》第 41 卷第 3 期(2012 年),第 984 页。

〔8〕 高橋前掲書・22 頁;见前注〔2〕,张明楷书,第 77 页。

〔9〕 内田文昭『刑法概要上巻』(青林書院,1995 年)34 頁。

〔10〕 アルビン・エーザー『「侵害原理」と法益論における被害者の役割』甲斐克則編訳(信山社,2014 年)61 頁参照。

序所承认的价值性质。〔11〕而据此形成的法益概念便是“形式的法益概念”，即立法者评价为值得刑法保护，并通过行为规范（犯罪构成要件）之设置从侵害行为中获得保护的法益。其亦被称为“方法论的法益论”，这也是构建现行刑法解释论体系的方法论原理之基石。〔12〕另一方面，既然是立法者基于（刑）法的立场针对实体性利益或价值所进行的“法的评价”，那么，该评价行为就是在确定应该将实在利益或价值中的哪一方面作为法益保护起来。为从此动态的评价过程中获得正当合理的法益概念，也必须要回答“此种利益或价值，为何具有法的承认的必要”；〔13〕为成为刑法的保护法益，“保护客体需要满足何种条件”〔14〕等一系列问题。这便是“实质的法益论”或“体系外的立法批判的”法益概念所关注的问题。其中关于法益概念内涵的宪法论、政策论、社会契约论、风险社会理论等多视角的探讨，便属此论域中的争论。这也就意味着关于“评价客体”的法的评价自身所内含的政治立场、政策性思考对于法益概念的生成将起到关键性作用。

3. 法的实践性，是指法所承认的利益或价值即法益作为刑法的保护目的，具有可通过规范的实践性操作得以实现的可能性。法的世界是当为的秩序、规范的世界，是在经验的自然世界上构筑制度的、法的价值的世界。因此，规范目的或法的价值的实现取决于其是否落实到了制度性规范中，“落实到了制度性规范，价值才参与到‘实在存在’的造化进程。因此，规范伦理学的核心不是描述现实世界的规范，而是‘构建’现实世界的规范，‘为世界立法’。立法的核心就是实现伦理价值从‘应然’（观念性的存在）到‘实然’的转变”。〔15〕“法益”概念也不单纯是抽象的立法者所确定的法规范目的，其必须能够联结法规范世界与现实世界，将法规范的价值实现于现实世界中。有学者称此为“法益概念的具体化功能”，“法益概念只扮演一种中介的角色，承担着抽象规范性理念的具体化功能”。〔16〕“抽象法概念不可能直接与现实世界无缝接轨，只有经由对应于具体事实关系的路径才能落实，而法益原则就是在法概念下的第一线承载了这样的功能，其表述出有关人类行止合法或非法在现象上的连结点。”〔17〕从这一层面上来讲，法益必须要具有“被侵害的可能性”，“成为行为侵害的对象”，从而从法益侵害行为中获得保护，即“基于法益侵害的法益保护”，这也是刑法法益保护原则的要求。

从以上关于法益概念基本构造所必备之三要素即价值实体性、法的评价性、法的实践性的内容探讨中，我们至少可以明确，“法益概念”是一个价值评价性概念，同时又是联结价值世界与现实世界的实践性概念。在这点上，有必要再次强调其与行为客体之间的区别，尽管两者在概念、功能上的区别已成学界共识。但是，正如后所述，当前理论界在探讨“数据权益的刑法保护”问题时，之所以出现混乱局面，其主要原因之一，就是混淆了作为“行为客体”的“数据”与作为“保护客体”的“数据权益”，而后者的具体内容之明确才是我们探讨“数据权益刑法保护”问题的关键之所在。

（二）法益与行为客体的区别及其关联

我国传统理论认为，“犯罪对象（行为客体）是指刑法分则条文规定的犯罪行为所直接作用的

〔11〕 アルビン・エーザー前掲書・85頁参照。

〔12〕 アルミン・エングレンダー「ドイツ刑法学における法益論—批判—考察—」伊東研祐等編者『市民的自由のための市民的熟議と刑事法（増田豊古賀祝賀論文集）』（勁草書房，2018年）3頁参照。另，アルミン・エングレンダー「法益論—刑事政策における判断的基準となりうるか?」小島秀夫訳「大東法学」第71号265頁以下参照。

〔13〕 アルビン・エーザー前掲書・87頁。

〔14〕 アルミン・エングレンダー前掲文・6頁。

〔15〕 邓庆安：《论尼古拉·哈特曼价值论伦理学的典范意义》，载《道德与文明》2020年第5期，第11页。

〔16〕 见前注〔7〕，周漾沂文，第987页。

〔17〕 见前注〔7〕，周漾沂文，第986页。

客观存在的具体人或者具体物”。〔18〕其与犯罪客体的联系在于:“作为犯罪对象的具体物是具体社会关系的物质表现,作为犯罪对象的具体人是具体社会关系的主体或者参加者。犯罪分子的行为作用于犯罪对象,就是通过犯罪对象即具体物或者具体人来侵害一定的社会关系。”〔19〕通说理论的此种表述,可理解为经验世界中具体的人或物是规范价值世界的具体价值关系的承载者,是载体;对于保护客体的侵犯,在这类犯罪中,也一定是现实行为通过作用于价值关系承载者的人或物来实现的。因此,犯罪客体价值层面意义上的侵害性在经验世界中便具有了具体的经验和可感知的物质表现样态,即犯罪结果。然而,对于行为性质的认定起重要作用的并非是经验世界中的物质性结果,而是通过物质性结果所表征的具体价值或利益(“社会关系”——通说)的侵害性,亦即“法益侵害性”。可见,行为针对犯罪对象或行为客体所造成的侵害即外界变动之结果,将构成行为社会危害性或法益侵害性的事实性基础,由此,法益侵害这一价值层面的损坏或侵犯便具有了实体性内容。

其实,自一百多年前德国学者李斯特区分“法益”与“行为客体”,将“法益”带离因果变更可能的经验世界,而只保留“行为客体”于自然因果作用领域并作为因果论的对象,进而导致法益概念的“精神化”〔20〕以来,德国学者为弥补两者之间的割裂所造成的法益侵害性认定上的困难,一直在对其做理论上的修补和完善。因为,一旦“法益”作为保护客体只适用价值关系方法,而有别于纯粹因果论考察方法的“行为客体”,便会产生“因果法则”上变更不能的法益如何证明其被侵害性,进而证明其需要受到刑法的保护这一问题。〔21〕德国学者坚信:“法益保护的必要产生于法益是侵害可能的,因此也被视为是因果的变更可能之时。”〔22〕不可否认,行为是自然界的现象,具有现实性,如何从事实行为中获得法益侵害这一价值判断,从“事实”的认定中完成“价值”评价,实现“事实”与“价值”之间所存在之鸿沟的跨越,一直是理论界在“法益论”上孜孜不倦探讨之永恒课题。因为,学者们担心,在“法益”概念的观念化、精神化、抽象化的理论建构发展脉络下,法益保护思想的贯彻会带来刑罚权的扩张和行为自由的全面丧失,〔23〕而当前的刑罚积极主义倾向更是说明了这一点。〔24〕正如有学者指出,“如果法益保护主义是指仅以法益保护目的为处罚提供正当化的原理,那它也可能是促进处罚范围之扩张与重罚化的原理”。〔25〕同时,法益的过度抽象化,过度强调刑法侵害的非实体性(incorporeality),“直接指向一般所认为的触知不可能的普遍价值,刑法这一武器便具有丧失社会现实必要性的危险”。〔26〕

由此,在“法益”与“行为客体”之区分下,重新建立起两者之间的“某种关联性”,就成为理论谋求刑法谦抑性和最后手段性的路径选择之一。此“关联性”就是指,作为刑法保护客体的“法益”

〔18〕 高铭暄、马克昌主编:《刑法学》(第10版),北京大学出版社、高等教育出版社2022年版,第54页。

〔19〕 同上注,第55页。

〔20〕 クヌート・アメルンク著『法益保護と社会の保護(一)』甲斐克則訳　九大法学第45号231頁。

〔21〕 クヌート・アメルンク著『法益保護と社会の保護(二)』甲斐克則訳　九大法学第46号52頁参照。

〔22〕 クヌート・アメルンク前掲文『法益保護と社会の保護(二)』・61頁。

〔23〕 クヌート・アメルンク前掲文『法益保護と社会の保護(二)』・54頁参照。

〔24〕 日本学者井田良教授在概括晚近日本刑事立法活性化所呈现的“刑罚积极主义”特征时,其中就包括为保护被抽象理解的法益而动用刑法倾向的“法益概念抽象化”特点。此外,还包括“犯罪化”“重罚化”“处罚早期化”特点。井田良「最近の刑事立法をめぐる方法論的諸問題」ジュリスト(No.1369)54頁以下参照。

〔25〕 松原芳博「立法化の時代における刑法学」『立法学のフロンティア3　立法実践の変革』(ナカニシヤ出版,2014年)140頁。

〔26〕 アルビン・エーザー前掲書・112頁以下。

中,必须含有刑法上的侵害所指向的物质性客体,[27]即行为客体。正如日本学者松原芳博教授所言,“法益概念通过与事物和人相联结,与事实和价值相联结,才能为刑事立法提供事实基础和价值正当性”。[28]

此种限缩刑罚的理论路径要求“法益必须借由外显的实体基础予以呈现”,刑法所保护的法益“至少可以透过外显的实体基础加以具体地掌握”。[29] 法益是否受到侵害的判断,“往往是从经验世界的角度观察,而判断的方法则是在于,先行观察实际的(或是潜在的)行为客体是否或如何受到侵害,以此进一步确认法益是否受到侵害”。[30] 据此,当“法益侵害”指的是“某种有价值的东西的破坏危险性或破坏,必须与因违法行为所损伤的物质性客体相关联”[31]时,行为现实地作用于人或物而带来的客观状态之变化,便构成“法益侵害”的事实性基础,也就具有了动用刑罚禁止此行为的正当根据。正如德国学者哈塞默(Hassemer)所言,“仅限于在特定行为‘实际’威胁法益的场合,法益才要求禁止此种行为”。[32]

此种“基于刑罚禁止法益侵害来保护法益”——刑法所特有的法益保护方式表明:“法益”作为侵害客体,在具体各犯罪类型的构成要件中,是通过探讨行为的攻击样态与行为客体之间的交互影响关系实现对法益侵害或威胁之内涵的认定的。因此,在各具体犯罪类型之构成要件的解释和适用中,行为样态(主观面与客观面)—行为客体—保护法益之间相互关联性的把握才是关键。具体而言,例如自然意义上的“人”享有法世界中的诸多权利,不同权利性质同时也决定了“何种攻击行为样态”才是刑罚禁止的对象。如在故意伤害罪与强奸罪中,行为攻击对象同样是自然意义上的“人”,刑法保护“健康权”或“性的自由权”的差异,也决定了二罪名各自的行为方式(具体法益的现实侵害可能性之方式)的不同。[33]

总之,以上关于刑法保护客体之“法益”概念构造及其与行为客体关联性的探讨,将构成本文探讨“数据权益刑法保护”问题的理论基点。作为问题的具体化,接下来需要讨论的是,“数据权益”具有何种具体内涵,其是否具备法益(格)?这也关联到刑法对“数据权益”这一法益特有保护方式的理解上。

三、问题探讨的前提基础:数据与数据权益的内涵

然而,随着互联网技术的发展,进入数字化时代才产生的关于数据的“权益”属性问题之争议,并不能直接从刑法规定或其解释论中获得答案。理由在于,在刑法的“最后手段性”思考下,其并不具有关于数据“权益”内涵及其主体归属的确认功能,即关于数据的确权不是刑法“应有的义务性工作”。换言之,刑法作为“最后手段”(ultimaratio),当其他刑法以外的法或者法以外的社会统

〔27〕 アルビン・エーザー前掲書・112 頁以下参照。

〔28〕 松原芳博前掲文・139 頁。

〔29〕 见前注〔1〕,古承宗书,第 38 页。

〔30〕 见前注〔1〕,古承宗书,第 37 页。

〔31〕 アルビン・エーザー前掲書・111 頁。

〔32〕 8 3 3 1 A B 3 5 8 3 [illegible] 3 8 8 3 3 4 B 9 3

〔33〕 在现实的案件事实中,对于客观上相同行为客体的攻击性行为的实施,其定性尽管离不开“法益”要素的考量,但具体是 A 法益被侵害还是 B 法益被侵害,其认定同样也离不开由行为人的主观面所决定的行为攻击样态。在此种意义上,作为行为侵害对象的具体被害法益,也是行为人主观选择的结果。

制手段不充分时，方可补充性地介入。这便是刑法的谦抑性（补充性）。[34] 这意味着，从刑法的法益保护角度来讲，刑法并非法益保护的唯一手段，“法益”也非刑法领域所特有。刑法的“最后手段性”表明，一般而言，刑法并不创造“法益”并进行保护，而是当其他手段对法益的保护不充分之时，才以补充性方式被适用。“民法或行政法的规制呈现充分之效果时，刑法不应出现。”[35]在关于“数据权益”的刑法保护问题上，也是如此。刑法上“数据权益”内涵的界定，只能依赖或借助于其他部门法先行确认的“数据权益”之内涵，在此基础上，才能论及刑法的“当罚性”与“要罚性”问题。[36]

然而，正当因“大数据时代”的到来，关于“数据”的法律属性、[37]数据与信息的界分、[38]数据的权益确定[39]等问题的法学探讨如火如荼之际，要想脱离刑法学领域，进入本文笔者所不熟悉的其他部门法领域，在汗牛充栋之研究成果中找寻答案，谈何容易，干脆直接承认“能力有限”也许更为坦率！因此，本文只能在“有限能力”下以刑法“法益”理论之视角去往深邃且令人迷茫的“数据”法学领域探寻关于“数据权益”的基本内涵。

（一）数据概念及其与信息的界分

近来，国内有学者做过非常有益的统计，即在我国 305 件法律性文件中，含有“数据”一词的法律文本共计 76 件，其大多集中出现在行政法与经济法领域。[40] 通过对含有“数据”一词的规范条文分析，认为“数据”一词在我国法律文本中主要有以下几种语义类型：（1）对客观事物的记录；（2）现代信息技术中的符号，特指以二进制数据 0 和 1 所标识的信息，需要通过代码技术方可呈现或获取其内容，集中在计算机信息系统保护、网络安全、电子签名等场景中出现；（3）现代信息技术的专称，如“数据库”“大数据”“信息数据系统”等用语。[41] 然而，在这些与“数据”相关的法律文本中，“数据”一词的语义语用却表现出“词性不明”“内涵不清”“外延不定”等特征。[42] 其中，“数据”与“信息”两者的语义内涵更是含混不清，逻辑关系混杂难分，存在着“高度混用的现象”。[43] 尽管此种混乱局面正是引发“学界对二者内涵与关系广泛讨论”的主要原因，但囿于各部门法有其特定的立法目的和法益调整方式，关于“数据”概念之内涵确定统一于各部门法之间几乎不可能。纵观这些理论探讨的背景，不外乎是承认互联网技术的发展导致的“大数据时代”“数字时代”或“数字

〔34〕 曽根威彦『刑法総論』（2008 年，弘文堂）8 頁参照。

〔35〕 井田良前掲書・19 頁。

〔36〕 谦抑的法益保护原则要求，只有在存在重大法益侵害且无法期待其他法规范提供充分的保护之时，基于刑法的犯罪化便成为必要。而“当罚性”与“要罚性”事关犯罪化要件问题，即前者指以行为存在重大法益侵害且值得刑罚处罚为必要，后者指为从当罚的法益侵害或其危险中保护社会，刑罚是不可或缺的手段。山中敬一『刑法総論Ⅰ』（2004 年，成文堂）50 頁以下参照。

〔37〕 参见梅夏英：《数据的法律属性及其民法定位》，载《中国社会科学》2016 年第 9 期，第 164 页以下。

〔38〕 参见彭诚信、向琴：《“信息”与“数据”的私法界定》，载《河南社会科学》2019 年第 11 期，第 25 页以下；梅夏英：《信息与数据概念区分的法律意义》，载《比较法研究》2020 年第 6 期，第 151 页以下；高志宏：《隐私、个人信息、数据三元分治的法理逻辑与优化路径》，载《法制与社会发展》2022 年第 2 期，第 207 页以下。

〔39〕 参见王利明：《论数据权益：以“权利束”为视角》，载《政治与法律》2022 年第 7 期，第 99 页以下；申卫星：《论数据用益权》，载《中国社会科学》2020 年第 11 期，第 110 页以下。

〔40〕 参见张红：《我国法律文本中的“数据”：语义、规范及其谱系》，载《比较法研究》2022 年第 5 期，第 63 页以下。

〔41〕 同上注，第 64 页以下。

〔42〕 同上注，第 65 页以下。

〔43〕 同上注，第 65 页以下。

社会”的到来对原有线下传统社会形态的冲击和挑战，而在法学领域就表现为“现实世界的法律规则与调整虚拟世界的法律规则能否相互接纳、相互调适，还是相互排斥”的问题，民法学者王利明教授直言，“这确实是数字时代的民法面临的重大问题”。〔44〕此言当然亦可直接用于刑法上。因此，尽管“数据”的原始含义单纯指“数字记录”，然而，在前述互联网技术下的“数字时代”（刑）法所面临的重大问题这一前提下，“数据”概念内涵的探讨也应该限定在由“数据、算法与算力三元素构成”的赛博空间或数字社会这一背景之下。〔45〕

1. 技术层面上的“数据”概念

技术层面上的“数据”概念，聚焦于计算机之运算处理层面，是指存在于计算机或网络系统技术中的由0和1表示的二进制码。其是信息存储、传输和处理的形式。有学者根据通信理论将通信系统划分为三个层次，即物理层、符号层（代码层）和内容层，亦将计算机数据划分为存储介质层、数据文件层和信息内容层，并认为“单纯的数据文件属代码层”，其可“非常方便地与物理层存储介质相分离”，同时也与“个人信息的内容层”相区别。〔46〕本文所指的技术层面上的“数据”概念，便是指此代码层的数据文件，其通过代码这一计算机语言，传输和表现信息内容。因此，在计算机或网络空间的世界里，离开代码层的数据，信息将无法生成、储存和传输，也更谈不上对于信息的利用。正如有学者所指出的那样，“数据及其所显示的信息只能在网络中存在”，“没有网络服务提供者的技术支持，数据以及其所承载的信息都将随之消失”。〔47〕

2. 意义层面上的“数据”概念——信息

意义层面上的“数据概念”，关注人所理解可能的数据之意义内容，其是前述技术层面上的“数据”经过计算机处理而获得的、于人而言具有有用（可能）性或价值（可能）性的“情报”或“信息”。〔48〕因此，在计算机数据技术与互联网技术下，技术层面上的“数据”构成计算机信息处理的对象，经过计算机处理而获得的结果便是作为数据所承载之内容的“信息”。而两者的外延范围未必是一致的，因为代码层的数据未必都含有“信息”内容，甚至是于人而言有价值的“信息”。其价值体现在含有“信息”的可能性上。另一方面，作为计算机处理数据之结果——对其所含“内容”的获取及解读，经过人之主观的价值评价活动，“数据”在发挥各种机能和作用的意义上，又具有了作为“信息”的功能。因此，在此种意义上，“信息＝数据＋意义”是数据被赋予现实意义后的映射。〔49〕

3. 数据、信息与法的保护

上述关于“数据”概念的不同解读，对于“法”世界而言，有着非凡的意义。当我们从现实世界通过计算机技术和网络技术进入网络空间中的虚拟世界时，信息的承载者全部都是代码数据形式。离开数据，也就不会存在“信息”，在此种意义上“信息＝数据”。当数据处理者所获取的“信息”具有某种社会性价值，能够被认识为具有作为某种财产加以利用的意义或具有保护必要性时，此“信息”作为信息财产（information asset），〔50〕便具有了法的保护必要性，即可作为“法益”进行保

〔44〕 王利明：《迈进数字时代的民法》，载《比较法研究》2022年第4期，第17页。

〔45〕 参见彭诚信：《数字社会的思维转型与法治根基——以个人信息保护为核心》，载《探索与争鸣》2022年第5期，第117页。

〔46〕 纪海龙：《数据的司法定位与保护》，载《法学研究》2018年第6期，第73页。

〔47〕 见前注〔37〕，梅夏英文，第169页。

〔48〕 夏井高人「情報財—法概念としての意義」明治大学社会科学研究所紀要第52巻第2号（2014年）214頁以下参照。

〔49〕 见前注〔40〕，张红文，第70页。

〔50〕 夏井高人前揭文・215頁以下参照。

护。因此,对于“法”世界而言,数据形式的“信息”内容和价值才是核心和重点。“0 与 1 组成的数据符号难以具有法律意义,具有法律意义的唯有其内容,即信息。”〔51〕

然而,如果仅仅关照“信息”的内容,仅主张只要根据其类型划分在法上进行保护即可,那么,以代码构建的网络空间和虚拟世界,也只是改变了“信息”的承载手段或呈现方式,对于“法”世界而言,其只是一种新类型的现象而已,并未对法规范体系造成冲击,由于线下针对不同的信息类型已经具有相对完备的法保护体系,遵照此法保护体系直接适用于该新类型“信息”即可,也不会出现前述的“重大问题”。

显然,问题出在“信息”的承载者——“数据”及其与“信息”的对应关系上。如果说,“数据”与“信息”之间只有一种即一对一的对应关系,一个数据文件中,只有一种“信息”内容或类型,那么“法”的调整对象只关照“信息”内容或类型方面即可。这与传统法保护方式无异。然而,在万物皆能“数字化”的时代,随着计算机数据处理能力的不断提高,海量数据的收集和分析的新技术正在改变我们的思考方式和生活方式。“大数据”已经成为我们“获得新的认知、创造新的价值的源泉”。〔52〕 由于“大数据的核心就是预测”〔53〕,尤其能够为宏观商业决策提供帮助,“大数据”已经成为商业资本,并创造新的经济价值。〔54〕 海量的“数据”包含海量的“信息”,且这些“信息”内容丰富、类型繁杂,法已“无能为力”去关照每个“数据”背后的每个“信息”并给予相应保护,因而转向对于具有经济价值的“大数据”自身的保护,为数字经济的发展保驾护航,才是上上之策。因此,法律需要为“大数据”赋权或确权,只有这样,才能为权利主体提供切实的法律保护。“大数据的权益”问题已然进入法(益)的世界。

(二)数据权益与《民法典》第 127 条的理解

现在,让我们进入与数据权益相关的《民法典》第 127 条的理解上。《民法典》第 127 条规定:“法律对数据、网络虚拟财产的保护有规定的,依照其规定。”尽管有民法学者认为,此规定是“明确将数据确认为民法上的财产性权益,彰显了人类对数据具有财产属性的基本共识”〔55〕,但主流观点对于其是关于“数据”之权利属性的规定,则持否定态度。如王利明教授认为,“该条虽然将数据规定在财产权之后,但其在性质上是否为财产权,并不明确”,〔56〕而且认为,“该条只是一个引致条款,即将数据的法律性质与保护方式链接到其他法律规范,并宣示了对数据权益应予以保护,但该条并没有对数据的权利属性作出明确规定”。〔57〕 显然,民法学上关于《民法典》第 127 条的此种理解,对于本论题的深入探讨而言,真是糟糕的局面! 因为,从刑法“法益”理论视角上来讲,民法上的“数据权益”之性质及其归属主体的确定是至关重要的。刑法对法益保护有其特有方式,即基于刑罚禁止法益侵害行为来保护法益。因此“数据权益”属性的确认,无论是在“刑法解释论”上基于实质解释方法对犯罪行为性质等的认定,还是在“刑法立法论”上如何为“数据权益”具体刑法保护措施的选定提供实质的正当性根据,都将产生重要影响。

然而,仍有乐观的一面是,从刑法保护的客体——“法益”是价值概念,关注法所保护的“利益”或

〔51〕 见前注〔45〕,彭诚信文,第 117 页。

〔52〕 [英]维克托·迈尔·舍恩博格、柯尼斯·库克耶:《大数据时代——生活、工作与思维的大变革》,盛杨燕、周涛译,浙江人民出版社 2013 年版,第 9 页。

〔53〕 同上注,第 16 页。

〔54〕 同上注,第 8 页。

〔55〕 沈健州:《数据财产的权利构架与规制展开》,载《中国法学》2022 年第 4 期,第 93 页。

〔56〕 见前注〔39〕,王利明文,第 100 页。

〔57〕 同上注。

“价值”这一层面上来讲，本文认为，民法学界关于“数据权益”性质的如下两种探讨模式，对于“数据权益”这一法益内涵的具体化操作还是有所助益的。一是以“信息”为视角，通过信息权益属性及其主体归属的认定，解决“数据权益”问题。可称之为“信息权益”模式。二是以“大数据”为视角，赋予“大数据”自身以独立性的权益性质而不是依附于各种“信息权益”性质，进而区别“数据权益”与其他各种“信息权益”在法律上的性质，赋予其独立保护地位。此种模式可被称为“数据自身权益”模式。

第一种“信息权益”模式，主要是根据数据所承载之“信息”的权益属性及主体归属之确定，并通过“信息权益”的保护间接地保护“数据”。亦可理解为，此种保护模式之所以承认关于“数据”存在保护的必要性，根本目的还在于保护“数据”背后的“信息”权益。由此，“数据”自身无法律属性问题。由于其只是“信息”的承载手段之一，“数据”的法律属性完全依存于“信息”的法律属性。“将数据权属问题归属为传统法律体系中有关信息权益保护范畴，是目前法学界流行的做法。”〔58〕例如，民法学者彭诚信教授认为，“数据、个人信息和隐私在本质上都是信息”。〔59〕数据只是个人信息传播方式的改变而已，“单独的、承载着个人信息或隐私的个人数据仍然没有独立价值；即使有一定的潜在价值，通过个人信息、隐私保护也已经足够，没有将其独立为新的权利客体的必要”。〔60〕因此，在法学规范意义上，与个人相关联，信息就是数据。这样，将会根据个人“信息”的内容如“隐私”“个人信息”等赋予相应的法上的“隐私权”“个人信息权”。

第二种，“数据自身权益”模式。与前述从“信息权益”角度认定“数据”的法律属性不同，此种模式聚焦于“数据”自身的法律属性问题，将“脱离人格权或个人信息保护语境下的数据权概念”，尤其是“企业对其所控制之大数据享有何种利益”〔61〕作为一个独立问题进行探讨。对此，民法学界有学者主张可从财产权角度对企业数据进行确权。例如，前述彭教授就主张“数字社会应然思维模式应该以数据控制者或数据利用者为思考问题的着眼点”，数据控制者层面的“数据”作为大数据时代背景下产生的新的权利客体，因其具有稀缺性、价值性和可交易性而具有了私人财产属性，进而形成“数据财产权”。构成“数据财产权”的数据，尽管也是信息，但必须是经“去标识化”或“脱敏化”处理的无法具体识别信息主体的“信息”，因而“其不再具有任何人格属性，仅具有财产属性，是纯粹的财产权利”。〔62〕

然而，另一民法学者梅夏英教授却认为，“作为整体的企业数据保护属于纯粹的数据问题”，因此，反对从“财产权”角度对企业数据进行确权。〔63〕在梅教授看来，数据问题要解决的是数据的访问和流通秩序，其关注的是网络空间中“数据”的完整性与安全性，“以防止因他人非法访问和攻击而致使自身控制的数据变动或流失”。〔64〕因此，在数字技术之下产生的企业对数据库或巨大数据池的自我控制本身，便构成企业数据的利益形态。“法律对这种控制状态（应）予以尊重和保护。”〔65〕

〔58〕 梅夏英：《企业数据权益原论：从财产到控制》，载《中外法学》2021年第5期，第1190页。

〔59〕 彭诚信、杨思益：《论数据、信息与隐私的权利层次与体系建构》，载《西北工业大学学报（社会科学版）》2020年第2期，第86页。

〔60〕 同上注，第83页。

〔61〕 见前注〔58〕，梅夏英文，第1195页。

〔62〕 见前注〔59〕，彭诚信、杨思益文，第87页以下。

〔63〕 见前注〔58〕，梅夏英文，第1195页。

〔64〕 同上注，第1196页。

〔65〕 但是，梅教授同时也认为，企业对数据的控制事实只能作为一种防御性的“法益”存在，其不享有实体权利，“只是为企业各种实际利益的实现提供一个基础或可能性，故在保护企业数据时将依实际利益被侵害的类型，存在不同的保护方式”。同上注，第1203页以下。

值得一提的是，近来也有民法学者关注在数据的全生命周期即数据的收集、处理、流通、交易、利用等诸多环节，针对不同阶段、不同主体所享有之信息的种类、信息的内容及其法律权利属性，主张数据权益在面对信息来源主体、信息处理主体、信息交易主体、信息利用主体时，会呈现为不同性质的权益，如隐私权、个人信息权、财产权、知识产权等，并以此“权利束”理论解读数据权益的多样性、集合性、复杂性特点。简单讲，根据“权利束”理论，“数据权益”在其形成过程中，混合了个人信息权益、著作权、商标权、专利权、名称权等等不同的权利类型，数据权利不完全是财产权。〔66〕

由此看来，至少在民法学界“数据权益属单一之财产权”这一认知已被打破，学者们逐渐认识到“以数据为载体的数据权益，交叉地分散于网状结构之上，并与其他权利相互联结，形成了独特而复杂的权利结构特征”，因此，“数据实际上是信息之上形成的各项权益的集合”。〔67〕 这也正是《民法典》第 127 条没有对数据权益的法律属性进行明确规定的缘由。

既然《民法典》第 127 条并非是依照“赋权规则”〔68〕的确权性规定，自然也可预见民法学界关于“数据权益”属性的争论仍旧会持续下去。尤其针对企业拥有的大数据，法律应采“数据库保护模式”抑或“商业秘密保护模式”，或者从财产权角度对其进行确权，民法学界更是做了很多理论上有益的尝试，〔69〕而这种“数据权益”内涵的多面性及法学争论持续的现状，也必将使“数据权益刑法保护”问题的探讨陷入“窘境”。这是因为，其一，从“刑法教义学”层面来讲，“数据权益”内涵的多面性，将直接阻碍“数据权益”这一刑法法益概念“体系解释机能”的发挥，无法作为具体罪刑规范的解释原理，为各犯罪构成要件的解释提供依据。其二，从“刑法立法论”层面来讲，正因为“数据权益”概念的抽象性能够包容内涵的多面性，也将导致“体系批判机能”的丧失。〔70〕 因为，“具有单纯概念性质的保护法益无法批判犯罪化是过度的”〔71〕，因此，法益概念的抽象性、模糊性也就意味着法益概念机能的丧失和法益理论的无用。如果欲在“法益”理论层面上深化“数据权益刑法保护”这一问题的探讨，必须要对“数据权益”的内涵进行具体化限缩，明确“数据权益”的具体内涵或权益属性，使其符合刑法上的“法益格”。就现状来看，无论从制度层面还是理论层面，“数据权益”内涵的确定，依旧是悬而未决的问题。

（三）小结

1.数据指计算机或网络空间中的代码，是信息存储、传输和处理的形式。信息指数据所承载之内容或情报，是计算机处理数据之结果，是意义层面上的数据概念。物理层意义上的数据，将构成所有与数据犯罪相关联之法益内容探讨中的行为客体内容。

2.《民法典》第 127 条之规定，并非是关于数据的确权性规定。数据的法律属性目前有赖于理

---

〔66〕 关于数据权益的“权利束”理论研究，见前注〔39〕，王利明文，第 99 页以下；闫立东：《以权利束视角探究数据权利》，载《东方法学》2019 年第 2 期，第 57 页以下。另外，参见许可：《数据权利：范式统合与规范分殊》，载《政法论坛》2021 年第 4 期，第 86 页以下。

〔67〕 见前注〔39〕，王利明文，第 104 页。

〔68〕 赋权规则（Property rule），指通过事前赋予权利，认定对人的法效果。林紘一郎『「個人データ保護」の法益と方法の再検討：実体論から関係論へ』情報通信学会誌 31 巻 2 期（2013）79 頁以下参照。

〔69〕 见前注〔58〕，梅夏英文，第 1190 页以下。此外，从财产权角度进行确权的尝试有“数据资产权”说、“数据所有权与用益权”的分离说、“数据公开传播权”说、“数据块权利”说等，见前注〔58〕，梅夏英文，第 1195 页以下及注〔15〕。

〔70〕 关于法益概念的“体系内在机能”与“体系批判机能”，曾根威彦「現代刑法と法益論の変容」『刑事法学の現代的課題—阿部純二古稀祝賀論文集』（第一法規出版社，2004 年）46 頁参照；同著『刑法原理』（成文堂，2016 年）14 頁以下参照。

〔71〕 8 3 3 1 A B 3 5 8 3 [illegible] 0

论界的解释。

3. 当“数据”的权益属性及主体归属之确定，以“信息权益”之认定为基准时，“数据”作为“信息”的承载者，其法律属性完全依赖于“信息”的法律属性。

4. 大数据时代，考虑到“数据”的价值源于其流通、利用和共享，因此在“数据”全生命周期中，“数据权益”呈现多种权益之集合样态。

5. 在刑法“法益论”意义上，在“数据权益”内涵的具体化操作要求下，民法学上的“数据财产权说”与“数据控制安全说”之争值得关注。但是，按照前述法益概念的基本构造，尽管能够认定“大数据”的价值实体性，但在法的评价性上，法究竟应该关注“大数据”价值实体的哪一面，对其给予何种法律保护，尚不明确。“数据权益”作为刑法保护客体的法益(格)，尚存疑问。

四、问题探讨的理论澄清：数据权益与刑法法益保护论

本文之所以不遗余力大胆深入民法学领域探寻“数据权益”的具体内涵，将讨论范围限缩至“数据财产权”或“数据控制安全”上，着实是因此项工作构成刑法保护客体之“法益”的具体化作业之一部分。因为，当针对具体犯罪构成要件的解释须以该罪的保护法益为指导时，“保护法益的确定一定要尽可能具体化，必须有经验的实在性，而不能过于抽象化和精神化”。〔72〕

问题是，现行刑法有哪些罪名可提供对“数据权益”的直接保护？如果我们必须坚持刑法所特有的法益保护方式——通过设定不法行为类型(具体犯罪构成要件)并通过刑罚对其进行规制来保护法益，对于“数据权益刑法保护”问题的探讨，便始终无法脱离关于实定刑法中具体罪名的实质解释。

其实，此种“刑法解释论”探讨路径重点关照的是现行刑法社会统制的效力边界问题，即在线下传统的现实社会中所创制和运行的现行刑法规范能否规制网络空间这一虚拟世界中的危害行为。当在刑法的世界中，我们必须遵从“罪刑法定主义”这一铁则来探讨针对数据权益之危害行为的刑罚处罚时，如果在既存的罪刑法规中能够找寻到相应的规制罪名自不待言，依此处理即可。但是，往往数字技术的发展所带来的数字犯罪类型行为的更新，会逾越刑法规制所预设之范围，而导致处罚上的空白和规制效力上的丧失。因此，围绕“数据权益的刑法保护”问题在探讨数据权益侵害之犯罪行为的刑法规制时，基于“法的安定性”之要求，刑法必须先在解释论上划定既存刑罚法规之适用边界之后，当该当行为超越刑罚法规所预设之范围时，再转向立法论考量是否增设能够包摄此行为类型的刑罚法规。〔73〕

(一) 关于“数据权益”类法益保护模式的质疑

当前刑法理论界，在关于“数据权益刑法保护”问题的探讨中，有一种理论研究倾向就是：在既有罪名体系中构建“数据权益”的“类”保护体系。即，将“数据权益”视为类法益，但凡现有罪名中的具体法益能够以“数据”形式呈现，便以此作为“数据权益”保护的具有共性的罪名，然后再根据具体法益内容划分刑法保护方式上的类别。

例如，有学者将我国现行《刑法》对个人数据的保护模式归纳为四种：1. 经济秩序保护模式，涉及罪名为“窃取、收买、非法提供信用卡信息罪”(第177条之一第2款)与“侵犯商业秘密罪”(第219条)；2. 人格权保护模式，涉及罪名为“侵犯通讯自由罪”(第252条)与“侵犯公民个人信息罪”

〔72〕 张明楷：《刑法学(下)》(第6版)，法律出版社2021年版，第846页。

〔73〕 渡邊卓也『ネットワーク犯罪と刑法理論』(成文堂，2018年)2頁以下参照。

(第253条之一);3.物权保护模式,涉及罪名为“盗窃罪”(第264—265条)与“诈骗罪”(第266条);4.公共秩序保护模式,涉及罪名为“非法获取计算机信息系统数据罪”(第285条第2款)与“破坏计算机信息系统罪”(第286条第2款)。〔74〕其进而指出,当前刑法保护框架在“数据滥用”“数据泄露”等行为的规制上和“虚拟财产”“数据主体权益保障”上,存在不足之处,并据此提出了若干具体的完善意见。〔75〕

也有学者认为,现行刑法规范保护数据安全,包括如下五种类型:一是,保护计算机管理秩序和网络秩序的刑法规范,涉及计算机信息系统安全和网络安全的规制方面的犯罪类型。前者包括“非法侵入计算机信息系统罪”(第285条第1款),“非法获取计算机信息系统数据”“非法控制计算机信息系统罪”(第285条第2款),“提供侵入、非法控制计算机信息系统程序、工具罪”(第285条第3款),“破坏计算机信息系统罪”(第286条);后者包括“帮助信息网络犯罪活动罪”(第287条之二)。二是,保护政府对网络服务提供者进行监管的秩序的刑法规范。涉及的罪名是“拒不履行信息网络安全管理义务罪”(第286条之一)。三是,保护个人信息的刑法规范。涉及的罪名是“侵犯公民个人信息罪”(第253条之一)。四是,保护国家秘密、国有档案的刑法规范。前者涉及的罪名包括“为境外窃取、刺探、收买、非法提供国家秘密、情报罪”(第111条),“非法获取国家秘密罪”和“非法持有国家绝密、机密文件、资料、物品罪”(第282条),“故意泄露国家秘密罪”“过失泄露国家秘密罪”(第398条);后者刑法规范涉及的罪名包括“抢夺、窃取国有档案罪”(第329条)。五是,保护商业秘密的刑法规范。涉及的罪名包括“侵犯商业秘密罪”(第219条),“为境外窃取、刺探、收买、非法提供商业秘密罪”(第219条之一)。〔76〕

如前所述,在“刑法解释论”探讨路径下,我们需要探讨的是:具体罪名下的具体保护客体即法益有无以“数据权益”为内容,分析哪些具体罪名中的不法行为类型以“数据权益”为直接侵害客体。所以,此种理论探讨路径拒绝在“类保护客体”意义上探讨“数据权益”的类保护问题。因为“同类客体”只具有刑法分则体系的建构意义,〔77〕并无针对分则具体罪刑法规的解释功能。因此,针对此种“类保护模式”的探讨路径,本文拟从“法益论”视角提出如下几点商榷意见:

第一,论证方法上手段与目的的偏离。无论是前者归纳的针对“个人数据”的四种保护模式所涉具体罪名,还是后者总结的关于“数据安全”的五种刑法规范保护类型中所涉具体罪名,无一是把“个人数据”或“数据安全”作为直接保护客体的。换言之,这些既有罪名中具体保护的“法益”与“数据权益”之间并无直接关联。理由很简单,在“数据权益”成为刑法保护问题之前,这些罪名既已存在,而且大多是涉及传统罪名中的信息类相关犯罪,如商业秘密、国家秘密、财产性信息、个人信息等。如果说,这些罪名与“数据”有何关联的话,那也是因为这些罪名保护法益所承载之媒介是“数据”,因有了新的关于信息的“承载”方式而已。因此,相对于犯罪构成的规范意义而言,只能说其是一种新的犯罪现象,是事实层面上的犯罪现象多样性的表现而已,其至多构成犯罪构成事实层面上的问题,不是“规范”层面上关于这些罪名之法益的“数据”保护问题。因此,也不是一个新的刑法规范问题。如果既有罪名不是侵害数据“法益”类型,而仅是使用数据“工具”类型,那么,这些罪名如何为“个人数据”或“数据安全”提供刑法保护,便值得怀疑。用传统罪名论证新的法益——“个人数据”或“数据安全”的保护方式,显然偏离了方向。

〔74〕 参见劳东燕:《个人数据的刑法保护模式》,载《比较法研究》2020年第5期,第39页以下。

〔75〕 同上注,第42页以下。

〔76〕 参见时延安:《数据安全的刑法保护路径及方案》,载《江海学刊》2022年第2期,第146页以下。

〔77〕 见前注〔18〕,高铭暄、马克昌书,第52页以下。

第二，刑法保护方式的误读。在“法益保护目的”思考下，刑法保护方式的提供一定要关照其“最后手段性”。现代“法益”理论的基本逻辑是，只有针对作为保护对象之“法益”直接造成侵害或危险的行为的处罚，才能基于法益论提供正当化根据。〔78〕因此，作为刑法保护方式内容之一的犯罪行为类型（行为规范）的设置，必须要具备“法益关联性”。“因为行为规范是为保护法益而设定的，所以是否违反行为规范的判断，必须是法益关联性的判断。”〔79〕当两位学者在寻求“个人数据”或“数据安全”的刑法保护时，所列罪名中不法行为类型的规制并不能为其提供直接性保护，这显然欠缺与数据权益的“直接关联性”。也许，两位学者就没有在“法益论”层面思考刑法保护问题，也难怪后者指出：“侵犯数据权益的犯罪是一个‘罪群’，在立法表达上应包括多个构成要件，形成多个罪名。”〔80〕前一学者所指的“个人数据”，也让人怀疑其究竟是不是现行《刑法》保护的法益。〔81〕退一步讲，如果是想表达相关的既有罪名“群”是对“数据安全”或“数据权益”抑或“个人数据”提供“间接性”保护，同样也会面临这些抽象的“类”法益也非刑法保护客体的问题。对“类”法益的“间接性”保护，如何实现刑法法益保护机能，更是值得怀疑。例如，当“数据安全”之保障作为2021年颁布的《数据安全法》的立法目的〔82〕时，刑法并不必然会为其提供保护，此立法目的也不能直接成为刑法保护的“法益”。正如有学者指出的那样，“刑法的法益保护功能不能化约为一项纯粹目的性的指导原则，而是更应该作为形塑刑罚最后手段性之实质内涵的准据”。〔83〕

第三，法益层面上“数据”保护与“信息”保护的混淆。关于“数据权益”刑法保护的理论探讨，上述两位学者研究进路的偏差，究其根源在于，其不仅混淆了行为客体层面上的“数据”与“信息”的区别，更是混淆了法益层面上的“数据权益”与“信息权益”之间的区别，进而使数字化社会背景下刑法所面临之新问题的探讨中，不加区分地杂糅进线下传统刑法的旧问题，使问题探讨的理论意义和实践意义大打折扣。法学界但凡谈论“数据”与“信息”的关系时，已形成“数据为信息的载体，信息是数据的内容”的通说共识，应无疑义。〔84〕在依附于计算机而存在的网络空间中，电子数字（数据）与信息的此种区分也只是物理层面的“形式”与“内容”的区分而已。但对于线下的传统刑法而言，尤其是对于作为刑法保护之客体的“法益”而言，其关注的是“信息”背后的“价值”，即信息所含内容给人带来的价值性和有用性，所以其会根据“信息”的不同类型给予不同罪名下的保护。因此，一旦以“法益”视角关注“信息”保护问题，“数据”对于“法益”而言已不重要，其只是“信息”的表现形式。若依两位学者以“秘密型”信息的刑法保护之罪名来谈论“数据安全”的刑法保护或“个人数据”的刑法保护，不外乎仍旧是线下传统刑法中关于个人信息、隐私或商业秘密等相关罪名的探讨而已。这些探讨不仅不能解决关于“数据权益”刑法保护的“新问题”，甚至也毫无关联。也难怪前者在文章最后的“具体保护模式的规范性调整”之建议中，主张增设“关于计算机诈

〔78〕 嘉門優前掲書・70頁参照。

〔79〕 高橋則夫『規範論と刑法解釈論』（成文堂，2007年）8頁。

〔80〕 见前注〔76〕，时延安文，第150页。

〔81〕 该学者从大数据的重要性、价值性中直接推论出“个人数据必然会成为包括刑法在内的法律规制的对象”这一结论，并由此展开论述。见前注〔74〕，劳东燕文，第35页以下。然而，从大数据的重要性、价值性中，并不必然能够推导出“个人数据”就是法益，甚至针对此法益刑法应不应该保护或如何保护的问题。

〔82〕 《数据安全法》第1条：“为了规范数据处理活动，保障数据安全，促进数据开发利用，保护个人、组织的合法权益，维护国家主权、安全和发展利益，制定本法。”

〔83〕 见前注〔1〕，古承宗书，第41页。

〔84〕 见前注〔40〕，张红文，第69页。

骗的犯罪”“独立的关于滥用个人数据的犯罪”，不再以诈骗罪或盗窃罪规制“虚拟财产”。〔85〕这些刑法面临的“新”问题，恰恰反映出当前刑法法益保护体系在数字社会下面临的数据权益保护，已显现出相当“疲软”的状态。

综上，在“法益”层面上，刑法对“数据权益”的保护，只能通过规制直接侵害“数据权益”的行为类型（不法类型）实现，类法益保护模式的探讨，显然脱离了问题的实质。

（二）《刑法》第285条第2款、第286条第2款与“数据犯罪”“数据安全”

目前，刑法理论界另一种理论研究倾向就是主张“数据安全”法益观，并将《刑法》第285条第2款“非法获取计算机信息系统数据罪”与第286条“破坏计算机信息系统罪”第2款视为“数据犯罪”的典型罪名代表。概言之，持“数据安全”法益观学者的基本主张是：狭义的数据犯罪是指以数据为犯罪对象，进而侵害数据安全即数据的保密性、完整性和可用性的犯罪。并且，“数据安全”作为独立于传统犯罪的新兴法益，在我国现行《刑法》中，主要受保护于在罪状描述中直接以“数据”为对象的罪名中。而且，《网络安全法》第10条和《数据安全法》第3条将构成刑法保护“数据安全”的前置法依据。

例如，刘宪权教授就认为，狭义的网络数据犯罪是指直接以网络数据作为行为的作用对象，意在侵害数据保密性（confidentiality）、完整性（integrity）和可用性（availability）的犯罪，即“纯正的”网络数据犯罪。“当前在计算机系统犯罪体系中，用于制裁网络数据犯罪、保护网络数据安全的罪名主要集中于《刑法》第285条第2款非法获取计算机信息系统数据罪以及第286条第2款破坏计算机信息系统罪。”〔86〕但刘教授认为，这两罪有不同的法益保护重点，前罪旨在保障网络数据的保密性；后罪则重在保障网络数据的完整性和可用性。据此，两罪所保护的法益互为补充，基本覆盖了刑法对网络数据法益的全方面保护。〔87〕又如，张勇教授在其发表的《数据安全分类分级的刑法保护》一文中，也明确主张：“本文中的‘数据犯罪’是从狭义层面来理解的，即直接以数据为对象、侵害数据安全法益的犯罪。具体来说，包括《刑法》第285条的非法获取计算机信息系统数据罪、第286条第2款破坏计算机信息系统罪中‘对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作’的规定，但同时，也将其放入数据安全保护的罪名体系中加以认识和把握。”〔88〕再如，杨志琼教授也主张：“数据犯罪是指以数据为对象、侵害数据安全法益的非法获取、删除、修改、增加数据的行为，主要包括《刑法》第285条第2款‘非法获取计算机信息系统数据罪’、第286条第2款‘破坏计算机信息系统罪’。”〔89〕

总之，持“数据安全”法益观的学者在围绕“数据权益刑法保护”问题的讨论中，基本一致认为，《刑法》第285条第2款与第286条第2款所涉两罪名已无力全面维护“数据安全”，因此应关注数据生存周期中的各环节，建立覆盖数据安全全生命周期的“动态的、连续的”刑法防护体系。

然而，关于“数据权益刑法保护”问题，上述基于“数据安全”法益观的探讨，在理论论证层面上依旧存在需要进一步澄清的几个问题：一是，《刑法》第285条第2款和第286条第2款罪名所保护的法益是“数据安全”吗，以致将此两罪名作为“数据犯罪”的典型代表进行探讨？此问题将关系

〔85〕 见前注〔74〕，劳东燕文，第47页以下。

〔86〕 刘宪权：《网络数据犯罪刑法规制体系的构建》，载《法治研究》2021年第6期，第45页。

〔87〕 同上注。

〔88〕 张勇：《数据安全分类分级的刑法保护》，载《法治研究》2021年第3期，第22页。

〔89〕 杨志琼：《数字经济时代我国数据犯罪刑法规制的挑战与应对》，载《中国法学》2023年第1期，第125页。

到在目前的刑法罪名体系中有无罪名为“数据权益”提供直接性保护。二是，数据犯罪概念与数据权益之间的关联性问题。这里涉及作为行为客体的“数据”概念与作为保护客体的“数据权益”概念的界分问题，而这对于界定现象层面上的“数据犯罪”概念与规范层面上的“数据犯罪”概念具有重大意义。三是，“数据安全”是刑法保护的法益吗？这里涉及“形式的法益概念”与“实质的法益概念”的界分问题。此种界分是我们在法益理论层面上探讨“数据权益刑法保护”问题的核心。

1.《刑法》第285条第2款与第286条第2款的保护法益

在关于数据犯罪的理论探讨和司法实践中，《刑法》第285条第2款“非法获取计算机信息系统数据罪”与第286条“破坏计算机信息系统罪”第2款之所以备受关注，无疑是因为这两条文的规定中都有“计算机信息系统中存储、处理或者传输的数据”这一表述。然而，关于这两个罪名的保护客体内容，理论界与实务界的看法却不尽一致。即使是持“数据安全”法益观的学者，究竟应该将这两个罪名视为侵害“计算机信息系统安全”法益的“计算机犯罪”还是与之相区别的侵害“数据安全”法益的“数据犯罪”，其前后的观点表述也不尽相同。

目前的通说观点仍旧认为，非法获取计算机信息系统数据罪的保护客体是“计算机信息系统的安全”，而“破坏计算机信息系统罪”的保护客体是“国家对计算机信息系统的安全运行管理制度和计算机信息系统的所有人与合法用户的合法权益”。〔90〕但是，也有学者认为，第285条第2款是第1款的补充，并将第285条第2款的保护法益具体化为“国家事务、国防建设、尖端科学技术领域之外的普通计算机信息的安全”，而后罪的法益则是“计算机信息系统（正常运行）的安全”。〔91〕

我们知道，第285条第2款“非法获取计算机信息网络数据罪”所规制的行为方式有两种组合方式：一是“非法侵入＋获取”；二是“采用其他技术手段＋获取”。在第一种组合方式中，一般认为，“非法侵入”是指未经授权者或者他人同意，通过技术手段避开或者突破他人计算机信息系统安全防护设置，进入他人计算机信息系统的行为。〔92〕如果结合本条第1款法益的理解，本组合方式——“侵入”计算机信息系统并“获取”计算机信息系统数据——的侵害法益，应该有二：一是计算机信息系统自身安全，二是计算机信息系统数据安全。如果将此两种具体法益内容概括为更为抽象的“计算机信息系统安全”概念，进而如同通说观点那般将此概念解释为本罪的保护法益，尽管针对本罪第一种组合方式而言无可厚非，但是，问题会出现在第二种组合方式上。因为，第二种“采用其他技术手段获取”一般被解释为“主要是指假冒或者设立虚假网站，或者利用网关欺骗技术，行为人并不需要进入他人的计算机信息系统就可获取其他计算机处理、传输的数据信息”。〔93〕故而，此种组合方式并不包含对“计算机信息系统自身安全”的直接侵害。如前所述，刑法的法益保护通过设定具体犯罪构成要件、明确所规制之行为方式来实现，因此，在第二种组合方式中，显然“计算机信息系统自身安全”并非是保护法益。否则，就会导致在通说主张的“计算机信息系统安全”这一法益内涵与刑法所规定的同一犯罪构成要件中行为方式的关联性上，产生偏差，会出现同一犯罪构成不同行为方式保护不同法益的局面。这显然不论是在立法技术上还是在司法适用上，都违背刑法的基本原理。

另一方面，与第1款将计算机信息系统领域限定在“国家事务、国防建设、尖端科学技术领域”

〔90〕 见前注〔18〕，高铭暄、马克昌书，第540页以下。

〔91〕 参见黎宏：《刑法学各论》（第2版），法律出版社2016年版，第362页以下。

〔92〕 参见王爱立主编：《中华人民共和国刑法——条文说明、立法理由及相关规定》，北京大学出版社2021年版，第1090页；陈兴良、刘树德、王芳凯编：《注释刑法全书》，北京大学出版社2022年版，第1581页；喻海松编著：《实务刑法评注》，北京大学出版社2022年版，第1240页。

〔93〕 黄太云：《刑法修正案（七）解读》，载《人民检察》2009年第6期，第17页。

不同，第 2 款规定对于这些重点领域之外的计算机信息系统的“侵入”行为自身，并不进行单独处罚，而是需要进一步实施数据的“获取”行为。这也就意味着对于第 2 款中“侵入＋获取”的行为方式而言，单独的“侵入”行为所侵害的重要领域之外的“计算机信息系统安全”并非是本款主要保护法益内容。由此可以推知，无论是第一种组合方式还是第二种组合方式，第 2 款重点规制的是同样的数据“非法获取”行为，是对“计算机信息系统数据安全”的保护。因此，将本罪法益内涵具体化为“计算机信息系统数据安全”或者前述的“计算机信息安全”更为合理。

《刑法》第 286 条“破坏计算机信息系统罪”第 2 款也同样是将“计算机信息系统中存储、处理或者传输的数据”作为行为客体，但与第 285 条第 2 款所规制之行为方式不同，本罪重点关照计算机信息系统数据的“删除、修改、增加”等操作行为。尽管多数见解认为，与第 285 条第 2 款相同，本罪的保护法益同样是“计算机信息系统安全”，〔94〕但在具体表述中，还是有学者强调其为“维护计算机信息系统的运行安全”或者“计算机信息系统的正常运行”。〔95〕 与此法益内容相关联，作为本罪不法行为类型——计算机信息系统数据的“删除、修改、增加”行为的违法实质内容，就体现为对“计算机信息系统运行安全或正常运行”的侵害。在物理层面上，单纯实施的计算机信息系统数据的“删除、修改、增加”行为，只有在据此造成计算机信息系统的不正常运行时，才构成本罪。2020 年 12 月 29 日发布的最高人民法院指导案例第 145 号（张某某等非法控制计算机信息系统案）也明确指出，通过修改、增加计算机信息系统数据，对该计算机信息系统实施非法控制，但未造成系统功能实质性破坏或者不能正常运行的，不应当认定为破坏计算机信息系统罪。〔96〕 此判决改变以往只关注数据的“删除、修改、增加”行为，而忽略这些行为与系统运行安全（法益）之间的关联性进行定罪的做法，真正实现了通过“计算机信息系统运行安全”这一保护法益来认定行为违法实质的“实质解释论”。

由此看来，尽管《刑法》第 285 条第 2 款“非法获取计算机信息系统数据罪”与第 286 条第 2 款“破坏计算机信息系统罪”中都有关于“计算机信息系统数据”的表述，但两罪的保护法益却不同，前罪是“计算机信息系统数据安全”，后罪是“计算机信息系统运行安全”。因此，后罪在保护客体层面上，也并非像刘教授所言是“数据的完整性和可用性”。从第 286 条第 2 款“破坏计算机信息系统罪”的实质违法层面上讲，尽管能够承认针对数据的“删除、修改、增加”行为同时也是对数据完整性和可用性的破坏，但这种破坏性还只是停留于物理层面，只有通过此物理层面或代码层面的数据完整性或可用性的破坏导致刑法所保护的法益——“计算机信息系统的运行安全”遭受侵害时，数据的“删除、修改、增加”行为才具备本罪的违法实质。本罪中的“计算机信息系统数据”仅具有“行为客体”层面上的意义。由此看来，“破坏计算机信息系统罪”并非是本文论题探讨中在“法益”层面上侵害“数据权益”的“数据犯罪”。

那么，学者们为何把不是将“数据安全”作为保护客体之法益的“破坏计算机信息系统罪”也视为“数据犯罪”呢？问题就出在“数据犯罪”的概念上。

2.“数据犯罪”概念之界定——作为“行为客体”的数据与作为“保护客体”的数据权益的二分

当前理论界，关于“数据犯罪”的名称或具体内涵之表述，可谓五花八门、莫衷一是，甚至同一

〔94〕 见前注〔93〕，黄太云文，第 17 页。此外，参见刘宪权：《数据犯罪刑法规制完善研究》，载《中国刑事法杂志》2022 年第 5 期，第 22 页以下；杨志琼：《我国数据犯罪的司法困境与出路：以数据安全法益为中心》，载《环球法律评论》2019 年第 6 期，第 153 页。

〔95〕 见前注〔72〕，张明楷书，第 1372、1376 页；见前注〔92〕，王爱立书，第 1099 页。

〔96〕 参见张某某等非法控制计算机信息系统案，最高人民法院指导案例第 145 号（2020 年）。

学者前后发表的论文中，对其名称或内涵的界定也不尽相同。

在名称上，多数学者使用“数据犯罪”〔97〕一词，但也有学者使用“网络数据犯罪”〔98〕或“数据安全犯罪”〔99〕一词。而关于“数据犯罪”的定义，则可从两个维度考察：一是广狭义维度；二是繁简维度。目前，学界普遍将“以数据作为犯罪对象或犯罪工具的犯罪”视为广义的数据犯罪概念，而狭义的数据犯罪概念仅指“以数据为犯罪对象的犯罪”。与广狭义维度只是在犯罪对象或犯罪工具上界定“数据犯罪”概念的过于“简单形式”不同，也有学者在其概念内涵的表述中增加“法益侵害”内容使之更加明确。如前述持“数据安全”法益观的杨志琼教授就指出，如果将所有“数据”表征的法益侵害行为都认定为“数据犯罪”，便会导致数据犯罪内涵过广。“数据犯罪的概念界定应突出其立法规范目的及保护法益，即在不法侵害数据的事实中区分传统犯罪行为和新型犯罪行为，以寻求更明确的数据犯罪构成要件。”据此，杨教授主张应采用“狭义‘数据犯罪’概念以限缩研究范畴，即将‘数据犯罪’限定为以数据为对象、侵害数据安全法益的行为”。〔100〕

由此可见，无论上述何种形式的“数据犯罪”概念，在强调数据犯罪以数据为犯罪对象这点上却保持了一致性，“数据犯罪”的核心是以数据为犯罪对象这一点看似已达成共识。正如有学者所指出的那样：“理论上以数据为对象实施的犯罪统称为数据犯罪，数据犯罪已然成为各个法域的规范重点。”〔101〕

然而，围绕“犯罪对象”界定数据犯罪概念，同时据此展开关于第 285 条与第 286 条相关罪名的“法教义学”解读，这显然在“刑法解释论”层面上存在对基本概念的误读。即，在“刑法解释论”层面上，应该关注的是“数据犯罪”概念的规范意义，而非其事实特征。

“刑法解释学以解释现行刑法为主要任务”〔102〕，并“通过解释现行刑法的规范意义”〔103〕建构刑法知识体系。这是因为，法教义学立场必须坚持法与法学的规范性。法教义学活动是围绕法律规范展开的规范性活动，其以法律规范为出发点，展开解释、建构与体系论操作。〔104〕 由此，在刑法解释学上，犯罪概念规范意义的把握与揭示才是核心。刑法作为法规范之一种，刑法规范的设置最终要服务于刑法的任务即法益保护，因此刑法上犯罪的核心要素不仅包括“行为规范违反”还应包括“法益侵害”〔105〕，“刑法解释学”也应该在行为规范违反与法益侵害的关联性上理解“犯罪概念”。

如果说，在刑法上“数据犯罪”的规范意义在于强调其通过数据犯罪的规制实现对“数据权益”

---

〔97〕 参见于志刚、李源粒：《大数据时代数据犯罪的制裁思路》，载《中国社会科学》2014 年第 10 期，第 100 页以下；马微：《理念转向与规范调整：网络有组织犯罪之数据犯罪的刑法规制路径》，载《学术探索》2016 年第 11 期，第 84 页；见前注〔94〕，杨志琼文，第 151 页以下；见前注〔89〕，杨志琼文，第 124 页以下；前注〔94〕，刘宪权文，第 20 页以下；见前注〔88〕，张勇文，第 17 页以下；孙道萃：《数据犯罪刑事合规治理的边界》，载《西南政法大学学报》2022 年第 6 期，第 55 页以下。

〔98〕 见前注〔86〕，刘宪权文，第 44 页以下。

〔99〕 参见王倩云：《人工智能背景下数据安全犯罪的刑法规制思路》，载《法学论坛》2019 年第 2 期，第 27 页以下。

〔100〕 见前注〔89〕，杨志琼文，第 125 页注 4。

〔101〕 童德华、王一冰：《数据犯罪的保护法益新论——“数据内容的保密性和效用性”的证成与展开》，载《大连理工大学学报(社会科学版)》2023 年第 3 期，第 54 页。

〔102〕 见前注〔2〕，张明楷书，第 3 页。

〔103〕 曾根威彦『刑法総論』(第四版・有斐閣，2008 年)3 頁。

〔104〕 参见雷磊：《法教义学的方法》，载《中国法律评论》2022 年第 5 期，第 80、81 页以下。此外，参见[德] 托马斯・M. J. 默勒斯：《法学方法论》(第 4 版)，杜志浩译，北京大学出版社 2022 年版，第 481 页以下。

〔105〕 高橋則夫前掲書・11 頁以下；8 [illegible]

的保护，那么，理论上“数据犯罪”概念的界定，也应该关照此刑法的规范意义，即其核心是对“数据权益”这一法益的侵害。一旦在“犯罪对象”（行为客体）层面把握“数据犯罪”概念，鉴于在理论上“犯罪对象”作为法益这一刑法保护客体的承载者，仅仅指经验世界中的具体人或物，将导致所界定的“数据犯罪”概念也只是经验现象层面上的事实概念，而非（刑法）规范意义上的概念。由此导致的结果就是，但凡将“数据”作为犯罪对象且犯罪样态呈现为数据被侵害的犯罪现象都将被作为数据犯罪来看待。因此，我们不难理解为何有些学者把无论是在刑法规定上将“数据”作为罪状内容描述的罪名还是在经验事实上将“数据”作为犯罪对象实施具体攻击的犯罪现象均作为理论上的“数据犯罪”进行探讨。这也是目前理论界在数据犯罪理论探讨上乱象丛生的主要原因之一。

诚然，学者从何种立场及关注“数据犯罪”哪一方面界定其概念内涵，实属其学术研究上的自由。但是，前述持“数据安全”法益观的学者断然肯定《刑法》第285条与第286条相关罪名属于“数据犯罪”，无非是因为这些条文中作为犯罪对象出现的“计算机信息系统中存储、处理或者传输的数据”这一用语，与其在理论层面上事先预设的将数据作为犯罪对象的数据犯罪概念相吻合，并非是通过对罪名的规范目的即所保护法益之内涵的探寻来把握和归类罪名性质。当《刑法修正案（十一）》所增设之罪名“危险作业罪”与“妨害药品管理罪”中分别出现“篡改、隐瞒、销毁其相关数据”“提供虚假的数据”等内容时，有学者更是将这两个罪名也纳入刑法对数据直接保护的罪名体系中，并认为这是直接以数据为对象的刑法规制体系的扩张，是“由妨害社会管理秩序罪向危害公共安全罪和破坏社会主义市场经济秩序罪延伸”。〔106〕然而，可以肯定的是，刑法规制范围的扩张，首先取决于刑法意欲保护的法益的性质和内容，甚至关系到“数据权益”内涵的抽象化程度，而非依赖于“数据”自身。在这两个罪名中，“数据”作为犯罪对象也只具有保护客体的物理承载功能，并不为本罪的实质违法提供任何根据性担保。很显然，不能单纯以法条中的“数据”这一用语，便直接断定该罪名属“数据犯罪”，是对“数据安全”法益的保护。

总之，作为犯罪对象（行为客体）的“数据”与作为保护客体之法益的“数据权益”的界分，也提醒我们注意在理论层面上需要区分事实现象层面上的“数据犯罪”概念与刑法规范意义上的“数据犯罪”概念。如前所述，关于“数据权益刑法保护”问题的“刑法解释论”探讨路径，就是在探寻目前刑法规范提供的罪名体系中有无直接将“数据权益”作为保护客体的犯罪类型。理所当然，《刑法》第285条与第286条相关罪名是否属于“数据犯罪”，也应该从这些罪名的保护客体是否为“数据权益”这一法益论视角进行探讨。

3.“数据安全”法益——形式的法益概念与实质的法益概念的区分

如果我们承认并遵循“刑法的任务是法益保护”这一命题，那么“法益”概念及功能的明确必然构成我们探讨“数据权益刑法保护”问题的理论基点。如前所述，“法益”概念，在理论层面上可划分为“形式的法益概念”与“实质的法益概念”。形式的法益概念是指立法者通过在成文法中设置犯罪构成要件而意欲保护的法益，据此提醒司法者在法适用中要格外关注立法者所设定的保护对象。而且，此概念具有犯罪构成要件体系化及其解释的工具功能。实质的法益概念则关注法益的实质内容，据此为合理的刑事立法划定界限，为刑事立法者提供刑事政策上的指引。此概念则发挥立法批判功能。〔107〕

---

〔106〕 于改之：《从控制到利用：刑法数据治理的模式转换》，载《中国社会科学》2022年第5期，第57页。

〔107〕 アルミン・エングレンダー前揭文・「法益論—刑事政策における判断の基準となりうるか?」265頁以下参照。另外，参见[德] 阿敏·英格兰德：《通过宪法振兴实质的法益论?》，马寅翔译，载赵秉志等主编：《当代德国刑事法研究》第1卷，法律出版社2017年版，第94页以下。

在前述持“数据安全”法益观的学者一方面以“数据安全”法益解释第285条第2款与第286条第2款并认定两罪是“数据犯罪”的同时，另一方面又以“数据安全”法益概念的全新解读批判当前数据犯罪刑事立法和相关司法解释的缺陷，进而以完善数据安全刑法规制之名发表具体立法意见的理论探讨路径中，显然，“数据安全”在此既是“形式的法益概念”又是“实质的法益概念”，同时发挥着“体系内的刑法解释机能”和“体系外的立法批判机能”。在这里，作为法益概念，“数据安全”的内涵界定将是至关重要的。因为这将直接关系到法益概念这两项功能能否发挥的问题。

关于“数据安全”概念，在制度层面上，主要涉及《数据安全法》和《网络安全法》。其中，《数据安全法》第3条明确规定：“数据安全，是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。”《网络安全法》第76条第2项则明确规定，网络数据的保密性、完整性和可用性构成网络安全的内容，通过防范针对网络的攻击、侵入、干扰、破坏和非法使用等行为，保障网络数据的安全。基于此等立法规定，理论界普遍主张“数据安全”包含三要素：数据的保密性、完整性和可用性。〔108〕近来，也有学者将此“数据的保密性、完整性和可用性”意义上的“数据安全”视为狭义的“数据自身安全”。除此之外，“数据安全”概念中还包括“数据利用安全”，具体包括“数据收集安全”“数据处理安全”和“数据使用安全”，确保数据大规模流动、处理、使用过程中风险的“可控性”。〔109〕

然而，有疑问的是，此种来源于《刑法》之外的“数据安全”概念究竟能否作为刑法中的法益概念而发挥相应的“解释功能”和“批判功能”。

首先，“数据安全”若要作为“形式的法益概念”，为《刑法》第285条第2款和第286条第2款的实质解释提供方法论上的指导，那么只能通过对这两个条文进行解释而实现。换言之，刑法规范的具体条文之解释，是探寻该规范目的——保护法益之内涵的唯一有效途径。

这是因为，基于罪刑法定原则与刑法谦抑性的要求，刑法对法益的片段性保护在分则中体现在各犯罪类型中有关法益侵害的结果与行为样态的规定中。因此，对个别的具体犯罪类型即具体犯罪构成要件的解释，必须以该罪的保护法益为指导，“在解释任何一个犯罪的构成要件时，首先必须确定该罪的保护法益”〔110〕。然而，个别的具体犯罪类型中的保护法益，却未必时常明确，需要对具体条文进行解释来获取。“在各具体刑罚法规的保护法益不明确之处（条文并未明确记载），则需要通过刑罚法规之解释明确。”〔111〕正如有学者指出的那样，刑法各论的研究在终局上也是关于个别犯罪构成要件解释的方法论。〔112〕本文无意在此深入展开探讨解释方法论问题，只是想强调“在刑法领域，由于罪刑法定原则的存在，文义射程即具有了决定性意义”〔113〕。“文义”才是每次解释活动的出发点，如果法的文义明确并且可通过其直接获知规范目的（法益内涵），“立法者的明确规定将优于法学的专业概念”〔114〕。关于第285条与第286条相关罪名的理解和解释，亦应如此。

---

〔108〕 参见杨志琼：《非法获取计算机信息系统数据罪“口袋化”的实证分析及其处理路径》，载《法学评论》2018年第6期，第167页以下；见前注〔94〕，杨志琼文，第159页以下；见前注〔86〕，刘宪权文，第45页以下；见前注〔88〕，张勇文，第19页以下。

〔109〕 见前注〔89〕，杨志琼文，第132页。

〔110〕 见前注〔72〕，张明楷书，第845页。

〔111〕 井田良『講義刑法学・各論』（有斐閣，2016年）6頁。

〔112〕 山中敬一『刑法各論』（成文堂，2005年）序論1頁参照。

〔113〕 见前注〔104〕，托马斯・M. J. 默勒斯书，第195页。

〔114〕 同上注，第197页。

具体而言，在方法论上，《刑法》第285条第2款“非法获取计算机信息系统数据罪”与第286条第2款“破坏计算机信息系统罪”的保护法益是否为“数据安全”，首先应该通过对这两个条文的解释来明确。针对“计算机信息系统中储存、处理或传输的数据”，立法者通过不同条款具体设置“侵入＋非法获取”行为或“删除、修改、增加”行为构建不同的构成要件内容，以不同罪名进行规制，究竟要实现何种规范保护目的，是对“数据自身安全”的保护，还是对“数据”所承载之“计算机信息系统安全”的保护，都需要我们首先从条文规范内部中探寻。

在前述关于第285条第2款“非法获取计算机信息系统数据罪”与第286条第2款“破坏计算机信息系统罪”保护法益的探讨中，本文指出尽管两罪名共同规定有“计算机信息系统中储存、处理或传输的数据”这一内容，但第286条第2款之罪名所保护的法益却是“计算机信息系统的运行安全”。“数据”在此条款中仅具有“犯罪对象”功能，而不具有作为犯罪客体的“法益”功能，因此本罪也不是保护“数据安全”法益的犯罪。

接下来的问题就是，第285条第2款所保护的“计算机信息系统数据安全”这一法益与“数据安全”法益是否具有同一内涵，进而能否肯定该罪是对“数据安全”法益进行保护的“数据犯罪”。这里涉及《刑法》第285条第2款中的“数据”与《网络安全法》或《数据安全法》中的“数据”在概念层面上是否同一的问题。

众所周知，《数据安全法》第3条规定中的“数据”指任何以电子或者其他方式对信息的记录。而《网络安全法》第76条第4项规定的则是“网络数据”，是指通过网络收集、存储、传输、处理和产生的各种电子数据。显然，从具体定义上看，《数据安全法》中的“数据”比《网络安全法》中的“网络数据”内容要广，“较诸《网络安全法》第76条项下‘网络数据’，《数据安全法》不但包括通过网络收集、存储、传输、处理和产生的‘网络数据’，也涵盖了线下的电子数据”。〔115〕相较于这两部法中的“数据”，《刑法》第285条第2款规定中的数据仅指“计算机信息系统中储存、处理或者传输的数据”，其不仅依托于“计算机信息系统”而存在，内容上也仅限于“用于确认用户在计算机信息系统上操作权限的数据”，因此不仅在外延上，而且在内容上也要远远窄于前两部法中的“数据”。由此看来，囿于刑事立法当时技术上的局限，刑法上的“数据”范围基本与计算机系统的边界保持一致，“信息系统”的概念扩张自然而然地也等同于“数据”的范围扩张。〔116〕刑法上的“数据”因立法上的缘故自始无法摆脱“计算机信息系统”这一枷锁的框定与束缚。

显然，与《网络安全法》维护网络运行安全过程中对于网络数据安全即数据的保密性、完整性与可用性的保护这一宗旨不同，《刑法》第285条第2款“非法获取计算机信息系统数据罪”的保护法益也仅限于与“计算机信息系统”相关联的“数据”的安全。其也不同于“旨在为电子数据确立基础性的安全规则”〔117〕的《数据安全法》的立法宗旨。

如果，持“数据安全”法益观的学者关注的是《网络安全法》上“网络数据安全”的刑法保护问题，在刑法解释论上，除重新解释第285条第2款中“数据”概念的内涵外，别无他法，即将《刑法》中的“计算机信息系统中储存、处理或传输的数据”这一用语内涵“扩张解释”至包含“网络数据”，进而在司法实践中将第285条第2款“非法获取计算机信息系统数据罪”与第286条第2款“破坏计算机信息系统罪”适用于与所有“数据”类型相关的侵害行为之处理上。确实，数字化时代，随着网络技术的迅猛发展与日新月异，大数据与云计算技术的出现，网络空间数据已经成为一个国家的

〔115〕 许可：《数据安全法：定位、立场与制度构造》，载《经贸法律评论》2019年第3期，第55页。

〔116〕 见前注〔97〕，于志刚、李源粒文，第107页以下。

〔117〕 见前注〔115〕，许可文，第56页。

基础性战略资源，也成为企业重要的生产要素。不依托于“计算机信息系统”而存在的“网页浏览记录、下载记录、关键词搜索记录等信息数据、云端的网络数据、大数据技术利用传感器获取的海量数据等”，在其共享或获取的过程中，数据的控制者、利用者和储存者如何主张权利，当其权利受到侵害时，刑法应该如何给予保护和应对均尚未有明确的答案，网络数据安全刑法保护的现实必要性和需求性已然凸显。

于是，我们看到，司法机关一方面通过规范性文件如2011年两高《关于办理计算机信息系统安全刑事案件应用法律若干问题的解释》扩张“计算机信息系统”和“计算机系统”的概念内涵，实现数据种类和范围的扩张；另一方面，在第285条第2款与第286条第2款的具体适用中，甚至突破法条文中“计算机信息系统”这一用语对“数据”范围认定的束缚，但凡涉及以“数据”为对象的危害行为，都可能成为“非法获取计算机信息系统数据罪”与“破坏计算机信息系统罪”的适用案件，这两罪最终也沦落为“口袋罪”。对于此种司法现象，正如有学者评价的那样，“在立法尚未积极作出回应前，为避免处罚漏洞，理论界和实务界多主张侵害计算机信息系统安全类犯罪的保护法益是数据安全，进而基于保护法益的目的，对数据内涵及其载体范围进行扩张解释，即突破刑法规定的‘计算机信息系统’‘计算机系统’的用语限定，将作为此类犯罪对象的数据扩大到一切数据。此种基于回应社会生活需要的客观目的论解释立场，一方面使得数据利益不再依附于计算机信息系统安全，实现了对数据法益的独立保护；另一方面通过扩张解释，侵害计算机信息系统安全的犯罪成为兜底条款，实现了对数据法益的补充性保护”。〔118〕

然而，在本文看来，基于客观目的论解释立场对《刑法》中的“数据”概念进行“扩张解释”，据此使第285条第2款与第286条第2款满足网络数据安全刑法保护的现实需求，此等以“应对新事态的刑事立法之缺陷为前提，基于解释补充立法，无异于违反罪刑法定主义之精神的解释论的自杀”。〔119〕诚然，“唯有目的性的论证方法，能够使法律与时代融合在一起”〔120〕，法律解释原则上也应以法律最能实现解决当前冲突的功能方式进行，使其适应社会状况。但是，不能对法官的“法律现代化机能”毫无限制。〔121〕尤其在刑法领域中，因罪刑法定原则之缘故，文义射程具有决定性意义，文义射程决定着犯罪构成的适用对象及其范围。在基于文义解释能够获得明确的规范目的之处，法官不能以“社会情势发生变化”为由，单靠打击和预防犯罪的现实需求这一刑事政策之目的掩盖立法原意，为刑罚的扩张处罚提供实质根据。此种因技术发展带来的立法滞后和“入罪漏洞”“可能违反了一般性的正义观念，但也不得不为人容忍，它仅仅可以构成启动立法改革的事由”。〔122〕

上述的详细论证和分析，无非是想指出：如果我们是基于数字化时代探讨大数据和云计算技术带来的网络空间数据的安全性保护问题，《刑法》第285条第2款和第286条第2款之规定，并不能提供刑法层面的保护。基于《网络安全法》和《数据安全法》建构的“数据安全”法益，不仅不能为这两罪名的实质解释提供方法论指导，也无法作为“形式的法益概念”发挥“体系内解释机能”。

另一方面，“数据安全”如何作为“实质的法益概念”发挥“体系外的立法批判功能”更是值得怀疑。换言之，来源于刑法之外的“数据安全”概念能否作为刑法的保护客体，为刑事立法的正当性

〔118〕 见前注〔106〕，于改之文，第61页。

〔119〕 山中敬一前掲書『刑法各論』・序論2頁。

〔120〕 见前注〔104〕，托马斯・M. J. 默勒斯书，第257页。

〔121〕 参见[奥] 恩斯特・A. 克莱默：《法律方法论》，周万里译，法律出版社2019年版，第110页。

〔122〕 见前注〔104〕，托马斯・M. J. 默勒斯书，第210页。

提供实质根据，在“法益论”层面上，仍有待进一步论证。

如前所述，无论是《网络安全法》第72条第2项关于“网络安全”的定义还是《数据安全法》第3条关于“数据安全”的定义，“安全”均重点指称某种“状态”和“能力”。而此种“状态”的维持和“能力”的保障，也都依赖于技术上“必要措施”的采取。由此看来，数据“安全”只是客观的事实状态而已，是计算机信息系统或网络系统相关操作规则被遵守的结果状态。如果将“数据安全”这种客观状态作为刑法的保护目的，违法的实质判断必然将落在行为规范（技术操作规则）的违反上，最终成为由刑罚保障“行为规范的效力”，而“数据安全”只是此规范效力被遵守后反映出的客观效果而已。据此，我们看到，在“数据安全”法益观下，违法判断的核心除了“侵入”“删除”“修改”“增加”等数据侵害行为之外，根本无法判断这些行为因为具体侵害到了什么样的数据利益而被作为犯罪处理。因为单纯这些行为的实施，便是对“数据安全”的侵犯，刑法最终也就成为具体网络操作规则或网络秩序的“守护神”，成为“秩序违反法”。也许这正是“数据安全”法益观下，刑法作为安全保障之手段的必然归结。如此一来，刑法法益保护的“最后手段性”或者“补充性的法益保护”思想将荡然无存。由此看来，“数据安全”能否成为刑法法益本身就成为问题，也就更谈不上“立法批判功能”的发挥问题。

在数字化时代，没人否定大数据的应用价值和其所带来的巨大利益，但并不能由此就一定得出“数据安全”就（应该）是刑法的保护法益的结论。这里需要明确如下几点：首先，维护数据安全的必要性来自数据自身的价值和利益，因此“安全”的概念自身并不具备价值的实体性，其只是表象法益而已。〔123〕 其次，在法益层面上，刑法关注的是大数据自身的价值或利益的保护问题。因此，重点是：“在什么样的特定条件下，这些被发现的财产或者说利益可以通过禁令来保护，并且它们的稳定状态可以通过刑罚防御来维护。”〔124〕最后，刑法应该始终秉持法益保护的最后手段性或补充性，这里要求“大数据价值”需要事先得到其他法的确权即上升为“法所保护的利益”之后，才有资格获得刑法的保护。

五、结语：数据确权的期待与刑法谦抑原则的遵守

总之，“数据权益的刑法保护”问题的理论探讨，首先，依赖于民法上的“数据权益”内涵的明确与法律属性的确定。其次，在刑法上，谦抑性的“法益保护原则”之坚守，在立法政策上要求对“数据权益”是否具备作为“预防性现代刑法”之保护法益的资格问题进行理论层面上的论证。不仅如此，更为重要的是，在立法技术上，刑法的法益保护是通过设置犯罪构成要件、规制不法行为类型来实现的。由此，各具体犯罪构成要件之设置的规范保护目的就成为判断行为之违法实质内容的根据。因此，在刑事立法上，对于何种行为类型的刑法规制才能够有效地保护“数据权益”，更应该深入考察行为法益侵害性的事实特征和规范特征并澄清两特征之间的关联性。因此，在“数据权益刑法保护”问题的探讨上，目前仍旧面临如下两个基本理论难题。

一是，与数据确权相关联的刑法保护目的的确定问题。数字经济的发展首要解决的便是数据确权问题。数据权益的法律属性之确定是促进数字经济发展，发挥数据市场要素功能的法律保

〔123〕 参见周漾沂：《重新理解抽象危险犯的处罚基础——以安全性理论为中心》，载《台大法学论丛》2019年第109期，第181页。

〔124〕 ［德］伊沃·阿佩尔：《通过刑法进行法益保护？——以宪法为视角的评注》，马寅翔译，载前注〔107〕，赵秉志等书，第73页。

障。刑法在诸项法律制度中作为最后手段性的保障法，数据确权不仅关系到刑法保护之法益类型的确定，也将决定着数据权益侵害行为类型即犯罪构成要件的设定问题。因此，与数据确权相关联，在刑法理论上首先需要澄清的是，数据确权后的权利属性是否为新兴权利。如果确权后的权利属性之相关刑法保护，在现行刑法原有罪名体系中存在可提供保护的犯罪类型，那就意味着在理论层面上无须进一步论证数据权益的刑法保护必要性以及侵害行为类型的设置与刑罚处罚能否有效保护数据权益等一系列与立法上的“比例原则”相关的问题。这时，“数据权益的刑法保护”在规范意义上并不构成新的理论问题，其只是与现有罪名的刑法解释论或刑法适用论相关联。例如，如果承认数据的“财产权”属性，于刑法而言，基于传统物债二分和物权理论建构的财产犯罪体系，能否有效保护“数据财产权”便成为问题。如果说，传统财产犯罪的实质危害表现为对他人之物的排他性占有的侵害，那么以无体的信息内容和数字化载体为基本构成要素的“数据财产”之侵害的具体表现是什么，其与传统财产犯罪之违法实质是否一致，首先涉及的便是财产犯罪的解释论或者说适用论问题。然而，数据确权并不意味着确权后的数据权益当然性地能够成为刑法保护的目的，其是否符合刑法保护的法益格，仍需给予立法上的评价，理论上更是应该给予关于法益评价基准的合理论证。

二是，与数据权益之侵害相关联的行为规制范围的确定问题。如果我们仍旧遵循关于犯罪本质的法益侵害说，认为通过刑罚所禁止的行为类型必须具有法益关联性，那也将意味着刑法只能通过规制具有法益侵害或危险的行为实现有效的法益保护。因此，与法益内容相关联，行为的方式或样态所具有的法益侵害的一般危险性之事实面的经验考察将是至关重要的。这也是刑法“行为原则”的要求。例如，当我们在刑法上把行为概念界定为人的身体的举动，进而根据现实的事实行为类型和具体样态在财产犯罪中划分出不同的犯罪类型时，窃取行为、抢劫行为、诈取行为、抢夺行为等具体行为样态便构成划分财产犯罪类型的核心要素之一。刑法作为当为之秩序，是在现实世界之上构筑法的价值世界。因此，对于现实世界运作机理的准确把握和认知，是我们实现刑法价值的必要条件。刑法为实现法益保护目的所发挥的行为规制机能，须以人的行为的事实基础为前提。问题是，当我们构建出由计算机技术和“数据、算法与算力”三元素组成的虚拟网络空间之后，现实世界的刑法行为原则如何在虚拟网络空间中得到贯彻和实现，以及现实世界的刑法规则与虚拟世界的技术规则之间如何调适，也将构成一个重大问题。例如，针对网络数据，基本的计算机操作行为均表现为侵入、复制、增加、修改、删除或爬取等，且这些操作行为自身带有浓厚的中立性质。因此，我们能否像现实世界按照行为样态或方式划分不同犯罪类型那样，在虚拟的网络世界中，也按照网络侵害行为类型划分出不同的网络数据犯罪类型，更是怀有疑问。因为，所有的网络数据犯罪类型都有其共同的事实基础，那就是相同的技术层面上的操作行为和物理层面上的作为载体的“数据”。因此，在数据犯罪的认定上，上述中立性质的操作行为与法益侵害之间的关联性并非像现实世界的犯罪行为类型那样明显和明确，导致在立法技术上，通过法益侵害行为的规制实现数据权益的保护这一目的，更加困难。总之，刑法并不保护也不应保护技术层面上为保障数据的完整性而采取的各项技术性保护措施自身，进而也不应该将单纯的技术性保护措施的违反行为作为犯罪处理。

本文将分析重点聚焦在立法论与解释论均无法回避的首要议题——“法益”保护论上。据此，可以认为，与“数据权益刑法保护”问题相关联，构建数据犯罪的刑法规范体系，基本上就是关于法益保护论在数据犯罪或数字刑法问题上的具体适用和贯彻的问题。唯有精准把握数据犯罪之保护法益即“数据权益”的应有内涵，才能准确掌握相关罪刑规定的正当性，并以此为基础展开后续的刑法归责议题。从目前刑法理论界的讨论状况来看，由于没有厘清“行为客体”与“保护客体”即

“法益”两者不同的规范定位及功能，导致在理论研究和探讨上，既没有区分物理层面上的“数据”完整性与规范层面上的“数据权益”；亦没有区分作为犯罪现象层级的“数据犯罪”概念与作为（刑）法规范意义的“数据犯罪”概念，最终导致其理论探讨欠缺如下最为关键性的法理论证，即“数据本身内含有何种价值以及其价值对于社会秩序究竟有何意义而值得刑法保护”。而这种理论认识的不足与欠缺，在司法实践中直接导致将物理层面上的“数据完整性”的破坏作为保护客体即法益之侵害来看待，进而带来刑罚适用上的不断扩张与膨胀。因此，在民法学界关于数据确权之探讨方兴未艾、尚未盖棺定论之前，“数据权益的刑法保护”问题理应采取审慎之态度，毕竟我们应该时刻保持对“刑法谦抑原则”的遵守！

Abstract The issue of “criminal protection of legal rights of data” can be explored theoretically from two perspectives: “criminal law interpretation” and “criminal law legislation”. The methodology of “criminal law interpretation” starts from the current criminal law accusation system, mainly for revealing which crimes are set up with the purpose of protecting “legal rights of data and interests” as the normative standard. The “theory of criminal law legislation” methodology is to explore the legitimacy of the criminal law protection of legal rights of data and interests at the level of criminal law legislation, and to explore the types of behaviors that are prohibited by criminal penalties. However, both methodologies will rely on the determination of the connotation of “legal rights of data” and the identification of legal interests. In other words, it is the specific application of the theory of criminal law interests to the issue of criminal law protection of legal rights of data. Article 127 of the Civil Code is not a provision on the confirmation of legal rights of data, and in the context of many disputes in the theoretical circle of civil law about the legal attributes of legal rights of data, the unclear connotation and legal attributes of “legal rights of data” have led to its lack of “legal interest” status as a protected object of criminal law. The current approach to the protection of legal rights of data in the criminal law theory community is a misreading of the criminal law approach to the protection of legal interests, and does not address the substantive issues of the normative aspects of criminal law protection of legal rights of data. The approach to the concept of “data security” legal interest not only confuses the distinction between the concept of “data crime” at the phenomenological and normative levels, but also leads to overly arbitrary conclusions due to the lack of argumentation on how “data security” can constitute a protected legal interest under criminal law. In terms of theoretical discussion, it is necessary to clarify the distinction between the concept of “data” on the physical level as the object of behavior and the concept of “legal rights of data” on the legal interest level as the object of protection, and accordingly determine whether the “criminal protection of legal rights of data” constitutes a new issue at the normative level.

Keywords Data, Legal Rights of Data, Protection of Legal Interest, Data Crime, Data Security

（责任编辑：樊传明）