将数据违法犯罪行为置于整个法律体系之中加以考量，综合运用刑事、民事和行政法律手段予以规制，形成刑民行关系的衔接协调

以数据安全前置法为法益参照系认定数据犯罪

观察

□张勇

□目前，我国有关数据犯罪刑事立法及司法解释仍偏重于对信息网络安全的保护，实践中易导致狭义的数据犯罪与其他计算机犯罪、侵犯公民个人信息罪、侵犯商业秘密罪等罪名难以界分或陷入误区。因此，准确界定某种数据行为所侵犯的重点法益，找到与之相应的前置性法律规范，作为评价该行为是否定罪、应定何罪的参照系，显得尤为必要和重要。

我国先后颁布实施的网络安全法、数据安全法和个人信息保护法，分别发挥着保护网络安全、数据安全、个人信息安全的重要功能。从1997年刑法、刑法修正案（七）、刑法修正案（九）到“两高”《关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》（下称《解释》），数据安全刑法保护经历了从附属保护到间接保护，最终趋向独立保护的发展过程。但从整体上看，数据安全的法益保护尚缺乏系统规划，各法律法规之间未实现有效衔接与协调，有必要运用参照系理论及方法，从体系化视角予以探索。

数据安全法益具有多元属性

首先，数据是对信息的记录，两者是形式与内容的关系，其本质属性即数据信息的完整性、保密性、可用性。信息的概念较为宽泛，可识别性是区分个人信息与一般数据的本质特征。根据网络安全法、数据安全法、个人信息保护法的相关规定，数据安全与信息安全的内涵存在交叉，前者除了包含个人数据信息权益的安全保障之外，还包含有关数据信息的公共安全和国家安全；数据安全与网络安全也存在交叉重合之处，前者指有效保护和合法利用数据并使之持续处于安全状态，后者主要是指保障网络稳定可靠的运行状态。从广义角度来看，数据安全是一个内涵丰富的概念，在不同立法中具有不同的法律属性。而且，同一种数据行为所涉及的数据安全往往是多层次的，数据安全的法益保护也具有多元性，由此决定了数据安全法益识别判断的复杂性。

其次，某种数据对象或数据处理行为所蕴含的法益可分为集体法益和个人法益。集体法益包括社会秩序、公共利益和国家安全，法益保护的重心在于安全价值。个人法益则包括公民个人和社会组织的权利自由，法益保护的重心在于自由价值。数据安全属于抽象的集体法益，具有脆弱性、易受攻击性和不可控制性，存在认定上的困难，需要通过客观、具体的个人法益予以衡量。实践中，集体法益可以被还原为个体的人格或财产权益，因而也是可感知、可评价、可衡量的。当然，评价和衡量集体法益并非一定要采取“法益还原”的方式。从法益内容来看，刑法首要保护的是数据利益主体对数据的排他性复制、使用与处分权益，即数据利益主体对数据控制状态、占有状态、使用状态的稳定性以及数据不被其他主体窃取、篡改、使用、破坏状态的稳定性。同时，在数据的流动和使用过程中，初始权利主体逐渐丧失对个人数据的完全控制，数据利益主体从数据权利主体扩展至数据的收集者、使用者及处理者。数据安全法益越来越多地呈现多元化趋势，对数据的非法获取、破坏和滥用行为不但会对个体权益造成严重侵害，还会对公共利益、社会秩序和国家安全造成实际侵害或危险。

法益识别参照系与数据犯罪前置法

数据安全法益识别的立法参照系。从刑法角度来看，某种数据只有经过以数据安全为核心的法益识别之后，才被视为刑法所必须保护的法益。对于数据安全的法益识别，有必要运用物理学中“参照系”理论及论证方法进行认识判断。“参照系”属于物理学概念，即为确定研究对象的位置和描述其运动而被选作标准的另一物体。从不同的参照系来看，同一物体的运动状态是不同的。同理，研究某一种法律，需要以其为质点，选取另一种法律作为参照系，将其固定下来进行对比；或者选择不同的法律作为参照系，从不同角度进行对比。同时，还需要参照该法律在其产生发展不同阶段的立法变化，从而更准确、深刻地把握作为质点的法律规范内容。

基于数据安全集体法益的抽象性、模糊性，对其进行法益识别宜以相关法规范为参照。具体而言，对某种数据对象或数据处理行为进行法益识别，首先要选择其所对应的法律规范作为参照系，在此基础上，再确定法律所要重点保护的法益内容和层次。如前所述，网络安全法、数据安全法、个人信息保护法三者之间存在交叉重合关系，作为数据安全法益识别的参照系，既存在功能的差异性，同时也有一定的互补性。在不同的立法参照系下，法益保护的重点并不相同，对于数据安全保护重要性的认识也存在差别。因此，对数据安全法益识别可选择多种参照系。司法机关应将不同的立法参照系都纳入考察范围，加以对比和衡量，从中选择某种法律法规作为主要参照系，其他相关法律法规及行业规范则作为补充。不同的立法参照系之间也可以相互援引，加以体系解释，以使数据安全法益识别和判断的结论得到更好的印证。

数据犯罪中前置法的参照系功能。在我国刑法中，数据犯罪有广义和狭义之分。狭义的数据犯罪，即以数据为对象危害数据安全的犯罪行为，具体包括刑法第285条第2款、第286条规定的非法获取计算机信息系统数据罪和破坏计算机信息系统罪。两罪名以计算机信息系统中的数据安全为核心，即以数据的保密性、完整性和可用性为法益保护内容。该类犯罪属于典型的法定犯，上述条款中“违反国家规定”的前置性行政法，是确定数据安全法益识别参照系的法律依据。从广义角度分析，数据犯罪包括所有以数据为对象、载体或工具，侵犯公民个人权益、社会秩序或公共利益、国家安全的犯罪。所涉罪名不限于上述狭义的数据犯罪，有的罪名是将数据作为个人信息加以保护，如侵犯公民个人信息罪；有的罪名则是将数据作为计算机信息系统的内在组成部分加以保护，如非法控制计算机信息系统罪。在涉及数据犯罪的不同罪名中，数据安全法益往往属于复杂客体，对计算机信息系统安全、公民个人信息安全及数据自身安全的保护重点也存在差别。目前，我国有关数据犯罪刑事立法及司法解释仍偏重于对信息网络安全的保护，实践中易导致狭义的数据犯罪与其他计算机犯罪、侵犯公民个人信息罪、侵犯商业秘密罪等罪名难以界分或陷入误区。因此，准确界定某种数据行为所侵犯的重点法益，找到与之相应的前置性法律规范，作为评价该行为是否定罪、应定何罪的参照系，显得尤为必要和重要。

基于法益参照系的数据犯罪司法认定

数据犯罪的罪质与罪量认定之参照系。其一，在罪质界定方面，司法机关需要对数据犯罪中数据本身的性质和内容、数据使用价值的大小、数据可能遭受的侵害风险进行规范评价，准确合理地解释数据犯罪的构成要件。如，最高人民法院于2020年发布的指导案例145号“张竣杰等非法控制计算机信息系统案”。法院裁判理由认为，被告人为了赚取赌博网站广告费，提高搜索引擎命中率，通过植入木马程序的方式，非法获取存在防护漏洞的网站服务器的控制权限，进而通过修改、增加计算机信息系统数据，上传网页链接代码。但这种行为未造成网络系统功能实质性破坏或者不能正常运行，因此不应认定为破坏计算机信息系统罪，而应认定为非法控制计算机信息系统罪。可见，将数据安全法、网络安全法等前置法作为法益识别参照系，判断行为所侵害的法益是数据安全还是计算机信息系统安全，是区分两罪的关键。其二，在罪量界定方面，根据刑法第285条第2款和第286条所规定罪名的罪量要件分别是“情节严重”和“后果严重”。司法机关应立足前置法的相关规定，以数据安全法益保护为重心，明确犯罪数额或数量标准、综合性情节的罪量评价要素。《解释》第1条、第4条作了列举规定，包括经济损失、违法所得、计算机台数、身份认证信息组数等，在一定程度上反映了该罪对具体个人法益所造成的危害，但未能充分评价其对数据安全集体法益所遭受的侵害程度。建议未来刑事立法或司法解释应依据相关前置法规定，设定更为科学合理的罪量评价标准，如数据流量、安全漏洞数量，注册会员数量、点击浏览或下载数量、系统正常运行时长、网络中断时长及影响用户数、网络故障导致的事故损害后果等。另外，数据安全法益本身是抽象的，在明确数据犯罪的罪量标准时，可设置一定的柔性规范或兜底规定，使司法人员在个案认定中保留一定的裁量空间，这样更有助于实现定罪量刑的实质公正。

不同参照系下关联性罪名之竞合适用。我国民法典、个人信息保护法、反不正当竞争法、保守国家秘密法等现行法律法规分别对个人信息、商业秘密、内幕信息、国家秘密、国家情报、军事秘密等予以保护，与数据安全法益保护的对象存在重合。在非法获取信息数据的行为可能触犯的侵犯公民个人信息罪、侵犯商业秘密罪、非法获取国家秘密罪以及非法获取军事秘密罪等罪名之间，也存在竞合关系。例如，如果行为人非法获取计算机信息系统中的数据，其行为触犯了非法获取计算机信息系统数据罪或侵犯公民个人信息罪，属于法条竞合，应按照“特别法优于普通法”的原则处理。但究竟何种罪名属于“特别法”的规定，离不开前置法的参照系作用。如果以着重保护个人信息权益的个人信息保护法为参照，非法获取计算机信息系统数据罪属于“特别法”规定的罪名；如果以重在保护计算机信息系统安全的网络安全法、数据安全法为参照，侵犯公民个人信息罪则为“特别法”规定的罪名。

最后须强调，数据安全法益识别需要运用多种立法参照系加以对比，从而选择适用合适的法律规范予以保护，尽量避免法律规范之间的重复和冲突。从法秩序统一性角度，司法机关应将某种数据违法犯罪行为置于整个法律体系之中加以考量，综合运用刑事、民事和行政法律手段予以规制，形成刑民行关系的衔接协调。

（作者为华东政法大学教授）

数字检察赋能监督促进治理

大数据与能动检察

□张晓东

□数字检察的核心要义，在于统筹数字化技术、数字化思维、数字化认知，培育数字能力和方法，构建检察数字治理机制体系，通过检察大数据能动运用打开价值创造新空间，努力实现由“事倍功半”“人海战术”转向“事半功倍”“蓝海赋能”，由粗放型“人力驱动”向集约型“数据驱动”跃变，确保社会正义特别是百姓关注的实质正义“看得见”而且“不迟到”。

信息化时代，数字检察、大数据法律监督是检察工作迈向现代化的“船”与“桥”，事关党的检察事业长远发展。6月29日，全国检察机关数字检察工作会议召开，对加快数字检察建设，以“数字革命”驱动新时代法律监督提质增效，更好以检察工作高质量发展服务经济社会高质量发展作出部署。在此，以近年浙江省域数字检察实践探索为样本，探讨数字检察的概念和加快数字检察建设应秉持的理念。

数字检察概念：以类案法律监督为语境

概念是问题讨论的基础与前提。当前，数字赋能检察监督已由以往的展示为主进入真正的场景应用，亟待进一步明确数字检察这一特定概念的内涵与外延。笔者认为，数字检察作为新时代检察机关依法能动履职的一种工作理念、工作样态、工作模式，理应在“检察大数据运用”或“技术赋能法律监督”框架内与时俱进，禀赋更具实质性、指导性、前瞻性的内涵。具体而言，数字检察，是指检察机关运用数字赋能深化法律监督，通过数据共享、线索归集、类案办理，能动推进社会治理体系、治理能力现代化的数字监督思维、理念、程序、效应的集成、跨越、引领、再造、重塑性变革。其基本特征包括三方面：第一，从理念思维看，表现为从传统的相对被动、消极的监督观，转向更积极、能动的法律监督观，与现代信息技术飞跃发展相结合，借助检察大数据、区块链、人工智能，形成以现代性、开放性为标志的融合思维、对向思维。第二，从规模样态看，以多元协作为实践追求，对打通数据壁垒、信息孤岛提出深化需要，从个案监督转化为类案监督。数字检察中的案件形态，应具有量化的规格标准，并非单一案件而是类案。简要来说，就是从办理个案中发现规律性问题，通过归纳特点、要素，开发应用性监督模型，从海量数据中筛选出批量类案监督线索，并交办监督，再从类案问题中归纳分析发现执法司法、制度机制、管理衔接等方面存在的系统性漏洞，提出对应的检察建议，促进社会治理。第三，从实践效果看，具有“监督促进治理”的整治效能。以“数字革命”驱动新时代检察工作高质量发展背景下的司法办案，有别于一般的法律监督案件之基本特征，除了必须借助现代网络信息技术外，另一个实质要件在于运用大数据办案启动法律监督程序介入社会治理。以数字赋能法律监督为抓手，深化构建法律职业共同体多方协调互动、优势互补、双赢多赢共赢的法治监督体系。

数字检察理念：以数智赋能法治为枢纽

我国检察机关作为法律监督机关、司法机关，是保护国家利益和社会公共利益的重要力量，加之大数据先天禀赋技术与制度、介质与场域纵横交织特质，内在决定了新时代数字检察必然带有数智赋能法治、监督促进治理的特点。加快数字检察建设，以“数字革命”驱动新时代法律监督提质增效，需秉持以下理念：

发展与安全相平衡理念。高质量发展的前提是守住安全底线，数字检察的着眼点是数字赋能，底线是数字安全，尤需防范化解数据被篡改、盗用、滥用的风险。《中共中央关于加强新时代检察机关法律监督工作的意见》提出：“运用大数据、区块链等技术推进公安机关、检察机关、审判机关、司法行政机关等跨部门大数据协同办案，实现案件数据和办案信息网上流转，推进涉案财物规范管理和证据、案卷电子化共享。”为此，应动态平衡发展与安全，建立健全数据流动安全管理机制，夯实执法司法制度化信任基础。2021年底，浙江省义乌市检察院依托检校合作机制，在中国人民公安大学专家团队指导下，创设“区块链技术检察应用研究中心”，探索运用集现代密码学、去中心化、点对点传输等优势于一体的区块链技术，为提档升级后的“行刑衔接案件闭环管理”应用构筑防火墙。

办案与监督相结合理念。“在办案中监督、在监督中办案”，既是一种工作方法，也是一种价值取向。数字检察领域的关联思维及其能动运用，不仅把“四大检察”一体贯通、“四级检察”有序连接，也为深化办案与监督融合发展开辟了广阔空间。某种意义上看，办案与监督相结合，既是数字检察的重要方法论，也是其强大生命力之所系。

公正与效率相统一理念。人工智能时代，法治如何经由算法实现正义，是执法司法无可回避的技术难题和法律命题。最高人民检察院检察长张军强调：“监督办案就好像农耕，不掌握春种夏锄秋收传统知识、基本农技不行，但信息化时代，必须用科技、大数据手段提升质效，才可能提高‘产能’！”数字检察的核心要义，在于统筹数字化技术、数字化思维、数字化认知，培育数字能力和方法，构建检察数字治理机制体系，通过检察大数据能动运用打开价值创造新空间，努力实现由“事倍功半”“人海战术”转向“事半功倍”“蓝海赋能”，由粗放型“人力驱动”向集约型“数据驱动”跃变，确保社会正义特别是百姓关注的实质正义“看得见”而且“不迟到”。

规范与治理相促进理念。数字检察带来的深刻变革，不仅体现在法律监督体系、监督能力的重塑性变革上，更为检察机关深度参与社会治理、深化监督功能价值、规范经济社会秩序创造了有利条件，有助于将社会治理“后半篇文章”，作成优化“中国之治”国家社会治理的“巧智慧”和“大手笔”。

制度与文化相融通理念。制度建设带有根本性、全局性、稳定性和长期性。运用大数据提升国家治理现代化水平，关键在于“建立健全大数据辅助科学决策和社会治理的机制，推进政法管理和社会治理模式创新”。例如，浙江数字检察是在省委统一领导下，高效协同数字政府、数字经济、数字社会、数字文化、数字法治建设的产物。只有高度重视以文化人，涵养以尊重事实、推崇理性、强调精确、注重细节为基本内涵的数据文化，方有助于破解重定性轻定量、重观点轻数据等传统观念瓶颈，把检察司法人文关怀、社会主义核心价值观融入看似冰冷的技术理性、专业认知，为数字检察制度机制创新注入思想文化血液。

（作者单位：浙江省义乌市人民检察院）

集萃

中国人民大学教授王欣新：

破产法修改需要创设新程序制度

在企业破产法的修订中需要创设一些新制度，其中较为重要的有个人破产制度、简易破产程序、小微企业破产程序和预重整制度。第一，我国建立个人破产制度的条件已经具备，个人破产应当适用于所有自然人，不应再区分商自然人和消费者分别立法。第二，简易破产程序是破产法应当增加的制度，同时还应当建立小微企业破产程序，因为单纯的简易程序不能解决小微企业破产中的诸多特殊问题，必须设立单独的程序。第三，预重整制度的立法目的不仅是解决实践中的个别操作性问题，而且是健全、完善我国企业挽救法律体系不可或缺的重要环节。预重整是在法律规则下由当事人主导的庭外重组程序，法院与地方政府不应进行权力干预。预重整的对象是具有挽救可能，不依赖于重整强制措施保障，有能力与主要债权人开展自主谈判的债务人。我国预重整实践发挥了拯救困境企业的有利作用，应在实践基础上建立起详细、全面的预重整规则。

湖南大学法学院教授曹薇薇：

完善妇女权益保障立法提高司法适用质量

妇女权益保障法自1992年颁布以来，历经两次重大修改，与相关法律法规共同形成了较完整的立法体系，在实践中积累了一定的司法适用经验。2022年4月18日，《中华人民共和国妇女权益保障法（修订草案）》提请十三届全国人大常委会第三十四次会议二审。妇女权益保障法的此次修改应明确该法作为保障法、实用法、奠基法的三重立法定位；探究具体制度如何革故鼎新及实施落地，完善妇女人身、财产、社会权益实现的各项具体制度；加强与不同位阶的其他规范进行体系互动，贯彻落实宪法关于男女平等的原则，协调同阶位法律，衔接下位行政规章和地方实施办法；关注该法在司法实践中的援引必要性、操作可能性、执行有效性。只有总结地方立法以及司法判决经验，在立法完善的基础上提高该法的司法适用质量，落实修法目标，才能真切回应新时代妇女权益保障和落实性别平等的现实需要与挑战。

中国社会科学院大学法学院副教授韩伟：

反垄断法应采用竞争内生模式

经营者集中，指两个或者两个以上的企业相互合并，或者一个或多个个人或企业对其他企业全部或部分获得控制。评估经营者集中对创新的影响存在竞争外生与竞争内生两种模式，前者将创新作为竞争的外在因素独立评估，后者将创新作为特定竞争维度纳入竞争机制一并分析。我国反垄断法的核心目的是“保护市场公平竞争”，为确保该法功能定位的稳定，应采用竞争内生模式，关注交易对竞争机制造成的创新竞争层面的具体损害。执法部门可通过相关市场、交易方以及交易的特征，来判断特定案件是否需要评估创新竞争损害。横向交易中的单边效应与纵向交易中的原料封锁是评估创新竞争损害的主要损害理论基础，实际竞争和潜在竞争以及产品创新和产业创新则是个案可能涉及的不同情形。执法部门应该合理把握创新竞争评估所面临的不确定性，在确认存在损害的案件中充分尊重交易方的效率抗辩。

天津大学法学院副教授于阳：

适应性是刑罚适用核心特性

适应性是现代社会的核心特性。现代法治社会必然也会遭遇适应性问题如何有效化解的现实瓶颈。延伸至刑罚适用领域，确定性和灵活性是其基本特性，适应性则是其核心特性。刑罚适应性的内涵是在刑事法治理念的支配下，通过有效消解确定性与灵活性间的紧张关系，从而积极促进法律的适应性在制刑、量刑和行刑三个重要环节中有序而合理地实现。刑罚适应性的外延较为广泛，几乎囊括包括刑罚适用在内的各个社会面向。刑罚适应性同时能够协调诸如成本与效益、报应与预防、威慑性与宽缓性、惩罚性与人道性、公正性与个别化等刑罚基本关系范畴。概言之，刑罚适应性概念的提出既注重对具体问题的分析和解决，也基本满足刑罚本身对制度实践理性的价值追求。因此，应当在刑罚论研究中提倡并践行刑罚适应性的理念、理论、制度及其相关命题。

（以上依据《法治研究》《人权》《清华法学》《政治与法律》，张宁选辑）