

网络运营者数据安全义务的构造与行政处罚的裁量

义务体系的展开与罚款幅度的确定

赵跃

(安徽国运律师事务所, 安徽 合肥 230000)

摘要: 网络安全法修订后, 网络运营者的数据安全义务密度显著提高, 行政处罚的幅度也大幅提升。义务的内容从管理制度延伸到技术措施, 从事件报告延伸到风险评估, 形成了多层复合的义务体系。本文认为, 义务的构造应当区分为管理义务、技术义务与报告义务三类。管理义务指向组织与制度, 技术义务指向措施与能力, 报告义务指向信息与协作。三类义务的功能不同, 违反的后果也应当有所区别。归责原则应当采过错推定。网络运营者掌握技术条件与数据信息, 受害人难以证明其过错, 故应由运营者证明已尽合理注意。免责的事由限于不可抗力、受害人过错与第三方独立行为, 且须以已履行法定措施为前提。行政处罚的构成, 应当以义务违反、损害后果、因果关系为要件。三个要件的认定, 应当避免结果归责, 不能仅以发生泄露的事实推定处罚的成立。罚款幅度的确定, 应当综合考量违法的性质、持续时间、影响范围、主观状态、补救措施与配合程度。修订后的规则设置了四档幅度, 裁量应当在档次之内进行, 并说明理由, 避免畸轻畸重。在制度层面, 应当细化义务的履行标准、建立合规激励、完善行政与民事、刑事的衔接, 使处罚既能形成威慑, 又不至于抑制数字经济的发展。

关键词: 网络运营者; 数据安全义务; 过错推定; 行政处罚; 罚款裁量

中图分类号: D922.11 **文献标识码:** A **文稿编号:** WJLT(2023)03-0038-12

Data Security Duties of Network Operators and Discretion in Administrative Penalties

ZHAO Yue

(Anhui Guoyun Law Firm, Hefei 230000, Anhui, China)

Abstract: After the revision of the Cybersecurity Law, the density of data security duties on network operators has increased markedly and the range of administrative penalties has expanded substantially. Duties now extend from management systems to technical measures and from incident reporting to risk assessment, forming a multi-layered composite framework. This article classifies duties into managerial, technical and reporting categories. Managerial duties concern organization and systems, technical duties concern measures and capacity, reporting duties concern information and cooperation. Their functions differ, and so should the consequences of breach. The standard of fault should be a presumption of fault. Operators command the technical conditions and data, while victims cannot readily prove fault, so operators should show reasonable care. Exemptions should be limited to force majeure, victim fault and independent third-party conduct, and presuppose compliance with statutory measures. Administrative liability requires breach, harm and causation, and should avoid result-based attribution: a leak alone does not establish liability. In fixing the amount, authorities should weigh the nature and duration of the breach, its scope, the actor's state of mind, remedial measures and cooperation, choosing within the statutory bands and giving reasons to avoid extremes. Reform should specify compliance standards, create compliance incentives, and improve coordination among administrative, civil and criminal liability.

Key words: network operator; data security duty; presumption of fault; administrative penalty; discretion in fines

说明: (本文为作者个人研究观点, 不代表所在单位意见)

作者简介: 赵跃, 安徽国运律师事务所执业律师, 主要研究行政处罚与数据治理的司法审查问题。

一、问题的提出

数字经济的运行, 建立在数据的流动之上。数据的收集、存储、使用、加工、传输、

提供、公开，每一个环节都伴随着风险。风险的极端形态，是泄露、篡改、丢失，其后果可能波及数以亿计的个人。

为控制风险，法律为网络运营者设定了密集的义务。建立管理制度、采取技术措施、制定应急预案、开展风险评估、报告安全事件，义务的内容覆盖了组织的架构、技术的措施、流程的管理。

义务的违反，伴随着行政责任。责令改正、警告、罚款、停业整顿、吊销许可证，责任的形态多样。修订后的网络安全法，大幅提高了罚款的幅度，对情节严重的违法行为，罚款可达数千万元。

幅度的提高，引发了新的问题。罚款的裁量如何把握？同样的泄露事件，不同的企业可能面临悬殊的处罚，裁量的标准是什么？法院在行政诉讼中如何审查？

实务中的处罚，存在明显的不均衡。有的案件以泄露的人数作为唯一的裁量因素，人数多则罚款高；有的案件以是否及时报告作为主要因素，报告则减轻；有的案件几乎不作区分，一律顶格处罚。

裁量的不均衡，损害了法的可预期性。企业难以预见违法的后果，也就难以合理地配置合规的资源；投资者难以评估风险，也就难以作出准确的定价。

学理上的讨论，多集中于义务的内容与比较法的经验，对裁量的方法关注不足。而行政执法与司法审查所需要的，恰恰是裁量的基准与说理的结构。

本文认为，裁量的妥当，前提是义务的清晰。只有明确了义务的内容与层次，才能判断违反的程度；只有明确了归责的原则，才能判断主观的过错；只有明确了处罚的构成，才能判断责任的有无。

故本文的讨论，从义务的构造开始，依次展开归责的原则、处罚的构成、裁量的方法、责任的衔接。目的在于为行政执法提供基准，为司法审查提供框架。

需要说明的是，本文的讨论以网络安全法、数据安全法、个人信息保护法为基础，兼及相关的行政法规与部门规章。规范的体系庞杂，本文只择其要者。

数据安全的治理，是技术、法律、管理的交叉领域。法律的规则不能替代技术的判断，但可以为技术的应用划定边界。这是本文的基本立场。

对于规范的冲突，还应当注意协调的方法。可以按上位法优先、新法优先、特别法优先的规则处理；仍无法协调的，可以请求有权机关解释或者裁决。

对于行业惯例，应当注意其地位。惯例不是法源，但可以作为判断义务履行的参考。行业普遍采取的措施，可以作为合理注意的标准。

二、义务的规范来源与体系

网络运营者的义务，来源于三个层次：法律、行政法规、部门规章。三个层次的规范相互配合，共同构成义务的体系。

第一个层次是法律。网络安全法规定了网络运行安全、网络信息安全的基本义务；数据安全法规定了数据分类分级、风险评估、应急处置的义务；个人信息保护法规定了处理规则的义务。

第二个层次是行政法规。关键信息基础设施安全保护条例、网络数据安全条例等，细化了法律的原则性规定，明确了具体的措施与程序。

第三个层次是部门规章与标准。等级保护的技术要求、数据出境的评估办法、安全事件的报告规范，都属于这一层次。其效力较低，但操作性最强。

三个层次的关系，是上位法与下位法的关系。下位法不得与上位法抵触，但可以在上位法的框架内细化。细化的限度，是不得增设上位法没有规定的义务。

实践中，企业往往面临规范的冲突。不同的规范对同一事项规定了不同的要求，企业难以同时满足。此时应当适用上位法优先、特别法优先的规则。

规范的密度，反映了治理的思路。传统的命令控制型规制，以明确的义务与处罚为核心；新型的激励型规制，以合规的激励与责任的减免为核心。二者在网络数据领域并存。

义务的性质，可以从两个角度观察。从内容看，有的是行为义务，要求为一定的行为；有的是结果义务，要求达到一定的效果。从相对人看，有的是对国家的义务，有的是对个人的义务。

行为义务的违反，以是否实施行为为标准，判断较为客观；结果义务的违反，以是否达到效果为标准，判断较为复杂。数据安全的义务，多为行为义务，而非结果义务。

这一点极为重要。它意味着，即使发生了泄露，若运营者已经履行了法定的义务，也不构成违法。责任的成立，取决于义务的履行，而非结果的发生。

但实务中，执法机关往往以结果倒推义务的违反。发生了泄露，即推定未采取有效措施；泄露的人数多，即推定管理存在重大缺陷。这种结果归责的思路，值得反思。

义务体系的另一特点，是动态性。技术的变化快于规范的更新，新的风险不断出现，旧的规范难以及时回应。故义务的履行，不能仅以遵守条文为满足，还应当符合技术的一般水平。

这一要求，被称为动态的安全义务。它的内容不是固定的，而是随着技术的能力与行业的标准而变化。判断的标准，是同行业的一般水平，而非最优的水平。

对于管理义务的具体内容，还应当注意组织架构的要求。规模较大的运营者，应当设立专门的安全管理机构；规模较小的，可以指定专职或者兼职的负责人。架构的设置，应当与业务的规模相匹配。

对于制度的执行，应当注意记录。制度的发布、修订、培训、考核，都应当留有记录。记录的作用，不仅是应对检查，更是发现制度缺陷的依据。

对于教育培训，应当注意针对性。管理人员、技术人员、普通员工，面临的风险不同，培训的内容也应当不同。泛泛的培训，难以形成实际的能力。

对于技术义务的具体内容，还应当注意等级保护的要求。不同等级的系统，防护的要求不同。运营者应当确定系统的等级，按等级的要求采取相应的措施。

对于日志的留存，应当注意期限。法律规定留存的期限不少于六个月，涉及重大事件的，可以延长。留存的内容应当完整，包括时间、用户、行为、结果。

对于数据的加密，应当注意场景。传输的加密与存储的加密，要求不同；敏感数据与一般数据，要求也不同。加密的方案应当与风险的等级相适应。

对于报告的时限，应当注意起算点。自发现或者应当发现之日起算，而非自事件发生之日起算。发现的认定，以运营者知道或者应当知道为标准。

对于报告的层级，应当注意。一般事件报告属地监管部门，重大事件报告上级监管部门，特别重大事件报告国家层面的监管部门。层级的划分，应当依事件的性质与影响。

三、义务的类型与内容

义务的类型，可以按功能分为三类：管理义务、技术义务、报告义务。三类义务指向不同的对象，发挥着不同的功能，违反的后果也应当有所区别。

管理义务，指向组织的架构与制度的建设。内容包括指定负责人、设立专门机构、建立管理制度、开展教育培训、制定操作规程。

管理义务的功能，是使安全成为组织的常态，而非偶然的应对。没有制度的支撑，技术的措施难以持续，人员的操作难以规范，风险的发现难以系统。

管理义务的履行，应当有据可查。制度的文本、会议的记录、培训的签到、考核的结果，都是履行的证据。仅有制度而无执行的，不能认定已履行。

技术义务，指向措施的实施与能力的建设。内容包括防范计算机病毒、防范网络攻击、监测网络运行、留存网络日志、采取数据加密、实施访问控制。

技术义务的功能，是使风险可以被发现、被阻断、被追溯。技术的措施是安全的基础，没有技术的支撑，管理的制度只是纸面的宣示。

技术义务的履行，应当符合标准。国家标准、行业标准规定的技术要求，是最低的门槛。达到门槛的，可以认定已履行；未达到的，构成违反。

但达到门槛，不等于没有过错。技术的水平在提高，攻击的手段在演进，固守旧的标准可能不足以应对新的风险。故履行的判断，还应当考虑行业的一般水平。

报告义务，指向信息的提供与协作的配合。内容包括事件报告、风险评估报告、年度报告的提交，以及配合监督检查、提供技术支持的义务。

报告义务的功能，是使监管者可以及时掌握风险，使其他主体可以及时采取防范。信息的畅通，是协同治理的前提。

报告义务的履行，有时限的要求。安全事件应当在发现后的规定时间内报告，重大事件应当立即报告。超期报告的，构成违反，即使事件本身已经处置。

对于报告的内容，应当真实、完整。隐瞒事实、虚报数据的，构成违反，且可能加重处罚。报告的真实性，是义务的核心。

三类义务的关系，是相互支撑的。管理为技术提供组织保障，技术为管理提供手段支撑，报告为二者提供信息的反馈。任一环节的缺失，都会使体系失效。

对于三类义务的违反，后果应当有所区别。管理义务的违反，往往是体系性的缺陷，影响面广，处罚应当从重；技术义务的违反，可能是局部的疏漏，处罚可以相对从轻。

报告义务的违反，性质上是对监管秩序的妨害，与泄露本身造成的损害不同。故其处罚应当独立评价，不因泄露的后果严重而当然加重。

对于过错推定的适用范围，应当注意区分。义务的违反，可以直接推定的，适用推定；损害的发生，仍需证明因果关系的，不适用推定。二者的界限，应当清晰。

对于运营者的举证，应当注意其可能性。要求运营者证明的事项，应当是其能够掌握的证据。超出其掌握范围的，不能要求其证明，否则推定将变成无过错责任。

对于第三方的行为，应当注意其独立性。第三方受运营者的指示、控制或者监督的，其行为视为运营者的行为，不能免责；第三方独立于运营者的，可以作为免责的事由。

对于用户的过错，应当注意其程度。用户的一般疏忽，不能完全免除运营者的责任；用户的重大过失，例如主动泄露密码、明知风险仍点击链接，可以减轻或者免除责任。

对于不可抗力，应当注意其认定。自然灾害、战争、政府行为，属于典型的不可抗力；技术故障、网络攻击，通常不属于不可抗力，因为其可以预见、可以防范。

对于免责的证明标准，应当注意。运营者应当证明其已履行法定的义务，且损害的发生与义务的履行无关。仅证明损害系第三方造成，尚不足以免责。

对于运营者的规模，还应当注意分层。大型平台与中小企业的能力悬殊，义务的履行标准应当有所区别，不能以同一尺度苛求。

四、归责原则与免责事由

行政处罚的归责，原则上是过错责任。但过错的证明，在网络数据领域极为困难。受害人难以知悉运营者的内部管理，也难以判断其技术措施是否充分。

故应当适用过错推定。运营者应当证明其已履行法定的义务，已采取合理的技术措施，已建立有效的管理制度。不能证明的，推定其有过错。

过错推定的正当性，在于信息的不对称与控制的可能性。运营者掌握技术条件与数据信息，最有能力防范风险，也最有能力提供证据。

过错推定的适用，不改变处罚的构成。执法机关仍应当证明义务的违反与损害的发生，只是在主观状态上减轻了证明的负担。

对于免责事由，法律规定了不可抗力。但不可抗力的认定，应当严格。技术故障、系统漏洞、员工失误，都不属于不可抗力，不能免除责任。

本文认为，免责事由还应当包括受害人过错与第三方独立行为。前者如用户泄露密码、点击钓鱼链接；后者如供应商的系统被攻破，且运营者已尽审查义务。

但免责事由的适用，须以运营者已履行法定的措施为前提。未采取基本的防范措施而主张免责的，不予支持。这一限制，避免了免责事由的滥用。

对于共同过错的情形，应当按过错的程度分担责任。运营者与第三方服务商均有过错的，各自承担相应的责任；运营者承担后，可以向服务商追偿。

对于过错的证明，运营者可以提供以下证据：制度的文本与执行记录、技术的方案与检测报告、培训的记录与考核结果、事件的处置与补救措施。

证据的充分性，应当综合判断。单一的证据往往不足以证明，多项证据相互印证，才能达到证明的标准。证据的保存，是履行的前提。

对于中小微企业，过错的判断应当考虑其能力。要求其达到大型企业的技术水平，既不现实，也不公平。判断的标准，应当与其规模、业务的性质相适应。

这一区分，符合比例原则。义务的履行，应当与能力的匹配；责任的承担，应当与过错的程度相当。一刀切的标准，将使中小微企业不堪重负。

数据泄露后的罚款档次与计算方式，可参见网站被黑、数据泄露，公司要罚多少钱：2026年新网络安全法的四档罚款一文对罚款档次所作的实务梳理，本文不再重复其数额对照，只就义务的构造与裁量的方法展开。

对于处罚的种类，应当注意选择。责令改正、警告、罚款、停业整顿、吊销许可证，轻重不同。选择应当与违法的程度相适应，优先适用较轻的处罚。

对于责令改正的前置，应当注意。法律以拒不改正作为处罚条件的，执法机关应当先作出责令改正的决定，给予合理的期限，期限届满仍未改正的，方可处罚。

对于情节严重，应当注意其认定。情节严重是法定的加重事由，其认定应当有具体的事实，不能仅凭执法机关的主观判断。常见的情节包括多次违法、拒不配合、造成重大损失。

对于一事不再罚，应当注意其适用。同一违法行为，不得给予两次以上的罚款。但可以并处其他种类的处罚，例如罚款与停业整顿。

对于处罚的时效，应当注意。违法行为在二年内未被发现的，不再给予处罚；涉及公民生命健康安全、金融安全的，时效为五年。时效的起算，自违法行为终了之日起。

对于裁量的说明，应当注意。处罚决定书应当载明裁量的因素与理由，不能只写结论。说明的充分，是裁量正当的前提，也是司法审查的基础。

对于处罚与教育的结合，应当注意。行政处罚法规定了处罚与教育相结合的原则，对轻微违法、及时改正、未造成危害后果的，可以不予处罚。

五、行政处罚的构成与裁量

行政处罚的构成，包括三个要件：义务的违反、损害后果的发生、二者之间的因果关系。三个要件缺一不可，不能以结果的发生推定处罚的成立。

义务的违反，是处罚的前提。没有违反义务，即使发生了泄露，也不构成处罚的对象。这一原则，被称为无义务即无责任。

损害后果，是处罚的条件。网络安全法的许多条款，以拒不改正、情节严重作为处罚的条件。后果的轻重，影响处罚的档次。

因果关系，是处罚的基础。义务的违反与损害的发生之间，须有因果关系。若泄露系由不可抗力或者第三方独立行为造成，即使存在义务的违反，也不能归责。

对于因果关系的判断，应当注意义务的保护目的。义务的设置，旨在防范特定的风险；损害的发生，若不属于该风险的范围，则因果关系不成立。

举例说明。法律要求留存网络日志，目的是便于追溯。若运营者未留存日志，而损害系由外部攻击直接造成，则未留存日志与损害之间没有因果关系，不能据此处罚。

裁量的第一步，是确定处罚的档次。修订后的规则，根据违法的性质与后果，设置了递进的档次：一般违法、拒不改正、情节严重、特别严重。

档次的选择，应当以法定事实为依据。拒不改正的，须有责令改正的前置程序；情节严重的，须有法定情节的认定；特别严重的，须有严重后果的证明。

裁量的第二步，是在档次之内确定具体的数额。数额的确定，应当综合考量以下因素：违法的性质、持续的时间、影响的范围、主观的状态、补救的措施、配合的程度。

违法的性质，包括违反的义务类型、违反的次数、是否累犯。管理义务的违反、多次违反、累犯的，应当从重；技术义务的偶发违反，可以从轻。

持续的时间，反映违法的严重程度。长期不改正的，说明主观恶性较大；及时纠正的，说明主观恶性较小。时间的计算，自义务应当履行之日起至改正之日止。

影响的范围，包括泄露的人数、数据的类型、传播的范围。涉及敏感个人信息、涉及大量人数、已经公开传播的，应当从重。

主观的状态，包括故意与过失。故意隐瞒、故意不报告、故意不采取措施的，应当从重；过失疏忽、能力不足、经验欠缺的，可以从轻。

补救的措施，包括及时处置、通知用户、修复漏洞、加强防护。积极补救的，可以从轻；消极应对、推诿拖延的，应当从重。

配合的程度，包括是否如实陈述、是否提供资料、是否接受检查。积极配合的，可以从轻；抗拒检查、隐匿证据、虚假陈述的，应当从重。

六个因素的权衡，应当有结构。可以先按性质与后果确定基准，再按其他因素上下调整。调整的幅度，应当说明理由，避免恣意。

对于罚款的性质，应当注意。罚款是行政处罚，其目的是制裁与威慑，而非填补损

失。故罚款的数额不应当以损失为限，也不应当归受害人所有。

对于按营业额计算的方式，应当注意其比例。比例的高低，应当与违法的严重程度相适应。一般违法适用较低的比例，特别严重适用较高的比例。

对于营业额为负或者为零的情形，应当注意。企业亏损或者尚未营业的，按营业额计算将导致罚款为零。此时应当适用定额罚款，以保障处罚的威慑。

对于从轻与减轻，应当注意其区别。从轻是在法定幅度内选择较低的数额，减轻是在法定幅度以下确定数额。二者的适用条件不同，不能混淆。

对于从重，应当注意其限制。从重应当在法定幅度内选择较高的数额，不得超过上限。从重的事由应当法定，不能随意扩大。

对于罚款的执行，应当注意。当事人应当在规定的期限内缴纳；逾期不缴纳的，可以加处罚款，或者申请法院强制执行。执行的程序，应当依法进行。

对于罚款的上限，还应当注意比例原则的约束。过高的罚款可能使企业破产，反而损害公共利益；过低则难以形成威慑。

对于罚款的公开，应当注意。处罚决定应当依法公开，接受社会监督；涉及商业秘密的，可以作技术处理。

六、罚款幅度的确定

罚款幅度的确定，是裁量的核心。修订后的规则，将罚款的上限大幅提高，对特别严重的违法行为，可以按上一年度营业额的百分比计算。

百分比的计算方式，使罚款与企业的规模挂钩。大企业的绝对数额高，小企业的绝对数额低，但相对负担相当。这一设计，符合过罚相当的原则。

但百分比的计算，也带来了新的问题。营业额的认定、计算的口径、年度的选择，都可能引发争议。规则的适用，需要细化的标准。

对于营业额的认定，应当以经审计的财务报表为准。未经审计的，可以参照纳税申报的数据。关联交易的，应当按合并报表计算，避免通过拆分规避。

对于计算的口径，应当明确。是营业收入还是营业利润，是全部业务还是相关业务，是境内还是全球，都应当在规则中明确，避免执法的随意。

对于年度的选择，应当以违法行为发生时的上一年度为准。违法行为持续的，以最后一年的上一年度为准。这一规则，使罚款与违法时的规模相匹配。

对于幅度的下限，也应当有约束。过低的罚款，不足以形成威慑；过高的罚款，可能导致企业倒闭，反而损害就业与创新。分寸的把握，是裁量的艺术。

本文主张，可以建立裁量的基准制度。由监管部门制定裁量的基准，明确不同情节对应的罚款区间，执法人员在区间内选择，并说明理由。

基准制度的优点，是提高可预期性，减少执法的差异。缺点是可能僵化，难以适应个

案的特殊情形。故基准应当是指导性的，而非强制性的。

对于偏离基准的处罚，应当说明理由。理由是裁量的说理，也是司法审查的入口。无理由的偏离，可能被认定为滥用职权。

对于同一事件涉及多个违法行为的，应当分别认定，合并处罚。合并的规则，依行政处罚法的规定，不得重复处罚同一行为。

对于连续状态的违法行为，应当按一个行为处理，但从重处罚。这一规则，避免了对同一行为的反复处罚，也体现了对持续违法的否定评价。

对于公益诉讼的适用，应当注意。检察机关或者法律规定的组织，可以对大规模的数据泄露提起公益诉讼。公益诉讼的赔偿，应当用于受害人的救济与公共利益的修复。

对于刑事责任的界限，应当注意。侵犯公民个人信息罪以情节严重为要件，拒不履行信息网络安全管理义务罪以经责令改正而拒不改正为要件。界限的把握，应当严格。

对于单位犯罪，应当注意。单位实施相关犯罪的，对单位判处罚金，对直接负责的主管人员与其他直接责任人员判处刑罚。责任人员的范围，依其职责与作用确定。

对于行政与刑事的证据转化，应当注意。行政程序中收集的证据，可以在刑事程序中作为证据使用，但应当符合刑事证据的合法性要求。

七、与民事赔偿、刑事责任的衔接

行政责任、民事责任、刑事责任，是三种不同的责任形态。三者的功能不同，可以并存，不因一种责任的追究而免除其他责任。

行政责任的功能，是维护管理秩序，惩罚违法行为。其目的是公共利益的保护，其方式是对违法者的制裁。

民事责任的功能，是填补受害人的损失。其目的是私人利益的救济，其方式是赔偿。个人因数据泄露受到损害的，可以请求运营者赔偿。

刑事责任的功能，是惩罚严重的危害行为。其目的是社会秩序的维护，其方式是刑罚。情节严重的侵犯公民个人信息、拒不履行信息网络安全管理义务，可能构成犯罪。

三者的衔接，应当注意以下几点。其一，事实的认定可以相互参考，但证明的标准不同。刑事的证明标准最高，行政次之，民事最低。

其二，责任的追究可以并行，但不得重复。行政罚款上缴国库，民事赔偿归个人，二者不冲突；刑事罚金与行政罚款，应当折抵。

其三，程序的衔接应当顺畅。行政执法中发现涉嫌犯罪的，应当移送；刑事侦查中发现行政违法的，应当通报。移送的机制，是衔接的关键。

对于民事赔偿的范围，应当包括财产损失与精神损害。财产损失包括因泄露而产生的费用、因诈骗而损失的财产；精神损害以严重的精神痛苦为条件。

对于因果关系的证明，可以适用推定的规则。个人证明信息被泄露、遭受诈骗、二者

有时间关联的，运营者应当证明泄露与损失之间没有因果关系。

对于赔偿的数额，可以适用酌定。损失难以计算的，法院可以根据信息的类型、数量、泄露的情节、运营者的过错程度酌定，避免因举证不能而使个人得不到救济。

对于审查的强度，应当注意区分。对事实认定，应当全面审查；对法律适用，应当严格审查；对裁量，应当有限审查，只有在明显不当或者滥用职权时才予干预。

对于举证的责任，应当注意。行政诉讼中，被告对其作出的行政行为负举证责任，应当提供作出该行为的证据与所依据的规范性文件。

对于判决的方式，应当注意。处罚违法的，可以判决撤销、部分撤销、变更或者确认违法；处罚明显不当的，可以判决变更。方式的选择，依违法的性质确定。

对于司法建议，应当注意。审理中发现执法存在普遍性问题的，可以向监管部门提出司法建议，促使其改进执法，完善规则。

对于典型案例的发布，应当加强。通过典型案例，明确义务的边界、裁量的基准、审查的标准，为行政执法与司法审查提供参照。

对于合规不起诉的探索，可以在行政领域借鉴。企业主动合规、主动补救的，可以从轻或者免于处罚，以激励企业建立有效的合规体系。

对于行政公益诉讼，应当注意。检察机关发现监管部门不依法履职的，可以提起行政公益诉讼，督促其履行监管职责。

八、裁判方法与制度完善

行政诉讼的审查，应当围绕合法性展开。职权依据、事实认定、法律适用、程序正当、裁量合理，五个方面逐一审查，确定处罚的合法性。

对于职权依据的审查，应当注意管辖的层级与范围。不同级别的监管部门，管辖的范围不同；不同地区的部门，管辖的地域不同。越权处罚的，应当撤销。

对于事实认定的审查，应当注意证据的充分性。处罚的事实，须有证据支持；证据须经质证；认定须符合逻辑。证据不足的，应当撤销。

对于法律适用的审查，应当注意义务的援引与档次的适用。援引错误的，构成适用法律错误；档次错误的，构成裁量不当。

对于程序正当的审查，应当注意告知、听证、送达。未告知处罚的事实与理由的，程序违法；符合听证条件而未组织的，程序违法。

对于裁量合理的审查，应当注意因素的考量与理由的说明。未考虑法定因素的，构成裁量不当；考虑无关因素的，构成滥用职权；明显不当的，可以变更。

裁判文书的说理，应当充分。义务的内容、违反的认定、档次的适用、数额的确定，都应当说明理由。说理充分，才能让当事人信服，也才能引导执法的规范。

制度的完善，首先是义务标准的细化。应当通过国家标准、行业标准，明确不同规

模、不同业务的企业应当达到的安全水平，使义务的履行有据可依。

其次是合规激励的建立。对主动开展合规建设、主动报告漏洞、积极配合处置的企业，可以从轻或者免于处罚。激励的机制，可以引导企业从被动应对转向主动防范。

再次是裁量基准的制定。监管部门应当制定裁量的基准，明确不同情节对应的处罚区间，并定期评估、动态调整，使裁量有章可循。

最后是救济渠道的畅通。企业不服处罚的，可以申请行政复议、提起行政诉讼；个人因泄露受损的，可以提起民事公益诉讼。救济的畅通，是权利保障的基础。

从治理的角度看，处罚只是手段，安全才是目的。过重的处罚可能抑制创新，过轻的处罚难以形成威慑。分寸的把握，是治理能力的体现。

从法治的角度看，处罚的正当性，来自规则的明确与程序的公正。规则明确，企业才能预见；程序公正，处罚才能服人。

从发展的角度看，数据安全与数字经济并非对立。安全的保障，是信任的基础；信任的建立，是发展的条件。二者相辅相成。

对于裁判者而言，每一个案件都是一次平衡的实践。平衡的智慧，来自对技术的理解，也来自对价值的坚守。

最后需要说明，本文的讨论以现行法为基础。随着网络安全法的实施与配套规则的完善，相关结论可能需要调整，本文的观点亦当接受检验。

数据的安全，最终要靠技术的进步、管理的完善与法律的保障共同实现。三者缺一，治理便会失衡。

愿每一家企业，都能在清晰的规则下安心经营；每一位用户，都能在可靠的安全中获得信任。

本文的讨论，以网络运营者的数据安全义务为限，未及关键信息基础设施运营者的加重义务；所引行政处罚案例，多为公开报道，未及全部裁判文书。这些，均有待进一步核实。核实的途径，是行政处罚决定的公开。

九、结语

数据安全的治理，是数字时代的基础命题。它既要防范风险，又要促进发展；既要约束企业，又要激励创新。二者的平衡，是制度设计的难点。

义务的构造，为平衡提供了基础。清晰的义务，使企业知道应当做什么；合理的归责，使企业知道做到什么程度可以免责；妥当的裁量，使处罚与过错相当。

三个环节相互关联，缺一不可。义务不清，则归责无据；归责不当，则裁量失衡；裁量失衡，则义务落空。体系的完整，决定了治理的成效。

对于裁判者而言，每一个行政处罚案件，都是一次对治理逻辑的检验。判决的结果，不仅解决个案的争议，也向市场传递规则的信号。

信号的清晰，决定了预期的稳定。预期稳定，企业才能安心地投入合规，创新才能持续地展开。这是法治的价值，也是发展的条件。

归结而言，网络数据的安全，需要政府、企业、社会的共同参与。政府提供规则与监督，企业承担义务与责任，社会形成共识与监督。三者协同，治理才能有效。

愿每一份数据，都能得到妥善的保护；每一次泄露，都能得到及时的处置；每一项处罚，都能经得起法律的检验。这是制度的目标，也是时代的期待。

参考文献

- [1] 周汉华：《网络安全法的主要制度与实施问题》，载《中国法学》2019年第2期。
- [2] 张新宝：《个人信息保护法释义》，中国人民大学出版社2021年版。
- [3] 王锡锌：《数据治理的行政法问题》，载《法学研究》2020年第6期。
- [4] 程啸：《个人信息保护中的行政责任》，载《中外法学》2021年第4期。
- [5] 洪延青：《数据安全义务的构造与履行》，载《法律科学》2022年第1期。
- [6] 刘权：《行政处罚裁量的基准与司法审查》，载《法学》2021年第8期。
- [7] 全国人大常委会法制工作委员会：《中华人民共和国网络安全法释义》，法律出版社2025年版。
- [8] 国家互联网信息办公室：《网络数据安全条例释义》，中国法制出版社2025年版。