如何科学运用在案证据构建符合逻辑、经验法则和法律规定的证据体系，是刑事司法办案过程中需要回答并解决的重要问题——

运用“异常性”判断寻找指控犯罪“突破口”

□王聚涛

□行为“异常性”的本质是对社会相当性的背离。所谓社会相当性，是指行为符合历史形成的社会伦理秩序范围内的正常活动。行为“异常性”可通过三个维度检验：是否与社会一般观念相背离、是否与行业规范相违反、是否与个体行为习惯相吻合。同时，“异常性”判断要能够排除合理怀疑和接受反证的检验。

构建以证据为中心的刑事指控体系，是刑事领域“高质效办好每一个案件”的基础和保障。证据的收集、审查、判断和运用是刑事指控体系的核心和基石。在犯罪嫌疑人、被告人不认罪或者辩护人作无罪辩护的情况下，如何科学运用在案证据构建符合逻辑、经验法则和法律规定的证据体系，是刑事司法办案过程中需要回答并解决的重要问题。

有这样一起“低价售车”式诈骗案。被告人丁某、王某以A公司名义在网络平台上发布“低价售车”广告。A公司收取客户的购车款并补足10%左右差价后交给B公司，以B公司名义购买车辆并登记在B公司名下。B公司再向融资公司抵押借款后将抵押款和车辆交给A公司，A公司再将车辆交给客户。A公司又与B公司签订车辆租赁合同，并按月向B公司支付租金。客户拿到车辆发现短期内无法过户后要求A公司办理过户手续。A公司编造各种理由拖延，并拒绝退还购车款，造成32名客户损失1000余万元。客户报案后，被告人及其辩护人以不具有非法占有目的为由进行无罪辩解，公安机关以“车辆使用权”获取“现金流”难以认定行为人具有非法占有目的为由而不予立案。最终检察机关通过刑事立案监督，被告人丁某、王某均因犯诈骗罪被判处十年以上有期徒刑，并处十万元以上罚金。在这类案件中，犯罪分子会精心设计一套复杂的交易模式，为其犯罪行为披上正常民事法律关系的“外衣”，待案发后以民事纠纷为借口掩盖刑事犯罪目的。正如上述案件中，被告人为掩盖犯罪事实，设计了抵押、融资租赁、反向担保等多重交易关系，颇具迷惑性。

然而，深入分析就能发现，这种交易模式并不符合商业逻辑。根据资金走向，A公司属于贴钱购车。按照这种交易模式，A公司根本不具有盈利可能性，而且卖得越多亏得越多。A公司的行为实质上是以“低价售车”为幌子骗取被害人购车款的“骗局”。检察机关正是抓住这种交易模式的“异常性”，最终成功指控犯罪。

因此，面对犯罪分子的辩解，可以通过对交易行为“异常性”进行深入分析，可顺利找到指控犯罪的“突破口”，从而实现“善于从纷繁复杂的法律事实中准确把握实质法律关系”。

“异常性”判断的规范原理和实践基础

进行“异常性”判断符合经验法则。无论是在日常生活还是经济生产中，都要遵循一定的准则，包括社会准则和行业准则。这些准则又称为经验法则，是人们在长期生产、生活等实践中，通过对客观现象的观察、识别和认知，在观念上形成的一种理性认知，是对有关事物的现象、表征和内在逻辑结构带有普遍性的领悟和把握。当一个人的行为不符合这种经验法则时，则具有“异常性”。因此，行为是否符合经验法则就成为司法人员裁决案件的重要依据，即常说的是否合乎“常情常理”或者是否合乎“生活经验”等。虽然经验法则具有内容不够明确、归纳不周延的缺陷，但在审查证据、认定事实过程中具有不可或缺的作用，可以帮助司法人员从纷繁复杂的行为碎片中发现不合理之处，同时作为自由心证证据规则的一部分引导司法人员进行决断。

将行为“异常性”作为定案依据符合司法解释规定。针对犯罪嫌疑人、被告人的无罪辩解，我国多个刑事司法解释都规定了通过行为“异常性”推定主观明知的内容。如，《关于办理洗钱刑事案件适用法律若干问题的解释》第3条规定，“认定‘知道或者应当知道’应当根据……交易行为、资金账户等异常情况，结合……等情况综合审查判断”。又如，《关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释》第11条规定，“交易价格或者方式明显异常的”可以认定行为人明知他人利用信息网络实施犯罪。可见，有关司法解释等规范性文件肯定了通过价格异常、地点异常、交易方式异常等行为的“异常性”来判断行为人具有主观明知故意，为司法办案提供了依据。

行为“异常性”判断具有指导性案例支持。最高检第二十六批指导性案例之“邓秋城、双善食品（厦门）有限公司等销售假冒注册商标的商品案”（检例第98号），针对被告人甄某否认自己明知涉案咖啡系假冒注册商标的商品的辩解，检察机关根据其采用夜间收发货、隐蔽包装运输等异常交易方式认定其对售假行为具有主观明知。该案明确“在认定犯罪的主观明知时，不仅考虑被告人供述，还应综合考虑交易场所、交易时间、交易价格等客观行为，坚持主客观相一致”进行判断。又如，最高检第四十七批指导性案例之“沈某某、郑某某贪污案”（检例第187号），针对被告人及其辩护人所提行为系正常期货交易，未侵吞公共财物、未造成国有公司损失的辩解，检察机关通过论证交易习惯的异常性、盈利比例的异常性、交易对象的异常性，综合认定被告人增设期货交易环节获利并非正常的市场交易行为，最终认定被告人构成贪污罪。

《最高人民检察院关于案例指导工作的规定》第15条规定，“各级检察院应当参照指导性案例办理类似案件”。据此，上述指导性案例确定的“异常性”判断应当作为办案参照。

行为“异常性”判断的三个维度

行为“异常性”的本质是对社会相当性的背离。所谓社会相当性，是指行为符合历史形成的社会伦理秩序范围内的正常活动。行为“异常性”可通过三个维度检验：

是否与社会一般观念相背离。德国刑法学家宾丁提出“外行人的平行评价”理论，即站在外行人的领域或立场以理性第三人标准判断行为是否显著偏离日常生活经验。比如，从普通人的立场上看，将现金用于购买房产、车辆是正常的，不仅能够满足日常居住、出行需要，也可以满足保值增值的需要，这就难以直接认为该行为具有“异常性”。又如，一般人不会频繁将一笔资金在多个账户之间进行划转，如果存在这种行为就有“异常性”。

是否与行业规范相违反。行业规则或者行业规范是在特定行业内，为了实现行业目标、维护行业秩序、保障行业成员的共同利益而制定的一系列行为准则和规定，对行业从业人员具有约束力。特定行业规则构成法定注意义务来源，违反该义务即具备“异常性”。一个行为虽然在一般人看来比较异常，但如果是行为人所处行业规则、规范所要求的，则认定具有正常性。比如，在集资诈骗犯罪案件中，犯罪分子许诺的高额收益显著高于行业平均利润率，这就与行业规范相违背，不符合基本的商业逻辑，从而可以推出行为人通过“空手套白狼”方式非法占有集资参与人投资款的结论。

是否与个体行为习惯相吻合。一个人会因为家庭环境、性格、自身经历等因素形成某些特殊的行为习惯、行为方式。当行为符合行为人稳定且可验证的个体模式时，可阻却其行为“异常性”的认定。否则，司法机关通过收集相应证据，证明其当前行为不符合固有模式，且结合其他证据可以证明其行为符合犯罪逻辑时，则可认定其具有主观明知。

运用“异常性”判断的注意事项

“异常性”判断系证据补强方法。认定犯罪向来都是对证据进行综合分析判断的过程，要对所有在案证据进行全面、系统分析，在确保证据“三性”“两力”后，合理运用证据规则、逻辑规则得出相应结论。之所以“孤证”不能定案，是因为证据越少则证明力就越弱，无法形成牢固的证据体系。因此，“异常性”判断具有补强性，可以在直接证据缺失的情况下，起到“填补空隙”的作用。司法实践中，要尽可能多收集行为“异常性”方面的证据，此类证据越多，则行为人无罪辩解的“荒诞”就越发突出。除了搜集“异常性”证据外，还要注意收集构成犯罪的基础性证据，否则证据体系就不健全。

“异常性”判断要能够排除合理怀疑。我国刑事诉讼法一贯坚持“案件事实清楚，证据确实、充分”的证明标准。“排除合理怀疑”是指“对于事实的认定，已没有符合常理的、有根据的怀疑，实际上达到了确信的程度”。换而言之，根据常识、常情、常理，在人们普遍认识水平和现有科技水平下，排除了符合犯罪构成要件之外的其他可能性，就是排除了合理怀疑。运用“异常性”判断认定犯罪时，同样要以是否“排除合理怀疑”为目标进行分析，重点是看这种“异常性”是否只有构成犯罪才能解释得通，否则就没有达到“排除合理怀疑”的程度。

“异常性”判断要接受反证的检验。“异常性”判断的内核是刑事推定规则。刑事推定，是司法人员根据事实之间的常态联系，以某一已经查明的事实推断另一难以证明的事实存在的过程。刑事推定被广泛规定和应用在我国刑事司法解释和司法实践中，是通达事实真相、指控刑事犯罪的重要方法和路径。但是，由于刑事推定的前提条件是有限的，造成推出的结论具有不稳定性，当行为人提出一个合理的辩解或者举出相反证据，则刑事推定就面临失效。所以，相关司法解释中也同时规定了“有证据证明确实不知道的除外”的“但书”内容，就是为了防止司法推定的绝对化。因此，“异常性”判断的结论也要经得起反证考验，否则将面临推定不具唯一性的局面。在办案过程中，要充分听取行为人的辩解，并通过自行侦查、引导侦查（调查）、退回补充侦查（调查），查明行为人辩解是否具有合理性。

（作者为江苏省常州市天宁区人民检察院检察委员会专职委员）

视角

强化检察履职促进数据安全管理

□曾粤兴　田颖

随着“数字中国”建设加速，“物联网”“云计算”等数字化技术正快速融入人们生产生活各个环节，在高效驱动数字化转型的同时，也给数据安全带来了新挑战。2024年7月，党的二十届三中全会审议通过的《中共中央关于进一步全面深化改革、推进中国式现代化的决定》（下称《决定》）对“健全促进实体经济和数字经济深度融合制度”作出专门部署，强调“提升数据安全治理监管能力”。检察机关作为宪法规定的法律监督机关，应进一步健全数据犯罪刑事案件办理机制，重视法律监督数据安全的内部监督，并以法律监督履职督促数据处理者履行数据安全保护义务。

进一步健全数据犯罪刑事案件办理机制。数据安全法将“保障数据安全”和“促进数据开发利用”确立为立法目的，强调保障数据安全与促进数据发展并重。基于法秩序统一性原理，数据犯罪刑事治理的目的取向，理应与前置法保持相对一致。检察机关在发挥法律监督职能时，应紧密围绕服务维护数据安全与数据发展大局，健全数据犯罪刑事案件的办理机制。

一方面，依法惩治数据犯罪，以高质效检察履职为数据安全保障筑起坚固堡垒。在数据犯罪刑事案件的处理中，检察机关既能向前引导和制约侦查，又能向后监督和制约审判，并在审查起诉环节拥有决定权。基于其在犯罪治理中的特殊定位，检察机关应立足自身职能，在保障数据安全方面承担相应的政治责任、法治责任和检察责任，坚持高质效办好每一个案件，以期更加有效地惩治数据犯罪。具体而言，检察机关在办理数据犯罪案件时，应加强全链条惩治，注重深挖“上下游”等关联性犯罪线索；发挥检察一体化优势，深化跨区域合作办案，做到信息互通、证据共享，以期形成打击数据犯罪的强大合力；以专业化办案为导向，吸收检察技术人员、其他有专门知识的人辅助案件办理，并积极探索运用云计算等信息技术辅助办案，提升数据犯罪案件办理的专业化水平。另一方面，秉持谦抑审慎理念，为数字产业发展和科技创新传递司法善意和检察温情。检察机关在办理案件时，应注意理性看待数据处理过程中的不规范行为，准确把握数据行为行政违法与刑事犯罪的界限，审慎运用司法权，促进数字空间依法、健康发展。具体而言，刑事司法应突出强调实质解释，即在政策导向下，诉诸规范目的，展开价值判断，妥当解决“形式合法实质不合理”的认定问题，更加重视行为的法益侵害性，避免将不应入罪的行为解释为犯罪，实现人权保障与司法善意相辅相成，强化公众对检察决定的可接受性，追求政治效果、法律效果与社会效果的有机统一。

重视数字检察中的数据安全管理。数字检察是“数据”与“检察业务”深度融合的产物，是对法律监督模式的重塑，不仅要求以数字化技术“辅助”“支撑”法律监督工作，更要求以数字化技术“引领”“驱动”法律监督。目前，在司法实践中，数字检察遵循“检察大数据收集—法律监督数字模型建构—类案监督线索核查—从类案监督到源头治理”的基本运行流程与步骤。其中，数据要素资源是基石，云计算、物联网等数字技术是支撑，系统应用是手段。数据提取、使用是检察机关“科技强检”建设的基础，但也可能带来数据安全风险。因此，检察机关应在推进数字检察建设时，加强对法律监督类数据的安全管理。

法律监督类数据的安全管理，不仅关系着数字检察战略工作的成效，而且影响着检察机关的形象，既需要理念跟进，还需要制度保障。深化数字检察工作，需要检察机关确保自身遵循边界规范，在应用创新数字技术的同时，对法律监督类数据采取有效的监管和保障措施，筑牢“数据安全阀”。具体而言：一是在检察机关内部由具体部门负责法律监督类数据安全监管与检查，对数据依法进行有序管理、标识、清洁，切实开展日常核查和系统监管，实时、同步、全程监督数字检察工作中的数据安全状况，并对法律监督类数据的保护效果进行评估，以便快速发现并消除数据安全风险；二是构建全流程数据安全防护机制，严格法律监督类数据在调取、传输、保存和应用等各环节的工作流程和技术标准，并明确相应的权力清单，加强对法律监督类数据的实时监测分析、安全风险预警和应急响应处置；三是注重法律监督类数据分类分级保护，检察机关应立足自身的业务需求，依据数据的重要程度对收集的法律监督类数据进行分类分级并形成目录清单，区分可公开数据、限制公开数据以及保密数据的边界，明确要求检察办案人员在使用法律监督数字模型时，必须严格遵守相关规定，并设立相应责任追究机制。

［作者分别为北京理工大学法学院教授、博士生导师，北京理工大学法学院博士研究生。本文系2022年度教育部人文社会科学重点研究基地（国家人权教育与培训基地）重大项目“网络犯罪治理现代化中的人权保障研究”（22JJD820042）的阶段性研究成果］

惩治“开盒”式网络暴力的检察着力点

观察

□魏晓娜　谢甜甜

魏晓娜

近年来，“开盒挂人”正在成为一种新型网络暴力。其模式通常是，不法分子通过网络搜索、挖掘、境外群组购买等方式，非法获取被害人的隐私信息，并在网络上公开发布，煽动网民对被“开盒”者进行侮辱、攻击、谩骂。与传统网络暴力相比，“开盒”式网络暴力会给被害人及其家人、朋友的身心健康和人身安全造成极大的伤害。对于这种严重的新型网络暴力，检察机关应当积极介入，严厉打击。

“开盒”式网络暴力参与者的行为大体上分为四种类型：提供信息，购买信息“开盒挂人”，参与线上侮辱、谩骂、转发、评论和参与线上线下伤害行为。根据刑法、行政法等相关规定，这四类行为分别会产生不同法律后果。根据最高法、最高检、公安部联合发布的《关于依法惩治网络暴力违法犯罪的指导意见》（下称《指导意见》），检察机关可从以下四方面做好“开盒”式网络暴力案件的处理。

刑事惩治：严惩“开盒”式网络暴力中的犯罪行为

根据《指导意见》的规定，对于“开盒”式网络暴力的始作俑者（**即提供信息，购买信息“开盒挂人”，引导网友对被害人侮辱、谩骂的人**），已达到犯罪门槛的，可以根据侵犯公民个人信息罪、非法利用信息网络罪、侮辱罪、诽谤罪等追究刑事责任。但这四个罪名中，前两个属于公诉案件，后两个属于自诉案件。将不同的罪名与“开盒”式网络暴力的特点相结合，检察机关在履职过程中，应各有侧重。

一是对侵犯公民个人信息罪与非法利用信息网络罪提起公诉。其中，根据刑法第253条之一和《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，对于侵犯公民个人信息罪的适用，应把握两个方面：一方面，准确把握入罪和刑期上档的数量门槛。例如，行踪轨迹信息、通信内容等是否达五十条以上，住宿信息、通信记录等是否达五百条以上；违法所得是否达到五千元以上等。另一方面，根据个案情形，合理解释“其他情节严重的情形”与“其他情节特别严重的情形”。当行为人的作案手段与后果都极为恶劣，但“开盒”信息数量未达入罪门槛时，可从开盒的信息类型、犯罪故意、传播范围、持续时间、行为方式、是否造成被害人罹患抑郁症等方面综合判断。对于非法利用信息网络罪的适用，应重点关注行为人设立群组的目的、网站注册数量、群组成员数量等。

二是侮辱罪、诽谤罪的自诉转公诉。根据刑法第246条与《指导意见》的相关规定，这两个罪名以“情节严重”作为入罪门槛，原则上属于自诉案件，但“严重危害社会秩序”的应依法适用公诉程序。此时，可以从两个方面切入：一是根据《指导意见》第12条，准确把握“严重危害社会秩序”的具体情形，开展立案监督。对于“造成被害人或者其近亲属精神失常、自杀等严重后果，社会影响恶劣的”“随意以普通公众为侵害对象，相关信息在网络上大范围传播，引发大量低俗、恶意评论，严重破坏网络秩序，社会影响恶劣的”等，属于侮辱罪、诽谤罪转为公诉案件的情形。此时，应当加强立案监督，重点审查以下内容：对于被害人提起自诉，法院认为符合“严重危害社会秩序”情形，要求撤诉或裁定不予受理的，被害人报案后，公安机关是否及时立案，对于不予立案的是否给出合理理由。二是对转为公诉的重大、敏感、复杂的侮辱、诽谤案件，根据《指导意见》第18条，强化与公安机关的衔接配合，通过提前介入方式，从“开盒”网络暴力相关电子数据的固定、发帖、发布网暴信息账号IP的追踪、匿名行为人真实身份的确定和抓捕等方面，为侦查工作提供切实可行的建议方案。对于仍属于自诉的侮辱诽谤案，当自诉人报案或因证据收集有困难寻求救助时，检察机关也可参照《指导意见》第11条，协助侮辱、诽谤刑事案件自诉人取证。

刑事司法与行政执法衔接：惩治“开盒”式网络暴力中的违法行为

根据《最高人民法院、最高人民检察院关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释》，“违法犯罪”包括犯罪行为和属于刑法分则规定的行为类型但尚未构成犯罪的违法行为。因此，通过刑事司法与行政执法衔接机制，根据刑事诉讼法第177条第3款和《指导意见》第7条规定，当行为人提供的信息数量、开盒的信息数量未达到相关罪名的入罪门槛时，对于参与线上侮辱、谩骂、转发、评论和线下伤害的行为等，仅符合治安管理处罚法等规定的，检察机关可以提出检察意见，移交公安机关予以行政处罚。

在履职过程中，检察机关应重点关注“开盒”式网络暴力的恶意发起者、组织者、恶意推波助澜者的惩处。“开盒”式网络暴力，借助虚拟网络空间，侮辱、谩骂、转发、评论者之间相互匿名，发言与转发的方式也是远程匿名。虚拟、陌生、远程甚至跨境，给参与“开盒”的网民造成一种现实的疏离感，造成道德感弱化。恶意发起者、组织者、恶意推波助澜者有组织地煽动，容易将不明情况的网友、辨别能力不强的未成年人等卷入“开盒”网暴的不当言论中，而恶意发起者、组织者、恶意推波助澜者则隐藏在幕后。因此，行刑反向衔接针对的治理对象，是尚未构成犯罪的恶意发起者、组织者、恶意推波助澜者。检察机关在履职过程中，可以依托数字检察与智能办案辅助工具，锁定非正常的IP与发帖账号，对其进行重点打击。

公益诉讼：阻断“开盒”链的不当传导

依托公益诉讼检察，对网络暴力行为损害社会公共利益的，依法向法院提起公益诉讼。根据刑法第286条之一与《指导意见》第6条规定，网络服务提供者不依法履行法律、行政法规规定的信息网络安全管理义务，经监管部门责令采取改正措施而拒不改正，致使违法信息大量传播的或者致使用户信息泄露，造成严重后果的，可以拒不履行信息网络安全管理义务罪追究网络服务提供者的责任。在“开盒”式网络暴力中，行为人往往借助网络平台公开“开盒”。此时，若网络服务提供者，在发现网络暴力迹象后，未能依照相关法律和行政法规的规定，履行信息网络安全管理义务，最终导致网暴信息泛滥，损害社会公共利益的，检察机关可以依法提起公益诉讼。同时，检察机关还可以通过检察建议，督促网络平台筛查整治，改进算法、数据筛查等技术，一旦发现有人“开盒”，可及时采取应对措施，制止“开盒”链条从被“开盒”者转向其家人、朋友等。

检察建议：助推治理侵犯公民个人信息的黑灰产业链

“开盒”式网络暴力的实施，依托侵犯公民个人信息的黑灰产业链，以非法获取公民个人信息为前提。因此，应当严厉打击“开盒”背后侵犯公民个人信息的整个黑灰产业链。当前各行各业在科技赋能之下，依托大数据开展生产经营。“开盒”式网络暴力涉及的数据类型，通常有姓名、身份证号码、家庭住址、手机号码等。这些信息常见于快递寄取信息、App信息收集、相关企事业单位的员工电子信息等。检察机关在办理案件过程中，可结合个案，通过信息溯源的方式，对相关个人信息收集主体、信息收集的合法合规程度、提供服务所必要的信息收集限度，以及App信息收集时用户知情权保障等，参照2019年国家网信办等联合印发的《App违法违规收集使用个人信息行为认定方法》进行审查。相关企事业单位在个人信息存储、保护等方面存在疏漏的，制发检察建议，督促相关单位进行整改。

（作者分别为中国人民大学法学院教授、博士研究生）