法学研究 Chinese Journal of Law
Vol.47，No.4（2025）

犯罪追诉数字化背景下嫌疑判断的演化与程序法规制的因应

裴　炜*

内容提要：数字技术的发展正在重塑犯罪嫌疑的生成与判断逻辑。传统的嫌疑判断，主要依赖执法人员对具体行为的直接观察以及以其为基础的经验推断。然而，大数据与人工智能等技术的深度应用，改变了嫌疑的信息基础结构，使嫌疑的信息基础从核心案件事实延展至更为广泛的外围信息。伴随这一变化，嫌疑的判断逐步呈现出由个体转向群体、由自然人转向数字人、由事实转向情报、由人类理性转向机器理性的变迁与融合。这一趋势在提升侦查效能与潜在犯罪发现能力的同时，也引发了“嫌疑稀释”的现象。该现象会削弱嫌疑作为刑事诉讼程序规制工具的核心功能，并对正当程序的实现及公民基本权利的保护构成严峻挑战。因此，现有刑事诉讼制度有必要作出相应调整，将“嫌疑信息密度”纳入嫌疑的评价维度，通过程序过滤机制确保嫌疑判断与具体诉讼措施和决策之间的匹配性，从而推动数字技术在嫌疑判断以及以其为基础的犯罪追诉中的合理应用，保障刑事诉讼在数字化转型中的制度稳定性。

关键词：犯罪追诉数字化　犯罪嫌疑　嫌疑稀释　信息密度　数字正当程序

引　言

数字监控、数据分析、预测性算法、人工智能等数字技术工具扩展了刑事司法机关收集和处理信息的能力，使其能够检测到传统方法无法察觉的可疑模式、行为和活动，从而深刻改变着追诉犯罪的过程。例如，大数据分析可以整合来自社交媒体、地理定位数据、财务记录和通信历史等多种来源的信息，构建嫌疑人个人档案，或者识别出犯罪意图的异常情况；预测性警务算法通过过去的犯罪数据，能够预测潜在的犯罪热点，甚至预测个人未来犯罪的可能性；面部识别技术和人工智能驱动的监控系统能够在公共场所识别个人，从而标记出从事可疑活动的嫌疑人。

这些进展从根本上触及了犯罪嫌疑的本质。在刑事诉讼中，嫌疑是推动犯罪追诉活动的重

* 北京航空航天大学法学院教授。
本文系2023年国家社科基金一般项目“数字正义视阈下刑事审判程序数字化法治路径研究”（23BFX142）的阶段性成果。

要触发点，是刑事司法机关针对特定相对人启动具体侦查行为或者适用强制措施的基础。其功能在于确保国家刑罚权的行使是基于客观、合理的依据，而不是出于臆断或者个人偏见。

传统上，嫌疑主要基于可直接观察的特定线索而产生，例如不寻常的行为、不一致的叙述、表明实施犯罪的证据等。在这种情况下，嫌疑的形成受到人类感知和经验判断的固有限制。随着数字技术的兴起，嫌疑的信息来源、范围和生成机制发生了显著变化。嫌疑不再仅仅依赖直接观察到的犯罪证据或线索，而是能够通过数据模式和不显著的信息关联来形成。这一转变为提高犯罪治理能力提供了巨大潜力，特别是在监测或预防犯罪方面，优势尤其明显。但与此同时，数字技术的介入也使得据以判断嫌疑存在与否及程度的信息基础发生变化，并引发有罪推定的事实性扩张、嫌疑阶层界限模糊、干扰执法效能评价、加大相对人辩驳负担等问题。随着数字技术在刑事司法中的应用不断普遍化、常规化和系统化，有必要重新考量刑事司法中的嫌疑概念，并调适相关制度以应对数字技术带来的挑战。

本文着重探讨刑事诉讼制度如何适应数字技术应用对嫌疑概念及其规则体系的冲击，并基于正当程序要求对这种应用予以适当规制。第一部分从犯罪嫌疑的本体出发，明晰其内涵及其形成过程和机制；在此基础上，第二部分分析数字技术介入嫌疑判断的主要形式以及由此形成的嫌疑稀释的整体效果；第三部分进一步剖析嫌疑稀释的具体呈现方式，并由此导出第四部分有关嫌疑稀释冲击刑事诉讼制度的论述；第五部分从刑事诉讼应用数字技术的独特要求出发，提出基于嫌疑程度与信息密度两个维度的数字嫌疑判断结构，以应对上述挑战。

一、传统刑事诉讼中嫌疑的构成

在刑事诉讼中，“嫌疑”是一个基本概念，是启动并推进刑事诉讼程序，适用特定诉讼措施，区分诉讼参与人身份并设置相应权利义务的关键要素。嫌疑，是在特定的制度语境与权力运行场景中，对可能性的一种专业判断。刑事诉讼的一系列制度设计均建立在存在犯罪嫌疑的基础之上。在探讨数字技术对嫌疑概念的冲击之前，有必要对这一概念进行先行解析。

（一）刑事诉讼中嫌疑的界定

在我国刑事诉讼法中，嫌疑主要有以下表述形式。第一种表述形式是与特定主体相关联，用以界定该主体在刑事诉讼中的诉讼地位：其一是指向“犯罪嫌疑人”这种特定类型的诉讼参与人；其二是指向实施犯罪可能性较高的人员，即“重大嫌疑分子”。〔1〕第二种表述形式是与具体作案方式相关联，例如“有流窜作案、多次作案、结伙作案重大嫌疑的”（2018 年刑事诉讼法第 82 条）。其含义与“重大嫌疑分子”相同，表明实施犯罪行为的高度可能性。

除上述直接采用“嫌疑”这一表述的情形外，刑事诉讼中还存在与嫌疑类似且功能相近的表述，典型如“有证据证明有犯罪事实”。以逮捕的适用条件为例，现有规范从正反两方面对“有证据证明有犯罪事实”进行了界定。从正面看，“有证据证明有犯罪事实”包含三层含义：有证据证明发生了犯罪事实；有证据证明犯罪事实系犯罪嫌疑人实施；证明犯罪嫌疑人实施犯罪行为的证据已经查证属实。从反面看，不构成“有证据证明有犯罪事实”的情形主要包括待证事实不构成犯罪、证据缺乏必要印证、证据间存在重大矛盾等情形。〔2〕

〔1〕 例如，在 2018 年刑事诉讼法中，“重大嫌疑分子”主要出现在第 82 条、第 91 条第 2 款、第 115 条。

〔2〕 参见 2010 年最高人民检察院《人民检察院审查逮捕质量标准》第 3 条。

在当前的刑事诉讼法框架中，嫌疑概念一方面与特定人员的身份紧密相连，另一方面与相应的处置决定和措施相衔接。所谓嫌疑，指向的是“凡行为之是否与现行刑事法令相抵触，而尚在揣度之中不能加以断定时之状态”。〔3〕正是在这个意义上，被调查人被称为“犯罪嫌疑人”，是案件进入刑事诉讼程序的重要标志；而某一主体能否具有刑事诉讼法意义上被追诉人身份，“完全取决于客观上是否有针对他的犯罪嫌疑”。〔4〕区别于日常表述中的“嫌疑”，在刑事诉讼的场景中，嫌疑概念主要包含以下要素。

首先，嫌疑本质上是一种可能性——“乃其为某事与否，不能断定，大率揣度其或然耳”。〔5〕这一点包含两方面的含义：一方面，嫌疑指向的可能性具有程度之分。嫌疑可大可小，由此形成与相关刑事诉讼措施的阶层化对应关系。例如在德国刑事诉讼中，存在初始嫌疑、充足嫌疑、重大嫌疑的区分，并对应不同的刑事诉讼阶段和措施。〔6〕另一方面，在整个刑事诉讼过程中，这种可能性处于持续变动的状态，并且其不是单向的线性变动，而是可能随着证据材料的积累而增大、减小或者反复。

其次，嫌疑表达的是一种负面评价，即认为可能存在某种过错。〔7〕在这个意义上，嫌疑与刑事诉讼的被追诉人联系在一起。以嫌疑为基础，刑事司法机关可以有限度、合比例地适用具有强制性的措施，并可以在一定程度上容忍对被追诉人合法权益的合理限制乃至剥夺。

再次，嫌疑对应的可能性判断，需要以特定程度的事实基础为前提。例如在德国法上，单纯的推测不足以启动刑事侦查。〔8〕在美国法上，“合理的嫌疑”（reasonable suspicion）需要具备以具体且清晰的事实为基础的特定客观依据，非此警察不得在公共场合截停并盘查他人。在我国刑事诉讼法上，被调查人能够被称为犯罪嫌疑人，需要以刑事立案为前提，而立案需要在已收集的证据材料的基础上形成有犯罪事实且需要追究刑事责任的判断才能成立。从这个角度看，尽管嫌疑表达的是可能性，但这种可能性需要具有一定程度的精确性。〔9〕

又次，嫌疑针对的是当前正在处理中的犯罪行为，原则上不用于考察和评价过往的犯罪活动，也不用于预防未来可能实施的犯罪活动。这一点将嫌疑与人身危险性、社会危险性等同样表示可能性的概念区别开来。

最后，嫌疑具有明显的程序功能。其一，嫌疑蕴含的评价性具有诉讼程序筛查功能，将没有实施犯罪行为的人与可能实施了犯罪行为的人区分开来，这是对无罪推定原则的程序化表达。其二，存在特定嫌疑是国家机关实施相应诉讼行为的前置条件，即先有嫌疑后有诉讼行为，二者不能倒置，由此防止刑事诉讼程序基于专断或者臆测而启动或者推进。其三，与前一含义相关的是，嫌疑概念天然与特定的国家强制力相关。国家机关不会止步于对嫌疑的判断，而是会基于该判断作出决策并采取行动，进而以此为基础干预公民的基本权利。

（二）传统刑事诉讼中嫌疑的形成

国家机关从接触涉案信息到形成符合刑事诉讼法要求的嫌疑，通常经历了一个由信息识别

〔3〕 郑兢毅、彭时编著：《法律大辞书》，商务印书馆1936年版，第1602页。

〔4〕 参见陈瑞华：《刑事诉讼法》，北京大学出版社2021年版，第223页。

〔5〕 汪翰章主编：《法律大辞典》，大东书局1934年版，第1456页。

〔6〕 参见［德］维尔纳·薄逸克、萨比娜·斯沃博达：《德国刑事诉讼法教科书》，程捷译，北京大学出版社2024年版，第120页。

〔7〕 See Bryan A. Garner (ed.), *Black's Law Dictionary*, 9th ed., West Publishing, 2009, p. 1585.

〔8〕 参见前引〔6〕，薄逸克等书，第117页。

〔9〕 See Emily Berman, *Individualized Suspicion in the Age of Big Data*, 105 Iowa Law Review 463, 468-469 (2020).

到事实判断再到认知确认的过程，其大致包含以下三个阶段。

第一阶段是观察和收集信息。在刑事诉讼中，形成嫌疑的过程通常始于执法人员对异常或可能指向潜在犯罪活动的行为或情况的初步观察。执法人员基于系统培训与经验积累，能够对上述征兆保持警惕并形成敏锐的观察力，从而利用其经验和情境意识来识别与社会规范、常规行为模式等相悖的行为。在这一阶段，嫌疑形成的信息来源多种多样，包括但不限于执法人员的直接观察、公民的报案或举报、国家机关之间的线索移交等等。执法人员通常依赖诸如时间、地点、个体行为等特定线索，评估是否有必要开展进一步调查。

第二阶段是基于信息的事实评估。在这一阶段，公安司法人员需要对各类线索材料进行筛选、分析与关联建构，识别出支持其怀疑的具体、可表述的事实，从而形成刑事诉讼中嫌疑的事实基础。事实评估在很大程度上受限于公安司法人员个人的能力和经验，针对特定区域、领域或群体犯罪模式的熟知，往往可以强化并合理化公安司法人员对事实的判断。该阶段是嫌疑判断从信息积累向事实构造转化的关键阶段，要求公安司法人员在尽可能排除主观臆测与经验误判的基础上，确立信息之间的逻辑链条，评估这些信息在支撑犯罪嫌疑认定中的解释力。

第三阶段是在事实基础上的认知评估，即将所认定的事实向法律层面的嫌疑进行转化。这是公安司法人员的心证过程，即在心理层面判断已掌握的事实是否达到嫌疑门槛。区别于事实评估中对客观信息和可观察行为的关注，此阶段更侧重于在公安司法人员的心理过程和认知机制中，嫌疑的判断可能受到公安司法人员过往经验、情绪、情境、偏见等因素的潜在影响。

在传统刑事诉讼中，上述嫌疑形成过程具有以下特征：首先，嫌疑具有特定性，即针对的是特定事件中处于特定时空维度下的特定个体。公安司法人员通常依赖事件发生的具体时间节点来评估嫌疑，这意味着某些行为在特定时间内可能被视为可疑行为，在其他时间则可能被忽视。嫌疑往往也与特定地点密切相关，公安司法人员必须识别嫌疑人与事件发生地点之间的联系，这种联系的识别常常嵌入特定区域的社会结构、文化背景以及地方性犯罪模式之中。

其次，嫌疑形成所依据的是相对分离的事实、有限的信息、局限的背景、稀缺的知识等“小数据”，〔10〕反映的是刑事司法机关（特别是侦查机关）基于经验和一定证据量对可能性的判断。一方面，嫌疑的形成往往依赖公安司法人员个人的具体观察和经验，信息的获取和分析相对零散。另一方面，对有限信息之间关联关系的判断，高度依赖公安司法人员的主观评价，在信息的交叉验证方面相对较弱。上述两方面特点意味着，传统个案中嫌疑判断的差异往往是非系统性、偶发性的。

再次，嫌疑形成过程的启动多具有被动性。执法人员收集信息并形成嫌疑所依赖的事实基础，更多是一种被动的过程，即仅在报案、线索移送等外部触发条件出现后，国家机关方能介入。这与刑事司法自身的被动性密切相关，而与诸如国家安全等场景下情报导向的主动监测、收集、评估具有明显差异。

最后，嫌疑的判断，一方面与执法人员的过往经验联系紧密，另一方面强调一般人的理性认知，但这二者不完全一致。一般人的理性认知通常构成确认嫌疑的底线要求，以限制主观判断的随意性，并在程序中承担着质疑和纠偏的功能。相较而言，执法人员对嫌疑构成的判断具有更专门的经验积累，以及在此基础上形成的更强的专业性。二者对比，过往经验在执法人员

〔10〕 See Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 University of Pennsylvania Law Review 327, 329 (2015).

的嫌疑判断中作用更大，因而其判断过程多具有时间更短、确认更早、依据材料相对更少等特点。上述特征一方面给予了执法人员一定的裁量空间，另一方面也容易影响嫌疑判断的客观性和中立性，尤其是在信息不足、情境复杂的情况下，缺乏必要规制的经验主义判断可能转化为刻板印象的固化与认知偏误的系统化。

二、数字技术对嫌疑形成机制的改造

数字技术与犯罪追诉的结合，开始逐渐改变刑事诉讼中嫌疑的形成和认定，大数据、人工智能等技术的迭代更新更是强化了这一趋势。一方面，通过数据的广泛汇聚、融合、挖掘，作为自然人“孪生体”的数字人不断立体化和丰富化，〔11〕开始成为国家机关了解该自然人的媒介，进而使原先处于刑事司法体系认知之外的个体进入到该体系。另一方面，基于数字技术的应用，一些关于相对人更深层次、更多维度的信息以及由信息推导出的行为模式等有可能被揭示出来。上述变化均在影响着嫌疑的概念以及与之相关的制度设计。

（一）数字技术与嫌疑判断的融合场景

数字技术与嫌疑判断的融合程度，往往与打击犯罪的具体场景密切相关。整体而言，数字技术介入嫌疑判断大致以两种路径进行：一是以人工智能等机器的结果输出作为嫌疑评价的整体基础，其既可能表现为所有要素均由机器决定，也可能表现为模型要素与人类添加要素的组合，人类介入则是在机器作出最终判断之前。二是以机器判断结果整体作为参考因素，由人类结合自身判断作出整体性结论，此时人类介入则是在机器决策之后。从目前有关技术的应用看，基于对机器决策取代人类决策的谨慎态度，相关应用主要呈现的是第二种路径。我们大致可以识别出该路径下的四种主要场景，其中数字技术介入嫌疑判断的程度是逐次上升的。

第一种场景是执法者亲身观察到实施过程的犯罪。这种场景中最典型的就是现行犯。在该场景中，数字技术的应用主要从两方面辅助推进嫌疑的判断：一是拓展执法者的观察范围，从而快速且规模化地对犯罪行为进行识别；二是通过关联相关涉案信息，使执法者能够形成特定嫌疑人生活、工作、社会关系等方面的综合画像，识别其身份、追踪其行踪轨迹、厘清作案组织关系等。例如警务无人机的高空侦查和建模性能极大地提升了侦查人员的视野和隐蔽性，同时通过链接数据智能化分析系统、大数据平台等可以快速比对、识别特定人像、车辆等数据。以2022年湖南省永州市公安局侦破的聚众赌博案为例，该案中侦查人员通过无人机对23层高楼顶层的聚众赌博全过程进行了远距离高空拍摄取证，对参赌人员进行逐个视频固定和智能化视频分析、比对，作为开展后续犯罪追诉活动的基础。〔12〕

第二种场景是执法者未亲身观察到实施过程的已发生的犯罪。区别于上一场景，此时执法者并无明确的追诉对象。如果说上一场景中数字技术的功能主要是强化执法者对特定主体的认知，在第二种场景中，数字技术的首要功能则是确定特定主体，即在先行构建的犯罪模型的基础上，将碎片化的数据进行聚合、关联、比对，逐步建立犯罪线索，进而从社会公众中排查出特定的可能涉案人员。该场景在近年来的电信网络诈骗治理领域较为典型，例如北京市检察系

〔11〕 See Danial Solove, *The Digital Person : Technology and Privacy in the Information Age*, NYU Press, 2004, p. 18.

〔12〕 参见沈林：《警务无人机智能化实战应用及常用战法研究》，https://www.faanw.com/zhihuijingwu/14769.html，2025年1月5日最后访问。

统建立了涉“两卡”案件漏犯漏罪大数据法律监督模型，以涉案人员及上下游人员身份强制登记所形成的数据池为基础，通过数据比对碰撞来发现可能遗漏的犯罪嫌疑人或案件。〔13〕又如，在2022年江苏省宿迁市的一起变压器电缆线盗窃案中，因案发位置偏僻没有监控，前期侦查过程中未能提取到有效物证，难以确定犯罪嫌疑人，后通过其智慧侦查中心开发的针对盗窃“三电”设施的图技一体化模型，进行数据碰撞和比对，在30分钟内锁定了犯罪嫌疑人。〔14〕

第三种场景是执法者未亲身观察到的可能正在实施的犯罪。在这一场景中，执法者对于是否发生了犯罪仅存在较低层次的怀疑，尚不足以达到刑事立案的程度，需要进一步收集线索。此时数字技术的应用主要是发现可疑线索，帮助执法者识别特定行为模式进而监测犯罪活动。执法者的认知和经验在嫌疑生成过程中的作用比重进一步下降，犯罪追诉也开始由被动向主动转变。例如广东省中山市公安局构建的“缉枪神探”数据模型，从寄递物流信息、身份背景信息、网络行为信息等维度挖掘网络贩卖枪支的可疑线索或高危人员，从而推进后续犯罪侦查。〔15〕又如江苏省南京市公安局研发的“非法处置危险废物数据研判平台”，以硫酸购买与处置记录间的异常差异，作为判断是否存在偷排酸洗废液嫌疑的重要指标，并以此为基础对模型研判出的可疑企业进行立案侦查。〔16〕近年来，我国数字检察法律监督的探索也反映出类似思路，基于数字模型分析形成从个案到类案的主动监督，即“在智慧裁判监督系统的帮助下，运用大数据快速抽取同案要素、发现异常类案。在此基础上，检察官再通过人工筛查，形成合理怀疑。初查后交由公安机关立案，并积极引导侦查”。〔17〕

第四种场景是执法者未亲身观察到的可能将要实施的犯罪。此时数字技术发挥着根据既有模型预测和提示犯罪风险的功能，代表性应用是预测警务。在此场景中，执法者通过大数据分析和人工智能算法，能够迅速处理海量数据，挖掘出潜在的犯罪模式和行为特征。同时，物联网设备、监控摄像头、智能传感器的广泛部署，为实时跟踪和定位潜在犯罪嫌疑人提供了技术支撑，从而有效减少侦查中的信息盲区。此外，数字技术还能通过分析社交媒体活动、通信记录和消费行为等，整合数据以构建高风险人群画像，从而揭示其动机和潜在风险。有学者概括出预测警务的基本逻辑：“通过理论和实证研究选择和验证客观的、机制性的、可重复的预测因素，将这些预测因素运用于通过大数据技术收集和处理的大量数据，在分析技术（算法）的支持下获得犯罪的概率或者预期值，这一概率或者预期值将成为指导警察行动的重要依据。”〔18〕近年来，我国公安系统开展的“情指勤舆”一体化实战平台建设，将预测警务推进到一个更高的阶段。例如安徽省公安厅针对中小学幼儿园个人极端事件搭建的智能研判预警“前哨”系统，通过布建前端多维感知网络、搭建风险人员全系档案库、搭建智能研判模型、建立智能预警防范处置机制，以期实现“对个人极端苗头动向早发现、快反应”。〔19〕

---

〔13〕 参见《破解“两卡”犯罪打击治理难题》，https://www.spp.gov.cn/spp/zdgz/202310/t20231031_632584.shtml，2025年1月5日最后访问。

〔14〕 参见徐同凯：《新形势下智慧侦查的实践探索》，《中国刑事警察》2022年第5期，第18页。

〔15〕 参见刘鹏：《网络涉枪犯罪侦查：现状、问题与路径》，《中国人民公安大学学报（社会科学版）》2021年第3期，第44页以下。

〔16〕 参见《南京警方研发“非法危废处置研判平台”，数据分析挖掘污染环境犯罪线索》，https://www.yzwb.net/zncontent/1390594.html，2025年1月6日最后访问。

〔17〕 胡铭：《论数字时代的积极主义法律监督观》，《中国法学》2023年第1期，第117页。

〔18〕 陈永生：《大数据预测警务的运作机理、风险与法律规制》，《中国法学》2024年第5期，第167页。

〔19〕 参见《防范处置中小学幼儿园个人极端案事件，智能研判预警“前哨”系统》，https://www.anpcn.com/gongan/3055.html，2025年1月6日最后访问。

上述四种场景的划分并非泾渭分明，且在实践中日趋融合。之所以进行场景类型化分析，是便于识别出一些有关嫌疑形成的演变规律和趋势。可以看到，上述四种场景中，一方面执法者对于特定相对人的基于亲身经验的认知逐渐弱化，另一方面据以形成嫌疑的信息基础逐渐脱离特定个体。二者相结合事实上造成了嫌疑稀释的后果。

（二）数字化的整体影响：嫌疑的稀释

总体而言，犯罪嫌疑本身是一个整体性判断，是刑事司法机关对其掌握的所有涉案信息的综合性考量。〔20〕在进行嫌疑判断时，考虑到其与后续犯罪追诉行为之间的对应关系，判断的重点往往是嫌疑的程度，即综合评价各种信息之后，是否达到了使刑事司法机关开展特定诉讼行为所需的犯罪嫌疑水平。

在有限数据的传统场景下，公安司法人员对嫌疑的判断所依赖的信息无论在类型上、体量上还是范围上，均大致可以事先明确。尽管执法人员在判断犯罪嫌疑时也会引入案外因素，例如根据嫌疑人过往经历、特定社会身份或行为习惯等主观经验作出初步判断，但如前所述，这种判断通常高度依赖执法人员的职业能力和经验基础，因而不具有结构化、系统化的特征。对此，刑事诉讼制度的回应以个案调控为主，依靠事后监督和程序救济来实现对违法或不当判断的纠偏。

随着国家机关掌握的背景信息越来越多，客观的、直观的、现实的具体行为在判断行为人是否可疑时的权重不可避免地会被稀释。〔21〕这种背景信息不仅限于行为人所处的环境，还包括行为人本身。以1996年的“奥尼拉斯诉美国案”（Ornelas v. United States）为例。〔22〕在该案中，警察注意到汽车旅馆前停着一辆1981年双门奥兹莫比尔牌汽车，根据警察的经验，贩毒分子在交易中经常使用这款汽车。随后警察根据车牌追查到车主奥尼拉斯，并在联邦麻醉品和危险药品信息系统中找到了奥尼拉斯的名字和过往违法行为记录。基于以上信息，警察对奥尼拉斯进行了盘查。可以看到，在该案中警察并未实际观察到任何具体可疑行为，但美国最高法院仍然认为，以上信息足以构成美国宪法第四修正案所规定的“合理根据”。与之类似，我国目前也有思路相同的风险评估软件，通过分析日常行为数据来评估某人实施犯罪的可能性，这些行为可能包括诸如频繁前往交通枢纽、购买法律书籍、前往刀具店等，其单独看并不具有明显的异常性，但组合在一起则可能使系统提升对该人犯罪风险等级的评估。〔23〕

当对行为人个人信息的事前知悉在侦查决定中的作用上升时，是否采取特定追诉措施的决定基础，不可避免地会由具体可疑行为的现实观察转为基于前期数据收集、分析所形成的风险预判。这恰恰是大数据以及以其为基础的司法人工智能的核心要义——通过数据挖掘来发现模式，通过模式提纯来形成预判，运用预判来提前干预行为。〔24〕

随着社会数字化转型的不断深入，达成某一程度嫌疑所需要的信息，无论在总量上，还是结构上均开始发生转变。从总量看，有更多的外部信息涌入国家机关的嫌疑判断之中。这些信息开始逐渐超出执法人员的自身经验和具体个案观察，而向着一般化、群体化的方向发展；同时，国家机关掌握的信息越多，越容易在外观上达成实施特定诉讼行为所需要的嫌疑

〔20〕 See Wesley M. Oliver *et al.*, *Computationally Assessing Suspicion*, 92 University of Cincinnati Law Review 1108, 1111 (2024).

〔21〕 参见前引〔10〕，Ferguson文，第341页。

〔22〕 Ornelas v. United States, 517 U. S. 690 (1996).

〔23〕 参见黄泽政、李双其：《回应犯罪演变的智慧侦查》，《湖南警察学院学报》2022年第2期，第9页。

〔24〕 See Julie E. Cohen, *What Privacy is for*, 126 Harvard Law Review 1904, 1920-1921 (2013).

程度。〔25〕此时，在相同程度的嫌疑内，聚焦具体个案的信息的比重在下降，脱离具体个案、基于案外因素所形成的信息的比重在上升，单个信息与案件事实的关联逐渐模糊，进而形成了事实上的“普遍嫌疑”。〔26〕更重要的是，随着算法建模、数据画像与风险评估等工具广泛介入嫌疑形成过程，案件外因素的系统性引入已由偶发行为演变为常态化结构。此种变化不仅拓展了嫌疑所依据的信息边界，也使得刑事诉讼程序面临从个案控制走向制度性规制的转型需求。

如果以具体案件事实作为评价达成特定嫌疑程度所需的信息质量基准，则上述变化可以描述为嫌疑的稀释，所形成的结果是嫌疑的信息密度下降。具体而言，嫌疑稀释指向的是这样一种现象：在嫌疑判断过程中，随着用于判断的信息范围扩大、来源多元化、类型多样化，直接指向具体犯罪事实的核心信息在全部信息结构中所占的比例和权重均下降。

究其核心，嫌疑稀释集中表现为在质和量两个维度上由核心信息逐渐向弱关联度信息的拓展，这一拓展由内向外可以粗略地划分为以下层次：（1）位于中心的是传统嫌疑判断的关键信息，即当下具体案件中可直接观察到的某人是否实施特定可疑行为的相关信息。（2）向外拓展的第二层涉及非直接可观察的、甚至是非可疑行为的信息，这些信息之所以进入公安司法机关的视野，是因为其与所涉案件特定时空上的关联。（3）向外拓展的第三层则进入到特定个人非原生的当下静态社会信息，诸如违法犯罪记录、婚姻状况、雇佣状态、资金情况等。这些信息并非该个人与生俱来的信息，其在当下的犯罪追诉中与特定行为的成因有密切关系。（4）向外拓展的第四层涉及特定个人非原生的历史动态身份信息及其积累，例如行为习惯、社交关系、生活履历等。这些信息虽然逐渐脱离正在办理的具体案件，但对于形成针对该人的社会评价具有重要借鉴意义。（5）到目前为止，各层信息仍然以特定个人为中心并与之发生直接联系。嫌疑判断信息向外拓展的第五层则开始与具体个人产生一定距离，考察的是诸如种族、性别、生物特征等原生性特征。这些信息与个人相关，却并非基于对个人自身特点的分析，而是以个人的某项社会属性所代表的群体为分析对象。（6）再向外拓展的第六层，碎片化的信息甚至无法与特定个人、特定案件建立联系，但整合之后能够揭示某种常规判断所难以识别的关联关系。例如针对电信网络诈骗所采用的聚类算法，其核心在于“通过全局分析和高危空间聚类，在无诈骗样本数据的情况下找出数据中隐含的共同特征，从而完成大规模关联诈骗团伙的自动发现”。〔27〕

上述信息圈层可以大致分为三个层级：第一层和第二层的一部分与具体个案的联系较为紧密，特别是可以直接指向所涉犯罪事实的线索和证据材料（核心圈层）；第三层和第四层的信息尽管与个案事实本身联系较弱，但仍然可以通过特定相对人本人的个体情况与个案建立起联系（辅助圈层）；第五层和第六层的信息则与具体个体本身相脱离，向着更为宽泛的数据领域拓展，甚至可能从直观上毫无关联的数据中挖掘出关联关系（背景圈层）。随着执法人员可以接触的数据量以及掌握的数字技术不断拓展和迭代升级，上述圈层也处于持续的变化之中，但从中可以识别出所蕴含的一些基本逻辑。

在前文论及的四类数字技术嵌入嫌疑判断的典型场景中，不同场景依赖的信息圈层结构存在显著差异，对嫌疑信息密度的影响路径亦各不相同。第一类“执法者亲身观察到实施过程

〔25〕 See Jane Bambauer, *Hassle*, 113 Michigan Law Review 461, 465-467 (2015).

〔26〕 参见施鹏鹏：《“普遍嫌疑”及其规制：以德国法为借鉴》，《中外法学》2024年第1期，第199页以下。

〔27〕 参见中国信通院：《电信网络诈骗治理与人工智能应用白皮书（2019年）》，http://www.caict.ac.cn/kxyj/qwfb/bps/201912/P020191230550658803494.pdf，2025年1月20日最后访问。

的犯罪”场景，往往依赖核心圈层信息，如直接可观察的行为、现场证据与即时反馈，该类信息与案件事实的关联性最强，因而信息密度最高，数字技术应用的冲击亦相对较低。第二类“执法者未亲身观察到实施过程的已发生的犯罪”场景，数字技术主要协助识别涉案线索和行为人身份。除部分核心圈层信息外，需依赖较多辅助圈层信息（如活动轨迹、行为模式、身份背景等）进行交叉印证，嫌疑的判断由此转为以间接证据拼接形成，信息密度呈下降趋势。第三类“执法者未亲身观察到的可能正在实施的犯罪”场景，更倚赖系统性研判和风险识别，信息基础进一步向背景圈层延伸。此时，信息的个案关联性弱化，群体特征和历史行为成为嫌疑判断的触发条件，信息密度明显降低。第四类“执法者未亲身观察到的可能将要实施的犯罪”场景，基本完全构建于非案件特定的高维数据模型和异常行为特征之上，主要依托背景信息和数据聚类算法，嫌疑信息密度降至最低，嫌疑判断机制几乎脱离了个案维度。

可以看到，不同信息圈层的适用差异，意味着嫌疑判断的信息基础不仅在量上呈现扩张趋势，更在结构上出现了由紧贴个案向远离案件核心的系统性偏移，即辅助圈层和背景圈层信息在嫌疑判断中的权重借由机器表达而不断上升。在此过程中，若无适当机制对不同圈层信息的应用进行分层控制，就可能导致嫌疑判断标准与国家权力介入程度之间的对应关系发生失衡，进而弱化程序法对公民权利的保障。因此，信息圈层结构不仅应成为刑事诉讼中评估嫌疑程度的基础，也应成为设置嫌疑门槛与审查刑事程序正当性的核心依据之一。

三、嫌疑稀释的底层逻辑

在数字技术的影响下，刑事诉讼中嫌疑判断所依赖的信息圈层正在经历由内向外的拓展。在忽略前述信息圈层差异的情况下，如果以综合考量的方式来衡量嫌疑的程度，那么国家机关掌握的信息量越大，就越容易满足特定执法或司法行为所需要的嫌疑程度。〔28〕这一变化并非单纯的嫌疑信息量的变化，而是对传统的嫌疑构成及其基础逻辑均会产生影响。

（一）从个体分析转向群体分析

嫌疑稀释，首先促使刑事诉讼的决策基础由个体分析向群体分析转变。如前所述，传统意义上的嫌疑是个体化的嫌疑，即犯罪追诉机关在判断嫌疑时所依赖的证据材料需指向实施特定行为的特定个人。换言之，犯罪追诉机关“不应当以刻板印象、假设、以偏概全或其他泛化的方式作为判断依据”。〔29〕嫌疑的个体化判断至少具有三层含义：第一，某人与其他具有实施犯罪嫌疑的人员之间的相似或邻近关系本身，不足以单独构成判断该人是否具有以及具有何种程度嫌疑的依据。第二，这种嫌疑的形成应当基于某人在涉及具体案件时的特定行为，而非基于该人的身份。〔30〕第三，嫌疑的评价原则上不应基于统计学或者概率分析，尤其要避免数值化的判断方式。〔31〕

在与数字技术的结合过程中，这种个体化的嫌疑开始向群体性的嫌疑转变。在当前的技术发展阶段，大数据和人工智能技术在犯罪治理中的应用，首先是基于基本模型的构建，其次是

〔28〕 参见前引〔10〕，Ferguson文，第387页。

〔29〕 See Andrew E. Taslitz, *What is Probable Cause, and Why Should We Care ?: The Costs, Benefits, and Meaning of Individualized Suspicion*, 73 Law and Contemporary Problems 145, 146 (2010).

〔30〕 See Ric Simmons, *Quantifying Criminal Procedure: How to Unlock the Potential of Big Data in Our Criminal Justice System*, Michigan State Law Review 947, 985 (2016).

〔31〕 参见前引〔25〕，Bambauer文，第461页以下。

投喂公共或私有数据以识别行为模式，进而基于系统的自动化方式或经由执法人员引导，将具体人员与相应的可能性等级进行匹配。在这一过程中，无论是基本模型还是之后的行为模式，所依据的均不只是特定案件中的具体行为分析，而是基于统计性算法，其核心是基于群体数据所形成的行为模式识别。〔32〕

更重要的是，这种转变最终会影响到立法和司法实践关于个体外因素的总体态度。在传统“小数据”场景下，立法和司法实践总体上对这种泛化的个体外因素的引入是持制约态度的，即尽可能压缩泛化因素在个案嫌疑判断中的应用空间，并以此为标准评价后续处置行为的合法性。在与数字技术的结合之下，群体性分析不仅在嫌疑判断中的比重上升，其甚至可能逐渐演变为嫌疑判断的先行步骤乃至基础。基于类似观察，有研究指出，新兴数字技术的应用在嫌疑判断的过程中降低了传统执法中确定嫌疑所需花费的社会成本，但伴随的潜在代价是执法相对人的泛化。〔33〕

（二）对象由自然人转向数字人

尽管嫌疑的实质判断开始脱离具体案件中的个人行为，但从数字技术应用所呈现的表象看，又反映出强烈的对特定个人的关注，特别是通过各种数字痕迹的追踪，似乎可以勾勒出该人立体且具有动态属性的数字形象。国家机关的数据收集和汇聚，使其可以掌握某具体个人更多的信息，呈现出一种将陌生个体转变为执法机关知识领域内个体的表象。然而，这种信息的聚合、分析以及由此描绘出的个体形象是预判式的、先决性的、标签化的数字人，其并不必然与现实社会中的真实个体全面对应。更重要的是，这种基于数字人的嫌疑判断可能造成国家机关熟知相对人的错觉，进而冲淡对真实相对人的关注。

在此背景下，犯罪追诉活动的相对人一定程度上发生了身份的分离。与之相对应，刑事司法机关在决定是否以及在何种程度上适用干预措施时，也发生了判断依据与适用对象的分离，即判断上更多依赖对数字人的评价，而措施适用针对的是具体的、现实的个人。二者之间形成了“数字孪生”语境下复杂的互动关系：对数字人的判断会直接或间接影响对现实人的处置，对现实人的处置又会进一步融入后续对数字人的判断之中；在这一过程中，不断有脱离现实人的其他因素进入到数字人的构成。

上述过程可能产生三方面影响：第一，针对现实人的众多社会评价要素在嫌疑判断中的比重并非同步变化，部分要素（特别是负面评价要素）更容易自强化，其他中性要素以及正面要素则可能被弱化乃至忽略。第二，群体化现象进一步强化，个性化因素进入到嫌疑判断要素体系中的难度会相应提升。第三，在前述两方面影响的共同作用下，数字人与现实人之间实非镜像关系，二者可能发生偏离。

（三）从事实导向转向情报导向

在形成嫌疑判断的信息基础不断向外围拓展的过程中，“预测”“预防”等表述开始广泛出现在犯罪治理领域。将杂乱的信息点连接起来，可以勾画出从某一个体的历史事实到未来犯罪行为之间的“路线图”，〔34〕从而试图通过斩断中间的通道而达到阻却犯罪的效果。

这一思路正是情报导向的典型体现。长期以来，刑事司法往往与国家安全执法存在区别，

〔32〕 See Tatiana Dancy, *Artificial Justice*, Oxford University Press, 2024, p. 2.

〔33〕 参见前引〔25〕，Bambauer 文，第 461 页以下。

〔34〕 See Equivant, *Practitioner's Guide to COMPAS Core*, issued in 4 April 2019, p. 3, available at https://equivant-supervision.com/wp-content/uploads/2023/05/equivant-Practitioners-Guide-to-COMPAS-Core-MAKE.pdf, last visited on 2025-01-03.

二者的核心差异之一是信息收集处理的逻辑不同。刑事司法以事后应对为起点，形成了以案件事实为核心的信息收集层次，案件事实构成了嫌疑的基础。国家安全执法的关注重点则是事前的能动性处置，其依赖对各种情报信息的广泛收集和分析。随着信息技术的发展以及防患于未然的现实需求，主要运用于国家安全领域的情报思路开始向刑事司法领域扩展。〔35〕与之相适应，犯罪嫌疑的形成机制从事实导向开始向情报导向转变。前者以执法机关被动获得的有关特定事件的信息为基础，是对即时性和可观察到的行为或证据的回应。后者则以数据分析和趋势判断为重点，从而在可能性分析和模式识别的基础上，对潜在犯罪风险进行主动应对。〔36〕

事实导向与情报导向的嫌疑判断之间的区别，可以进一步细化为以下方面：第一是嫌疑的信息来源不同。事实导向的犯罪嫌疑以实时观察、各类证据材料以及直接的和特定情境下的触发事件为基础，情报导向的犯罪嫌疑则形成于包括犯罪数据、社会网络分析、监控数据等在内的多种信息源，通常包含的是与犯罪事实仅有间接关联的线索。第二是嫌疑形成的关键时间点不同。事实导向的犯罪嫌疑通常在具体犯罪或可疑行为出现之后形成，情报导向的犯罪嫌疑则在犯罪实施或被发现之前即已有痕迹。第三是嫌疑关注的视野范围不同。事实导向的犯罪嫌疑关注的事项范围相对较窄，以特定事件相关的行为人或即时状况为核心。情报导向的犯罪嫌疑关注的范围较广，与被评价为高风险的人员相关的社会网络、热点区域、档案信息等均可能被纳入观察范围。第四是判断和评价嫌疑的机制不同。事实导向的犯罪嫌疑主要依赖特定执法人员对具体事件以及其中可观察到的要素的考察，情报导向的犯罪嫌疑判断则依赖数据分析、策略制定以及相关部门之间的协作。

（四）从人类理性转向机器理性

传统犯罪嫌疑的判断，依赖执法人员在具体案件中对特定可观察到的事项的判断；在评价嫌疑的合理性时，对应的是以该执法人员为代表的一般理性执法者的判断。嫌疑判断所依赖的信息圈层的向外拓展，在纳入更多信息来源和信息量的同时，也引入了机器的自动化判断。在此背景下，嫌疑的判断逐渐从以自然人为基础的理性执法者标准向机器理性标准转变。尽管对于理性概念存在多种多样的解读，但当我们说某一主体是理性的，往往包含两项评价标准：一是该主体能够实现其目标，并且这一目标表现为效用最大化；二是该主体能够在实现效用最大化的同时，最小化其资源的消耗。〔37〕有研究指出，与机器相比，人类作出理性决策主要面临三方面挑战：一是信息的有限性及信息缺陷；二是头脑处理信息的能力有限且不一致；三是决策难以优化。〔38〕

数字技术的介入旨在克服上述缺陷，使决策向着更为理性的方向发展。但是，机器理性与人类理性在目标和功能上并不等同，甚至二者在界定“理性”时就存在差异。机器理性的基础是形式化的算法、计算模型和编程规则，其运行严格遵守逻辑论证、优化技术和清晰的预定目标。人类理性则受到情绪、认知、社会规范、个人经历等因素的影响，通常包含直觉性或启发式的论证过程，其目标设定也可能是不清晰的、主观化的、甚至是彼此冲突的。在涉及不确定性时，机器理性主要依赖概率推理、统计模型或者基于贝叶斯定理的算法等方式加以处理，而人类理性经常通过经验或演绎的方式寻求结论。从评价方式看，机器理性是结果理性，其达

〔35〕 参见李训虎：《侦查情报化之批判》，《法学》2024年第7期，第125页以下。

〔36〕 See OSCE, *OSCE Guidebook : Intelligence-Led Policing*, issued on 3 July 2017, p. 13, available at https://www.osce.org/chairmanship/327476, last visited on 2025-01-03.

〔37〕 See Tshilidzi Marwala, *Rational Machines and Artificial Intelligence*, Academic Press, 2021, p. xi.

〔38〕 同上书，第111页。

到理性结果的过程可能不为人所理解，或者与人类形成理性结果的过程全然不同。

机器理性与人类理性的上述差异，不可避免地会影响到二者对犯罪嫌疑的判断。特别是在机器参与不断上升、嫌疑的信息基础逐渐脱离具体执法者经验认知范围的情况下，上述影响会进一步显现。

四、嫌疑稀释趋势下刑事诉讼面临的挑战

从整体看，更多信息通过数字技术进入刑事司法机关治理犯罪的系统，是刑事司法体系随时代同步演进，充分利用数字技术以提升犯罪治理整体效能的客观结果。在进一步探讨嫌疑稀释对刑事诉讼制度的冲击之前，有必要先行说明后续探讨所依赖的基础性前提。首先，嫌疑的判断并非一成不变，而是会随着社会发展不断演进。其次，“存在犯罪嫌疑”并非国家机关干预公民基本权利的必要条件，典型如在机场、火车站等大型公共交通场所，乘客需要不加区分地接受具有一定强制性的安全检查。再次，刑事诉讼中的嫌疑是一种制度安排，其具有调节和规制国家行为的功能。最后，从前几项前提延伸出的一个适当推论是，嫌疑的信息圈层外扩并不必然与公民权益保障相矛盾。换言之，二者并非此消彼长的零和关系；相反，在适当的制度设计下，二者理应是同步增长关系。〔39〕这就涉及在技术演进背景下制度调整方向的问题。

除上述前提之外，也需要对数字技术介入犯罪嫌疑判断所产生的正向价值予以肯认。从最直接的角度看，数字技术的应用可以提升执法者进行嫌疑判断的效率。执法的资源性成本由执法机关自行承担，相关技术的自发应用即可以反映出这一价值。此外，数字技术的应用也可能产生以下方面的效用：一是提升区分普通公民与可疑人员的精准度；二是提升嫌疑判断的整体性和全面性，能够融入更多对非罪性因素的考量；三是压缩执法者的裁量空间，避免出现无合理理由支撑的决策；四是通过数字技术，犯罪追诉系统涌现出全局犯罪模式洞察的能力。〔40〕

从这个角度讲，探讨刑事诉讼在嫌疑稀释趋势下面临的挑战，更多是一种中立性的判断，是在确认刑事司法与数字技术融合的总体趋势之下，对二者适配性的系统化调适。其关注的核心问题是，通过数字技术介入所形成的嫌疑判断，是否存在冲击刑事司法基石的风险，以及是否有必要进行制度调整。对于这种调整，主要从两个维度进行考察：一是嫌疑稀释对规制国家机关行为的影响；二是嫌疑稀释对公民基本权益的影响。从这两重维度出发，可以观察到刑事诉讼制度可能面临的以下方面的挑战。

（一）有罪推定的事实性扩张

2018 年刑事诉讼法第 12 条强调，“未经人民法院依法判决，对任何人都不得确定有罪”。犯罪嫌疑的确认尽管不等同于有罪判决，但嫌疑的积累会逐步导向最终的有罪判决。长期以来，关于大数据、人工智能等数字技术介入刑事司法的一个主要担忧就是，这些基于过往数据而形成的机器判断可能强化有罪预判。〔41〕从嫌疑的形成过程以及所依赖的信息基础看，数字

〔39〕 See Ric Simmons, *Smart Surveillance: How to Interpret the Fourth Amendment in the Twenty-First Century*, Cambridge University Press, 2019, pp. 5-10.

〔40〕 参见前引〔20〕，Oliver 等文，第 1108 页。

〔41〕 See e. g., Athina Sachoulidou, *Going Beyond the "Common Suspects": To be Presumed Innocent in the Era of Algorithms, Big Data and Artificial Intelligence*, Artificial Intelligence and Law, online published on 22 February 2023, available at https://link. springer. com/content/pdf/10. 1007/s10506-023-09347-w. pdf, last visited on 2025-01-08; Joshua A. T. Fairfield & Erik Luna, *Digital Innocence*, 99 Cornell Law Review 981, 981 (2014).

技术介入嫌疑判断所导致的嫌疑稀释效果，在一定程度上简化甚至异化了这种形成过程，从而在事实上造成了法院定罪之前有罪推定的扩张。

当前的研究主要观察到这种简化或异化三个方面的主要来源。首先，大数据、人工智能等数字技术的技术原理使其可能强化社会已有偏见和刻板印象。〔42〕对此，有关司法中算法歧视的讨论已经较为充分。〔43〕其次，过往数据中存在的不利要素以及由此形成的嫌疑判断会影响执法资源的分布。由于内嵌既有数据和执法反馈，算法决策的结论往往会通过这种反馈循环得到自我验证。再次，数字技术的上述效果会进一步引发犯罪防控方面的“棘轮效应”（ratchet effect），即在特定情况下系统或行为倾向于只朝一个方向演进而难以回归原状。具体到犯罪治理领域，该效应呈现为如下状态：如果某些因素已被认为与较高的犯罪水平相关，预测算法就会促使国家机关对具备这些因素的嫌疑人加大追查力度，结果导致更多符合该因素特征的人被捕，从而“验证”了这些因素与犯罪之间的关联。〔44〕长期来看，上述机器决策自我强化的机制可能进一步加剧嫌疑判断标准的失真。

从刑事诉讼的角度看，嫌疑信息基础向外层信息圈层的拓展，将历史犯罪数据、人口统计信息、社交媒体活动等信息纳入嫌疑判断的范围，使得一些尚未被正式立案的人员，可能仅因算法评估的高风险而被纳入执法机关的监控视野，甚至可能遭受不必要的调查和干预。由于案件尚未正式立案，这些人员尽管面临的是针对犯罪或犯罪风险的涉刑事评价，却难以获得刑事诉讼法所提供的权益保障。同时，犯罪嫌疑中针对人而非行为的比重加大，使得相对人需要进行反驳和辩护的事项不仅限于当下具体案件，还需要面向其过往经历、事项和数据等，一定程度上加重了相对人“自证清白”的任务量和总体难度。此外，机器判断的介入使得相对人更容易被常规化地认定为高风险或者进入高概率匹配名单，而且由于其采用的是“除非有相反证据否则认定为有嫌疑或风险”的逻辑，从该名单移出的难度事实上更大。〔45〕更重要的是，在忽视前述嫌疑稀释的情况下，形式正当程序可能会进一步偏离实质正当程序。某种程度上看，此时刑事诉讼程序在处置端越强调公正、平等对待，其在嫌疑形成端所存在的有罪倾向越有可能被掩藏和固化。〔46〕

（二）嫌疑阶层界限的模糊化

如前所述，犯罪嫌疑并非单纯的事实判断，而是具有规制国家机关行为的重要程序功能，这一功能的实现主要依赖嫌疑形成过程及嫌疑程度层级的划分。但是，随着嫌疑判断所依赖的信息圈层不断外扩，以及辅助圈层和背景圈层信息权重的上升，上述界限划分逐渐模糊，这导致嫌疑的程序规制功能难以有效发挥。从整体看，这种功能弱化源于嫌疑程度与嫌疑依据之间的不匹配，即嫌疑判断所依赖的信息圈层已经发生变化，但用以合比例划定与特定强度犯罪追诉措施相匹配的相应嫌疑标准却未能同步调整。这种失衡具体体现在两个方面：

一方面，此前不被视为可疑的某些行为，在信息圈层外扩后可能转变为可疑行为。此时，

〔42〕 参见前引〔9〕，Berman文，第463页。

〔43〕 参见王燃：《大数据证明的机理及可靠性探究》，《法学家》2022年第3期，第57以下，第192页；魏斌：《智慧司法的法理反思与应对》，《政治与法律》2021年第8期，第111页以下；谢澍：《人工智能如何“无偏见”地助力刑事司法——由“证据指引”转向“证明辅助”》，《法律科学》2020年第5期，第109页以下。

〔44〕 See Bernard E. Harcourt, *Against Prediction : Profiling, Policing, and Punishing in an Actuarial Age*, The University of Chicago Press, 2006, pp. 145-171.

〔45〕 See Margaret Hu, *Big Data Blacklisting*, 67 Florida Law Review 1735, 1735 (2016).

〔46〕 See Margaret Hu, *Algorithmic Jim Crow*, 86 Fordham Law Review 633, 633 (2017).

行为自身的性质、状态、模式和情境等并未发生变化，变化的是评判所依据的外部参照系。由于用于形成犯罪嫌疑的“异常要素”的范围扩大，那些原先不会列入可疑范围进而不会进入国家机关视野的人员，可能因此被纳入种种“灰名单”。并且，从前述提及的具体应用看，这类名单的构成伴有群体化的趋势。在这二者的共同作用下，国家机关在具体案件追诉过程中更易于针对特定个人形成嫌疑判断。

另一方面，嫌疑程度标准在表面上的稳定性可能会掩盖其背后特定国家机关行为强制性方面的变化，从而事实上打破刑事诉讼中原有的国家行为层级划分。例如，嫌疑信息圈层的扩张在很大程度上依赖于网络服务提供者等第三方主体的数据与技术协助，但此类协助行为的法律定性并不统一，其可能被视为行政法上的一般平台义务，或者属于刑事追诉正式启动前的公民报案、举报义务，又或者属于案件立案后配合公安司法人员侦查取证的义务。不同定性对应不同的法律责任和程序要求，同时匹配的国家机关措施强度亦存在差异。〔47〕在嫌疑信息基础日益依赖第三方数据与技术的情况下，网络服务提供者的数据与技术协助尽管可能会用于支撑后续带有较强强制性的刑事诉讼措施，但在其实施过程中也可能将其定性为协助行政执法或立案前调查核实，从而规避刑事诉讼程序针对强制性措施所设置的限制性条件。归根结底，这反映出数字化条件下嫌疑判断标准变得更加模糊：在运用数字技术进行犯罪追诉时，何种程度的信息异常可视为“存在犯罪嫌疑”缺乏明确界定，原有按照强制性措施不同而设定的嫌疑标准层级因此变得并非那么层次分明。

从我国当前刑事司法实践看，嫌疑稀释所造成的嫌疑程度层级虚化的影响并不明显，但这不是因为我国刑事司法对人工智能、大数据等数字技术的应用不充分，而是因为刑事诉讼法尽管规定了嫌疑概念，但缺乏对嫌疑程度层级划分的细化规定，也缺乏对不同强制性措施所需嫌疑信息基础的实证分析。在传统规则相对模糊的情况下，数字技术介入嫌疑判断不可避免地会进一步弱化嫌疑判断在规制国家机关行为方面的程序性功能。

（三）干扰执法效能的判断

数字技术介入嫌疑判断所引发的嫌疑稀释现象，可能会干扰执法效能的判断。这一效果主要源于数字技术应用下执法措施在“干扰率”和“命中率”两个维度上的变化。干扰率评价的是尚未被确定有罪的相对人遭受国家机关强制性措施的几率，命中率则关注相关强制性措施成功导向罪证进而推动案件侦破的几率。〔48〕尽管执法措施的命中率往往是评价执法质量和效能的重点关注指标，但从保障公民合法权益和生活安宁的角度看，干扰率同样具有重要意义。

基于数字技术应用而形成的嫌疑稀释，可能会同时影响执法措施的干扰率和命中率。就干扰率而言，数字技术能够通过大规模数据分析和自动化流程降低执法成本，这种低成本高效率的特性可能导致执法部门在目标选择上更加倾向于大规模覆盖而非精准定位，一方面可能导致更多尚无犯罪嫌疑的无辜人员成为犯罪预防与打击的目标，另一方面则可能不当降低执法机关对某些群体的关注和相应的资源分配。此外，这种规模化执法依赖于广泛收集和分析个人数据，例如通信记录、地理位置和社交媒体行为等，其同样可能对个人隐私或个人信息等相关权益构成普遍意义上的干预。

〔47〕 参见裴炜：《论刑事诉讼中网络信息业者的数据提供义务》，《上海政法学院学报（法治论丛）》2022 年第 6 期，第 60 页以下。

〔48〕 参见前引〔25〕，Bambauer 文，第 461 页。

就命中率而言，判断带有强制性的国家机关执法行为是否成功命中的主要方式是审查定罪率。因此，即使执法人员在采取诸如搜查、扣押等强制性措施时发现罪证的比例相同，如果某些群体后续的定罪率较高，则统计数据仍然会显示针对这些群体的执法措施的命中率高于其他群体。换言之，由于这些群体以更高比例被定罪，针对这些群体的执法措施会在外观上表现为更加有效和准确。

与执法措施在形式上的命中率提高形成反差的是，实质上的命中率则可能降低。从现有研究看，这种反差集中体现在以下方面：首先，算法决策高度依赖历史数据，这些数据通常包含偏见或“噪音”，导致误报率上升，执法资源被过度耗费于无辜目标，从而削弱搜查的精准性和效能。〔49〕其次，许多数字技术更关注数据覆盖的广度而非精准性，目标泛化使得真正的犯罪行为在庞杂的数据流中被掩盖。〔50〕再次，数字技术推动了执法行为的规模化和自动化，其伴随着低效执法的扩张，进一步稀释了整体命中率。〔51〕最后，数字技术的普及在一定程度上削弱了人类执法者的情境化判断能力，过度依赖技术会导致现场分析不足，增加错失关键线索的风险。〔52〕

（四）嫌疑决策的辩驳难度加大

犯罪嫌疑的判断不仅仅停留于执法人员的认知层面，还会进一步与后续具体执法措施相对应，进而与纳入嫌疑认知的相对人的权益发生关联。基于此，刑事诉讼法设置了一系列程序规则以确保嫌疑判断是合理、正当且公正的。当嫌疑的信息基础被稀释时，不可避免会影响相对人的权益保障。在程序规则未发生相应变化的情况下，这种稀释可能在三个层面提升相对人挑战执法者判断和后续决策的难度：一是针对过往经历的辩解；二是针对群体特征的辩解；三是针对正常行为的辩解。

首先，嫌疑的稀释使得相对人需要对其过往经历进行辩驳。嫌疑信息基础的稀释，使得执法机构可以轻松获取并重新审视相对人过去的行为数据，这些数据包括通信记录、社交媒体内容、位置轨迹、甚至财务和医疗记录等。在数字技术的支持下，即使这些行为在发生时是合法的，执法人员仍然能够利用算法模型将这些历史数据拼接成“犯罪模式”。这种重新诠释的过程不仅放大了无关行为的“可疑性”，还可能掩盖真正的犯罪线索。〔53〕相对人在这种情况下不得不为其历史行为的背景和动机进行辩解，而数据的模糊性和算法决策的复杂性使这种辩解变得异常困难。

其次，嫌疑的稀释使得相对人需要对其个人所属群体特征进行辩驳。如前所述，数字技术在嫌疑判断中的广泛应用经常依赖基于统计学模型的风险评估，这些模型可能引入对特定群体的系统性偏见。即使某些群体中个体的实际行为与犯罪无关，算法仍然可能将该群体定义为高风险目标。这种标签化会使得相对人不仅要证明自身行为的正当性，还要反驳基于群体特征的风险评估。更为复杂的是，算法的黑箱属性使得群体特征的使用往往隐藏在复杂的技术结构中，从而难以被披露或者被有效质疑。

〔49〕 See Rebecca Wexler, *Privacy as Privilege: The Stored Communications Act and Internet Evidence*, 134 Harvard Law Review 2721, 2723-2725 (2021).

〔50〕 See Hannah Bloch-Wehba, *Visible Policing: Technology, Transparency, and Democratic Control*, 109 California Law Review 917, 931-934 (2021).

〔51〕 See Anna Lvovsky, *Rethinking Police Expertise*, 131 Yale Law Journal 475, 524-527 (2021).

〔52〕 See Andrew Guthrie Ferguson, *Big Data Prosecution & Brady*, 67 UCLA Law Review 180, 180 (2020).

〔53〕 See Aziz Z. Huq, *The Private Suppression of Constitutional Rights*, 101 Texas Law Review 1259, 1321-1324 (2023).

最后，嫌疑的稀释进一步要求相对人对某些正常行为进行辩驳。算法模型倾向于根据统计关联而非实际情境来识别风险，这使得某些日常行为可能被错误归类为“犯罪信号”，迫使相对人不得不解释该行为的合法性和合理性。同时，正常行为的嫌疑标签通常源于算法对数据的统计关联和模式识别，进而将特定行为与犯罪可能性联系在一起。然而，这种基于大数据的关联并未考虑行为的实际背景和合法性，相对人必须结合众多案外信息解释行为发生的背景、时间、地点和动机等，而这些信息往往难以直观呈现，由此进一步加大了辩解的难度。

五、数字时代犯罪嫌疑的制度回应

面对嫌疑稀释所形成的挑战，刑事诉讼制度的回应，一方面要考量自身的独特需求，对相关技术应用予以必要且合理的规制，从而确保刑事诉讼基本价值的实现；另一方面也要适应数字时代犯罪治理的整体生态，进行必要的具体制度调整。这一调整首先要明确其前提假设，以此划定后续制度回应的外部框架；在此基础上，从嫌疑的信息圈层结构出发，在“嫌疑程度”之外引入“嫌疑信息密度”的判断维度，以发挥嫌疑概念的程序规制功能。

（一）刑事诉讼应用数字技术的独特需求

与商业领域相比，数字技术在刑事司法领域的应用需要适应这一场景的独特需求，这些需求源于刑事司法的高风险性质及其保护人权、维护社会公平正义的核心价值。这不仅要求新兴数字技术系统应具备更高的准确性和可靠性，还要求其在设计和应用上应充分考虑隐私等公民基本权益保护、偏见规避、透明性和问责机制等关键要素。具体而言，刑事司法场景在数字技术应用方面的独特性主要表现在以下方面。

第一是更高水平的公民权益保障。这一需求源于刑事司法的强权益干预属性。相较于商业领域，刑事诉讼中的数字技术应用涉及诸多敏感场景，例如犯罪嫌疑人监控、犯罪风险预测等，这些场景都可能深刻影响个体的人身自由、财产权、隐私权等基本权利。在数字时代，这种高水平的权益保障需求集中反映在隐私及个人信息保护、非歧视性原则以及程序正义等方面。一旦数字技术的设计或应用存在问题，不仅可能直接侵害个体权利，还可能削弱公众对司法系统的信任。

第二是更低的容错率。相较其他场景中的数字技术应用，刑事司法决策对个人权利和社会公正会产生深刻且重大的影响，例如错误的犯罪预测可能导致无辜者遭受不公正的处置和权益减损，真正的罪犯也可能因此而逃脱法律制裁。低容错率意味着数字技术的应用必须具备更高的准确性和稳定性，例如相关技术需要进行系统和全面的测试和验证，需要具备实时监测和纠错能力等。

第三是更高的透明性和可解释性需求。这一方面源于刑事司法决策对具体相对人权益的强干预性，另一方面源自实质程序正义对司法公开透明的内在要求。这就要求数字技术在应用于刑事司法这一特殊场景时，其所依赖的算法逻辑必须清晰明确，相关工具要经过独立的司法伦理评估和法律审查，并在应用构成中提供必要的决策依据和相应的解释说明，以确保其在设计和运行中符合司法公平正义的核心原则。

第四是更高的数据质量和合法性要求。刑事司法决策必须建立在合法性的基础上，基于合法性对证据资格的限制是其典型例证。在这一场景中，数据不仅是算法运行的基础，更直接决定了案件处理的公正性和合法性。例如，低质量或偏差性数据可能导致算法输出错误，进而影

响司法决策的准确性。这意味着数字技术的应用要确保其基础数据来源的合法性，同时基于数字技术在司法场景中应用所需要满足的质量需求设置明确标准，这有赖于严格的数据清洗、验证、安全保障和管理。

第五是更严格的问责机制。刑事司法中的数字技术应用会直接影响社会公平与正义，例如某些算法决策会导致边缘群体面临更大的不公风险，这就要求在数字技术应用于这一场景时，技术问责机制要覆盖包括开发、部署和使用等环节的整个技术生命周期：建立独立的监督与审查机制，以确保技术开发和使用符合法律和伦理标准；定期评估技术对特定群体或社会整体的影响，以识别潜在问题并及时调整政策；设置明确的责任追溯和补救措施，以快速定位责任方并采取有效的纠正措施。

（二）刑事诉讼回应嫌疑稀释的逻辑起点

上述刑事诉讼的内在需求构成后续制度设计的基本框架，在此基础上，仍有必要就刑事诉讼回应嫌疑判断数字化，明确三个基础性假设。

第一个假设是，人类决策亦有局限性。对数字技术的诸多批判，实质上是对人类判断固有缺陷的延伸。现有刑事诉讼中对犯罪嫌疑的判断，蕴含着人类自身潜在的、甚至是显性的偏见与歧视，〔54〕而这些判断遵循的是模糊不清的标准。这些标准之所以长期以模糊的状态存在，正是因为人类的主观判断难以外化和精确呈现，从而难以被客观观察和评价。

这一状况事实上为执法人员恣意甚至矛盾的决策提供了空间。以1989年“美国诉索科洛夫案”为例，〔55〕持反对意见的美国最高法院大法官瑟古德·马歇尔列举了一系列过往案件中执法人员认为的“可疑行为”，包括“嫌疑人第一个下飞机”“嫌疑人最后一个下飞机”“嫌疑人在乘客中间下飞机”“嫌疑人买单程票”“嫌疑人买往返票”“嫌疑人买直飞票”“嫌疑人买换乘票”“嫌疑人未携带行李”“嫌疑人携带运动包”“嫌疑人携带新的行李箱”“嫌疑人独自旅行”“嫌疑人相伴旅行”“嫌疑人表现紧张”“嫌疑人表现得过于平静”等等。这些相互矛盾的“可疑行为”被马歇尔大法官描述为“像变色龙一样”的嫌疑判断方式。

尽管对于经验丰富、掌握信息更全面、尽职尽责的专业执法人员而言，对犯罪嫌疑的判断有其专业性和准确性，但这种判断具有高度的个人化特征和对具体情境的依赖性。〔56〕一方面，这种判断难以外化为可以外部审查的过程，由此降低了决策过程的透明度，也使得相对人难以实质性地质疑相关决策。另一方面，这种判断方式难以向其他执法人员、后续的司法人员传递，从而形成个案、地区、机构等之间执法和司法的不一致。从这个角度看，对于机器判断的一些质疑要找到恰当的参照系，在此基础上找到机器判断与人类决策的恰当融合点，避免主观上予以直接批判。

第二个假设是，工业时代确立的嫌疑判断标准及判断方式并不天然适用于数字时代，也未必是最优制度设计。工业时代的刑事诉讼模式主要建立在有限信息环境中，其判断犯罪嫌疑的

〔54〕 See Wayne A. Logan, *Policing Emotions: What Social Psychology Can Teach Fourth Amendment Doctrine*, 72 Buffalo Law Review 685, 685 (2024).

〔55〕 United States v. Sokolow, 490 U. S. 1, 13-14 (1989) (Marshall, J., dissenting)。该案涉及被告人索科洛夫在夏威夷檀香山机场被缉毒执法人员拦截，执法人员认为索科洛夫符合“缉毒特征”的若干行为模式，例如使用现金购买机票、使用不同姓名、旅行时间短、未携带任何行李等。执法人员基于这些“可疑特征”对索科洛夫实施了搜查，发现了大量非法毒品。该案的核心争议点在于，执法人员列举的行为特征是否足以构成合理怀疑。美国最高法院以6∶3的裁决支持政府立场，认为执法人员基于对一系列可疑行为的综合判断有权临时拘留索科洛夫。

〔56〕 参见前引〔51〕，Lvovsky文，第475页。

方式更多依赖实物证据、目击证人的证词和直接的人际互动。这种基于个案逐步推进的模式，在数据驱动的数字时代显得效率低下，且难以应对复杂犯罪行为。同时，工业时代的刑事诉讼强调程序化和标准化，以确保执法和司法的公正性。然而，数字时代的犯罪行为具有高度动态性、全球性、突发性、扩散性等特征，风险社会治理的需求进一步提升，由此强化了运用数字技术应对数字时代犯罪活动的现实需求。此外，现行刑事诉讼法基于工业时代的规则设计，缺乏处理大规模数据和算法判断的能力。如前所述，嫌疑判断标准的模糊性，很大程度上正是对人类理性模糊判断的适应性产物。

从这个角度看，数字技术介入嫌疑判断所引发的嫌疑基础信息圈层在质和量上的外扩，并非问题本身。需要关注的是该现象所引发的对刑事诉讼制度的冲击，其既牵涉嫌疑程度标准的设置问题，又涉及更为隐性的嫌疑判断的信息基础问题。对此，刑事诉讼制度中嫌疑的评价标准和方式也要作出相应调整：一方面朝着更加清晰、准确、透明的方向发展，以适应数字技术；另一方面，除了考量嫌疑程度，还要增加嫌疑信息密度的评价维度。〔57〕

第三个假设是，嫌疑信息密度的变化并非均质化的过程。从前文分析可以看出，在数字技术与犯罪追诉融合的不同类型场景中，嫌疑信息的聚焦程度、关联强度与验证能力存在显著差异。在部分场景中，信息高度集中于案件事实本身，辅助性和背景性数据占比较低，因此嫌疑构造较为清晰、稳定，制度风险相对有限。而在另一些场景中，嫌疑判断依赖的是跨域整合、模糊推演或行为预测，其信息基础呈现去中心化和多维度稀释的状态。

信息密度的下降不仅表现为核心信息比重的稀释，也体现在因果路径的断裂和行为关联的弱化。这一密度下降的表现，并不意味着嫌疑不成立，而是其构成基础的验证结构变得松散和复杂，这会直接影响判断的可靠性，此时刑事诉讼决策的正当性开始面临实质挑战。这意味着在分析和应对信息圈层的外扩趋势及其引发的具体问题时，最需要关注的不是信息密度下降本身，而是要明确不同场景下嫌疑判断的信息构造特点，并结合相应场景进行制度设计。

（三）基于嫌疑程度与信息密度的嫌疑判断结构

从嫌疑程度的角度看，应对数字技术冲击下的嫌疑稀释，刑事诉讼制度要重新审视犯罪嫌疑标准的划分。如前所述，我国刑事诉讼法并未明确犯罪嫌疑的具体衡量要素和标准，因而在不同轻重罪名、不同紧急情况、不同权益干预程度之间，现有规则并未在其依赖的嫌疑基础上有所界分。这就在事实上消解了犯罪嫌疑的程序规制功能，亦难以对相关犯罪追诉措施的合理性进行外部审查。在数字时代，若仍沿用概括且模糊的嫌疑标准，并且不区分嫌疑所依据的信息层级，就不可避免地会为执法恣意留下空间。

对此，有必要在刑事诉讼中建立起分层的犯罪嫌疑标准谱系，这是后续审查和判断犯罪追诉措施合理性的基础。之所以称为“谱系”，强调的是依据不同要素设置不同程度的嫌疑水平。从维系刑事诉讼程序正当性的角度出发，该谱系关注的核心问题是，如何避免使较低信息密度的嫌疑判断获得与之不合比例的程序启动效力。

具体而言，这一谱系应至少包含以下考量因素：第一，确立犯罪嫌疑人身份应具备最低程度的嫌疑，其标准应不低于刑事立案所需要的依据，这是针对特定相对人采取追诉措施的初始条件。第二，嫌疑的程度应与所采取的具体追诉措施的侵扰性相匹配。原则上，措施对相对人基本权利的侵扰程度越高，所要求的嫌疑信息就应当越贴近核心圈层信息。这并不是排除辅助

〔57〕 参见前引〔50〕，Bloch-Wehba 文，第 917 页。

圈层和背景圈层的信息，而是强调核心圈层信息在决策中的关键地位。第三，嫌疑的判断标准要结合特定情境，特别是要考量紧迫性因素。在必须于短时间内快速反应的情形下，允许嫌疑判断与通常标准存在一定偏离。第四，在设定和评估嫌疑标准时应引入干扰率和命中率这两个指标，尤其要将后者作为特定技术应用于嫌疑分析时的动态评估要素。〔58〕

细化嫌疑程度谱系只是建立数字嫌疑制度的形式条件，更重要的是在实质层面关注嫌疑的信息密度。如前所述，在相同嫌疑程度下，随着信息来源由核心圈层向辅助圈层再到背景圈层逐级扩张，嫌疑信息与具体案件事实的关联程度逐级降低，也即确定性不断减弱、预测性不断提升。换言之，嫌疑的信息依据无论在质还是量的层面越偏离核心圈层信息，就越具有预测性质、越缺乏确定性，这可以被视为嫌疑信息密度降低的具体体现。

为应对嫌疑稀释所形成的挑战，刑事诉讼需要经历一个逆向过滤的过程，即从群体分析回归个体分析、从数字人回归自然人、从情报导向回归事实导向、从机器理性回归人类理性。这一过程并不是要求排斥数字技术的应用，而是要将嫌疑信息圈层与特定的执法措施之间形成以下五个维度的匹配关系。

第一是国家机关决策的终局性。越靠近终局性决策，原则上该决策所依赖的嫌疑信息密度应当更高，也即越贴近核心案件事实。相反，越是处于刑事诉讼早期阶段，越是可以适当容忍嫌疑的基础信息圈层外扩。

第二是具体措施的强制性。原则上，对相对人采取的措施的强制性越高，所依赖的嫌疑信息密度应当越高。特别是像技术侦查这类具有高度侵入性的措施，其应当主要依赖核心圈层信息作为嫌疑判断的关键性基础。

第三是区分建立嫌疑和洗脱嫌疑。建立嫌疑时，越严重的执法行为对应信息密度越高的嫌疑；洗脱嫌疑时，越严重的处置结果则要对应越宽泛的信息圈层。同时，不在核心信息圈层这一情况，应足以阻却严重措施的适用。此外，基于数据分析所形成的概率尽管不宜单独作为嫌疑判断的基础，但其可以用来推翻嫌疑，即对于嫌疑的成立如果采用数字技术进行分析，应当有一个符合技术标准的概率值。

第四是具体案件的特性。某些犯罪活动的模式化程度要高于其他犯罪，例如贩卖毒品相较于激情杀人。同时，某些犯罪的隐匿程度也要高于其他犯罪，例如性侵幼女相较于醉酒驾驶。此时，对于更为随机的或隐匿性更强的犯罪活动，拓展嫌疑的信息圈层就有一定的必要性。

第五是要适当考量所涉犯罪类型，针对更严重、危害性更大的犯罪，有必要在嫌疑信息密度上予以一定程度的宽松要求。与公民权益保障的维度不同，这一维度更多是从嫌疑作为刑事诉讼措施的调节与规制工具出发，考察特定措施的成本收益关系，这是执法效能中干扰率和命中率评价的必要考量因素。

结 论

数字时代犯罪嫌疑的形成机制和司法应用面临着转型的任务。数字技术的应用不仅扩展了执法机关获取信息的能力，还重塑了嫌疑判断的信息结构和评价模式，使得犯罪嫌疑从过去依赖人类观察与推断的核心圈层信息逐步延展至更宽泛的辅助圈层信息和背景圈层信息，并且后

〔58〕 参见前引〔25〕，Bambauer文，第461页以下。

二者在机器决策引入司法决策过程中的权重也在不断上升。这种变化虽然带来了侦查效能的显著提升，但也稀释了嫌疑的信息密度，对刑事诉讼中的正当性、比例性以及公民权利保护带来了严峻挑战。

为应对上述挑战，刑事诉讼制度需要引入嫌疑信息密度的评估机制，将嫌疑的判断从单纯关注“程度”扩展到兼顾“密度”。对此，应根据案件处理的阶段、措施的强制性、嫌疑信息的来源等要素，构建嫌疑信息密度逐级提升的框架，以确保在终局性决策中嫌疑判断的依据更贴近案件核心事实，避免外围信息对执法行为的过度干扰。此外，数字技术在嫌疑形成中的应用要强化透明性，确保算法和数据处理过程的公开化和可审查性，降低执法偏差和决策失误的风险。

总体而言，在社会整体数字化的过程中，刑事诉讼制度要在遵循自身特性和规律的基础上，对数字技术的系统性融入予以回应和规制，从而实现数字时代犯罪治理中公民权益保障与治理效能提升之间的平衡。

Abstract: The ongoing advancement of digital technologies is fundamentally reshaping the generation and assessment logic of criminal suspicion. Traditionally, suspicion has been assessed through law enforcement officers' direct observation of specific conduct, coupled with inferential reasoning grounded in their professional experience. However, the widespread adoption of big data analytics and artificial intelligence has restructured the informational basis of suspicion, extending it beyond concrete case-specific facts to more widespread information of outside. This shift manifests in the transformation and merger of suspicion from an individual-based to a group-based orientation, from natural persons to digital identities, from concrete factual indicators to predictive intelligence, and from human to machine-mediated rationality. While such developments promise enhanced efficiency of investigation and the ability of crime discovery, they also give rise to what may be termed the dilution of suspicion. This dilution weakens the role of suspicion as a core regulatory threshold for initiating coercive state interventions, thereby generating systemic tensions with procedural safeguards and fundamental rights protections. To address these challenges, it is necessary to recalibrate existing procedural frameworks by incorporating information density as a complementary evaluative dimension of suspicion. A layered filtering mechanism should be established to ensure proportionality and coherence between the assessment of suspicion and the procedural actions and decisions. In doing so, the criminal justice system can promote the responsible integration of digital technologies into suspicion assessment and criminal prosecution, while preserving procedural legitimacy and institutional integrity amidst ongoing digital transformation.

Key Words: digitalization of criminal justice, suspicion, dilution of suspicion, information density, digital due process