面向多模态灾害数据共享隐私合规的道义知识图谱

Kelvin Uzoma Echenim 马里兰大学巴尔的摩县分校 马里兰州，美国
kelvine1@umbc.edu

Karuna Pande Joshi 马里兰大学巴尔的摩县分校 马里兰州，美国
karuna.joshi@umbc.edu

arXiv:2601.03587v1 [cs.CR] 7 Jan 2026

摘要

灾害响应需要在多项隐私要求交织的情况下共享异构制品，从表格化援助记录到无人机影像皆是如此。运营系统通常将合规简化为二元访问控制，这在时间紧迫的工作流程中显得脆弱。我们提出一种新颖的基于义务知识图谱的框架，将灾害管理知识图谱（DKG）与源自 IoT-Reg 以及美国联邦紧急事务管理局/美国国土安全部隐私驱动因素的政策知识图谱（PKG）相结合。我们的发布决策函数支持三种结果：允许、阻止和允许并转换。对于后一种结果，框架会将义务与转换相绑定，并通过来源关联的派生数据制品验证转换后合规性；被阻止的请求则会记录为语义隐私事件。对包含 510 万个三元组和 31.6 万张图像的 DKG 进行评估后发现，该框架实现了精确匹配的决策正确性、每项决策的延迟低于一秒，并且在单图谱和联邦式工作负载中均具备交互式查询性能。

关键词

隐私合规、知识图谱、道义逻辑、灾害管理、物联网、语义网

1 引言

在大规模灾害发生后的最初阶段，及时掌握态势是有效响应的关键。应急管理机构日益依赖多模态数据，包括无人机系统（UAS）影像和遥感数据流，以及幸存者名册等表格数据，以评估损害、识别灾害隐患、分配资源并协调搜救行动 [20]。这些纷繁的数据有助于构建共同作战态势图，这对跨机构协调至关重要。然而，在居民区大规模收集视觉数据不可避免地会采集到个人身份信息（PII），例如人脸和车牌，从而引发重大的隐私顾虑 [22, 26]。

1.1 考虑政策的灾害数据共享

联邦机构必须遵守严格的监管规定，以保护这些数据。例如，美国联邦紧急事务管理局（FEMA）在其针对无人航空系统（UAS）的隐私影响评估（PIA）中明确指出，尽管其并非以个人为目标，但任何收集到的附带个人身份信息（PII）都必须在存储或传播前进行混淆处理或删除 [27]。同样，美国联邦紧急事务管理局的记录系统通知（记录系统通知 DHS/FEMA-008）要求对跨机构个人身份信息传输实施严格的访问控制和审计日志记录 [5]。灾害响应的紧迫性往往与这些合规审查的程序僵化相冲突 [22]。应急管理人员面临一个关键的两难抉择：立即发布数据以协助响应，但承担隐私违规的风险；或延迟发布，以便进行人工审查并承担行动效率低下的风险。为解决这一矛盾，我们需要能够执行策略感知型数据共享的自动化系统——通过动态分类、评估、转换和发布数据，在确保合规的同时避免造成不可接受的延迟。

1.2 多模态隐私合规的挑战

在灾害响应中实现隐私合规自动化颇具挑战，因为灾害数据种类繁多，且依赖具体情境。与结构化数据库记录不同，灾害工件通常包含非结构化媒体（如图像和视频），以及记录地理空间和时间信息的复杂元数据。

1.2.1 异构数据模态。 单个灾害事件会关联文本声明（例如事件类型、位置和日期）、地理空间特征（例如影响区域多边形）、影像和传感器数据。每种模态都带来独特的隐私风险；例如，航空影像可能包含非结构化且难以检测的附带采集的个人身份信息 [29]。

1.2.2 情境完整性与受众依赖型政策。 数据敏感性往往取决于接收方。根据特定的信息共享访问协议（ISAAs），向可信的执法合作伙伴共享原始影像或许是允许的，而向公众或志愿者组织共享同一影像则需要进行严格的匿名化 [25]。政策必须考虑接收方，并针对具体活动制定。

1.2.3 动态合规状态。 随着转换的应用，制品会在不同合规状态之间转换。无人机系统图像最初可能不合规，但应用特定转换（例如移除 EXIF 元数据）后即可共享。系统必须追踪这些派生制品的溯源信息，以确保在发布前履行义务。

1.2.4 监管交互。合规并非由单一、静态的规则所决定，而是受一个复杂的生态系统所支配，其中包含相互重叠的框架，涵盖联邦法规、技术标准和机构特定指令。对于无人航空系统（UAS）等联网传感器，美国国家标准与技术研究院跨机构报告（NI-STIR） 8228 [2]等指导方针尤其相关；该报告将这些平台归类为物联网边缘设备，并要求其遵循特定的网络安全与隐私风险管理规程。

1.3 我们的贡献

先前研究已证明，知识图谱（KG）和语义网技术有助于自动实现法规

合规性 [3, 15]。IoT-Reg框架 [8] 运用这些技术为可穿戴设备建立隐私规则模型 [9]。然而，现有语义框架主要支持二元访问控制，根据静态属性授予或拒绝访问。在灾害管理场景中，这种二元方式并不适用，因为仅因轻微违反隐私规定而限制数据访问，可能会妨碍及时响应。在本研究中，我们将道义逻辑（用于建模义务、许可和禁止）直接整合到灾害管理系统的操作流程中，而故障关闭安全机制至关重要。

为弥补这一空白，我们提出了一个策略感知决策框架，将领域专用的灾害管理知识图谱（DKG）与 IoT-Reg 的监管智能相结合。我们的具体贡献如下：

- 我们设计了一个综合性 DKG，整合了美国联邦紧急事务管理局的真实灾害声明、地理空间特征，以及美国国家海洋和大气管理局（National Oceanic and Atmospheric Administration）的应急响应影像。
- 我们扩展了 IoT-Reg 本体，将美国联邦紧急事务管理局/美国国土安全部的灾害管理概念映射到隐私规则。我们将无人航空系统和遥感平台视为联网的物联网设备，并依据 NISTIR 8228 [2] 以及《通用数据保护条例》和美国联邦紧急事务管理局特定要求等指导方针，推导出隐私风险缓解规则。
- 我们基于道义逻辑制定了发布决策函数，不仅支持“允许”或“阻止”决策，还支持有条件的“允许并变换”判定结果。该引擎弥合了策略义务与满足这些义务所需技术措施之间的差距。
- 我们实现了一个端到端系统，可自动执行所需的转换并记录每项决策。我们引入了一种语义事件检测机制，将被阻止的共享记录为知识图谱中的隐私事件，从而支持自动审计和报告，并符合美国国土安全部隐私事件处理指南 [28]。

本文其余部分安排如下：第 2 节介绍灾害管理领域、IoT-Reg框架、相关监管驱动因素，以及威胁模型和系统要求。第 3 节详细介绍灾害与策略知识图谱的模式设计。第 4 节对策略感知决策框架及其安全属性进行形式化阐述；第 5 节介绍操作性执行层和转换流程。第 6 节介绍用于合规审计的分析监控层。第 7 节从知识图谱规模和结构有效性、策略决策正确性、转换引起的状态变化以及查询性能等方面评估该框架。第 8 节讨论其可推广性与局限性，第 9 节回顾相关工作，第 10 节总结全文。

2 背景与问题设定

2.1 道义逻辑与 IoT-Reg 框架

规范互联系统的隐私法规本质上具有规范性：它们规定数据控制者必须、可以以及不得如何处理个人数据。道义逻辑提供了一套用于表达此类规范的词汇，并已被广泛用于以机器可解释的方式对法律和政策约束进行建模 [15]。

从宏观层面来看，道义逻辑为行动引入了三个主要算子：

- 义务：某项行动应当执行（例如，记录个人身份信息（PII）的披露）。
- 许可：在特定条件下允许执行某项行动。
- 禁止：某项行动不得执行，通常表示为有义务不执行该行动。

这些算子本身并未规定具体的执行策略；它们提供了一个语义层，在此基础上可以定义具体的决策程序和安全条件。

面向物联网隐私的 *IoT-Reg* 义务本体。 IoT-Reg 是一种 OWL（Web 本体语言）/资源描述框架（RDF）本体，使用这一义务词汇表，以知识图谱的形式对物联网数据隐私法规进行建模 [8]。它扩展了 W3C 的标准词汇表，例如溯源本体（PROV-O）[1] 和传感器、观测、样本与执行器（SOSA）[2] 本体，并加入了针对隐私和法规合规而定制的概念。从概念上讲，它提供了：

- 义务陈述类：iot-reg:Permission 表示在特定条件下允许执行的操作，iot-reg:Obligation 表示必须执行的操作（例如加密和日志记录），而 iot-reg:Prohibition 表示不允许执行的操作；这些类被建模为通用义务陈述类的子类。
- 面向生命周期的活动：隐私和安全要求按照 iot-reg:DataLifecycle 的子类进行分层，包括数据收集、数据处理、数据共享、数据保留和数据删除。这一设计将 NISTIR 8228 强调的、作为关键风险向量的具体数据处理活动付诸实施，同时与《通用数据保护条例》等法规中的生命周期模型保持一致。
- 数据与接收方语境：义务个体与数据类型（iot-reg:PersonalData、iot-reg:Image、iot-reg:FeatureOfInterest）以及建模为 iot-reg:Recipient 的受众（如内部操作员和合作机构）相关联。
- 法规溯源：IoT-Reg 使用 PROV-O 将义务陈述与其来源条款相关联，把具体的许可、禁止和义务关联到《通用数据保护条例》和 NISTIR 8228 等法规中的条款。这支持对合规决策进行解释和审计。

IoT-Reg 已用于编码 NISTIR 8228 中针对可穿戴设备的风险缓解目标和风险缓解领域，并评估供应商隐私政策与 NIST 对物联网设备的预期是否一致 [7]。此外，它还纳入了《通用数据保护条例》场景，并与大语言模型结合，用于回答面向物联网制造商的义务性（规范性）和非义务性（事实性）合规查询 [9]。在这些场景中，IoT-Reg 作为可复用的基础框架，用于表示物联网数据处理活动所涉及的许可、义务和禁止。

[1] http://www.w3.org/ns/prov# [2] https://www.w3.org/ns/sosa/

在本文中，IoT-Reg 为灾害数据提供政策基础框架。我们沿用其义务类别（许可、义务、禁止）、数据活动的生命周期视图，以及将数据和接收方视为一等实体的处理方式。在这一现有框架之上，我们引入灾害特定政策概念，并将其与 DKG 中的多模态制品相连接（第 3 节）；随后将系统的发布决策函数和安全属性作为独立贡献进行定义（第 4 节）。

2.2 监管驱动因素

我们的系统设计由一系列联邦指导方针驱动，这些方针规定了灾害数据必须如何处理。我们综合了三个主要监管框架，以推导出适用于政策知识图谱（PKG）的道义逻辑规则。

2.2.1 NISTIR 8228：物联网隐私基线。 NIST 跨机构报告 8228，《物联网网络安全与隐私风险管理注意事项》 [2], 阐述了联网感知设备面临的隐私挑战。我们将美国联邦紧急事务管理局的无人机系统机队视为物联网边缘设备：它们与物理世界交互、持续采集数据，且缺乏传统的同意机制。

NISTIR 8228 的风险缓解目标涉及个人身份信息的数据操作，包括收集、存储、处理和传输。具体而言，目标*3*：保护个人隐私 强调，必须缓解个人身份信息处理所引发、且设备和数据安全控制未能管理的隐私风险。在此基础上，我们采用 IoT-Reg 框架，将这些概念形式化为分层的数据生命周期模型（收集、处理、共享、保留和删除），并据此设计多模态知识图谱，使制品能够独立于采集设备追踪自身的溯源信息和生命周期状态。

2.2.2 FEMA SORN DHS/FEMA-008：结构化个人身份信息限制。《灾害恢复援助档案记录系统通知》(SORN)[5] 规范从灾民处收集的结构化个人身份信息（姓名、地址、财务数据）。该通知规定了作为有条件许可的常规用途：

- 常规用途 J（未满足需求）：允许与志愿组织共享信息，但仅限于满足特定的灾害相关需求。
- 常规用途 I（福利重复领取）：允许与其他机构共享信息以防止欺诈，但要求严格遵循数据最小化原则。

我们将这些建模为特定受众许可。例如，与合作机构共享信息须以加密和履行日志记录义务为条件。除非存在特定例外，否则默认禁止向公众共享信息。

2.2.3 FEMA UAS PIA-055：非结构化影像要求。针对无人机系统生成的影像的隐私影响评估 (PIA) [27] 探讨了空中监视带来的独特风险。评估指出，尽管 FEMA 不以个人为目标，无人机系统传感器仍不可避免地会采集附带的个人身份信息。

- 隐私影响评估规定，影像中发现的任何个人身份信息都必须在共享前进行混淆或删除。这是一项必须在任何公开发布前履行的强制性义务。
- 它禁止使用无人航空系统数据来识别个人，或监控个人或群体的移动。这构成一项全局性禁止，适用于任何涉及面部识别或追踪的处理活动，并优先于任何其他许可。

这些规则驱动我们的基于转换的执行机制。公开发布请求会触发所需的转换，以满足 PIA 的混淆要求。

2.3 威胁模型和系统要求

2.3.1 威胁模型。我们考虑这样一种多方参与的灾害响应环境：中央管理机构（例如美国联邦紧急事务管理局）管理 DKG，并在监管约束下向不同接收方分发制品。根据应用安全方法论，我们以对手的资源和意图为基础，列举威胁。 [6]。我们的威胁模型涵盖对手行为和运行故障。

可信计算基（*TCB*）。我们假定知识图谱基础设施和访问控制、本体与 PKG 定义、策略引擎逻辑以及可信转换服务的完整性。对合规性至关重要的断言，其写入权限严格由可信服务控制；不允许最终用户直接更新三元组存储。

对手模型。我们考虑：（i）诚实但好奇的授权合作伙伴，他们遵循协议，但试图从允许发布的信息中推断敏感信息；（ii）恶意内部人员（或遭入侵的账户），他们试图绕过合规控制以窃取个人身份信息。

威胁分类体系。 我们使用 LINDDUN [4]对隐私威胁进行分类，并使用 STRIDE [23]对完整性威胁进行分类。我们重点应对以下对手能力：

A1 超范围共享 （STRIDE：权限提升；LINDDUN：不合规）。获授权用户可能试图超出其许可范围共享数据，原因可能是恶意行为，也可能是对政策的误解（例如，发布未经匿名化处理的原始无人机影像）。A2 语义歧义利用 （LINDDUN：不知情／不合规）。对手可能利用自然语言政策中的歧义，为未经授权的访问寻找理由；例如，将合作机构宽泛地解释为包含未经授权的承包商。A3 绕过净化／义务（LINDDUN：可识别性／披露）。参与者可能试图在未执行所需转换的情况下发布制品，或者声称某个制品已匿名化（例如），但其中仍包含敏感视觉个人身份信息。A4 元数据伪造 （STRIDE：篡改）。对手可能试图向制品注入虚假元数据，以绕过自动化合规检查。A5 行为抵赖 （STRIDE：抵赖）。内部人员可能否认自己发起了不合规发布。若没有防篡改审计记录，问责便无从实现。

运行故障。 除了对抗性威胁外，系统还必须应对影响合规性的非恶意故障：

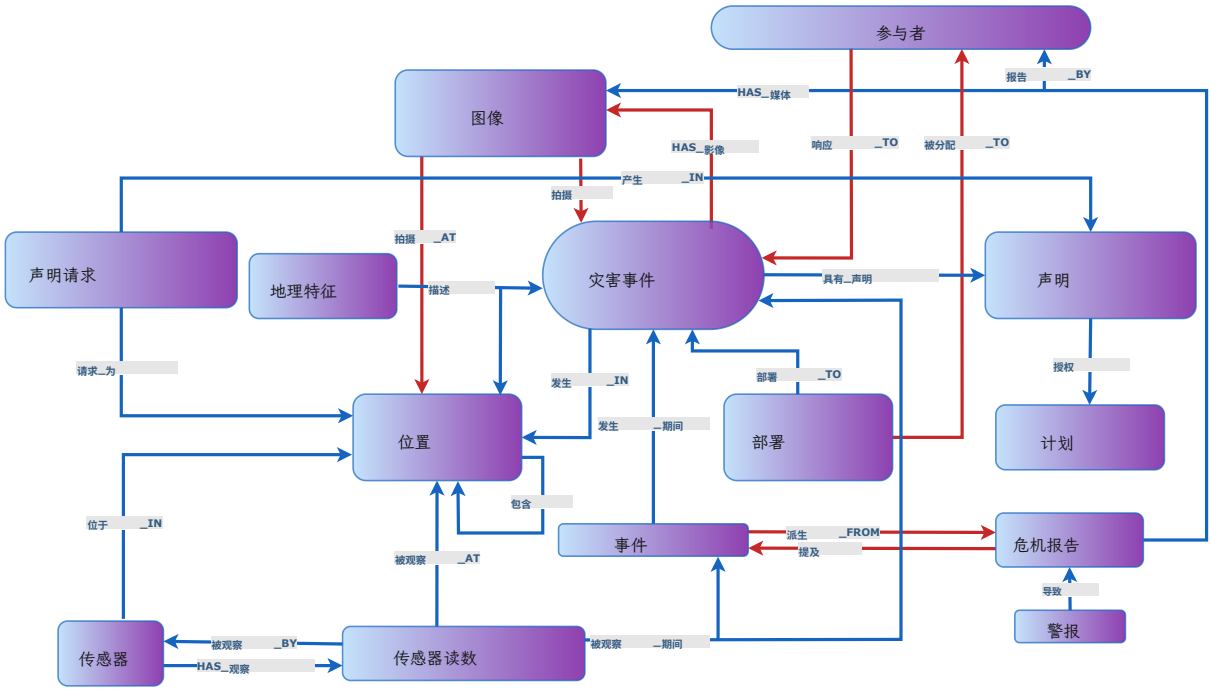


图 1：灾害管理本体

F1 策略漂移。随着法规和指导方针的变化，静态硬编码规则可能会过时，从而导致不合规共享。F2 静默转换失败。自动化转换可能会静默失败，导致生成的制品表面上符合合规要求，但仍包含个人身份信息。F3评估/查询故障。 如果不进行明确处理，查询中断或策略评估故障可能会导致故障开放行为。

我们排除网络层拒绝服务、对数据中心的物理入侵以及隐写术数据窃取。

2.3.2 系统要求。 为缓解这些威胁并与监管驱动因素（定义见第 2.2 节）保持一致，系统必须满足以下要求：

R1 禁止优先（防御 A1、A2）。明确的禁止必须优先于许可。如果某项禁止与请求匹配，无论是否存在其他许可，判定结果都必须为阻止。R2 故障关闭默认原则（防御 F3）。系统必须采用默认拒绝策略。如果策略查询失败、PKG 无法访问，或没有明确的许可与请求元组匹配，判定结果必须默认为阻止。R3 可验证义务履行（防御 A3、F2）。必须依据 DKG 中记录的制品状态验证义务，而不能依据用户声明。系统必须将义务映射为可验证的合规标志，并要求在发布前满足这些标志。

R4 溯源绑定与防篡改审计（防御 A4、A5）。派生制品必须通过 prov: [17] 关联至原始制品。合规声明只能由可信的转换流水线生成（不得由用户手动输入），且发布决策必须记录在防篡改审计日志中，以支持问责。

R5 语义事件检测（防御 A1、F1）。被阻止或异常的请求必须作为隐私事件记录在 DKG 中，以支持符合美国国土安全部指导方针 [28] 的审计和响应工作流。事件记录应对原因进行分类（例如，Prohibited_Share、No_Permission），以支持策略优化。

R6 受众绑定（防御 A2）。策略必须将每个请求绑定到经过身份验证的受众类别（例如，公开与合作伙伴），并执行依接收方而定的规则，以防止不同发布渠道之间发生语境坍塌。

3 知识图谱设计

我们通过两个相互作用的 RDF 图实现具备策略意识的灾害数据共享。灾害管理知识图谱（DKG）对多模态灾害数据进行建模，而策略知识图谱（PKG）则使用 IoT-Reg 和扩展命名空间，对美国联邦紧急事务管理局/美国国土安全部的隐私和数据共享规则进行编码。发布决策函数（第 4 节）会查询这两个图：DKG 展示制品的当前状态，PKG 则提供适用的道义逻辑。

3.1 灾害管理知识图谱模式

DKG 定义在 disaster_mgt（dm:）命名空间中，并以一个权威的、以文本为中心的层为基础，该层主要派生自美国联邦紧急事务管理局的灾害宣告数据集。此文本层作为骨干层，影像、地理空间特征及未来的模态通过标识符、位置和时间跨度以确定性方式关联到该层。主要的文本类包括 dm:DisasterEvent、dm:Declaration、dm:DeclarationRequest、dm:Program 和 dm:Location。

- dm:DisasterEvent表示主要灾情（例如，有名称的飓风、野火或洪水），其关键属性包括标识符（dm:disasterNumber）、灾害描述信息（dm:incidentType、dm:declarationTitle）和时间锚点（dm:incidentBeginDate、dm:incidentEndDate、dm:declarationDate）。每个事件通过dm:occured_in关联至少一个dm:Location；若已发布声明，则通过dm:has_declaration关联一个dm:Declaration。
- dm:Declaration记录政府的正式响应。dm:femaDeclarationString、dm:declaration Type、dm:declarationDate和dm:disasterCloseoutDatemodel等属性描述声明生命周期，而dm:authorizes将声明与dm:Program个体关联，这些个体代表个人援助（IA）、公共援助（PA）、灾害减缓（HM）及相关计划 [11]。
- dm:DeclarationRequest 表示可能导致声明、也可能不会导致声明的正式申请。诸如 dm:declarationRequestNumber、申请事件时间段、申请援助标记和 dm:requestStatus 等属性，使图谱即使在未发布联邦声明时，也能保留潜在未满足需求 [10]。
- dm:Program 对各种援助形式进行建模，以便查询某一事件或地点有哪些项目可用。
- dm:Location 对地理实体（州、县、部落地区）进行编码，并包含 dm:placeName、dm:stateName 和 dm:placeCode 等属性，同时通过层级结构参与 dm:contains 关系。

图 1 展示了我们的灾害管理本体。这些类别的数据来自美国联邦紧急事务管理局的四个开放数据集：灾害声明摘要、网络宣告区域、宣告否决记录和网络灾害摘要 [10–13]。我们采用一种映射策略，仅在某列有助于确定身份、位置、时间或援助类型时才将其纳入。

该模式还引入了 dm:CrisisReport（其子类包括 dm:FieldReport 和 dm:SocialMediaPost）、dm:Alert、dm:Actor、dm:Sensor 和 dm:SensorReading。这些类支持未来接入更多数据源，例如综合公共预警与警报系统警报[14], 流式传感器数据、众包报告和其他公开数据集，但当前原型尚未填充这些类。

地理空间特征与影像。为支持多模态推理，文本主干扩展加入了 dm:GeoFeature 和 dm:Image 作为主要类。

- dm:GeoFeature 表示影响区域的地理足迹，数据来自网络声明源和 Shapefile 端点。属性包括用于表示几何形状的 geo:asWKT（归一化为 WGS 84[3] 并采用开放地理空间联盟 (OGC) GeoSPARQL 标准 [19] 编码），以及 dm:hasAreaSqKm 等派生汇总信息。每个 dm:GeoFeature 都通过 dm:describes 链接到其所描述的事件或位置。
- dm:Image 表示无人航空系统及其他应急响应影像。当前实例派生自美国国家海洋和大气管理局应急响应影像元数据 [18]，并同时被赋予 dm:Image 和 iot-reg:Image 两种类型。其属性包括 dm:fileUrl、dm:captured_time 和可选的地理空间键；图像分别通过 dm:captures 和 dm:taken_at 与事件和位置关联。

隐私标志。图像带有布尔标志，用于编码与合规相关的状态；这些标志附加在模式中，而非作为自由格式注释：

- dm:containsPII：表示该制品是否被认为包含个人身份信息。
- iot-reg:isAnonymized：表示是否已应用个人可识别信息混淆转换。
- iot-reg:isEncrypted：表示存储的制品是否已加密。
- dm:isRetained：表示该制品是否作为长期记录保存。

这些标志旨在由操作层中的转换服务以编程方式设置，而非由用户直接编辑。

3.2 策略知识图谱：IoT-Reg 中的美国联邦紧急事务管理局/美国国土安全部规则

策略知识图谱复用 IoT-Reg 本体 [8]，将美国联邦紧急事务管理局和美国国土安全部的隐私需求建模为义务逻辑陈述，并通过 policy-ext 命名空间对其进行扩展。该图谱作为独立的 RDF 图进行维护，并根据 FEMA 系统记录通知 DHS/FEMA-008 [5], FEMA 无人航空系统 PIA-055 [27], 以及美国国土安全部隐私事件处理说明 [28]手动填充。图 2 展示了这一填充流程。

复用 *IoT-Reg*。IoT-Reg 提供以下基础类：iot-reg:Regulation、iot-reg:Permission、iot-reg: Prohibition、iot-reg:Obligation 和 iot-reg:Recipient。在我们的 PKG 中，一个名为 policy-ext:FEMA_Controller 的核心个体（iot-reg:Controller 的实例）代表作为数据控制者的美国联邦紧急事务管理局，而 policy-ext:FEMA_DisasterDataPolicy 则通过 iot-reg:hasPermission、iot-reg:hasProhibition 和 iot-reg:hasObligation 汇总相关规则。

policy-ext 扩展。这些道义规则是通过系统地编码三份源文档中的每一条许可、禁止和义务声明推导而来的；这些声明根据受众或数据类型对工件共享作出限制。为将这些规则与 DKG 中的制品状态关联起来，我们定义了以下属性：

- policy-ext:concernsData：扩展其父属性 iot-reg:involvesPersonalData，以涵盖传统的个人身份信息记录和影像。
- policy-ext:requiresTransform：iot-reg:Obligation 上的一个数据类型属性，用于列出满足该义务的转换函数名称（例如，剥离_exif）。

[3] https://www.w3.org/2003/01/geo/

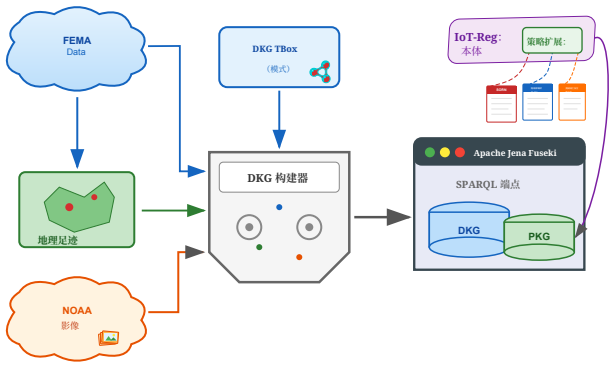


图 2：知识图谱填充流程，展示外部数据源、DKG 构建器处理组件，以及由此生成的 SPARQL 端点。该端点托管灾害知识图谱和政策知识图谱，其中的政策规则源自美国联邦紧急事务管理局/美国国土安全部的监管文件。

- policy-ext:checksFlag：一个数据类型属性，用于命名 DKG 中证明义务已满足的布尔标志（例如，iot-reg:isAnonymized）。

3.3 溯源信息与事件建模

为了使合规状态可供审计，我们将溯源信息和事件视为一等图实体，而不是不透明的日志条目。

制品派生与状态。 DKG 遵循 W3C PROV-O 标准 [17] 来表示转换。应用转换时，我们通过创建新的 dm:Image 实例来表示，而不是修改原始实例。派生图像通过 prov:wasDerivedFrom 与原始图像关联，通过 prov:generatedAtTime 记录创建时间，并携带更新后的隐私标志。

事件与审计。隐私事件在 DKG 中表示为 iot-reg:PersonalDataBreach 个体。每个事件都带有 dm:incidentCategory 和 dm:incidentReason 等注释。审计活动建模为 policy-ext:IncidentAudit 实例，并通过 dm:auditsIncident 与事件关联。

4 策略感知决策框架

本节将灾害响应中的自动化隐私合规问题形式化为一个发布决策函数。我们定义灾害管理知识图谱（DKG）与政策知识图谱（PKG）之间的交互，并确立确保操作安全的必要安全属性。

4.1 问题构建

我们将合规性验证流程建模为两个动态知识图谱上的确定性函数。令 D 表示 DKG，其中存储多模态制品、其元数据和来源信息。令 P 表示 PKG，其中将监管规则编码为道义逻辑构造（许可、义务、禁止）。

我们将发布请求定义为一个元组 $r = a, u, \alpha, \tau$，其中 $a \in$ D 是所请求制品的唯一标识符（URI），$u \in \mathrm{P}_{\mathrm{Actors}}$ 是目标接收方或受众（例如 policy-ext:PublicAudience），$\alpha \in \mathrm{P}_{\mathrm{Activities}}$ 是预期的数据生命周期活动（例如 iot-reg:DataSharing），τ 是通过对 D 进行类型推断得出的 a 的抽象数据类型（例如 iot-reg:PersonalData）。

发布决策函数 δ 将图谱的当前状态和请求映射为合规判定结果以及一组必要的转换：

$$\delta(\mathcal{D}, \mathcal{P}, r) \to \langle v, T \rangle$$

其中，$v \in$ {允许,阻止, 允许并转换}是决策判定结果，T 是为履行待履行义务所需的有序转换函数集。当 v = 允许时，$T = \emptyset$ 和原始制品 a 可以发布。当 v =允许并转换时，强制执行层（第 5 节）应用 T 以生成派生制品 a'；该制品通过溯源信息与 a 关联，并在发布前进行合规验证。

4.2 合规逻辑与安全属性

为确保系统遵循监管标准，决策函数 δ 必须满足三项公理化安全属性。

4.2.1 性质 *1*：禁止优先。 明确的禁止规则优先于所有许可。如果策略图 P 包含一条禁止规则 ρ，且该规则与元组 u, α, τ 匹配，则无论是否存在其他许可，判定结果都必须为阻止。

4.2.2 性质 *2*：故障关闭默认原则。 默认情况下拒绝访问。只有当存在与 r匹配的明确许可 $\pi \in$ P 时，才会生成允许或允许并转换的判定结果。如果未找到此类许可，或者针对 D 或 P 的查询执行失败，系统默认 v = 阻止。

4.2.3 性质 *3*：义务一致性。 只有在附加义务得到满足时，许可 π 才有效。对于与许可 π 关联的义务 o，设 f_o 为由 o跟踪的 D 中的合规标志属性。

- 如果 a 已满足 f_o（即 D $\models f_o(a)$），则该义务已履行。
- 如果 a 不满足 f_o，系统必须确定能够断言 f_o的转换 $t \in$ T。
- 如果 P 中不存在此类转换，则判定结果退回为阻止。

4.3 算法设计

我们通过两个主要算法定义合规框架：决策逻辑和事件记录机制。

4.3.1 算法 *1*：策略感知发布决策。 算法 1 详细说明了发布决策流程。该流程优先进行禁止性检查，以确保快速失败行为。随后，它尝试匹配许可，并通过查询政策知识图谱中映射的转换函数来解决未满足的义务。

4.3.2 算法*2*：事件登记。为满足《通用数据保护条例》和 NISTIR 8228 的监管问责要求，被阻止的

算法1 策略感知发布决策 要求：灾害知识图谱 D、策略知识图谱 P、请求 $r = a, u, \alpha, \tau$ 确保：判定结果 v、转换集 T 定义：$\Phi(p)$：获取附加到许可 p的义务Flag(o)：获取义务o检查的布尔属性Func(o)：获取满足 o的转换函数1：阶段 1：检查禁止项（快速失败）2：$\mathbf{R}_{prohib} \leftarrow$ 查询(P，与 u, α, τ匹配的禁止项) 3：如果 $\mathbf{R}_{prohib} \neq \emptyset$ 则 4：返回 阻止 $\emptyset$ 5：结束如果 6：阶段 2：检查许可（失败关闭） 7：$\mathbf{R}_{perm} \leftarrow$ 查询 (P，与 u, α, τ 匹配的许可) 8：如果 $\mathbf{R}_{perm} = \emptyset$ 则 9：返回 阻止 $\emptyset$ 10：结束如果 11：阶段 3：评估义务 12：选择优先级最高的许可 $p \in \mathbf{R}_{perm}$ 13：T $\leftarrow \emptyset$ 14：对每个义务 $o \in \Phi(p)$执行 15：$flag \leftarrow$ Flag(o) 16：如果 查询(D $\neg$具有标记($a, flag$)) 则 ▷ 检查资产是否违反义务 17：如果 $\exists$Func(o) 则 18：T $\leftarrow$ T $\cup$ {Func(o)} ▷ 映射补救函数 19：否则 20：返回 阻止 $\emptyset$ ▷ 义务无法满足 21：结束如果 22：结束如果 23：结束循环 24：阶段 4：最终裁决 25：如果 T $= \emptyset$ 则 26：返回 允许 $\emptyset$ 27：否则 28：返回 允许并转换, T 29：结束如果

算法2事件登记

要求： 灾害知识图谱 D，请求 r，判定结果 v，原因 msg
确保： 事件 URI i

1: **阶段 1：条件检查**
2: **如果** $v \neq$ 阻止 $\vee\, r.\tau \neq$ iot-reg:PersonalData **则**
3: **返回** $\emptyset$ ▷ 没有需要记录的隐私事件
4: **结束如果**

5: **阶段 2：对事件类别进行分类**
6: $c \leftarrow$分类（msg）
▷ 将原因映射为 {Prohibited_分享，无_许可，无效_受众，转换_失败，其他}

7: **阶段 3：构建知识图谱三元组**
8: $i \leftarrow$ **新建 URI(D,事件) 9:** $t_{\text{now}} \leftarrow$**当前时间戳() 10: Insert(D,** i**, rdf:type, iot-reg:PersonalDataBreach) 11: Insert(D,** i**, prov:wasDerivedFrom** $r.a$**) 12: Insert(D,** i**, dm:incidentCategory** c**) 13: Insert(D,** i**, dm:incidentReason** msg**) 14: Insert(D,** i**, dm:incidentDetectedAt** t_{now}**) 15: return** i

涉及个人数据的请求必须以不可篡改的方式记录。算法2定义了事件登记流程：如果请求因违反政策而被阻止，则将一个PersonalDataBreach实例插入DKG。

5 操作执行层

我们将策略感知决策框架实现为一个操作性强制执行层：该层接收结构化的发布请求，调用第 4 节中的决策算法，执行所需的转换，并使用派生制品和事件记录更新灾害知识图谱。见图 3。本节描述该数据包抽象、转换流水线、工件派生工作流和事件记录机制。

5.1 用于发布请求的数据包模型

发布决策由请求数据包驱动。数据包编码了拟议共享的上下文，同时不会向策略引擎暴露原始文件。每个数据包都是由发布决策运行器处理的 JSON 文档：

- 工件标识符： 一个 URI a，必须已存在于灾害知识图谱中（例如，源无人机系统图像或派生的加密制品）。
- 受众与活动： 预期接收方 u（例如 policy-ext:PublicAudience）以及生命周期活动 α（重点关注 iot-reg:DataSharing）。
- 数据类型： 经断言或推断的数据类型 τ。如果数据包未提供 τ，数据类型检测器会查询灾害知识图谱，根据 RDF 类型推断数据类型。
- 文件位置： 可选的文件 URL 或本地路径，执行层使用它来获取制品以进行转换。

因此，数据包是决策逻辑中所用抽象请求 $r = a,\ u,\ \alpha,\ \tau$ 在运行时的对应形式。运行器会补全缺失字段（例如，推断 τ），然后通过合规策略适配器调用决策函数，后者会针对 PKG 和 DKG 执行 SPARQL 查询。如果这些查询失败，或不存在匹配的许可，则根据故障关闭属性，判定结果仍为阻止。受众身份验证由外部处理；强制执行层使用经过身份验证的受众标识符，但本身不实现身份管理。

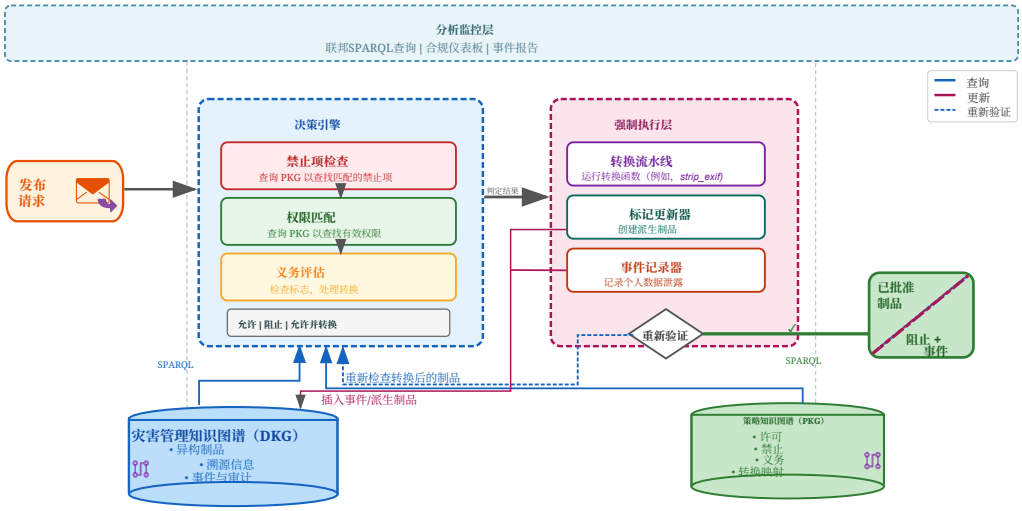


图 3：隐私感知灾害数据共享框架的端到端架构，展示了从发布请求到策略评估、变换执行和合规性验证的流程，并以灾害知识图谱和策略知识图谱作为双重知识源。

5.2 转换流水线

当算法 1 返回允许并转换的判定结果以及一组有序的必需转换 T 时，强制执行层会对底层文件运行转换流水线。每项转换都是一个确定性函数，接收本地路径并返回新路径和成功标志；转换操作针对由文件解析器解析出的本地副本进行。

在我们的原型中，转换是由强制执行层调用的模块化函数。我们定义了两类：

匿名化： 对于计划公开发布的无人机影像，原型实现了 strip_exif，使用标准图像库移除 EXIF 元数据。此函数满足与 Oblig_ObfuscatePII 相关联的 policy-ext:requiresTransform 属性。需要进行视觉个人身份信息混淆（例如人脸模糊化）的部署，可集成其他计算机视觉转换，而无需修改决策逻辑。

加密： 对于与合作机构共享个人身份信息，原型使用 Fernet 对称加密（AES-128-CBC 与 HMAC）实现 encrypt_file。已加密制品会与元数据一起打包；解密密钥则单独存储。这满足 FEMA SORN [5] 和 DHS 事件处理指南 [28]要求的加密义务。

我们的决策框架会确定何时需要进行转换，并验证转换后的合规性——但不会执行转换本身，因为转换因领域而异，且可插拔。转换会按照决策逻辑返回的顺序执行。如果任何必需的转换失败（例如，由于缺少库或文件损坏），运行器会将请求视为不合规，返回阻止判定，并在决策日志中记录失败。不会尝试部分发布或尽力而为的发布，从而保持第 4 节规定的故障关闭行为。

5.3 制品派生与标志更新

为维护不可变的溯源信息（需求 R4），执行层绝不会修改 DisasterKG 中的制品。相反，当必需的转换成功后，FlagUpdater 会创建一个表示转换后制品的新 RDF 个体，并将其链接到原始制品。

对于匿名化，系统会构造一个派生 URI a'（例如，追加 _已匿名化后缀），将其类型设为 iot-reg:Image 和 iot-reg:FeatureOfInterest，并更新隐私标志以反映其状态。此处，dm:containsPII 设为 false，dm:isRetained 设为 true，iot-reg:isAnonymized 设为 true，iot-reg:isEncrypted 设为 false。

派生制品通过 prov:wasDerivedFrom 与原始制品关联，并添加 prov:generatedAtTime、dm:transformedBy（全局唯一决策标识符）、dm:appliedTransforms 以及更新后的 dm:fileUrl 注释。

对于加密的合作方共享，派生制品的类型同时设为 iot-reg:Image 和 iot-reg:PersonalData，因为其中仍包含个人身份信息。在这种情况下，dm:containsPII 保持为 true，iot-reg:isEncrypted 设为 true，并额外添加 iot-reg:usesEncryptionMethod 字面量，以记录加密方案。与匿名化派生制品一样，溯源链和转换元数据也会写入灾害知识图谱。

验证。 插入 a'后，运行器会再次调用决策函数，对派生制品使用相同的受众与活动进行判断。它会验证知识图谱中的新标志是否满足所有义务，以及是否有任何禁止适用。只有再次检查返回“允许”时，运行器才会将 a' 作为已批准的制品返回。这验证了性质 3（义务一致性）：每次允许共享，都对应一个合规状态在知识图谱中得到明确表示并经过独立验证的制品。

5.4 事件检测与日志记录

算法2规定了何时必须将被阻止的请求记录为隐私事件。操作层通过与灾害知识图谱交互的事件记录器来实现这一逻辑。

当决策对类型包含 iot-reg:PersonalData 的制品产生阻止判定时，日志记录器会对原因进行分类（例如禁止共享、无匹配的许可、转换失败），并将一个事件实例插入知识图谱。每个事件均被标记为 iot-reg:PersonalDataBreach，通过 prov:wasDerivedFrom 与受影响的制品关联，并使用 dm:incidentCategory 进行结构化分类，使用 dm:incidentReason 携带决策引擎提供的文本说明，使用 dm:incidentDetectedAt 记录检测时间戳。

后续审计表示为 policy-ext:IncidentAudit 个体，并通过 dm:auditsIncident 与事件关联，同时包含 dm:auditTime 和 dm:auditNotes 字段。由于事件和审计与灾害工件及政策规则共享同一个知识图谱，分析层（第 6 节）可以发出 SPARQL 查询，以汇总事件类别、识别未解决事件，并追踪禁止共享或失败共享的处理方式。这将第 4 节中的抽象事件登记逻辑与可查询的合规实证联系起来。

5.5 实现技术栈

操作性执行层通过 Python 中间件服务实现，用于协调策略评估和转换。DKG 和 PKG 部署为独立的 Apache Jena Fuseki 数据集，并由其三元组数据库（TDB2）提供支持，可在持久化存储之上执行事务性SPARQL 1.1 查询和更新 [24]。评估与强制执行组件通过 SPARQL 端点与两个知识图谱交互，从而将策略逻辑与数据持久化解耦。

6 分析监控层

操作性执行层负责处理逐请求的发布决策，而分析人员则需要全面了解事实、合规状态、待履行义务和隐私事件。为此，我们基于对 DKG 和 PKG 执行的联邦SPARQL查询构建了分析监控层。该层不会重新实现决策逻辑，而是读取相同的道义规则和制品标志，以生成实时合规仪表板。

6.1 联邦式策略–数据查询

DKG 和 PKG 部署为独立的 SPARQL 端点：DKG 存储运行数据（灾害、影像、隐私标志、事件、地理特征和审计记录），PKG 存储道义规则（许可、禁止和义务）。分析查询使用 SERVICE子句将两个知识图谱联接为统一视图。

每个监控查询都遵循一种通用模式：

- 查询 DKG，以获取制品、隐私标志和溯源信息。
- 查询 PKG，以查找相关许可和义务，并获取它们的 policy-ext:checksFlag 属性。
- 按数据类型和受众联接两个子查询，以计算合规摘要。

清单 1 展示了全球合规性仪表板所采用的这一模式。该设计将 PKG 作为规则的唯一事实来源，将 DKG 作为数据状态的唯一事实来源；当法规发生变化时，这种设计可简化维护工作。

```
选择 ?imgName ?audience ?status其中 {
  服务  <http://dkg-endpoint/sparql> {
    ?img a iot-reg:Image ;
         iot-reg:isAnonymized ?isAnon .
    绑定(strafter(str(?img), '#')作为?imgName)
  }
  服务 <http://pkg-endpoint/sparql> {
    ?永久 iot-reg:hasRecipient ?接收方 ;
          iot-reg:hasObligation ?oblig .
    ?oblig policy-ext:checksFlag ?flagProp .
    BIND(strafter(str(?接收方), '#') AS?受众)
  }
  BIND(
    如果(?flagProp  = "iot-reg:isAnonymized",
       IF(BOUND(?isAnon) && ?isAnon, "合规",          "不合规"),
       “未知”
    ) AS ?状态
  )
}
```

清单 1：用于确定合规状态的联邦 SPARQL 查询。

6.2 合规仪表板与受众视图

我们定义了一组联邦查询模板，用于驱动仪表板视图：(i) 全局合规状态，列出每个制品针对各受众的合规状态；(ii) 需要转换的图像，指出不合规的图像及其所需的补救措施；(iii) 受众专属的可共享性，回答“现在可以与受众 u 共享哪些图像？”；(iv) 跨受众合规矩阵，显示哪些情况下需要不同的制品版本；以及 (v) 基于策略的解释，返回阻止请求的具体禁止条款或未履行的义务。每个模板都会动态关联 PKG规则与 DKG状态，从而实现可筛选的实时合规视图。

6.3 事件与审计分析

同样的联邦式方法也为事件分析提供支持。模板可识别未经审计的 iot-reg:PersonalDataBreach 实例，检索特定事件的审计历史，并按 dm:incidentCategory 汇总事件，以揭示系统性问题。解释查询会结合 DKG标记与 PKG规则，追溯特定请求遭到阻止的原因。

这些模板将知识图谱转变为用于监督和策略调整的实时监控界面；相关性能将在第 7 节中进行评估。

7 评估

我们从四个维度评估该框架：DKG 的规模和结构质量；相对于指定策略，发布决策的正确性；转换对 DKG 内合规状态的影响；以及单知识图谱和联邦模板的查询性能。

7.1 实验设置与数据集

我们在涵盖美国联邦紧急事务管理局记录的 2005–2024 年灾害的 DKG 和 PKG 固定快照上进行评估。DKG 汇总了

表1：灾害管理图谱和 PolicyKnowl- edge 图谱的规模，包括类实例计数，以及用于验证评估快照中引用完整性和标志一致性的结构质量保证检查。

规模指标		质量保证检查	
灾害事件	5,060	无地点的事件	0
声明	5,060	无事件的声明	0
声明请求	1,257	派生图像（无来源）	0
位置	5,935	冲突标记	0
地理特征	2,690		
图像	316,090		
DKG 三元组	**5,102,618**		
义务个体	15		
模式类/属性	47		

第 3 节所述的四个 OpenFEMA数据集和美国国家海洋和大气管理局影像来源。所有实验均基于第 5.5 节所述的技术栈进行，PKG 使用 IoT-Reg 本体以及从美国联邦紧急事务管理局/美国国土安全部隐私文件中派生的 15 条领域特定义务逻辑陈述构建。

表1总结了评估中所用知识图谱的规模。DKG快照包含5,060个dm:DisasterEvent个体、5,060个dm:Declaration个体、1,257个dm:DeclarationRequest个体、5,935个dm:Location个体、2,690个dm:GeoFeature足迹，以及从美国国家海洋和大气管理局应急响应影像中派生的316,090个dm:Image实例，共计5,102,618个RDF三元组。Policy KG规模较小，包含IoT-Reg模式、policy-ext本体模块和15个义务个体。

在添加影像之前，我们通过根据美国联邦紧急事务管理局文档检查声明—事件关联、时间字段一致性和项目计数，验证了文本主干。值得注意的是，源数据流中仅有23.4%的事件公开了影响区域URL，因此我们单独进行了GeoFeature摄取。

多模态结构验证。 对于完整快照，我们运行基于 SPARQL 的检查，以检测跨模态链接问题：(i) 没有位置的事件；(ii) 没有关联事件的声明；(iii) 没有 prov:wasDerivedFrom 链接的派生图像；以及 (iv) 隐私标志不一致的图像。在评估快照中，这四项指标均为零：每个事件至少有一个位置，每项声明都关联到一个事件，所有派生图像均包含溯源信息，并且没有公开图像带有冲突标记（表1右侧），这证实摄取管道在策略测试之前会维护结构不变量。

7.2 策略决策正确性

第3.2节和第4节定义了确定性决策逻辑，为每种相关的数据类型、受众和选定标志组合规定预期的判定结果和义务。我们通过构建一组数据包实例金标准集，并将系统的决策与预期结果进行比较来评估这一点。

金标准集由24个数据包组成，这些数据包根据18种策略场景实例化，系统地覆盖了决策空间。这些场景列举了数据类型（图像、个人数据）、受众（公开、合作伙伴、内部、未知）以及合规状态（原始、预转换、错误条件）的所有有效组合，确保每条可达的判定路径都经过检验。核心场景包括：(i) 向公众发布影像，分别考察事先进行和未进行匿名化的情况；(ii) 向合作机构提供个人数据，分别考察是否加密的情况；(iii) 面向公众的个人数据（无论是否经过匿名化，均禁止）；以及 (iv) 面向缺少明确权限的受众的制品（图像面向合作伙伴，以及面向内部和未知受众）。边缘情况包括 DKG 中不存在的制品、格式错误的 URI、变换执行失败、满足的义务超出要求的制品、空值合规标志、针对先前已转换制品的重新请求（幂等性），以及未知数据类型。对于每个数据包，我们都指定了预期的初始判定结果（允许、阻止、允许并转换）、所需义务（如有），以及是否应创建隐私事件。表2汇总了这24个黄金数据包、其预期和实际观察到的判定结果、所需义务，以及是否创建了隐私事件。本文的两位作者分别根据策略文档独立推导金标准集的判定结果，并对结果进行了交叉核对；由于第4节中的决策规则将请求映射到判定结果的方式定义为确定性的，因此双方没有出现分歧。

在这组金标准数据上，系统在全部24个案例中都给出了正确的判定结果和义务，完全匹配准确率达到1.0。在我们的单机环境中，每次决策的延迟中位数为0.06秒，平均值为0.10秒，第95百分位数为0.18秒。系统行为符合规范性决策逻辑：例如，向公众提供未匿名化图像时，会被分配“允许并转换”判定结果，并附带混淆个人身份信息的义务；向合作机构提供加密的个人数据时，会予以允许且不会触发事件；而面向公众的个人数据则会被阻止，并触发事件创建。由于策略引擎完全确定，并直接实现了指定的策略语义，因此预期能够取得满分，这证实该实现针对我们计划支持的组合落实了指定的策略语义。

7.3 转换对合规状态的影响

上一小节评估了系统是否选择了正确的判定结果和义务。我们还需要验证，当需要执行转换时，DKG 中生成的制品和标志是否与预期的合规状态一致。为此，我们在执行黄金数据包后，对知识图谱进行一致性评估，并检查以下三个不变量：

- 图像匿名化：对于初始判定结果为允许并转换、带有混淆义务，且最终判定结果为允许的图像数据包，DKG 必须包含一个派生的 dm:Image 资源，该资源通过 prov:wasDerivedFrom 与原始资源关联，标记为已匿名化（iot-reg:isAnonymized=true），且不再标记为包含个人数据。
- 个人身份信息加密： 对于初始判定结果为允许并转换、负有加密义务且最终裁决为允许的个人数据数据包，DKG 必须包含一个标记为已加密（iot-reg:isEncrypted=true）且与原始制品建立溯源关联的派生制品。

表2：在涵盖18个场景的24个发布请求包金标准集上的策略决策正确性，按结果类别分组。

Pkt.	场景	请求	判定结果	转换	Inc.
允许（预合规）					
P2	预匿名化	图像†→公开 个人身份信息′→合作伙伴	允许	–	–
P4	预加密		允许	–	–
P9	过度转换	图像†→公开 个人身份信息′→合作伙伴	允许	–	–
P10	过度转换		允许	–	–
P11	不存在个人身份信息	图像°→公开	允许	–	–
P15	加密图像	图像†→合作伙伴	允许	–	–
P23	派生制品	图像′→公开	允许	–	–
P24	重新请求	个人身份信息′→合作伙伴	允许	–	–
通过转换允许					
P1	原始图像	图像→公开 个人身份信息→合作伙伴	AwT→允许	剥离	–
P3	原始个人身份信息		AwT→允许	enc	–
P19	空值标志	图像→公开	AwT→允许	剥离	–
P21	未保留	图像→公开	AwT→允许	剥离	–
P22	多重义务	个人身份信息→合作伙伴	AwT→允许	enc	–
阻止（禁止）					
P5	个人身份信息至公开	个人身份信息→公开	阻止	–	✓
P16	匿名个人身份信息公开	个人身份信息†→公开	阻止	–	✓
阻止（无许可）					
P6	无图像→合作伙伴永久图像→合作伙伴		阻止	–	–
P7	未知受众	个人身份信息→未知	阻止	–	✓
P14	内部受众	个人身份信息→内部	阻止	–	✓
P17	未知受众	图像→未知	阻止	–	–
阻止（错误条件）					
P8	文件缺失	图像‡→公开 个人身份信息*→合作伙伴	AwT→B	–	–
P12	不在 DKG 中		阻止	–	✓
P13	转换失败	图像×→公开 个人身份信息×→合作伙伴	AwT→B	–	–
P18	格式错误的 URI		阻止	–	✓
P20	未知类型	传感器→发布区块		–	–

准确率： 24/24 (1.0) **延迟：** μ=0.10 秒，中位数=0.06 秒，p95=0.18 秒

AwT=允许并转换，A=允许，B=阻止。Pub=公开，Ptnr=合作伙伴，Unk=未知，Int=内部。
†预转换。○无个人身份信息。′派生/重新请求。‡文件缺失。◎不在 DKG 中。×损坏。△格式错误的 URI。转换：剥离=剥离_EXIF，加密=加密_文件。事件=已记录。

- 事件记录： 对于最终裁决为阻止且数据类型为 iot-reg:PersonalData 的数据包，DKG 必须包含一个与原始制品关联的 iot-reg:PersonalDataBreach 资源，并为其标注事件类别和原因。

在所有黄金数据包中，图像匿名化、个人身份信息加密和事件记录的所有适用一致性检查均已通过。表 3 详细说明了其中一个案例的制品状态转换。

7.4 查询性能与可扩展性

现在，我们评估已配置查询模板的行为。如第6节所述，分析监控层基于一个包含 DKG 和 PKG 上 SPARQL 查询模板的库构建，并通过命令行界面向用户开放。为了进行评估，我们定义了两种工作负载：21 个仅针对 DKG 的模板，以及 5 个同时涉及 DKG 和 PKG 的联邦模板。

表 3：联邦决策追踪：合作机构个人身份信息共享

	图	查询	结果
阶段 *1*：义务逻辑评估			
1	PKG	是否匹配禁止规定?	None
2	PKG	权限匹配	:允许_个人身份信息_至_合作伙伴
3	PKG	附加义务	:义务_加密并记录
4	PKG	检查标志	iot-reg:isEncrypted
5	DKG	标志已满足?	false
6	PKG	需要转换	"加密_文件"
判定结果：允许并转换 加密_文件			
阶段 *2*：转换执行与验证			
7	–	调用加密_文件	dm:Image_..._已加密
8	DKG	插入派生制品	已加密 ← true
9	DKG	重新验证义务	已满足
最终裁决： 允许 — 将 dm:Image_..._enc 发布给 :PartnerAgency			

请求： r = ⟨dm:Image_17dd9ac6cded_2005_飓风_Katrina、: PartnerAgency、iot-reg:DataSharing、iot-reg:PersonalData⟩。对比： 同一制品的受众为 :PublicAudience 时，在第 1 步通过 :Prohibit_Partner_Reshare 触发阻止，并将 dm:Incident_f1508633... 记录为 iot-reg:PersonalDataBreach。

表4：SPARQL查询模板库的延迟统计，比较单图DKG查询与联邦式 DKG+PKG合规性查询在 316K图像评估快照上的表现。

工作负载	N	通过	平均值	Med	p95
单知识图谱（DKG）	21	100%	0.05 秒	0.02 秒	0.13秒
联邦式 (DKG+PKG)	5	100%	7.0 s	5.3 s	10.5s

单知识图谱模板。 这 21 个仅针对 DKG 的模板涵盖了分析员任务，从灾害筛选（按州、年份和事件类型）到图像溯源检查。每个模板都提供一个参数化自然语言提示（例如，“显示在 {state} 中具有地理特征的灾害”），并配有少量参数，因此无需具备 SPARQL 专业知识，即可在不同查询中重复使用。全部 21 个模板均成功执行，且延迟较低：参见表4。

联邦模板。 该工作负载通过执行联邦SPARQL查询并联接 DKG 和 PKG，测试了更丰富的策略感知行为。这五个模板实现了：(i) 汇总所有图像状态的全局合规仪表板；(ii) 展示发布前需要进行转换的图像；(iii) 受众特定合规摘要；(iv) 检索针对特定图像所作决定的策略依据的解释查询；以及 (v) 针对卡特里娜飓风等具名事件的跨受众合规摘要。五个模板均成功执行。延迟统计显示，平均值为 7.0 秒，中位数为 5.3 秒，第 95 百分位数为 10.5 秒。初始实现的延迟较高，这是因为联接包含 31.6 万张图像的 DKG 与 PKG 规则时产生了笛卡尔积；通过调整 SERVICE 子句的顺序，优先查询规模较小的 PKG，并根据合规标志进行预筛选，将开销最高的查询时间从 1,200 秒以上缩短至 5 秒以内。这些交互式延迟

与美国联邦紧急事务管理局数据共享治理下的人工合规审查相比，表现更为出色；人工审查可能需要数天至数周，具体取决于请求渠道。

两种工作负载的成功率均达到 100%，这是设计选择的结果：模板由人工编写，并针对固定的 DKG 和 PKG 模式进行参数化；用户从这些模板中进行选择，而不是输入任意的自由文本。因此，评估衡量的是配置好的查询库能否在其旨在支持的各类问题中保持一致的行为，而不是模型能否生成 SPARQL。

8 讨论：可推广性与局限性

本节讨论我们的框架在其他领域的可推广性，并承认其当前的局限性。

8.1 可推广性

虽然我们的实现面向美国联邦紧急事务管理局灾害数据，但底层架构与领域无关。领域特定 DKG 与政策编码 PKG 之间的分离意味着，将该框架适配到其他情境只需：(i) 定义新的领域本体（类似于 dm:），并包含工件类型、溯源信息和隐私相关标记；(ii) 使用适合该领域的道义规则实例化 IoT-Reg，将许可、义务和禁止映射到新的工件类型和受众；以及 (iii) 实现针对该领域数据模态的转换函数。

8.2 局限性

我们的原型实现了 strip_exif，用于移除 EXIF 元数据；还实现了 encrypt_file，用于基于 Fernet 的对称加密。目前尚未实现视觉个人身份信息混淆（例如人脸模糊化）；需要此功能的部署可将计算机视觉管线集成为额外的转换函数。不过，框架的设计已考虑到这一点：转换可以插拔，而第 5.3 节中的验证步骤会检查合规标志，不受标志设置方式的影响。因此，我们的评估验证系统是否选择了正确的判定结果和义务，但并未衡量转换本身的有效性。未来工作可整合转换管线提供的置信度分数，并将置信度较低的转换标记出来以供人工审核，从而进一步应对第 2.3 节所述的威胁 F2（静默转换失败）。

当前的 PKG 包含 15 个道义个体，派生自三份美国联邦紧急事务管理局/美国国土安全部文件。对于我们的用例而言，这已足够；但若扩展到数百条规则，可能会出现无法通过简单的禁止优先解决的冲突。将可废止道义逻辑或优先级注释纳入其中，是未来工作的一个方向。

我们的框架不对灾害幸存者的个人同意进行建模。美国联邦紧急事务管理局的运作环境依赖法定授权，而非个人同意；将基于同意的权限纳入 PKG 则是未来的工作。

9 相关工作

我们从三个领域阐述本研究的贡献：语义隐私框架、灾害信息学和策略感知数据系统。

Joshi 等人 [16] 提出了一种用于云数据合规的集成知识图谱，以机器可处理的格式捕捉《通用数据保护条例》和其他法规，展现了语义方法在隐私合规自动化方面的价值。LegalRuleML [15]为以兼容 XML 的格式编码道义算子提供了标准。我们的工作以 IoT-Reg [8], 为基础，扩展了针对灾害影像的变换-义务绑定。近期用于合规查询的知识图谱-大语言模型集成 [9]与我们确定性的、经溯源验证的决策引擎相辅相成。

Pak 和 Mostafavi [20] 指出，态势感知是灾害韧性的核心，这促使人们开展多源数据集成。Sanfilippo 等人 [22] 将灾害中的隐私-效用权衡概括为“灾害隐私／隐私灾害”。我们的“允许并变换”判定结果直接应对这一权衡，使得能够在明确义务约束下进行有条件共享。以往的灾害知识图谱侧重于事件抽取和资源协调；我们则将隐私合规作为一项首要要素纳入其中。

XACML [21] 提供策略决策点，其结果包括允许／拒绝／不适用／不确定，并支持义务。我们的框架对此进行了细化，区分允许与允许并转换，将义务与转换绑定，并在发布前通过来源关联的派生数据制品重新验证合规性。不同于将执行交由外部处理的 XACML 系统，我们将变换要求嵌入策略图，并依据知识图谱验证变换后状态。希波克拉底数据库 [1]等基于用途的系统会根据声明用途跟踪数据使用情况。我们通过使合规状态可跨关联知识图谱查询，对这些系统作出补充。

我们的工作具有以下特色：（1）采用具有溯源验证合规性的形式化允许并转换语义；（2）应用于受重叠联邦授权要求约束的多模态灾害工件；（3）实现端到端覆盖策略建模、决策逻辑、变换执行和事件记录。

10 结论

我们提出了一个框架，用于调和灾害响应中行动紧迫性与隐私合规之间的矛盾。通过将多模态灾害知识图谱与监管政策知识图谱相结合，我们超越了二元访问控制，构建出支持允许并转换决策的道义模型。该机制将抽象义务绑定到可执行补救措施（如匿名化或加密），并通过来源关联的派生数据制品验证合规性。在包含 510 万个三元组的快照上进行的评估证实，该系统实现了精确匹配决策正确性和亚秒级延迟，在数据封锁与不受约束的发布之间提供了一条可行的折中路径。尽管目前侧重于美国联邦紧急事务管理局的授权要求，但该架构可推广到任何需要合规共享敏感多模态数据的领域，例如智慧城市或医疗保健。未来的工作将探索可撤销推理，以解决复杂的监管冲突，并整合基于同意的权限，以实现以幸存者为中心的隐私保护。

致谢

本研究部分由美国国土安全部通过美国国家科学基金会奖项 2310844（IUCRC第二阶段，实时加速分析中心，CARTA）提供的补充资金资助。

参考文献

[1] Rakesh Agrawal、Jerry Kiernan、Ramakrishnan Srikant 和 Yirong Xu。2002年。《希波克拉底数据库》。载于第28届超大型数据库国际会议（VLDB）论文集。Morgan Kaufmann，中国香港，143–154。[2] K. Boeckl、M. Fagan、W. Fisher、N. Lefkovitz、K. Megas、E. Nadeau、D. G. O'Rourke、B. Piccarreta 和 K. Scarfone。2019年。互联网 of Things（物联网）网络安全与隐私风险管理注意事项。技术报告 NISTIR 8228。美国国家标准与技术研究院。https://doi.org/10.6028/NIST.IR.8228 访问日期：2025-12-02。[3] Piero A. Bonatti、Sabrina Kirrane、Axel Polleres 和 Rigo Wenning。2020年。透明的个人数据处理：未来之路。《IEEE会刊》108，1（2020），197–213。探讨语义网在隐私／《通用数据保护条例》合规中的应用。[4] Mina Deng、Kim Wuyts、Riccardo Scandariato、Bart Preneel 和 Wouter Joosen。2011年。隐私威胁分析框架：支持隐私需求的引出。《需求工程》16，1（2011年3月），3–32。https: //doi.org/ 10 1007 00766 010 0115 7 . /s - - - 美国国土安全部和美国联邦紧急事务管理局。2024年。《1974年隐私法》；记录系统。《联邦公报》，页码 73104–73109。https://www.govinfo.gov/content/pkg/FR-2024-09-09/pdf/2024- 20155.pdf《联邦公报》文件 2024-20155。[6] Quang Do、Ben Martini 和 Kim-Kwang Raymond Choo。2019年。对手模型在应用安全研究中的作用。《计算机与安全》81（2019年3月），–。https://doi.org/ . /j.cose. . . Kelvin Echenim、Lavanya Elluri 和 Karuna P. Joshi。2023年。通过物联网法规确保可穿戴设备的隐私政策合规。载于2023年IEEE智能系统、应用领域的信任、隐私与安全国际会议（TPS-ISA）论文集。IEEE。验证了 IoT-Reg 对可穿戴设备的适用性，并以 NISTIR 8228 为依据。[8] Kelvin Echenim 和 Karuna P. Joshi。2023年。IoT-Reg：用于实时物联网数据隐私合规的综合知识图谱。载于2023年IEEE大数据国际会议（Big Data）论文集。IEEE，4077–4084。https://doi.org/10.1109/ BigData 59044 2023 10386545 . . Kelvin U. Ec henim 和 Karuna P. Joshi。2025年。通过将知识图谱与大语言模型相结合，实现物联网数据隐私合规自动化。《IEEE Access》13（2025），118438–118451。https://doi.org/10.1109/ACCESS.2025. 3586278[10] 美国联邦紧急事务管理局。2024年。OpenFEMA数据集：灾害声明驳回记录 - v1。https://www.fema.gov/openfema-data-page/declaration-denials-v1 访问日期：2025年12月4日。[11] 美国联邦紧急事务管理局。2024年。OpenFEMA数据集：灾害声明摘要 - v2。https://www.fema.gov/openfema-data-page/ disaster-declarations-summaries-v2 访问日期：2025年12月4日。[12] 美国联邦紧急事务管理局。2024年。OpenFEMA数据集：FEMA网页灾害声明区域 - v1。https://www.fema.gov/openfema-data-page/fema-web- declaration-areas-v1 访问日期：2025年12月4日。[13] 美国联邦紧急事务管理局。2024年。OpenFEMA数据集：FEMA网页灾害摘要 - v1。https://www.fema.gov/openfema-data-page/fema-web-disaster-summaries-v1 访问日期：2025年12月4日。[14] 美国联邦紧急事务管理局。2024年。OpenFEMA数据集：IPAWS归档警报 - v1。https://www.fema.gov/openfema-data-page/ipaws- archived-alerts-v1 访问日期：2025-12-12。[15] Guido Governatori、Tara Athan、Harold Boley 和 Adam Wyner。2015年。Legal-RuleML：核心规范与法律规则建模。载于第15届人工智能与法律国际会议（ICAIL）论文集。ACM，197–202。用于在语义网中建模道义逻辑的标准。[16] Karuna Pande Joshi、Lavanya Elluri 和 Ankur Nagar。2020年。用于云数据合规自动化的集成知识图谱。《IEEE Access》8（2020），148541 148555 10 1109 2020 3016373 –。https://doi.org/ . /2013[17] ACCESS. . Timothy Lebo、Satya Sahoo 和 Deborah McGuinness。. PROV-O：PROV本体。W3C建议。万维网联盟（W3C）。https://www.w3.org/TR/prov-o/[18] 美国国家大地测量局。2024年。NOAA应急响应影像。https: //storms.ngs.noaa.gov/ 访问日期：2025年12月4日。[19] 开放地理空间联盟。2012年。OGC GeoSPARQL——RDF数据的地理查询语言。https://www.ogc.org/standards/geosparql[20] Hongrak Pak 和 Ali Mostafavi。2025年。在复合灾害与人工智能时代，态势感知是实现灾害韧性的关键能力。arXiv预印本（2025年）。arXiv:2508.16669 [cs.CY] https://arxiv.org/ abs/2508.16669[21] Erik Rissanen。2013年。可扩展访问控制标记语言（XACML）3.0版。OASIS标准。OASIS。http://docs.oasis-open.org/xacml/3.0/xacml-3.0- core-spec-os-en.html 访问日期：2025-12-10。[22] Madelyn R Sanfilippo、Yan Shvartzshnaider、Irwin Reyes、Helen Nissenbaum 和 Serge Egelman。2020年。灾害隐私／隐私灾害。《信息科学与技术协会期刊》71，9（2020），1002–1014。[23] Adam Shostack。2014年。《威胁建模：面向安全的设计》。John Wiley & Sons，印第安纳波利斯，印第安纳州。[24] 阿帕奇软件基金会。2024年。Apache Jena。https://jena.apache.org/ 访问日期：2025年12月4日。[25] 美国国土安全部。2011年。隐私政策与合规。技术报告指令 047-01-001。美国国土安全部。https://www.dhs.gov/sites/default/files/publications/privacy-policy-compliance-instruction-047-01-001_0.pdf 访问日期：2025-12-02。[26] 美国国土安全部。2024年。航空器系统隐私影响评估更新。技术报告 DHS/CBP/PIA-018(b)。美国国土安全部。https://www.dhs.gov/sites/default/files/2024-05/24_0508_ priv_ pia-cbp-018b-tsuas-update_0.pdf 访问日期：2025-12-02。[27] 美国国土安全部和联邦紧急事务管理局。2020年。联邦紧急事务管理局应急响应使用无人机系统（*UAS*）衍生影像的隐私影响评估。技术报告 DHS/FEMA/PIA-055。美国国土安全部。https://www.dhs.gov/sites/default/files/ publications/privacy_pia_fema_055_uas_ may2020_0.pdf[28] 美国国土安全部隐私办公室。2024年。隐私事件处理指令。技术报告 DHS 指令 047-01-008，修订版 00.2。美国国土安全部。https://www.dhs.gov/sites/default/files/ 2024-07/2024_0618_ privacyincidenthandlinginstructions.pdf 最初于2017年12月4日发布；纳入已于2024年6月18日批准的变更 2。[29] Jean-Paul A. Yaacoub、Hassan N. Noura、Ola Salman 和 Ali Chehab。2023年。关于无人机安全与隐私问题的综述。《计算机网络》224 (2023), 109626. https://doi.org/10.1016/j.comnet.2023.109626