联合国推荐实践 纲要 在反恐斗争中负责任地使用和分 享 生物识别技术

联合国
反恐怖主义办公室
联合国反恐怖主义中心

联合国安理会
反恐怖主义委员会执行局 (反恐执行局)

BIOMETRICS INSTITUTE

联合国推荐实践
纲要
在反恐斗争中负责任地使用和分享生物识别技术

由联合国反恐怖主义委员会执行局和联合国反恐怖主义办公室于2018年共同编制

联合国推荐实践
纲要
在反恐斗争中负责任地使用和分享生物识别技术

与生物识别学会协作制作

目录

执行摘要

本纲要高水平地概述了反恐行动背景下的生物识别技术和操作系统。本纲要主要供在生物识别应用程序方面可能具有较少或无经验及可能在实施该技术时面临技术援助和能力建设挑战的联合国会员国阅读。

各章节末尾提供了供拓展阅读的综合参考文献，此外，还提供了推荐的实践摘要。整个纲要全文中贯穿引入了很多案例研究，提供良好做法和新兴技术的示例。

第一节介绍了生物识别技术和身份管理的主要要素，包括生物识别技术在法医学和执法调查领域的广泛应用以及由此引起的问题复杂化现象。

第二节从国际法、人权法、伦理审查、数据保护要求和隐私权的角度介绍了生物识别技术的管理和监管要求。随后，对生物识别系统和一些可以用来降低风险的控制措施的潜在漏洞进行了概述。接着，探讨了国际技术和科学操作标准，包括生物识别应用程序的认证和鉴定以及用于相关法医学流程的质量管理系统。该章节最后一部分讨论了反恐生物识别系统或网络的获得、维护和资源要求，尤其对评估未来的新系统或扩展系统时需要进行的关键操作和财务决策进行了介绍。

最后一节对目前执法、边境管理和军事应用范围内的反恐生物识别系统和数据库进行了总体概述。该章节还介绍了进行生物识别数据的双边、多边分享或在区域内或全球范围内分享该等数据的好处，以及在与其他情报资料一同使用时，如何在生物识别数据作为调查工具的惯常用途之外，前瞻性地运用该等数据防止恐怖主义行为。随后，在国际人权和充分知情、需要合法和相应回应的背景下，对主管当局根据生物特征的匹配而采取的行动进行了介绍。本节最后一部分探讨了将生物识别技术纳入会员国和各地区的反恐战略的问题，以及边境和执法机构在积极支持这些策略方面发挥的重要角色。

本纲要是一份动态文件，且已为下列目的，进行了版本控制：

- 了解生物识别技术领域迅猛发展的技术创新和科技并采取应对之策，以及
- 适应并紧跟新出现和不断演变的国际恐怖主义威胁。

前言

安全理事会关于加强国际执法和反恐司法合作的第 2322 号决议（2016 年）明确呼吁会员国共享国外恐怖主义作战人员 (FTF) 以及其他个人恐怖分子和恐怖组织的信息，包括生物识别信息和个人资料。安全理事会在其 2396 号决议（2017 年）中决定，各国应根据国内法律和国际人权法开发并实施生物特征数据收集系统，该系统中可能会纳入指纹、相片、人脸识别和其他相关生物特征识别数据，以便以负责任和正确的方式识别恐怖分子，包括 FTF。该决议还鼓励会员国以负责任的方式向其他会员国以及国际刑警组织 (INTERPOL) 和其他相关国际机构分享相关数据。

有效地交换生物数据对调查跨国犯罪及识别恐怖分子身份而言，至关重要。在恐怖主义相关调查的背景下，生物识别和其他法医技术可通过（除其他事项外）将个人与特定活动、事件、地点、材料或其他个人相联系，为调查者和检察官提供极大帮助。因此，强化会员国在此方面的能力十分关键。

本良好做法和推荐做法纲要由反恐执行工作队 (CTITF) 与反恐有关的边境管理和执法工作组共同编写，同时获得设于联合国反恐办公室 (UNOCT) 的联合国反恐中心 (UNCCT) 提供的财政支持。本纲要探讨了治理、法规、数据保护、隐私政策、人权法以及风险管理和弱点评估等关键问题。

各国政府必须处理此项技术在人权方面产生的影响，以防止被该等系统识别出身份的人遭受虐待，并确保在规划阶段及随后采取的行动符合国际和区域人权文书中所载的国际法义务。如同所有安全措施，生物识别技术也存在漏洞。关键在于如何识别、理解并尽量减少系统漏洞。其能否成功，关键取决于设计是否用心，录入的生物识别数据是否准确以及如何设置匹配参数。有多种软件和硬件方面的技术可以用来检测、抵御并降低欺骗[1]攻击风险。

本纲要是与生物识别学会合作编制的。生物识别学会 是一家非盈利组织，旨在促进以负责任和符合伦理的方式使用生物识别技术并未为物识别技术的使用者和其他相关方提供独立、公正的论坛。生物识别学会与反恐怖主义委员会执行局 (CTED) 密切合作，以组建国际专家联盟，为本纲要的制定提供指导，联盟成员包括具有反恐、执法、边境管理、生物识别技术、隐私和数据保护背景的政府专家和生物识别专家。

本纲要在一个长期项目的框架内制定，旨在强化会员国以及相关国际和地区实体根据上述安全理事会决议，收集、记录和分享恐怖分子（包括 FTF）相关生物识别信息的能力。本生物识别技术项目由 CTED 和 CTITF 实体（如 INTERPOL、联合国毒品和犯罪问题办公室 (UNODC)、国际民用航空组织 (ICAO) 和联合国难民事务高级专员署 (UNHCR)）共同实施。本项目旨在提高人们在地区和国际行动方面的意识，以推广生物识别技术的使用；强化相关实体之间的合作和协调；在全球范围内加强生物识别技术的使用和分享（包括通过促进在 INTERPOL 和通知中系统性地纳入与恐怖分子概况相关联的生物识别信息）；及使向本地区会员国提供的协助发挥更大效力。

[1] “欺骗”（亦称呈现攻击）指呈现合法、注册用户的虚假生物识别特征（如乳胶面罩、相片、假手指或录音），以在未经授权的情况下进入生物特征识别系统。

Vladimir Voronkov
联合国反恐办公室
副秘书长
联合国反恐中心
执行主任

Michèle Coninsx
反恐怖主义委员会执行局
常务副秘书长
执行主任

关于生物识别学会

生物识别学会是一家非盈利组织，旨在促进以负责任和符合伦理的方式使用生物识别技术，该组织愿意为本项目提供支持。生物识别学会为生物识别技术的使用者和其他相关方提供独立、国际化的公正论坛。学会负责为其会员、关键利益相关者和公众提供生物识别技术方面的教育并使其了解相关知识，为标准、政策和最佳实践的制定和了解提供支持，并提升生物识别系统和项目的安全性和完整性。

该学会于 2001 年成立，在伦敦和悉尼设有办事处。其会员为 30 个不同国家的 230 多家组织，所涵盖的用户群体范围较广，包括政府机构、边境、执法机构、银行和航空公司以及研究人员、供应商和隐私专家。该学会并非推广生物识别技术，而是强调以负责任的方式使用生物识别系统以及该等系统的安全性和完整性，最重要的是，强调隐私和数据保护。该学会认识到，生物识别技术存在固有弱点，且需要对该等弱点进行识别和缓解。

生物识别技术、隐私和人权

生物识别技术变得越来越普及，同时，由于在手机上应用了生物识别技术，公众更加接纳该项技术，而不一定了解其带来的影响。在此情况下，提供更多与生物识别应用程序的好处与风险相关的教育显得十分有必要。生物识别技术十分简便，可提高安全级别。但仍然存在一些挑战，如隐私权保护、数据保护和防欺骗等。只应在必要和适当的时候，收集并存储个人数据，如生物识别数据。

生物识别技术在全球反恐行动（即反欺诈、识别恐怖分子为开展相关行动而做出的盗窃和其他犯罪行为）中发挥着越来越重要的作用。但政府必须对被该等系统识别出身份的人员采取保护措施，并确保根据包括《公民权利及政治权利国际公约》(ICCPR) 和《联合国世界人权宣言》(UDHR) 在内的国际人权和隐私法进行生物识别数据的收集、存储和使用，以充分运用生物识别技术。

必须对生物识别特征/身份被盗或遇到系统故障的人员进行保护。恢复个人身份并不像重置密码那样简单。您的生物识别数据将伴随您终身，不能有丝毫大意。本纲要载述将有效的反恐战略与隐私权和其他人权相结合这一艰难的任务及可能的解决方案。

生物识别系统的漏洞和攻击

如同所有安全措施，生物识别技术也存在漏洞。关键在于如何尽量减少系统漏洞。其能否成功，关键取决于设计是否用心，录入的生物识别数据是否准确以及如何设置匹配参数。如果将参数设置过高，则可能产生“伪报错”，使真正用户的访问请求遭拒。如果参数值设置地不够高，则可能产生“漏报”，使冒充用户者可以访问。

生物识别学会保持合理程度的谨慎，以确保本纲要中提供的材料的准确性。由于在实施生物识别技术期间及之后输入内容和变量，该学会不对结果或合规情况负责。本纲要仅供参考，无意提供法律或合规意见。

Andrew Rice
主席兼董事
生物识别学会

Isabelle Moeller
首席执行官
生物识别学会

1. 生物识别系统和身份介绍

第一节介绍了生物识别技术和身份管理的主要要素，包括生物识别技术在法医学和执法调查领域的广泛应用以及由此引起的问题复杂化现象。

人类是群居动物，具有识别、进而区分其熟悉的人的特殊能力。同时，人类具有强烈的自我意识，以及个体特殊性。将自己视为独特的个人并承认他人的独特性是我们的社会本能。从生物角度来说，人类是独特的（就所有实际目的而言）。但我们的"人类识别引擎"在生物学上却无法运转，实际上，人类在区分不熟悉的人时表现得并不如人意。人类使用的身份识别系统也不符合生物学规律。相反，该等系统同时使用身份属性和背景属性作为标记。这些标记可以表示所描述的生物实体，但却与实体有所不同[2]。

身份属性包括姓名、出生日期和地点、国籍、性别和生物识别[3]标识符。背景属性是交易信息，通常与地点和时间有关。使用背景属性，可提高身份识别的准确性。身份属性可以是个人资料或生物识别数据，在特定情况下，可能会发生变化。例如，可能发生变化的个人资料身份属性可能包括：

- 姓名 — 受音译影响，即同一名字可能有不同拼法
- 出生日期 — 受延迟登记或官方记录不一致因素影响
- 出生地点 — 可能用多种方式表示
- 性别 — 受个人偏好、身体重置等因素影响。
- 国籍 — 可以有多重国籍且可能发生变化

在人类的生命周期中，生物识别身份属性（如其体型相对大小或可推断特征的阐述和定义）可能会随着年岁的增长或患病而发生变化。有些人的生物识别特征可能会损坏或缺失。例如，指纹在妊娠期内形成，除非损坏，否则终身不变，且可能在死后保留相当长的时间，尤其会在对皮肤起干燥作用的温暖、干燥环境中保留。尽管指纹结构中的纹路布局不会改变，但一生中，手指本身的大小却会发生变化，且指纹特征的质量可能会因坏境破坏、其他损伤或年龄的增长而下降。其他生物识别特征也可能发生类似变化。因此，正在开发生物识别应用程序中使用了现代算法，针对该等变化进行适当调整，以使系统中注册用户的数量最大化，而且，即使年龄发生变化或其生物识别特征的质量轻微下降，也能使尽可能多人的记录保留在系统中。

生物识别标记是身份属性，由于这些标记可以准确地表示所描述人员的特征，其为数字对比提供了良好的基础。但如同个人资料身份属性，生物识别样本一旦以图像形式捕获或转换为模板或配置文件，便与它描述的生物实体不同。捕获并记录身份属性，包括生物识别属性，是一个永远都不可能尽善尽美的过程，因此，可能会出错。生物特征比较中固有的概率性匹配受到统计方差的影响。除非实施稳健的防护措施并在系统风险管理流程中不断更新该等措施，否则人类识别系统中出现的错误和统计方差可能使其容易遭受一系列攻击（参见第 2.3 节）。[4]如何缓解人类识别系统的上述固有

[2] *Identity verification- The importance of context and continuity of identity*, p11-16 Keesing Journal of Documents & Identity, Annual Report Identity Management 2011-2012

[3] 1995 年，美国政府生物识别联盟将"生物识别技术"定义为"……根据个人行为和生物特征对个人进行的自动识别。"

[4] "人类识别系统本质上具有概率性，因此本质上容易出错。出错的概率可以降低，但错误不可消除。系统设计人员和操作人员应该预期到错误的发生并为此制定计划，即使错误预计很少出现。"*Biometric Recognition: Challenges and Opportunities（生物特征识别：挑战与机遇），第 1 页，National Research Council（国家研究委员会），华盛顿（2010 年），下载地址：* http://www.nap.edu/openbook.php?record_id=12720&page=1

弱点是本纲要的关键主题之一。

生物识别系统旨在通过使用个人生物和生理特征，如指纹、手静脉纹、虹膜、人脸、DNA 和其他特征，对个人进行识别。[5]上述各项特征均代表一种生物模态。何种生物识别模态是最佳选择，将取决于应用程序用例的背景（参见第 2.5 节）。一般而言，生物识别模态或多或少都具有以下几个固有特征[6]：

- 普遍性 — 所有人都具有该等模态（生物识别特征受损或缺失的人除外）
- 独特性 — 其可以区分注册人员的个人身份。对于特定模态而言，这可以变化，例如，同卵双胞胎的 DNA 图谱可能相同，但指纹不同。
- 永恒性 — 考虑到人类生命周期引起的变化，该等模态应该较为稳定，不随时间变化。
- 可测量 — 系统应该可以轻松获取该等模态，并将其数字化
- 有效执行 — 该等模态在主要和转介业务流程中，应该准确、快速及稳健
- 可接受 — 其应符合社会规范和期待，且能够被很大比例的适用的注册人群所使用
- 容易遭受规避风险 — 除非采取严格的应对措施并对该等措施进行持续更新，否则冒名使用者可以使用各种人工制品和替代品进行未经授权的访问

由于许多生物识别系统都涉及与参考数据相比较，在选择偏好的模态时，是否有可供使用的遗留数据（该等数据已经或可以编译到可用及有用的参考数据库，以进行身份确定或验证）是考虑的关键因素之一。系统可能只使用一种模态（单模式功能），例如人脸识别，或者可能综合运用多个模态（多模式功能），如指纹、虹膜和面部。生物识别系统在各个公共和商业领域的运用范围正在迅速扩大，包括：

- 国家民事登记（以使民众更容易获得当地或国家政府服务）
- 驾照
- 刑事司法记录
- 犯罪侦查
- 闭路电视监控系统监控
- 边境安全/护照签发系统
- 难民援助
- 金融服务
- 计算机系统
- 安全数据库访问
- 场馆访问
- 智能手机访问
- 医疗身份管理
- 工作场所考勤管理

[5] **注**本纲要主要讨论与人类身份相关的身体生物识别特征（人脸、指纹、DNA 等），而非行为。行为生物识别特征包括衡量人类活动方式的模态，如步态、击键和“鼠标”使用特征、手写签名等。

[6] 列表改编自“Biometrics: Personal Identification in Networked Society（生物识别特征：网络社会中的个人身份识别）”（Jain 等人），马萨诸塞州诺威尔：克鲁维尔学术出版社（1999 年）

该等应用程序中使用的模态可以对个人身份进行识别，即使其出示虚假信息或试图冒充他人。这一属性的价值不可估量，在追踪和发现恐怖分子以及破坏恐怖分子的全球活动方面，其可以发挥重要作用。生物识别技术拥有强大和充满活力的商业研发文化，市场中定期会出现新的应用程序以及新模态。

基本生物识别系统（如用于访问控制的生物识别系统）的标准运行模式分为下列阶段：

- *获取和录入* — 使用数据捕获设备获取个人（主体）的生物识别样本。可使用安装在固定、永久地点的设备或可从远处上传数据的移动设备进行采集流程。可通过与数据捕获设备接触，在附近（如在实时捕获人脸图像的情况下）或以远程方式获取生物识别特征（如指纹）。但系统能否取得重大成功，取决于录入的生物识别特征的质量。若录入的特征质量不佳，则系统性能将显著降低，因此，获得一贯高标准的生物特征数据对于提供最佳匹配能力而言十分关键（参见第 2.3.3.节）。
- *数据提取* — 将获取的样本转化为生物特征模板，例如，指纹图像可能被处理成数字化数字阵列，以便进行存储、搜索和对比。因此，数据提取过程旨在将原始图像或原始样本转化为可用、高效的数字化数据组。该数据组可以进行精准查找，可以与数据库中的参考模板进行对比，其在系统中占用的存储空间远远低于原始生物特征图像/样本。
- *数据存储* — 将登记的数据保留在系统或数据库中，有时在搜索/对比阶段结束后，每人仅可使用一种模板。大多数数据捕获设备将数据上传到服务器上或中央数据库中，以便进行搜索，但一些移动设备有自己自带的数据库，因此，可以进行远程部署，而无需连接到任何其他设备。
- *数据对比* — 访问数据库并获取一个或多个以往登记的模板，以将其与当前查询的模板进行对比。
- *数据匹配* — 使用计算算法，以确定查询的模板是否与选择的数据库模板匹配。若查询的模板已与数据库中的参考模板匹配，则一般不会留存。
- *输出* — 查询结果“匹配”或“不匹配”将为整个系统的运行提供支持，例如，如果生物识别要素旨在对确认的数据库中具有访问安全建筑的合法权限的人员的身份进行核实，在结果为“匹配”时，将根据对确认的身份模板进行的核实，允许人员进入，在结果为“不匹配”时，将拒绝进入。

但并非所有应用程序都使用了确认的身份，因为生物识别系统中使用了两种截然不同的流程。流程一中使用了确认的身份，该流程为：

验证 — （亦称一比一或 1:1 对比）。此模板使用已确认的身份，以从数据库或电子文件中选择唯一模板，与查询的模板进行对比。此流程将查询的模板与数据库模板进行对比，得到的结果有两种，即两种模板源自或并非源自同一个人。
在验证过程中将询问问题“您是否与进行身份验证且身份信息已登记到数据库的人士是同一人？”

流程二为搜索模板，该流程为：

身份识别 — （亦称一比多或 1:n 对比）这是一项搜索功能，其并不倚赖于建议的身份，因此查询模板将在整个数据库中进行查询，以进行可能的匹配。搜索和匹配软件将为潜在的匹配生成相似性得

分，并自动选择高可信度匹配或向操作人员显示一份建议匹配候选清单，以便与查询模板进行对比。

在身份识别过程中将询问问题"您的数据是否已录入参考数据库，如果已录入，与您匹配的记录是哪一条？"

验证或身份识别系统的输出值和背景将取决于应用程序的操作模型。例如，在某些情况下，正值的身份识别是常规输出结果，而负值结果是例外（如安全地区的人员访问），但在其他模型中，负值输出是常规结果，正值结果则是例外（如在生物识别恐怖分子观察名单中搜索所有乘客的姓名）。行之有效的生物识别系统将独立的验证和身份识别工作相结合，以增加身份的可信度和参考数据集对比的可靠度。

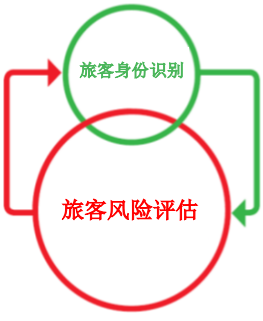
对于用户而言，许多生物识别应用程序从采集到输出的过程似乎都是全自动的，但在更为复杂的系统中，人为干预在相关流程的不同阶段通常都必不可少，这样做是为了确保系统能够无缝运行，尽管这一点对用户而言并非显而易见。但随着计算机功能和新的处理技术的持续、指数式发展，人为干预的必要性正在快速减退，然而，虽然生物特征样本的自动匹配预期将成为常态，在更为复杂的情况下，仍可能根据人类做出的决策，将匹配的样本与其他身份和背景属性相关联。

案例研究 1 — 边境生物识别技术

对照观察名单和情报数据集进行 1:n 对比，在边境通过 1:1 验证对旅客过境进行授权，为旅客风险评估提供信息，并通过旅客风险评估进行通告（参见图 1）。观察名单中记录的身份属性和情报数据集一般不完整。原因是确定纳入观察名单中的目标人物身份所依据的标准不一，且情况不同。并不是所有个人资料或生物识别属性都能够与每份观察名单或情报清单相关联。背景属性不完整。观察名单和情报数据集中的所有属性要素都可能有误。

图 1 — 改编自*"ICAO TRIP Guide on Border Control Management, Montreal (2018)（ICAO TRIP 蒙特利尔边境控制管理指南（2018 年））"*

（获得国际民用航空组织 (ICAO) 许可）



对比	参考数据来源	个人资料对比依据	生物特征对比依据	背景属性的关联
1:1 验证	旅游证件	• 姓名 • 出生日期 • 性别 • 国籍	• 人脸 • 指纹 • 虹膜	• 时间和地点 • 国籍 • 旅游证件检查
1:n 身份识别	- 观察名单 - 情报资料	• 姓名 • 出生日期 • 性别 • 国籍	• 人脸 • 指纹 • 虹膜 • 声音 • DNA	• 时间和地点 • 国际刑警组织失窃与遗失旅行证件 • 先前事件 • 联系属性（手机、电子邮件联系方式等）

通过身份验证，可以更加可靠地与个人资料、生物特征和背景属性相关联，因此可以更加有效地对观察名单和情报数据库进行搜索。重要的一点是，生物特征对比会影响身份匹配的结果，但并非是对该等结果起决定作用的唯一因素。[7]

[7] 请参阅"ICAO TRIP Guide on Border Control Management (2018)（ICAO TRIP 蒙特利尔边境控制管理指南（2018 年））"，

1.1 系统性能

任何生物识别系统的性能在很大程度上都取决于下列因素：(1) 预期用途的范围和规模，(2) 所选用于支持该应用程序的最合适模态，(3) 根据较低维护要求进行的可靠、一致的及时处理。生物识别系统的关键性能指标有准确率、错误率[8]、吞吐量、例外处理量和速率。一般而言，准确率是系统正确地与同一个人的生物识别身份属性相匹配，并且避免与他人的生物识别身份属性进行错误匹配的量度标准。以下要素用于表示生物识别系统的准确率（以百分比或比例形式），相关结果通常来自实地试验或实验室试验。

正确接受率 (TAR) — 衡量系统正确匹配同一个人的生物识别身份属性的能力标准。

错误接受率 (FAR) — 若系统将查询的某位人士的生物识别模板与数据库中另一位人士的生物识别模板进行错误匹配，则发生误识。FAR 指误识的数量在理应拒绝的生物识别查询总数中的占比（即*系统生成并显示为匹配的*不匹配项数量在真正不匹配项中的占比）。

正确拒绝率 (TRR) — 衡量将一名人员的生物识别身份属性与数据库中他人的生物识别身份属性正确地匹配的次数的标准，即正确不匹配的频次。

错误拒绝率 (FRR) — 即使查询的生物识别模板与正确的数据库模板来自同一个人，但是两者仍然不匹配，则出现错误拒绝。FRR 是错误拒绝的数量在理应接受的生物特征查询总数中的占比，即*系统生成并显示为不匹配的*匹配项数量在真正匹配项中的占比。

因此，可以在设计系统时，将 TAR 和 TRR 值最大化，将 FAR 和 FRR 值最小化。简单举例而言，如果将准确率 TAR 设置为 70%，则将得到 30% 的 FAR，而如果将 TAR 设置为 97%，则意味着 FAR 只有 3%。应注意，没有任何生物识别系统能够以 100% 的准确率运行。

而 FAR 和 FRR 值也存在密切的关系，这两个错误率之间的最佳平衡点在很大程度上取决于特定生物识别系统的商业用途。例如，若员工进入公司场所与生物识别应用程序相关联，则设置较高的 FRR 会阻止公司人员常规进入，而若将 FAR 设置得过高，则未经授权的人员可能会以常规方式进入。因此，该应用程序要求允许对使 FRR 和 FAR 维持平衡的临界值进行调整，以允许相关人员无障碍地访问，同时使*大部分*未获授权的人员无法进入。如果需要提高安全级别，则需要通过尽量降低 FAR 值，对临界值进行重新调整，以防未经授权的人员访问，哪怕这样做会使 FRR 升高，进而影响合法人员的访问。因此，该临界值通常是 FRR 和 FAR 之间实用的折中方案，该方案提高了系统就拟定用途而言的有效性，且对安全性需求与客户便利程度以及处理速度和系统总成本进行了权衡。等错误率 (EER) [9]指在 FRR 和 FAR 相等，即错误接受比例等于错误拒绝比例的情况下，为某些模态设置的临界值。

获取更多详情

[8] 错误率的计算要求进行抽象化处理，即对闭集进行数值假定，以便随后完成数据库的所有对比，以得出并计算错误率。在许多情况下，这些计算都是在模拟的情境下，使用可能代表或并不代表实际实时数据的标准化数据集进行的。错误率抽象化处理在进行系统设计和 1:1 验证表现预测时十分有用。在现实世界中，全球人口超过 70 亿人，从数据集之外进行替换是有可能实现的，其预计会在提供观察名单和情报数据集的情况下发生。使用错误率时务必谨慎，只能在进行验证时使用。生物识别系统的实际匹配性能可能与错误率模拟中的预测值相差极大。

[9] 亦称交越错误率

还有其他一些影响准确性的因素，如错误采集率 (FTA)。该比率一般指因呈现（如无捕获的图像）、特征提取或质量控制阶段出现的故障，而无法完成的所有记录交易的比例。除系统故障外，还包括个人生物特征受损、受伤或缺失的情况。FTA 是系统实施操作能力的重要衡量标准。若 FTA 值较高，则要求采用替代方法，以捕获由于任何原因无法进行登记的人员的生物特征。这可能还要求使用类似的替代性生物特征，如使用左手拇指替代右手拇指，或者甚至要求添加第二个不同的生物特征识别功能，此项功能要求开发多模式系统。如果这些替代方案不可行，则将采用例外处理这一非生物识别解决方案。例如，对于无法进行生物特征登录的人员，此流程可能要求操作人员对其身份进行核验或使用其他安全系数可能较低的方法（如 PIN 码或书面签名）。上述方法均可能会使系统的整体有效性降低。正因如此，多模式应用程序通常才受到青睐。原因是它可以使登记数量的占比增加，同时降低 FTA。

吞吐率决定了在特定时间范围内可以访问系统的人数，即容量对比速度。例如，设有生物特征电子护照入口的机场需要计算当前和预计的客流量，以安装足够数量的生物识别闸门，以在人流高峰期，促进乘客的有效流动。这使生物识别系统能够在预先确定的错误率范围内运行（出于安全方面的原因），同时在几秒钟内同时处理多个验证，以满足客户需求，提高经营效率。

1.2 生物识别技术在法医学方面的作用

法医学一般处理人、物体和位置之间的实际资料或电子、数字媒介的转移。该等资料可能可见（如墙上的血迹），也可能不可见（如枪声、爆炸残留物或电子图像（如闭路电视摄像机拍摄的人脸）等微观痕迹证据）该等资料或数据可以在作出犯罪行为之前、期间或之后被转移。其中一些资料还可以捕获*生物*特征，如印在在玻璃杯上的沾有汗水的指纹、电话通话时录下的声音或根据杯子边缘处的唾液生成的 DNA 图谱。该等"法医生物识别特征"[10]由于具有识别个人的潜在功能，而成为法医学的关键要素以及执法调查过程中的重要元素。其对于有效及成功开展反恐行动而言，同样至关重要，其通过以下方式，促进反恐行动的有效及成功开展：

- 通过由本人或在其他证据中提供有罪或无罪证明，证明某人参与或未参与犯罪行为（参见案例研究 2）。
- 根据法律规则提供客观、可靠的程序，以减少在刑事调查中对口供的依赖（如果这些口供是通过使用酷刑或其他胁迫性手段获得则更为重要）。
- 犯罪现场和相关事件中的口译活动
- 在事件发生之前、期间或之后，将个人与活动、事件、地点或他人相关联
- 将一个事件与其他一个或多个事件相关联
- 在不同电子和数字系统中查找数据并进行数据关联

若要发挥这些功能，则需要法医学其他相关学科以及专门技术和实验室专业领域的人员作出协同努力。[11]应根据国际标准和相关质量管理体系在犯罪现场及在实验室进行所有法医学资料的处理（参见第 2.4.2. 节）。法医学的主要学科如下：

- 生物证据 — 脱氧核糖核酸 (DNA)、体液、头发、组织等
- 印迹 — 指纹和掌纹、仪器印迹、鞋印、轮胎印迹等
- 火器和弹道学
- 痕量证据 — 油漆、玻璃、纤维、爆炸物等
- 数字和电子证据 — 设备访问、数据下载、分析、损害重建等
- 毒品 — 识别和量化
- 文献分析
- 爆炸物分析

将在案例研究中使用法医生物特征资料，进行一对一的对比（例如，将从犯罪现场获取的指纹与从嫌疑人处获得的一组指纹进行对比），该等资料构成法医科学家使用的下列三种主要类别数据库中的一种：[12]

[10] Forensic Biometrics: from two communities to one discipline（法医生物识别特征：从两个社区到一个学科）.Proceedings of the International Conference of the Biometrics Special Interest Group（生物特征特别兴趣小组国际会议论文集）（2012 年 9 月 6 日至 7 日）；德国达姆施塔特。

[11] 联合国毒品和犯罪问题办公室 (UNODC) 发布了下列两本出版物，其对大部分学科进行了详细载述："Police: Forensic services and infrastructure（警察机关：法医服务和基础设施）"和"Staff skill requirements and equipment recommendations for forensic science laboratories（法医学实验室员工的技能要求和设备推荐）"(www.unodc.org)

[12] 法医情报数据库通常由法医科学家在法医学实验室内进行管理和操作，但某些生物特征数据库（如指纹、DNA、语音和面部系统）可能会在执法环境中由其他人员进行操作。

1. *案例研究资料参考数据库*，如天然和人造纤维集合库，数据通常来自制造商和零售店，将使用该等数据库对犯罪现场提交的纤维进行识别、分类及对比分析
2. *非生物特征研究数据库* — 如武器和发射弹药、鞋印等
3. *生物特征研究数据库* — 人类生物资料和特征（如 DNA 和指纹）的集合库。

在法医学和调查范围背景下处理生物特征样本时，必须遵循法医证据处理的基本原则，否则任何生物特征搜索系统产生的结果均在随后的司法程序中失去价值。因此，从犯罪现场回收每件样本/物品时，必须使用以下记录和程序：

- *出处* — 样本/物品位置的书面和照片记录
- *保存* — 获取和包装法医样品/物品过程中，须确保证据不会被污染、损毁、更改、或遗失或质量降低；包装还必须为样品提供保护，以免其在运输过程中损坏，且应防止其污染其他物品或环境或被其他物品或环境污染；样品应在适当的温度下存放且应确保其达到最佳的测试条件以便进行实验室分析
- *完整性* — 包装必须牢固、完整，且须进行有效封口，以防未经授权的使用或干扰；不得在包装过程中添加或移除材料（包括微粒，气体或液体）
- *连续性（监管链）* — 从在犯罪现场开始，必须一直对保管包装好的样品/物品的每位人员保存记录

案例研究 2 — 清白专案

清白专案由美国纽约本杰明·卡多佐法学院的 Paul Neufeld 和 Barry Sheck 在 1992 年建立。成立该组织的目的是利用法医 DNA 图谱分析为被错误定罪的人洗清罪责，并对美国刑事司法体系进行改革，以防未来继续出现不公正的行为。这一想法依据的原则是如果 DNA 技术可以证明人们有罪，其同样可以证明被错误定罪的人无罪。迄今为止，DNA 检查已为 356 人洗清罪责，并对 153 名潜在的罪犯替代者进行身份鉴定。

1.2.1 法医学生物特征数据库：数据类别

法医学生物特征数据库，亦称法医情报数据库，通常供法医学实验室和执法机构使用。100 多年来，这些数据库对许多国家的犯罪调查，尤其是恐怖主义案件，都产生了重大影响。常用的模态包括指纹、DNA、人脸和声音。每个数据库都由两个不同的数据集组成：

参考数据 — 在受控的条件下，从因犯罪而被捕或涉嫌犯罪的人员采集，如使用扫描仪以电子方式或使用墨水和纸张以传统方式采集的双手 10 根手指的指纹；从被捕者的脸颊、头发或血样内采集的经处理后，可形成完整 DNA 图谱的口腔拭子[13]；面部数码照片等。还可以在作出犯罪行为之前、期间或之后，从警察或有访问犯罪现场合法权限的人员处获取参考数据，以对其留存的任何法医资料进行识别并将其从调查中剔除。

[13] 采用现代 DNA 技术，目前可以在一个小时内，使用实验室或警察局/边境哨所的全自动设备对从人身上采集的 DNA 口腔拭子进行快速图谱分析。这意味着可以进行 DNA 数据库搜索，以在该人员被扣留或拘留期间确定是否存在与犯罪现场样本匹配的 DNA。

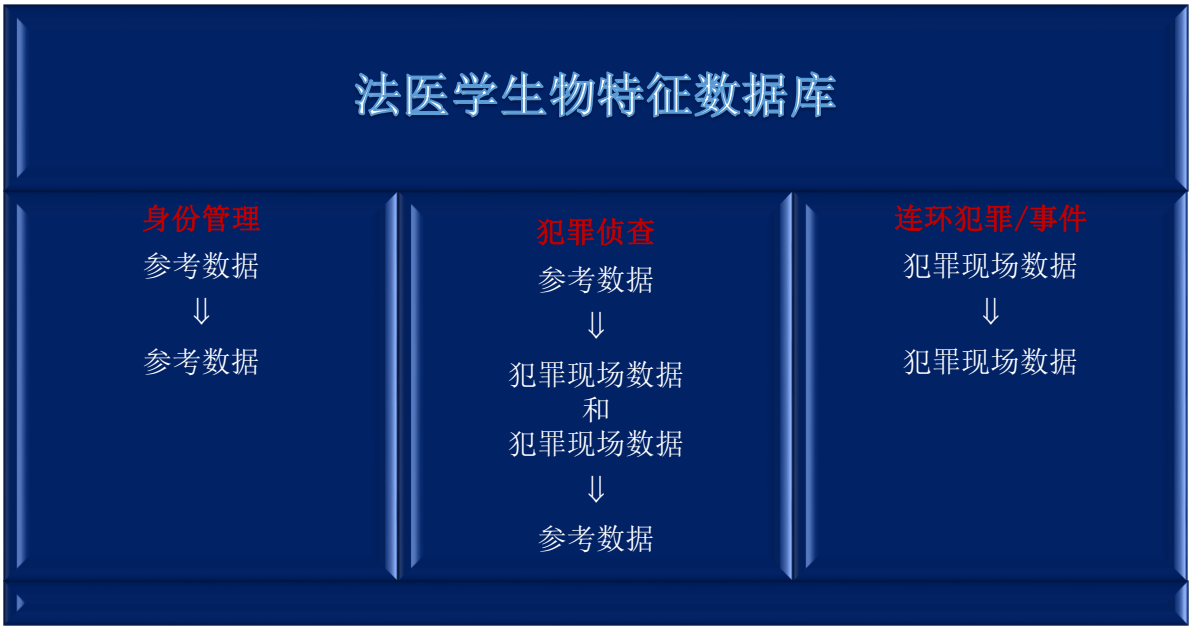
犯罪现场数据 — 根据从犯罪现场获取的样本和物品生成。[14]犯罪现场的生物特征数据的质量参差不齐。回收的法医资料可能因各种原因被损坏、污染或在内容上有缺失或在细节方面不够清晰。这使得搜索和对比过程中产生的结果的范围更加宽泛。该等结果有别其他“非法医”生物识别系统，如访问控制应用程序产生的两种常规结果 —“匹配”和“不匹配”。

一些国家还使用大型生物识别系统，为其公民的民事登记（如身份证计划）提供支持。这为每一名公民提供了正式的身份，并使其获得政府服务及其他社会和商业设施，如福利、住房、保险和银行业务等。

民事登记系统 — 该等系统中使用的模态通常有指纹、人脸或虹膜或多种模态的组合。该等数据库中可能包含数以百万计、数以千万计或数以亿计的生物特征模板（参考数据），具体数目取决于国家人口规模。这些数据旨在用于搜索参考数据。因此，如果法律和监管体系允许执法机构为犯罪调查之目的在该等数据中搜索，则一般只能搜索参考数据。可搜索从某人采集的一系列指纹或人脸图像，以确认其是否在系统中注册，但若搜索的是从犯罪现场采集的指纹或人脸图像，则不太可能产生匹配。这是因为民事登记系统的匹配算法处理犯罪现场数据的方法一般不同于法医学实验室中的法医搜索系统。正因如此，民事生物特征数据库才很少用于犯罪调查，即使在发生严重罪行和恐怖主义行为的情况下，用该数据库进行搜索，成功率通常也极低。但在某些模态（如人脸）领域出现的新技术和数据来源或许会使未来的搜索结果更加准确。还可以选择将法医匹配软件内置或附加到该等民事登记系统中。

1.2.2 法医学生物特征数据库：搜索类别

图 2 — 法医学生物特征数据库 — 搜索排列



有四种基本的法医搜索排列方式，可用于为执法和刑事调查提供支持，这些排列方式通过以下三种搜索配置进行提交（参见图 2）：

[14] 在这里，“犯罪现场”一词的应用范围扩至最大，包括物理位置、嫌疑人、受害人、证人以及数字和电子环境。

身份管理搜索 *排列 1* — 参考数据到参考数据

可通过此类搜索，对数据库中提交的所有参考数据进行主体参考数据搜索，从而确定其是否已在数据库中登记。该项技术通常用于确认某名人士是否是警察熟识并且有犯罪前科和犯罪记录的人，尤其用于此人提供虚假信息的情况。以往，指纹被用于此目的。从被捕人采集一整套十指滚动按压[15]指纹（“十指指纹”），并在已知罪犯的十指指纹数据库中进行搜索。如在数据库中含有高质量指纹图像（即所有指纹的质量均有保证且由受训的操作人员在受控条件下进行采集）的现代、高效的自动指纹识别系统 (AFIS) 中进行搜索，则搜索结果十分准确（即 TAR 极高 — 参见第 1.1 节）。该等搜索通常在“熄灯”模式下进行，即除非需要对匹配进行验证，否则很少或不需要人为干涉。这意味着该等搜索的处理速度非常快。现代移动数据捕获设备使执法人员能够在很远的地方以及边境过境处采集相关人员的指纹和掌纹，并向中央服务器发送数据，以便进行即时搜索。一般会在几秒钟或几分钟内收到结果。一些移动设备有独立的数据库，以便在本地运行所有搜索功能，而无需将数据传输到远程服务器上。

当然，还可以使用其他生物识别模态，如 DNA、人脸、虹膜等进行身份管理。还可以使用身份管理搜索，对死者或患失忆症的人进行识别。获得一致标准的高质量的参考数据，以使所有搜索配置发挥最大潜能，是一项为所有生物特征搜索奠定基础的关键要求。质量欠佳的参考资料会影响所有搜索排列的有效性和准确性。[16]

进行身份管理搜索时，会询问一个问题：“我们之前是否遇到过您，您是谁？”

犯罪侦查搜索：*排列 2* — 参考数据到犯罪现场数据和*排列 3* — 犯罪现场数据到参考数据

此搜索协议要求在参考数据库和含有从犯罪现场采集的法医生物识别资料，如犯罪现场污迹 DNA（研究中的样本）、指纹和掌纹、人脸图像等的犯罪现场数据库之间建立双向接口。新登记的参考数据，如果在参考数据库中未有记录，则可在犯罪现场数据库中进行搜索，反之，新登记的犯罪现场数据可在参考数据库中进行搜索。该等类型的搜索的准确性可能比身份管理搜索要低得多，因为犯罪现场数据的质量参差不齐。

在犯罪侦查搜索中，会询问这一问题：“您是否犯有罪行？”“您是否与该物体/地点有关联？”以及“您是否与其他人在一起”

连环犯罪/事件：*排列 4* — 犯罪现场数据到犯罪现场数据

此类型的搜索可以对不同地点的犯罪现场资料进行识别并将其捆绑在一起，并向该等案件的调查人员提供情报线索，从而将不同罪行的犯罪现场或单个重要调查中可能出现的犯罪现场联系起来。在犯罪现场留下材料的人员身份未知，但确定相同人员在两起或更多罪行或事件中留下生物识别材料

[15] 在扫描仪压盘或指纹表格上将每根手指的指尖从指甲的一个边缘滚动到另一个边缘，以记录尽可能详细的指纹纹路流向和特征。其他指纹按压方式称为“平压”或“多指按压”。这些指纹是通过将手指直接向下按压到压盘/表格上，同时（两根手指同时，每只手的四根手指）采集的。平压法是一种质量保证措施，可确保以正确的顺序将滚动按压的指纹录入。

[16] 因此，将对英国因恐怖主义相关罪行被捕的所有人员采集至少三套指纹和掌纹，此过程在指纹专家的监督下进行。每套指纹包含手上的摩擦嵴细节处的所有区域，即标准滚动按压和平压指纹、指尖、所有指骨的滚动压纹、手掌完整表面和手部尺侧（书写时手掌接触纸张的区域）以及足底纹（脚底和脚趾）。这一过程专注细节，可产生一套最佳参考指纹，供 AFIS 搜索和存档之用，同时，还提供最大的可用摩擦嵴细节数据集，以便与犯罪现场采集的指纹/掌纹/脚底纹，尤其是脚趾、手指侧面或手掌任何区域的纹路进行 1:1 对比。

，对调查人员和情报分析人员起到的帮助作用不可估量。此类搜索是否成功、结果是够准确在很大程度上取决于犯罪现场数据以及从犯罪现场获取的兼容资料的质量。一些模态比其他模态更适合使用此类搜索，例如，在许多不同类型的调查（如恐怖主义、凶杀和性犯罪）中，DNA 在进行罪行/事件联系方面特别有效。

在进行连环犯罪搜索时，将询问这一问题："该等犯罪现场数据是否与其他罪行/事件的犯罪现场数据相匹配？"

注 本节介绍的数据库的错误拒绝率各不相同，该数值的高低取决于数据库中生物特征数据的类型和质量。与其他生物识别系统相同、不匹配或负值结果（即匹配时未得到 1:n 的搜索结果）并不一定意味着数据库中未收录匹配数据，而是系统可能由于各种原因未能找到相关数据。

DNA[17] — 其他搜索类别

还有一些专为其他 DNA 样本研发的专门搜索技术。DNA 参考图谱由 DNA 非编码区生成，由于含有其他基因信息极少，仅作识别之用。从犯罪现场采集的研究中的 DNA 样本通常含有更多基因资料，其他 DNA 提取物和图谱分析技术也可为调查人员提供帮助。但该等技术通常须要在负责法医学法律和道德监控的人员的密切监督下实施，因为如果不对该等技术进行严格管制，其可能会侵犯隐私和数据保护法。一些示例包括：

表现型评估 — 一种在犯罪现场留下的污迹中寻找特定基因物理特征（如红头发或眼睛颜色）的技术。尽管此过程目前存在极大限制，但 DNA 科学方面的进展将来无疑会使表型特征的范围扩大。这使得调查人员可以从犯罪现场遗留的污迹的 DNA 中获知已知嫌疑人的更多详细"描述"。

家族（亲缘）搜索 — 在刑事 DNA 参考数据库中进行搜索时，可能无法对由犯罪现场的污迹生成的 DNA 图谱进行识别。在例外情况下，可使用其他专业软件在同一数据库中对此图谱进行搜索，以确定该图谱是否与信息已可能已在系统归档中的任何近亲或血亲的图谱极为类似。这样做可能会产生相对较少或数以千计的答案，具体情况取决于与数据库人口的整体基因图谱相比，查询的 DNA 图谱的相对稀有程度。

1.2.3 法医学生物特征数据库 — 限制和报告标准

法医资料通常会在准备实施或实施罪行期间无意存入或记录，且可能受到一系列有害的条件和限制性因素的影响，该等条件和限制性因素会使其无法在生物识别搜索系统中与参考数据得到同样有效的利用。这些条件中有一些是通用的，许多条件则根据样本模态进行选用。一些经常遇到的示例如下：

人脸 — 闭路电视监控系统和其他外部视觉记录技术

- *相机视角兼容性* — 在采用正面拍摄及与脸部保持统一水平线的方式对在押人员进行"正面照片"采集的时候，闭路电视摄像机通常放在较高的位置。因此，很难对两种类型的图像进

[17] 另请参见"DNA Database management review and recommendations, 2017（2017 年 DNA 数据库管理审查和建议）"，ENSFI DNA 工作小组，2017 年 4 月 http://enfsi.eu/wp-content/uploads/2017/09/DNA-databasemanagement-review-and-recommendatations-april-2017.pdf

行精确对比，有时候，这甚至不可能。

- *照明和曝光* — 能否获得最佳图像相机传感器取决于 (a) 环境中提供的整体照明条件和 (b) 快门速度、光圈和 ISO 等的设置。
- *相机分辨率* — 一些相机的分辨率较低，即其只能记录有限像素数，如果相机离拍摄物体有一段距离，获得的图像通常是粗糙、模糊的，在环境光线不佳的情况下尤其如此。所获得图像较少可用的细节，即使将其放大仍无法使用。
- *压缩* — 相机的数据记录组件会删除微小的细节，以增强其存储低清晰度图像的功能
- *面部特征和遮盖物* — 年龄、表情或面部特征等不明显的因素可能会对识别面部以及外部障碍物（如眼镜、面部毛发、帽子、头盔等）的能力构成影响（参见第 2.3.2.节）。

指纹或掌纹（亦称“潜在”纹路或“潜在纹”）：

- *充分性和暴露区* — 手指或手掌只有很小的区域会和表面接触，因此，只显示出相对较少的特征详情。若采集的参考指纹质量不佳，则可能会使这一问题复杂化，因为其可能无法显示出这一小范围的手指区域，进而与相关指纹进行对比。
- *叠印* — 两个或多个指纹存在于同一位置，在此表面上，难以从视觉上将一个指纹与另一个指纹区分。
- *干预* — 底层的背景干扰可能会使部分或全部指纹变得模糊。指纹一般会在存储于非多孔基材后显示在表面，或被吸收到多孔基材的表面。因此，表面处的指纹可能会受到损坏或者会受到环境破坏的影响。灰尘、污染物或其他人工制品也可能会使指纹中的特征详情变得模糊或损坏。
- *压力* — 与表面接触时，手指可能受到垂直或侧向压力的影响，造成指纹因皮肤弹性而扭曲变形。
- *移动* — 与表面接触时，手指可能会滑向一侧，造成指纹脏污或（在某些情况下）扭曲变形并叠在一起。
- *显现技术的局限性* — 使用指纹显现粉末或化学处理方法可能无法在图像中清楚显示所有纹路，得到的图像不是过浅就是过深，对比不足。

DNA — 从犯罪现场收集的生物和细胞资料（亦称“犯罪现场污迹”）：

- *数量和质量* — 与指纹一样，犯罪现场的 DNA 的数量和质量也参差不齐，因此，一些 DNA 匹配被归类为“部分”，而非“全部”匹配。在提供的 DNA 资料不足或质量不佳，无法生成完整 DNA 图谱的情况下会发生这一情况。在该等情况下，须对匹配概率比或似然比作出相应调整，以反映不确定程度。
- *混合图谱* — 采集自多个提供者的 DNA 可能会被存放在同一位置，得到的图谱可能包含两名或多名人士的混合结果。法医科学家使用统计分析对相关结果进行阐释，如若可能，将为分离各提供者的 DNA 及进行相关图谱分析提供协助混合图谱中的个人图谱的质量同样不统一。
- *出处* — 使用现代 DNA 实验室技术，生成少量细胞 DNA 的图谱。但由于科学家目前正在处理这些少量样本，并未始终可以确定在犯罪现场发现的 DNA 的出处（如来自特定体液）。
- *污染* — DNA 样本检测和图谱分析的能力极低，因此，相关资料在本质上是有流动性的，

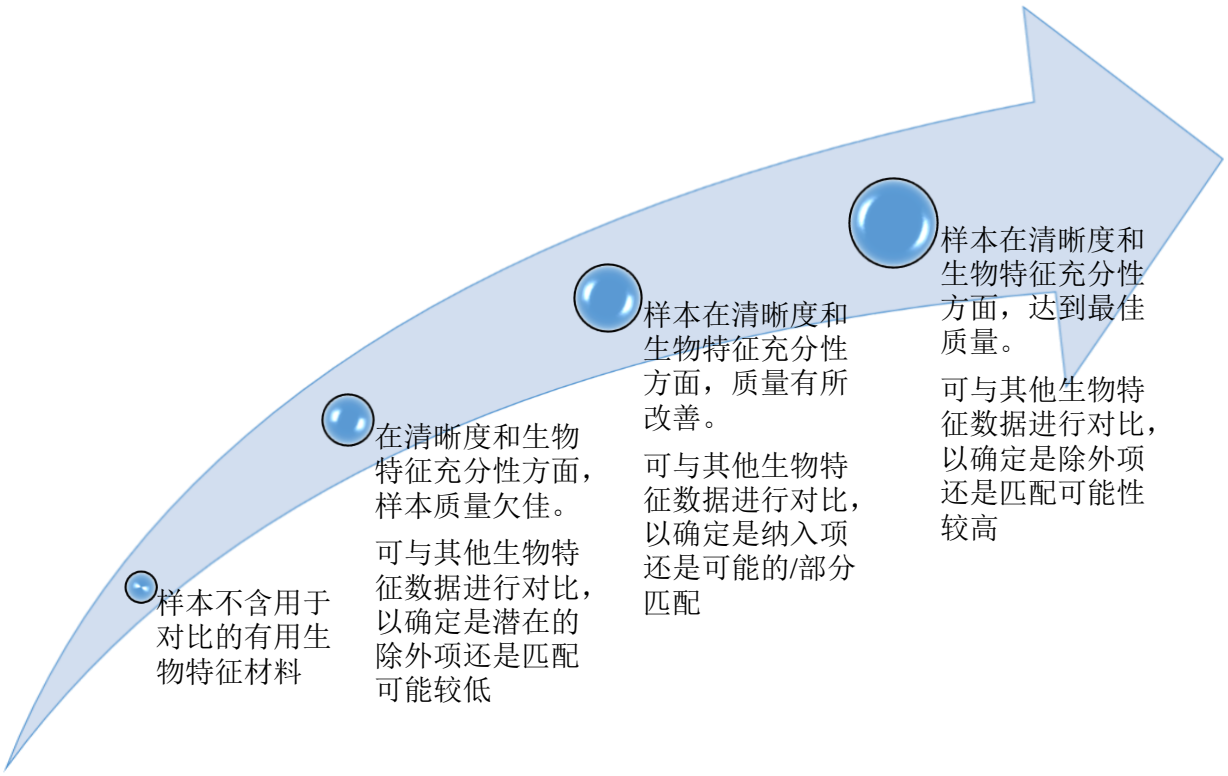
即可以在人、物品和地点之间转移。需要在犯罪现场和实验室采取一系列防护措施，以防因警察或法医科学家的相关操作，使 DNA 不慎转移（参见第 2.3 节）。

- *环境破坏* — 如果长时间暴露在不利的环境条件，如极端温度、湿度和污染物条件下，DNA 可能被破坏、质量下降或发生性质改变。

因此，从犯罪现场获取的生物特征材料的质量逐渐提高，从无价值（即无法提取出生物特征或数据）变为高价值（即生物特征资料可提供充分数量和清晰度的特征，以便能够与其他生物特征数据进行对比并提高匹配的可能性）。对比中使用的其他生物特征数据（无论是参考样本还是犯罪现场样本）的相对质量对该流程而言同样十分关键。能否在对比过程中获得任何程度的匹配与两种样本的质量有直接关系。正因如此，从个人采集的与恐怖主义罪行相关的生物特征参考数据必须符合可能的最高标准。

图 3 从生物特征样本质量和从低匹配到高匹配可能性的相应匹配度方面描绘了此变化的代表性阶段。在对比结果显示两个生物特征样本并非由同一人产生时，使用低质量的生物特征，更容易确认除外项，而非纳入项（即匹配），但如果质量过低，两个过程都变得具有挑战性，对比的结果可能无法确定。

图 3 — 犯罪现场生物特征数据 — 生物特征样本质量和匹配可能性的关系



数据库登记标准 — 质量欠佳的生物特征数据通常缺乏充分的区分性搜索功能，这意味着，数据在存入系统（如 AFIS）后，可能会不断以不相称的方式对即将进行的搜索作出回应，这最终可能会影响系统的有效性。之所以会这样是因为系统以分层候选列表形式显示出潜在生物特征匹配，且通常

会对响应预先设置编号（如可能性排名前十的匹配）。将由操作人员确定其中任何条目是否是实际匹配项。系统中存入的任何质量不佳的数据可能会将真实匹配项挤出名单。因此，在确定对生物识别样本进行登记时，必须在各样本的证明、操作和情报价值和其技术或科学质量之间进行权衡（参见第 2.4.2. 节）。在数据库网络中，该等质量欠佳的生物特征数据的登记临界值必须符合最低集体标准，以确保在网络中进行平稳、顺利的操作，防止合作方进行可能影响搜索效率的数据登记。

犯罪现场生物特征数据质量变化的直接结果是，法医科学家、指纹鉴定者和处理法医资料的其他人员研究出了各种不同方法，将其对比的一系列结果呈现给调查人员、情报分析人员或法庭。该等方法大致包括：

- “贝叶斯”逻辑概率和检测推断的统计推断，包括构成 DNA 图谱对比基础的概率比。注：一些法庭和国家司法管辖区不接受该等统计方法的某些变化[18]
- 语言等值量表，如现代指纹对比和许多其他法医学学科
- “绝对”结论，如传统指纹对比

这意味着各国或者甚至各司法管辖区的*相同模态*法医报告方法均可能因相关科学、司法、监管和法律规定有所不同。这反过来会影响各数据库的登记标准以及生成的结果的类型。

研究案例 3 — 传统指纹标准

一些国家仍然在指纹鉴定时使用“绝对”方法，即一套基于二元决策程序（即匹配或不匹配）的传统系统，且要求预先确定嵴纹特征（生物特征）的最少数目，以对匹配进行确认并在法庭上出示证据。在某些司法管辖区，此标准被写入司法立法中。因此，如果指纹或指印对比的嵴纹特征数目低于公认标准，则不能作为证据而出示。对于在司法系统中采用完全披露原则的司法管辖区而言，难度显然上升了，因为法庭可能会要求专家对法庭感兴趣、但专家认为低于公认标准门槛而无法在法庭出示的指纹对比（如其可能会对相关案件产生重大影响或与被告的案情有特别关联）发表意见。为克服这些限制，近几十年来，其他国家已研究出并已采用了非数字的整体方法，该方法不在嵴纹特征的最低数目方面作出要求，而在严格按顺序进行的系统评估中从三个不同的层面研究摩擦嵴详情。[19]可用此方法，选用下列四种方式之一：鉴定、排除、非充分或非确定详情 — 或等效术语，对*任何*指纹对比的结果进行报告，因此，可用此方法，表达与其他现代法医学学科相符的“不确定”程度。因此，在进行指纹数据的国际交换时，必须考虑到在对该等模态进行科学报告时作出的相关变更。

过去十年，围绕此话题进行了许多国际讨论和研究，因为许多司法管辖区都希望运用单一的方法进行科学结果的展示，该方法涉及传统法医学学科及与数字和电子技术相关的法医检查。已提出各种方案，但尚未商定出最后的模式，此问题在国际上仍然存在争议。恐怖主义使全球面临威胁，因此，处理生物特征数据和搜索结果的人员务必完全熟悉其所在国家和国际数据分享合作方的法医学报告标准。采取任何行动前，确保根据东道主国家的法医分析协议和报告标准进行匹配，从而对其他

[18] 参见 Bernard Robertson 和 G.A. Vignaux 撰写的“Interpreting Evidence: Evaluating Forensic Science in the Courtroom（解释证据：在法庭评估法医学）” (Wiley ISBN 0471 96026 8)、David Lucy 撰写的“Introduction to Statistics for Forensic Scientists（法医科学家统计学导论）”(Wiley ISBN 0-470-02200-0)，以及美国国家科学院国家研究委员会撰写的“Strengthening Forensic Science in the United States: A Path Forward（加强美国的法医学：前进之路）”（国家学术出版社 ISBN-13：978-0-309-13135-3），获取与此主题相关的更多信息。

[19] 此方法称为 ACE-V，即 Assessment（评估）、Comparison（对比）、Evaluation（评价）和 Verification（验证）。

合作国家/司法管辖区生成的任何结果进行独立验证，也是不错的方法（参见第 3.3.3. 节）。

1.2.4 科学解释：身份和活动

这是区分标准商业生物识别应用程序（如建筑生物特征访问系统）和法医学生物特征数据库的另一个重要因素。二者均可通过 1:1 或 1:n 搜索对个人身份进行识别，但法医应用程序在犯罪现场数据方面具有重要的附加功能，不但能提供活动证明，还能提供身份证明。可对法医学证据的地点、位置、分布和方向进行科学解释，以提供有关事件发生期间的事件发生事件和顺序以及所涉人员活动的额外信息。这一额外背景相关证据显然增加了犯罪现场资料的证明价值，且处理法医学生物特征数据库输出结果的调查人员或分析人员必须完全理解并考虑此证据（参见第 3.3.3. 节）。

注：可以采用与生物特征数据类似的方法，对边境管理流程（参见第 3.1.1. 节）中收集的个人资料和相关数据进行使用，以提供活动和身份证明。*此过程对使用和分享犯罪现场和边境生物特征数据，以预测、追踪和破坏恐怖主义活动所产生的效果进行阐释*（参见第 3.3.2.1. 节）。

1.3 推荐实践

a) 鼓励各国采用生物识别系统或加大该系统的使用力度，以对个人的身份进行认证，并防止其提供错误的信息，或试图冒充他人。

b) 设计生物识别系统，并在准确性、安全性、用户访问量、吞吐量和运行可靠度方面对系统进行调整，以使其符合特定商业需求。因此，各国应在投入资金开发新生物识别应用程序前，仔细评估其用例要求。

c) 可通过将生物特征身份管理流程与法医学生物特征数据库相结合，强化生物特征身份管理流程，以建立有效的全国性调查和情报框架，打击恐怖主义行为和相关犯罪活动。

d) 国际法医学报告标准和方法发生了一些变更。因此，建议对处理法医学生物特征数据库输出结果的所有人员进行培训，以使其了解相关结果的相对价值和潜在限制。

1.3.1 参考文件

Identity verification- The importance of context and continuity of identity（身份验证 — 背景和身份持续性的重要性），第 11 至 16 页，Keesing Journal of Documents & Identity（Keesing 档案与身份期刊），Annual Report Identity Management 2011-2012（2011 至 2012 年身份管理年报）

1995 年，美国政府生物识别联盟将“生物识别技术”定义为“……根据个人行为和生物特征对个人进行的自动识别。”

Biometric Recognition: Challenges and Opportunities（生物特征识别：挑战与机遇），第 1 页，National Research Council（国家研究委员会），华盛顿（2010 年），下载地址：http://www.nap.edu/openbook.php?record_id=12720&page=1

“Biometrics: Personal Identification in Networked Society（生物识别特征：网络社会中的个人身份识别）”（Jain 等人），马萨诸塞州诺威尔：克鲁维尔学术出版社（1999 年）

Understanding Biometrics Guide（了解生物识别技术指南）（工作副本） — 生物识别学会 *www.biometricsinstitute.org*

PAS 92:2011 Code of Practice for the implementation of a biometric system（PAS 92:2011 生物识别系统的操作规范）— 英国标准学会 www.bsigroup.com

联合国毒品和犯罪问题办公室 (UNODC) "Police: Forensic services and infrastructure（警察机关：法医服务和基础设施）"和"Staff skill requirements and equipment recommendations for forensic science laboratories（法医学实验室员工的技能要求和设备推荐）"www.unodc.org

英国法医学监管机构年报 2016 年 11 月至 2017 年 11 月 — Gillian Tully 博士

DNA Database management review and recommendations, 2017（2017 年 DNA 数据库管理审查和建议），ENSFI DNA 工作小组，2017 年 4 月"http://enfsi.eu/wp-content/uploads/2017/09/DNA-databasemanagement-review-and-recommendatations-april-2017.pdf

Forensic DNA Typing: Biology, Technology and Genetics of STR Markers（法医 DNA 分型：短串联重复序列标记的生物学、技术和遗传学）— John M. Butler。出版社：爱思唯尔学术出版社 ISBN-13: 978-0-12-147952-7

Interpreting Evidence: Evaluating Forensic Science in the Courtroom（解释证据：在法庭评估法医学）— Bernard Robertson 和 G.A.Vignaux。出版社：约翰威立 ISBN 0471 96026 8

Introduction to Statistics for Forensic Scientists（法医科学家统计学导论）— David Lucy 出版社：约翰威立 ISBN 0-470-02200-0

Strengthening Forensic Science in the United States: A Path Forward（加强美国的法医学：前进之路），美国国家科学院国家研究委员会。出版社：国家学术出版社 ISBN-13: 978-0-309-13135-3。

2. 治理和法规

为清楚和一致性起见，以下治理和监管章节适用于本纲要所有章节，且应视为适用于当前版本的纲要中陈述和解释的所有做法、措施和建议。

第 2 节从国际法、人权法、伦理审查、数据保护要求和隐私权的角度介绍了生物识别技术的治理和监管要求。随后，对生物识别系统和一些可以用来降低风险的控制措施的潜在漏洞进行了概述。接着，探讨了国际技术和科学操作标准，包括生物识别应用程序的认证和鉴定以及用于相关法医学流程的质量管理系统。该章节最后一部分讨论了反恐生物识别系统或网络的获得、维护和资源要求，尤其对评估未来的新系统或扩展系统时需要进行的关键操作和财务决策进行了介绍。

2.1 包括人权法在内的国际法

各国有义务保护其司法管辖区内人士的安全，防止其受到恐怖袭击，且须在遵守人权要求的同时将此类行为的实施者绳之以法。联合国安全理事会和联合国大会强调，各国必须确保采取的旨在打击恐怖主义的任何措施符合其在国际法，尤其是国际人权法、难民法和人道主义法下的所有义务。遵守人权和法律规则是有效的发恐措施的补充，且是反恐工作成功的必要条件[20]。

不同成员国的人权适用范围确实不同。一些成员国并未签署某些全球人权文书，许多成员国签署了地区性的人权文书[21]，该等文书在某些方面有所区别。在将国际人权法标准纳入国内法律方面，各国的情况而有所不同。此外，一些成员国在批准或加入时引入了保留意见和声明，因此将其承诺限制在特定条约义务上。

联合国安理会在其第 2396 (2017) 号决议中号召成员国对疑似的外国恐怖分子即其随性的家人（包括配偶和孩子）进行评估和调查，并为这些人员拟定和实施综合风险评估方案。开发生物特征数据收集系统时，有必要制定与数据保护和人权标准相关的保障措施，[22]同时特别注意需要确保以负责任的方式使用和共享为收集和记录有关儿童的信息（包括生物统计数据）而开发的任何系统，从而根据国内和国际法充分保护儿童的人权，特别包括《联合国儿童权利公约》(CRC)（1989 年）所列的要求。

符合人权要求的生物识别技术使用

各成员国越来越频繁地将生物识别技术用作重要的反恐工具。声音识别、虹膜扫描、人脸识别、指纹、DNA、全身扫描和个人步态仅是正在开发和运用的用于反恐的众多数字技术中的几个例子。该等技术措施带来了与成员国的反恐工作及其人权义务履行有关的在法律和政策方面错综复杂的挑战。虽然生物识别系统是对恐怖分子嫌疑人进行身份鉴定的合法工具，但该项技术的范围扩大和迅速发展更值得关注，因为其与人权（包括但不限于隐私权）保护相关。ICCPR 17 规定，任何人均不得在其隐私、家庭、住宅或通信方面遭受任意或非法干扰，或在荣誉或名誉方面遭到非法攻击；任何人均拥有受法律保护、不受此类干扰或攻击影响的权利。联合国人权理事会认识到，“违反或滥用隐私权可能会影响公民享有其他人权，包括言论自由权、有权持有主张而不受干扰以及自由进行和平

[20] 参见（例如）联合国安理会第 1373(2001)、1624 (2005)、2178 (2014) 和 2396 (2017) 号决议；联合国安理会第 A/RES/68/276 和 A/70/L.55 号决议

[21] 比如，可参见欧盟基本权利署的出版物“Under Watchful Eyes – Biometrics, EU-IT Systems & Fundamental Rights（接受监督 — 生物识别技术、EU-IT 系统和基本人权）”http://fra.europa.eu/en/publication/2018/biometrics-rights-protection

[22] S/2015/975，第 8 段；S/2015/939，原则 15 (e)。

集会与结社的权利……”[23]尽管在国际法下的隐私权不是绝对的，但对隐私权的任何干扰都必须符合合法性、合理性和必要性原则这一点已得到公认。此外，国家授权的隐私干预只能在合法的基础上进行，而且该法律必须符合公约规定、宗旨和目标，且在特定情况下应该是合理的。[24]同时，任何相关干扰不得构成基于种族、语言、宗教、国家或社会起源、政治或其他意见或国际法确定的任何其他依据进行的歧视。[25]

联合国隐私权问题特别报告员注意到，全球一些国家/地区已确定了尊严权利和人格可不受阻碍自由发展的基本权利，隐私权违反行为可能会对该等权利造成负面影响。[26]《世界人权宣言》和《公民权利和政治权利国际公约》首先承认人类大家庭所有成员的固有尊严以及平等和不可剥夺的权利是世界自由、正义与和平的基础。[27]该等权力可能因生物特征数据的不当使用而受到威胁。此类数据的不当使用还可能会对正当法律程序权利，包括无罪推定权及与刑事诉讼相关的其他权利构成严重风险。[28]此外，如果在不遵守必要性和合理性原则的情况下大规模收集此类数据，此行为本身可能会构成违反隐私权。[29]

各国应考虑调整与个人数据保护相关的法律，使其符合已增强的生物识别技术的当前应用，从而对该等法律进行审查，以防出现对生物识别技术的不当使用。各国还应对其法规进行审查，以应对生物识别技术的进一步发展带来的挑战。应在采用基于人权的生物识别技术的运用方法时，使用程序保障措施并对该项技术的应用进行有效监督。[30]这包括建立适当独立监督机构，对各国负责在发生违反行为时提供有效补救措施的机构的活动进行监督，及建立独立监督监管机构，确保各国的国家机构和私营部门遵守隐私和数据保护法[31]。

2.1.1 伦理和生物识别技术

由于技术创新和生物识别等技术相关法规的出台之间存在时间差，该等技术带来了特定挑战。因此，一些国家引入了伦理审查或其他监督机构，以对此类新技术或相关应用进行预测和考虑，并对当前或未来法规、政府政策和战略规划提供建议。该等机构通常由来自民间团体的具有较高资质的高级专业人员组成，可能还包括公共和私营部门、科学和技术、学术界以及非专业人士。该等伦理监督小组试图从较为广泛的视角，包括生物识别技术对特定群体或社区（尤其是种族、性别、年龄、宗教信仰和性取向群体或社区）的潜在影响，对问题进行审议。

以下案例研究对此方法进行阐释：

---

[23] 人权理事会第 A/HRC/RES/34/7 (2017) 号决议。
[24] 人权事务委员会第 16 号一般意见： 第 17 条（隐私权），第 3 至 4 段。
[25] ICCPR，第 2(1) 条 和 26 条。
[26] 隐私权问题特别报告员的报告，A/HRC/31/64 (2016)。
[27] 《世界人权宣言》和《公民及政治权利国际公约》(ICCPR) 序言。
[28] ICCPR 第 9 和 14 条。
[29] ICCPR，第 2(3) 条。
[30] 人权事务委员会在其第 16 (1988) 号一般意见中强调，各国必须采取有效的措施，确保与个人的私人生活相关的信息不会落到未获法律授权获取、处理及使用相关信息的人员之手，且相关信息不会被用于违反《公民权利和政治权利国际公约》的用途。有效的保护措施应能够使所有人以可理解的形式确定是否有个人数据存储在自动数据文件中，如果有，存储的数据是什么类型，以及该等数据所作用途，同时，该等措施应赋予个人要求改正或删除错误数据的相应权利。所有个人均应能够确定是哪些公共机构、个人或私人机构在控制或可能控制其文件。参见：http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=INT%2fCCPR%2fGEC%2f6624&Lang=en
[31] 联合国大会关于电脑化个人数据文件规范指南的第 45/95 (1990) 号决议和欧盟《通用数据保护条例》（2018 年）第 51 条（监管机构）。

案例研究 4 — 英国生物识别技术和法医学伦理小组[32]

此小组由最初的全国 DNA 伦理小组发展而来，该小组旨在对世界首个 DNA 数据库中使用的科学技术和策略进行监督。其目前职权范围一般包括法医学以及生物识别技术。该小组在法律、道德和社会政策考虑因素的广泛框架下考虑新出现的各种问题。其将根据下列指导原则开展工作：

指导原则 ***适用于生物识别和法医程序***	**指导原则** ***实施原则***
□ 应利用相关程序增强公共安全、改善公共利益； □ 应利用相关程序促进正义事业的发展； □ 相关程序应尊重个人和群体的人权； □ 相关程序应尊重所有个人的尊严； □ 相关程序应尽可能在不与刑事司法系统的合法目标发生冲突的情况下，保护尊重私人和家庭生活的权利； □ 应利用科学和技术的发展，使无辜者能够迅速脱罪，为受害人提供保护和解决措施，并未刑事司法程序提供协助； □ 相关程序应建立在有力证据的基础之上。	□ 公正 — 应用程序过程中不得带有偏见或存在不公平的歧视行为； □ 相称 — 应在个人权利和公共利益之间进行权衡； □ 开放和透明； □ 需要建立相关系统，对错误进行识别； □ 需要进行质量控制； □ 需要采用公共问责机制； □ 需要在适当时，进行独立监督； □ 需要提供充分的信息，且需在适当时，征得提供数据和样本的人员的同意。

该小组在数据收集和处理方面同样制定了一套明确的原则：

- □ 只能收集、存储和使用数据用于特定合法目的；
- □ 必须根据法律要求，对数据进行收集、存储和使用；
- □ 应采取相关措施，确保收集、存储和使用的数据的准确性、安全性和完整性；
- □ 相关流程应健全、符合国际标准，且应由经过训练的专业人员进行使用；
- □ 应尽量避免侵犯私人生活；
- □ 应考虑到二级数据主体（即可能受到从他人处收集数据影响的人士，如家人）的利益。

恐怖主义威胁影响到许多国家，因此，执法机构正在以较快的速度，开发和运用生物识别和法医学领域的新技术，以提供保护，并增强调查能力。伦理监督小组参与到此过程之中，对任何新技术或策略的准备和采纳发表知情评论。进行此过程后，并非无需后续立法，但此过程可能会防止引入不相符或者甚至没有必要的新方法和做法。此过程还将提醒立法者正在审议的问题的紧迫性

[32] https://www.gov.uk/government/publications/biometrics-and-forensics-ethics-group

和相对重要性。

伦理和生物识别技术互动方式的相关标准和示例

目前，与以合乎伦理的方式提供和使用生物识别技术或最新技术相关的标准在全球甚至是国家范围内，都具有不均衡性。国际标准化组织 (ISO) 颁布了有关司法管辖区和社会考虑因素及商业应用第 1 部分 通用指南 (ISO/IEC TR 24714: 2008) 及其第 71:2014 号指南相关的标准，该等标准在伦理方面作出规定，并在第 71 号指南中，提供老年和残疾人相关无障碍标准。

以合乎道德的方式使用生物识别技术的范围扩大到人道主义领域。在许多项目中，使用生物识别技术都能带来好处。例如，联合国难民事务高级专员署 (UNHCR) 办公室自 2002 年开始就一直使用生物识别系统，为其项目提供支持，且越来越多地运用生物识别技术进行注册。借助 UNHCR 全球生物识别解决方案 — 生物特征识别管理系统 (BIMS)，该机构能够确保各注册的独特性，并对合法接受者是否收到该机构可能提供的各种形式的援助（包括食物、现金、保护或安置干预等等）进行核实。还有其他一些例子，表明使用基于生物识别技术的身份识别可最大程度避免出现选举或财务舞弊 — 可能助长叛乱或恐怖主义的两个潜在不安定因素。

UNHCR 还建议对申请庇护的人进行生物特征登记，将该项登记作为对保护敏感的入境系统的必要环节。这要求实施适当的防护措施，以防止犯罪分子或恐怖主义分子或极端组织成员的可能渗入。在这方面的良好实践包括：(1) 适当登记，包括在相关安全、难民和人权保护方面接受训练的边境管理机构采用生物识别技术；和 (2) 将寻求国际保护的人员转介至庇护程序。一般而言，除非庇护程序已结束且已批准提供保护，否则不得与原籍国分享庇护申请者/难民的生物特征和其他个人数据，以免使其面临危险。在对庇护申请者或难民采取的有效保护措施可能遭受威胁的情况下，这一点对第三国同样适用。[33]

2.2 数据保护和隐私权

生物识别技术是全球反恐的重要资产。借助该项技术，可侦察并破坏恐怖主义活动，并保护社会不受任意攻击。但该项技术是以个人数据的收集、存储和使用为基础的。如前文所述，法律必须为该等生物特征数据提供保护，且应在不违反基本人权（如隐私权）的情况下，对该等数据进行处理。

2.2.1 合法注册条件和数据标准

联合国安全理事会在其第 1373 (2001) 号决议中提到，国际恐怖主义和有组织的跨国犯罪、非法药物、洗钱、非法武器贩运之间存在紧密联系。安理会在该决议中确定，各国应采取有效的边境控制措施以及身份证件和旅行证件签发控制措施，并采取旨在防止身份证件和旅行证件的造假、伪造和冒用的措施，防止恐怖主义或恐怖主义团体行动。

为对抗这一关系，关键要培养各成员国的反恐能力，使其能够采取充分、有效的反恐措施。[34]使用生物识别技术是培养此项能力的重要工具。[35]由于恐怖分子使用的策略通常包括窃取证件或身份，生物

[33] 参见 UNHCR“Addressing security concerns without undermining refugee protection（在不影响难民保护的情况下，解决安全问题）”第 E 部分第 17 段 http://www.refworld.org/docid/5672aed34.html
[34] 亦请参见安理会第 2195 (2014) 和 2178 (2014) 号决议
[35] 联合国安全理事会第 2396 (2017) 号决议及此前的第 2178 (2014) 号决议

识别技术为重新确定身份被窃者身份提供了有价值的工具（参见第 2.3.5. 节）。

为实施行之有效且符合数据保护法的生物识别系统，并维护隐私权，需要考虑以下因素：

登记质量保证 — 必须制定高质量的登记标准，以便在加速乘客处理同时确保准确性需求日益上升的各种环境（如在偏远的地区，设置的边防哨所或机场）中准确使用生物特征登记和匹配。如果儿童或法定的未成年人随同父母或独自旅行，应当承认儿童的某些生物特征可能会在成长过程中发生变化。此外，联合国安全理事会在其第 2396 (2017) 号决议中强调，必须遵循适用国际法，以尊重儿童权利及儿童尊严的方式对待儿童。

隐私法例 — 如果采取的措施属必要、合理且符合国际人权法，则执法机构可以限制一些隐私权。例如，可能会在紧急情况下，使用嫌疑人和同伙的个人数据，在此情况下，可能会不遵循知情同意或相关个人数据的收集等关键隐私原则。但在大多数情况下，知情同意、收集和使用数据仅用于所述目的以及纠正错误或误导性记录的权利等隐私原则应被视作默认要求。此外，应对偏离该等默认要求的原因进行记录和记载。操作人员对该等系统的访问同样通过生物识别系统进行控制，以确保维持高安全标准。

恐怖主义资助 — 可在一系列旨在减少金融系统的恐怖主义威胁的措施中使用生物识别技术，以帮助预防恐怖主义相关欺诈、身份盗窃和金融交易。因此，使用生物识别技术对交易进行访问控制是一个行之有效的选项。一个旨在为消费者提供保护、防止其遭遇与恐怖主义相关的欺诈和身份盗窃的全国性计划为社区和警方带来了诸多益处。[36]

国际个人数据标准 — 应根据国际标准制定个人数据标准，而不得使用基于本土行业游说等因素的不太常见模态或技术标准，或者援助者免费提供的系统。相关国际标准化组织 (ISO)、国际民用航空组织 (ICAO) 和世界海关组织标准是选择系统时应使用的初始标准，同时使用的还有生物识别学会隐私准则和隐私影响评估检查表。[37]

证据的可采性 — 应注意确保所有生物特征和个人数据仅用于获得其目的之批准用途。这也将确保为数据库收集的数据可用于起诉目的。这应包括旨在确保信息和通信技术行业开展合作的条款，前提是已为相关合作确定法律基础。

解释生物识别结果 — 拘留或起诉恐怖分子的执法机构应了解生物识别数据库结果解释不当所带来的风险，例如，理解由于在低质量的环境中捕获人脸图像而由环境问题引起的部分 DNA 匹配的价值或人脸对比未能确定结果。在该等情况下，在采取任何行动前进行背景分析是绝对有必要的（参见第 3 节）。

2.2.2 数据保留或删除政策

在此方面，必须根据国际人权法（包括隐私法）进行执法及开展反恐程序。例如，只有在需要对证人或持续调查的机密性进行保护的情况下，才有权查看某人的文件、进行更改或要求删除（该权利通常

[36] 参见国际货币基金组织网站（该网站上载列了反洗钱和其他反欺诈文件）：www.imf.org

[37] 参见 www.biometricsinstitute.org

在隐私法（如欧盟 *《通用数据保护条例》*(GDPR)[38]）中获得保障）。

全球各地的数据保留政策相差较大，对于在执法调查期间被捕的人而言，尤其如此。许多司法管辖区保留了被定罪人员一生中的生物特征数据，但对于那些涉嫌犯罪、被捕，而后并未被定罪的人员而言，却并没有统一的标准。

将生物特征数据与其相关个人数据分开存储是很好的做法。身份被窃者（通过犯罪或恐怖分子活动）可能需要在发生身份丢失或误用后，快速重建身份。有必要在进行系统设计时，对发生该等情况时进行的生物识别和个人数据重新连接进行规划。这可以通过以独特参考编号的形式向生物特征记录分配元数据的单个分段实现。但应对重新连接采取保障措施，以确保系统和数据始终完整，且要求达成完善的安全协议，例如：

- 要求访问人员为组织内资质较高的人员，和
- 使用其生物特征访问系统，和
- 对访问进行正式记录，和
- 对要求进行相关访问的原因进行正式记录

可通过使组织中的多名人员参与条目验证或撤销流程，进一步增强安全性。此措施将履行相关职能的员工的工作轮调考虑在内，并建立了另一层安全保障。

2.2.3 数据处理

负责数据处理的机构必须举荐一名数据控制人，其将负责管理所有数据处理活动，包括数据的收集、存储、使用和删除。即使将数据处理职责外包给他方，相关责任仍归数据控制人所有。

内容极全的隐私法作出此项要求：收集个人数据的机构要确保不会在隐私法的级别低于数据收集国的国家处理或存储数据。

任何第三方供应商或操作者均应受到以下条件合同的约束：此类合同要求较高安全级别、且要求由委托机构进行外部审计并对不遵守合同规定的安全和隐私要求的行为进行处罚。

2.2.4 数据共享

联合国在若干声明中强调了各国在完善法律方面进行合作，以起诉恐怖分子，尤其是国外恐怖分子，同时根据法律保护人权和隐私提供保护的重要性。[39]在管理机构和各国之间实时共享个人数据（如生物特征数据）亦要求进行合作，以实现平台和格式之间的互操作性的协调。[40]

如果恐怖分子或疑似恐怖分子的个人数据被共享，则需在诸多问题方面给予极大信任，如共享数据的用途、数据的准确性和背景以及可共享数据的数量和类型。应根据各相关方作出的正式安排制定

[38] 欧盟《通用数据保护条例》（2018 年）第 7 条（同意）、第 17 条（删除权）、第 15 条（数据访问权）
[39] 联合国安全理事会关于国际合作的第 2322 (2016) 号决议和联合国安全理事会第 2396 (2017) 号决议强化措施，以应对卷土重来的外国恐怖分子构成的威胁。
[40] 联合国安全理事会第 2178 (2014) 号决议和外交部部长在安全理事会反恐委员会特别会议上发表的马德里宣言（2015 年 7 月 28 日）。

数据共享安排。

共享过程中还需将其他因素纳入考虑。这些因素包括请求获得个人数据应以真正存在恐怖主义活动嫌疑为依据的规定、证据要求的细节和确定数据是否在压迫的条件下获得 — 许多国家的关键证据问题。

以下原则一般适用：

1. 个人数据（包括生物特征数据）的共享必须在国内依法获得批准，且必须根据在国内外发送和接收数据的实体之间确立的清晰法律框架进行
2. 此类数据只能用于其批准的用途
3. 只能与信任的接收方分享数据。[41]第 2.2.3. 节中载列的原则延伸至数据共享，且不得将个人数据发送至隐私保护级别低于发送国家的司法管辖区。
4. （根据第 2.1. 节）除非庇护程序已结束且已批准提供保护，否则不得与原籍国分享庇护申请者/难民的生物特征和其他个人数护，以免使其面临危险。（亦请参见案例研究 10）

2.2.5 防止数据滥用

此处，至少有两个与数据滥用相关的关键问题。

第一个是防止在未经授权的情况下访问所有个人数据，包括生物特征数据及对该等数据进行滥用的绝对必要性。这既包括外部威胁，也包括授权人员作出的内部渎职行为。

第二个是确保提供的个人数据正确无误，已置于相关背景下，且以善意的目的提供。这一点在政府或另一方可能试图将政治对手列入观察名单以影响其基本权利时尤其重要。

2.2.6 数据安全和验证

各组织应委任一名具有足够资历、接受充分培训并掌握充分专业知识的数据管理人。此人将负责所有个人数据（包括生物特征数据）的收集、使用和移动。

此职位的关键职责应包括政策制定和标准操作程序。任职人还应负责在系统设计阶段决定哪种或哪些生物识别模态最适合相关应用。

所有有效的隐私和安全政策和做法都要求至少确定下列事项，无论是否使用生物特征数据：

- □ 是否在引入新的商业实践或新技术前完成隐私影响评估？[42]
- □ 是否制定了培训和意识增强计划和程序，以保证充分的隐私权和人权文化，并且使所有系统操作人员具备生物技术操作知识？
- □ 是否在个人数据（包括生物特征数据）的收集、存储、使用和共享的关键阶段使用了加密

[41] 值得信赖的接受者之间共享个人数据的示例包括英国可记录犯罪数据 ACRO 与美国联邦调查局或其他欧盟警察局、移民局或由 INTERPOL 盗窃或遗失旅行证件数据库和通知系统相关的旅行证件提供支持的 INTERPOL I-24/7 安全警方对警方通信系统之间的协议。

[42] 隐私影响评估 (PIA) 构成公共和商业组织中“从设计方面着手进行隐私保护”的数据管理方法的一部分。PIA 流程可通过识别潜在风险并制定风险管理策略，确保遵守隐私方面的法律和监管规定。

或数据缩减技术？

- □ 是否有要求敏感个人数据文件访问者提供生物识别特征的严格访问控制和访问记录流程？
- □ 是否有备存记录的程序，对在发生隐私和安全违规行为时所需的报告机制和补救措施进行界定？
- □ 是否进行定期测试和审计，以确保遵循安全和隐私做法，且该等做法依旧强有力、行之有效？
- □ 是否有正式程序，对定期审计过程中显现出来的问题作出记录，而后进行解决？
- □ 是否对系统内保留的个人数据的有效性和完整性进行定期、随机检查？

有若干国际标准和准则可为数据控制人及其机构提供建议。[43]

就收集数据（包括生物特征数据）的验证而言，务必遵循正当程序，以保护人权（包括隐私权），同时确保完全遵守定罪方面的司法要求或引渡程序等。在引渡程序中，某些国家的这些要求可能比其他国家更加严格，在证据和审讯标准方面尤其严格。

对执法和边境管理机构而言，有一项关键指导原则，即必须组建专门的分析师团队。团队内的分析师必须有提供可执行、准确结果的技能和资源。这有助于在事前和事后进行恐怖主义监控以及获取可接受的证据，包括 DNA、指纹、人脸和声音等生物特征数据。此项功能应充分利用所有生物特征数据捕获和搜索技术。

2.2.7 监督

可能会在滥用（无论是恶意还是错误使用）个人数据的过程中给他人造成不利法律后果和其他损害。这尤其适用于观察名单或其他预警机制。

在将恐怖分子嫌疑人或罪犯列入观察名单时应小心谨慎。应在将个人数据列入名单前，进行严格、彻底的检查，以对纳入的原因和所有请求的有效性进行评估。必须对观察名单中包含的数据进行定期审核，以确保该等数据的时效性和相关性。

同样，根据国际人权法和隐私法规，数据主体应有权对纳入任何名单的项目进行审核。上市管理局应公布审查权、上诉权和投诉机制的存在情况。

纳入过程中，执法、反恐和边境管理机构负有收集、存储和分析恐怖分子嫌疑人及其同伙数据以及其行为方式（如航班行程、金融交易和住所活动）的法律职责。但必须确保对与嫌疑人及其同伙相关的信息保密，且该等信息未超出授权的法律框架，以免发生非法监禁或迫害。

必须对任意收集、存储和使用个人数据的行为实施强有力的保障措施，包括具有独立机构的监督机制。各成员国可能已经设立了可以在现有或延伸到的职权范围内承担这一职责的隐私监督机构。但若成员国目前并未设立此机构，则应该设立，以履行此重要职责。

尤其是有必要依法建立独立、有效和公正的监督机制。该等机制应有权对生物特征数据的保障措施（

[43] 联合国大会关于电脑化个人数据文件的管理准则的第 45/95 (1990) 号决议和生物识别学会在国际范围内适用的*生物识别技术隐私准则* www.biometricsinstitute.org

包括此类数据的国际共享方面）适当性进行监控和评估。个人应能够联系监督机制，以获取与其数据相关的信息并在感觉其权利受到威胁时进行投诉。在可能的范围内，应以清晰简化的形式，向数据主体提供与其数据的处理相关的信息。对于在处理生物特征数据时作出的违反人权行为（包括违反隐私权的行为），应根据法律提供适当的补救措施。

2.3 系统风险管理

系统风险管理要求在某一部件（比如生物特征数据读取器）或整个系统（系统配置）的范围内为系统故障编制目录，并确定相关故障是否导致整个系统无法按预期方式运行。其识别威胁和风险，然后对正在实施或利用的威胁的后果进行分析，最后实施缓解措施（如有必要）。

反恐应用程序中用到的生物识别系统通常较为复杂，涉及多个 IT 组件、与采集环境的互动和人工解释。这导致出现存在多个故障点的多方面风险情况，这尤其是因为恐怖主义活动的打击目标具有高度积极性，且通常有良好的资源，可以绕过安全控制措施。

如果在不进行适当风险管理的情况下，实施系统，打击恐怖主义行动，可能导致对系统有效性产生不切实际的自信。从而导致对通缉的人员进行的身份识别出错、高度敏感的观察名单信息泄露或恶意代码的插入。

已知或涉嫌恐怖分子经常以虚假或伪造的身份出行。因此，从风险管理的角度来说，有必要以正确的方式实施传统的个人资料匹配系统（参见第 3.1.4. 节）。国家边境管理机构可进行生物特征验证并在观察名单上进行搜索，以帮助缓解此风险（参见第 3.3.1.2 节）。

生物识别系统的建立对环境的依赖度较高。例如，每座机场的环境都有所不同，且在乘客行为和人口特征方面也有所差异。这将引发不同风险，该等风险要求采取相应缓解措施。但有一个所有人都常用的重要缓解措施，即由专业测试人员定期进行主动渗透测试，以确保风险被暴露和理解。

风险管理是一项专门的活动，且须符合国际标准和国内多种标准（参见本节末尾的参考资料）。

业务连续性对任何用户而言都至关重要，且应急协议必需构成任何生物识别系统的标准操作程序的一部分。因此，如果系统的任何部分出现故障，因而无法提供正常服务，通常会提供一个或多个应急措施，以提供临时服务。采取的该等措施可能是操作人员（在自动生物识别闸门出现故障时，负责护照手动检查工作的边境人员）进行的人工干预，也可以是返回到备份系统或部件阵列。[44]

2.3.1 漏洞和新出现的威胁

就分析目的而言，生物识别技术在应用于反恐行动时，主要面临下列几个方面的威胁：

- *通用信息技术：*所有用于管理数据库、确保信息传输安全、审核用户活动和防止病毒的后

[44] 在此方面，一个典型的示例是自动指纹识别系统 (AFIS) 中常用的独立驱动器冗余阵列 (RAID)。可将服务期内较小驱动器的配置组合起来，构成较大的阵列，从而提升性能和安全性，并在综合服务器中提供冗余。大多数执法用户要求其 AFIS“一年 365 天，每周 7 天，每天 24 小时”不间断地运行，因此，关闭系统以进行长时间的维护、升级或维修并不是理想的选择。因此，灵活运用复制的 RAID，即可使系统不间断地运行，因为可能不止一个磁盘会出现故障或从实时运行中移除，且数据将保存到活动磁盘中，以确保向用户提供不间断的服务。

端技术。政府系统 IT 安全方面的最佳实践应已涵盖这一点。

- *生物识别传感器和环境：*使用技术的类别和特定风险。例如，假指纹、深色眼镜或变声技术的使用。
- *生物特征识别匹配引擎：*匹配引擎的配置包括临界值的设置、可疑呈现检测和观察名单管理。
- *人为监督:* 所有生物特征识别系统均存在一定的错误接受率和错误拒绝率，在犯罪侦查搜索的背景下，尤其如此，因为登记的生物特征数据质量可能参差不齐（参见第 1 节）。必需由经过适当训练的操作人员对该等错误接受和错误拒绝进行调查和评估。若处理不当，则可能导致拘留错误的人员、工作无效或者错过观察名单中构成较大威胁的目标人物。

表 1

威胁领域	责任	后果	缓解措施举例
通用信息技术	IT 安全管理员	观察名单曝光、系统安全性下降、匹配更改。盗窃的生物特征识别模板被用于生物特征识别重建。	通信安全、防病毒、防火墙（服务拒绝）、个人资料观察名单管理、与外部系统安全连接。可撤销的生物特征识别技术。
生物特征识别传感器和环境	供应商/系统集成商	观察名单中的目标人物可通过欺诈传感器避过检测	环境设置、可疑呈现检测、质量过滤。防欺诈算法（呈现攻击检测）。
生物特征识别匹配引擎	供应商/系统集成商/IT 安全	观察名单中的目标人物可避过检测	系统调校、登记质量管理、适当后端管理。使用多模态生物特征识别技术，而非单一生物特征识别模态。
人为监督	政府安全机构/操作人员	拘留错误的人员、工作无效、错过观察名单中构成较大威胁的目标人物	教育、培训和认证、审计、用户界面设计、适当术语

2.3.2 模态带来的威胁

生物特征识别系统面临的威胁较为复杂，且随着此项技术应用范围的扩大，该等威胁仍在不断演变。对这一领域的所有漏洞和风险进行全面的细分并不在本文件的讨论范围之内，但这些漏洞和风险已在 ISO/IEC 30107-2_2017 标准 [1] 和边境管理机构的一些特定示例 [2] 中进行了记录。

用于反恐的常见生物特征识别模态包括：

人脸 — 人脸通常通过近端或远程捕获系统获得及轻松获取，但这些系统可能会面临特定挑战和技术限制，导致人脸图像质量不佳。该等图像会显著影响正确检测的可能性（或者相反，系统生成误接受的数量）。登记照片（用于创建观察名单的照片）以及摄像头拍摄照片的质量均会受到影响。可查看参考文件 [3]，获取有关如何改善人脸识别监督措施的相关示例。具体质量属性包括：照明、姿势、摄像头位置、表情、头部遮盖物、眼镜、胡须、分辨率（两眼之间的像素）和年龄。

面部常见漏洞的部分示例包括：

- *长相相似欺诈：*长得像真正目标对象的人使用身份证件。通过这种方式，观察名单上的人可在被发现后，声称其并非真正的目标人物。
- *面罩：*先进的乳胶面罩正在逐渐面世，该等面罩难以通过随机观测检测出来。
- *化妆：*为了避免被发现，正确地使用化妆，掩盖面部特征，同时给观察人员以自然之感。
- *眼镜：*深色或镜片较厚的有框眼镜可以掩盖用于识别的部分重要面部特征。
- *行为：*如果目标人物怀疑有人监视他们，则会使用手机并将望向地面，使相关人员无法难以获得高质量的图像。
- *变化：*将从两个或更多贡献人采集的生物特征样本（如人脸图像）合并，以便能够成功对照变化的身份，对任何贡献主体进行成功验证。

指纹 — 指纹生物特征在全球范围内用于执法目的，因此，许多现有的数据库和观察名单中都有指纹模板（参见第 1 节）。基于指纹的生物识别系统的部分常见漏洞包括：

- *假手指：*使用由模拟皮肤特征的物质制成的假指纹。可以单独戴在每根手指上，也可以作为整个手套的一部分，套在每只手上。
- *故意破坏：*如果目标人物怀疑其可能遭到监视，其可能会试图使用化学品、研磨物质或其他技术破坏指纹。
- *尸体指纹捺印：*恐怖分子已经在创建身份时，用到死者的指纹捺印，开立银行账户并进行金融交易，以获取行动资金。

虹膜 — 虹膜识别法提供了准确、可信赖的生物识别模态。虹膜不会随时间变化，且难以伪造。在虹膜识别系统方面正在进行大量研究和开发工作，以防止欺诈行为，同时引入该等系统，作为边境管理措施的替代/补充模态。相关漏洞包括：

- 使用印有虹膜图案的*美容隐形眼镜*。
- 使用网络上提供的高质量人脸图像，获得*人眼的打印图*。
- 尽可能*放大瞳孔*。这样，扫描仪可能就无法识别虹膜图案了（如果将匹配算法应用于瞳孔大小明显不同的同一只眼睛，虹膜识别性能会下降）。
- *点阵隐形眼镜*，此眼镜上印有虚假图案，可直接覆盖在人眼上。这将使虹膜扫描系统无法识别其数据库中的虹膜。
- *绘有虹膜图案的巩膜镜*。此类眼镜覆盖眼球的整个可见区域，佩戴此眼镜的人会呈现出完全不同的眼睛图案。
- 通过手术在人的实际虹膜前*植入彩色虹膜*。许多人选择动手术的唯一目的是改变眼睛颜色，与此同时，那些希望掩饰自己身份的人也可以使用此程序。
- 必需在认证期间提供参考模板，才能进行匹配，这使得攻击者有机会盗窃模板，这反过来会助长进一步的攻击行为。

声音 — 可使用说话者识别技术，对电话通话进行监控，并提高对目标人物的警觉。对较大交易量或大型数据库而言，说话者识别技术通常具有边缘准确性（尤其是通过不同电话渠道）。但此项技术的应用可在搜索的通话和观察名单上的人员数量较小且有限的情况下发挥作用。

一些常见的声音漏洞包括：

- *变声器：*目前，智能手机有多个应用程序可使声音发生变化。
- *合成语音：*新出现的威胁向量是指使用可在语音方面进行训练的工具，以便使用合成的声音自然读取输入的信息。

2.3.3 登记质量

无论采用何种模态，如果生物特征数据的质量过低，则不值得纳入观察名单。如果质量不达标，则产生的结果可能并非是生物特征的真正匹配项，且可能产生较大的错误接受量。生物特征数据质量的衡量和管理对确保生物识别系统结果的准确至关重要。各模态有自己的质量措施，例如，就人脸而言，存在照明、姿势和头部遮盖物等问题。在登记过程中使生物特征质量下降或模糊的任何因素都将影响系统的搜索和匹配功能。一系列 ISO 标准均对质量标准作出了定义（参见第 2.4 节）。

2.3.4 吞吐量和功能管理

对系统吞吐量起天然决定作用的是匹配和处理时可用的计算资源。生物特征匹配通常是一个耗资巨大的计算过程，对于较长的观察名单而言，尤其如此。人力资源是生物特征匹配的最大限制因素之一。对于需要进行调查的每项匹配，都要有训练有素的操作人员进行评估。这意味着，比如，即使使用在临界值平衡方面进行细微调整的人脸系统，在繁忙的环境中需要处理的误接受量依然相当大。了解此类要求是一项重要的预算考虑因素，不仅对于预期最初的建设要求是这样，对于未来运行也是如此。

2.3.5 身份盗窃

身份盗窃一般指在未经授权的情况下，获得个人数据（如姓名、出生日期、地址等）以实施犯罪行为，尤其指使用盗窃的数据进行冒名贷款、信用卡使用或购买昂贵物品的欺诈行为。涉及生物特征数据的身份盗窃会引起一些重要的问题，因为生物特征通常会伴随一个人的终身，且不会像个人身份识别码或密码一样能够被轻易重置。盗窃生物特征数据可能涉及个人的实际身体生物特征，如建立复制的指纹或面罩，或者盗窃应用程序或数据库中保留的生物特征模板。已制定一些重要的缓解措施以应对这些风险，其中一些主要措施包括：

*活体检测：*生物特征捕获设备中内置有各种传感器，以观察呈现的生物特征底层之外的特征，并对活体皮肤和假冒人工制品进行区分。

*可撤销的生物识别技术：*生物特征数据登记到系统之后，其特征会不断被故意扭曲。如果模板随后被破坏或被盗，则使用不同的扭曲特征创建为相同生物特征创建替代性模板，以使盗窃的模板立即变得多余。因此，相同的生物特征可以用于多种用途，而相关模板各不相同。原始的非扭曲生物特征数据不会被登记，这将为用户提供更好的隐私保护和保证。

应当注意，当生物特征与身份证件（如护照）一同使用时，身份盗窃的风险将降至最低，因为如果生物特征被“盗”或复制，从属人员仍需要有效的证件，如果有必要，可使该证件无效。希望获得相关图像的人员可秘密或从网络资源捕获人脸等生物特征。这意味着在正式文件中使用人脸作为生物特征的机构应确保，其已将此类盗窃的风险纳入考虑且已采取适当减轻损失措施。

2.4 国际标准

2.4.1 技术操作标准

务必确保任何反恐生物识别系统安全、始终可靠且可传达用户的特定商业需求。该等要求建立在多个关键因素的基础之上，如：

- 进行系统测试，以确保符合当前和未来性能规格和指标
- 确保操作环境和网络安全
- 进行法律和隐私影响评估
- 对端到端系统进行风险管理
- 操作人员具有可论证的能力
- 所有系统特征（如生物特征捕获设备）、数据登记和身份凭证保证、数据存储和检索、匹配性能和错误率以及任何非生物识别特征的元数据在数据处理和完整性方面均有保证
- 软件和硬件可靠度
- 互操作性 — 与其他系统之间的数据传输和交换
- 人机界面设计 — 在下列方面使用简便：(1) 数据主体的采集和登记 (2) 系统操作人员 — 工具集、工作站、功效学、环境

已有一系列国际、区域性和国家标准，对该等重要的元素和外设功能作出规定。生物识别系统的所有人、用户和客户倚赖该等标准，以确保其应用程序在整个生命周期内均根据制造商的性能规格有效运行。其同样倚赖相关标准，来为生物识别系统的采购（参见第 2.4 节）、维护和升级等流程提供保证，在系统属于更广泛的国家或国际数据交换网络的一部分时，尤其如此。如果该网络中的部分成员未根据国家或国际标准运行其各自的生物识别系统，此网络中的合作伙伴或潜在合作伙伴不太可能会同意参加。

国际标准化组织[45] (ISO) 制定并发布了各个行业（包括生物识别技术和法医学）的标准。ISO 是一个全球性的国家标准机构联盟，会员来自 162 个国家，其通过成为各主题的委员会的会员，参与标准的制定。其他国家可能会以通讯或订阅会员身份加入，以获取标准相关信息。

ISO 还与国际电工委员会[46] (IEC) 组建了两个联合委员会，IEC 负责制定标准并为所有电气、电子和相关产品进行合格评定 (CA)。进行合格评定可使不完全了解系统或产品复杂性的有意购买者确信，相关系统或产品符合所需的技术和安全标准或规定的其他标准。有以下三种类型的 CA：由供应商进行的*第一方* CA、由用户实施的*第二方* CA、由独立机构进行的最为严格的 CA — *第三方* CA。该流程称为认证，因为通常在成功评估后颁发证书。该流程旨在对产品或服务是否符合特定规格或 ISO/IEC 标准进行核实。

区域机构也可制定相关标准，以使系统符合国家集团的工作实践。例如，欧洲标准化委员会[47] (CEN) 汇集了 34 个欧洲国家的国家标准化机构，且设立了专门的生物识别技术工作小组 (WG18)，该工

[45] http://www.iso.org
[46] http://www.iec.ch
[47] https://www.cen.eu

作小组对国际和国家组织的标准进行改编，以遵守隐私和数据保护法等欧洲规定。

国家的相关组织负责在国家层面制定一些标准，例如美国有国家标准学会 (ANSI) 和国家标准与技术研究院 (NIST) 负责制定在法医学和相关生物识别应用方面适用的标准。NIST 标准已被许多国家广泛应用于若干关键领域，如在网络中以电子方式传输指纹。对于其他生物特征模态（如人脸和虹膜），NIST 还对在商业上可获得的生物特征搜索和对比算法进行竞争力测试和排名。[48]这使生物特征匹配系统的有意购买者可以获得有关国际市场中的制造商对手使用的算法的相对表现的客观信息。

2.4.2 科学操作标准和质量管理程序

除适用于生物识别系统的技术标准和认证程序外，还制定了对法医学流程适用的 ISO 标准（如 ISO/IEC 17025:2017）“检测和校准实验室的一般能力要求。”此标准对需要进行科学测试和/或校准（包括采样）的流程和能力作出规定。其对流程的管理以及科学家的能力和公正性及其使用方法的有效性进行审核。该标准运用实验室本身进行的内部审核和测试以及由外部认证机构执行和监督的外部审核和水平测试，促进持续改进并对实验室进行认证。通过进行该等定期、独立检查，可确定实验室是否符合所需标准，以取得或获得 ISO17025:2017 下的认证。认证过程对实验室是否建立完全可运行的质量管理体系 (QMS) 及有能力根据相关标准实施科学测试和校准进行确认。

QMS 对有助于实验室发挥有效性能的所有因素（最重要的是，对任何不合规的实例）进行定期审核。采用矫正措施程序，对任何不合规行为的根源进行识别，且制定了预防措施，以防再次发生。内部管理审查对照根据实验室质量手册制作的组织、资源、流程和管理要求综合检查表，对实验室的表现进行系统评估。

有一些标准适用于犯罪现场调查等其他法医学领域（如 ISO 17020:2012）。因此，可以且有必要在反恐行动方面采用基于标准的方法，该方法须涵盖从犯罪现场到法庭的所有法医学流程，包括：

- 犯罪现场管理和检查，包括法医学和生物识别策略（参见第 3.3.3.2. 节）解释性评估、资源协调、采样方法、防污染程序、包装材料以及对嫌疑人、证人和受害人的审查。
- 实验室流程，包括采样、分享、数据库管理、员工能力和结果报告。
- 法庭证据 — 专家证人协议、公正性和证据出示技巧。

2.5 采购和资源管理

2.5.1 采购

国家政府建立了本国的监管框架和选择标准，以对商品或服务的采购进行控制。但在评估生物识别系统的必要性和某些与用于应对恐怖主义威胁的应用程序购买相关特定方面时，应将若干相关要点纳入考虑：

商业需求 — 应在商业计划中，清楚阐述使用生物识别技术，而非替代性识别和认证方式的优势和原因。应在该项技术带来的好处和潜在劣势（如成本、技术漏洞、公众/客户可能提出的反对意见和带来的阻力、伦理问题和风险评估流程中识别的其他威胁）之间进行仔细权衡。应对当前和未来用户

[48] http://www.nist.gov

访问量和数据库功能水平进行仔细评估，以确保该系统能够应对预期的吞吐量，尤其是需求高峰时期的吞吐量。（参见第 2.3.4. 节）。

隐私和数据保护 — （参见第 2.2 节）生物识别系统在识别已知或嫌疑恐怖分子时，必须遵守个人依据国家和国际法所享有的尊重隐私和个人数据保护的权利。生物识别系统可能会出错 — 识别错误或未能识别出某人，这两种错误都可能使数据所有人面临极大的声誉风险。必须在任何生物识别应用程序的设计阶段仔细考虑这些方面，且需制定合适的流程，以便在发生这种情况时，对相关事件采取应对和缓解措施。

注：对于所有国家或地区性政策或为反恐生物识别系统的开发而制定的项目计划，都应考虑扩大任何现有隐私监督机构职权范围或建立新机构所需的资源（参见第 2.2.7. 节）。

安全 — 对于使用恐怖分子和恐怖主义行为相关数据的生物识别系统或网络的任何部分，它们都可能成为外部电子/网络或物理攻击或因员工的渎职行为而出现的内部干扰或破坏的目标。因此，必须采取高级别的分层保护措施，以保护运行环境、硬件、软件、通信网络和存储的数据。应考虑审查负责操作系统并确保其未遭受恐怖分子或其同伙任何形式的胁迫的工作人员。应定期进行审核，以识别内部腐败和不当行为的证据。还需要处理并预防呈现攻击等其他威胁（参见第 2.3 节），这是整体安全战略的要求。

性能 — 用于反恐的生物识别应用程序必须以最高精准度运行，即保持极低的错误率，同时维持可接受的吞吐率。如果系统在运行的任何阶段因任何原因未能识别出恐怖分子，则许多人的生命都会受到威胁。在系统的整个生命周期内，此生物识别性能水平的获得、维持和定期升级都可能耗资巨大。较高的风险同样意味着，必须实施全面彻底的例外情况处理程序，以防恐怖分子故意避开生物特征识别检查，而采用可能不那么严格的备用系统。

生物特征模态 — 选择哪种或哪些特定的模态可能取决于下列因素：

- 可访问性和功能性 — 确定对应用程序运用单一的生物模态还是使用多模式方法，是一项基本的采购决策。选择的模态必须对其拟进行的验证 (1:1) 和识别 (1:n) 对比工作适用。单模式系统的购买和运行成本一般较低，但其无法满足所有人的需要。比如，有许多人可能因为在工作中永久受伤、失去手或手指或皮肤受损（比如，需要处理化学品或可能使手指和手部表面的摩擦嵴模糊、扭曲或受损的某些类型体力工作的人）而无法登入指纹系统。如果生物识别应用程序需要登记尽可能多的人，则最好使用多模式系统（如指纹和虹膜），因为该系统可从更大比例的所需人口中捕获生物特征。在功能性方面也需要进行类似的采购决策，例如购买只提供一项功能的生物识别应用程序（如警方犯罪记录指纹系统）是否是明智的决定，或者建立多功能的网络（如犯罪记录加犯罪数据库与边境管理相结合的应用程序）是否同时能为投资带来附加价值？甚至还可以在国家法律允许的情况下，扩充功能和模态，以使某个国家最终只运行一个生物识别系统。一些国家正在采用多模式、多功能的方法，以便实现规模化经济，通过整合类似功能，对人员总数作出合理解释，并使这一国家系统只需要一个单一的治理和管理结构。
- 模态的兼容性和面向未来 — 为反恐应用程序选择最合适的模态时，有一个十分关键的问题，即获得并与国内或国际合作伙伴分享该等数据，以识别潜在恐怖分子的可能性。例如，可能会在分享从其各自边境进入的所有签证申请者指纹数据的国家之间建立区域性网络

。因此，任何希望加入此网络，并从中获得好处的国家都可能需要使用指纹以用于签证申请者生物识别系统的目的，即使由于其他原因，起初在最初的商业案例中建议使用其他模态。此外，还应考虑特定模态，因为它们同样是常见的犯罪现场生物特征，且允许进行交叉搜索以用于反恐目的。例如，比起虹膜或手静脉模态，可能更推荐指纹和人脸。

- 数据捕获和登记 — 例如，目标接触或极为接近捕获设备是否可取？或者进行远程捕获对操作环境而言是否是更好的选择？
- 可接受性和吞吐量可操作性 — 客户可能对一些生物识别模态存在先入为主的看法、合理担忧，甚至将该等模态视为社会耻辱（例如，由于在治安方面的历史传统，指纹通常和犯罪联系在一起）。一些模态可能会因提高数据捕获和登记程序的速度和便捷性而受到青睐，这两点对于需要定期处理大量客户（如在边境控制点）的应用程序而言通常会是考虑因素。

2.5.2 资源管理

为采购大型、大体积的生物识别应用程序，必须投入大量资金，以购买必要的硬件和软件，并创造合适、安全的操作环境（如登记和数据捕获站、服务器机房、操作员套房等）。此外，某些应用程序还存在与人员招聘、培训和以滚动方式进行认证（如果采用基于标准的方法）相关的成本。

安装系统并成功完成验收测试后，将进行定期维护，且偶尔将进行软件性能和安全性升级，相关成本从年度预算中拨付。该笔金额是员工薪资和系统的常规、有效运行的基本年度收支的补充。生物识别系统一般需要全年、每天 24 小时不间断地运行，同时需要尽量减少系统的停机时间。

在商业的驱动下，生物识别技术领域的现代研发工作在全球范围内开展，使新的软件迭代和功能升级不断快速出现。许多生物识别系统可运行二十年或以上，因此，需要进行多方面的性能升级，以避免变得冗余。如果不在生命周期内进行定期维护和升级，任何生物识别应用程序都可能严重损坏或发生全面故障[49]。

采购和规划流程还需要考虑其他未来需求（如增强处理能力，以应对增加的需求，这直接导致需要扩大数据库的存储容量）。还有一项操作方面的需求：连接到其他系统或数据库，并能够与其互相操作。任何该等功能的增强都要求在未来投入额外资金，如果预算随后缩减或者优先处理其他竞争性需求，则可能无法提供该等资金。因此，在规划阶段预设该等功能和要求，并在新系统中纳入尽可能多的功能是可取的。应用程序应设计有空闲的处理和存储能力，或已在采购合同中对该等升级进行成本估算和协定。如果在开始的时候将网络功能纳入考虑，则可为新系统内置与其他系统的连接和相互操作的功能。在设计阶段构建该等接口比在后期阶段建立的费用要低得多，如果在后期阶段建立，则可能会干扰系统的正常运作，且可能要求在两个/所有系统中安装或重新配置连接组件和路径。

2.6 推荐实践

a) 各国应在运用反恐生物识别技术时，采用基于人权的方法，该方法包括程序保障措施的使用及对该项技术的应用进行有效监督。这包括建立独立、适当的监督机构或将该机构的职权范围扩大，以

[49] 正因如此，ICAO 才授权使用图像，而非电子护照模板。这种面向未来的方法可确保向优化匹配算法的升级依然是可纳入边境检测系统的一项选择，该系统依赖于从电子护照读取的生物特征（通常是人脸图像）。

对相关隐私法规的实施及在发生相关方面的违反行为时采取的有效补救措施进行监督。此外，还应实施伦理审查程序，公布将生物识别技术用于反恐用途的所有相关国家政策和决策。

b) 运用生物识别技术打击国际恐怖主义行为和相关罪行时，必须遵守所有个人在隐私及其个人数据（包括生物特征）的法律保护方面的基本权利。

c) 生物识别系统可能很容易出现故障及遭到许多形式的故意攻击。因此，建议各国定期对其生物识别应用程序端到端的流程进行风险评估，以减轻当前或新出现的威胁。

d) 建议各国根据国际技术标准运行其所有生物识别程序，并根据国际科学标准为其法医学和质量管理流程申请正式认证。这不但会为生物识别流程的有效性奠定坚实的基础，而且将打消希望进行生物特征数据共享的国际合作伙伴的疑虑。

e) 生物识别系统的采购要求进行长期战略规划，以便解决当前和未来的资源需求，因此，各国应考虑下列因素：

- 购置和测试系统所需的初始投资
- 员工和系统维护外加安全和性能升级方面的可持续年度开支
- 系统生命周期内需要的预算、数据库容量和处理能力
- 与国家或国际网络的潜在连接和互操作性以及各模态的兼容性
- 对于任何反恐生物识别系统，都应在安全性、客户访问和可用性、吞吐量以及处理速度方面的关键操作要求之间进行权衡。

2.6.1 参考文件

联合国安全理事会第 1373(2001)、1624 (2005)、2178 (2014)、2195 (2014) 和 2396 (2017) 号决议以及联合国大会第 A/RES/68/276 和 A/70/L.55 号决议

欧盟基本权利署的出版物"Under Watchful Eyes – Biometrics, EU-IT Systems & Fundamental Rights（接受监督 — 生物识别技术、EU-IT 系统和基本人权）"http://fra.europa.eu/en/publication/2018/biometrics-rights-protection

S/2015/975，第 8 段；S/2015/939，原则 15 (e)。

人权理事会第 A/HRC/RES/34/7 (2017) 号决议。

人权事务委员会第 16 号一般意见：第 17 条（隐私权），第 3 至 4 段。

隐私权问题特别报告员的报告，A/HRC/31/64 (2016)。

《世界人权宣言》和《公民及政治权利国际公约》（ICCPR）序言。ICCPR，第 2(1)、 2(3)、9、14 和 26 条。

人权委员会第 16 (1988) 号一般意见，参见：
http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=INT%2fCCPR%2fGEC%

2f6624&Lang=en

联合国大会关于电脑化个人数据文件规范指南的第 45/95 (1990) 号决议和欧盟《通用数据保护条例》（2018 年）第 51 条（监管机构）。

隐私权问题特别报告员的报告，A/HRC/31/64 (2016)。

《世界人权宣言》序言。

国际货币基金组织网站（该网站上载列了反洗钱和其他反欺诈文件）www.imf.org

国际标准化组织 http://www.iso.orghttp://www.iso.org/

国际电工委员会 http://www.iec.chhttp://www.iec.ch/

欧洲标准化委员会 https://www.cen.euhttps://www.cen.eu/

国家标准与技术研究院（美国） http://www.nist.govhttp://www.nist.gov/

欧盟《通用数据保护条例》（2018 年）第 7 条（同意）、第 17 条（删除权）、第 15 条（数据访问权）

关于言论自由的《公民权利及政治权利国际公约》第 19 条。

UNHCR"Addressing security concerns without undermining refugee protection（在不影响难民保护的情况下，解决安全问题）"http://www.refworld.org/docid/5672aed34.html

联合国人权宣言第 9 条（任意逮捕和流放自由）和第 10 条（在被证明有罪之前被认为无罪）

外交部部长在安全理事会反恐委员会特别会议上发表的联合国马德里宣言（2015 年 7 月 28 日）。

UK Biometrics & Forensics Ethics Group（英国生物识别技术和法医学伦理小组）
http://www.gov.uk/government/publications/biometrics-and-forensics-etchics-group

Biometrics Institute's Biometric Privacy Guidelines designed for international use（生物识别学会在国际范围内适用的生物识别技术隐私准则）www.biometricsinstitute.org

ISO/IEC 30107-2_2017：Biometric presentation attack detection（生物识别呈现攻击检测）.数据格式

[2] Frontex, Vulnerability Assessment and Testing for Automated Border Control (Abc) Systems (2017)（（欧盟边境管理局）自动边境控制 (Abc) 系统的漏洞评估和检测（2017 年））

[3] Ted Dunstone and Neil Yager, Biometric System and Data Analysis: Design, Evalua-tion and Data Mining (2008)（生物识别系统和数据分析：设计、评估和数据挖掘（2008 年））Springer。

ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management

systems – Requirements（信息技术 — 安全技术 — 信息安全管理系统 — 要求）

ISO 31000:2009 Risk management - Principles and guidelines（风险管理 — 原则和准则）

IEC 31010:2009 — Risk management -- Risk assessment techniques（风险管理 — 风险评估技术）

NIST SP 800-30 Guide for Conducting Risk Assessments（进行风险评估的指南）

NIST SP 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach（对联邦信息系统应用风险管理框架的指南：安全生命周期法）

ISO/IEC 17025:2017 The general requirements for the competence of testing and calibration laboratories（检测和校准实验室的一般能力要求）

3. 反恐生物识别系统和数据库

第 3 节对目前执法、边境管理和军事应用范围内的反恐生物识别系统和数据库进行了总体概述。该章节还介绍了进行生物识别数据的双边、多边分享或在区域内或全球范围内分享该等数据的好处，以及在与其他情报资料一同使用时，如何在生物识别数据作为调查工具的惯常用途之外，前瞻性地运用该等数据防止恐怖主义行为。随后，在国际人权和充分知情、需要合法和相应回应的背景下，对主管当局根据生物特征的匹配而采取的行动进行了介绍。本节最后一部分探讨了将生物识别技术纳入会员国和各地区的反恐战略的问题，以及边境和执法机构在积极支持这些策略方面发挥的重要角色。

3.1. 当前反恐生物识别系统和数据库

3.1.1. 边境应用

边境管理[50]这一日益复杂的事务在整个反恐斗争，尤其是拦截国外恐怖主义作战人员方面发挥着重要作用。运输方式在很大程度上决定了过境点 (BCP) 的运作特征和范围。就国际航空旅行而言，BCP 高度标准化。就陆路、水路和海上旅行而言，一般有两种 BCP，一种是为所有国际旅客设立的，另一个供来自边境任何一侧的国民使用。国际旅客必须向 BCP 报告，才能合法进入某一国家。供当地人使用的 BCP 一般位于陆路边界处或服务两个或更多邻国的指定港口。此类地方 BCP 通常与经济区一同运营，经济区的边界线一般位于两侧的内陆区域，长 25 公里，向来自边境两侧的所有国民开放。其他国际旅客不得使用此类地方 BCP。

位于国际边境的 BCP 充当有效的过滤器，可根据威胁级别扩展和收缩。该过滤器一般为“正常”水平，但其预警状态有时也会随威胁的升级，变为红色或橙色（或同等预警状态），在一些极端情况下，可能会完全关闭边境。在大量人口可能需要迅速进入一国（如邻国发生自然或人为灾害）的情况下，可能会开放边境，以便他们轻松进入，在这些人通过边境，抵达安全的区域之后，将进行必要的正式检查。

负责移民、出入控制和安全、执法、海关和检疫事务的机构将对旅客和货物进行进境清关。边境机构要求提供高效的运作环境，配备训练有素、积极工作的员工、先进的技术并掌握最新信息。增加生物识别应用程序是现代 BCP 的重要元素，该应用程序为边境管理流程提供了极大帮助。其构成更广泛技术方法的一部分，该方法涵盖跨境旅游的方方面面，从最初组织旅游的那一刻到游客抵达和最后离境。此过程各个阶段收集的信息由不同来源进行整理，并提供给边境管理人员，以便其根据该等信息和其他信息，决定是否允许相关旅客进入该国。

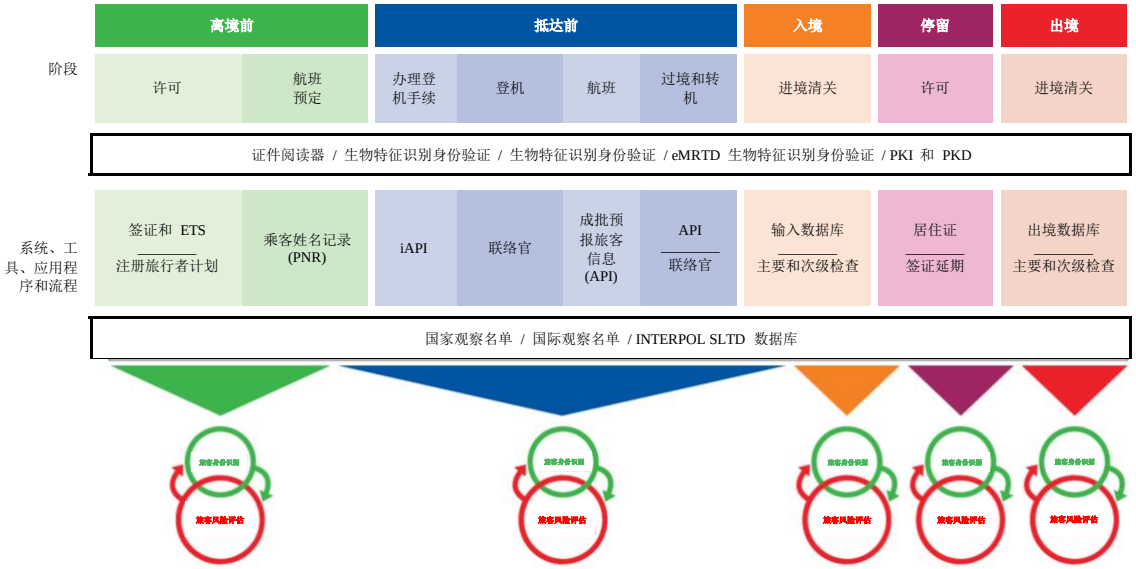
国际航空旅行是发展最为迅速的领域，该领域过去促进了基于标准的技术创新，该技术创新随后被运用到陆路和海上边境。这一存在已久的模式可能会继续运用于生物识别技术的新兴应用中，以对恐怖分子进行识别。为国际航空旅行建立的现代化进境清关体系结构，使得随着目的国或出发国获

[50] “边界”通常指两个国家的领土和海域之间的分界线，“边境”则指进入某一国家所需要通过的地方。它们有时完全重合，但在更多情况下，边境包括基础设施，如移民检查点、海关设施、设有围栏并派人巡逻的越过边境的道路；如果设在国际机场和海港，边境可能位于距边界数百公里的位置。本质上，边界是一条界定线，而边境通常更为复杂，包括若干线条和/或区域，其主要功能是对人员和货物的流动进行管理。”*英国杜伦大学 Martin Pratt 教授*

得额外信息，相关机构可以在旅客的整个旅行过程中不断进行旅客身份识别和风险评估。国际航空旅游旅客数据的主要来源是航空公司和政府，生物识别技术应用方面的新兴解决方案将维护这两个数据来源。

图 4 — 旅行连续统一体的不同阶段[51]

（获得国际民用航空组织 (ICAO) 许可）



从目的国的角度来看，此端对端的流程分为五个阶段（参见图 4）：

1. 离境前
2. 抵达前
3. 入境
4. 停留
5. 出境

但从整个系统和国际角度来看，旅行是一个连续统一体，因为从旅游开始的国家离开的流程对该次旅行的过境和目标国而言，是抵达前流程。

阶段 1：离境前

现如今，许多国家要求所有旅客在抵达边境前提前提供信息。该信息主要包括详细个人信息、证明文件和旅行数据。各国也越来越需要旅客提供生物特征信息，以便确认入境外籍人士的身份。以前，这些旅客可能会被分为两类，即需要签证和无需签证进入某国的人。自 20 世纪 90 年代以来，就一直以预报旅客信息 (API) 和互动式 API 的形式向各国提供航空公司离港控制系统数据。现在，各国会通过一系列机制在旅行开始前收集旅客的信息。目前，可使用以下流程和系统，收集必要的抵达前信息：

1.a.“经典”签证申请 — 许多国家通用的要求，以历史、人口和经济因素以及相关国家的政治关系为

[51] 请参阅“ICAO TRIP Guide on Border Control Management (2018)（ICAO TRIP 蒙特利尔边境控制管理指南（2018 年））”，获取更多详情。

依据。该流程通常要求申请者通过综合申请流程提交个人资料和生物特征身份属性，需要在综合申请流程中，向目的国的外交官员或代表提交旅行证件并缴纳一笔费用。生物特征识别资料可以是一张面部照片，也可以是一组指纹等注册信息。随后将对该申请进行审查，之后会签发或拒签签证。在签发前的审查流程中，可能对就此目的编写数据集的国家的生物特征观察名单进行 1:n 搜索。

1.b. 地区签证申请 — 各国经常会开展区域性的合作，每个大州至少都有一个区域性实体，例如东南亚有 ASEAN[52]、西非有 ECOWAS[53]，欧洲有 EU、南美有 UNASUR[54]，加勒比地区有 CARICOM[55]。该等实体之间的合作水平各不相同。此类地区体系的一个示例是欧盟，其采纳了一项条例，该条例要求所有成员国实施本国的签证信息系统 (VIS)。该等系统与中央 VIS 枢纽相连，后者由负责对大型 IT 系统 (eu-LISA) 进行操作管理的欧盟机构进行管理。VIS 采用面部照片和十根手指的系列指纹的形式进行生物特征检查，以在边境对旅客身份进行验证，其还通过申根信息系统 II (SIS-II)[56] 和国家数据库进行个人信息核验。该等地区系统的结构使得有可能在签发前进行审查，该审查要求对就此目的编写数据集的国家的生物特征观察名单进行 1:n 搜索。

1.c. 外包应用程序 这种模式在许多国家越来越受欢迎，其利用商业提供商收集并整理所有申请人的证件和签证申请过程中需要的信息。还可能会在此业务过程中登记申请人的生物特征（人脸图像、虹膜扫描图和/或指纹）。完整申请将转发给适当的外交官员，以便其进行必要检查并决定是否签发签证。可能需要在签发前的审查流程中，将生物特征图像或模板提交给相关国家，以便其对就此目的编写数据集的国家的生物特征观察名单进行 1:n 搜索。

1.d. 在线/电子签证申请 该申请程序完全在网上通过申请人的电子表格和相片扫描图像（根据 ICAO 要求）和护照个人信息页进行。将集中进行决策流程和任何生物特征审查。如果签发签证，将向申请人发送确认信息，且将通过对比申请人的面部和提交的相片，确认申请人和旅客是同一人，进而在边境进行 1:1 的生物特征核实。在签发前的审查流程中，可能对就此目的编写数据集的国家的生物特征观察名单进行 1:n 搜索。

1.e. 电子旅行系统 (ETS) 将在此过程中收集旅客的基本身份数据，无论签证作出何种要求。其操作与在线/电子签证类似，但是除面部照片以外的生物特征信息都是在边境而非离境前阶段获得的。

旅行开始前，旅客数据的另一主要来源是航空公司收集的数据：[57]

1.f. 旅客姓名记录 (PNR) 系统 旅客获得签证/旅行授权后，接下来将需要通过在线填写 PNR 信息以预订机票。PNR 数据存储在航空公司的电脑订票系统 (CRS) 中，以便航空公司用于商业和操作目的，但也用于在旅客离境前将该等数据提供给边境机构。WCO 与 IATA 和 ICAO 一同制定并维

[52] ASEAN：东南亚国家联盟
[53] ECOWAS：西非国家经济共同体
[54] UNASUR：南美洲国家联盟
[55] CARICOM：加勒比共同体
[56] eu-SIS-II 为申根公约签署国家在欧洲地区的公共安全、边境控制和执法合作提供支持。各国将分享警方数据库和边境观察名单中的信息。该等信息在国内和边境均可获取，亦可用来对进出欧盟的人员进行检查。该系统中包含与通缉和失踪人员、遗失或被盗身份/旅行证件、生物特征、被盗车辆等相关的数据。

[57] 就 PNR 和 API 而言，“Chicago Convention（芝加哥公约）”附件 9（第 15 版）在第 9 章“Passenger Data Exchange System（旅客数据交换系统）”中收集了标准和推荐做法。世界海关组织 (WCO)/国际航空运输协会 (IATA)/国际民用航空组织（ICAO） 在《PNR 准则》（第 9944 号文件）和《API 准则》中共同确定并商定了标准电子信息（包括数据集）。

护有关航空公司操作人员和政府之间协调统一的 PNR 数据交换的技术标准 (PNRGOV)[58]。*PNR 记录中不含任何生物特征数据。*PNR 数据的价值在于，其提供了重要的背景信息，可提高身份的可靠度，并告知基于风险以相关旅客为目标的相关信息。

阶段 2：抵达前

2.a. 在航空公司离境控制系统中创建*预报旅客信息 (API)*。API 是在办理登机手续时逐步编写的，但此信息只会在所有旅客办理完登机手续、登上飞机且机舱门关闭后发送给指定政府机构。很重要的一点是，API 将在连续长途航班的转机站进行完善。API 使用以下两个数据来源：(1) 旅客护照机器可读区域 (MRZ) 提供的信息；(2) 航班详情和登机信息，可同时包括标准和额外数据元素，如托运的行李、座椅号、搭乘航班的旅客人数、航班号以及离境和抵达日期、时间和地点。这使得接收机构可以在所有乘客抵达前对其进行预先检查。在 API 数据传输方面的当前现有标准*并未纳入生物特征数据，但是将来可能通过护照/旅行证件从非接触式芯片中收集符合 ICAO 要求的照片。这要求在登机柜台或终端处安装电子护照阅读器，目前，并不是所有国家都掌握了此项技术。*

2.b. 互动式预报旅客信息 (iAPI) 这是 API 的增强版本，因为其在办理电子登机手续时，向指定接收机构转发旅客信息。该等信息是单独而非批量（如同在 API 流程中那样）发送的。通过 iAPI 流程，可以在旅客登机前完成观察名单和其他检查，因此，为飞机、飞机上的乘客和目的国提供了额外保护。*生物特征要素可能与上述 2a 段中的 API 相似。*

案例研究 5 — 在不出示旅行证件的情况下入境

目前正在考虑一项对澳大利亚和新西兰之间的旅行使用下一代自动边境控制 (ABC) 闸门的计划。该项技术将升级现有 iAPI 系统，并将护照上的人脸图像与签证数据库中的人脸图像相联系，进而为所有搭乘航班抵达的旅客建立动态的预期抵达数据库。在此应用程序中，电子护照一直装在乘客的口袋里，ABC 生物识别闸门会将旅客的人脸图像和预期抵达数据库中的图像进行对比，只有在两张图像一致的情况下才允许进入。小范围内的 1:n 生物特征识别技术的应用是一项正在开发中的解决方案。

许多国家在进行抵达前筛查的同时，还部署了联络官（即来自目的国的政府官员）在航空公司的登机处和过境机场协助进行旅客身份识别和风险评估工作。

阶段 3：入境

旅客只能在成功填写抵达前协议后，才能开始踏上旅程。但对大多数司法管辖区而言，完成阶段 1 离境前流程和阶段 2 抵达前流程都无法保证在抵达时能进入相关国家。边境官员将在旅客抵达时出示所需证件和凭证后作出最后决定。移民官员的决定必须基于多种因素，并且已经开发出边境管理信息系统 (BMS) 来辅助此过程。但应注意，某些国际 BCP 目前并未掌握 BMS 技术。BMS 在其功能的复杂性方面差别很大。在技术更加先进的司法管辖区，生物特征身份验证技术正在发展之中。使用生物特征观察名单变得不那么常见了。主要的变体包括：

3.a 标准边境管理信息系统 (BMS) 国家法律和法规对边境检查的数量和类型（例如是否记录进入某一国家的所有旅客的详细信息，还是只对观察名单或制裁名单进行搜索）进行控制。记录所有乘客抵

[58] PNRGOV EDIFACT 和 XML 信息实施指南：www.wcoomd.org/en/topics/facilitation/instrument-and-tools/tools/api-pnr.aspx

达情况的国家必需配备某一形式的 BMS。可以手动输入数据，但大多数现代系统使用护照阅读器上传旅行证件机器可读区域提供的数据，且边境官员将输入与身份、访问时长和原因以及在相关国家的地址等有关的额外信息。随后，将在观察名单中搜索该等数据。*标准 BMS 并不会捕获生物特征数据用于自动验证。*

3.b. 电子边境管理信息系统 (e-BMS) e-BMS 使用电子护照阅读器访问机器可读的电子旅行证件 (eMRTD) 中嵌入的非接触式芯片[59]。该芯片中含有 MRZ 数据以及符合 ICAO 要求的人脸数码照片，通常还含有两个指纹。在一些国家，只能在 e-BMS 中含有签发国家颁发的、允许打开包含指纹数据组的电子证书的情况下，才能获取该等指纹用于验证目的。为验证芯片中嵌入的生物特征所提供的身份，必须将 e-BMS 连接到生物识别系统，且 e-BMS 必须能够使用人脸相机、红外线虹膜相机或指纹扫描仪捕获旅客的生物特征，以与芯片中的数据进行对比。eBMS 支持使用从电子护照读取的生物识别特征图像对生物特征身份验证进行 1:1 检查。eBMS 可能要求对就此目的编写数据集的国家进行生物特征观察名单进行 1:n 搜索。

恐怖分子可能会使用伪造的旅行证件跨境旅行而不被察觉。其使用的策略包括使用替代相片或与其长相相似人员的护照，以及创建完整文件的伪造复印件。因此，连入集成生物识别系统的独立型电子护照阅读器在打击护照欺诈行为方面是有价值的证件审查工具，对于打击这类欺诈行为方面资源有限的 BCP 尤其如此。在次级设施中安装此类设备，可为负责对证件首先引起 BCP 怀疑的旅客进行调查的边境官员提供极大帮助。

案例研究 6 — 逻辑数据结构第 2 版

最新开发的逻辑数据结构 (LDS) 第 2 版使获取电子护照中存储的额外生物特征变得更加便捷。LDS 存储在电子护照或旅行证件的非接触式芯片中，且可与含有称为数据组的 16 个抽屉的“橱柜”进行对比。部分信息的存储是强制性的，但对其他信息的纳入则是可选的，各国可酌情决定是否纳入。数据组必须遵守 ICAO – PKI[60] 结构。这可以确保 LDS 中包含的数据是由真正的主管当局签发的，且未经更改或撤销。LDS-2 在 LDS 结构中加了三个或更多要素，分别是：(1) 旅行记录、入境和出境盖章；(2) 签证记录；和 (3) 其他生物特征数据。可根据签发机构的酌情决定，在签发新护照时将 LDS-2 存储在电子护照的非接触式芯片中。

这意味着签证和边境控制机构现在可以在其他国家的非接触式芯片中写入与三个新的数据组相关的信息。然后，可由边境控制机构对旅行记录进行存储，同时以电子方式在护照上盖章，签证详情可由指定机构直接输入到数据组中，且可以在抵达边境时对此类信息进行电子验证。加入注册旅行计划的旅客可要求将相关生物特征模板存储在电子护照中，以便在加入此计划国家的 ABC 闸门处进行使用。

注：在非接触式芯片中写入新数据的法律条件是电子护照发行机构和希望添加数据的国家之间交换了 ICAO-PKI 证书。除非满足这一法律条件，否则无法使用 LDS-2。

[59] eMRTD — 拥有内嵌的非接触式集成电路、且能够用于根据 ICAO 第 9303 号文件中规定的标准对 MRTD 持有人的生物特征身份进行识别的一种机器可读的旅行证件 (MRTD)（护照或卡片）

[60] ICAO 将 PKI（公钥基础设施）界定为一套政策、程序和技术，旨在对安全应用程序的用户进行验证、登记和核证。PKI 采用公开密钥密码学和秘钥证书的做法，确保通信安全。

3.c. 电子边境和生物特征管理信息系统 (e-2BMS) 此系统与 e-BMIS 类似，但并不使用电子护照阅读器，因为生物特征数据在边境处通过签证系统进行登记。该系统的优点是整个生物识别程序由目的国所有，且该系统使相关官员能够对登记质量进行控制，以使生物特征验证 1:1 匹配系统发挥最大性能。例如，美国可通过采纳此架构，对照美国政府为所有抵达的外国护照持有人编制的大量观察名单记录，对 1:n 生物特征观察名单检查进行整合。

3.d.自动边境控制系统 (ABC) — 近几十年来，国际旅客人数呈指数式增长，这一现象推动了边境处的技术创新和自动化。自从荷兰在斯希普霍尔机场引入首个自动边境控制系统后，ABC 系统遍布全球，目前，已成为许多国家的常规工具。该系统的现代迭代版使用高速传感器和存储在旅行电子证件芯片中的生物特征（如人脸、虹膜、指纹），对生物特征 1:1 验证进行完善，以使旅客能够从边境闸门自动入境。这使得预先获得资格的国民或获得优先权的群体能够大量、迅速通过 BCP，而将延误时间降至最少，减轻边境管理的压力，使其能够集中精力对可能需要更仔细的检查的其他旅客进行检查。由国家或地区机构在任何指定时间根据当前风险评估和相关法规，决定哪些国籍的人士或群体可能需要使用 ABC 闸门。ABC 解决方案可能要求对就此目的编写数据集的国家进行生物特征观察名单 1:n 搜索。

阶段 4：停留

各国有责任对可能短暂拜访、停留较长时间或在其边境处居住的非该国国民进行管理。根据国家法律和法规，这项任务可能需要不同的当局和机构负责，但其职责类似，如颁发居住和学生许可、处理难民和庇护申请者以及入籍申请，还有执法责任（如处理人员非法逾期停留、人口贩卖和劳动力剥削罪行等）。

在此方面有一个典型的示例，即上述第 1.b. 段中所述的欧盟 eu-VIS 和 eu-SIS-II 系统。利用这些数据库，欧盟国家的所有适用机构均能够在其各自的边境之内对外籍人士进行管理。此外，还有 Eurodac（欧洲指纹数据库，一个集中式的欧盟数据库），可收集并处理寻求庇护者的数字化指纹。目前，有 28 个欧盟国家以及挪威、冰岛、瑞士和列支敦士登在使用此数据库。Eurodac 处理、存储和/或对比年满 14 周岁且符合以下条件的第三国国民或无国籍人士的指纹：(1) 申请任何加入 Eurodac 的国家的庇护，或 (2) 因非法通过外部边境被捕，或 (3) 被发现非法出现在 Eurodac 国家。Eurodac 在执行《都柏林规则》方面亦发挥重要作用。该法规对寻求庇护者的申请作出规定，旨在防止有人在多个欧盟国家作出多重庇护申请。制定该法规的主要目的是为单个成员国分配处理庇护申请方面的职责，通常分配给寻求庇护者最开始进入欧盟以进行后续处理的国家。自 2015 年 7 月以来，执法机构对 Eurodac 进行访问方面的权限受到了限制，需要在极为严苛条件的约束下才能进行目标指纹的搜索。该等搜索只能逐案进行，且只能进行搜索用于特定严重罪行和恐怖主义罪行的预防、侦查和调查目的。

在适当调查或情报收集的背景下，可与执法和安全机构分享边境机构在更早的旅行阶段收集的生物特征数据。

阶段 5：出境

离境前流程与抵达前的方案类似。旅客需要在登机前在线或在机场办理登机手续，并出示其证件。许多常见的旅客计划，如“注册旅客计划”，对 ABC 系统作出补充。这些计划要求旅客注册会员，登记生物特征数据，有些计划还包含审查流程。例如，美国有全球入境计划，该计划允许在通过美

国边境时，对预先批准的低风险旅客进行快速放行。计划会员前往指定的全球入境自助检查机，出示其机器可读的护照或美国永久居民卡，在扫描仪上录指纹进行指纹验证，并填写报关单。自助检查机为旅客出具交易收据。旅客必须取得全球入境计划的预先审批。必须在注册前对所有申请者进行严格的背景审查和当面访谈。

尽管并非所有国家都进行离境时的移民出境控制，但许多国家仍会对离开该国的旅客进行检查。这通常包括检查登机牌上的姓名是否与旅行证件上的一致，在生物特征观察名单中搜索姓名，以及检查航班详情是否与当日的日程相符及旅客是否逾期逗留。除以上检查外，他们还对旅行者进行评估，根据旅行证件、登机牌和其他具体标准，寻找毒品和现金运送者，被贩运到其他国家的人，特别是外国恐怖主义战斗人员。

案例研究 7 — 离境生物特征验证

在美国有一种模式正在兴起：航空公司、机场和政府共同投资，在登机门处采取便利化措施，以提供获取离境生物特征验证的替代机制。2018 年初，德国汉莎航空和英国航空利用人脸识别开展试验。这是对已知旅客进行 *1:n* 生物特征验证的进一步应用，与澳大利亚和新西兰在航空公司和政府合作中制定的安排类似（参见案例研究 5）。

3.1.2 维持治安和 INTERPOL 应用程序

维持治安时使用的生物特征数据库通常包括被捕者参考数据库（人脸图像、指纹和 DNA 图谱）、犯罪现场数据和其他来源不明的数据，如失踪或已故人士的调查或情报收集活动的数据。该等系统可在本地、本省或本国运行，以实现保留犯罪记录、进行犯罪调查或生成法医情报产品等功能。可将恐怖主义调查过程中生产的生物特征数据添加到该等系统或上传到指定的数据库，作为额外安全措施。无论使用何种数据库配置，由于恐怖主义行为和一般罪行可能会交叉（例如，个人为了对恐怖主义活动提供特别资助而犯下欺诈或金额较高的盗窃罪行等），操作时，可能需要在所有系统中进行搜索。*该等数据库最好还应该能够与边境生物特征应用程序进行互相操作（如果国家法律允许）。*

国际警察可以通过双边、多边或区域性协议交换生物特征数据，但唯一的全球性官方方法是通过国际刑警组织（ICPO 或更常见的叫法为 INTERPOL），该组织可促进国际警务合作。应注意，向 Interpol 数据库贡献数据的国家：

1. *保留对其数据的所有权*，且可以随时要求将数据从数据库中删除（参见第 3.3.2.节单向搜索）。
2. *负责确定搜索数据的范围*，即其搜索的数据和提交的数据不会暴露在指定国家的生物特征数据中

INTERPOL 有三个可供其 190 个成员国使用的生物特征数据库：

人脸 — 提供以下功能：

- 识别逃犯和失踪人员
- 识别未知的相关人员
- 识别公共媒体图片中的主体

- 对照数据库对收到的“面部照片”（托管图像）进行验证 (1:n)。

指纹 — AFIS 闸道。该系统使来自成员国的获授权执法官员能够远程访问数据库，并使用 I-24/7 Interpol 安全全球通信网络获得自动回复。该数据库中包含参考数据（指纹和掌纹）和犯罪现场数据（指印和掌印）。

DNA — DNA 闸道（运行方式与 AFIS 闸道类似）。INTERPOL 已就 DNA 数据的处理规则与所有成员国进行商定，数据库由下列四个部分组成：

- 未解犯罪现场
- 已知罪犯
- 失踪人员
- 未确定身份的人体残骸

INTERPOL 还提供 DNA 双边匹配器服务，该项服务为两国间的 DNA 搜索和对比提供私人平台。该项安排以共同信任、警务战略、相容的法规和互相协定的匹配标准（如最低地点数量）为依据。DNA 图谱由各国进行选择并安全发送到 INTERPOL。告知双方发现的任何匹配且随后将相关数据从系统中删除。各国可使用此工具进行一次性对比，或将其用作常规匹配操作的一个环节。

收集外国恐怖主义作战人员和其他恐怖分子的生物特征数据，以防止其跨过边境是 INTERPOL 生物特征数据库的一项重要功能。这为 Interpol 全球系列反恐战略行动提供支持，该行动的首要任务是对已知跨国恐怖组织的成员进行身份识别。

3.1.3 INTERPOL 生物特征数据库：监督和管理

由 Interpol 文件控制委员会 (CCF) — 一家独立机构对 INTERPOL 生物特征数据库的内部管理和运行进行监督。其具有三项功能：

1. 确保 INTERPOL 进行的个人数据处理符合该组织的规例。
2. 向 INTERPOL 提供与涉及个人数据处理的任何事项相关的建议。
3. 处理与组织文件中包含的信息相关的请求。

当第 77 届联合国大会于 2008 年就修订《宪法》，以将 CCF 纳入其内部法律结构，进而强化其地位进行投票后，CCF 成为该组织的官方机构。2016 年 11 月，Interpol 大会采纳了一套与 Interpol 监督机制有关的改革方案，包括采纳新的 CCF 法规，该法规对其组成、结构和程序进行了深刻改革。这一新的法律框架于 2017 年 3 月 11 日生效，强化了该委员会的监督和咨询功能，同时增强了其针对可能在 INTERPOL 档案中处理的有关个人数据提供有效补救措施的能力。

3.1.4 生物特征和个人资料观察名单数据的管理

观察名单是根据各类数据建立的一种预警系统，在国家，有时也在地区层面运行。其旨在提供预警和检查程序，进而为过境点的罪犯、恐怖分子和可疑物品或材料的识别和身份识别提供帮助。观察名单可分为以下类别：

- *个人资料观察名单：*与通缉或失踪人员、相关人员、飞行禁令等相关的信息。
- *生物特征观察名单：*常见模态包括指纹、人脸图像和虹膜（DNA 目前尚未广泛使用），且与个人资料观察名单的功能类似，即提供通缉或失踪人员、相关人员、已知或可疑恐怖分子等相关信息。
- *观察名单中含有与物品和证件相关的信息：*盗窃车辆、遗失和盗窃旅行文件[61]、盗窃艺术作品等。
- *观察名单中包含与犯罪手法或危险物品识别相关的信息：*用于实施某一罪行或系列罪行而使用的特定方法、假币或旅行证件的新识别方法、制造非法药物时使用的方法和化学成分等。

此外，国际和地区执法机构（如 INTERPOL[62] 和欧洲刑警组织 (EUROPOL)[63]）以及非执法机构也使用观察名单，进行其他方面的应用，因此，其用户范围较为广泛：

- *执法：*
  - 国际[64]；INTERPOL[65]。
  - 区域：EUROPOL[66] 和其他区域性组织
  - 国家[67]：警务、移民、海关等
- *国际组织*
  - 联合国 (UN[68]) 等
- *公共组织，*
  - 护照签发机构、[69]驾照签发机构等
- *私人/商业组织，*
  - 航空公司、保险公司、食品制造商等

非执法机构在其职责或业务范围内使用观察名单，对其产品和流程进行保护，并防止出现欺诈行为。

3.2 个人资料观察名单限制

大部分执法观察名单根据个人的个人信息（如姓名、出生日期等）制作。该等信息可能并不可靠且可能发生变更或存在错误。一些常见的示例包括：

- 姓名拼写错误或翻译错误
- 使用变更的姓名或别名，而非旅行证件中的正式姓名。
- 出生日期错误或数字顺序不正确，如将 01-12-1967 误写为 12-01-1967

[61] 参见：https://www.interpol.int/INTERPOL-expertise/I-Checkit
[62] 参见：https://www.interpol.int/
[63] 参见：https://www.europol.europa.eu/
[64] 参见：ICAO TRIP Guide on Border Control Management（ICAO TRIP 边境控制管理指南），第 1 版第 5-M 章
[65] 参见：https://www.interpol.int/INTERPOL-expertise/Databases
[66] 参见：https://www.europol.europa.eu/activities-services/services-support/information-exchange/europol-information-system
[67] 参见：ICAO TRIP Guide on Border Control Management（ICAO TRIP 边境控制管理指南），第 1 版第 4-M 章
[68] 参见：https://www.un.org/sc/ctc/
[69] 参见：https://www.consilium.europa.eu/prado/en/check-document-numbers/check-document-numbers.pdf

- 主体拥有双重国籍
- 主体变更其姓名并取得新的身份或旅行证件
- 主体出示使用其他姓名的伪造、假冒或以欺诈手段获得的旅行证件
- 主体出示其他人士的真实旅行证件，企图冒充原证件持有人
- 主体使用“变换”的相片（即由两张人脸合成的图像）与某人分享旅行证件（参见第 2.3.2. 节）
- 双胞胎或多胞胎互换身份和/或旅行证件

因此，对主体积极进行身份识别至关重要，因此创建了生物特征观察名单。

3.3 生物特征观察名单

生物特征观察名单在边境处进行的 1:1 生物特征验证流程中发挥了另一项作用。进行 1:1 核验（参见第 3.1 节）时，使用存储在电子旅行证件芯片中的生物特征数据，对抵达边境的人员的身份进行验证。观察名单概念来到了另一阶段，其引入了 1:n （一对多）搜索功能，以对照相关个人的生物特征数据库对旅客的生物特征数据进行核查。这两项流程都需要使用类似的生物特征注册设备，但数据库将需要 1:n 搜索软件以及 1:1 匹配软件，以便在需要时执行其中一项或两种任务。这显然需要额外投资。观察名单 1:n 搜索的有效性取决于以下因素：

- 登记数据的质量
- 存储在数据库中的数据的类型
- 系统性能（参见第 1.1 节）
- 系统是否容易遭受使用变形或欺骗技术实施的呈现攻击的威胁（参见第 2.2 节）

较长的国际和区域观察名单的示例包括：

INTERPOL I-24/7 — 可通过接入所有 INTERPOL 国家中央局 (NCB) 的 I-24/7 网络实时访问所有 INTERPOL 数据库，不包括 INTERPOL 导弹信息网络 (IBIN)。该系统已连接到 INTERPOL 通知系统，以就逃犯、犯罪嫌疑人、与正在进行的犯罪调查相关联或有关的人员、受到联合国安全理事会制裁的人员和实体、潜在威胁、失踪人员和死者实体发布国际警报。

EUROPOL-EIS Europol 信息系统 — 此数据库中含有涉及所有 Europol 授权犯罪领域，包括恐怖主义活动的犯罪和情报信息。

案例研究 8 — ETIAS

欧盟委员会提议建立欧洲旅行信息和授权系统 (ETIAS)[70]，以增强根据免签证协议到申根区旅行的安全性。ETIAS 观察名单将由 Europol 负责创建和管理，该份名单中包含以下人员相关的数据：涉嫌犯罪或参加犯罪行为的人员；或者有事实迹象或合理根据使人相信其将犯下罪行的人员。
观察名单将根据下列因素创建：

1) 联合国制裁委员会名单

[70] http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU%282017%29583148

2) 由成员国提供的与恐怖主义罪行或其他严重罪行相关的信息
3) 通过国际合作获取的与恐怖主义罪行或其他严重罪行相关的信息

3.3.1 反恐生物识别应用程序的好处

3.3.1.1 国家边境以内

自从首个指纹分类和搜索系统在 19 世纪 90 年代运用以来，生物特征数据库在犯罪调查方面发挥着越来越重要的作用。20 世纪，人类在计算机化和科技方面取得了长足发展，这极大提高了该等系统的效率和处理能力，并且拓宽了可供使用的模态（如人脸、DNA、语音等）的范围。当前，许多执法机构使用的生物特征搜索系统都以算法先进、复杂为特点，这有助于对大量数据进行快速、准确搜索。但与其他调查和情报收集流程相比，犯罪侦查数据库具有一项巨大优势，即全年每天 24 小时提供监测服务，只要数据还保留在数据库中。如果匹配的数据已经在数据库中，就可以在进行数据登入和搜索后，找到匹配的选项，或者也可以在系统中提交数据，在数周、数月、数年，甚至是几十年后，生成匹配选项。因此，犯罪侦查数据库搜索被认为是最具有成本效益、且可供现代调查人员和情报分析师使用的始终有用的资产之一。数据库还可以

1. 在国家层面上进行整合，使得无论国家的实际规模和相对人口如何，都能够有效覆盖整个国家
2. 被设置成可与生物识别系统进行相互操作，和
3. 连接到国际或其他相关生物特征数据库。

实时法医调查

许多国家的执法机构已开发出此生物识别技术，并对其加以利用，以确定犯罪分子的身份，并确认其犯罪历史并且对嫌疑人参与到犯罪和连环罪行进行证明或反驳。事实证明，该等数据库在恐怖主义调查中尤其具有价值，近年来，随着“实时法医调查”的出现，其发挥了更大的作用。此流程中运用从犯罪现场（例如从电子设备或照片中检索到的面部图像，快速分析的 DNA 样本图谱）或以电子方式直接从犯罪现场将指印数字图像传输到 AFIS 的过程中快速恢复和生成的可搜索法医数据，进行即时搜索。现在，可以在犯罪现场检查仍在进行时搜索并对比在证据方面十分重要的生物识别材料，且这一现象变得越来越常见。此过程中可能会生成法医情报。可利用该等情报，在调查早期，迅速识别嫌疑犯或为调查人员创建或更改动态调查线索。在恐怖主义调查中，可利用此项功能，在事件发生后，立即识别出更多嫌疑犯或同伙人员，并防止进一步袭击。在实时搜索的生物特征数据池的范围尽量最大的情况下，此项功能显然会得到进一步增强。

在“自杀性爆炸”中，轰炸者的尸体残骸可能会与受害者的尸体残骸混在一起，数据库在处理这一爆炸事件的余波时非常有用。在该等情况下，有必要尽快确定轰炸者的身份，以使调查取得进展并防止进一步袭击，同时，还要代受害者家人尽快确定受害者的身份。DNA、指纹和牙科学（法医牙科学）是使用的主要生物特征，因为该等特征是用于识别灾害受害者身份的主要身份标识[71]。

[71] 灾害受害者身份识别 (DVI) 是一项国际认可的程序，其恢复并确认大规模死亡事件的受害者身份，并且在此过程中为死者亲友提供支持。该程序由执法人员负责进行，且可通过加入 Interpol DVI 委员会，对该等流程进行国际层面的商定。Interpol 可能还会在发生大型、复杂国际事件的情况下，提供直接协助和协调。

3.3.1.2 跨越国家边境

如上文所述，在边境处进行的生物识别干预分为以下两类：

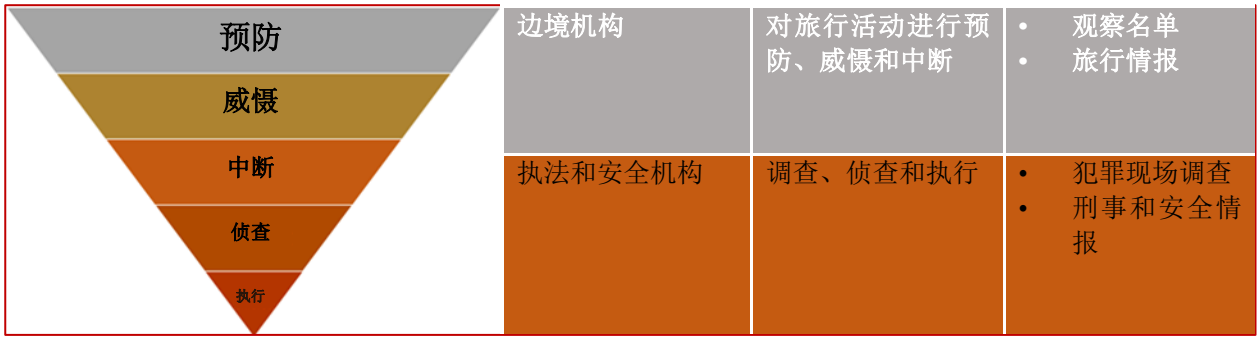
(1) *生物特征身份验证 (1:1)* — 将在边境处从旅客获得的生物特征与存储在旅行证件（如电子护照）等地的生物特征进行对比

(2) *生物特征观察名单搜索 (1:n)* — 通过含有相关人士（如执法机构通缉的人员或已知或可疑恐怖分子等）生物特征的观察名单，对在边境处从旅客获得或从其电子护照或旅行申请文件上获得的旅客生物特征进行搜索。

各流程通过身份管理来改善旅客风险评估。[72]最佳的配置是跨边境运行两个流程。将在边境身份验证过程中，对照记录和认证的生物特征对旅客的身份进行识别，但生物特征观察名单搜索可能会显示已确认的身份为相关主体。此方法要求增加投资，但该等投资所带来的保障和安全性的增强，通常将证明额外投资是值得的。

图 5 — 改编自*"ICAO TRIP Guide on Border Control Management (2018)（ICAO TRIP 蒙特利尔边境控制管理指南（2018 年））"*

（获得国际民用航空组织 (ICAO) 许可）



观察名单的长度和内容复杂性可能有所不同一些生物特征观察名单将由从特定类别的相关个人获取的参考数据的独立数据库组成。其他生物特征观察名单可能会添加选择的犯罪现场生物特征数据，以扩大其范围。但对观察名单这一概念最广义的解释是，如图 5 所阐释，以合法的方式将所有国家执法生物特征数据（参见第 3.3.2 节）整合到"国家观察名单"配置中。这将使最大数量的相关数据暴露在观察名单搜索中，且将为出行的公众和国家安全提供最大程度的保护。但可能存在国家法律和监管方面的限制，使该解决方案无法实施。

3.3.1.3 国家边境以外

国家可能会有资产位于海外，这些资产被认为容易遭受恐怖袭击。生物特征可能构成任何威胁缓解计划的重要环节。例如，其可能要求对在母国所拥有的场所（如大使馆）工作的东道国人员进行检查。这可能要求两国进行合作，最好在两国的数据库中搜索生物特征和个人数据方面达成法律协议，以确定相关员工无犯罪记录或与任何一国的恐怖主义行为均无已知关联。同样，如果东道国的国民在母国境内从事恐怖主义活动，则两国均将从互相交换和搜索生物特征数据中受益，从而首先保护

[72] 请参阅"ICAO TRIP Guide on Border Control Management (2018)（ICAO TRIP 蒙特利尔边境控制管理指南（2018 年））"，获取详情

母国的海外资产（如商业运营、外交场所和活动等），其次，协助东道国识别任何涉嫌参加恐怖主义活动的国民身份，并对其遣返事宜进行管理。第 3.3.2 节对此形式的双边合作和其他数据交换选择进行了概述。

3.3.1.4 军事来源的生物特征数据

一些国家动用军事力量打击其国家境内或海外的恐怖主义行为。在这类部署过程中，生物识别数据被经常用于揭露可能试图藏匿在当地人口中，或混入该等人口中，以躲避侦查或将该等人口作为“人体盾牌”的恐怖分子的身份。军事部队所用的技术可能与执法机构使用的技术相似，如使用移动或静态生物特征捕获设备，获取可疑恐怖分子的参考样本；或对从事与恐怖主义或叛乱活动有关的居留者或相关地点找到的物品进行法医学鉴定。

从此类军事活动中获取的生物特征数据还可能对与其恐怖主义调查相关的执法机构具有重大价值，但在该等数据的分享和使用方面可能存在较大限制，这在很大程度上取决于：

- 根据国家法律和国际人权法进行相关生物特征数据交换的法律机构
- 军事生物特征数据和民事法庭中的其他证据的可采纳性
- 该国民事机构使用的军事生物特征质量标准和法医学质量标准是否相容

因此，尽管数据交换合法，相关数据也可能不符合规定的法律标准，因而无法被采纳为证据，即使该等数据具有重要的情报价值（参见第 3.3.3.）。

案例研究 9 — 恐怖分子爆炸装置分析中心

美国联邦调查局恐怖分子爆炸装置分析中心 (TEDAC) 是此类功能的一个示例。TEDAC 负责协调整个政府的工作，从执法、情报到军事工作，以收集并共享与简易爆炸装置 (IED) 的拆除及破坏设备、战略、技术和程序相关的法医学数据和情报，并将该等数据和情报与其制造商相关联，最重要的是，防止未来出现袭击。迄今为止，TEDAC 已收到 50 多个国家提交的超过 100,000 个 IED。生物识别分析单元 (BAU) 通过及时、高质量的法医潜在指纹和 IED 资料 DNA 检查帮助美国政府和国际合作伙伴在全球范围内打击和战胜 IED 威胁，产生可用于调查的可使用情报。

3.3.1.5 确保提供共同保护

只有各国开展合作并共享数据，生物识别系统才能在追踪和侦查恐怖分子方面发挥充分作用。一个国家可以在边境之内以及跨境设有综合、有效的国家生物识别系统，甚至可以加入复杂的地区性网络，但如果其无法从该国家和区域性网络以外的其他国家访问恐怖主义数据，则仍可能容易受到攻击。国家、双边和区域性数据分享（参见第 3.3.2. 节）提供部分解决方案，但必须在全球范围内对恐怖主义生物特征数据进行国际共享，进而为所有国家提供共同保护。这还将有助于震慑暂时可能将根据地设在具有较低或无生物识别能力国家的恐怖分子并破坏其活动，使其采用新的身份或获取伪造的旅行证件，以隐埋身份的方式前往其他目的国。必需建立强大的国际生物特征数据综合共享系统，以应对这些战略并揭露恐怖分子的身份，或者不让其有开展相关行动的“安全港”。

Interpol 生物特征数据库是此类全球能力的典型示例。该数据库旨在通过允许各国共享与恐怖主义相

关的生物特征数据来履行这一重要的保护性功能，最重要的是，该数据库受到接受独立监督的国际议定管理措施的规限。

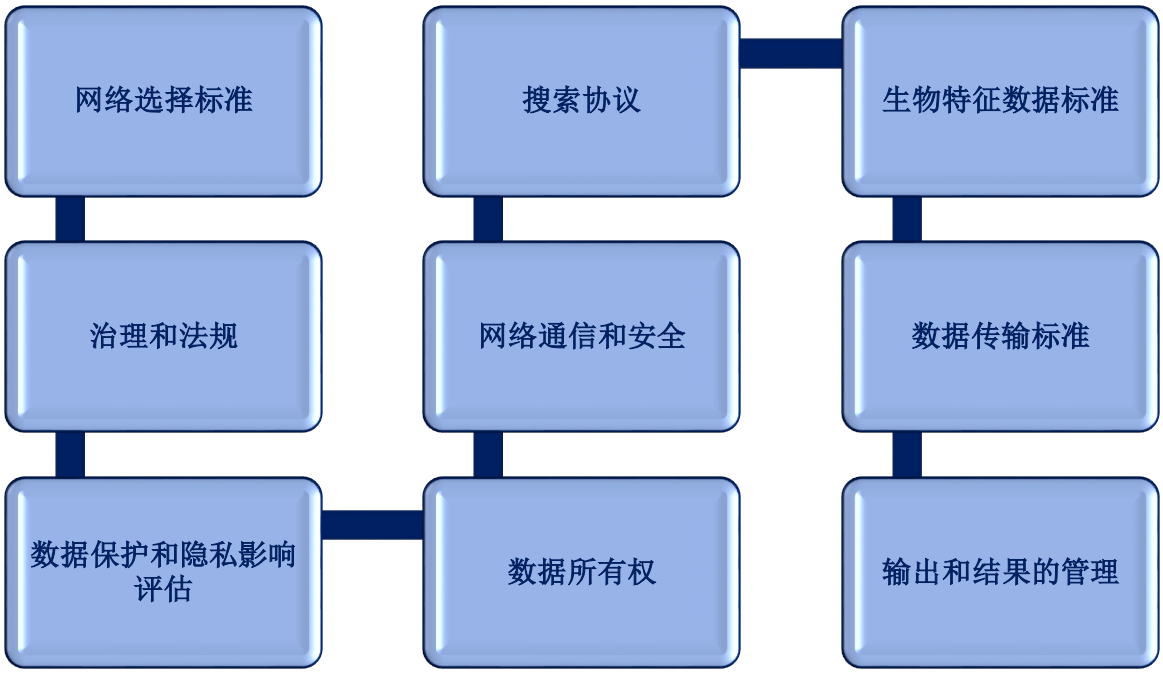
图 6 显示了由国家和国际公共组织持有、可用于反恐的*潜在*生物特征数据来源的广泛范围。图片中并未列出所有内容，且对任何该等数据库的访问理所当然都受到国家法律和监管的限制。但其并未显示生物特征数据在理论上如何可以关联，以提供共同保护，防止出现国家、区域和全球范围内的恐怖主义威胁。

图 6 — 生物特征数据来源

3.3.2 数据共享协议和数据库合法整合

传统上，执法生物特征数据库以独立系统的形式运行，因为各个应用程序服务于不同、单独的业务需求，并且在这些系统之间共享数据并没有明显的优势。该等数据库专为与维持治安、边境管理或监狱相关的业务职能而设计。但随着近几十年来全球恐怖主义威胁日益严峻，许多政府被迫重新考虑其数据库使用方式及其可能以何种方式相互分享数据，进而为公民提供更强大的保护。其结果是，国家级数据库的互联性和相互操作性得到提高，且开发出了国际级的双边、多边和区域性数据库网络。这以整合不同、单模式的数据库为开端，然后（在某些国家和地区）演化为先进的、替代性网络，这一网络拥有互连、多模式数据库，该数据库旨在满足执法、边境管理和其他政府职能方面的一系列国家和国际业务需求。此类连接的要求如下：

图 7 — 生物特征网络的连接要求



网络选择标准 — 生物特征数据所有人评估其生物特征网络会员不仅应基于其自身业务要求和经营目标（尽管这一点十分重要），还应基于更加广阔的角度考虑 — 考虑为其所在国或地区以及该网络中的其他合作伙伴带来的潜在附加值。此方法对于开发网络化的反恐生物特征数据库十分重要且基础。希望参加国际网络的数据所有人不太可能会冒险与没有原则或不可信的合作伙伴共享数据，任何拥有较多国际会员的网络都必需对这些问题进行适当管理，例如，参见第 3.1.2.节。维持治安和 INTERPOL 应用程序。

治理和管理 — 生物识别网络必需在允许传输生物特征数据和其他相关元数据的法律框架内运行。各现有数据库应早已根据国家法律和人权法运行，但还需要进一步制定法律，以允许在某一国家或全球在不同数据库之间进行搜索。如果是国际数据库，这通常是通过加入的实体或国家之间的正式协议（如谅解备忘录）实现的。合法搜索仅限于逐案进行的单个搜索（例如为特定罪犯进行的搜索），或者可以进行更广泛的应用，如在网络中对所有登记的数据进行自动搜索。

监管框架应对整个网络的独立监督作出规定，且应尤其关注数据管理功能和数据所用的用途，以防止在未获授权的情况下扩大范围，例如进行法律或当前操作协议下禁止的网络内外的数据集搜索。一些国家已任命相关官员履行这一职能，例如生物特征监管人或特派员。此外，其他监管者（如英国法医学监管人）有责任对科学流程进行监督，包括创建该等数据库中使用的法医学生物特征数据和资料的流程。这意味着数据库的运行和数据库中包含的法医学生物特征数据都必须接受独立审查和监督，该等检查和监督包括伦理审查委员会或类似机构的工作。（参见第 2.1.1. 节）

数据保护和隐私影响评估 — （参见第 2.2.3.和 2.2.4.节）。

数据所有人 — 必须为各条生物特征记录指定数据所有人（参见第 2.2.6. 节），根据法律，数据所有人负责相关数据的登记、使用、保留和删除。在处理包含来自不同数据来源的大量数据的生物特征数据库网络时，这尤其重要。

网络通信和安全 — 生物特征数据流和其他信息必须高效、及时。鉴于网络所持有数据的性质，网

络必须安全，且必须具有适当的安全级别，从而为人员和操作环境（包括数据、硬件、软件和通信网络）提供保护。只在网络系统中保留生物特征数据是不错的做法。应在单独的系统中对与相关生物特征数据相关联的个人、个人数据进行存档。这一保障措施可防止从某一应用程序访问个人信息和生物特征数据。因此，生物特征数据通常只有唯一的参考编号，以便在需要时，使用安全的操作程序将其与相应个人数据相关联。

搜索协议 — 该网络必须有同步、系统的搜索词条和存档协议，对各次搜索的时间和顺序进行控制，以确保其可以暴露在该网络中的各数据库的完整数据集中，即任何内容都不会有遗漏，即使在需求高峰期也是如此（参见下段 — 网络化生物特征数据库：搜索协议）。

生物特征数据标准 — 只能在合作伙伴已提交相容类型的生物特征数据的情况下在网络中进行搜索。例如，在全球（例如在澳大利亚、欧洲和美国），已经使用了多种 DNA 图谱分析化学物质。除所有合作伙伴都常用的 STR 基因座外，各化学物质都采用独特的 STR 基因座。但只要有足够数量的常见基因座，就可以在任何其 DNA 数据库中搜索来自该等不同化学物质的图谱。最新图谱分析化学物质使用更多的 STR 基因座，以便相应增加所有合作伙伴都常用的基因座的数量。

第 2.4 节中所述的技术和科学标准（如 ISO 17025）应增强网络的所有操作功能。

数据传输标准 — 若图像质量不达标，生物特征网络可能遭受严重的不必要风险，比如增加错误拒绝，甚至是错误识别的数量。为确保在网络中进行传输的时候，图像（如人脸或指纹）质量不会降低，应制定相关标准[73]，对图像分辨率作出规定。这意味着无论在网络上的哪个位置查看，照片都将保持同样的清晰度。

输出和结果管理 — 必须根据法律要求、严格的科学标准和严格的组织协议，对搜索网络生成的生物特征数据匹配结果以及根据该等匹配（结果）采取的措施进行认真管理（参见第 3.3.3. 节）。应由另一名专家或者最好由两名专家在结果发布前，对生物特征匹配结果进行同行评审，这是质量管理体系中的一个环节。这可以防止在只有一个人的情况下，做出不当识别。

网络化生物特征数据库搜索协议 — 以下两种基本方法，可将不同数据库之间的搜索同步：

单向搜索 — 在数据库 1 中，进行生物特征数据 (a) 的登记和搜索。如果无法找到匹配结果，则将相关数据归档到数据库 1，然后发送到数据库 2，以便进行搜索，如果还是没有找到匹配结果，则归档到数据库 2。

注：如果数据 (a) *只*在数据库 2 中进行搜索，而*未*归档到该数据库，则可能会错过潜在匹配项，因为搜索结果将受到确切搜索时间的限制。例如，如果在进行数据 (a) 的搜索*后*在数据库 2 中对与生物特征数据 (a) 匹配的进一步搜索数据 (b) 进行登记和搜索，则不会产生任何匹配结果，因为并未对数据 (a) 进行归档，因此其未显示在数据 (b) 的搜索范围内。因此，在两个和多个数据库之间进行单向数据传输时，有必要确保各数据库在搜索之后对数据进行归档，以确保其能够被之后的搜索所识别，因而保持持续的覆盖度。

数据管理也可以是单向传输方面的问题，在数据库位于不同司法管辖区或国家的情况下，尤其如此

[73] 如 NIST 第 1152 号特别刊物“Latent Interoperability Transmission Specification（潜在互操作性传输规范）”www.nist.gov

。各数据所有人应寻求与其他合作伙伴签订与共享数据的保留时间和删除政策相关的正式协议。如果未签订此协议，则不能强制要求其他数据库的所有人遵守主机数据库所必须遵守的相同法律。他们还可能因其他原因（如财务、资源或时间限制）而不愿进行必要的删除。

互惠双向搜索 — 在数据库 1 中进行生物特征数据的登记和搜索。如果无法找到匹配结果，则将相关数据归档到数据库 1，然后发送到数据库 2 进行搜索，但数据库 2 中不会保留数据 (a)。同样，如果生物特征数据 (b) 在数据库 2 中进行登记和搜索，然后发送到数据库 1 进行搜索，其不会被数据库 1 保留。此方法被复制到网络中任何数量的数据库，因为各数据库通过其他数据库进行新登记数据的搜索。可在数据库中进行搜索*之前*在主机数据库中进行数据归档，以防出现时间间隔（这可能会导致网络上即将同时出现不同搜索，从而错过彼此），进而避免错过潜在的匹配项（如同在单向搜索中）。

注：本系统通常被称为“单次登记多次搜索”或“一次输入多次搜索”。对数据文件拥有所有权的数据库在搜索后进行数据归档，但所有其他数据库只进行搜索。这使得数据管理流程得以简化，因为所有人的数据只存储在其数据库中，这同样减少了网络中归档数据的数量。必须对数据库之间的搜索顺序进行认真管理，尤其是当一个司法管辖区内的多个数据库被传输到位于其他司法管辖区的数据库时。例如，必须在任何数据库向司法管辖区 (2) 发送搜索结果前，将司法管辖区 (1) 的数据库之间的搜索排列方式使用殆尽，否则，可能会在司法管辖区 (2) 披露应该已经在司法管辖区 (1) 发现的匹配结果。通过由接受管理的单一渠道从司法管辖区(1) 向司法管辖区 (2) 发送搜索结果，可以避免这一情况。

3.3.2.1 预测性生物识别技术：前瞻性地使用生物特征数据库网络预防恐怖袭击

通过整合执法和边境管理这一广阔领域的生物特征数据库（以及军事生物特征数据（如可用）），不仅可以从独立业务需求的角度（如犯罪侦查或边境身份检查等），还能够以更广泛的“生物特征事件”系列或模式的形式利用其自身功能对网络集中输出的结果进行分析。就恐怖主义威胁而言，各事件可能存在直接或间接关联，或者可能看起来完全无害，且表面看起来不具有价值，但若置于其他信息或生物特征事件的背景下，其可能会对更为广阔的图景 — 恐怖主义运动和活动情报工作，提供极大帮助。这些输出结果中有些非常清楚，如揭示可疑的旅行安排或确定与恐怖主义罪行之间的关联，而另外一些结果则不那么明显，但与其他相关资料一同考虑时，仍能够提供有价值的指示信息。此方法（如下方图 8 所示）建立在为调查之目的，对生物识别数据库进行传统、反应式以及很大程度上被动使用的基础上，其试图通过在相关袭击事件发生前，前瞻性地使用来自最广泛来源的生物识别数据以及其他情报产品，来预防恐怖袭击，进而拯救生命。

图 8 — 预测性生物识别技术模型

传统生物特征数据库（如第 1 节所述）被设计为反应式数据库，且根据身份和*当前*或*以往*活动提出调查问题，如*"我们是否认识您？您的同伙是谁？您干了什么？"*整合的数据库显然可以回答同样的问题，但它们也可以前瞻性地用于推断和预测潜在未来行动和关联，即*"您和您的同伙计划或者可能在何时何地做什么？*因此，对网络中的所有输出结果进行综合、仔细的分析至关重要，且若与其他情报一并使用，是成功评估和预测恐怖主义活动的关键因素。这对随后的结果管理同样适用。

3.3.3 结果管理

3.3.3.1 输出结果背景分析

在独立的生物特征数据库中，输出结果可能在很大程度上是自动化的，极少使用人机交互（参见第 1 节），但当该等系统中包含的数据被整合到多功能生物特征数据库中，并对数据进行交叉搜索，则完全有必要在采取任何措施前，对输出结果进行完整查看及完全理解该等结果。在对该等输出结果进行背景评估时，管理由此产生的结果的人员必须考虑以下因素：

确保进行合法适当回应并且管理不当或附带的身份识别 — 接收并处理任何类型的生物特征数据库所产生结果的人员自然会形成贬损的观点，认为系统识别的任何人都必然是恐怖分子。但这并不一定都对，原因如下：

1. 可能因人为或系统错误对某人进行错误的身份识别，尽管这非常罕见。这一点应该在任何审查协议中进行载述，在其他数据或证据似乎对结果提出质疑的情况下，尤其应该如此。
2. 政府或其他方客户想要通过对恐怖主义活动进行错误的指控，滥用生物特征输出结果，以挫败其反对派人士、政治活动家或人权活动者的活动（参见第 2.2.5. 节）。
3. 被识别的人士可能并没有以任何方式参与恐怖主义活动。正因如此，才必须在采取任何行动*之前*对任何结果的背景和相对价值进行妥善评估。

例如，恐怖主义调查中的关键物品或场所可能会被未参与任何恐怖主义活动的人员或粗心的执法人员无辜地污染。随后，这些法医学材料由犯罪现场调查人员和法医科学家收集，然后被登记到适当数据库网络中。随后，该等“附带”法医学数据可能会对网络中的搜索作出回应，并生成匹配结果，例如当该个人随后提供生物特征数据，以跨过边境时。因此，该等边境机构采取的措施必须基于任何生物特征匹配的整个背景，而不能仅仅基于生成的生物特征匹配结果，就作出相关人士是恐怖分子的自动假设。应对执法机构作出的回应进行衡量，且该等回应应符合国际人权法。必须对该等背景评估程序进行严格的独立监督，以防止出现任何潜在的不当拘留或潜在误判。

通信策略 — 为确保在对结果进行管理时以一致、有效的方式进行背景评估，相关机构必须在生物特征输出结果评估人员与必须对相关信息采取措施的前线操作人员和决策者之间构建清晰、安全和连续的沟通线。这包括促进犯罪现场数据所有人（执法机构）和负责处理而被拘留人员（因犯罪现场数据的匹配结果而被拘留）的官员之间进行紧急对话。进行这类和其他类型的信息交换十分常见，且通常是国家和国际执法界的标准操作程序。通信网络还将要求优化数据库结果以及在协定的时间范围内运行（尤其是当有人因生物特征的匹配结果而被逮捕或拘留的时候）。通信策略还必须列出网络生物特征输出结果的接收者完整名单并且制定消除冲突标准，以防止两名接收者在管辖权主导地位和调查优先性等方面出现争议或解决该等争议。

模态、法医学情报数据报告标准和科学解释 — 一些生物特征数据库网络可能只使用一种模态，但在生物特征网络中，同时运行一系列模态（如指纹、DNA、人脸）更为常见及有效。若与含有从犯罪现场采集的法医学情报数据以及来自多个来源的参考数据的多功能系统一同使用，多模式系统的输出结果可为相关活动提供最全面的信息。由于第 1 节中所述的原因，从犯罪现场获得的法医学资料可能无法始终提供与参考数据“完全”匹配的结果，但其仍对调查具有巨大的证据价值。整理数据库输出结果的人员应充分领会及理解这两个要素。应编辑整理并向相关官员、调查人员或分析人员报

告匹配结果的相对优势及其潜在证据或调查价值，以及在背景评估中获取的任何其他相关信息，以便采取适当和相应的行动。因此，只登记可在法庭中作为证据出示的数据是一种良好的做法。这使得可以在调查中对所有匹配结果进行充分利用，并在法庭中披露或出示。

案例研究 10 — INTERPOL 通知管理程序

国际数据交换管理的操作示例

尽管 INTERPOL 红色通缉令系统并不处理生物特征结果，但其与第 3.3.3.1.节中的评估流程极为相似，且提供了全球数据管理的一个绝佳模型。该通缉令必须根据国际法律规则和该组织的规则运行，并确保促进关键方之间的有效沟通，并且建立了一个系统，用于对必须受红色通缉令流程规限的人员提出的投诉和上诉进行独立、有效处理。

红色通缉令是一项总秘书处应成员国请求、根据有效的国家逮捕令发布的要求，用于临时逮捕等待引渡的个人。红色通缉令也可能会根据国际法庭的要求发布。

除红色通缉令外，INTERPOL 还会发布其他类型的通缉令，例如应成员国请求发布的蓝色通缉令，用于在犯罪调查的背景下查找信息。成员国可能还会发布扩散通报，这是一项在成员国之间直接流通的合作要求。

INTERPOL 不能坚持要求或强迫任何成员国逮捕红色通缉令的目标人物。INTERPOL 亦不能要求任何成员国应其他成员国的要求采取任何措施。由 Interpol 的各成员国自行决定在其境内赋予红色通缉令何种法律价值。在对通缉令或任何其他请求作出采取何种措施的决定时，国家对该项决策承担全部责任。红色通缉令的操作有效性取决于其在可一年 365 天、每周 7 天、每天 24 小时全天候接受管理的国家中央局 (NCB) 之间的转递情况。

所有通缉令和扩散通报都必须符合 INTERPOL 的规则和法规，包括《国际刑警组织宪章》第 2 条（对《世界人权宣言》的精神进行明确提述）和《国际刑警组织宪章》第 3 条（此条款“严令禁止该组织进行任何政治、军事、宗教或种族性质的干预或活动”）。《国际刑警组织关于数据处理的规则》对各类通缉令的发布、在各实体（即请求国、总秘书处、接收国等）之间进行责任分配的额外标准作出规定。

监管监督 — 设有各级控制，以确保遵守 INTERPOL 条例。首先是发送警务合作要求的 NCB（如红色通缉令请求）。NCB 对其向 Interpol 数据库提供或使用 INTERPOL 信息系统进行流通的任何信息承担全部责任。其必须确保该等信息正确、相关并且为最新，并且根据该组织的宪章及其国家法律进行处理。

其次是 INTERPOL 总秘书处总部。2016 年，总秘书处成立了由多学科单元（包括律师、警察、分析人员和操作专家）组成的专门工作小组，对各级数据处理，包括与红色通缉令和扩散通报相关的数据处理进行审查。该工作小组仔细审查所有请求，以确保其遵守 INTERPOL 的宪章或规则。该工作小组可能会在开展审查工作时，要求提供所有相关来源的额外信息，以确定是否已发布通缉令。此外，如果成员国认为相关行为不符合 Interpol 规则，其可以提出与其他成员国处理的信息（包括红色通缉令的发布）相关的疑虑。

难民管理 — 自 2014 年 6 月以来，INTERPOL 实施了与难民相关案件有关的新政策。这使得 Interpol 可以在预防犯罪分子滥用难民身份方面，为成员国提供支持，同时，提供充分有效的保障措

施，保护难民权利。由总秘书处（如适用，由 Interpol 文件控制委员会（参见第 3.1.2.节））逐案评估针对难民发出的各份红色通缉令和扩散通告。一般而言，如果难民或寻求庇护者的身份已得到确认，且该人士所担心对其实施迫害的国家已作出通缉令/扩散通告的请求，则不能处理针对难民的红色通缉令和扩散通告。

受通缉令/扩散通报影响的个人权利 — 是否在 INTERPOL 数据库中发布通缉令或登记信息的决定不会对个人权利（包括其被假定无罪的权利、针对案件向发布逮捕令并寻求 INTERPOL 援助的国家相关机构提出挑战的权利，或针对案件向考虑引渡请求的国家机构提出挑战的权利）构成影响。
个人至少可以选择通过下三种方式之一，对通缉令或扩散通报提出挑战：

- 直接或通过聘请法律代表到请求国家的国家机构就其案件进行申辩。由于红色通缉令是根据有效逮捕令发布的，如果国家主管机构将逮捕令撤销，则红色通缉令将会被删除。
- 联系 INTERPOL 文件控制委员会
- 请求其母国自行处理相关案件并对红色通缉令提出抗议。

如果红色通缉令或扩散通告因任何原因被取消，则向告知其相关决定的所有成员国发送信息，且要求该等国家删除其国家数据库中的任何相关信息。

这些保障措施可确保提供透明、结构化的流程，以应对并解决相关问题并防止出现红色通缉令的潜在滥用行为。

3.3.3.2 战略目标和调查人员准则

国家和区域性反恐战略应反映法医学和生物特征技术的重要性。执法和边境管理机构应通过运用其可以使用的所有法医学和生物识别资源并维持有效的数据库，积极支持这些战略。

还可以在调查层面制定法医学和生物识别战略，通过培训和操作原则鼓励采取这一做法。负责恐怖主义调查的高级调查人员应在调查开始时，设定主要法医学和生物识别目标，生物特征通常应包括：

- 在调查期间获得的所有被捕者生物特征参考模板必须达到最佳质量
- 所有犯罪现场 — 必须接受全面、完全按顺序进行的法医学检查，尽量增加 DNA 和指纹的采集量，以在调查的特定法医学要求之外，建立更广泛的恐怖主义联系。
- 在调查期间获得的所有相关生物特征数据都必需在所有相关国家和国际数据库中进行登记和/或搜索。

这三种生物识别策略解决：

1. *调查需求*，即高质量生物特征参考数据，用于与犯罪现场的资料和数据库中登记和搜索的内容进行有效的 1:1 对比，进而推进调查过程，和
2. *其他恐怖主义调查和情报行动的要求*，通过采用犯罪现场和生物特征资料的获取这一更为广阔的视角，这些资料可能不一定与核心调查相关，但可能揭露以前并不知晓的同伙、组织或网络，并且

3. 在某一调查过程中收集的生物特征数据不仅可以帮助解决或建立与其他调查之间的联系，还可能*防止未来出现恐怖主义袭击*，进而拯救众多人的生命。

3.4 推荐实践

a) 各国应通过应用旨在保护其边境和国家资产的生物识别系统以及以合法的方式与国际合作伙伴分享生物特征数据，应对跨越国际边界进行的持续恐怖主义活动所引起的威胁。

b) 通过同时使用 1:1 生物特征验证技术和旨在对恐怖分子及其同伙进行追踪和侦查的 1:n 生物特征观察名单检查，可对边境安全进行更有效的管理。可以根据国家法律、监管限制和国际人权法，创建任何规模的生物特征观察名单，从小型参考数据的集合，到完全连接到执法身份管理和犯罪侦查数据库。

c) 强烈建议各国尽量多使用 Interpol 生物特征数据库（人脸、指纹、DNA），以应对恐怖主义行动和外国恐怖主义作战人员的威胁。

d) 在国际范围内分享生物特征数据是十分重要的反恐工具，但必须遵循国际人权法进行分享。各国政府必须确保，其在分享生物特征数据的过程中不会为导致酷刑或被处以死刑的逮捕提供帮助。

e) 务必在采取任何行动前对所有生物特征匹配结果的整个背景进行详尽调查，以确保完全遵守国际人权法。

f) 国家和区域性反恐战略应通过赋予执法和边境管理机构以下责任：尽量以合法的方式收集和使用法医学或生物特征资料，以及维持有效的数据库和数据共享协议，进而反映法医学和生物识别技术的重要性。

3.4.1 参考文件

ICAO TRIP Guide on Border Control Management, Montreal (2018)（ICAO TRIP 蒙特利尔边境控制管理指南（2018 年））

PNRGOV EDIFACT & XML Message Implementation Guide（PNRGOV EDIFACT 和 XML 信息实施指南）：www.wcoomd.org/en/topics/facilitation/instrument-and-tools/tools/api-pnr.aspx

WCO/IATA/ICAO Guidelines on PNR（WCO/IATA/ICAO PNR 准则）（第 9944 号文件）

ICAO 第 9303 号文件 — Machine Readable Travel Documents（机器可读的旅行证件）

www.interpol.int/INTERPOL-expertise/I-Checkit

www.interpol.int/INTERPOL-expertise/Databases

The INTERPOL DNA Gateway（INTERPOL DNA 网关）— 于 2017 2 月年正式发布

The INTERPOL Facial Images Best Practices Guide（INTERPOL 人脸图像最佳做法指南）（2015 年 10 月）和 Facial Recognition Fact Sheet（人脸识别情况说明书）

INTERPOL Guidelines concerning Fingerprint Transmission 2012（2012 年 INTERPOL 指纹传输相关准则）

INTERPOL Rules on the processing of information for the purposes of international police co-operation（INTERPOL 为国际警务合作而进行的信息处理的相关规则）

ETIAS
http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU%282017%29583148

www.europol.europa.eu/activities-services/services-support/information-exchange/europol-information-system

www.consilium.europa.eu/prado/en/check-document-numbers/check-document-numbers.pdf

www.un.org/sc/ctc/

https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/fact-sheets/docs/20161116/factsheet_-_etias_en.pdf

http://europa.eu/rapid/press-release_MEMO-16-3706_en.htm

NIST 第 1152 号特别刊物“Latent Interoperability Transmission Specification（潜在互操作性传输规范）”www.nist.govhttp://www.nist.gov/

4. 附录

4.1 首字母缩略词

ABC	自动边境控制	IEC	国际电工委员会
AFIS	自动指纹识别系统	ICAO	国际民用航空组织
API	预报旅客信息	iAPI	互动式预报旅客信息
BCP	过境点	ISO	国际标准组织
BMS	边境管理信息系统	LDS	逻辑数据结构
CCF	Interpol 文件控制委员会	MRZ	机器可读区域
CCTV	闭路电视	PKI	公钥基础设施
eBMS	电子边境管理信息系统	PNR	旅客姓名记录
EER	等错误率	QMS	质量管理体系
ETS	电子旅行系统	SIS	申根信息系统
FAR	错误接受率	STR	短串联重复序列
FRR	错误拒绝率	TAR	正确接受率
FTA	错误采集率	TRR	正确拒绝率
FTF	外国恐怖主义作战人员	VIS	签证信息系统

4.2 生物识别术语表

认可 — ISO 将认可定义为“通常称为认可机构的独立机构对认证机构根据国际标准运行进行的正式认可。”

自动指纹识别系统 — 一种电子系统，旨在存储和搜索大量下列内容：(1) 指纹和掌纹的参考数据集，和 (2) 从犯罪现场采集的指印和掌印。身份管理搜索通常只生成一个响应结果或不产生跟踪结果。犯罪侦查搜索结果以可能匹配项的响应列表的形式列出。对系统生成的任何匹配结果进行确认的指纹审查员将对响应结果进行审核。

生物特征模态 — 在系统中或操作背景下使用的生物特征类型，如指纹、人脸、虹膜等。

认证 — ISO 将认证定义为“独立机构提供的确认相关产品、服务或系统符合特定要求的书面保证（证书）”。

符合性评估 — IEC 将符合性评估定义为“与产品、流程、系统、人员、机构相关的特定要求得到满足的证明。”

犯罪侦查搜索 — 对下列数据进行的双向搜索方案：(1) 对照犯罪现场数据搜索参考数据；(2) 对照参考数据搜索犯罪现场数据

犯罪现场数据 — 根据从犯罪现场获取的样本和物品生成。

等错误率 (EER) 指错误接受率和错误拒绝率相等时的特定临界值的设置。

例外情况处理 — 在生物识别系统出现故障时采取的应急措施，如人为干预、备份系统等。

错误采集率 (FTA) 指因呈现（如无捕获的图像）、特征提取或质量控制阶段出现的故障，而无法完成的所有记录交易的比例。

错误接受率 (FAR) — 误识的数量在理应拒绝的生物识别查询总数中的占比（即系统*生成并显示为匹配的不匹配项数量在真正*不匹配项中的占比）。

错误拒绝率 (FRR) — 错误拒绝的数量在理应接受的生物特征查询总数中的占比，即系统*生成并显示为不匹配的匹配项数量在真正*匹配项中的占比。

身份识别 —（亦称一比多或 1:n 对比）这是一项搜索功能，其并不倚赖于建议的身份，因此将在整个数据库中进行查询，以进行可能的匹配。

身份管理搜索 — 通过系统中归档的参考数据，搜索主体的生物特征参考数据，从而确定主体是否曾登记于数据库中

变形 — 将从两个或更多贡献人采集的生物特征样本（如人脸图像）合并，以便能够成功对照变化的身份，对任何贡献主体进行成功验证。

质量管理体系 — 一种正式协议，定义和记载流程、程序和责任作出，以实现质量目标。该体系旨

在协调组织活动并提供相关指导，以符合客户和监管要求，处理不遵守行为并营造持续改进的文化。

参考数据 — 在控制的条件下从被捕者或嫌疑犯采集的数据，例如用扫描仪以电子方式或使用油墨与纸采用传统方式采集的 10 根手指的指纹、从被捕者的脸颊内采集的口腔拭子，或经处理后，将生成完整的 DNA 图谱的头发样本或血样、面部数码照片等

连环犯罪/事件搜索 — 通过在拥有类似犯罪现场数据的数据库中搜索生物特征或法医学犯罪现场数据，对任何匹配项进行识别，从而在单个调查中确定犯罪行为或事件之间的联系。

欺骗 — （亦称呈现攻击）指呈现合法、注册用户的虚假生物识别特征（如乳胶面罩、相片、假手指或录音），以在未经授权的情况下进入生物特征识别系统。

临界值 — 对生物识别系统进行的可调整设置。 其控制特定应用程序的接受和拒绝之间的平衡。

吞吐率 — 在指定的期限内使用生物识别系统的人员的数量。

正确接受率 (TAR) — 衡量系统正确匹配同一个人的生物识别身份属性的能力标准。

正确拒绝率 (TRR) — 衡量将一名人员的生物识别身份属性与数据库中他人的生物识别身份属性正确地

匹配的次数的标准，即正确不匹配的频次。

验证 — （亦称一比一或 1:1）。此模板使用建议的身份，从数据库中选择一个模板，与查询的模板进行对比。本质上，这是一个验证流程，将查询的模板与数据库模板进行对比，得到的结果有两种，即两种模板源自或并非源自同一个人。

4.3 国际组织目录

生物识别学会 www.biometricsinstitute.org

国际民用航空组织 www.icao.int

红十字国际委员会 www.icrc.org

国际刑警组织 (INTERPOL) www.interpol.int

国际电工委员会 www.iec.ch

国际标准化组织 www.iso.org

4.4 联合国反恐办公室 (UNOCT)

联合国秘书处、机构、基金和计划以及关联机构通过其个人职权以及加入联合国全球反恐协调契约工作小组 (GCTCCTF) 促进联合国反恐战略的实施。

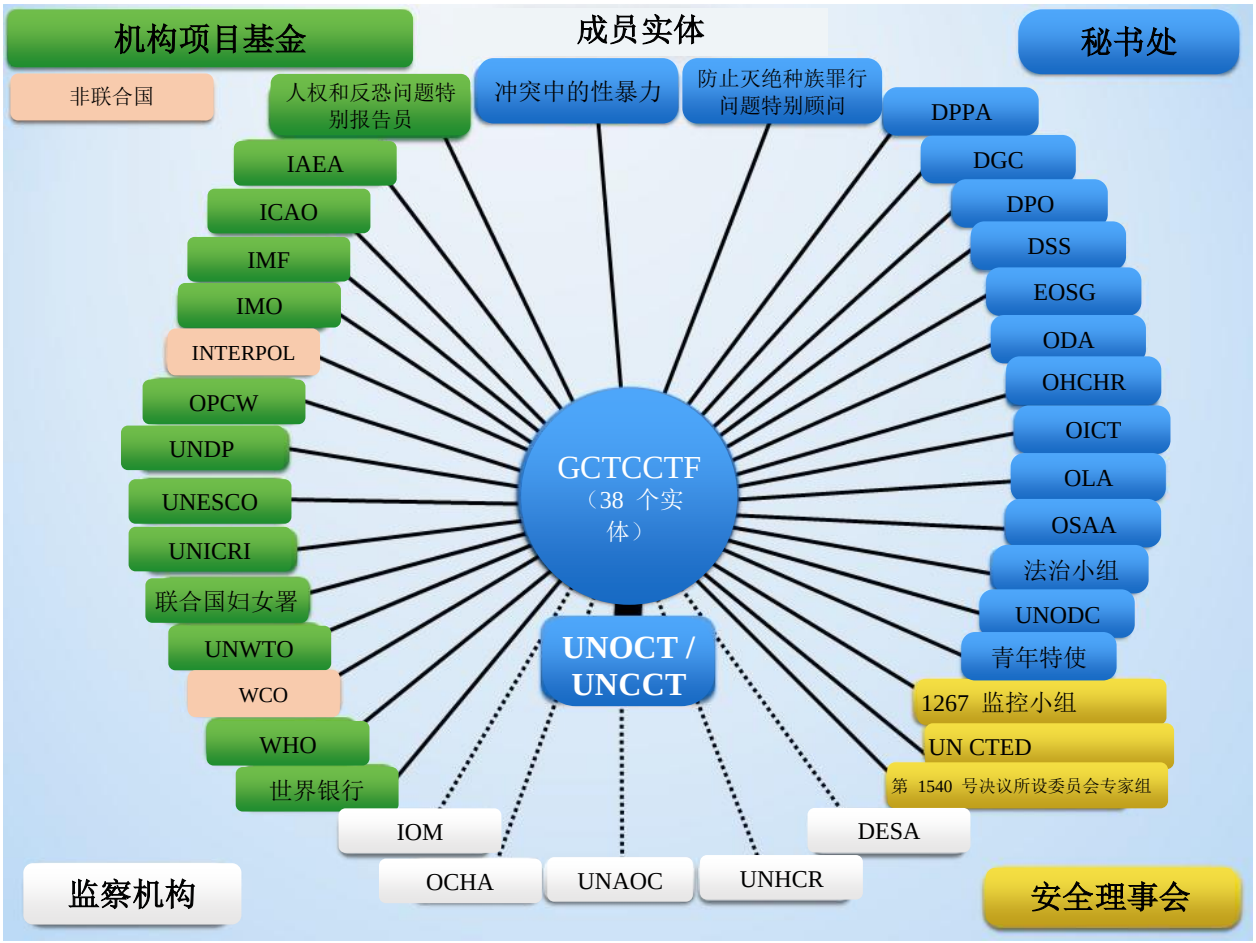
该工作小组由 38 个国际实体和 INTERPOL 组成，由于其开展的工作，对多边反恐成果产生影响。各实体根据自己的职责作出贡献。该工作小组的成员包括 UNOCT 以及下列实体：

1. 基地组织和塔利班问题监测小组
2. 反恐怖主义委员会执行局 (CTED)
3. 维持和平行动部 (DPO)
4. 政治和建设和平事务部 (DPPA)
5. 全球传播部 (DGC)
6. 安全和安保部 (DSS)
7. 第 1540 号决议所设委员会专家组
8. 国际原子能机构 (IAEA)
9. 国际民用航空组织 (ICAO)
10. 国际海事组织 (IMO)
11. 国际货币基金组织 (IMF)
12. 国际刑警组织 (INTERPOL)
13. 裁军事务厅 (ODA)
14. 人权事务高级专员办事处 (OHCHR)
15. 法务事务厅 (OLA)
16. 秘书长办公厅 (OSG)
17. 防止灭绝种族罪行问题特别顾问办公室
18. 儿童与武装冲突问题的秘书长特别代表办公室 (CAAC)
19. 冲突中的性暴力问题秘书长特别代表办公室 (SVC)
20. 秘书长青年特使办公室
21. 禁止化学武器组织 (OPCW)
22. 促进和保护人权同时打击恐怖主义问题特别报告员
23. 联合国开发计划署 (UNDP)
24. 联合国教育、科学及文化组织 (UNESCO)
25. 联合国区域间犯罪和司法研究所 (UNICRI)
26. 联合国毒品和犯罪问题办公室 (UNODC)
27. 联合国非洲问题特别顾问办公室 (OSAA)
28. 联合国法治小组
29. 联合国妇女署
30. 联合国世界旅游组织 (UNWTO)
31. 世界海关组织 (WCO)
32. 世界银行
33. 世界卫生组织 (WHO)

监察机构

34. 国际移民组织 (IOM)
35. 人道主义事务协调厅 (OCHA)
36. 联合国经济和社会事务部 (DESA)

37. 联合国难民事务高级专员署 (UNHCR)
38. 联合国文化联盟 (UNAOC)



4.5 UNOCT 与反恐问题有关的边境管理和执法工作小组

联合国跨部门工作小组旨在就所需法律、制度和实用反恐相关边境控制措施，为成员国提供指导。其尤其关注以下方面的问题：恐怖分子的流动；旅行证件的完整性和安全性；现金和不记名可转让票据的非法流动；物品的流动和处理；小型武器、轻型武器、弹药、具有大规模杀伤力的爆炸物和武器的非法流动；航空和海洋安全；预警和警报系统；开放边境的控制。

职权

该工作小组旨在帮助成员国增强联合国全球反恐战略 (A/RES/60/288) 第二支柱第 4、5、7、8 和 13 到 16 段和第 III 支柱第 2、4 和 11 到 13 段所载的边境管理和边境控制系统。

已经为反恐问题相关边境管理工作小组确定了职责范围。

地位

该工作小组目前正在实施协调边境管理项目，正在以可执行和方便用户使用的格式编写所有相关国际公约、标准和最佳实践，以帮助相关国家为有效的边境管理系统建立制度和程序机制。该工作小组敲定了协调边境管理的工作模板。此模板将通过与成员国和国际组织之间的持续对话和协商得到强化。

实体

联合主席：

- 反恐怖主义委员会执行局（CTED）（主要）
- 世界海关组织（WCO）
- 国际刑警组织（INTERPOL）

核心实体：

- 联合国反恐办公室（UNOCT）
- 联合国全球反恐协调契约工作小组（GCTCCTF）
- 国际民用航空组织（ICAO）
- 国际海事组织（IMO）
- 联合国毒品和犯罪问题办公室（UNODC）
- 国际移民组织（IOM）
- 人权事务高级专员办事处（OHCHR）
- 联合国区域间犯罪和司法研究所（UNICRI）
- 裁军事务厅（ODA）
- 1267 监控小组
- 第 1540 号决议所设委员会专家组
- 联合国难民事务高级专员署（UNHCR）（监察机构）

其他成员实体：

- 维持和平行动部（DPO）
- 禁止化学武器组织（OPCW）
- 联合国开发计划署（UNDP）
- 世界卫生组织（WHO）
- 经济和社会事务部（DESA）

该工作小组在下列若干关键领域开展活动：

- 人员的流动和处理
- 证件签发流程的完整性和安全性
- 现金和其他不记名可转让票据的流动
- 货物的流动和处理
- 小型武器、轻型武器、弹药、爆炸物和化学、生物、辐射和核材料（CBRN）的流动
- 海事安全
- 航空安全
- 预警和警报系统
- 开放边境的控制
- 在尊重人权方面的首要需要

人员的流动和处理

最近几十年在全球实施的恐怖袭击造成的重大效果之一是，使跨边境人员流动和采取的国家安全保

护措施之间的联系增加了。因为对旅行和经济、文化交流起促进作用的流程同样被恐怖分子加以利用，旨在防止恐怖主义行为的措施与跨境流动的管理和监管之间的联系变得明显。该等措施包括执行将旅客纳入其中的边境管理系统、签发安全旅行文件、促进利益相关者之间的信息交流、培训和能力建设。在这些领域实施的改进有助于增强安全和移民系统功能，同时促进人员的跨境流动。该等措施中有些在技术上十分复杂且具有高度创新性，但可以在移民管理的传统领域实施许多更为简化的措施，以强化综合功能。此类措施应始终以所面临的威胁程度为依据，这尤其是因为提高安全级别可能会导致阻碍增加并且可能侵犯隐私权和公民权利。

证件签发流程的完整性和安全性

旅行证件的安全性和身份管理是防止恐怖分子流动和打击跨境犯罪行为的重要工具。如果证件落到恐怖分子之手，伪造的旅行证件可能和武器一样危险。现代护照越来越安全且难以伪造，犯罪分子和恐怖分子在伪造证件（如出生证明、身份证等）或申请“官方签发的”护照方面进行了越来越多的尝试。因此，各国有必要制定并实施通用规范，以进行身份管理并确保旅行证件的安全性（包括签发流程中的安全性），从而解决这些漏洞。

现金和其他不记名可转让票据的流动

现金和/或不记名可转让票据 (BNI) 的跨境走私是恐怖分子进行资金的跨国际边境转移时热衷使用的方法，无论就恐怖主义融资还是清洗非法活动所得收益而言。政府委托其海关部门执行符合国际规范的边境控制措施，以对现金和 BNI 的非法流动进行侦查并防止出现这一行为。严格遵守该等规范有助于提高此方面的边境管理效力。打击恐怖主义融资活动是联合国反恐措施的一个组成部分，这在联合国的许多决议和公约中都有所体现。

货物的流动和处理

全球贸易和全球供应链尤其容易受到恐怖分子的操纵。为尽量不受恐怖分子的操控，应采取一系列措施，包括确保收到提前提供的与入境、出境和过境运输相关的电子货物信息；运用一致的风险管理方法以应对货物安全方面的威胁；使用非侵入式侦查设备；促进海关管理部门的合作（例如通过对高风险集装箱和货物进行出境检查）；以及通过认可经济营运商 (AEO) 计划，就在供应链的各阶段实施安全做法与私营部门建立合作关系。实施该等和相关措施对增加国际贸易的安全性和促进货物的跨国际边境流动至关重要。

小型武器、轻型武器、弹药、爆炸物和化学、生物、辐射和核材料 (CBRN) 的流动

小型武器、轻型武器、常规弹药和爆炸物以及化学、生物、放射、核 (CBRN) 材料以及两用物品的流动，加之军火贸易格局的变化和非交易行为者的参与，带来了重大的问题，必须开展全球反恐工作，才能对这些问题加以解决。如果这些弹药和材料落到恐怖分子的手中，则将成为恐怖袭击的工具。采用有效的监管、出口控制和边境管理措施，包括法律和强制执行措施，可以尽量减少该等物品被转移到非国家行为者或被非国家行为者非法获取的风险。该等措施应符合在出口控制和促进合法交易之间维持适当平衡的要求。

海事安全

全球交易的总货物总中有超过 90% 沿全球主要海上贸易线路从来源地运输至目的地。因此，海洋领域的安全是一个全球性的问题。海事安全工作旨在对安全威胁进行侦查和震慑；采取预防性措施，防止出现影响船舶和港口设施的安全事件；并保护旅客、船员和其他货物、港口设施以及在港口区域工作和生活的人员的安全，同时允许海上贸易安全、有效的移动。为防止对国际航程的旅客和船员以及为其提供服务的港口设施采取非法行为，有必要有效实施相关法律和实用的安全措施。

航空安全

恐怖主义行为始终对国际民用航空构成严重威胁。若要解决此类威胁，必须制定旨在确保飞机和机场的物理安全的全面、可靠的政策和安全措施。通过采用立法条款，将针对民用航空采取的行为或进行的非法干扰定为不合法，以及有效实施和执行相关航空安全标准和做法，可以显著增强各国抵御相关威胁的能力。

预警和警报系统

边境安全是一个动态、不断发展的流程。由于人员的非法跨境流动不仅会对各国的安全，还会对其政治、经济和社会福利造成不利影响，政府在认识到单边行动不再有效后，现如今，将重点关注放在合作开展安全工作上。因此，综合预警和警报系统对有效的边境管理系统至关重要。该等系统通过促进机构间的合作以及及时分享并交换相关、可靠的信息，提高了各国的整体侦查、预防和打击恐怖主义活动能力，因而使其可以负责任的方式作出关键决策。

许多负责边境控制的国际机构都使用单个组织开发的工具或国际社会开发的可供使用的工具对预警和警报系统加以利用或进行改进。这些工具包括 WCO CEN 和 RILO 网络；IMO SOLAS、LRIT 和 AIS；安全理事会“制裁”委员会综合名单和国际刑警组织 (INTERPOL)“I-24/7”安全全球通信系统、SLTD 数据库和通知机制。

开放边境的控制

开放边境（官方陆路边境和海港检查点之间的边界）持续促进人员（包括恐怖分子和犯罪人员）和货物（包括小型武器、轻型武器、弹药和爆炸物、化学、生物、放射和核材料）的跨边境合法流动。政府认识到保护开放边境安全的重要性，且尝试通过一系列措施，包括监测、巡逻、物理障碍、联合控制行动和巡逻、信息交换、情报评估和就控制和警务问题与边境社区接触来保护开放边境的安全。相关机构必须共同开展控制工作，以有效解决开放边境带来的风险问题。

在尊重人权方面的首要需要

联合国全球反恐战略代表成员国提出一项清晰的主张，即有效的反恐措施和人权保护并不存在冲突，而是相辅相成、相得益彰，且人权法和法律规则构成全球反恐工作的基础。采取全球战略及其行动计划时，成员国决定“承认我们为防止和打击恐怖主义行动而进行的国际合作和采取的任何措施必须符合我们在国际法律，包括《联合国宪章》和相关国际公约和协议，尤其是人权法、难民法和国际人道主义法律下的义务”（A/RES/60/288，附件、序言第 3 段，在 A/RES/64/297 中重申）。联合国大会同样在有关国际反恐的 60 多项决议中，强调了在进行反恐工作时确保遵守人权的首要需要。就边境控制而言，联合国大会号召各国“确保所有边境控制行动和其他入境前机制中适用的准则和做

法清晰且完全符合其在国际人权法、尤其是难民法和人权法下对寻求国际保护的人士所负有的义务”（A/RES/62/159，第 8 段，在 A/RES/64/221 中重申）。