عرض الأمم المتحدة التجميعي بشأن الممارسات الموصى بها بشأن الاستخدام والمشاركة المسؤولة للأنظمة البيومترية في مكافحة الإرهاب

عرض الأمم المتحدة التجميعي للممارسات الموصى بها بشأن الاستخدام والمشاركة المسؤولة للأنظمة البيومترية في مكافحة الإرهاب

تم جمعها من قبل المديرية التنفيذية لمكافحة الإرهاب ومكتب الأمم المتحدة لمكافحة الإرهاب في عام 2018

عرض الأمم المتحدة التجميعي للممارسات الموصى بها

بشأن الاستخدام والمشاركة المسؤولة
للأنظمة البيومترية في مكافحة الإرهاب

بالتعاون مع معهد القياسات الحيوية

جدول المحتويات

الموجز التنفيذي

يقدم هذا العرض التجميعي نظرة عامة رفيعة المستوى عن التقنية البيومترية ونظم العمل ضمن السياق المعني بمكافحة الإرهاب. وهو موجه في المقام الأول للدول الأعضاء الذين قد يلمون إلمامًا طفيفًا بالتطبيقات البيومترية أو ليس لديهم أي معرفة بذلك، والذين قد يواجهون أيضًا تحديات بشأن المساعدة التقنية وبناء القدرات عند تنفيذ هذه التقنية.

يتوفر في نهاية كل قسم مجموعة مراجع شاملة للمزيد من الاطلاع، إضافةً إلى موجز للممارسات الموصى بها. وتُقدم عبر هذا العرض التجميعي دراسات حالة لتوفير أمثلة على الممارسات الجيدة والتقنيات الناشئة.

يقدم القسم الأول العناصر الأساسية للتقنية البيومترية وإدارة شؤون الهوية، بما في ذلك الاستخدام الموسع للأنظمة البيومترية في مجالات علم الأدلة الجنائية وتحقيقات إنفاذ القانون والتعقيدات الإضافية التي تنجم عن ذلك.

يتناول القسم التالي الحوكمة والمتطلبات التنظيمية للتقنية البيومترية من وجهات النظر الخاصة بالقانون الدولي، وقانون حقوق الإنسان، والاستعراضات الأخلاقية، ومتطلبات حماية البيانات، والحق في الخصوصية. ويلي ذلك طرح نظرة أوسع على مواطن الضعف المحتملة للأنظمة البيومترية وبعض من التدابير الرقابية التي يمكن استخدامها للتخفيف من المخاطر. ومن ثمَّ يتم النظر في المعايير الدولية للعمل التقني والعلمي، ويشمل ذلك عمليتي التوثيق والاعتماد للتطبيقات البيومترية، إضافةً إلى أنظمة إدارة الجودة التي يتم الانتفاع بها في العمليات الجنائية المرتبطة. ويغطي الجزء الأخير من هذا القسم الاحتياجات من الموارد والصيانة والشراء الخاصة بالنظام - أو الشبكة - البيومترية لمكافحة الإرهاب، ولا سيما القرارات التشغيلية والمالية الرئيسية التي يجب اتخاذها عند تقييم أي نظام ممتد أو جديد مرتقب.

يقدم القسم الأخير نظرة عامة عن قواعد البيانات والأنظمة البيومترية الحالية لمكافحة الإرهاب على مستوى مجموعة تطبيقات إنفاذ القانون وإدارة الحدود والتطبيقات العسكرية. كما يتناول كذلك المزايا الخاصة بمشاركة البيانات البيومترية على الصعيد ثنائي الأطراف، ومتعدد الأطراف، والإقليمي والعالمي، وكيف يمكن للبيانات البيومترية، عند استخدامها مع بيانات الاستخبارات الأخرى، أن تُستخدم بشكل استباقي لمنع الأعمال الإرهابية، إضافةً إلى دورها بصفتها أداة من أدوات التحقيق. ومن ثمَّ يتم النظر في الإجراءات التي اتخذتها السلطات نتيجة لحالات التطابق البيومتري، ضمن السياق المعني بحقوق الإنسان الدولية والحاجة إلى استجابة مستنيرة وقانونية ومتناسبة. ويغطي الجزء الأخير من القسم عملية تضمين الأنظمة البيومترية في استراتيجيات مكافحة الإرهاب الخاصة بالمناطق والدول الأعضاء والدور الأساسي لوكالات إنفاذ القانون وضبط الحدود في تقديم الدعم بفعالية إلى هذه الاستراتيجيات.

هذا العرض التجميعي عبارة عن وثيقة قابلة للتعديل وهو نسخة خاضعة للرقابة من أجل:

- الحفاظ على حداثته واستجابته للتقدم السريع في الابتكار التكنولوجي والتطور العلمي ضمن مجال الأنظمة البيومترية
- وليكون ملائمًا ووثيق الصلة بالتهديدات الجديدة ومستمرة الظهور على صعيد الإرهاب الدولي.

تمهيد

إن قرار مجلس الأمن رقم 2322 (2016)، بشأن تعزيز إنفاذ القانون والتعاون القضائي على الصعيد الدولي في سبيل مكافحة الإرهاب، يدعو الدول الأعضاء بوضوح إلى مشاركة المعلومات – بما في ذلك البيانات البيومترية ومعلومات السير الذاتية – عن المقاتلين الإرهابيين الأجانب (FTFs) وغيرهم من الأفراد الإرهابيين والمنظمات الإرهابية. وقد نص المجلس في قراره الصادر برقم 2396 (2017)، على ضرورة أن تقوم الدول بتطوير النظم وتفعيلها لجمع البيانات البيومترية، وذلك بما يتوافق مع القانون المحلي والقانون الدولي لحقوق الإنسان، وقد تتضمن تلك البيانات بصمات الأصابع، والصور الفوتوغرافية، والتعرف إلى الأشخاص من سمات وجوههم، وغيرها من البيانات البيومترية لتحديد الهوية ذات الصلة، وذلك من أجل تحديد هوية الإرهابيين على نحو مسؤول ومناسب، ومنهم المقاتلون الإرهابيون الأجانب. كما شجع القرار كذلك الدول على مشاركة هذه البيانات على نحو مسؤول مع غيرها من الدول، ومع المنظمة الدولية للشرطة الجنائية (الإنتربول) كذلك وغيرها من الهيئات الدولية وثيقة الصلة بالموضوع.

إن التبادل الفعال للبيانات البيومترية أمر أساسي للتحقيق في الجرائم العابرة للحدود ولكشف هوية الإرهابيين. ففي السياق المعني بالتحقيقات المتعلقة بالإرهاب، يمكن للتقنية البيومترية وغيرها من التقنيات الجنائية تقديم مساعدة كبيرة إلى المحققين والمدعين العامّين من خلال - على سبيل المثال - ربط أي فرد بنشاط أو حدث أو مكان أو مادة معينة أو ربطه بفرد آخر. ولذلك كان تعزيز قدرات الدول الأعضاء في هذا المجال أمرًا بالغ الأهمية.

لقد قام الفريق العامل المعني بإدارة الحدود وإنفاذ القانون فيما يتعلق بمكافحة الإرهاب التابع لفرقة العمل المعنية بالتنفيذ في مجال مكافحة الإرهاب (CTITF) بصياغة العرض التجميعي الحالي للممارسات الجيدة والتوصيات، وذلك بدعم مالي من مركز الأمم المتحدة لمكافحة الإرهاب (UNCCT)، الموجود ضمن مكتب الأمم المتحدة لمكافحة الإرهاب (UNOCT). ويتناول العرض التجميعي القضايا الحاسمة، مثل: الحوكمة، والتنظيم، وحماية البيانات، وسياسة الخصوصية، وحقوق الإنسان، إضافةً إلى إدارة المخاطر وتقييمات مواطن الضعف.

يجب أن تتناول الحكومات الآثار المترتبة على هذه التقنية في مجال حقوق الإنسان من أجل حماية هؤلاء الذين يتم تحديد هوياتهم عن طريق مثل هذه الأنظمة من التعرض للإساءة وضمان أن الإجراءات التي يتم اتخاذها في مرحلة التخطيط وفيما بعد ذلك تتم بما يتوافق مع التزامات القانون الدولي، كما تنص على ذلك صكوك حقوق الإنسان الدولية والإقليمية. وكما هو الحال مع جميع تدابير الحماية، تعاني الأنظمة البيومترية مواطن ضعف. والأمر المهم هنا هو الكيفية التي يتم بها تحديد مواطن الضعف بالنظام وفهمها والحد منها. فلا شك أن التصميم الحذر والتسجيل الدقيق للبيانات البيومترية وكيفية تحديد معايير التطابق أمر حاسم في نجاح النظام. وهناك عدد من التقنيات، على صعيد كلٍّ من البرامج والأجهزة، يمكن استخدامها لاكتشاف خطر هجمات الانتحال[1] ومكافحته والتقليل منه.

لقد تم إعداد هذا العرض التجميعي بالتعاون مع معهد القياسات الحيوية، وهو منظمة غير هادفة للربح، تعمل على تعزيز الاستخدام الأخلاقي والمسؤول للأنظمة البيومترية ويقدم محفلًا مستقلًا وغير متحيز إلى مستخدمي الأنظمة البيومترية وغيرهم من الأطراف المهتمة. يعمل معهد القياسات الحيوية بشكل وثيق مع المديرية التنفيذية للجنة مكافحة الإرهاب لتشكيل اتحاد دولي من الخبراء لتوجيه عملية إعداد العرض التجميعي، بما في ذلك الخبراء الحكوميون وخبراء الأنظمة البيومترية أصحاب الخلفية في مجال مكافحة الإرهاب، وإنفاذ القانون، وإدارة الحدود، والتقنية البيومترية، والخصوصية وحماية البيانات.

[1] "الانتحال" (يُعرف كذلك باسم هجوم عرض) هو عرض سمات بيومترية زائفة (مثل: قناع وجه مطاطي، أو صورة فوتوغرافية، أو إصبع زائف، أو تسجيل صوتي زائف) لمستخدم قانوني مُسجل للتمكن من الوصول غير المصرح به إلى أي نظام للتعرف إلى السمات البيومترية.

لقد تم إعداد العرض التجميعي ضمن إطار مشروع طويل الأمد يهدف إلى تعزيز قدرة الدول والكيانات الدولية والإقليمية ذات الصلة على جمع البيانات البيومترية عن الإرهابيين، ومنهم المقاتلون الإرهابيون الأجانب، وتسجيلها ومشاركتها، بما يتوافق مع قرارات مجلس الأمن الموضحة أعلاه. وقد قام بتنفيذ مشروع الأنظمة البيومترية هذا المديرية التنفيذية للجنة مكافحة الإرهاب، بالتعاون مع كيانات فرقة العمل المعنية بالتنفيذ في مجال مكافحة الإرهاب، مثل: الإنتربول، ومكتب الأمم المتحدة المعني بالمخدرات والجريمة، ومنظمة الطيران المدني الدولي، ومفوضية الأمم المتحدة السامية لشؤون اللاجئين. وتتمثل أهداف المشروع في زيادة الوعي بالمبادرات الإقليمية والدولية الرامية إلى تشجيع عملية استخدام الأنظمة البيومترية، وتعزيز التعاون والتنسيق بين الكيانات وثيقة الصلة بالموضوع، وتحسين استخدام الأنظمة البيومترية ومشاركتها على الصعيد العالمي، بما في ذلك من خلال تشجيع التضمين المنهجي للبيانات البيومترية المرتبطة بالصور النمطية للإرهابيين في قواعد البيانات والنشرات الخاصة بالإنتربول وزيادة فعالية المساعدة المقدمة إلى الدول الأعضاء في هذا الميدان.

فلاديمير فورونكوف
وكيل الأمين العام
مكتب الأمم المتحدة لمكافحة الإرهاب
المدير التنفيذي
مركز الأمم المتحدة لمكافحة الإرهاب

ميشيل كونينسكس
مساعد الأمين العام
المدير التنفيذي
المديرية التنفيذية للجنة مكافحة الإرهاب

حول معهد القياسات الحيوية

يرحب معهد القياسات الحيوية بالفرصة لدعم هذا المشروع، وذلك بوصفه منظمة غير هادفة للربح، ويشجع على الاستخدام المسؤول والأخلاقي للأنظمة البيومترية. ويقدم معهد القياسات الحيوية محفلًا مستقلًا ودوليًّا غير متحيز إلى مستخدمي الأنظمة البيومترية وغيرهم من الأطراف المهتمة. ويتمثل دوره في تثقيف أعضائه والجهات الرئيسية صاحبة المصلحة والجمهور بشأن الأنظمة البيومترية وتزويدهم بالمعلومات عنها؛ ودعم عملية تطوير المعايير والسياسة وأفضل الممارسات والتوعية بها، وتعزيز السلامة والحماية في أنظمة البيانات البيومترية وبرامجها.

لقد تأسس المعهد في عام 2001 وله مكاتب في لندن وسيدني. وتغطي قاعدة عضويته التي تضم أكثر من 230 منظمة من 30 بلدًا مختلفًا نطاقًا عريضًا من المستخدمين، مثل: وكالات الحكومة، والحدود، وسلطات إنفاذ القانون، والبنوك وشركات الطيران، إضافةً إلى الباحثين والبائعين وخبراء الخصوصية. ولا ينصب اهتمام المعهد على تشجيع التقنيات البيومترية، بل على الاستخدام المسؤول لأنظمة البيانات البيومترية، وسلامتها وحمايتها، والأهم من ذلك الخصوصية وحماية البيانات. ويدرك المعهد أن أنظمة البيانات البيومترية تعاني مواطن ضعف كامنة يجب تحديدها والتخفيف منها.

الأنظمة البيومترية والخصوصية وحقوق الإنسان

يزيد انتشار مفهوم الأنظمة البيومترية، كما يزيد في نفس الوقت، تقبل الجمهور للتقنية، وذلك من خلال استخدام الأنظمة البيومترية على الهواتف المحمولة دون العلم بالضرورة بالآثار المترتبة على ذلك. وهذا الأمر يسلط الضوء على الحاجة إلى المزيد من التثقيف بشأن المزايا والمخاطر الخاصة بالتطبيقات البيومترية. الأنظمة البيومترية مريحة ويمكنها تقديم مستوى أعلى من الأمان. ومع ذلك، لا يزال هناك صعوبات، مثل حماية الحق في الخصوصية، وحماية البيانات، ومكافحة الانتحال. فيجب عدم جمع البيانات الشخصية، مثل البيومترية، وتخزينها إلا بشكل متناسب وإذا دعت الحاجة إلى ذلك.

تضطلع الأنظمة البيومترية بدور مهم *على نحو متزايد* في سبيل مكافحة الإرهاب على مستوى العالم، أي مكافحة الاحتيال، وانتحال الشخصية، وغيرها من الجرائم الجنائية التي يستغلها الإرهابيون لدعم عملياتهم. ولكن لكي ندرك القدرات الكاملة للأنظمة البيومترية، يجب على الحكومات كذلك الاهتمام بحماية الذين يتم تحديد هوياتهم بواسطة مثل تلك الأنظمة وضمان أن عملية الجمع والتخزين والاستخدام للبيانات البيومترية تتم بما يتوافق مع قوانين الخصوصية وحقوق الإنسان الدولية، بما فيها العهد الدولي للحقوق المدنية والسياسية وإعلان الأمم المتحدة العالمي لحقوق الإنسان.

يجب أن يحظى الأفراد، الذين يتعرضون لسرقة هوياتهم/بياناتهم البيومترية أو الذين يقعون ببساطة ضحية لأحد أخطاء النظام، بالحماية. فاستعادة هوية أحد الأشخاص ليست بنفس بساطة إعادة تعيين إحدى كلمات المرور. فالبيانات البيومترية تبقى معك طوال حياتك والعناية الكاملة مطلوبة لذلك. يوضح هذا العرض التجميعي المشاكل والحلول الممكنة لهذه المهمة الصعبة للمزج بين استراتيجيات مكافحة الإرهاب الفعالة والحق في الخصوصية وحقوق الإنسان الأخرى.

مواطن الضعف والهجمات على الأنظمة البيومترية

كما هو الحال مع جميع تدابير الحماية، تعاني الأنظمة البيومترية مواطن ضعف. والأمر المهم هنا هو الكيفية التي يتم من خلالها الحد من مواطن الضعف بالنظام. فلا شك أن التصميم الحذر والتسجيل الدقيق للبيانات البيومترية وكيفية تحديد معايير التطابق أمر حاسم في نجاح النظام. قد يؤدي إرساء المعايير المرتفعة جدًا إلى ظهور "سلبيات زائفة"، تحرم المستخدم الحقيقي من الوصول. ولكن قد يؤدي إرساء معايير منخفضة إلى ظهور "إيجابيات زائفة" تسمح بوصول المستخدمين المحتالين.

لقد تبنى معهد القياسات الحيوية مستوى معقولًا من العناية لضمان دقة المواد المقدمة في هذا العرض التجميعي. وبسبب المحتوى والمعطيات المتغيرة أثناء عملية تنفيذ التقنية البيومترية وبعدها، لا يتحمل المعهد المسؤولية عن النتائج أو الامتثال. لقد أعد هذا العرض التجميعي لأغراض معلوماتية فقط وليس المقصود منه تقديم نصائح قانونية أو متعلقة بالامتثال.

أندرو رايس
الرئيس والمدير
معهد القياسات الحيوية

إيزابيل موللر
الرئيس التنفيذي
معهد القياسات الحيوية

1- مقدمة عن الأنظمة البيومترية والهوية

يقدم القسم 1 العناصر الأساسية للتقنية البيومترية وإدارة شؤون الهوية، بما في ذلك الاستخدام الموسع للأنظمة البيومترية في مجالات علم الأدلة الجنائية وتحقيقات إنفاذ القانون والتعقيدات الإضافية التي تنجم عن ذلك.

البشر ما هم إلا حيوانات اجتماعية تمتلك قدرة استثنائية على الإدراك، ومن ثمَّ تمييز الأشخاص المألوفين لديهم. كما أن البشر يمتلكون، في نفس الوقت، إحساسًا قويًا بالذات وبتفردهم بصفتهم شخصيات فردية. وبفضل غرائزنا الاجتماعية نعد أنفسنا شخصيات فردية متفردة ويمكننا إدراك الشخصية الفردية للآخرين. وعلى المستوى البيولوجي، البشر متفردون من نوعهم (بالنسبة إلى جميع الأغراض العملية). ومع ذلك، فإن "ماكينة التعرف إلى البشر" لدينا لا تعمل من الناحية البيولوجية، وفي الحقيقة مستوى أداء البشر سيء في مجال تمييز الأشخاص غير المألوفين لديهم. وأنظمة تحديد الهوية التي يستخدمها البشر لا تعمل باستخدام السمات البيولوجية كذلك. وبدلًا من ذلك، يستخدمون مجموعات من سمات تحديد الهوية والسمات السياقية بمنزلة علامات لتمثيل، وليس لتمييز، الكيان البيولوجي الذي يصفونه[2].

تتضمن سمات تحديد الهوية الأسماء، وتاريخ الميلاد ومحله، والجنسية، والنوع الاجتماعي، والقياسات الحيوية[3] المحدِّدة للهوية. والسمات السياقية هي المعلومات بشأن المعاملات، التي ترتبط على الأغلب بالمكان والزمان. واستخدام السمات السياقية يُحسِّن عملية تأكيد الهوية. وقد تكون سمات تحديد الهوية إما سيرًا ذاتية أو بيومترية وربما، في ظل ظروف معينة، تكون عرضة للتغيير. فقد يتضمن التغيير في سمات تحديد الهوية من نوع السير الذاتية، على سبيل المثال:

- ☐ الأسماء – تخضع لاختلاف الكتابة، أي أن هناك عدة هجاءات لنفس الاسم
- ☐ تاريخ الميلاد – يخضع للتسجيل المتأخر أو للتضارب في السجلات الرسمية
- ☐ محل الميلاد – يمكن تقديمه بعدة طرق
- ☐ النوع – يخضع لتفضيل الفرد، وإعادة التشكيل المادي، وغير ذلك
- ☐ المواطنة – يمكن تعددها وعرضة للتغيير

خلال دورة حياة الإنسان، قد تتعرض سمات تحديد الهوية البيومترية للتغيير، مثل: حجمها النسبي أو وضوح الملامح البارزة وإمكانية تحديدها، وذلك عبر عملية النمو وكبر العمر أو المرض. قد يعاني بعض الأفراد فقدان السمات البيومترية أو تلفها. وهكذا، على سبيل المثال، تتشكل بصمات الأصابع في المراحل المبكرة من الحمل وتظل دون تغيير طوال الحياة، ما لم تتعرض للتلف، وقد تظل كما هي لوقت طويل بعد الوفاة، وخاصة في البيئات الدافئة الجافة التي تؤدي إلى تجفيف الجلد. ورغم أن ترتيب التضليع ضمن هيكل البصمة يظل ثابتًا، إلا أن البصمة ذاتها عرضة للتغييرات في المقاس بفعل مرور الزمن، وجودة الملامح التي تمتلكها البصمة قد تتدهور بفعل الإساءة البيئية أو كبر العمر أو غير ذلك من التلف. وقد تتعرض السمات البيومترية الأخرى لتغييرات مشابهة. وتبعًا لذلك، يجري تصميم الخوارزميات الحديثة المستخدمة في التطبيقات البيومترية لإجراء تعديلات معقولة لهذه التغييرات حتى يمكن تسجيل أقصى عدد من الأشخاص والاحتفاظ به في أي نظام بغض النظر عن متغيرات العمر أو التدهور الطفيف في ملامحهم البيومترية.

---

[2] *التحقق من الهوية - أهمية السياق واستمرار الهوية*، ص 11-16 مجلة Keesing Journal of Documents & Identity، التقرير السنوي لإدارة الهوية لعام 2011-2012

[3] في عام 1995، تم تعريف "الأنظمة البيومترية" بواسطة الموجز البيومتري لحكومة الولايات المتحدة على أنها "...التعرف الآلي إلى الأفراد اعتمادًا على سلوكهم وخصائصهم البيولوجية."

العلامات البيومترية هي سمات تحديد الهوية ولأنها تمثل بدرجة كبيرة البشر الذين تصفهم، فإنها تقدم أساسًا جيدًا للمقارنات الرقمية. ومع ذلك، ومثل سمات تحديد الهوية من نوع السير الذاتية، نجد أن العينة البيومترية بمجرد التقاطها في شكل صورة أو تحويلها إلى قالب أو صورة نمطية تختلف عن الكيان البيولوجي الذي تصفه. إن التقاط سمات تحديد الهوية وتسجيلها، بما فيها السمات البيومترية، هي عملية يشوبها دائمًا عدم الاكتمال وعدم الكمال ومن ثمَّ قد تكون عرضة للخطأ. فالتطابق الاحتمالي الكامن في المقارنات البيومترية عرضة للاختلاف الإحصائي. ولا شك أن وجود الخطأ والاختلاف الإحصائي في أنظمة التعرف إلى البشر يمكن أن يُوجد احتمال تعرضها لمجموعة متنوعة من الهجمات (راجع القسم 2-3) ما لم يتم اتخاذ ضمانات قوية وتحديثها باستمرار كجزء من عملية إدارة مخاطر النظام.[4] والتخفيف من مواطن الضعف الكامنة هذه هو الموضوع الأساسي لهذا العرض التجميعي.

تصمم الأنظمة البيومترية لتمييز الأفراد باستخدام خصائصهم البيولوجية والفسيولوجية، مثل: بصمات الأصابع وأنماط أوردة اليدين والحدقة والوجه والحمض النووي وغيرها.[5] حيث يمثل كلٌّ منها شكلًا بيومتريًا. ويعتمد اختيار الشكل أو الأشكال البيومترية الأفضل على السياق الخاص بحالة استخدام التطبيق (راجع القسم 2-5). وعامة، تتشارك الأشكال البيومترية في الملامح[6] التي تجعلها كما يلي، وذلك إلى حد كبير أو صغير:

- ☐ عامة – يمكن العثور عليها في جميع الأفراد (باستثناء من يعاني ملامح بيومترية تالفة أو مفقودة)
- ☐ فريدة – يجب أن تكون قادرة على التمييز بين الأفراد ضمن قطاع السكان المُسجل. وقد يختلف ذلك في أشكال بيومترية معينة، على سبيل المثال، سيتشارك التوائم المتماثلة نفس صورة الحمض النووي ولكن ستختلف بصمات أصابعهم.
- ☐ دائمة – يجب أن تكون مستمرة وثابتة على مر الزمان، فيما يتعلق بخوارزمية التطابق، مع الأخذ في الاعتبار الاختلافات الناجمة عن دورة حياة الإنسان
- ☐ قابلة للقياس – يجب أن يسهل على النظام الحصول عليها ومعالجتها رقميًّا
- ☐ تقدم أداء فعالًا – يجب أن تكون دقيقة وسريعة وقوية في عمليات العمل الرئيسية والإحالة
- ☐ مقبولة – يجب أن تلبي المعايير والتوقعات الاجتماعية وأن تكون متاحة للاستخدام من جانب نسبة كبيرة من قطاع السكان المسجل المقصود
- ☐ عرضة لخطر الإفساد – من المحتمل أن يتمكن النصابون من الوصول غير المصرح به باستخدام العديد من الأدوات والبدائل ما لم يتم استخدام تدابير مضادة صارمة وتحديثها باستمرار

[4] "أنظمة التعرف إلى البشر احتمالية في الأساس، ولذلك فهي عرضة للخطأ بطبيعتها. ويمكن التقليل من فرص الخطأ وليس القضاء عليها. ويجب على مصممي النظام ومشغليه توقع حدوث أخطاء والتخطيط لذلك، حتى إذا كان المتوقع أن تكون الأخطاء نادرة." صفحة 1، *التعرف إلى السمات البيومترية: التحديات والفرص، مجلس البحوث الوطني، واشنطن (2010)، متاح للتنزيل على:* http://www.nap.edu/openbook.php?record_id=12720&page=1

[5] **ملاحظة** يتناول هذا العرض التجميعي بصفة أساسية تلك السمات البيومترية الجسمية التي ترتبط بهوية الإنسان (الوجه، والبصمات، والحمض النووي، وما شابه ذلك) وليس السلوك. وتشمل السمات البيومترية السلوكية الأشكال البيومترية مثل طريقة المشي، وخصائص استخدام لوحة المفاتيح و"الماوس"، والتواقيع المكتوبة، وغيرها، والتي تقيس أنماط النشاط البشري.

[6] القائمة مقتبسة من جاين وآخرين "الأنظمة البيومترية: كشف الهوية الشخصية في المجتمع المترابط شبكيًا"، نورويل، ماساتشوستس: دار Kluwer Academic Publisher (1999)

نظرًا إلى أن معظم الأنظمة البيومترية تنطوي على مقارنات مع بيانات مرجعية، فإن العامل الأساسي عند اختيار شكل بيومتري مفضل هو توفر البيانات القديمة التي تكون، أو يمكن أن تكون، مجمعة في قاعدة بيانات مرجعية مفيدة وقابلة للاستخدام لإثبات الهوية والتحقق منها. ويمكن للأنظمة استخدام شكل بيومتري واحد فقط (وظيفة أحادية الشكل)، كالتعرف إلى الأشخاص من سمات وجوههم على سبيل المثال، أو جمع أشكال بيومترية (وظيفة متعددة الأشكال) مثل البصمات والحدقة والوجه. وهناك مجموعة من التطبيقات آخذة في التوسع السريع للأنظمة البيومترية عبر القطاعات العامة والتجارية، بما في ذلك:

- ☐ السجلات الوطنية المدنية لتسهيل الوصول إلى خدمات الحكومة المحلية أو الوطنية
- ☐ رخص القيادة
- ☐ سجلات العدالة الجنائية
- ☐ كشف الجرائم
- ☐ المراقبة بكاميرات الفيديو
- ☐ أنظمة إصدار جوازات السفر/أمن الحدود
- ☐ مساعدة اللاجئين
- ☐ الخدمات المالية
- ☐ أنظمة الكمبيوتر
- ☐ الوصول إلى قاعدة بيانات مؤمنة
- ☐ دخول الأماكن
- ☐ دخول الهواتف الذكية
- ☐ إدارة هوية الرعاية الصحية
- ☐ إدارة الحضور إلى مكان العمل

يمكن للأشكال البيومترية المستخدمة في هذه التطبيقات تحديد هوية أي فرد حتى إذا قدم مواصفات فردية زائفة أو حاول انتحال صفة شخص آخر. وهذه سمة لا تقدر بثمن ويمكن الاستفادة منها بصورة كبيرة في تتبع الإرهابيين والكشف عنهم وإيقاف أنشطتهم على الصعيد العالمي. هناك ثقافة بحث وتطوير تجارية تتسم بالقوة والنشاط في الأنظمة البيومترية وتظهر تطبيقات جديدة على نحو منتظم في السوق، إضافةً إلى الأشكال البيومترية الجديدة.

إن نموذج التشغيل القياسي لأي نظام بيومتري أساسي، مثل النظام المستخدم لمراقبة الدخول، يتضمن المراحل الآتية:

- ☐ *الحيازة والتسجيل* – الحصول على عينة بيومترية من أي فرد (شخص) باستخدام جهاز لالتقاط البيانات. ويمكن إتمام عملية الحيازة باستخدام إما جهاز مثبت في موقع دائم وثابت أو جهاز متحرك يمكنه تحميل البيانات من موقع بعيد. ويمكن الحصول على السمات البيومترية بملامسة جهاز التقاط البيانات (مثل بصمات الأصابع)، سواء من مكان قريب كما يحدث في حالة الالتقاط الفوري لصور الوجه أو عن بُعد. إلا أن عامل النجاح الحاسم لأي نظام هو جودة السمات البيومترية المسجلة. فالتسجيلات ذات الجودة الرديئة ستقلل بشكل ملحوظ أداء النظام، ولذلك من المهم الحصول باستمرار على مستوى عالٍ من البيانات البيومترية من أجل توفير إمكانية تطابق أفضل (راجع القسم 2-3-3-).
- ☐ *استخلاص البيانات* – تحويل العينة التي تم الحصول عليها إلى قالب بيومتري، على سبيل المثال قد تتم معالجة صورة بصمة إلى مصفوفة رقمية من الأرقام لأغراض التخزين والبحث والمقارنة. وهكذا، تُصمم عملية استخلاص البيانات لتحويل الصورة الخام أو العينة الأصلية إلى مجموعة بيانات رقمية فعالة ومفيدة يمكن البحث فيها ومقارنتها بدقة بالقوالب المرجعية الموجودة في قاعدة البيانات، إضافةً إلى حاجتها إلى مساحة تخزين قليلة للغاية ضمن النظام مقارنة بالصورة/العينة البيومترية الأصلية.
- ☐ *تخزين البيانات* – استبقاء البيانات المسجلة في النظام أو قاعدة البيانات، وقد تقتصر أحيانًا على قالب واحد فقط لكل شخص بعد اكتمال مرحلة البحث/المقارنة. وتقوم معظم أجهزة التقاط البيانات بتحميل البيانات إلى خادم أو قاعدة بيانات مركزية لإتاحة البحث، ولكن بعض الأجهزة المتحركة تمتلك قاعدة بياناتها المتكاملة الخاصة حتى يمكن استخدامها عن بُعد دون الحاجة إلى الاتصال بأي معدات أخرى.
- ☐ *مقارنة البيانات* – الوصول إلى قاعدة البيانات واستعادة قالب واحد أو أكثر من القوالب المسجلة مسبقًا للمقارنة مع القالب الحالي محل البحث.
- ☐ *مطابقة البيانات* – استخدام خوارزميات الحوسبة لتحديد ما إذا كان القالب محل البحث يطابق قالب (قوالب) قاعدة البيانات المحدد. ولا يتم عادة الاحتفاظ بالقوالب محل البحث إذا تمت مطابقتها بأي قالب مرجعي موجود في قاعدة البيانات.
- ☐ *النتيجة* – سيدعم الناتج، سواء "تطابق" أو "عدم تطابق"، وظيفة النظام الكلي، فعلى سبيل المثال، إذا تم تصميم المكون البيومتري للتحقق من مدى توافق هوية مع الهويات الموجودة في قاعدة البيانات لأصحاب حق الوصول الشرعي إلى مبنى مؤمن، فإن

نتيجة "تطابق" ستسمح بالدخول، وذلك اعتمادًا على التحقق مقابل قالب الهويات المؤكدة، ولكن ستؤدي النتيجة "عدم تطابق" إلى رفض الدخول.

ولكن، لا تلجأ كل التطبيقات إلى استخدام الهويات المؤكدة نظرًا إلى وجود عمليتين مختلفتين في الأساس يتم استخدامهما في الأنظمة البيومترية. العملية الأولى التي تستخدم الهوية المؤكدة، هي:

التحقق – (تعرف كذلك باسم مقارنة واحد لواحد أو مقارنة 1:1). يستخدم هذا النموذج هوية مؤكدة لتحديد قالب واحد فقط من قاعدة البيانات أو وثيقة إلكترونية للمقارنة مع القالب محل البحث. إنها عملية تقارن القالب محل البحث بقالب قاعدة البيانات وإما تؤكد نشأة كلا القالبين من نفس الشخص وإما تنفي ذلك.
تطرح عملية التحقق السؤال "هل أنت نفس الشخص الذي تمت مصادقة هويته بالفعل وتسجيلها في قاعدة البيانات؟"

العملية الثانية التي تُعد نموذج بحث، هي:

المطابقة – (تعرف كذلك باسم مقارنات واحد للكثير أو 1:كثير) هذه وظيفة بحث لا تعتمد على هوية مقترحة، ولذلك فإن القالب محل البحث يبحث في قاعدة البيانات بالكامل للعثور على تطابق محتمل. ويقوم برنامج البحث والمطابقة بإصدار نتيجة تشابه لحالات التطابق المحتملة وإما يحدد تلقائيًا تطابقًا عالي الثقة وإما يقدم قائمة مرشحة بحالات التطابق المقترحة إلى مشغل بشري ليقوم بالمقارنة مع القالب محل البحث.
تطرح عملية المطابقة السؤال "هل أنت موجود في قاعدة البيانات المرجعية، وإذا كنت كذلك، فما السجل الذي تتطابق معه؟"

تعتمد القيمة والسياق الخاصان بالنتائج الصادرة عن أنظمة إما التحقق وإما المطابقة على نموذج التشغيل الخاص بالتطبيق. على سبيل المثال، في بعض الحالات قد تكون المطابقة الإيجابية هي النتيجة الروتينية والنتيجة السلبية هي الاستثناء (مثل دخول شخص إلى منطقة مؤمنة) ولكن في نماذج أخرى، تكون النتيجة السلبية هي الأمر المتوقع العادي وتكون النتيجة الإيجابية هي الاستثناء (مثل البحث عن جميع الركاب ضمن قائمة المراقبة البيومترية للإرهابيين). تدمج الأنظمة البيومترية الفعالة مهام التحقق والمطابقة المنفصلة لتحسين تأكيد الهوية وموثوقية المقارنات بقواعد البيانات المرجعية.

قد يبدو للمستخدم أن العديد من التطبيقات البيومترية مؤتمتة بالكامل بداية من الحيازة ووصولًا إلى النتيجة، ولكن التدخل البشري مطلوب غالبًا في الأنظمة الأكثر تعقيدًا، وفي مراحل متعددة خلال العملية، لضمان عمل النظام بسلاسة حتى إذا لم يتضح ذلك للمستخدم. ومع ذلك، ومع النمو الثابت والمستمر للقدرة الحاسوبية وتقنيات المعالجة الجديدة، فإن الحاجة إلى التدخل البشري تقل بسرعة، ولكن بينما نتوقع أن يصبح التطابق الآلي للعينات البيومترية هو القاعدة الشائعة، ستظل على الأرجح عملية اتخاذ القرار بيد الإنسان في الحالات الأكثر تعقيدًا، عندما يتعلق الأمر بربط العينات المتطابقة بالسمات السياقية وسمات تحديد الهوية الأخرى.

دراسة الحالة 1 – الأنظمة البيومترية عند الحدود

إن تصريح عبور الحدود للمسافرين عبر نظام التحقق 1:1، يتشارك معلوماته مع تقييمات مخاطر المسافرين ويتسلَّم معلومات منها باستخدام مقارنات 1:كثير مقابل قوائم المراقبة وقواعد بيانات الاستخبارات (راجع الشكل 1). وتكون سمات تحديد الهوية المسجلة في قوائم المراقبة وقواعد بيانات الاستخبارات غير كاملة عادة. وذلك لأن الأهداف المراد تضمينها في قوائم المراقبة يتم تحديد هويتها من خلال مجموعة من الظروف والمعايير المختلفة. ولا تتيح كل السمات البيومترية وسمات السير الذاتية إمكانية ربطها بكل قائمة مراقبة أو قائمة استخبارات. كما أن السمات السياقية ليست كاملة. وجميع عناصر السمات الموجودة في قوائم المراقبة وقواعد بيانات الاستخبارات تكون عرضة للخطأ.

الشكل 1 - مقتبس من *دليل إدارة مراقبة الحدود لبرنامج تحديد هوية الركاب التابع لمنظمة الطيران المدني الدولي (الإيكاو)، مونتريال (2018) (بإذن من الإيكاو)*

المقارنة	مصدر البيانات المرجعية	أساس مقارنات السير الذاتية	أساس المقارنات البيومترية	ارتباط السمات السياقية
التحقق ١:١	وثائق السفر	• الاسم • تاريخ الميلاد • النوع • الجنسية	• الوجه • البصمة • الحدقة	• فحص الوقت والمكان • الجنسية • وثائق السفر
المطابقة ١:كثير	- قوائم المراقبة - الاستخبارات	• الاسم • تاريخ الميلاد • النوع • الجنسية	• الوجه • البصمة • الحدقة • الصوت • الحمض النووي	• الوقت والمكان • الوثائق الصادرة أو المسروقة حسب الإنتربول • الأحداث السابقة • ارتباط السمات (الهاتف المحمول، جهات اتصال البريد الإلكتروني غير ذلك)

تُسهِم الهويات المُتحقق منها في الربط بمزيد من الموثوقية بين سمات السير الذاتية والبيومترية والسياقية ومن ثمَّ المزيد من عمليات البحث الفعالة في قوائم المراقبة وقواعد بيانات الاستخبارات. كما تُسهِم المقارنات البيومترية بصورة كبيرة في تحديد نتائج التطابق، ولكن لا تقرر هذا الأمر وحدها.[7]

[7] راجع دليل إدارة مراقبة الحدود لبرنامج تحديد هوية الركاب التابع لمنظمة الطيران المدني الدولي (الإيكاو)، مونتريال (2018) للاطلاع على المزيد من التفاصيل

1-1 أداء النظام

سيعتمد أداء أي نظام بيومتري بصورة كبيرة على (1) النطاق والحجم للاستخدام المقصود، و(2) اختيار الشكل أو الأشكال البيومترية الأكثر ملاءمة لدعم هذا التطبيق، و(3) المعالجة الموثوقة والمتسقة والآنية المدعومة بمتطلبات صيانة قليلة. مقاييس الأداء الرئيسية للأنظمة البيومترية هي المعدلات والأحجام للدقة، ومعدل الأخطاء[8]، والإنتاجية ومعالجة الاستثناء. وبصفة عامة، الدقة هي مقياس قدرة النظام على المطابقة الصحيحة لسمات تحديد الهوية البيومترية من نفس الشخص، وفي نفس الوقت، تجنب المطابقة الخاطئة لسمات تحديد الهوية البيومترية من شخص مختلف. وتستخدم المكونات الآتية للتعبير عن دقة أي نظام بيومتري، إما في صورة نسبة مئوية وإما حصة وتُستمد عادة من التجارب الميدانية أو الاختبارات المعملية.

معدل القبول الصحيح (TAR) – مقياس قدرة النظام على المطابقة الصحيحة لسمات تحديد الهوية البيومترية من نفس الشخص.

معدل القبول الخاطئ (FAR) – يظهر القبول الخاطئ عندما يتطابق القالب البيومتري محل البحث من أحد الأشخاص نتيجة خطأ النظام مع القالب البيومتري لشخص آخر في قاعدة البيانات. معدل القبول الخاطئ هو عدد حالات القبول الخاطئة في صورة نسبة من العدد الإجمالي للاستعلامات البيومترية التي كان يجب رفضها، أي عدد حالات عدم التطابق *التي أصدرها النظام وقدمها على أنها حالات تطابق* في شكل نسبة من حالات عدم التطابق الأصلية.

معدل الرفض الصحيح (TRR) – مقياس عدد الحالات التي تكون فيها سمة تحديد الهوية البيومترية لأحد الأشخاص *غير* مطابقة على نحو صحيح لسمات تحديد الهوية البيومترية للآخرين في قاعدة البيانات، أي عدد حالات عدم التطابق الصحيحة.

معدل الرفض الخاطئ (FRR) – يظهر الرفض الخاطئ عندما يكون القالب البيومتري محل البحث غير مطابق لقالب قاعدة البيانات الصحيح رغم أنهما من نفس الشخص. معدل الرفض الخاطئ هو عدد حالات الرفض الخاطئة في صورة نسبة من العدد الإجمالي للاستعلامات البيومترية التي كان يجب قبولها، أي عدد حالات التطابق *التي أصدرها النظام وقدمها على أنها حالات عدم تطابق* في شكل نسبة من حالات التطابق الأصلية.

ولذلك، من المجدي عند تصميم النظام زيادة معدل القبول الصحيح ومعدل الرفض الصحيح مع تقليل معدل القبول الخاطئ ومعدل الرفض الخاطئ. على سبيل المثال، وبشرح بسيط، إعداد الدقة بنسبة 70٪ في معدل القبول الصحيح سيؤدي إلى معدل القبول الخاطئ بنسبة 30٪ بينما إعداد الدقة بنسبة 97٪ في معدل القبول الصحيح سيعني الحصول على معدل القبول الخاطئ بنسبة 3٪ فقط. وتجدر الإشارة إلى عدم وجود نظام بيومتري يعمل بمعدل دقة بنسبة 100٪.

[8] يتطلب حساب معدلات الأخطاء تبني فكرة تجريدية، افتراض وجود مجموعة مغلقة، للسماح بالإكمال اللاحق لعملية مقارنة الكل: لقاعدة البيانات لاستنتاج معدلات الأخطاء وحسابها. وتتم هذه الحسابات في العديد من الحالات في عمليات المحاكاة باستخدام مجموعات بيانات قياسية قد تكون - أو لا تكون - تمثيلًا للبيانات الفعلية في العالم الواقعي. وقد تكون الفكرة التجريدية لمعدل الخطأ مفيدة في تصميم النظام وتوقع أداء التحقق 1:1. في العالم الواقعي، مع وجود قطاع سكان عالمي يزيد عن 7 مليارات، من الممكن وجود بدائل من خارج المجموعة، وتكون متوقعة الظهور في حالة قوائم المراقبة وقواعد بيانات الاستخبارات. ويجب الانتباه عند استخدام معدلات الأخطاء وتطبيقها فقط على مهمة التحقق. وقد يختلف بصورة كبيرة أداء التطابق للأنظمة البيومترية في العالم الواقعي عن الأداء الذي توقعته عمليات محاكاة معدل الأخطاء.

ومع ذلك، هناك أيضًا علاقة قوية بين قيم معدل القبول الخاطئ ومعدل الرفض الخاطئ ويعتمد التوازن المفضل بين معدلات أخطاء هذين الاثنين بصورة كبيرة على الاستخدام التجاري للنظام البيومتري بعينه. على سبيل المثال، إذا كان دخول موظف إلى إحدى منشآت الشركة يرتبط بتطبيق بيومتري، فإن قيمة معدل الرفض الخاطئ المرتفعة ستمنع موظفي الشركة من الدخول على أساس منتظم، وبالعكس إذا كانت قيمة معدل القبول الخاطئ مرتفعة جدًا، فإن الشخص غير المصرح له سيتمكن من الدخول بشكل روتيني. وتبعًا لذلك، يتطلب التطبيق قيمة حد أساسي قابلة للضبط توازن بين معدل الرفض الخاطئ ومعدل القبول الخاطئ للسماح للموظفين بالدخول دون عائق بينما تمنع الدخول غير المصرح به في معظم الحالات. في حالة الحاجة إلى مستويات مرتفعة من الأمان، فسيستلزم الأمر إعادة ضبط قيمة الحد الأساسي لإيقاف الدخول غير المصرح به من خلال تقليل قيمة معدل القبول الخاطئ إلى أقصى حد ممكن، حتى إن كان على حساب زيادة قيمة معدل الرفض الخاطئ، ومن ثمَّ التأثير في دخول الموظفين المشروعين. وغالبًا ما تكون قيمة الحد الأساسي هذه، بناء على ذلك، مفاضلة واقعية بين معدل الرفض الخاطئ ومعدل القبول الخاطئ تعمل على تحسين فعالية النظام من أجل التطبيق المقصود وتوازن بين الحاجة إلى الأمان مقابل راحة العميل، وسرعة المعالجة وتكاليف النظام الكلية. يشير معدل الخطأ المتساوي (EER)[9] إلى إعداد الحد الأساسي لبعض الأشكال البيومترية حيث تتساوى قيم كلٍّ من معدل الرفض الخاطئ ومعدل القبول الخاطئ، أي أن نسبة حالات القبول الخاطئة تساوي نسبة حالات الرفض الخاطئة.

هناك عوامل أخرى تؤثر في الدقة مثل معدل فشل الحيازة (FTA)، والذي يعني بشرح بسيط، نسبة جميع المعاملات المسجلة التي يتعذر إكمالها بسبب حالات الإخفاق عند مراحل العرض (على سبيل المثال، لم يتم التقاط صورة)، أو استخلاص الملامح، أو مراقبة الجودة. إضافةً إلى إخفاق النظام، يتضمن الأمر أيضًا الحالات التي يكون فيها الأفراد يعانون سمات بيومترية تالفة أو متضررة أو مفقودة. ولا شك أن معدل فشل الحيازة مقياس مهم لتحديد القدرة التشغيلية الفورية لأي نظام. ويتطلب معدل فشل الحيازة المرتفع منهجًا بديلًا من أجل التقاط السمات البيومترية من الذين يتعذر تسجيلهم لأي سبب. وقد ينطوي ذلك على استخدام سمات بيومترية مشابهة ولكن بديلة، مثل الإبهام الأيسر بدلًا من الإبهام الأيمن أو حتى إضافة قدرات تمييز بيومترية ثانية ومختلفة، والتي قد تستلزم تطوير نظام متعدد الأشكال. وإذا كانت هذه البدائل غير مجدية، يمكن تبني حل غير بيومتري، يُعرف باسم معالجة الاستثناءات. على سبيل المثال، قد تتطلب هذه العملية من الأفراد، الذين يتعذر تسجيلهم بيومتريًا، أن تتم مراجعة هوياتهم بواسطة مُشغل بشري أو استخدام وسائل أخرى من المحتمل أنها مأمونة أقل، مثل رمز PIN أو التوقيع المكتوب، والتي قد يقل جميعها الفعالية العامة للنظام. وغالبًا ما تُفضل التطبيقات البيومترية متعددة الأشكال لهذا السبب لأنها تسمح عادة بنسبة أعلى من التسجيلات بينما تقلل معدل فشل الحيازة.

يحدد معدل الإنتاجية عدد الأشخاص الذين يمكنهم الوصول إلى النظام خلال إطار زمني محدد، أي القدرة مقابل السرعة. على سبيل المثال، مطار يعمل بنظام المرور بجواز السفر الإلكتروني البيومتري سيحتاج إلى حساب أحجام المسافرين الحالية والمتوقعة من أجل توفير أعداد كافية من البوابات البيومترية لتسهيل حركة التدفق الفعال للمسافرين خلال أوقات الذروة. الأمر الذي يسمح لنظام السمات البيومترية بالعمل حسب معدلات أخطاء محددة مسبقًا، لأسباب أمنية، بينما يعالج العديد من حالات التحقق في نفس الوقت خلال ثوانٍ لتلبية أغراض تتعلق برضا العملاء وفعالية العمل التجاري.

[9] يُعرف أيضًا باسم معدل الخطأ التقاطعي

2-1 دور السمات البيومترية في علم الأدلة الجنائية

يتعامل علم الأدلة الجنائية، بشكل عام، مع نقل المادة الملموسة أو الوسائط الرقمية الإلكترونية بين الأشخاص والأجسام والمواقع. وقد تكون هذه المادة مرئية، مثل نقاط دم على حائط، أو غير مرئية مثل دليل أثر مجهري مثل بقايا طلقة أو متفجرات أو صورة إلكترونية، مثل وجه التقطته كاميرا مراقبة. يمكن نقل هذه المواد أو البيانات قبل الفعل الإجرامي أو في أثنائه أو بعده. ويلتقط بعض من هذه المواد أيضًا ملامح *بيومترية* مثل أثر بصمة باقية في عرق على زجاج، أو صوت مسجل أثناء محادثة هاتفية، أو صورة حمض نووي مأخوذة من لعاب موجود على حافة قدح. إن هذه "السمات البيومترية الجنائية"[10] هي مكونات أساسية في علم الأدلة الجنائية وعناصر حيوية في تحقيقات إنفاذ القانون بسبب قدرتها المحتملة على تحديد هوية الأفراد. كما أنها مهمة في التنفيذ الفعال ونجاح عمليات مكافحة الإرهاب من خلال الآتي:

- ☐ إثبات أو دحض اشتراك أحد الأفراد في أي جريمة من خلال تقديم أدلة تجريم أو تبرئة في حد ذاتها أو كجزء من أدلة أخرى (راجع دراسة الحالة 2).
- ☐ تقديم عمليات موضوعية موثوق بها تحت مظلة القانون تقلل الاعتماد على الاعترافات ضمن سياق التحقيقات الجنائية، وخاصة إذا تم الحصول عليها باستخدام التعذيب أو غيره من التدابير القسرية
- ☐ تفسير النشاط في أماكن الجرائم والأحداث المرتبطة
- ☐ ربط شخص بنشاط أو حدث أو موقع أو شخص آخر قبل الحادث أو في أثنائه أو بعده
- ☐ ربط حدث واحد بحدث آخر أو عدة أحداث
- ☐ تحديد أماكن البيانات وربطها عبر الأنظمة الإلكترونية والرقمية المختلفة

تتطلب هذه الإمكانيات الإدخال المنسق للتخصصات الأخرى وثيقة الصلة بالموضوع ضمن علم الأدلة الجنائية ومجالات الخبرات التقنية والمعملية المتخصصة.[11] يجب تنفيذ عملية معالجة جميع مواد الأدلة الجنائية، سواء في مكان الجريمة أو في المعمل، بما يتوافق مع المعايير الدولية وأنظمة إدارة الجودة المرتبطة بذلك (راجع القسم 2-4-2-). تخصصات علم الأدلة الجنائية الأساسية هي:

- ☐ الأدلة البيولوجية - الحمض النووي، وسوائل الجسم، والشعر، والأنسجة، وغيرها.
- ☐ العلامات – علامات الأصابع وراحة اليد، وعلامات الأدوات، وعلامات الأحذية، وعلامات الإطارات، وغيرها.
- ☐ الأسلحة والقذائف
- ☐ دليل الأثر – طلاء، أو زجاج، أو أنسجة، أو متفجرات أو غيرها.
- ☐ دليل رقمي وإلكتروني – الوصول إلى الأجهزة، وتنزيل البيانات، والتحليل، وإعادة بناء التالف، وغيرها.
- ☐ العقاقير – التمييز وتحديد الكمية
- ☐ تحليل الوثائق
- ☐ تحليل المتفجرات

[10] السمات البيومترية الجنائية: من مجتمعين إلى نظام واحد. محاضر المؤتمر الدولي للفريق المختص بالسمات البيومترية بتاريخ 6-7 أيلول/سبتمبر 2012، دارمستاد، ألمانيا.

[11] تم وصف العديد منها بالتفصيل في منشورين أتاحهما مكتب الأمم المتحدة المعني بالمخدرات والجريمة: "الشرطة: خدمات الأدلة الجنائية والبنية التحتية" و"مهارات الموظفين المطلوبة وتوصيات المعدات لمعامل علم الأدلة الجنائية." (www.unodc.org)

تُستخدم المواد البيومترية الجنائية في تقصي الحالة للمقارنات واحد لواحد (مثل مقارنة علامة إصبع مستخلصة من مسرح جريمة بمجموعة من بصمات الأصابع التي تم الحصول عليها من أحد المشتبهين) وتشكل كذلك واحدة من ثلاثة أنواع رئيسية من قواعد البيانات المستخدمة بواسطة علماء الأدلة الجنائية[12]:

1- *قواعد البيانات المرجعية لمواد تقصي الحالة* – مثل: مجموعة من الألياف الطبيعية والصناعية، عادة ما يكون مصدرها الشركات المصنعة ومنافذ البيع، التي تُستخدَم في التحديد والتصنيف والمقارنة مع الألياف الواردة من مسارح الجرائم
2- *قواعد بيانات البحث غير البيومترية* – مثل الأسلحة والذخائر المستعملة، وطبعات الأحذية، وغيرها
3- *قواعد بيانات البحث البيومترية* – مجموعة من المواد والملامح البيولوجية البشرية، مثل الحمض النووي وبصمات الأصابع.

يجب اتباع المبادئ الأساسية للتعامل مع الأدلة الجنائية عند التعامل مع العينات البيومترية ضمن سياق علم الأدلة الجنائية والتحقيقات، وإلا فإن النتائج التي يصدرها أيٌّ من أنظمة البحث البيومتري ستكون بلا قيمة في أي إجراء قضائي لاحق. ولذلك يجب استخدام السجلات والإجراءات الآتية بانتظام عند استخلاص أي عينة/عنصر من أي موقع من مواقع الجرائم:

- ☐ *المصدر* – سجل كتابي وفوتوغرافي لموقع العينة/العنصر
- ☐ *الحفظ* – يجب استخلاص العينة/العنصر الجنائي وتعبئته بطريقة لا تعرض الدليل للتلوث أو التلف أو التغيير أو الفقد أو الفساد، كما يجب أن تحمي العبوة العينة من التلف أثناء النقل وتحول دون تلوثه أو تلويثه للعناصر الأخرى أو البيئات؛ ويجب تخزين العينة في درجة حرارة مناسبة للحفاظ عليها وضمان وصولها في حالة اختبار مثلى لإجراء التحليل المعملي
- ☐ *السلامة* – يجب أن تكون العبوة قوية وسليمة ومحكمة الإغلاق بفعالية لمنع أي تدخل أو وصول غير مصرح به؛ يجب عدم التمكن من إضافة أي مادة أو إزالتها (بما في ذلك الجسيمات أو الغازات أو السوائل) عبر العبوة
- ☐ *الاستمرارية (تسلسل الحيازة)* – يجب الاحتفاظ بسجل بدايةً من مسرح الجريمة إلى ما بعد ذلك بكل شخص وقعت العينة/العنصر المعبأ في حوزته

دراسة الحالة 2 – مشروع البراءة

تأسس مشروع البراءة عام 1992 على يد بول نيوفيلد وباري شيك من كلية حقوق بنجامين ن. كاردوزو في نيويورك، الولايات المتحدة الأمريكية. وكان الهدف وراء المشروع هو استخدام صورة الحمض النووي الجنائية لتبرئة من تم اتهامهم بالخطأ وإصلاح نظام العدالة الجنائية الأمريكي لمنع حالات الظلم في المستقبل. وقد اعتمد المفهوم على المبدأ القائل بأن إذا كانت تقنية الحمض النووي يمكنها إثبات إدانة الأشخاص بارتكاب الجرائم، يمكنها أيضًا إثبات براءة الأشخاص الذين تم اتهامهم عن طريق الخطأ. وقد جاءت نتائج تحليل الحمض النووي، حتى يومنا هذا؛ لتبرئة عدد 356 شخصًا وكشف هوية 153 بديلًا من مرتكبي الجرائم المحتملين.

[12] غالبًا ما يكون علماء الأدلة الجنائية هم المسؤولون عن إدارة قواعد بيانات الاستخبارات الجنائية وتشغيلها، ويكون مقر ذلك في معامل الأدلة الجنائية، إلا أن بعض قواعد البيانات البيومترية، مثل بصمات الأصابع والحمض النووي وأنظمة الصوت والصورة قد تُدار ضمن سياق بيئات إنفاذ القانون بواسطة أشخاص آخرين.

1-2-1 قواعد البيانات البيومترية الجنائية: فئات البيانات

تُستخدم قواعد البيانات البيومترية الجنائية، وتُعرف كذلك باسم قواعد بيانات الاستخبارات الجنائية، بشكل روتيني في معامل الأدلة الجنائية ووكالات إنفاذ القانون. وقد كان لقواعد البيانات هذه أثر بالغ في التحقيقات الجنائية، وخاصة في قضايا الإرهاب، في العديد من البلدان على مدى أكثر من 100 عام. والأشكال البيومترية الأشيع استخدامًا هي بصمات الأصابع والحمض النووي والوجه والصوت. وتتألف كل قاعدة بيانات من مجموعتي بيانات بارزتين:

البيانات المرجعية – المستخلصة في ظل ظروف خاضعة للرقابة من المقبوض عليهم في جرائم أو مشتبه بهم لارتكابها، مثل بصمات الأصابع العشرة لكلتا اليدين والتي يتم أخذها إلكترونيًا بواسطة ماسح ضوئي أو بواسطة الطرق التقليدية باستخدام الحبر والورق؛ ومسحات اللعاب التي يتم أخذها من داخل فم المقبوض عليه أو عينات الشعر أو الدم التي تتم معالجتها لإنشاء صورة حمض نووي كاملة[13]؛ والصور الفوتوغرافية الرقمية للوجه وغيره. كما يمكن الحصول على البيانات المرجعية كذلك من ضباط الشرطة وممن يتمتع بحق وصول شرعي إلى مسرح الجريمة قبل أي جريمة أو في أثنائها أو بعدها، بغية تحديد أي مواد جنائية يتركونها واستبعادها من التحقيق.

بيانات مسرح الجريمة – صادرة عن العينات والعناصر المستخلصة من مسارح الجرائم.[14] وقد تتباين جودة البيانات البيومترية لمسرح الجريمة بصورة كبيرة. قد تتعرض المواد الجنائية المستخلصة للتلف أو التلوث أو الافتقار إلى ما يكفي من المحتوى أو وضوح التفاصيل لمجموعة مختلفة من الأسباب. وهذا يقدم مجموعة واسعة إضافية من النتائج الواردة من عملية البحث والمقارنة بدلًا من النتيجة الثنائية العادية "تطابق" أو "عدم تطابق" التي يتم الحصول عليها من الأنظمة البيومترية "غير الجنائية" الأخرى، مثل تطبيقات مراقبة الدخول.

تستخدم بعض البلدان كذلك أنظمة بيومترية كبيرة لدعم التسجيل المدني لمواطنيها، مثل أنظمة بطاقات الهوية. ويوفر هذا الأمر لكل مواطن هوية رسمية ويسمح له بالحصول على الخدمات الحكومية وغيرها من المنافع الاجتماعية والتجارية، مثل الرعاية والسكن والتأمين والبنوك وغيرها.

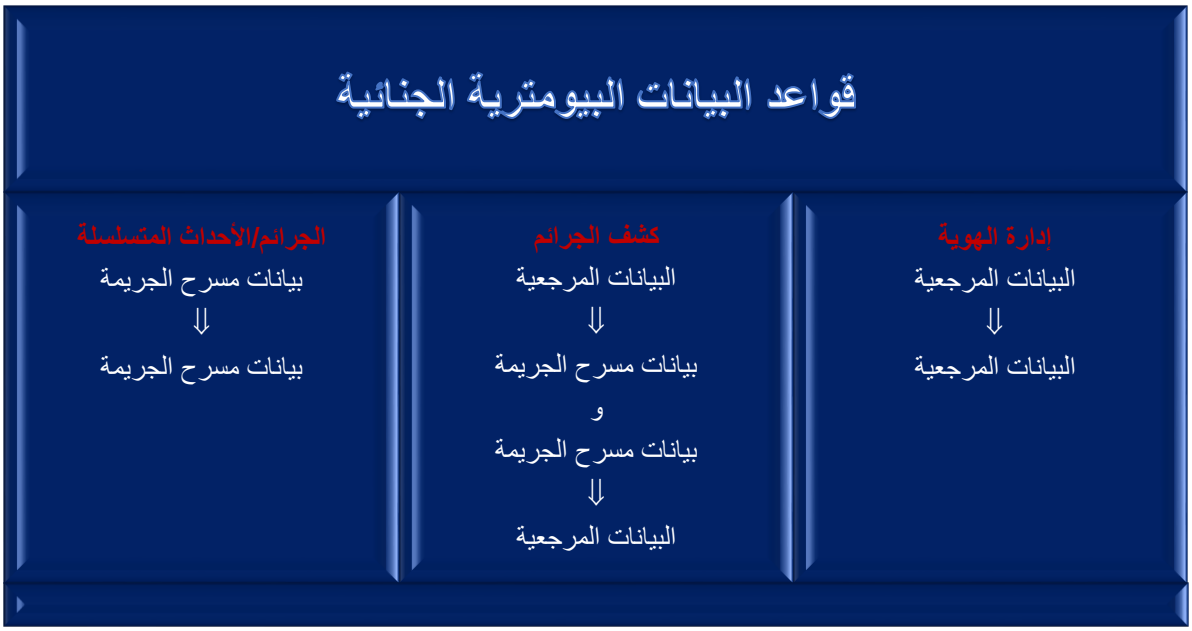
أنظمة التسجيل المدني – عادة ما تكون الأشكال البيومترية المستخدمة في هذه الأنظمة هي البصمات أو الوجه أو الحدقة أو مجموعة متعددة الأشكال. وقد تحتوي قواعد البيانات هذه على الملايين أو عشرات الملايين أو مئات الملايين من القوالب البيومترية (البيانات المرجعية)، وذلك اعتمادًا على حجم قطاع السكان المحلي، وتُصمم أساسًا للبحث في البيانات المرجعية. لذلك، إذا كان النظام التنظيمي والقانوني الوطني يسمح لوكالات إنفاذ القانون بالبحث في قواعد البيانات هذه، لأغراض تتعلق بالتحقيق في الجرائم، فستكون عمليات البحث عادة مقصورة على البيانات المرجعية فقط. وسيكون متاحًا البحث في مجموعة من البصمات أو صورة وجه مأخوذة من شخص للتأكد مما إذا كان تم تسجيلها في النظام، ولكن من غير المحتمل أن ينجم أي حالة تطابق حال البحث عن علامات الأصابع أو صور الوجه من أي مسرح جريمة. وهذا لأن خوارزميات التطابق في أي نظام تسجيل مدني لا تصمم عادة للتعامل مع بيانات مسرح الجريمة بنفس الطريقة التي يصمم بها نظام البحث الجنائي في معامل الأدلة الجنائية. وهذا هو السبب وراء ندرة استخدام قواعد البيانات البيومترية المدنية في تحقيقات الجرائم وحتى عند البحث فيها في حالات الجرائم الخطيرة والإرهاب، فإن معدل النجاح غالبًا ما يكون منخفضًا للغاية. مع ذلك، قد تُسهم التقنيات ومصادر البيانات الجديدة لبعض الأشكال البيومترية، مثل الوجه، في تمكين المزيد من عمليات البحث الدقيقة في المستقبل. وهناك أيضًا خيار تضمين برنامج تطابق جنائي في أنظمة التسجيل المدني هذه أو إلحاقه بها.

[13] إن تقنية الحمض النووي الحديثة تسمح بإجراء التصوير السريع للحمض النووي من مسحات اللعاب التي يتم أخذها من الأشخاص باستخدام أجهزة آلية بالكامل، إما في المعمل وإما في مراكز الشرطة/المراكز الحدودية خلال ساعة واحدة فقط حاليًا. وهذا يعني إمكانية إتمام عمليات البحث في قاعدة بيانات الحمض النووي، لإثبات مدى وجود حالات تطابق للحمض النووي مع عينات مسرح الجريمة، بينما الشخص موجود قيد الاحتجاز أو السجن.

[14] يستخدم المصطلح "مسرح الجريمة" هنا بسياقه الواسع، بما في ذلك الأماكن المادية والمشتبهون والضحايا والشهود والبيئات الرقمية والإلكترونية.

2-2-1 قواعد البيانات البيومترية الجنائية: فئات البحث

الشكل 2 – قواعد البيانات البيومترية الجنائية – تبديلات البحث



هناك أربعة تبديلات أساسية للبحث الجنائي تُستخدم لدعم إنفاذ القانون والتحقيقات الجنائية وهي تنجم عن أشكال البحث الثلاثة الآتية (راجع الشكل 2):

بحث إدارة الهوية/*التبديل 1* - البيانات المرجعية للبيانات المرجعية

يحدد هذا النوع من البحث ما إذا كان أحد الأشخاص مسجلًا بالفعل في أي قاعدة بيانات من خلال البحث في بياناته المرجعية مقابل كل البيانات المرجعية المحفوظة في قاعدة البيانات. ويستخدم هذا الأسلوب على نحو أكثر شيوعًا لإثبات ما إذا كان أحد الأشخاص معروفًا لدى الشرطة ولديه إدانة سابقة وسجل إجرامي، وخاصة إذا كان قد قدم خصائص فردية زائفة. لقد استخدمت البصمات على مر التاريخ، لهذا الغرض. حيث يتم أخذ مجموعة كاملة من بصمات الأصابع العشرة الملفوفة[15] ("عشر بصمات") من أي معتقل والبحث عنها في قاعدة بيانات للعثور على عشر بصمات لمجرمين معروفين. وعند إتمام ذلك باستخدام نظام حديث وفعال للتعرف الآلي إلى بصمات الأصابع مع وجود قاعدة بيانات تحتوي على صور عالية الجودة للبصمات، أي أنه تم تأكيد جودة جميع البصمات وأخذها في ظل ظروف خاضعة للرقابة بواسطة مشغلين مدربين، تكون النتيجة دقيقة للغاية (أي قيمة معدل القبول الصحيح مرتفعة جدًا - راجع القسم 1-1). يتم تنفيذ مثل عمليات البحث هذه بانتظام "بسرعة"، أي دون حاجة إلى تدخل بشري أو مع تدخل بسيط ما لم يكن التحقق من أي حالة تطابق مطلوبًا. وهذا يعني أن عمليات البحث هذه سريعة المعالجة للغاية. إن أجهزة التقاط البيانات المتحركة الحديثة تمكن ضباط إنفاذ القانون من أخذ طبعات الإصبع وراحة اليد من الأشخاص الموجودين في أماكن بعيدة والمعابر الحدودية وإرسال البيانات إلى خادم مركزي لإتمام عملية البحث الفورية. ويتم تسلُّم النتيجة عادة خلال ثوانٍ أو دقائق. وتمتلك بعض الأجهزة المتحركة قاعدة بيانات مستقلة حتى يمكن إتمام جميع وظائف البحث محليًا دون الحاجة إلى نقل البيانات إلى خادم بعيد.

[15] يتم لف طرف كل إصبع على أسطوانة الماسح الضوئي أو لف بصمة الإصبع من حافة الظفر إلى حافة الظفر لتسجيل أقصى حد من منطقة التضليع والتفاصيل المميزة. وتُعرف الطبعات الأخرى التي تؤخذ من الأصابع باسم طبعات "مستوية" أو "مستوية رباعية". حيث يتم أخذها في وقت واحد (الإبهامان معًا والأصابع الأربعة لكل يد) من خلال الضغط على الإصبع مباشرة لأسفل على الأسطوانة/النموذج. ويتم أخذ الطبعات المستوية بوصفها من تدابير ضمان الجودة للتأكد من تسجيل الطبعات الملفوفة بالتسلسل الصحيح.

وبالطبع، يمكن أيضًا تنفيذ أي عملية من عمليات بحث إدارة الهوية باستخدام الأشكال البيومترية الأخرى، مثل: الحمض النووي والوجه والحدقة وغيرها. كما يمكن استخدام عمليات بحث إدارة الهوية لتحديد هوية المتوفين أو الأشخاص الذين يعانون فقدان الذاكرة. إن المطلب الأساسي، الذي يُعد الأساس لجميع عمليات البحث البيومتري، هو الحصول على بيانات مرجعية عالية الجودة ذات معايير متسقة حتى تعمل كل أشكال البحث بأقصى إمكاناتها. فالمواد المرجعية رديئة الجودة تقلل فعالية جميع تبديلات البحث ودقتها.[16]

يطرح بحث إدارة الهوية السؤال **"هل صادفناك من قبل ومن أنت؟"**

بحث كشف الجرائم: *التبديل 2* - البيانات المرجعية لبيانات مسرح الجريمة *والترتيب 3* - بيانات مسرح الجريمة للبيانات المرجعية

يتطلب بروتوكول البحث هذا واجهة ثنائية الاتجاه بين قاعدة البيانات المرجعية وقاعدة بيانات مسرح الجريمة التي تحتوي على المواد البيومترية الجنائية المستخلصة من مسارح الجرائم مثل الحمض النووي من بقع الجريمة (العينات المشكوك فيها)، وعلامات الأصابع وراحة اليد، وصور الوجه وغيرها. ويتم البحث عن البيانات المرجعية المسجلة حديثًا، إذا لم تكن موجودة بالفعل في قاعدة البيانات المرجعية، في قاعدة بيانات مسرح الجريمة وبالعكس، يتم البحث عن بيانات مسرح الجريمة المسجلة حديثًا في قاعدة البيانات المرجعية. وتكون دقة هذه الأنواع من عمليات البحث أقل كثيرًا من بحث إدارة الهوية بسبب الجودة المتغيرة لبيانات مسرح الجريمة.

يطرح بحث كشف الجرائم السؤال **"هل ارتكبت جريمة؟"** و**"هل تربطك علاقة بهذا الجسم/الموقع؟"** و**"هل يوجد شخص آخر بصحبتك؟"**

بحث الجرائم/الأحداث المتسلسلة: *التبديل 4* - بيانات مسرح الجريمة لبيانات مسرح الجريمة

يكون هذا النوع من البحث قادرًا على ربط مسارح الجرائم من الجرائم المنفصلة أو تلك التي قد تظهر خلال تحقيق رئيسي واحد من خلال تمييز مواد مسرح الجريمة وربطها معًا من مواقع مختلفة وتزويد ضباط التحقيق بدليل ذكي من هذه القضايا. فهوية الشخص الذي ترك مادة مسرح الجريمة غير معروفة ولكن تحديد أن نفس الشخص ترك مادة بيومترية في جريمتين أو حادثين أو أكثر يُعد مساعدة قيمة تفيد المحققين ومحللي الاستخبارات. ويعتمد مستوى النجاح والدقة في هذا النوع من البحث بصورة كبيرة على جودة بيانات مسرح الجريمة واستخلاص المواد القابلة للمقارنة من مسارح الجرائم. وتناسب بعض الأشكال البيومترية هذا النوع من البحث بصورة أفضل من غيرها، فالحمض النووي على سبيل المثال فعال بصفة خاصة في ربط الجرائم/الأحداث في العديد من الأنواع المختلفة من التحقيق، مثل جرائم الإرهاب والقتل والجرائم الجنسية.

[16] هذا هو السبب وراء أخذ ثلاث مجموعات على الأقل من طبعات البصمات وراحة اليد لأي شخص يتم القبض عليه بجرائم تتعلق بالإرهاب في المملكة المتحدة ويتم هذا الإجراء تحت إشراف خبير بصمات. وتتضمن كل مجموعة كل المناطق الخاصة بتفاصيل مضلع الاحتكاك الموجودة باليد، أي الطبعات الملفوفة والمستوية القياسية، وأطراف الأصابع، والطبعات الملفوفة لجميع السلاميات، والسطح الكامل لراحة اليد والجانب الزندي من اليد (راحة الكاتب)، إضافةً إلى الطبعات الأخمصية (أخمص القدم وأصابع القدم). وتُقدم هذه العملية شديدة التدقيق أفضل مجموعة من البصمات المرجعية المتاحة لأغراض البحث والتسجيل في نظام التعرف الآلي إلى بصمات الأصابع، إضافةً إلى أكبر مجموعة بيانات متاحة لتفاصيل مضلع الاحتكاك للمقارنة 1:1 مع علامات إصبع/راحة/أخمص من مسرح الجريمة، وخاصة تلك الناجمة عن أطراف الأصابع أو جوانبها أو أي منطقة من راحة اليد.

يطرح بحث الجرائم المتسلسلة السؤال "هل تطابق بيانات مسرح الجريمة هذه بيانات مسرح الجريمة من الجرائم/الحوادث الأخرى؟"

ملاحظة قواعد البيانات الموصوفة في هذا القسم لديها جميعًا معدلات رفض خاطئة مختلفة اعتمادًا على نوع البيانات البيومترية التي تحتويها وجودتها. وعلى غرار جميع الأنظمة البيومترية الأخرى، لا تعني بالضرورة النتيجة السلبية أو عدم التطابق (أي أن عملية البحث 1:كثير لم ينتج عنها أي تطابق) أن بيانات التطابق غير موجودة في قاعدة البيانات ولكن ربما أخفق النظام في العثور عليها، أيًّا كان السبب.

الحمض النووي[17] – فئات البحث الإضافية

هناك بعض تقنيات البحث المتخصصة الإضافية التي تختص بعينات الحمض النووي المشكوك فيها. تنشأ الصور المرجعية للحمض النووي من المناطق غير المرمزة للحمض النووي وتُستخدم فقط في أغراض المطابقة؛ لأنها تحتوي على قدر ضئيل جدًا من المعلومات الجينية الأخرى. عادة ما تحتوي عينات الحمض النووي المشكوك فيها المستخلصة من مسارح الجرائم على الكثير من المواد الجينية وغيرها من خلاصات الحمض النووي ويمكن استخدام تقنيات التصوير لمساعدة المحققين. إلا أن هذه التقنيات عادة ما تخضع للتدقيق الشديد من جانب المسؤولين عن الرقابة القانونية والأخلاقية على الأدلة الجنائية؛ لأنها قد تخالف قوانين الخصوصية وحماية البيانات دون حوكمة قوية. وتتضمن بعض الأمثلة:

تقييم النمط الظاهري – تقنية تبحث عن آثار مادية جينية معينة، مثل الشعر الأحمر أو لون العين في بقعة الجريمة. ورغم أن هذه العملية محدودة الاستخدام حاليًا إلا أن التقدم في علوم الحمض النووي سيزيد بلا شك نطاق مزايا النمط الظاهري في المستقبل. مما سيزيد احتمالية أن يتمكن المحققون من استخلاص المزيد من "الوصف" المفصل للمشتبه غير المعروف من الحمض النووي لبقعة الجريمة.

البحث العائلي (النسب) – قد لا يتم التعرف إلى صورة الحمض النووي الواردة من بقعة الجريمة عند البحث عنها في قاعدة البيانات المرجعية للحمض النووي الجنائي. ويمكن في الظروف الاستثنائية البحث عبر نفس قاعدة البيانات باستخدام برنامج متخصص إضافي من أجل تحديد ما إذا كانت الصورة تمثل إلى حد ما الصورة الخاصة بأي قريب (أقرباء) بالدم ربما يكون محفوظًا في النظام. وقد يصدر عن ذلك عدد قليل نسبيًا من النتائج أو عدة آلاف اعتمادًا على ندرة المقارنة لصورة الحمض النووي محل البحث عند المقارنة بصورة جينية عامة لقطاع السكان في قاعدة البيانات.

3-2-1 قواعد البيانات البيومترية الجنائية – القيود ومعايير إعداد التقارير

تتعرض عادة المواد الجنائية للترك أو التسجيل عن طريق الخطأ أثناء إعداد موقع الجريمة أو التحقيق فيها وقد تتعرض لمجموعة من ظروف الإتلاف والقيود التي تحول دون استخدامها بفعالية بصفتها بيانات مرجعية في أي نظام من أنظمة البحث البيومترية. وبعض من هذه الظروف يكون عامًّا، إلا أن العديد منها يعتمد على الشكل البيومتري للعينة. بعض من الأمثلة شائعة الحدوث:

[17] راجع أيضًا الاستعراض الإداري لقاعدة بيانات الحمض النووي والتوصيات، لعام 2017، الفريق العامل المعني بالحمض النووي التابع للشبكة الأوروبية لمعاهد علوم الأدلة الجنائية، نيسان/أبريل 2017" http://enfsi.eu/wp-content/uploads/2017/09/DNA-databasemanagement-review-and-recommendatations-april-2017.pdf

الوجه – كاميرا مراقبة وغيرها من تقنيات التسجيل المرئي الخارجية

- *توافق زاوية الكاميرا* – غالبًا ما توجد كاميرات المراقبة في مكان مرتفع بينما يتم التقاط صور الحبس "صورة جنائية تعريفية" من الأمام وبمستوى الوجه. ويؤدي هذا إلى جعل المقارنة الدقيقة بين هذين النوعين من الصور صعبة وأحيانًا مستحيلة.
- *الإنارة والتعرض* – لإصدار أفضل صورة، تعتمد مستشعرات الكاميرا على (أ) الإضاءة العامة المتاحة في البيئة و(ب) الإعدادات مثل سرعة الغالق وحاجب العدسة وحساسية ISO.
- *دقة الكاميرا* – دقة بعض الكاميرات منخفضة، أي إنها تسجل فقط عددًا محدودًا من البكسل وإذا كانت الكاميرا بعيدة عن الهدف فإن الصورة الناتجة غالبًا ما تكون محببة وغير واضحة، ولا سيما إذا كان الضوء المحيط ضعيفًا. وستحتوي الصورة الناتجة على تفاصيل مفيدة قليلة حتى مع تكبيرها.
- *الضغط* – يعمل مكون تسجيل البيانات الخاص بالكاميرا على إزالة التفاصيل الدقيقة من أجل زيادة السعة الخاصة بتخزين صور ذات مواصفات أقل
- *ملامح الوجه والأغطية* – العوامل مثل العمر أو التعبيرات أو ملامح الوجه غير الواضحة قد تؤثر في القدرة على تمييز الأوجه، إضافةً إلى العوائق الخارجية مثل النظارات وشعر الوجه والقبعات والخوذ وغيرها (راجع القسم 2-3-2-).

علامات الأصابع أو راحة اليد (تُعرف كذلك باسم طبعات "خافية" أو "الخافيات"):

- *الكفاية والمنطقة المكشوفة* – إن الجزء الذي يلامس أي سطح هو مساحة صغيرة فقط من الإصبع أو راحة اليد ولذلك لا يكشف إلا عن القليل نسبيًا من التفاصيل المميزة. وقد تكون بصمات الأصابع المرجعية التي تم أخذها على نحو سيّئ هي المشكلة؛ لأنها قد لا تكشف عن نفس المساحة الصغيرة من الإصبع للمقارنة مع علامة الإصبع.
- *تراكب إضافي* – علامتان أو أكثر من علامات الأصابع متروكة في نفس الموقع على أي سطح، مما يجعل من الصعب العزل البصري لإحدى الطبعتين عن الأخرى (الأخريات).
- *التداخل* – تداخل الخلفية من الركيزة الأساسية قد يخفي جزءًا من علامة الإصبع أو كلها. وبشكل عام، توجد عادة علامات الأصابع إما على السطح حيث تُركت على ركيزة أساسية غير مسامية أو امتصت داخل السطح على ركيزة أساسية مسامية. ومن ثمَّ، تتعرض تلك الموجودة على السطح للتلف والإساءة البيئية. فقد تُخفي أيضًا الأتربة أو الملوثات أو غيرها من الأجسام التفاصيل المميزة في العلامة أو تُتلفها.
- *الضغط* – ربما يتعرض الإصبع للضغط الرأسي أو الجانبي عند التلامس مع أي سطح، مما يؤدي إلى تشوه علامة الإصبع بسبب مرونة الجلد.
- *الحركة* – ربما ينزلق الإصبع جانبيًا أثناء التلامس مع أي سطح، مما يؤدي إلى طبعة ملطخة أو في بعض الحالات التشوه والتراكب الإضافي.
- *قيود أسلوب الإظهار* - استخدام مسحوق إظهار البصمات أو المعالجات الكيميائية قد لا يكشف عن كل العلامة بوضوح وقد يؤدي إلى الحصول على صورة باهتة للغاية أو قاتمة للغاية ذات تباين قليل.

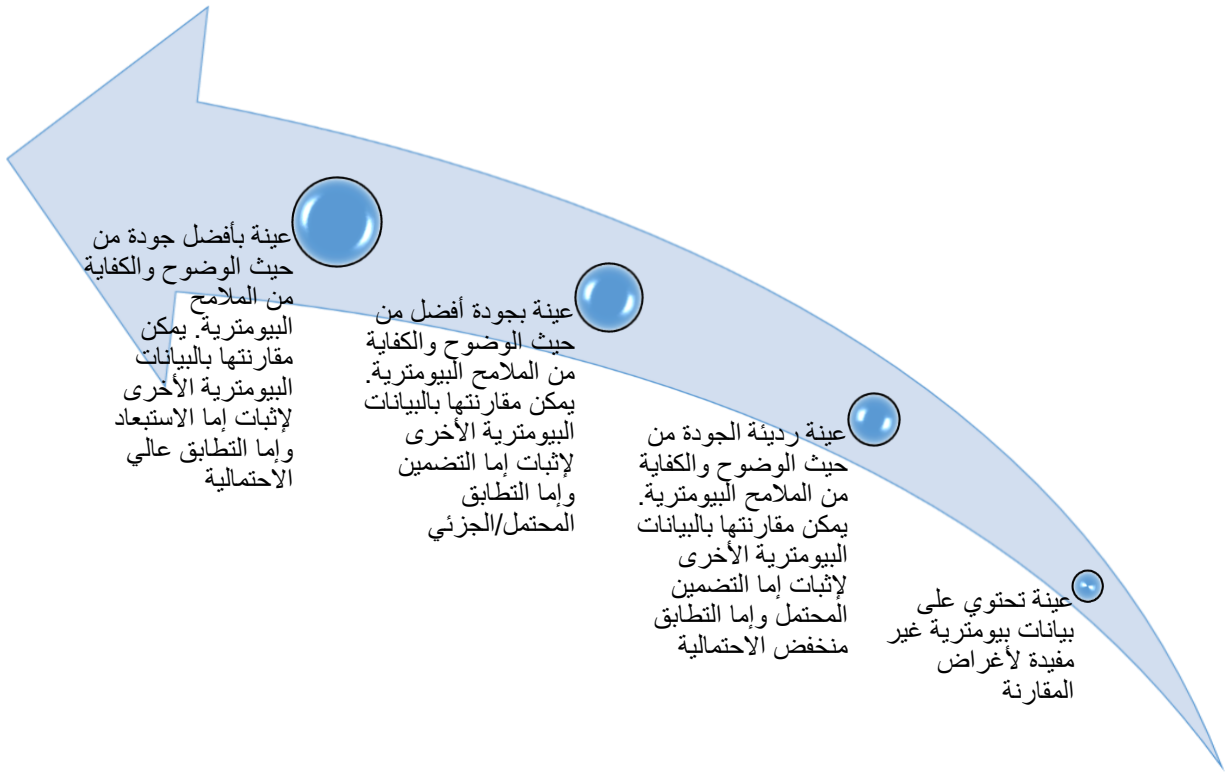
الحمض النووي – المادة الخلوية والبيولوجية المستخلصة من مسارح الجرائم (تُعرف كذلك باسم "بقع الجريمة"):

- *الكمية والجودة* – كما هو الحال مع علامات الأصابع، الكمية والجودة الخاصة بالحمض النووي المتروك في مسارح الجرائم متباينة ولهذا السبب يتم تصنيف بعض من حالات تطابق الحمض النووي على أنها "جزئية" وليست "كاملة". ويحدث هذا عندما تكون مادة الحمض النووي المتاحة بجودة رديئة أو غير كافية لإنتاج صورة حمض نووي كاملة. وفي هذه الظروف، يتم تعديل احتمالية التطابق أو نسبة الإمكانية وفقًا لذلك لعكس درجة عدم التأكد.
- *الأمزجة* – قد يكون الحمض النووي المتروك في أي موقع من أكثر من واهب وقد تحتوي الصورة الناتجة على مزيج من شخصين أو أكثر. يستخدم علماء الأدلة الجنائية تحليلًا إحصائيًا لتفسير مثل هذه النتائج وكلما أمكن يساعد على فصل الحمض النووي لكل واهب وإعداد صورته. وقد تكون الصور الفردية في المزيج ذات جودة متباينة كذلك.
- *المصدر* – تُسهم التقنيات الحديثة في معامل الحمض النووي في إصدار صور من كميات ضئيلة من الحمض النووي على المستوى الخلوي. ولكن، نظرًا إلى تعامل العلماء حاليًا مع مثل هذه العينات الصغيرة، لا يُتاح دائمًا تحديد مصدر الحمض النووي الذي عُثر عليه في أي مسرح جريمة، على سبيل المثال من سائل جسم معين.
- *التلوث* – إن نتيجة هذه القدرة التي تُتيح تحديد عينات الحمض النووي وإعداد صورها عند مثل هذه المستويات المنخفضة هي أن مثل هذه المواد هائمة بطبيعتها، أي أن لديها قدرة التنقل بين الأشخاص والعناصر والمواقع. يجب اتخاذ احتياطات شاملة في مسارح الجرائم وفي المعامل؛ لتجنب التنقل غير المتعمد للحمض النووي بسبب إجراءات الشرطة أو علماء الأدلة الجنائية (راجع القسم 2-3).
- *الإساءة البيئية* – يمكن أن يتعرض الحمض النووي للتلف أو الفساد أو التمسخ بسبب فترات التعرض الطويلة لظروف بيئية مناوئة، مثل: المستويات المفرطة من درجات الحرارة والرطوبة والملوثات.

بناء على ذلك، تتراوح جودة المواد البيومترية المستخلصة من مسارح الجرائم تصاعديًا من عدم وجود قيمة، حيث لا توجد ملامح أو بيانات بيومترية يمكن استخلاصها، وحتى القيمة المرتفعة، أي أن المواد البيومترية كافية من حيث الكمية ووضوح الملامح لإتاحة إمكانية المقارنة مع غيرها من البيانات البيومترية والقدرة على إنتاج تطابق عالي الاحتمالية. كما أن الجودة النسبية للبيانات البيومترية الأخرى المستخدمة في المقارنة، سواء كانت عينة مرجعية أو عينة مسرح جريمة، مهمة كذلك لهذه العملية. فالقدرة على الحصول على أي درجة تطابق من عملية المقارنة تتعلق مباشرة بجودة كلا العينتين. ولذلك، يجب أن تكون البيانات البيومترية المرجعية المأخوذة من الأفراد المرتبطين بالجرائم الإرهابية، بأعلى جودة ممكنة.

يقدم الشكل 3 المراحل التقليدية لهذا التباين فيما يتعلق بجودة العينة البيومترية والتسلسل الموافق من حالات التطابق منخفضة إلى عالية الاحتمالية. وعادة ما يكون إثبات حالات الاستبعاد أسهل مع العينات البيومترية رديئة الجودة، حيث تُظهر المقارنة أن العينتين البيومتريتين ليستا من نفس الشخص، وذلك مقارنة بحالات التضمين (أي التطابق)، ولكن عندما يكون تسلسل الجودة في أسوأ حالاته، تصبح كلا العمليتين تحديًا وقد تكون نتائج المقارنات غير حاسمة.

الشكل 3 – البيانات البيومترية لمسرح الجريمة – العلاقة بين جودة العينة البيومترية واحتمالات التطابق



معايير التسجيل في قاعدة البيانات - عادة ما تفتقر البيانات البيومترية رديئة الجودة إلى خصائص البحث التمييزية الكافية وهذا يعني أن البيانات عند حفظها في أي نظام مثل نظام التعرف الآلي إلى بصمات الأصابع، ستستجيب على الأرجح بصورة متكررة وغير متناسقة في عمليات البحث القادمة وقد يؤدي ذلك في النهاية إلى تقويض فعالية النظام. ويحدث ذلك لأن حالات التطابق البيومترية المحتملة التي قدمها النظام في شكل قائمة مرشحين بتسلسل هرمي، عادة ما تضم عددًا مسبق التحديد من الاستجابات، مثل أهم عشر حالات تطابق على الأرجح. والذين يقوم مشغل بشري بالتحقق منهم لتحديد ما إذا كانت أي حالة منهم هي حالة تطابق فعلية. وأي بيانات رديئة الجودة محفوظة على النظام يمكنها إخراج حالات التطابق الحقيقية من هذه القائمة. لذلك، يجب أن يكون القرار بتسجيل أي عينة بيومترية يحقق التوازن بين الأهمية الإثباتية والتشغيلية والمعلوماتية لكل عينة مقابل جودتها التقنية أو العلمية (راجع القسم 2-4-2-). ويجب أن تخضع حدود التسجيل هذه الخاصة بالبيانات البيومترية رديئة الجودة، في أي شبكة من قواعد البيانات، لمعايير دنيا جماعية لضمان العمل الانسيابي المتوازن عبر الشبكة ومنع الشركاء من تسجيل البيانات التي قد تعطل عملية البحث الفعالة.

من النتائج المباشرة لتسلسل جودة البيانات البيومترية لمسرح الجريمة، قيام علماء الأدلة الجنائية واختصاصيي البصمات وغيرهم ممن يعالجون المواد الجنائية بتطوير العديد من الطرق المختلفة لتقديم مجموعة من نتائج مقارناتهم إلى التحقيقات أو تحليلات الاستخبارات أو في المحاكم القانونية. وتتضمن هذه الطرق بصورة عامة:

- ☐ احتمال "بايزي" المنطقي والاستدلال الإحصائي لاختبار الفرضيات، بما فيها نسب الإمكانية التي تشكل الأساس لمقارنات صورة الحمض النووي. ملاحظة: لا تقبل بعض المحاكم والولايات القضائية الوطنية تباينات معينة لهذه الطرق الإحصائية [18]
- ☐ مقاييس التكافؤ الرسمية مثل مقارنات البصمات الحديثة والعديد من المجالات الجنائية الأخرى
- ☐ الاستنتاجات "المطلقة" مثل مقارنات البصمات التقليدية

وهذا يعني أن طريقة إعداد التقارير الجنائية *لنفس الشكل البيومتري* قد تختلف من بلد إلى آخر أو حتى من تخصص قضائي إلى آخر حسب المتطلبات العلمية والقضائية والتنظيمية والتشريعية ذات الصلة. وهذا بدوره قد يؤثر في معيار التسجيل لكل قاعدة بيانات، إضافةً إلى نوع النتيجة الصادرة.

دراسة الحالة 3 – معايير أنظمة البصمات القديمة

لا تزال بعض البلدان تستخدم الطريقة "الأساسية" للتعرف إلى بصمات الأصابع، وهي نظام قديم يعتمد على عملية اتخاذ قرار ثنائية، أي التطابق أو عدم التطابق، وتتطلب وجود عدد أدنى محدد مسبقًا من خصائص التضليع (الملامح البيومترية) لتأكيد التطابق وتقديم الدليل في المحاكم. وهذا المعيار مكتوب في التشريعات القضائية لبعض الولايات القضائية. فمقارنة بصمة الإصبع أو علامة الإصبع التي تحتوي على عدد أقل من خصائص التضليع مقارنة بالمعيار المقبول لا يمكن تقديمها بمنزلة دليل. ومن شأن هذا أن يزيد بوضوح العوائق في الولايات القضائية التي تتبنى مبادئ الكشف الكامل ضمن أنظمتها القضائية، حيث قد تتطلب المحاكم وجود خبير لإعطاء رأيه عن أيٍّ من مقارنات بصمات الأصابع التي تثير شك المحكمة (على سبيل المثال، ربما ترتبط بصورة كبيرة بالقضية أو تتعلق بشكل خاص بقضية المتهم) ولكن يعدها الخبير أدنى من حد المعيار المقبول للتقديم في المحكمة. وللتغلب على هذه القيود، طورت بعض البلدان الأخرى وتبنت نهجًا شموليًا غير رقمي في العقود الأخيرة لا يتطلب حدًّا أدنى من عدد خصائص التضليع ولكن يهتم بثلاثة مستويات مميزة من تفاصيل مضلع الاحتكاك بوصفها جزءًا من عملية تقييم تسلسلية ونظامية صارمة.[19] يمكن لهذه الطريقة الإبلاغ عن نتيجة *أي* مقارنة لبصمات الأصابع بواحدة من أربع طرق (أي التطابق أو الاستبعاد أو تفاصيل غير كافية أو غير حاسمة - أو مصطلح مشابه) ومن ثمَّ يمكنها التعبير عن "درجة من عدم التأكد" بما يتماشى مع مجالات علم الأدلة الجنائية الحديثة الأخرى. وبناء على ذلك، في أي عملية تبادل دولي لبيانات بصمات الأصابع، يجب الإقرار بهذه التباينات في التقارير العلمية لنفس الأشكال البيومترية.

لقد شهد العقد الماضي نقاشًا وبحثًا كبيرًا على الصعيد الدولي بخصوص هذا الموضوع، حيث فضل العديد من الولايات القضائية طريقة واحدة لتقديم النتائج العلمية بحيث تغطي مجالات الأدلة الجنائية التقليدية والفحوص الجنائية المرتبطة بالتقنيات الرقمية والإلكترونية. وقُدم العديد من المقترحات ولكن لا يزال النموذج الحاسم بانتظار الموافقة ولا تزال المسألة مطروحة للنقاش الدولي. إن الإرهاب تهديد دولي، لذلك لا بد أن يكون الذين يتعاملون مع البيانات البيومترية ونتائج البحث ملمين بالكامل بمعايير إعداد تقارير الأدلة الجنائية الخاصة بالشركاء الدوليين لمشاركة البيانات. ومن الممارسات الجيدة كذلك التحقق بصورة مستقلة من أي نتائج تقدمها البلدان/الولايات القضائية الشريكة الأخرى من خلال إخضاع حالات التطابق إلى بروتوكولات التحليل الجنائي ومعايير إعداد التقارير للبلد المضيف قبل اتخاذ أي إجراء (راجع القسم 3-3-3-).

[18] للمزيد من القراءة عن هذا الموضوع، راجع "تفسير الأدلة: تقييم الأدلة الجنائية في قاعات المحاكم" بقلم برنارد روبرتسون وج.أ. فيجناكس (Wiley برقم 8 96026 0471) و"مقدمة عن الإحصائيات لعلم الأدلة الجنائية" بقلم ديفيد لوسي (Wiley برقم 0-02200-470-0) و"تعزيز الأدلة الجنائية في الولايات المتحدة: طريق إلى المستقبل" بقلم مجلس البحوث الوطني للأكاديميات الوطنية (The National Academies Press برقم 13: 3-13135-309-0-978).

[19] تُعرف هذه الطريقة اختصارًا باسم ACE-V الذي يشير إلى التقدير والمقارنة والتقييم والتحقق.

4-2-1 التفسير العلمي: الهوية والنشاط

هناك عامل مهم آخر يميز أي تطبيق بيومتري تجاري نموذجي، مثل أنظمة الدخول البيومترية لأحد المباني، عن أي قاعدة من قواعد البيانات البيومترية الجنائية. كلاهما يمتلك القدرة على تحديد هوية فرد بواسطة إما البحث 1:1 أو 1:كثير ولكن التطبيق الجنائي يمتلك قدرة إضافية مهمة، وهي أن بيانات مسرح الجريمة يمكنها أيضًا تقديم دليل على النشاط بجانب الهوية. حيث يمكن تفسير الموقع والوضع والتوزيع والاتجاه للأدلة الجنائية على نحو علمي لتقديم معلومات إضافية عن الوقت وتسلسل الأحداث أثناء أي حادث والأنشطة الخاصة بالمتورطين. وتحسن هذه الأدلة السياقية الإضافية بشكل واضح القيمة الإثباتية لمواد مسرح الجريمة ويجب فهمها بالكامل وأخذها في الاعتبار من جانب المحققين أو المحللين الذين يتعاملون مع النواتج الواردة من قواعد البيانات البيومترية الجنائية (راجع القسم 3-3-3-).

ملاحظة بيانات السير الذاتية والبيانات المرتبطة المجمعة أثناء عمليات إدارة الحدود (راجع القسم 3-1-1-) يمكن استخدامها بطريقة مشابهة بالتوافق مع البيانات البيومترية لتقديم دليل على النشاط بجانب الهوية. *يوضح هذا فعالية الاستخدام والمشاركة لكلٍ من بيانات مسرح الجريمة والبيانات البيومترية للحدود لتوقع الأنشطة الإرهابية وتتبعها وإيقافها* (راجع القسم 3-3-2-1-).

3-1 الممارسات الموصى بها

أ) تُشجع الدول على تبني أنظمة بيومترية أو زيادة استخدامها لتوثيق هوية الأفراد ومنعهم من تقديم مواصفات فردية زائفة أو محاولة انتحال صفة شخص آخر.

ب) يتم تصميم الأنظمة البيومترية وضبطها حسب احتياجات كل عمل تجاري من حيث الدقة والأمان وأحجام المستخدمين والإنتاجية وموثوقية التشغيل. ولذلك يجب على الدول تقييم متطلبات استخدامهم الخاصة بدقة قبل الاستثمار في أي تطبيق بيومتري جديد.

ج) يمكن تحسين عمليات إدارة الهوية بالاستدلال البيولوجي من خلال جمعها مع قواعد البيانات البيومترية الجنائية لإنشاء إطار وطني فعال للتحقيق والاستخبار في سبيل محاربة الإرهاب والأنشطة الإجرامية المرتبطة بذلك.

د) هناك تباينات في المنهجية والمعايير الدولية لإعداد التقارير الجنائية. وبناء على ذلك، يوصى بتدريب جميع الموظفين الذين يتعاملون مع النواتج الواردة من قواعد البيانات البيومترية الجنائية لفهم القيمة النسبية والقيود المحتملة للنتائج.

1-3-1 الوثائق المرجعية

التحقق من الهوية - أهمية السياق واستمرار الهوية، ص 11-16 مجلة Keesing Journal of Documents & Identity، التقرير السنوي لإدارة الهوية لعام 2011-2012

في عام 1995، تم تعريف "الأنظمة البيومترية" بواسطة الموجز البيومتري لحكومة الولايات المتحدة على أنها "...التعرف الآلي إلى الأفراد اعتمادًا على سلوكهم وخصائصهم البيولوجية."

الصفحة 1، التعرف إلى السمات البيومترية: التحديات والفرص، مجلس البحوث الوطني، واشنطن (2010)، متاح للتنزيل على: http://www.nap.edu/openbook.php?record_id=12720&page=1

جاين وآخرون "الأنظمة البيومترية: كشف الهوية الشخصية في المجتمع المترابط شبكيًا"، نورويل، ماساتشوستس: دار (1999) Kluwer Academic Publisher

فهم دليل الأنظمة البيومترية (نسخة العمل) – معهد القياسات الحيوية www.biometricsinstitute.org

وثائق المواصفات المتاحة للعموم رقم 92:2011 مدونة قواعد الممارسات المتعلقة بتنفيذ أي نظام بيومتري - المعهد البريطاني للمعايير www.bsigroup.com

مكتب الأمم المتحدة المعني بالمخدرات والجريمة: "الشرطة: خدمات الأدلة الجنائية والبنية التحتية" و"مهارات الموظفين المطلوبة وتوصيات المعدات لمعامل علم الأدلة الجنائية." www.unodc.org

التقرير السنوي لمنظم الطب الشرعي بالمملكة المتحدة تشرين الثاني/نوفمبر لعام 2016 - تشرين الثاني/نوفمبر 2017 – د. جيليان تولي

الاستعراض الإداري لقاعدة بيانات الحمض النووي والتوصيات، لعام 2017، الفريق العامل المعني بالحمض النووي التابع للشبكة الأوروبية لمعاهد علوم الأدلة الجنائية، نيسان/أبريل 2017" http://enfsi.eu/wp-content/uploads/2017/09/DNA-databasemanagement-review-and-recommendatations-april-2017.pdf

تنميط الحمض النووي الجنائي: علم البيولوجيا، والتكنولوجيا، والوراثة لواسمات التكرارات المترادفة القصيرة - جون م. باتلر. نُشر بواسطة Elsevier Academic Press برقم-13: 978-0-12-147952-7

تفسير الأدلة: تقييم الأدلة الجنائية في قاعات المحاكم - بقلم برنارد روبرتسون مع ج.أ. فيجناكس. نُشر بواسطة Wiley برقم 8 96026 0471

مقدمة عن الإحصائيات لعلم الأدلة الجنائية - ديفيد لوسي. نُشر بواسطة Wiley برقم 0-02200-470-0

تعزيز الأدلة الجنائية في الولايات المتحدة: طريق إلى المستقبل - بقلم مجلس البحوث الوطني للأكاديميات الوطنية. نُشر بواسطة The National Academies Press برقم-13: 978-0-309-13135-3.

2- الحوكمة والتنظيم

لأغراض تتعلق بالوضوح والاتساق، ينطبق القسم التالي عن الحوكمة والتنظيم على جميع الأقسام الواردة في هذا العرض التجميعي ويجب عدّه ساريًا على جميع الممارسات والتدابير والتوصيات المُقدمة والموضحة عبر النسخة الحالية من هذا العرض التجميعي.

يتناول القسم 2 الحوكمة والمتطلبات التنظيمية للتقنية البيومترية من وجهات النظر الخاصة بالقانون الدولي، وقانون حقوق الإنسان، والاستعراضات الأخلاقية، ومتطلبات حماية البيانات، والحق في الخصوصية. ويلي ذلك طرح نظرة أوسع على مواطن الضعف المحتملة للأنظمة البيومترية وبعض من التدابير الرقابية التي يمكن استخدامها للتخفيف من المخاطر. ومن ثمَّ يتم النظر في المعايير الدولية للعمل التقني والعلمي، ويشمل ذلك عمليتي التوثيق والاعتماد للتطبيقات البيومترية، إضافةً إلى أنظمة إدارة الجودة التي يتم الانتفاع بها في العمليات الجنائية المرتبطة. ويغطي الجزء الأخير من هذا القسم الاحتياجات من الموارد والصيانة والشراء الخاصة بالنظام - أو الشبكة - البيومترية لمكافحة الإرهاب، ولا سيما القرارات التشغيلية والمالية الرئيسية التي يجب اتخاذها عند تقييم أي نظام ممتد أو جديد مرتقب.

2-1 القانون الدولي، متضمنًا قانون حقوق الإنسان

الدول مُلزمة بحماية الذين يخضعون لولايتهم القضائية من الهجمات الإرهابية وتقديم مرتكبي مثل تلك الجرائم إلى العدالة بينما تمتثل لحقوق الإنسان. لقد أكد مجلس الأمن التابع للأمم المتحدة والجمعية العامة على ضرورة أن تضمن الدول أن أي تدابير يتم اتخاذها لمحاربة الإرهاب تتوافق مع جميع التزاماتها بموجب القانون الدولي، ولا سيما القانون الدولي لحقوق الإنسان، وقانون اللاجئين، والقانون الإنساني. ولا شك أن احترام حقوق الإنسان وسيادة القانون عوامل *تكميلية* للتدابير الفعالة لمكافحة الإرهاب وضرورية لنجاح جهود مكافحة الإرهاب[20].

إنها حقيقة أن نطاق تطبيق حقوق الإنسان يختلف بين الدول الأعضاء. فبعض الدول ليست مشاركة في بعض صكوك حقوق الإنسان العالمية والعديد منها مشاركون في صكوك حقوق الإنسان الإقليمية[21] التي تختلف في نقاط معينة. كما تختلف الدول الأعضاء أيضًا في تضمين معايير حقوق الإنسان الدولية في القانون المحلي. علاوة على ذلك، أعربت بعض الدول عن تحفظات أو قدمت تصريحات في وقت الاعتماد أو الالتحاق، مما يحد من التزامهم بالتزامات تعاهدية معينة.

دعا مجلس الأمن في قراره 2396 (لعام 2017) الدول الأعضاء إلى التقييم والتحقيق بشأن المقاتلين الإرهابيين الأجانب المشتبه بهم وأعضاء أسرهم المصاحبة لهم، بما في ذلك الأزواج والأطفال، وإعداد تقييمات مخاطر شاملة لهؤلاء الأفراد وتفعيلها. من المهم، عند تطوير الأنظمة لجمع البيانات البيومترية، اتخاذ احتياطات تتعلق بحماية البيانات ومعايير حقوق الإنسان،[22] مع الانتباه بصفة خاصة للحاجة إلى ضمان أن أي أنظمة مطورة لجمع المعلومات وتسجيلها (بما فيها البيانات البيومترية) حول الأطفال يتم استخدامها ومشاركتها بطريقة مسؤولة، الأمر الذي يحمي بالكامل حقوق الإنسان الخاصة بالأطفال بما يتوافق مع القانون المحلي والدولي، بما في ذلك، بصفة خاصة، تلك المنصوص عليها بموجب اتفاقية حقوق الطفل التابعة للأمم المتحدة (1989).

[20] راجع على سبيل المثال قرارات مجلس الأمن 1373 (2001)، و1624 (2005)، و2178 (2014) و2396 (2017)؛ وقرارات الجمعية العامة A/RES/68/276 وA/70/L.55

[21] راجع على سبيل المثال منشور وكالة الحقوق الأساسية التابعة للاتحاد الأوروبي "تحت المراقبة - الأنظمة البيومترية، وأنظمة تكنولوجيا المعلومات الأوروبية، والحقوق الأساسية http://fra.europa.eu/en/publication/2018/biometrics-rights-protection

[22] S/2015/975، الفقرة 8؛ S/2015/939، المبدأ 15 (e).

استخدام الأنظمة البيومترية المتوافق مع حقوق الإنسان

تسعى الدول على نحو متزايد إلى تضمين استخدام الأنظمة البيومترية بوصفها أداة مهمة لمكافحة الإرهاب. إن التعرف إلى الصوت، ومسح حدقة العين، والتعرف إلى الوجه، وبصمات الأصابع، والحمض النووي، ومسح الجسم، وطريقة مشي الفرد ما هي إلا أمثلة قليلة على العديد من التقنيات الرقمية التي طُورت واستخدمت لأغراض مكافحة الإرهاب. وتنطوي هذه التدابير التكنولوجية على صعوبات قانونية وسياسية معقدة تتعلق بكلٍّ من جهود الدول في سبيل مكافحة الإرهاب وبالتزاماتها بخصوص حقوق الإنسان. ففي حين أن الأنظمة البيومترية قد تكون أداة قانونية لكشف هوية المشتبه بهم الإرهابيين، يحتاج النطاق التقني الواسع والتطور السريع لهذه التقنية إلى قدر أكبر من الاهتمام لأن الأمر يتعلق بحماية حقوق الإنسان، بما في ذلك على سبيل المثال لا الحصر حق الخصوصية. لقد نصت المادة 17 من العهد الدولي للحقوق المدنية والسياسية على أنه لا يجوز تعريض أي شخص، على نحو تعسفي أو غير قانوني، لتدخل في خصوصياته أو شؤون أسرته أو بيته أو مراسلاته، ولا لأي حملات غير قانونية تمس شرفه أو سمعته، وأن من حق كل شخص أن يحميه القانون من مثل هذا التدخل أو المساس. وقد أقر مجلس الأمم المتحدة لحقوق الإنسان بأن "الانتهاكات أو التجاوزات التي تمس الحق في الخصوصية قد تؤثر في التمتع بحقوق إنسان أخرى، بما فيها الحق في حرية التعبير وفي اعتناق الآراء دون تدخل، والحق في حرية التجمع السلمي وتكوين الجمعيات...."[23] وفي حين أن الحق في الخصوصية في ظل القانون الدولي ليس مطلقًا، إلا أنه من المعروف جيدًا أن أي تدخل في الحق يجب أن يتماشى مع مبادئ الشرعية والتناسب والضرورة. علاوة على ذلك، لا يجوز أن يحدث التدخل في الخصوصية الذي تأذن به الدول إلا على أساس القانون، الذي يجب أن يكون متفقًا بنفسه مع أحكام العهد ومراميه وأهدافه، وأن يكون التدخل معقولًا بالنسبة إلى الظروف المعينة التي يحدث فيها.[24] كما يجب ألا ينطوي مثل هذا التدخل على أي تمييز على أساس العرق، أو اللغة، أو الدين، أو الأصل القومي أو الاجتماعي، أو الرأي سياسيًا أو غير سياسي، أو أي أساس آخر يقره القانون الدولي.[25]

أحاط مقرر الأمم المتحدة الخاص المعني بالحق في الخصوصية علمًا بأن العديد من البلدان في جميع أنحاء العالم قد حددت حقًا أساسيًا شاملًا في الكرامة والتطوير الحر دون عوائق لشخصية الفرد، والذي قد يتأثر سلبًا بسبب الانتهاكات التي تمس الحق في الخصوصية.[26] وقد بدأ إعلان الأمم المتحدة العالمي لحقوق الإنسان والعهد الدولي للحقوق المدنية والسياسية بالتأكيد على أن الاعتراف بالكرامة المتأصلة في جميع أعضاء الأسرة البشرية وبحقوقهم المتساوية الثابتة هو أساس الحرية والعدل والسلام في العالم.[27] وقد تتعرض هذه الحقوق للتهديد بسبب الاستخدام غير المناسب للبيانات البيومترية. فإساءة استخدام مثل هذه البيانات قد يؤدي كذلك إلى تعريض حقوق مراعاة الأصول القانونية لمخاطر شديدة، بما في ذلك الحق في افتراض البراءة والحقوق الأخرى المرتبطة بالإجراءات الجنائية.[28] علاوة على ذلك، قد يؤدي جمع مثل هذه البيانات بكميات كبيرة دون الامتثال لمبادئ الضرورة والتناسب إلى انتهاك الحق في الخصوصية نفسه.[29]

---

[23] قرار مجلس حقوق الإنسان A/HRC/RES/34/7 (2017).
[24] اللجنة المعنية بحقوق الإنسان، التعليق العام رقم 16: المادة 17 (الحق في الخصوصية)، الفقرة 3-4.
[25] العهد الدولي للحقوق المدنية والسياسية، المادة 2(1) و26.
[26] تقرير المقرر الخاص المعني بالحق في الخصوصية، A/HRC/31/64 (2016).
[27] إعلان الأمم المتحدة العالمي لحقوق الإنسان والعهد الدولي للحقوق المدنية والسياسية، الديباجة.
[28] العهد الدولي للحقوق المدنية والسياسية، المادة 9، 14.
[29] العهد الدولي للحقوق المدنية والسياسية، المادة 2(3).

يجب أن تفكر الدول، بغرض منع إساءة استخدام البيانات البيومترية، في مراجعة قوانينها المعنية بحماية البيانات الشخصية وتعديلها؛ لتتماشى مع التطبيقات الحالية للتقنيات البيومترية المحسنة. كما يجب على الدول مراجعة تشريعاتها؛ لتتماشى مع الصعوبات الناجمة عن عملية التطوير الإضافي للتقنيات البيومترية. ويجب أن يتضمن أي منهج قائم على مراعاة حقوق الإنسان في استخدام التقنية البيومترية، استخدام الاحتياطات الإجرائية والمراقبة الفعالة لتطبيقه.[30] ويتضمن ذلك تأسيس هيئات رقابية مناسبة ومستقلة للإشراف على أنشطة الوكالات الحكومية المنوطة بتقديم علاجات فعالة في حالة الانتهاكات، وتأسيس سلطات إشراف مستقلة لضمان امتثال الوكالات الحكومية والقطاع الخاص لقوانين الخصوصية وحماية البيانات[31].

1-1-2 الأخلاقيات والأنظمة البيومترية

إن التقنيات مثل الأنظمة البيومترية تخلق شكلًا خاصًا من الصعوبات الناجمة عن الفجوة التي يُسببها الابتكار التكنولوجي وسن التشريعات التي تنظم مثل هذه التقنيات. ولذلك، لجأت بعض الدول إلى تأسيس هيئات معنية بالاستعراض الأخلاقي أو غيرها من الهيئات الرقابية للتنبؤ بمثل هذه التقنيات أو التطبيقات الجديدة ودراستها وتقديم النصح حول الحالي أو المرتقب من التشريعات وسياسة الحكومة والتخطيط الاستراتيجي. وعادة ما تضم هذه الهيئات اختصاصيين من أعلى المراتب أصحاب الكفاءات العالية من مختلف مستويات المجتمع المدني وقد تضم أشخاصًا من القطاعين الخاص والعام، والعلوم والتكنولوجيا، والأوساط الأكاديمية وغير المتخصصين. وتحاول هذه الفرق المعنية بالرقابة الأخلاقية استعراض القضايا من منظور واسع، بما في ذلك الأثر المحتمل الذي قد تتركه التقنيات البيومترية على مجموعات معينة من الأشخاص أو المجتمعات، ولا سيما فيما يتعلق بالعرق والنوع الاجتماعي والعمر والمعتقدات الدينية والميل الجنسي.

توضح دراسة الحالة التالية هذا المنهج:

---

[30] اللجنة المعنية بحقوق الإنسان في تعليقها العام رقم 16 (1988)، شددت على ضرورة أن تتخذ الدول تدابير فعالة لكفالة عدم وقوع المعلومات المتعلقة بالحياة الخاصة للشخص في أيدي الأشخاص الذين لا يُجيز لهم القانون الحصول عليها أو تجهيزها أو استخدامها، وعدم استخدامها على الإطلاق في أغراض تتنافى مع العهد الدولي للحقوق المدنية والسياسية. ولكي يتسنى حماية الحياة الخاصة للفرد على أكفأ وجه ينبغي أن يكون من حق كل فرد أن يتحقق بسهولة مما إذا كانت هناك بيانات شخصية مخزنة في حزم البيانات البيومترية، وإذا كان الوضع كذلك، من ماهية هذه البيانات، والغرض من الاحتفاظ بها، مع حق كل فرد في أن يطلب تصحيح البيانات غير الصحيحة أو حذفها. كما ينبغي أن يكون بمقدور كل فرد أن يتحقق من هوية السلطات العامة أو الأفراد العاديين أو الهيئات الخاصة التي تتحكم أو قد تتحكم في هذه الحزم. راجع: http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=INT%2fCCPR%2fGEC%2f6624&Lang=en

[31] قرار الجمعية العامة رقم 95/45 (1990) حول المبادئ التوجيهية لتنظيم استخدام ملفات البيانات الشخصية المحوسبة واللائحة العامة لحماية البيانات للاتحاد الأوروبي لعام 2018، المادة 51 (سلطة إشرافية).

دراسة الحالة 4 – الأنظمة البيومترية بالمملكة المتحدة وفريق الأخلاقيات الجنائية[32]

نشأ هذا الفريق من الفريق الوطني الأصلي المعني بأخلاقيات الحمض النووي الذي أُسس للإشراف على التقنيات والأساليب العلمية المستخدمة في أول قاعدة بيانات للحمض النووي في العالم. ويشمل نطاق مسؤوليته في الوقت الراهن الأدلة الجنائية بشكل عام، إضافةً إلى التقنية البيومترية. حيث يدرس الفريق كل مسألة جديدة مقابل مجموعة كبيرة من الاعتبارات القانونية والأخلاقية والسياسة الاجتماعية. ويعملون حسب المبادئ المنظمة الآتية:

المبادئ المنظمة ***الواجب تطبيقها على الإجراءات البيومترية والجنائية***	**المبادئ المنظمة** ***تنفيذ المبادئ***
☐ يجب استخدام الإجراءات لتحسين السلامة العامة والمنفعة العامة؛ ☐ يجب استخدام الإجراءات إحقاقًا للعدالة؛ ☐ يجب أن تحترم الإجراءات حقوق الإنسان للأفراد والمجموعات؛ ☐ يجب أن تحترم الإجراءات كرامة جميع الأفراد؛ ☐ يجب أن تحمي الإجراءات، إلى أقصى حد ممكن، الحق في احترام الحياة الخاصة والعائلية ما دام لا يتعارض ذلك مع الأهداف الشرعية لنظام العدالة الجنائية لحماية الجمهور من التعرض للضرر؛ ☐ يجب أن تكون التطويرات العلمية والتكنولوجية مُجهزة لتعزيز الإعفاء السريع عن البريئين، وتوفير الحماية والحل للضحايا، ومساعدة عملية العدالة الجنائية؛ ☐ يجب أن تعتمد الإجراءات على الأدلة القوية.	☐ الحياد - يجب تطبيق الإجراءات دون تحيز أو تمييز ظالم؛ ☐ التناسب - موازنة حقوق الأفراد والمنفعة العامة؛ ☐ الانفتاح والشفافية؛ ☐ ضرورة وضع الأنظمة موضع التنفيذ لتحديد الأخطاء؛ ☐ الحاجة إلى مراقبة الجودة؛ ☐ الحاجة إلى المساءلة العامة؛ ☐ الحاجة إلى الإشراف المستقل عند اللزوم؛ ☐ الحاجة إلى توفير معلومات كافية والحصول، عند اللزوم، على الموافقة من هؤلاء الذين يجب أخذ البيانات أو العينات منهم.

كما يمتلك الفريق كذلك مجموعة محددة من المبادئ المتعلقة بجمع البيانات ومعالجتها:

☐ يجب جمع البيانات وتخزينها واستخدامها فقط للأغراض المحددة والقانونية؛
☐ يجب أن تلتزم عملية جمع البيانات وتخزينها واستخدامها بالمتطلبات القانونية؛
☐ يجب اتخاذ الخطوات اللازمة لضمان الدقة والحماية والسلامة للبيانات المجمعة والمخزنة والمستخدمة؛
☐ يجب أن تكون العمليات قوية ومتوافقة مع المعايير الدولية وأن يتم تطبيقها بواسطة فريق عمل مدرب بصورة احترافية؛
☐ ينبغي الحد من التدخل في الحياة الخاصة؛
☐ ينبغي مراعاة مصالح أصحاب البيانات الثانويين (أي الأشخاص الذين يُحتمَل أن يتأثروا من جراء البيانات المُجمّعة من الآخرين، مثل أفراد الأسرة).

يؤثر تهديد الإرهاب في العديد من الدول ونتيجةً لذلك يتم تطوير تقنيات جديدة في إطار الأنظمة البيومترية والأدلة الجنائية ونشرها بسرعة من قِبل وكالات إنفاذ القانون بغية تقديم الحماية وتعزيز قدرات التحقيق. وتلعب مجموعات الرقابة الأخلاقية دورًا في هذه العملية حيث إنها في وضع يتيح لها تقديم تعليقات مستنيرة بشأن إعداد أي تقنية أو استراتيجية جديدة أو تبنيها. غير أن هذا الأمر لا يحل محل الحاجة إلى وضع تشريعات لاحقة ولكنه قد يساعد على منع استحداث طرق وممارسات جديدة غير متناسبة أو حتى غير ضرورية. كما أن هذه العملية ستنبه المشرعين أيضًا إلى الضرورة الملحة والأهمية النسبية للمسألة قيد النظر.

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

المعايير والأمثلة على كيفية تأثير الأخلاقيات والأنظمة البيومترية في بعضهما

في الوقت الحالي، تتسم المعايير الخاصة بالتقديم والاستخدام للأنظمة البيومترية أو معظم التقنيات الجديدة بالتفاوت على المستوى الدولي أو حتى المستوى الوطني. وقد أصدرت المنظمة الدولية لتوحيد المقاييس (الأيزو) معاييرها المتعلقة بالاعتبارات القضائية والاجتماعية والتطبيقات التجارية، الجزء 1 التوجيهات العامة (ISO/IEC التقرير التقني 24714:2008) ودليلها 71:2014، التي يتناول جميعها الأخلاقيات، ويتناول دليلها 71 معايير التيسير لذوي الاحتياجات مثل كبار السن وذوي الإعاقة.

يمتد الاستخدام الأخلاقي للأنظمة البيومترية إلى مجال الشؤون الإنسانية. فهناك العديد من البرامج التي أتاح فيها استخدام الأنظمة البيومترية تقديم المزايا. لقد استخدم مكتب مفوضية الأمم المتحدة السامية لشؤون اللاجئين (UNHCR)، على سبيل المثال، أنظمة بيومترية دعمًا لبرامجه القائمة منذ عام 2002، ويؤكد بشكل متزايد عملية التسجيل في الأنظمة البيومترية. ويتيح الحل البيومتري العالمي الخاص بالمفوضية، وهو نظام إدارة الهوية بالاستدلال البيولوجي (BIMS)، لمنظمة الأيزو إمكانية ضمان تفرد كل تسجيل، والتأكد من تسلُّم مختلف أشكال المساعدة التي قد تقدمها المنظمة (بما في ذلك الغذاء، أو الأموال النقدية أو الحماية أو تدخلات إعادة التوطين، من بين أمور أخرى) من قِبل مستفيديها المستحقين. وتوجد أمثلة أخرى حيث يتم تقليل عمليات تزوير الانتخابات أو الاحتيال المالي، وهما عاملان محتملان لزعزعة الاستقرار قد يشجعان على التمرد أو ازدياد الإرهاب، من خلال استخدام تحديد الهوية القائم على الأنظمة البيومترية.

توصي كذلك مفوضية الأمم المتحدة السامية لشؤون اللاجئين بالتسجيل البيومتري للأشخاص المتقدمين بطلب اللجوء بوصفه عنصرًا تكميليًا لأنظمة الدخول التي تراعي متطلبات الحماية. ويتضمن ذلك إيجاد ضمانات مناسبة لمنع التسلل المحتمل للمجرمين أو أولئك المنتمين إلى المنظمات الإرهابية أو المتطرفة. وتتضمن الممارسات الجيدة في هذا الصدد الآتي: (1) التسجيل المناسب؛ بما في ذلك السمات البيومترية من قِبل السلطات الحدودية المدربة على جوانب الحماية ذات الصلة المتعلقة بالأمن واللاجئين وحقوق الإنسان، و(2) إحالة أولئك الذين يطالبون بالحماية الدولية إلى إجراءات اللجوء. *كمبدأ عام، بهدف عدم تعريض طالبي اللجوء/اللاجئين للخطر، ينبغي عدم مشاركة بياناتهم البيومترية والشخصية الأخرى مع بلدانهم الأصلية، ما لم ينتهِ إجراء اللجوء ولم يتم منح الحماية. وينطبق هذا أيضًا على البلدان الثالثة في الظروف التي قد تتعرض فيها الحماية الفعّالة لمقدمي طلبات اللجوء أو اللاجئين للخطر.*[33]

[33] راجع القسم هـ، الفقرة 17 من وثيقة مفوضية الأمم المتحدة لشؤون اللاجئين "مواجهة المخاوف الأمنية دون تقويض حماية اللاجئين" http://www.refworld.org/docid/5672aed34.html

2-2 حماية البيانات والحق في الخصوصية

إن التقنية البيومترية من الأصول المهمة في مكافحة الإرهاب على صعيد عالمي. حيث تتميز بالقدرة اللازمة للكشف عن الأنشطة الإرهابية وعرقلتها وحماية المجتمع من الهجمات العشوائية. ولكن، تعتمد التقنية على تجميع البيانات الشخصية وتخزينها واستخدامها. وكما ذُكِر من قبل، يجب حماية تلك البيانات البيومترية بموجب القانون ويجب معالجتها دون انتهاك لحقوق الإنسان الأساسية مثل الحق في الخصوصية.

2-2-1 معايير التسجيل القانوني ومعايير البيانات

ذكر مجلس الأمن التابع للأمم المتحدة في قراره رقم 1373 (لعام 2001) الارتباط الوثيق بين الإرهاب الدولي والجريمة المنظمة عبر الوطنية، والعقاقير غير المشروعة، وغسيل الأموال، والإتجار غير المشروع بالأسلحة. وفي نفس ذلك القرار، قرر المجلس أنه يتعين على الدول منع تنقل الإرهابيين أو الجماعات الإرهابية من خلال الضوابط الحدودية الفعّالة والضوابط المفروضة على إصدار أوراق الهوية ووثائق السفر، ومن خلال التدابير الرامية إلى منع التزوير، أو الاحتيال أو الاستخدام الاحتيالي لأوراق الهوية ووثائق السفر.

لمكافحة تلك العلاقة، من المهم بناء قدرة كافية وفعّالة لمكافحة الإرهاب في جميع الدول الأعضاء.[34] ولا شك أن استخدام الأنظمة البيومترية يعد أداة حيوية في تطوير تلك القدرة.[35] ونظرًا إلى أن الأساليب التي يستخدمها الإرهابيون غالبًا ما تتضمن سرقة الوثائق أو الهويات، فإن استخدام الأنظمة البيومترية يوفر أداة قيّمة لإعادة إثبات الهويات لضحايا سرقة الهوية (راجع القسم 2-3-5-).

ومن أجل تنفيذ نظام بيومتري يتميز بالفعالية والتوافق مع قوانين حماية البيانات ويدعم الحق في الخصوصية، ينبغي مراعاة العوامل الآتية:

ضمان جودة التسجيل - يجب وضع معايير تسجيل عالية الجودة بحيث يمكن استخدام التسجيل والمطابقة البيومتريين بدقة في مجموعة كبيرة من البيئات مثل المناطق البعيدة، أو المراكز الحدودية الثابتة، أو المطارات التي تتطلب بشكلٍ متزايد معالجة أسرع للركاب مع الحفاظ على مستويات الدقة. وفي حالة الأطفال أو القُصر الشرعيين المرافقين لآبائهم أو المسافرين بمفردهم، ينبغي الاعتراف باحتمال تعرض بعض السمات البيومترية الخاصة بهم للتغيير أثناء نموهم. إضافةً إلى ذلك، يؤكد مجلس الأمن التابع للأمم المتحدة في قراره رقم 2396 (2017) ضرورة التعامل مع الأطفال بطريقة تراعي حقوقهم وتحترم كرامتهم، بما يتوافق مع القانون الدولي المعمول به.

تشريعات الخصوصية - يمكن لسلطات إنفاذ القانون أن تحد من الحق في الخصوصية، إذا كانت التدابير المتخذة ضرورية ومتناسبة ومتوافقة مع القانون الدولي لحقوق الإنسان. فعلى سبيل المثال، يمكن استخدام البيانات الشخصية للمشتبه بهم والمرافقين لهم في حالات الطوارئ، حيث يتم تنحية مبادئ الخصوصية الرئيسية، مثل الموافقة المستنيرة أو جمع البيانات الشخصية ذات الصلة جانبًا. ومع ذلك، يجب التعامل مع مبادئ الخصوصية تلك، مثل الموافقة المستنيرة، والجمع والاستخدام للأغراض المُعلَنة فحسب، والحق في تصحيح السجلات غير الدقيقة أو المضللة بوصفها المتطلبات الافتراضية في معظم الحالات. وعلاوة على ذلك، ينبغي توثيق أسباب الانحراف عن تلك المتطلبات الافتراضية وتسجيلها. ويجب أيضًا التحكم في وصول المُشغِّل إلى مثل هذه الأنظمة عن طريق الأنظمة البيومترية لضمان تحقيق مستويات عالية من الأمن.

[34] راجع أيضًا قراري مجلس الأمن 2195 (2014) و2178 (2014)
[35] قرار مجلس الأمن التابع للأمم المتحدة رقم 2396 (2017) وقراره السابق رقم 2178 (2014)

تمويل الإرهاب - للمساعدة على منع التعرض لحالات الاحتيال، وانتحال الشخصية، والمعاملات المالية المرتبطة بأنشطة الإرهاب، يمكن استخدام الأنظمة البيومترية بوصفها جزءًا من مجموعة من التدابير المتخذة للتخفيف من مثل هذه التهديدات على مستوى المنظومة المالية. ولذلك فإن استخدام الأنظمة البيومترية لمراقبة الوصول إلى المعاملات، يُعَد خيارًا فعَّالًا. كما أن توافر برنامج على الصعيد الوطني لحماية المستهلكين من التعرض لحالات الاحتيال وانتحال الشخصية المرتبطة بأنشطة الإرهاب، له فوائد عديدة على مستوى المجتمع المحلي ومستوى ضبط الأمن.[36]

المعايير الدولية للبيانات الشخصية - يجب تحديد معايير البيانات الشخصية وفقًا للمعايير الدولية بدلًا من استخدام أشكال بيومترية أو معايير تقنية أقل شيوعًا، التي قد تستند إلى عوامل مثل ضغط الصناعة المحلية أو حتى الأنظمة التي توفرها الجهات المانحة مجانًا. ويجب أن تكون المعايير المناسبة الخاصة بالمنظمة الدولية لتوحيد المقاييس (الأيزو)، ومنظمة الطيران المدني الدولي (الإيكاو)، ومنظمة الجمارك العالمية، هي المعايير الأولية عند انتقاء النظام، ومدعومة بالقائمة المرجعية لتقييم الأثر على الخصوصية والمبادئ التوجيهية للخصوصية الخاصة بمعهد القياسات الحيوية.[37]

مقبولية الأدلة - ينبغي إيلاء العناية لضمان اقتصار استخدام جميع البيانات البيومترية والشخصية على الأغراض المُعتمَدة، التي من أجلها تم الحصول على تلك البيانات. وسيضمن هذا أيضًا قبول البيانات التي تم جمعها لقواعد البيانات لأغراض المقاضاة. وينبغي أن يشمل ذلك أحكامًا لضمان التعاون من جانب صناعة تكنولوجيا المعلومات والاتصالات شريطة أن يتم وضع أساس قانوني لمثل هذا التعاون.

تفسير النواتج البيومترية – ينبغي أن تكون وكالات إنفاذ القانون، التي تحتجز الإرهابيين أو تلاحقهم قضائيًا، على علم بمخاطر إساءة تفسير نتائج قاعدة البيانات البيومترية، على سبيل المثال، فهم قيمة تطابق جزئي للحمض النووي أو مقارنة وجه غير حاسمة، نظرًا إلى المشاكل البيئية التي قد تحدث عند التقاط صورة للوجه في أماكن منخفضة الجودة. وفي تلك الحالات، يُعَد التحليل السياقي أمرًا ضروريًّا للغاية قبل اتخاذ أي إجراء (راجع القسم 3).

2-2-2 سياسة استبقاء البيانات أو حذفها

هذا مجال يجب فيه اتخاذ الإجراءات الخاصة بإنفاذ القانون ومكافحة الإرهاب بما يتوافق مع القانون الدولي لحقوق الإنسان، بما في ذلك الحق في الخصوصية. على سبيل المثال، قد يكون الحق في رؤية ملف الفرد، أو إجراء التصحيحات، أو طلب الحذف (الذي غالبًا ما يكون مضمونًا في التشريعات المتعلقة بالخصوصية، على سبيل المثال، *اللائحة العامة لحماية البيانات* للاتحاد الأوروبي (GDPR))[38] مقيدًا بالحاجة إلى حماية الشهود أو سرية التحقيقات الجارية.

[36] راجع الموقع الشبكي لصندوق النقد الدولي حيث يتم سرد أدوات مكافحة غسيل الأموال وغيرها من أدوات مكافحة الاحتيال www.imf.org

[37] راجع http://www.biometricsinstitute.org

[38] اللائحة العامة لحماية البيانات للاتحاد الأوروبي لعام 2018، المادة 7 (الموافقة)، والمادة 17 (حق محو البيانات)، والمادة 15 (حق الوصول إلى البيانات)

تتفاوت سياسات استبقاء البيانات تفاوتًا كبيرًا في جميع أنحاء العالم، ولا سيَّما بالنسبة إلى أولئك الذين تم القبض عليهم أثناء إجراء التحقيقات في إطار إنفاذ القانون. ويحتفظ العديد من الولايات القضائية بالبيانات البيومترية الخاصة بالمُدانين بارتكاب جرائم عقوبتها السجن المُؤبَّد، إلا أنه لا يوجد معيار مشترك خاص بالمُشتبَه في ارتكابهم للجرائم أو من أُلقي القبض عليهم بتهمة ارتكاب الجرائم، ولكن لم تثبُت إدانتهم بعد ذلك.

من الممارسات الجيدة تخزين البيانات البيومترية على نحو منفصل عن بيانات السير الذاتية ذات الصلة الخاصة بها. فقد يحتاج ضحايا سرقة الهوية (من خلال الجريمة أو النشاط الإرهابي) إلى إعادة إثبات هويتهم بسرعة بعد سرقتها وإساءة استخدامها. عند تصميم النظام، سيكون من الضروري التخطيط لإعادة اتصال البيانات البيومترية وبيانات السير الذاتية عند حدوث ذلك. ويمكن تحقيق ذلك من خلال تخصيص شريحة واحدة من البيانات الوصفية للسجلات البيومترية على هيئة رقم مرجعي فريد. ومع ذلك، يجب حماية عملية إعادة الاتصال هذه، لضمان سلامة النظام والبيانات في جميع الأوقات، وتتطلب وجود بروتوكول أمان قوي مثل:

- ☐ اشتراط أن يكون الموظف المختص بالوصول على مستوى رفيع داخل المنظمة
- ☐ استخدام السمات البيومترية الخاصة به للوصول إلى النظام
- ☐ تسجيل ذلك الوصول على نحو رسمي
- ☐ تسجيل أسباب السعي لهذا الوصول على نحو رسمي

يمكن تعزيز الأمان على نحو أكبر من خلال وجود أكثر من شخص واحد داخل المنظمة، يشارك في التحقق من صحة عمليات الإدخال أو عملية الإلغاء. ومن شأن ذلك أن يسمح بتناوب الموظفين، الذين يؤدون هذه الوظائف، ويخلق المزيد من الأمان.

3-2-2 معالجة البيانات

يجب أن تقوم منظمة مسؤولة عن معالجة البيانات بتعيين مراقب بيانات، الذي سيكون مسؤولًا عن إدارة جميع الأنشطة الخاصة بمعالجة البيانات، بما في ذلك جمع البيانات، وتخزينها، واستخدامها، وحذفها. ويتحمل مراقب البيانات المسؤولية، حتى في حال الاستعانة بأطراف خارجية لإتمام وظيفة معالجة البيانات.

يتطلب قانون الخصوصية الأكثر شمولًا من السلطات، التي تجمع البيانات الشخصية، ضمان عدم إمكانية إجراء أي معالجة للبيانات أو تخزينها في البلدان، حيث يكون قانون الخصوصية الخاص بها في مستوى أدنى مما هو عليه في بلد التجميع.

يجب أن يلتزم أي مُورّد أو مُشغِّل من الجهات الخارجية بالعقود، التي تتطلب مستوى عاليًا جدًا من الأمان ويجب أن تتضمن عمليات تدقيق خارجية من جانب الوكالة المُكلَّفة وعقوبات على عدم الامتثال لمتطلبات الأمان والخصوصية الواردة في العقد.

4-2-2 مشاركة البيانات

شددت الأمم المتحدة، في عدد من التصريحات، على ضرورة التعاون بين الدول من حيث التحسينات التشريعية لمحاكمة الإرهابيين، ولا سيَّما المقاتلين الإرهابيين الأجانب، وفي الوقت نفسه، الحماية بموجب القانون، وحقوق الإنسان، والخصوصية.[39] وتحتاج المشاركة في الوقت الفعلي للبيانات الشخصية، مثل السمات البيومترية داخل السلطات الحكومية وبين الدول أيضًا، إلى التعاون بهدف تنسيق أداء التشغيل المتبادل للمنصات والتنسيقات.[40]

فحيثما تتم مشاركة البيانات الشخصية للإرهابيين أو الإرهابيين المُشتبَه بهم، ستدعو الحاجة إلى وجود ثقة كبيرة بشأن عدد من القضايا مثل الاستخدام المحدد لتلك البيانات المشتركة، ودقة البيانات وسياقها، وكمية البيانات التي يمكن مشاركتها ونوعها. ويجب أن تستند ترتيبات مشاركة البيانات إلى الاتفاقات الرسمية المبرمة بين جميع الأطراف المعنية.

هناك عوامل أخرى يجب أن تؤخذ في الاعتبار في عملية المشاركة هذه. وتشمل هذه العوامل الشرط المتمثل في استناد الطلبات للكشف عن البيانات الشخصية إلى اشتباه حقيقي في وجود نشاط إرهابي، وتفاصيل متطلبات الإثبات، وتحديد ما إذا تم الحصول على البيانات في ظل ظروف قمعية - تمثل مسألة إثبات رئيسية للعديد من البلدان.

وبصفة عامة، تنطبق المبادئ الآتية:

1- وجوب الموافقة على مشاركة البيانات الشخصية، بما في ذلك السمات البيومترية، على نحو مشروع محليًا وخضوعها لإطار قانوني واضح بين الكيانات المُرسِلة للبيانات والمُتلقِّية لها، على الصعيدين المحلي والدولي
2- وجوب اقتصار استخدام مثل هذه البيانات على الأغراض المُعتمَدة التي من أجلها تم الحصول على تلك البيانات
3- لا يمكن مشاركة البيانات إلا مع المتسلِّمين الموثوق بهم.[41] حيث يشمل المبدأ المنصوص عليه في القسم 2-2-3- مشاركة البيانات ويجب عدم إرسال البيانات الشخصية إلى الولايات القضائية، حيث يكون مستوى حماية الخصوصية أقل من مستوى البلد المُرسِل.
4- (وفقًا للقسم 2-1-) من أجل عدم تعريض طالبي اللجوء أو اللاجئين للمخاطر، ينبغي عدم مشاركة البيانات البيومترية وغيرها من البيانات الشخصية الخاصة بهم مع بلدانهم الأصلية، ما لم ينتهِ إجراء اللجوء ولم تُمنَح الحماية (راجع أيضًا دراسة الحالة 10).

5-2-2 منع إساءة استخدام البيانات

توجد مسألتان رئيسيتان على الأقل هنا تتعلقان بإساءة استخدام البيانات.

المسألة الأولى هي الضرورة الملحة لتأمين جميع البيانات الشخصية، بما فيها السمات البيومترية، من الوصول غير المصرح به لها وإساءة استخدامها. ويشمل ذلك كلًّا من التهديدات الخارجية والمخالفات الداخلية من جانب الموظفين المأذون لهم.

---

[39] قرار مجلس الأمن التابع للأمم المتحدة رقم 2322 (2016) بشأن التعاون الدولي وقرار مجلس الأمن التابع للأمم المتحدة رقم 2396 (2017) بشأن تعزيز تدابير مواجهة التهديدات التي تشكلها عودة الإرهابيين الأجانب.

[40] قرار مجلس الأمن التابع للأمم المتحدة رقم 2178 (2014) وإعلان مدريد الصادر عن وزراء الخارجية في الاجتماع الخاص للجنة مكافحة الإرهاب التابعة لمجلس الأمن في (28) الثامن والعشرين من شهر تموز/يوليو لعام 2015.

[41] من الأمثلة على مشاركة البيانات الشخصية بين المتسلِّمين الموثوق بهم الاتفاقات بشأن بيانات الجرائم القابلة للتسجيل بين مكتب السجلات الجنائية التابع لرابطة كبار ضباط الشرطة ومكتب التحقيقات الفيدرالي الأمريكي أو غير ذلك من شرطة الاتحاد الأوروبي، أو السلطات المعنية بشؤون الهجرة أو نظام اتصالات الشرطة المأمونة I-24/7 الخاص بمنظمة الإنتربول الذي تدعمه قاعدة بيانات الإنتربول المتعلقة بوثائق السفر الضائعة أو المسروقة ونظام وثائق السفر المرتبطة بالنشرات.

المسألة الثانية هي الحاجة إلى التأكد من أن البيانات الشخصية المُقدَّمة دقيقة، أي تم وضعها في سياق ذي صلة وتقديمها دون وجود نوايا خبيثة. ويكتسي هذا الأمر أهمية خاصة حيث قد تسعى حكومة أو حزب آخر إلى وضع المعارضين السياسيين على قوائم المراقبة بنية التأثير في حقوقهم الأساسية.

6-2-2 أمن البيانات والتحقق من صحتها

ينبغي لكل منظمة تعيين مراقب بيانات يتمتع بالأقدمية، والتدريب، والخبرة الكافية، الذي سيتحمل مسؤولية جمع كل البيانات الشخصية، واستخدامها، ونقلها، بما في ذلك السمات البيومترية.

يجب أن تشمل المسؤوليات الرئيسية لهذا الدور صنع السياسات وإجراءات التشغيل الموحدة. ويجب أن يقرر صاحب الدور أيضًا، أثناء مرحلة تصميم النظام، الشكل البيومتري أو الأشكال البيومترية التي ستكون الأنسب للتطبيق.

تتطلب جميع السياسات والممارسات الفعَّالة المتعلقة بالأمن والخصوصية القرارات الآتية على الأقل، بغض النظر عما إذا تم استخدام إحدى السمات البيومترية أم لا:

- ☐ هل تم إجراء تقييم الأثر على الخصوصية[42] قبل استحداث ممارسة تجارية جديدة أو تقنية جديدة؟
- ☐ هل تتوفر البرامج والإجراءات اللازمة للتدريب والتوعية، التي تحافظ على الخصوصية المناسبة وثقافة حقوق الإنسان، إضافةً إلى معرفة عملية بالأنظمة البيومترية من جانب جميع العاملين الذين يُشغِّلون النظام؟
- ☐ هل يتم استخدام تقنيات التشفير أو اختزال البيانات في المراحل الحرجة من جمع البيانات الشخصية، وتخزينها، واستخدامها، ومشاركتها، بما في ذلك السمات البيومترية؟
- ☐ هل توجد ضوابط صارمة للوصول إلى البيانات وتسجيل لمرات الوصول التي تتطلب إظهار السمات البيومترية لأولئك الذين يصلون إلى ملفات البيانات الشخصية الحساسة؟
- ☐ هل توجد عمليات مُوثَّقة تحدد آليات الإبلاغ والإجراءات التصحيحية المطلوبة في حال وجود انتهاكات للخصوصية والأمن؟
- ☐ هل يتم إجراء الاختبارات وعمليات التدقيق المنتظمة للتأكد من اتباع الممارسات المتعلقة بالأمن والخصوصية وأنها قوية وفعَّالة ولا تزال كذلك؟
- ☐ هل هناك عملية رسمية لتوثيق المسائل التي تظهر نتيجة لإجراء التدقيق المنتظم، ومن ثمَّ معالجتها؟
- ☐ هل يتم إجراء الفحوص العشوائية والمنتظمة على صلاحية البيانات الشخصية الموجودة في النظام وسلامتها؟

يوجد عدد من المبادئ التوجيهية والمعايير الدولية التي تقدم المشورة إلى مراقبي البيانات ومنظماتهم.[43]

[42] يشكل تقييم الأثر على الخصوصية (PIA) جزءًا من منهج "الخصوصية حسب التصميم" لإدارة البيانات داخل المنظمات العامة والتجارية. وتضمن عملية تقييم الأثر على الخصوصية الامتثال للمتطلبات القانونية والتنظيمية للخصوصية من خلال تحديد المخاطر المحتملة وتطوير استراتيجيات التخفيف لإدارتها.

[43] قرار الجمعية العامة رقم 95/45 (1990) بشأن المبادئ التوجيهية لتنظيم استخدام ملفات البيانات الشخصية المحوسبة *والمبادئ التوجيهية للخصوصية البيومترية* الصادرة عن معهد القياسات الحيوية، المخصصة للاستخدام الدولي www.biometricsinstitute.org

فيما يتعلق بالتحقق من صحة البيانات المُجمَّعة، بما في ذلك السمات البيومترية، فمن الضروري اتباع الإجراءات القانونية الواجبة من أجل حماية حقوق الإنسان، بما في ذلك الحق في الخصوصية، بل وأيضًا من أجل ضمان الامتثال الكامل للشروط القضائية للإدانة أو، على سبيل المثال، إجراءات تسليم المطلوبين. وفي مجال إجراءات تسليم المطلوبين، قد تكون هذه الشروط أكثر صرامة في بعض البلدان منها في بلدان أخرى، لا سيما فيما يتعلق بمعايير الإثبات والاستجواب.

يجب أن يكون المبدأ التوجيهي الرئيسي لوكالات إنفاذ القانون وسلطات مراقبة الحدود هو الحاجة إلى وجود فرق مخصصة من المُحلِّلين، يتمتعون بالمهارات والموارد لتحقيق نتائج دقيقة وقابلة للتنفيذ. ويساعد هذا على رصد الأنشطة الإرهابية قبل وقوع الحادث وبعده والحصول على الأدلة المقبولة، بما في ذلك السمات البيومترية مثل: الحمض النووي، وبصمات الأصابع، والوجه، والصوت. وينبغي لهذه القدرة أن تحقق الاستفادة التامة من جميع التقنيات الخاصة بالتقاط السمات البيومترية والبحث فيها.

7-2-2 الرقابة

قد تحدث عواقب قانونية غير محمودة وأضرار أخرى للأفراد من خلال إساءة استخدام البيانات الشخصية (سواء بسبب الحقد أو بالخطأ). وينطبق هذا بصفة خاصة على قوائم المراقبة أو غيرها من آليات الإنذار.

ينبغي الحرص عند وضع الإرهابيين أو المجرمين المُشتبَه بهم على قوائم المراقبة. كما ينبغي إجراء فحوص صارمة وشاملة لتقييم أسباب الإدراج وصلاحية جميع الطلبات قبل وضع بيانات الفرد في القائمة. ويجب أن تخضع البيانات الواردة في قوائم المراقبة للمراجعة المنتظمة للتأكد من أنها حديثة وذات صلة على حدٍ سواء.

وعلى نحو مشابه، وفقًا للقانون الدولي لحقوق الإنسان وتشريعات الخصوصية، يجب أن يكون لأصحاب البيانات الحق في إعادة النظر في إدراج أسمائهم في أي قائمة. وينبغي أن تعلن سلطات الإدراج عن حق إعادة النظر، والاستئناف، ووجود آليات للشكوى.

أثناء عملية الإدراج، تتحمل وكالات إنفاذ القانون، وسلطات مكافحة الإرهاب، والسلطات الحدودية واجبًا قانونيًا للجمع، والتخزين، والتحليل للبيانات الخاصة بالإرهابيين المُشتبَه بهم والمرافقين لهم، وأنماط سلوكهم مثل مسارات الرحلات الجوية، والمعاملات المالية، وحركات الإقامة. ومع ذلك، يجب التأكد من أن المعلومات المتعلقة بالمُشتبَه بهم ومرافقيهم، تظل سرية وضمن الأطر القانونية المأذون بها لتجنب حدوث حالات السجن أو الاضطهاد التعسفية.

يجب أن تكون هناك احتياطات قوية ضد الجمع، والتخزين، والاستخدام التعسفي للبيانات الشخصية، بما في ذلك آليات الرقابة من جانب إحدى الهيئات المستقلة. وقد يكون لدى الدول بالفعل هيئات رقابة على الخصوصية، التي من شأنها القيام بهذه الوظيفة بوصفها جزءًا من اختصاص قائم حاليًا أو اختصاص مُوسَّع ومع ذلك، إذا كانت إحدى الدول ليس لديها هيئة من هذا القبيل في الوقت الحالي، فعليها إنشاء هيئة من أجل أداء هذا الدور الحيوي.

على وجه الخصوص، من الضروري وجود آليات رقابة منصوص عليها في القانون، التي تكون مستقلة، وفعَّالة، ومحايدة. وينبغي أن تتمتع بصلاحيات لرصد مدى كفاية الاحتياطات للبيانات البيومترية وتقييمها، بما في ذلك ما يتعلق بالمشاركة الدولية لهذه البيانات. وينبغي أن يتمتع الأفراد بالقدرة على الاتصال بالآلية الرقابية للحصول على معلومات عن بياناتهم وتقديم شكوى، إذا شعروا أن حقوقهم في خطر. وينبغي - إلى أقصى حد ممكن - تقديم المعلومات لأصحاب البيانات عن كيفية التعامل مع بياناتهم، في شكل واضح ومُبسَّط. كما ينبغي أن تكون هناك سبل انتصاف مناسبة منصوص عليها في القانون بشأن انتهاكات حقوق الإنسان في مجال التعامل مع البيانات البيومترية، بما في ذلك انتهاكات الحق في الخصوصية.

3-2 إدارة مخاطر النظام

تتضمن إدارة مخاطر النظام فهرسة حالات الفشل بالنظام، إما داخل جزء منه (مثل قارئ بيومتري) وإما في النظام برُمَّته (تكوين النظام)، وتحديد ما إذا كانت حالات الفشل هذه تؤدي إلى خطر مؤداه عدم عمل النظام على النحو المنشود. وتحدد تلك الإدارة التهديدات والمخاطر، ثم تحلل عواقب أي تهديد يتم إدراكه أو استغلاله، وتُنفِّذ أخيرًا عمليات التخفيف عند الاقتضاء.

عادةً ما تكون الأنظمة البيومترية المُتضمَّنة في التطبيقات المتعلقة بمكافحة الإرهاب معقدة، حيث تتضمن مكونات متعددة لتكنولوجيا المعلومات، وتفاعلات مع بيئة الاستحواذ، وتفسيرات بشرية. ويؤدي ذلك إلى التعرض إلى حالات المخاطر متعددة الأوجه مع العديد من نقاط الفشل المحتملة، لا سيَّما أن أهداف الإرهاب لديها دوافع قوية وغالبًا ما تكون مُزوَّدة بموارد كافية لتجاوز الضوابط الأمنية.

يمكن أن يؤدي تنفيذ أنظمة مكافحة الإرهاب - دون تطبيق إدارة المخاطر المناسبة - إلى اكتساب ثقة غير واقعية بفعالية النظام. وقد تشمل العواقب عدم التعرف إلى هوية الأفراد المطلوبين، أو تسريب معلومات شديدة الحساسية تتعلق بقائمة المراقبة، أو إدخال تعليمات برمجية ضارة.

غالبًا ما يسافر الإرهابيون المعروفون أو المُشتبَه بهم بهويات مُزيَّفة أو مُزوَّرة. لذلك، من المهم - من منظور إدارة المخاطر - أن يتم تنفيذ أنظمة المطابقة التقليدية للسير الذاتية على نحو صحيح (راجع القسم 3-1-4-). ويمكن لسلطات الحدود الوطنية تنفيذ عمليات التحقق البيومتري وعمليات البحث في قائمة المراقبة للمساعدة على التخفيف من هذه المخاطر (راجع القسم 3-3-1-2).

تعتمد عملية إعداد أي نظام بيومتري اعتمادًا كبيرًا على السياق. على سبيل المثال، يختلف كل مطار من الناحية البيئية وقد يختلف أيضًا من حيث سلوك الركاب والخصائص الديموغرافية. وسيؤدي ذلك إلى ظهور أنواع مختلفة من المخاطر التي تتطلب وضع استراتيجيات للتخفيف. ومع ذلك، فإن إحدى استراتيجيات التخفيف المهمة والمشتركة بين الجميع، تتمثل في قيام المختبِرين المحترفين بإجراء اختبارات الاختراق النشطة والمنتظمة لضمان كشف المخاطر وفهمها.

إدارة المخاطر هي نشاط متخصص وتخضع للمعايير الدولية وكذلك للمتغيرات المحلية (انظر المراجع في نهاية هذا القسم).

لا شك أن استمرارية تصريف الأعمال التجارية يمثل عاملًا حاسمًا لأي مستخدم ويجب أن تكون بروتوكولات الطوارئ جزءًا لا يتجزأ من إجراءات التشغيل الموحدة لأي نظام من الأنظمة البيومترية. ونتيجة لذلك، في حالة حدوث عطل لأي جزء من أجزاء النظام والذي يؤدي إلى عدم قدرته على تقديم خدمة طبيعية، فإنه من المعتاد أن يكون لديك تدبير واحد أو أكثر من التدابير العاجلة المتاحة لتوفير تغطية خدمات مؤقتة. وقد يتخذ ذلك الأمر شكل التدخل اليدوي من جانب المُشغِّلين من بني البشر (مثل مسؤولي الحدود، الذين يتولون مهمة فحص جوازات السفر يدويًا عند تعطُّل البوابات البيومترية الآلية) أو الرجوع إلى نظام احتياطي أو صفيف المكونات.[44]

[44] خير مثال على ذلك الصفائف المكررة للأقراص المستقلة التزامنية (RAID)، التي توجد عادة في أنظمة التعرف الآلي إلى بصمات الأصابع (AFIS). ويمكن دمج هذا التكوين للأقراص الأصغر داخل الخادم لتشكيل صفيف كبير، يعمل على تحسين الأداء، والأمن، ويوفر أيضًا دعمًا احتياطيًا داخل مُجمَّع الخادم. وسيحتاج معظم المستخدمين لإجراءات إنفاذ القانون إلى عمل أنظمة التعرف الآلي إلى بصمات الأصابع الخاصة بهم على مدار اليوم طوال أيام الأسبوع طوال العام، ونتيجة لذلك، فإنه ليس بالخيار المتاح إغلاق النظام فترة طويلة لإتمام أعمال الصيانة، أو الترقية، أو الإصلاح. ومن ثمَّ، فإن الاستخدام السريع للصفائف المكررة للأقراص المستقلة التزامنية المزدوجة، يسمح للنظام بالعمل على نحو مستمر نظرًا إلى إمكانية تعطُّل أكثر من قرص واحد أو إزالته من عمليات التشغيل المباشرة، وسيتم الاحتفاظ بالبيانات على الأقراص النشطة لضمان تقديم الخدمات إلى المستخدم دون انقطاع.

1-3-2 مواطن الضعف والتهديدات الجديدة

تحقيقًا لأغراض التحليل، تم تصنيف أوجه التهديد في التطبيقات البيومترية لمكافحة الإرهاب إلى المجالات الرئيسية الآتية:

- *تكنولوجيا المعلومات العامة:* جميع أنواع تكنولوجيا الواجهة الخلفية المستخدمة لإدارة قواعد البيانات، وتأمين نقل المعلومات، والتدقيق في أنشطة المستخدم، ومنع انتشار الفيروسات. ويتعين تغطية ذلك الأمر من خلال الالتزام بأفضل الممارسات في مجال أمان تكنولوجيا المعلومات للأنظمة الحكومية.
- *المستشعرات البيومترية والبيئة:* نوع التقنية المُستخدَمة والمخاطر المُحدَّدة. على سبيل المثال، استخدام بصمات أصابع مُزيَّفة، أو نظارات سوداء، أو تقنية تغيير نبرة الصوت.
- *ماكينات المطابقة البيومترية:* تكوين ماكينات المطابقة، بما في ذلك إعداد الحد الأساسي، وكشف العروض المشبوهة، وإدارة قوائم المراقبة.
- *الإشراف البشري:* ستتمتع جميع الأنظمة البيومترية بمستوى معين من معدلات القبول والرفض الخاطئة، وينطبق ذلك بصفة خاصة في سياق العمليات الخاصة ببحث كشف الجرائم، حيث قد تكون السمات البيومترية المُسجَّلة متفاوتة الجودة (راجع القسم 1). وستتطلب عمليات القبول والرفض الخاطئة هذه التحقيق والتقييم من جانب مشغلين مُدرَّبين تدريبًا مناسبًا. ويمكن أن يؤدي التعامل غير الصحيح إلى احتمالية احتجاز الأفراد الخطأ، أو تنفيذ ممارسات عمل غير فعَّالة، أو بدلًا من ذلك، فقدان أهداف قائمة المراقبة الذين يمثلون تهديدًا عالي المستوى.

الجدول 1

مجالات التهديد	المسؤولية	العواقب	أمثلة التخفيف
تكنولوجيا المعلومات العامة	المديرون في مجال أمان تكنولوجيا المعلومات	كشف قائمة المراقبة، واختراق أمن النظام، وتغيير المطابقات. وإمكانية استخدام القالب البيومتري المسروق في إعادة إنشاء سمات بيومترية.	أمن الاتصالات، ومكافحة الفيروسات، وجُدُر الحماية (قطع الخدمة)، وإدارة قوائم مراقبة السِيَر الذاتية، والتفاعل المؤمن مع الأنظمة الخارجية. والقوالب البيومترية القابلة للإلغاء.
المستشعرات البيومترية والبيئة	المُورّد / موظف تكامل النظم	أهداف قائمة المراقبة قادرة على تجنب الانكشاف من خلال خداع المستشعر	إعداد البيئة، وكشف العروض المشبوهة، وتصفية الجودة. خوارزميات مكافحة الانتحال (كشف هجوم العرض).
ماكينات المطابقة البيومترية	المُورّد / موظف تكامل النظم / أفراد أمن تكنولوجيا المعلومات	أهداف قائمة المراقبة قادرة على تجنب الانكشاف	ضبط النظام، وإدارة جودة التسجيل، والإدارة المناسبة للواجهة الخلفية. واستخدام الأنظمة البيومترية متعددة الأشكال بدلًا من استخدام شكل بيومتري واحد.
الإشراف البشري	وكالات/ مشغلو الأمن الحكومي	احتجاز الأفراد الخطأ، وممارسات عمل غير فعَّالة، وفقدان أهداف قائمة المراقبة الذين يمثلون تهديدًا عالي المستوى.	التعلم، والتدريب والاعتماد، والتدقيق، وتصميم واجهة المستخدم، والمصطلحات المناسبة

2-3-2 التهديدات حسب الشكل البيومتري

تنطوي الأنظمة البيومترية على وجه من أوجه التهديد المُعقَّدة، الذي لا يزال يتطور مع انتشار التقنية على نطاق أوسع. ولا يدخل في نطاق هذه الوثيقة تقديم تصنيف شامل لجميع مواطن الضعف والمخاطر في هذا المجال – ولكن تم توثيقها في المعيار ISO/IEC 30107-2_2017 [1]، إضافةً إلى بعض الأمثلة المحددة لوكالات مراقبة الحدود [2].

فيما يلي الأشكال البيومترية الشائعة المُستخدَمة لأغراض مكافحة الإرهاب:

الوجه - يكون الوجه متاحًا بشكل عام ويمكن الحصول عليه بسهولة عن طريق أنظمة الالتقاط القريبة أو البعيدة، ولكنها تخضع لصعوبات وقيود تقنية معينة يمكن أن ينتج عنها إصدار صور وجه رديئة الجودة. وتؤثر مثل هذه الصور بشكل كبير في احتمالية الكشف الصحيح (أو بالعكس قد تؤثر في عدد حالات القبول الخاطئة التي يُصدرها النظام). وقد تكون من العوامل المؤثرة جودة كلٍّ من صورة التسجيل (الصورة المستخدمة لإنشاء قائمة المراقبة) والصورة المأخوذة من أي كاميرا. ويمكن العثور على أمثلة بشأن كيفية تحسين نظام المراقبة باستخدام تقنية التعرف إلى الوجه في الوثيقة المرجعية [3]. وتشمل سمات الجودة المحددة: الإضاءة، والوضعية، وموضع الكاميرا، والتعبير، وأغطية الرأس، والنظارات، واللحى، والدقة (وحدات البكسل بين العينين)، والعُمر.
وفيما يلي بعض مواطن الضعف الشائعة في حالة الوجه:

- *احتيال التشابه:* عبارة عن وثيقة هوية يستخدمها شخص يشبه الشخص الحقيقي المقصود. وتسمح هذه الوثيقة للشخص المُدرَج في أي قائمة مراقبة بادعاء أنه ليس الهدف الصحيح إذا تم اكتشافه.
- *الأقنعة:* أصبحت الأقنعة المطاطية المتقدمة متاحة ويصعب اكتشافها من خلال الملاحظة العادية.
- *مستحضرات التجميل:* عندما يكون الهدف هو تجنب الانكشاف، فإن الاستخدام الصحيح لمستحضرات التجميل، يمكن أن يحجب ملامح الوجه بينما تبدو طبيعية للملاحظ من بني البشر.
- *النظارات:* يمكن للنظارات ذات الإطارات السمكية أو القاتمة أن تحجب جزءًا مهمًا من ملامح الوجه المُستخدَمة في التعرف إليه.
- *السلوك:* إذا اشتبهت الأشخاص المُستهدَفة في أنها تخضع للمراقبة، فإن استخدام هاتف محمول والنظر نحو الأرض، يمكن أن يجعل الحصول على صورة جيدة أمرًا صعبًا.
- *تحويل الصور:* العينات البيومترية (مثل صور الوجه) المأخوذة من اثنين أو أكثر من الواهبين، التي يتم دمجها للسماح بالتحقق الناجح من أيٍّ من الأشخاص الواهبين مقابل الهوية المُحوَّلة.

بصمات الأصابع - تُستخدَم الأنظمة البيومترية القائمة على بصمات الأصابع في جميع أنحاء العالم لإنفاذ القانون، ولذلك هناك العديد من قواعد البيانات وقوائم المراقبة الحالية، التي تحتوي على قوالب لبصمات الأصابع (راجع القسم 1). وفيما يلي بعض مواطن الضعف الشائعة للأنظمة البيومترية القائمة على استخدام بصمات الأصابع:

- *الأصابع المُزيَّفة:* استخدام بصمات أصابع مُزيَّفة مصنوعة من مواد تحاكي خصائص الجلد. ويمكن ارتداؤها على كل إصبع على نحو فردي أو دمجها بوصفها جزءًا من قفاز كامل لكل يد.
- *الإتلاف المُتعمَّد:* عندما يشتبه شخص مُستهدَف في أنه قد يكون تحت المراقبة، يمكنه محاولة إتلاف بصمات الأصابع باستخدام مواد كيميائية، أو مواد كاشطة، أو تقنيات أخرى.
- *بصمات أصابع المتوفين:* استخدم الإرهابيون طبعات بصمات الأصابع الخاصة بالمتوفَّى من أجل إنشاء هويات بهدف فتح حسابات مصرفية وإجراء معاملات مالية لتمويل عملياتهم.

حدقة العين - توفر تقنية التعرف إلى الحدقة شكلًا بيومتريًا دقيقًا وموثوقًا به. ويكون ذلك الشكل مستقرًا على مر الزمن ويصعب تزويره. وهناك قدر كبير من أعمال البحث والتطوير، التي يتم إجراؤها على أنظمة التعرف إلى الحدقة لمكافحة الانتحال وتقديمها أيضًا بوصفها شكلًا بيومتريًا بديلًا/إضافيًا لأغراض إدارة الحدود. وتتضمن مواطن الضعف الآتي:

- استخدام *العدسات اللاصقة التجميلية* ذات نمط الحدقة المطبوع.
- استخدام صور الوجه عالية الجودة المتوفرة على الإنترنت من أجل *نُسَخ العيون المطبوعة*.
- *اتساع حدقة العين* إلى أقصى حد ممكن. وبهذه الطريقة، قد لا يتعرف الماسح الضوئي إلى نمط الحدقة (ينخفض أداء التعرف إلى الحدقة عند استخدام خوارزمية مطابقة على العين نفسها، التي لها حجم حدقة مختلف إلى حد كبير).
- وضع *العدسة اللاصقة مصفوفة النقاط* ذات النمط المُزيَّف مباشرة على عين الشخص. سيؤدي ذلك إلى منع نظام مسح الحدقة من التعرف إلى أي حدقة موجودة في قاعدة البيانات الخاصة به.
- *العدسة الصلبوية ذات الحدقة المرسومة فوقها*. يغطي هذا النوع من العدسات المنطقة المرئية بالكامل من مقلة العين، وسيبدو الشخص الذي يرتديها بنمط عين مختلف تمامًا.
- *زرع حدقة ملونة جراحيًا* في الجزء الأمامي من حدقة العين الحقيقية للشخص. في حين أن العديد من الأشخاص الذين يختارون الجراحة، لا يرغبون في سوى تغيير لون عيونهم، فإنه يمكن للفرد الذي يرغب في إخفاء هويته أيضًا استخدام هذا الإجراء.
- تتطلب عملية المطابقة أن تكون القوالب المرجعية جاهزة أثناء إجراء المصادقة، مما يخلق فرصًا أمام أي مهاجم لسرقة القوالب، الأمر الذي يتيح بدوره مزيدًا من الهجمات.

الصوت - يمكن استخدام تقنية تحديد المتحدث لمراقبة المكالمات الهاتفية ورفع مستويات التأهب بخصوص الأفراد المُستهدَفين. وتتميز تقنية تحديد المتحدث بصفة عامة بالدقة الهامشية لأحجام المعاملات الكبيرة أو قواعد البيانات الكبيرة (لا سيَّما عبر قنوات الهاتف المختلفة). ومع ذلك، قد يكون تطبيق هذه التقنية فعَّالًا، عندما يكون عدد المكالمات المراد البحث عنه وعدد الأفراد الموجود في قائمة المراقبة صغيرًا ومحدودًا نسبيًا.
وفيما يلي بعض مواطن الضعف الشائعة في حالة الصوت:

- *مغيرات الصوت:* هناك عدد من التطبيقات المتاحة للهواتف الذكية، تسمح بتعديل الصوت.
- *الخطاب الصناعي:* من عوامل التهديد الجديدة استخدام الأدوات التي يمكن تدريبها على أحد الأصوات، بحيث يمكن قراءة رسالة مكتوبة على نحو طبيعي من خلال الخطاب الصناعي.

3-3-2 جودة التسجيل

بغض النظر عن الشكل البيومتري المُستخدَم، قد لا تستحق السمات البيومترية ذات الجودة الرديئة للغاية تضمينها بوصفها جزءًا من قائمة مراقبة. وفي حال عدم كفاية الجودة، فمن المُرجَّح أن تفوت الأنظمة البيومترية المطابقات الحقيقية وقد تُصدر عددًا كبيرًا من حالات القبول الخاطئة. ويمثل قياس جودة السمات البيومترية وإدارتها جانبًا مهمًا لضمان وجود نظام بيومتري دقيق. ويتميز كل شكل بيومتري بمقاييس الجودة الخاصة به، فالوجه على سبيل المثال تتعلق به مسائل مثل الإضاءة، والوضعية، وأغطية الرأس. وأي عامل يؤدي إلى خفض جودة السمة البيومترية أو حجبها أثناء عملية التسجيل، سيؤثر في قدرة البحث والمطابقة للنظام. وتتناول سلسلة من معايير الأيزو تحديد مقاييس الجودة (راجع القسم 2-4).

4-3-2 الإنتاجية وإدارة القدرات

تعتمد إنتاجية النظام على نحو طبيعي على الموارد الحاسوبية المتاحة للمطابقة والمعالجة. وغالبًا ما تكون عملية المطابقة البيومترية، عملية حاسوبية باهظة الثمن، ولا سيَّما بالنسبة إلى قوائم المراقبة الكبيرة. وتُعَد الموارد البشرية من أكبر القيود التي تعانيها عملية المطابقة البيومترية. فكل عملية مطابقة بحاجة إلى التحقيق تتطلب مشغلًا مُدرَّبًا لإجراء عملية تقييم. وهذا يعني، على سبيل المثال، أنه حتى باستخدام نظام تعرف إلى الوجه ذي التوازن المضبوط بدقة للحد الأساسي، فإن عدد حالات القبول الخاطئة الواجب معالجتها في بيئة مزدحمة قد يكون كبيرًا. ويمثل فهم هذه المتطلبات اعتبارًا مهمًا من اعتبارات الميزانية، ليس لتوقع احتياجات الإنشاء الأولية فحسب، ولكن للعمليات المستقبلية كذلك.

5-3-2 سرقة الهوية

سرقة الهوية، عمومًا، هي الحصول غير المصرح به على بيانات شخصية لفرد ما، على سبيل المثال الاسم، وتاريخ الميلاد، والعنوان، وما إلى ذلك لارتكاب أعمال إجرامية، ولا سيَّما الاحتيال مثل استخدام البيانات المسروقة لتقديم الطلبات المُزيَّفة للحصول على قروض أو للحصول على بطاقات ائتمان، أو شراء سلع عالية القيمة. وتتسبب سرقة الهوية، التي تنطوي على بيانات بيومترية، في مشاكل خطيرة نظرًا إلى بقاء الملامح البيومترية عادةً مع أي شخص طوال حياته وعدم إمكانية إعادة تعيينها بسهولة بالطريقة نفسها المتبعة مع كود رقم التعريف الشخصي أو كلمة المرور. وقد تتعلق سرقة البيانات البيومترية بالسمات البيومترية المادية الفعلية للفرد، على سبيل المثال إنشاء نسخة مماثلة من بصمة الإصبع أو قناع الوجه أو قد تكون سرقة القالب البيومتري الموجود داخل تطبيق ما أو قاعدة بيانات. وقد تم تطوير العديد من تدابير التخفيف الرئيسية لمواجهة هذه المخاطر، ومن أهمها:

الكشف عن وجود حياة: يتم دمج العديد من المستشعرات في أجهزة التقاط السمات البيومترية للنظر إلى ما وراء الركيزة الأساسية للسمة البيومترية التي يتم تقديمها، والتمييز بين الجلد الحي والقطع الصناعية المُزيَّفة.

القوالب البيومترية القابلة للإلغاء: بمجرد تسجيل سمة بيومترية في النظام، يتم تشويه ملامحها عمدًا على نحو قابل للتكرار. وإذا تم اختراق القالب أو سرقته لاحقًا، يتم إنشاء قالب بديل للسمة البيومترية ذاتها باستخدام خصائص تشويه مختلفة، بحيث يصبح القالب المسروق على الفور قالبًا مُكرَّرًا. وبذلك يمكن استخدام السمة البيومترية نفسها في مجموعة متنوعة من التطبيقات، ولكن ستكون القوالب مختلفة. ولا يتم تسجيل الملامح البيومترية "الأصلية"، غير المُشوَّهة مطلقًا، وهذا يوفر حماية أكبر للخصوصية ويطمئن المستخدم.

وتجدر الإشارة إلى أنه حيثما يتم استخدام السمات البيومترية بالاقتران مع وثائق الهوية (مثل جوازات السفر)، تقل مخاطر التعرض لسرقة الهوية إلى أدنى حد؛ لأنه في حالة "سرقة" إحدى السمات البيومترية أو نسخها، لا يزال المضيف بحاجة إلى وثيقة صالحة يمكن جعلها غير صالحة، إذا لزم الأمر. ويمكن التقاط السمات البيومترية مثل الوجه سرًا أو من مصادر عبر الإنترنت من جانب أولئك الذين يرغبون في الحصول على الصورة. وهذا يعني أن السلطات المُستخدِمة للوجه بوصفه سمة بيومترية في الوثائق الرسمية، يجب أن تضمن أنها قد نظرت في مخاطر هذا النوع من السرقة واعتمدت تدابير التخفيف المناسبة.

4-2 المعايير الدولية

1-4-2 معايير التشغيل التقني

من الضروري أن يكون أي نظام من الأنظمة البيومترية لمكافحة الإرهاب مؤمنًا، ويمكن الاعتماد عليه باستمرار، ويفي بمتطلبات العمل المُحدَّدة للمستخدم. وتستند هذه المتطلبات إلى عوامل رئيسية مثل:

- اختبار النظام لضمان توافقه مع مواصفات الأداء ومقاييسه الحالية والمستقبلية
- بيئة تشغيل وشبكة آمنتَين
- تقييم الأثر على الخصوصية والتقييم القانوني
- إدارة المخاطر للنظام الشامل
- كفاءة المُشغِّل الملموسة
- التعامل مع البيانات وضمان سلامتها لجميع ميزات النظام مثل أجهزة التقاط البيانات البيومترية، وتسجيل البيانات، والتأكد من بيانات اعتماد الهوية، وتخزين البيانات واسترجاعها، وأداء المطابقة ومعدلات الخطأ، وأي بيانات وصفية غير بيومترية
- موثوقية البرامج والأجهزة
- قابلية التشغيل المتبادل - نقل البيانات وتبادلها مع الأنظمة الأخرى
- تصميم واجهة بشرية – سهولة الاستخدام من أجل (1) الحصول على أصحاب البيانات وتسجيلهم و(2) لمُشغِّلي النظام - مجموعة الأدوات، ومكان العمل، وهندسة بيئة العمل، والبيئة

توجد مجموعة واسعة من المعايير الدولية، والإقليمية، والوطنية، لتضمين هذه العناصر الأساسية والوظائف الثانوية. ويعتمد مالكو الأنظمة البيومترية، ومستخدموها، وعملاؤها على هذه المعايير، لضمان عمل تطبيقاتهم بفعالية طوال دورة حياتها ووفقًا لمواصفات الأداء للشركة المُصنِّعة. كما يعتمدون أيضًا على المعايير لتوفير ضمانات لعمليات مثل الشراء (راجع القسم 2-4)، والصيانة والترقية للأنظمة البيومترية، لا سيَّما إذا كانت تمثل جزءًا من شبكة وطنية أو دولية أوسع نطاقًا، لتبادل البيانات. ومن غير المحتمل أن يوافق الشركاء أو الشركاء المحتملون على المشاركة في مثل هذه الشبكة، في حال عدم تشغيل بعض أعضاء الشبكة للأنظمة البيومترية الخاصة بهم بما يتوافق مع المعايير الوطنية أو الدولية.

تقوم المنظمة الدولية لتوحيد المقاييس[45] (الأيزو) بتطوير المعايير ونشرها عبر مجموعة كبيرة من الصناعات، بما في ذلك الأنظمة البيومترية والأدلة الجنائية. وتمثل منظمة الأيزو اتحادًا عالميًا لهيئات المعايير الوطنية، مكونًا من 162 بلدًا، يُسهمون في وضع المعايير من خلال عضوية اللجان المتخصصة المختلفة. وقد تنضم بلدان أخرى بوصفها أعضاء مراسلة أو مشتركين لتلقي معلومات عن المعايير.

[45] http://www.iso.org

تضم منظمة الأيزو أيضًا لجنتين مشتركتين مع اللجنة الدولية للتقنيات الكهربائية[46] (IEC) التي تضع المعايير وتقييمات الامتثال (CA) لجميع المنتجات الكهربائية، والإلكترونية، والمنتجات ذات الصلة. ويمكن أن يُطمئِن تقييم الامتثال أي مشترٍ محتمل، الذي قد لا يفهم تمامًا تعقيدات النظام أو المنتج، أنه يفي بالمعايير التقنية ومعايير السلامة المطلوبة أو غيرها من المعايير على النحو المحدد. وهناك ثلاثة أنواع من تقييم الامتثال. تقييم الامتثال خاصة *الطرف الأول* الذي يتم تنفيذه من جانب المُورّد، وتقييم الامتثال خاصة *الطرف الثاني* الذي يتم تنفيذه من جانب المُستخدِم ولكن النموذج الأكثر فعالية من تقييم الامتثال، هو *الجهة الخارجية*، الذي يتم تنفيذه من جانب هيئات مستقلة. وتُعرَف عملية التقييم باسم التوثيق حيث يتم إصدار شهادة عادةً بعد إجراء عملية تقييم ناجحة. ويتمثل الغرض منها في التحقق من أن منتجًا أو خدمة تفي بمواصفات معينة أو معيار ISO/IEC معين.

قد تضع الهيئات الإقليمية أيضًا معايير من أجل تنسيق الأنظمة وممارسات العمل لمجموعة من البلدان. على سبيل المثال، تجمع اللجنة الأوروبية للتوحيد القياسي[47] (CEN) بين هيئات التقييس الوطنية في 34 بلدًا أوروبيًّا، ولديها فريق عامل محدد للأنظمة البيومترية (WG18) يعمل على تكييف المعايير من المنظمات الدولية أو المنظمات الوطنية للامتثال للمتطلبات الأوروبية مثل قانون الخصوصية وحماية البيانات.

قد تضع المنظمة ذات الصلة بعض المعايير على صعيد المستوى الوطني لذلك البلد، على سبيل المثال، يوجد في الولايات المتحدة الأمريكية هيئات مثل المعهد الوطني الأمريكي للمقاييس والمعايير (ANSI) والمعهد الوطني للمواصفات القياسية والتكنولوجيا (NIST)، التي تضع المعايير التي تنطبق على قسم الأدلة الجنائية والتطبيقات البيومترية المرتبطة بها. وقد اعتمد العديد من البلدان معايير المعهد الوطني للمواصفات القياسية والتكنولوجيا على نطاق واسع في المجالات الرئيسية مثل النقل الإلكتروني لبصمات الأصابع عبر الشبكات. ويقوم المعهد أيضًا بإجراء الاختبار التنافسي والتصنيف لخوارزميات البحث والمقارنة البيومترية المتاحة تجاريًا المُستخدَمة من أجل الأشكال البيومترية الأخرى مثل الوجه والحدقة.[48] ويتيح ذلك للمشترين المحتملين لأنظمة المطابقة البيومترية الحصول على معلومات موضوعية فيما يتعلق بالأداء النسبي للخوارزميات التي تستخدمها الشركات المُصنِّعة المنافسة في السوق الدولية.

2-4-2 معايير التشغيل العلمية وإجراءات إدارة الجودة

إضافةً إلى المعايير التقنية وبرامج التوثيق المتاحة للأنظمة البيومترية، هناك معايير منظمة الأيزو المتعلقة بإجراءات علم الأدلة الجنائية مثل ISO/IEC 17025:2017 "المتطلبات العامة لكفاءة مختبرات الفحص والمعايرة." وتتناول هذه المعايير الإجراءات والكفاءات المطلوبة لإجراء الاختبارات و/أو المعايرات العلمية، بما في ذلك أخذ العينات. حيث تستعرض تلك المعايير إدارة العمليات، إلى جانب كفاءة العلماء وحياديتهم، وصحة أساليبهم. وتستخدم تلك المعايير كلًّا من الاختبارات وعمليات التدقيق الداخلية، التي يُجريها المختبر نفسه، واختبارات الكفاءة وعمليات التدقيق الخارجية، التي تُجريها هيئات الاعتماد الخارجية وتُشرِف عليها من أجل إعطاء زخم لعملية التحسين المستمر واعتماد المختبر. وتحدد عمليات التفتيش المستقلة المنتظمة هذه، ما إذا كان المختبر يفي بالمعايير المطلوبة لتحقيق الاعتماد أو الحفاظ عليه بموجب المعيار ISO17025:2017. ويؤكد الاعتماد أن المختبرات تطبق نظام إدارة الجودة (QMS) بكامل طاقته وأنها مؤهلة لإجراء عمليات الاختبار والمعايرة العلمية باتساق بما يتوافق مع المعيار.

[46] http://www.iec.ch
[47] https://www.cen.eu
[48] http://www.nist.gov

يستعرض نظام إدارة الجودة (QMS) على نحو منتظم جميع العوامل، التي تُسهم في تحقيق الأداء الفعَّال للمختبر، والأهم من ذلك، فإنه يراجع أي حالة من حالات عدم المطابقة. ويتم استخدام إجراءات العمل التصحيحية لتحديد السبب الجذري لأي حالة من حالات عدم المطابقة ويتم صياغة الإجراءات الوقائية لمنع تكرار ذلك. وتقوم الاستعراضات الإدارية الداخلية بتقييم أداء المختبر على نحو منهجي وفقًا لقائمة مرجعية شاملة للمتطلبات التنظيمية، والاحتياجات من الموارد، ومتطلبات الإجراءات، واحتياجات الإدارة التي تستند إلى دليل الجودة الخاص بالمختبر.

هناك معايير يمكن تطبيقها في مجالات أخرى للأدلة الجنائية مثل التحقيق في مسرح الجريمة (مثل المعيار ISO 17020:2012). لذلك من المحتمل والمهم للغاية أن يكون هناك منهج قائم على المعايير فيما يتعلق بعمليات مكافحة الإرهاب، يشمل جميع العمليات الخاصة بالأدلة الجنائية بدايةً من مسرح الجريمة إلى قاعة المحكمة، بما في ذلك:

- إدارة مسرح الجريمة وفحصه، التي تشمل استراتيجيات جنائية وبيومترية (راجع القسم 3-3-3-2-) التقييمات التفسيرية، وتنسيق الموارد، وطرق أخذ العينات، وإجراءات مكافحة التلوث، ومواد التعبئة، وفحص الأشخاص المُشتبَه بهم، والشهود، والضحايا.
- العمليات المختبرية، التي تشمل أخذ العينات، وإجراء التحاليل، وإدارة قواعد البيانات، وكفاءة الموظفين، والإبلاغ عن النتائج.
- أدلة المحاكم – بروتوكولات الشاهد الخبير، وأساليب الحياد وعرض الأدلة.

5-2 المشتريات وإدارة الموارد

1-5-2 المشتريات

سيكون للحكومات الوطنية إطارها التنظيمي ومعايير الانتقاء الخاصة بها لمراقبة المشتريات من السلع والخدمات. ومع ذلك، هناك عدد من النقاط وثيقة الصلة بالموضوع، التي يجب مراعاتها عند تقييم الحاجة إلى وجود نظام بيومتري وبعض الجوانب المحددة المتعلقة بشراء التطبيقات، التي سيتم استخدامها لمواجهة تهديد الإرهاب:

متطلبات الأعمال التجارية – يجب تقديم توضيح مفصل لمزايا الأنظمة البيومترية وأسباب استخدامها بدلًا من الأشكال البديلة للمصادقة والتعرف إلى السمات البيومترية في خطة العمل. وينبغي الموازنة بعناية بين الفوائد والعيوب المحتملة مثل التكلفة، ومواطن الضعف التقنية، والاعتراضات وسُبُل المقاومة المحتملة من الجمهور/العملاء، والمخاوف الأخلاقية، والتهديدات الأخرى التي تحددها عملية تقييم المخاطر. كما ينبغي تقييم أحجام المستخدمين الحالية والمستقبلية ومستويات السعة لقواعد البيانات بعناية، للتأكد من أن النظام سيكون قادرًا على التعامل مع معدلات الإنتاجية المتوقعة، لا سيَّما في أوقات ذروة الطلب. (راجع القسم 2-3-4-).

الخصوصية وحماية البيانات – (راجع القسم 2-2) يجب أن تمتثل قدرة أي نظام بيومتري للتعرف إلى الإرهابيين المعروفين والمُشتبَه بهم لحقوق الأشخاص بأن يتم احترام خصوصيتهم وحماية بياناتهم الشخصية، وفقًا للقانون الوطني والدولي. حيث يمكن أن ترتكب الأنظمة البيومترية أخطاء إما عن طريق الخطأ في التعرُّف إلى الأشخاص، وإما الفشل في التعرف إليهم، وكلاهما ينطوي على مخاطر كبيرة على سُمعَة مالك (مالكي) البيانات. ولا بد من النظر في هذه الجوانب بعناية أثناء مرحلة التصميم لأي تطبيق بيومتري ووضع إجراءات مناسبة للتعامل مع مثل هذه الحوادث والتخفيف منها عند حدوثها.
ملاحظة إن الموارد المطلوبة لتوسيع اختصاص أي هيئة قائمة من هيئات الرقابة على الخصوصية أو لإنشاء هيئة جديدة، (راجع القسم 2-2-7-) ينبغي أن تُؤخَذ في الاعتبار في أي سياسة وطنية أو إقليمية أو خطة مشروع تسعى إلى تطوير الأنظمة البيومترية الرامية إلى مكافحة الإرهاب.

الأمان – إن أي جزء من نظام أو شبكة للسمات البيومترية، التي تستخدم البيانات المتعلقة بالإرهابيين وأعمال الإرهاب يمكن أن يصبح هدفًا للهجمات الإلكترونية/السيبرانية أو الهجمات المادية الخارجية، أو التدخل الداخلي، أو أعمال التخريب من خلال تصرفات الموظفين المخالفة للقانون. ونتيجة لذلك، يجب أن تكون هناك مستويات عالية من الأمان متعدد الطبقات لحماية بيئات التشغيل، والأجهزة، والبرامج، وشبكات الاتصالات، والبيانات المُخزَّنة. وينبغي النظر أيضًا في عملية فحص الموظفين، الذين يقومون بتشغيل النظام والتحقق من أنهم ليسوا عُرضة لأي شكل من أشكال الإكراه من جانب الإرهابيين أو مرافقيهم. كما يجب إجراء عمليات تدقيق منتظمة بهدف تحديد حالات الفساد الداخلي والأدلة على وجود حالات سوء التصرف. ويجب أيضًا التصدي للتهديدات الأخرى مثل هجمات العرض (راجع القسم 2-3) ومنعها بعدّ ذلك جزءًا من الاستراتيجية الأمنية العامة.

الأداء – يجب أن تعمل التطبيقات البيومترية المُستخدَمة لمكافحة الإرهاب بأعلى درجات الدقة، أي بمعدلات خطأ منخفضة للغاية مع الحفاظ على تحقيق معدل إنتاجية مقبول. فقد تتعرض حياة العديدين للخطر، إذا أخفق النظام في تحديد هوية أحد الإرهابيين، لأي سبب من الأسباب، في أي مرحلة من العملية. ومن المحتمل أن يتطلب الحصول على هذا المستوى من الأداء البيومتري، وضمان المحافظة عليه، والتحسين الدوري له تمويلًا كبيرًا طوال دورة حياة النظام. ولا شك أن وجود هذه المخاطر العالية يعني أيضًا أن إجراءات معالجة الاستثناءات، يجب أن تكون شاملة ودقيقة لمنع الإرهابيين الذين يتفادون عمدًا الخضوع للفحوص البيومترية ويفضلون الأنظمة الاحتياطية التي من المحتمل أن تكون أقل قوة.

الشكل البيومتري – قد يعتمد القرار بانتقاء شكل أو أكثر من الأشكال البيومترية المعينة على عوامل مثل:

- إمكانية الوصول والأداء الوظيفي – يتمثل أحد قرارات الشراء الأساسية في إما استخدام وضع بيومتري واحد وإما استخدام منهج متعدد الأشكال البيومترية. ويجب أن يكون الشكل البيومتري أو الأشكال البيومترية المنتقاة مناسبة لمهام المقارنة المتعلقة بالتحقق (1:1) والمطابقة (1:كثير)، التي ستُستخدم فيها. وعادةً ما تكون الأنظمة ذات الشكل البيومتري الواحد أقل تكلفة في الشراء والتشغيل، ولكنها لا تستطيع تغطية كل فرد من السكان. فقد يكون هناك، على سبيل المثال، عدد كبير من الأشخاص غير القادرين على التسجيل في نظام بصمات الأصابع نظرًا إلى إصابتهم بعاهات مستديمة، أو فقدانهم لليدين والأصابع، أو تلف جلدهم بسبب المتطلبات المهنية، على سبيل المثال أولئك الذين يعملون باستخدام المواد الكيميائية، أو الذين يمتهنون أنواعًا معينة من الأعمال اليدوية، التي قد تؤدي إلى حجب مضلع الاحتكاك على سطح الأصابع واليدين، أو تشوُّهه، أو تدميره. وإذا كان التطبيق البيومتري يحتاج إلى تسجيل أكبر عدد ممكن من الأشخاص، فمن الأفضل استخدام نظام متعدد الأشكال (مثل بصمات الأصابع والحدقة) حيث سيكون قادرًا على التقاط السمات البيومترية من نسبة مئوية أعلى بكثير من عدد السكان المطلوب. ويجب اتخاذ قرار شراء مشابه فيما يتعلق بالأداء الوظيفي، على سبيل المثال هل من المُستصوَب شراء تطبيق بيومتري يغطي وظيفة واحدة فقط مثل نظام بصمات الأصابع الخاص بالسجلات الجنائية التابعة للشرطة أو هل يمكن منح الاستثمار قيمة مضافة من خلال إنشاء شبكة متعددة الوظائف، مثل السجلات الجنائية إضافةً إلى قواعد بيانات الجرائم، جنبًا إلى جنب مع تطبيقات إدارة الحدود في الوقت نفسه؟ بل إنه من الممكن توسيع الوظائف والأشكال البيومترية، إذا سمحت القوانين الوطنية بذلك، بحيث يدير أي بلد في النهاية نظامًا واحدًا للسمات البيومترية. وتتبنى بعض البلدان هذا المنهج متعدد الأشكال والوظائف، بحيث يمكن تحقيق الاستفادة من وفورات الحجم، ويمكن ترشيد أعداد الموظفين من خلال تجميع الوظائف المشابهة، وعليه، لا يلزم سوى هيكل واحد لإطار الحوكمة والإدارة للنظام الوطني.
- توافق الأشكال البيومترية والتحوُّط للمستقبل – من المسائل الأساسية، عند انتقاء الشكل البيومتري الأفضل لأي تطبيق متعلق بالإرهاب، احتمالية الحصول على مثل هذه البيانات ومشاركتها مع الشركاء الوطنيين أو الدوليين لتحديد الإرهابيين المحتملين. على سبيل المثال، قد تكون هناك شبكة إقليمية من البلدان، التي تشارك بيانات بصمات الأصابع المستمدة من جميع طالبي التأشيرات، الذين يدخلون عبر حدود بلدانهم المعنية. وهكذا، فإن أي بلد يرغب في المشاركة في هذه الشبكة والحصول على فوائدها، سيحتاج إلى استخدام بصمات الأصابع لنظام السمات البيومترية الخاص بطالبي التأشيرات، حتى في حال التوصية باستخدام شكل بيومتري آخر في بداية الأمر، لأسباب أخرى، في حالة العمل الأصلية. ولاستكمال هذا الأمر، يمكن النظر في أشكال بيومترية معينة، نظرًا إلى أنها تُعَد أيضًا سمات بيومترية شائعة الاستخدام في مسرح الجريمة وقد تسمح بالبحث الشامل لأغراض مكافحة الإرهاب. على سبيل المثال، قد يتم تفضيل الأشكال البيومترية لبصمات الأصابع والوجه على الأشكال البيومترية للحدقة أو أوردة اليد.
- التقاط البيانات وتسجيلها – على سبيل المثال هل من الأفضل أن يكون الشخص المَعنِي على اتصال بجهاز الالتقاط أو قريبًا منه أم أن الالتقاط عن بُعد يُعَد خيارًا أفضل لبيئة التشغيل؟
- القبول وقابلية التشغيل الإنتاجي – قد تخضع بعض الأشكال البيومترية لتصورات مسبقة من العميل، أو مخاوف حقيقية، أو حتى وصمة اجتماعية، على سبيل المثال غالبًا ما ترتبط بصمات الأصابع بالإجرام، نظرًا إلى إرثها التاريخي في مجال العمل الشُرَطي. وقد يتم تفضيل استخدام أشكال بيومترية معينة؛ لأنها تيسر إجراءات التقاط البيانات وتسجيلها على نحو أسرع وأسهل، وهو أمر غالبًا ما نضعه في الاعتبار فيما يتعلق بالتطبيقات التي تحتاج إلى التعامل مع عدد كبير من العملاء على أساس منتظم، مثل نقاط مراقبة الحدود.

2-5-2 إدارة الموارد

إن شراء تطبيق بيومتري رئيسي يعالج أحجامًا كبيرة، يتطلب تمويلًا رأسماليًّا كبيرًا لشراء الأجهزة والبرامج اللازمة، وإنشاء بيئات تشغيل مناسبة ومؤمنة، مثل مراكز التسجيل والتقاط البيانات، وغرف الخوادم، وأجنحة المُشغِّلين، وما إلى ذلك، وعلاوة على ذلك، قد تكون هناك تكاليف مرتبطة بتعيين الموظفين وتدريبهم، بالنسبة إلى بعض التطبيقات، وفي حال استخدام منهج قائم على المعايير، يجب الاعتماد على أساس متجدد.

بمجرد تثبيت النظام واكتمال اختبارات القبول بنجاح، يجب احتساب التمويل اللازم من أجل أعمال الصيانة الدورية وترقيات البرنامج لتحسين الأداء والأمان من آن إلى آخر، في إطار الميزانيات السنوية. ويُحتسب هذا التمويل إضافةً إلى نفقات الإيرادات السنوية الأساسية لرواتب الموظفين والتشغيل الروتيني والفعَّال للنظام. وعادةً ما يستلزم الأمر تشغيل الأنظمة البيومترية مدة 24 ساعة كل يوم على مدار العام وبأقل وقت تعطُّل للنظام.

إن أنشطة البحث والتطوير الحديثة ذات الدوافع التجارية في جميع أنحاء العالم في مجال التقنيات البيومترية تُقدم باستمرار إصدارات جديدة للبرامج وقدرات مُطوَّرة بمعدل سريع. وحيث إن العديد من الأنظمة البيومترية يعمل مدة عشرين عامًا أو أكثر، فإنه بحاجة إلى الكثير من ترقيات الأداء، حتى لا تصبح مُكرَّرة. وقد يصبح أي تطبيق بيومتري غير قادر على العمل على نحو مناسب أو يتعطل كليًّا، إذا لم تتم صيانته وترقيته بصفة منتظمة خلال دورة حياته[49].

تحتاج إجراءات الشراء والتخطيط أيضًا إلى مراعاة المتطلبات المستقبلية الأخرى مثل الحاجة إلى زيادة قوة المعالجة من أجل مواجهة الطلب المتزايد، الذي قد يستلزم بعد ذلك، زيادة سعة تخزين قاعدة البيانات بوصفها نتيجة مباشرة. وقد تكون هناك أيضًا حاجة تشغيلية إلى الاتصال والتشغيل المتبادل مع أنظمة أو قواعد بيانات أخرى. وسيتطلب أي من هذه التحسينات تمويلًا إضافيًا في المستقبل قد لا يكون متاحًا، في حال تخفيض الميزانيات لاحقًا أو في حال إعطاء المتطلبات الأخرى الأولوية. لذلك، فمن المُستصوَب تَوقُّع مثل هذه الميزات والمتطلبات في مرحلة التخطيط وتهيئة أكبر عدد ممكن من هذه العوامل في الأنظمة الجديدة. ويجب تصميم التطبيقات، بحيث تكون مُزوَّدة بسعة معالجة وسعة تخزين إضافية أو تقدير تكاليف مثل هذه الترقيات بالفعل والاتفاق عليها في عقود الشراء. ويمكن أيضًا دمج إمكانية الاتصال وقابلية التشغيل المتبادل مع الأنظمة الأخرى في أي نظام جديد، في حال النظر في قدرات الشبكة منذ البداية. ولا شك أن إنشاء مثل هذه الواجهات في مرحلة التصميم أقل تكلفة بكثير من تقديمها لاحقًا، حيث قد تؤدي عندئذٍ إلى تعطُّل الأداء التشغيلي وربما تتطلب تثبيت أو إعادة تكوين مكونات الاتصال والمسارات في كلٍّ من النظامَين/كل الأنظمة.

6-2 الممارسات الموصى بها

أ) ينبغي للدول اعتماد منهج قائم على مراعاة حقوق الإنسان في استخدام التقنية البيومترية لمكافحة الإرهاب، الذي يتضمن استخدام الاحتياطات الإجرائية والمراقبة الفعالة لتطبيقه. ويتضمن ذلك تأسيس هيئات رقابية مناسبة ومستقلة أو توسيع نطاق اختصاصات القائمة منها، للإشراف على تنفيذ تشريعات الخصوصية ذات الصلة وتقديم العلاجات الفعالة في حالة حدوث انتهاكات في هذا الصدد. ويتعين استكمال ذلك من خلال عملية استعراض أخلاقي، تقوم بإثراء جميع السياسات وعمليات صنع القرار على المستوى الوطني فيما يتعلق باستخدام الأنظمة البيومترية لأغراض مكافحة الإرهاب.

ب) يجب أن يتوافق تطبيق التقنية البيومترية لمكافحة الإرهاب الدولي والجرائم المرتبطة به مع الحقوق الأساسية لجميع الأفراد في الخصوصية والحماية القانونية لبياناتهم الشخصية، بما في ذلك السمات البيومترية.

ج) يمكن أن تكون الأنظمة البيومترية عُرضة للإخفاق والعديد من أشكال الهجوم المتعمد. لذلك تُنصَح الدول بإجراء تقييمات مخاطر منتظمة للعمليات الشاملة للتطبيقات البيومترية الخاصة بها من أجل التخفيف من التهديدات الحالية أو الجديدة.

د) يُوصَى بأن تقوم الدول بتشغيل جميع أنظمتها البيومترية بما يتوافق مع المعايير التقنية الدولية وأن تسعى للحصول على الاعتماد الرسمي لعمليات الأدلة الجنائية وإدارة الجودة لديها وفقًا للمعايير العلمية الدولية. ولن يوفر هذا أساسًا قويًّا للمعالجة البيومترية الفعالة فحسب، بل سيُطمئِن أيضًا الشركاء الدوليين الذين قد يرغبون في مشاركة البيانات البيومترية.

[49] من أجل هذه الأسباب، تفرض منظمة الطيران المدني الدولي استخدام الصور بدلًا من القوالب في جوازات السفر الإلكترونية. ويضمن هذا التحوُّط للمستقبل أن تظل الترقيات إلى خوارزميات المطابقة المُحسّنة خيارًا يمكن دمجه في نظام الفحص على الحدود بالاعتماد على السمات البيومترية (عادةً صور الوجه) التي يتم قراءتها من جوازات السفر الإلكترونية.

هـ) يتطلب شراء الأنظمة البيومترية تخطيطًا استراتيجيًّا طويل الأمد، يلبي كلًّا من الاحتياجات الحالية والمستقبلية من الموارد، لذلك ينبغي أن تفكر الدول في:

- الاستثمار الرأس مالي الأولي لاقتناء النظام واختباره
- النفقات السنوية المستدامة بشأن التوظيف وصيانة الأنظمة، إضافةً إلى ترقيات الأمان والأداء
- الميزانيات، وسعة قاعدة البيانات، وقوة المعالجة المطلوبة خلال دورة حياة النظام
- قابلية التشغيل المتبادل وإمكانية الاتصال المحتملة مع الشبكات الوطنية أو الدولية وتوافق الأشكال البيومترية
- موازنة المتطلبات التشغيلية الرئيسية لأي نظام بيومتري لمكافحة الإرهاب من حيث الأمان، وإمكانية وصول العملاء وسهولة الاستخدام، وأحجام الإنتاجية، وسرعة المعالجة.

1-6-2 الوثائق المرجعية

قرارات مجلس الأمن التابع للأمم المتحدة رقم 1373(لعام 2001)، و1624 (2005)، و2178 (2014)، و2195 (2014) و2396 (2017) وقرارا الجمعية العامة التابعة للأمم المتحدة A/RES/68/276 وA/70/L.55

منشور وكالة الحقوق الأساسية التابعة للاتحاد الأوروبي "تحت المراقبة - الأنظمة البيومترية، وأنظمة تكنولوجيا المعلومات الأوروبية، والحقوق الأساسية http://fra.europa.eu/en/publication/2018/biometrics-rights-protection

S/2015/975، الفقرة 8؛ S/2015/939، المبدأ 15 (e).

قرار مجلس حقوق الإنسان A/HRC/RES/34/7 (2017).

اللجنة المعنية بحقوق الإنسان، التعليق العام رقم 16: المادة 17 (الحق في الخصوصية)، الفقرة 3-4.

تقرير المقرر الخاص المعني بالحق في الخصوصية، A/HRC/31/64 (2016).

إعلان الأمم المتحدة العالمي لحقوق الإنسان والعهد الدولي للحقوق المدنية والسياسية، الديباجة. العهد الدولي للحقوق المدنية والسياسية، المادة 2(1)، و2(3)، و9، و14 و26.

اللجنة المعنية بحقوق الإنسان، التعليق العام رقم 16 (1988)، راجع:
http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=INT%2fCCPR%2fGEC%2f6624&Lang=en

قرار الجمعية العامة رقم 45/95 (1990) حول المبادئ التوجيهية لتنظيم استخدام ملفات البيانات الشخصية المحوسبة واللائحة العامة لحماية البيانات للاتحاد الأوروبي لعام 2018، المادة 51 (سلطة إشرافية).

تقرير المقرر الخاص المعني بالحق في الخصوصية، A/HRC/31/64 (2016).

إعلان الأمم المتحدة العالمي لحقوق الإنسان، الديباجة.

الموقع الشبكي لصندوق النقد الدولي حيث يتم سرد أدوات مكافحة غسيل الأموال وغيرها من أدوات مكافحة الاحتيال www.imf.org

المنظمة الدولية لتوحيد المقاييس http://www.iso.org

اللجنة الدولية للتقنيات الكهربائية http://www.iec.ch

اللجنة الأوروبية للتوحيد القياسي https://www.cen.eu

المعهد الوطني للمواصفات القياسية والتكنولوجيا (الولايات المتحدة الأمريكية) http://www.nist.gov

اللائحة العامة لحماية البيانات للاتحاد الأوروبي لعام 2018، المادة 7 (الموافقة)، والمادة 17 (حق محو البيانات)، والمادة 15 (حق الوصول إلى البيانات)

المادة 19 من العهد الدولي للحقوق المدنية والسياسية المتعلقة بحرية التعبير.

وثيقة مفوضية الأمم المتحدة لشؤون اللاجئين "مواجهة المخاوف الأمنية دون تقويض حماية اللاجئين" http://www.refworld.org/docid/5672aed34.html

إعلان الأمم المتحدة لحقوق الإنسان في المادة 9 (عدم جواز الاعتقال أو الحجز التعسفي) والمادة 10 (الحق في اعتبار كل شخص متَّهم بجريمة بريئًا إلى أن يثبت ارتكابه لها)

إعلان مدريد التابع للأمم المتحدة الصادر عن وزراء الخارجية في الاجتماع الخاص للجنة مكافحة الإرهاب التابعة لمجلس الأمن في (28) الثامن والعشرين من شهر تموز/يوليو لعام 2015.

الأنظمة البيومترية بالمملكة المتحدة وفريق الأخلاقيات الجنائية http://www.gov.uk/government/publications/biometrics-and-forensics-etchics-group

المبادئ التوجيهية للخصوصية البيومترية الصادرة عن معهد القياسات الحيوية، المخصصة للاستخدام الدولي www.biometricsinstitute.org

المعيار ISO/IEC 30107-2_2017: كشف هجوم العرض البيومتري. تنسيقات البيانات

[2] وكالة حرس الحدود وخفر السواحل الأوروبية، تقييم مواطن الضعف واختبار أنظمة مراقبة الحدود الآلية (Abc) (2017)

[3] تيد دانستون ونيل ياغير، النظام البيومتري وتحليل البيانات: التصميم والتقييم واستخراج البيانات (2008) شركة Springer.

المعيار ISO/IEC 27001:2013 تكنولوجيا المعلومات -- التقنيات الأمنية -- أنظمة إدارة أمن المعلومات – المتطلبات

المعيار ISO 31000:2009 إدارة المخاطر - المبادئ والتوجيهات

المعيار IEC 31010:2009 - إدارة المخاطر -- تقنيات تقييم المخاطر

المعهد الوطني للمواصفات القياسية والتكنولوجيا، المنشور الخاص 800-30 دليل إجراء تقييمات المخاطر

المعهد الوطني للمواصفات القياسية والتكنولوجيا، المنشور الخاص 800-37 الدليل المعني بتطبيق إطار إدارة المخاطر على أنظمة المعلومات الفيدرالية: نهج دورة الحياة الأمنية

المعيار ISO/IEC 17025:2017 المتطلبات العامة لكفاءة مختبرات الفحص والمعايرة

3- قواعد البيانات والأنظمة البيومترية لمكافحة الإرهاب

يقدم القسم 3 نظرة عامة عن قواعد البيانات والأنظمة البيومترية الحالية لمكافحة الإرهاب على مستوى مجموعة تطبيقات إنفاذ القانون وإدارة الحدود والتطبيقات العسكرية. كما يتناول كذلك المزايا الخاصة بمشاركة البيانات البيومترية على الصعيد ثنائي الأطراف، ومتعدد الأطراف، والإقليمي والعالمي، وكيف يمكن للبيانات البيومترية، عند استخدامها مع بيانات الاستخبارات الأخرى، أن تُستخدم بشكل استباقي لمنع الأعمال الإرهابية، إضافةً إلى دورها بصفتها أداة من أدوات التحقيق. ومن ثمَّ يتم النظر في الإجراءات التي اتخذتها السلطات نتيجة لحالات التطابق البيومتري، ضمن السياق المعني بحقوق الإنسان الدولية والحاجة إلى استجابة مستنيرة وقانونية ومتناسبة. ويغطي الجزء الأخير من القسم عملية تضمين الأنظمة البيومترية في استراتيجيات مكافحة الإرهاب الخاصة بالمناطق والدول الأعضاء والدور الأساسي لوكالات إنفاذ القانون وضبط الحدود في تقديم الدعم بفعالية إلى هذه الاستراتيجيات.

3-1- قواعد البيانات والأنظمة البيومترية الحالية لمكافحة الإرهاب

3-1-1- التطبيقات الخاصة بالحدود

إن الإدارة المتطورة على نحو متزايد للحدود[50] تضطلع بدور حاسم في مكافحة الإرهاب، بشكل عام، واعتراض سبيل المقاتلين الإرهابيين الأجانب بشكل خاص. وتحدد طريقة النقل، إلى حد كبير، الخصائص والنطاق لتشغيل نقاط العبور الحدودية (BCP). ففي حالة الرحلات الجوية الدولية، نجد أن نقاط العبور الحدودية قياسية وموحدة للغاية. أما بالنسبة إلى الرحلات البرية، والمائية، والبحرية، يوجد عادةً نوعان من نقاط العبور الحدودية، أحدهما لجميع المسافرين الدوليين والآخر يستخدمه حصرًا المواطنون من أيٍّ من جانبي الخط الفاصل. ولكي يتمكن المسافرون الدوليون من دخول أي دولة بشكل قانوني، يتعين عليهم إبلاغ نقطة العبور الحدوديةً الخاصة بها. وتقع نقاط العبور الحدودية للسكان المحليين، بشكل عام، على الحدود البرية أو الموانئ المحددة، التي تخدم دولتين أو أكثر من الدول القريبة. وغالبًا ما يتم تنفيذ نقاط العبور الحدودية المحلية هذه بالاقتران مع المناطق الاقتصادية، حيث يمتد الخط الحدودي بشكل عام لمسافة 25 كم داخل البلاد على كلا الجانبين ويكون مفتوحًا أمام المواطنين من جانبي الحدود. ولا يمكن للمسافرين الدوليين الآخرين استخدام نقاط العبور الحدودية المحلية هذه.

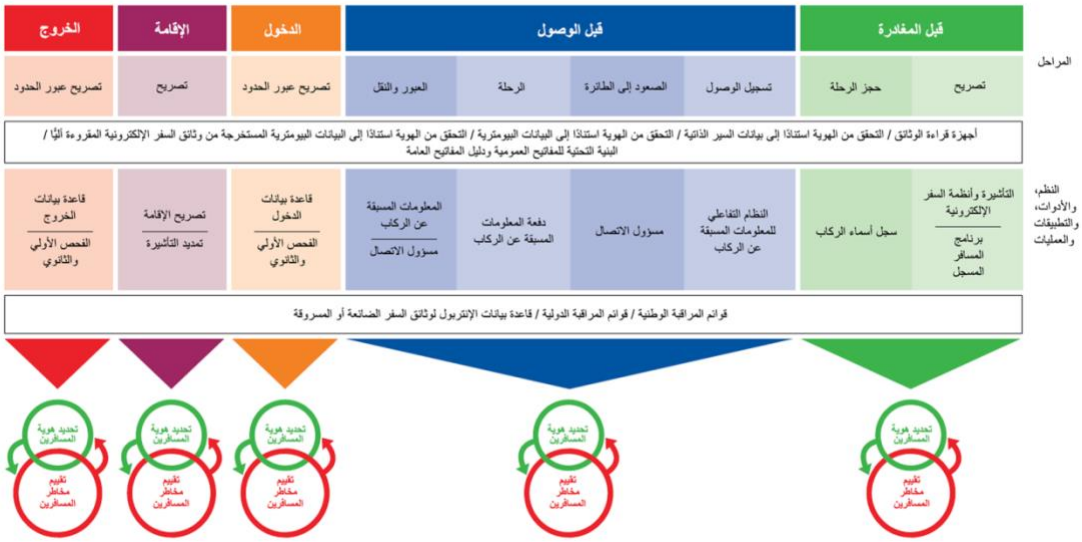
تعمل نقاط العبور الحدودية الواقعة على الحدود الدولية بمنزلة عامل تصفية فعال يمكن توسيعه أو تضييقه حسب مستوى التهديد. وبشكل عام، سيكون عامل التصفية عند مستوى "عادي" ولكن في أوقات التهديد المتزايد، سيتغير عامل التصفية إلى الرمز البرتقالي أو حتى الرمز الأحمر (أو مستويات التنبيه المكافئة) وفي بعض الحالات القصوى، سيتم إغلاق الحدود تمامًا. وفي الحالات التي قد يحتاج فيها عدد كبير من الأشخاص إلى دخول البلد بسرعة، مثل كارثة طبيعية أو كارثة من صنع الإنسان في بلد مجاور، يمكن فتح الحدود للسماح بسهولة العبور وسيتم إجراء الفحوص الرسمية المطلوبة لاحقًا بمجرد وصول الأشخاص إلى المناطق الآمنة عبر الحدود.

[50] "عادةً ما يُستخدَم مصطلح "الخط الفاصل" للإشارة إلى الخط الذي يقسم الفضاء الإقليمي أو البحري إلى دولتين، في حين أن مصطلح "حدود" يمثل ما يجب عبوره لدخول دولة ما. وفي بعض الأحيان يتطابق المصطلحان في المعنى تمامًا، ولكن الأكثر شيوعًا في الحدود هو أن تشتمل على بنية تحتية، مثل نقاط التفتيش الحدودية، والمرافق الجمركية، والسياج، وطرق الدوريات، التي تمتد إلى ما وراء الخط الفاصل؛ وفي حالة الموانئ الجوية والبحرية الدولية، يمكن أن تقع الحدود على بُعد مئات الكيلومترات من الخط الفاصل. وأي خط فاصل في الأساس هو خط للتحديد، في حين أن الحدود عادةً ما تكون كيانًا أكثر تعقيدًا، يتكون من عدة خطوط و / أو مناطق، تتمثل وظيفتها الأساسية في تنظيم حركة الأشخاص والبضائع." *الأستاذ الدكتور مارتن برات من جامعة دورهام في المملكة المتحدة*

تتولى الوكالات المسؤولة عن الهجرة، ومراقبة الدخول والأمن، وإنفاذ القانون، والجمارك، والحجر الصحي عمليات التصريح بعبور الحدود للمسافرين والتخليص الجمركي للبضائع. حيث تتطلب الوكالات الحدودية بيئة تشغيل فعالة مزودة بموظفين مدربين تدريبًا جيدًا ومتحمسين، وتقنيات متطورة، ومعلومات مُحدَّثة. وتمثل إضافة التطبيقات البيومترية، التي تساعد بشكل كبير في عمليات إدارة الحدود، أحد العناصر المهمة في نقاط العبور الحدودية الحديثة. فهي تشكل جزءًا من منهج تقني أوسع نطاقًا، يشمل جميع جوانب السفر عبر الحدود بداية من النقطة التي يتم فيها تنظيم السفر لأول مرة حتى الوصول والمغادرة النهائية للزائر. ويتم تجميع المعلومات المُجمعة من كل مرحلة من مراحل هذه العملية من مصادر مختلفة وتقديمها إلى مسؤول الحدود، الذي يستخدمها، مع معلومات أخرى، لتحديد ما إذا كان سيُسمَح للمسافر بدخول البلد.

إن مجال السفر الجوي الدولي هو الأكثر تطورًا، والذي دفع - فيما مضى - عجلة الابتكار التكنولوجي القائم على المعايير، والذي تم تطبيقه بعد ذلك على الحدود البرية والبحرية. ومن المُرجَّح أن يستمر هذا النمط طويل الأمد في الاستخدام الناشئ للأنظمة البيومترية لتحديد هوية الإرهابيين. كما أن الهيكل الحديث لعملية التصريح بعبور الحدود فيما يخص السفر الجوي الدولي يتيح إمكانية تكرار تحديد هوية المسافر وتقييم المخاطر خلال رحلة المسافر، نظرًا إلى توفر معلومات إضافية إلى دولة المقصد أو دولة المغادرة. وتكون المصادر الرئيسية للبيانات المتعلقة بالمسافرين في مجال السفر الجوي الدولي هي شركات الطيران والحكومات، وتستخدم الحلول الجديدة لتطبيق الأنظمة البيومترية مصدرَي البيانات أنفسهما.

الشكل 4 – المراحل الخمس لمسار السفر[51]
(بإذن من الإيكاو)



من منظور دول المقصد، يتم تقسيم العملية الشاملة إلى خمس مراحل (انظر الشكل 4):

[51] راجع دليل إدارة مراقبة الحدود لبرنامج تحديد هوية الركاب التابع لمنظمة الطيران المدني الدولي (الإيكاو)، مونتريال (2018) للاطلاع على المزيد من التفاصيل.

1- قبل المغادرة
2- قبل الوصول
3- الدخول
4- الإقامة
5- الخروج

في حين أن السفر، من منظور المنظومة الشاملة والمنظور الدولي، يمثل مسارًا متصلًا، حيث إن معالجة الخروج من الدولة التي يبدأ عندها السفر، تُعَد المعالجة السابقة للوصول لدول العبور والمقصد لذلك السفر.

المرحلة 1: قبل المغادرة

في الوقت الراهن، يتطلب العديد من الدول معلومات مسبقة من جميع المسافرين قبل وصولهم إلى الحدود. وتتكون هذه المعلومات في الأساس من بيانات السيرة الذاتية، والوثائق، وبيانات السفر. وعلى نحو متزايد، تطلب الدول أيضًا بيانات بيومترية لتمكينها من تأكيد هوية الرعايا الأجانب الوافدين. وفيما سبق، كان من الممكن تقسيم هؤلاء المسافرين إلى مجموعتين، وهما من يحتاج إلى تأشيرة لدخول البلاد ومن لا يحتاج إليها. ومنذ تسعينيات القرن الماضي، أصبحت بيانات نظام مراقبة المغادرة لشركات الطيران متاحة للدول في صورة نظام المعلومات المسبقة عن الركاب والنظام التفاعلي للمعلومات المسبقة عن الركاب. وتجمع الدول - في الوقت الحالي - معلومات عن المسافرين قبل السفر عبر مجموعة من الآليات. ويتم استخدام العمليات والأنظمة الآتية حاليًا لجمع المعلومات الضرورية قبل الوصول:

1-أ- طلب الحصول على التأشيرة "الكلاسيكية" - شرط عادي في العديد من البلدان، يعتمد على عوامل تاريخية، ودبلوماسية، واقتصادية، إضافةً إلى العلاقات السياسية للدولة. وتنطوي هذه العملية عادةً على أن يقوم مقدم الطلب بتقديم سمات تحديد الهوية من نوع السير الذاتية والبيومترية عبر عملية تقديم شاملة، تتضمن تقديم وثائق السفر ورسومًا إلى المركز الدبلوماسي لبلد الوجهة أو مَنْ يمثله. وقد تكون السمات البيومترية صورة وجه، أو تسجيلًا، مثل مجموعة من بصمات الأصابع. وسيتم بعد ذلك التحقق من الطلب وإصدار تأشيرة أو رفضها. وقد يتضمن الفحص الذي يسبق إصدار التأشيرة عملية بحث 1:كثير في قائمة مراقبة بيومترية خاصة بالدول التي قامت بتجميع قواعد بيانات لهذا الغرض.

1-ب- طلب الحصول على التأشيرة الإقليمية - التعاون الإقليمي بين البلدان أمر شائع وتمتلك كل قارة كيانًا إقليميًّا واحدًا على الأقل على سبيل المثال، جنوب شرق آسيا - رابطة أمم جنوب شرق آسيا[52]، وغرب أفريقيا - الجماعة الاقتصادية لدول غرب أفريقيا[53]، وأوروبا - الاتحاد الأوروبي، وأمريكا الجنوبية – اتحاد أمم أمريكا الجنوبية[54]، ومنطقة البحر الكاريبي - الجماعة الكاريبية[55]. ويختلف مستوى التعاون بين هذه الكيانات. ومن الأمثلة على النظام الإقليمي هذا، الاتحاد الأوروبي الذي اعتمد لائحة تتطلب من كل دولة من الدول الأعضاء تطبيق نظام المعلومات عن التأشيرات (VIS) الخاص بها. وترتبط هذه الأنظمة بمحور نظام المعلومات عن التأشيرات المركزي الذي تديره الوكالة الأوروبية للإدارة التشغيلية لأنظمة تكنولوجيا المعلومات واسعة النطاق (eu-LISA). ويستخدم نظام المعلومات عن التأشيرات الفحوص البيومترية على هيئة صورة وجه ومجموعة من بصمات الأصابع العشرة للتحقق من هوية المسافر عند الحدود، إضافةً إلى فحص السير الذاتية من خلال الجيل الثاني من نظام شنغن للمعلومات (SIS-II)[56] وقواعد البيانات الوطنية. وتتيح بنية هذه الأنظمة الإقليمية إمكانية دمج الفحص قبل الإصدار، الذي يتضمن عملية بحث 1:كثير في قائمة مراقبة بيومترية للدول والمناطق، التي قامت بتجميع قواعد بيانات لهذا الغرض.

---

[52] ASEAN رابطة أمم جنوب شرق آسيا

[53] ECOWAS الجماعة الاقتصادية لدول غرب أفريقيا

[54] UNASUR اتحاد أمم أمريكا الجنوبية

[55] CARICOM الجماعة الكاريبية

[56] يدعم الجيل الثاني من نظام شنغن للمعلومات في الاتحاد الأوروبي التعاون بين وكالات الأمن العام، ومراقبة الحدود، وإنفاذ القانون في أوروبا فيما بين الدول المُوقِّعة على معاهدة شنغن. حيث تتم مشاركة المعلومات من قواعد بيانات الشرطة وقوائم مراقبة الحدود بين الدول. ويمكن الوصول إلى هذه المعلومات داخل البلد وعند الحدود على حدٍّ سواء، كما يتم استخدامها للتحقق من المسافرين من الاتحاد الأوروبي وإليه. ويتضمن النظام بيانات عن الأشخاص المطلوبين والمفقودين، ووثائق الهوية/السفر الضائعة أو المسروقة، والسمات البيومترية، والمركبات المسروقة، وما إلى ذلك.

1 -ج- الطلب بالاستعانة بمصادر خارجية إن هذا النموذج الذي يصبح شائعًا على نحو متزايد في العديد من الدول، يستخدم مقدمي الخدمات التجاريين لجمع كل الوثائق والمعلومات لمقدم الطلب وترتيبها اللازمة لعملية طلب الحصول على التأشيرة. وقد تسجل العملية أيضًا السمات البيومترية من جانب مقدم الطلب (صورة الوجه، و/أو مسح حدقة العين، و/أو بصمات الأصابع). ويتم توجيه الطلب الكامل إلى المركز الدبلوماسي المناسب لإجراء الفحوص اللازمة وتحديد ما إذا كان سيتم إصدار تأشيرة. وقد يتضمن الفحص الذي يسبق إصدار التأشيرة إحالة صورة أو قالب بيومتري إلى الدولة لإجراء عملية بحث 1:كثير في قائمة مراقبة بيومترية خاصة بالدول التي قامت بتجميع قواعد بيانات لهذا الغرض.

1 -د- طلب الحصول على التأشيرة الإلكترونية/عبر الإنترنت تتم عملية التقديم عبر الإنترنت بالكامل من خلال نماذج إلكترونية وصور ممسوحة ضوئيًا للصورة الفوتوغرافية لمقدم الطلب (متوافقة مع منظمة الإيكاو) وصفحة السيرة الذاتية لجواز السفر. وتتم عملية اتخاذ القرار وأي عملية فحص بيومتري على نحو مركزي. وفي حال إصدار التأشيرة، فسيتلقى مقدم الطلب تأكيدًا وسيتم إجراء الفحص من خلال نظام التحقق البيومتري 1:1 عند الحدود، من خلال مقارنة وجه مقدم الطلب بالصورة الفوتوغرافية المُقدمة للتأكد من أن مقدم الطلب والمسافر هما الشخص نفسه. وقد يتضمن الفحص الذي يسبق إصدار التأشيرة عملية بحث 1:كثير في قائمة مراقبة بيومترية خاصة بالدول التي قامت بتجميع قواعد بيانات لهذا الغرض.

1 -هـ- أنظمة السفر الإلكترونية تجمع هذه العملية بيانات الهوية الأساسية من المسافرين بغض النظر عن متطلبات التأشيرة. وتشبه هذه العملية في خطوات عملها عملية طلب الحصول على التأشيرة الإلكترونية/عبر الإنترنت، ولكن يتم الحصول على السمات البيومترية، بخلاف صورة الوجه، عند الحدود بدلًا من مرحلة قبل المغادرة.

والمصدر الرئيسي الآخر لبيانات المسافرين، قبل بدء السفر، هو ما تقوم شركات الطيران بتجميعه:[57]

1 -و- نظام سجل أسماء الركاب بعد حصول المسافر على تأشيرة/تصريح سفر، تكون المرحلة التالية هي حجز رحلة جوية من خلال استكمال المعلومات الخاصة بسجل أسماء الركاب عبر الإنترنت. ويتم تخزين بيانات سجل أسماء الركاب في نظام الحجز بالكمبيوتر (CRS) الخاص بشركات الطيران، لاستخدامها التجاري والتشغيلي الخاص، ولكن يتم إتاحتها أيضًا للوكالات الحدودية قبل مغادرة المسافر. وقد وضعت منظمة الجمارك العالمية، بالتعاون مع اتحاد النقل الجوي الدولي ومنظمة الإيكاو، معايير تقنية (النموذج الموحد لنقل البيانات)[58] وحافظت عليها من أجل التبادل المنسق لبيانات سجل أسماء الركاب بين العاملين بشركات الطيران والحكومات. *لا توجد بيانات بيومترية واردة ضمن سجل أسماء الركاب.* وتكمن قيمة بيانات سجل أسماء الركاب في أنها توفر معلومات سياقية مهمة، لتحسين عملية تأكيد الهوية وإثراء عملية استهداف مواطن الخطر للمسافرين المعنيين.

[57] بالنسبة إلى سجل أسماء الركاب والمعلومات المسبقة عن الركاب، فقد جمع الملحق 9، للإصدار الخامس عشر من اتفاقية شيكاغو، المعايير والممارسات الموصى بها، في الفصل 9 "نظام تبادل بيانات الركاب". وقد تم تطوير الرسائل الإلكترونية القياسية، بما في ذلك مجموعات البيانات والموافقة عليها على نحو مشترك من جانب منظمة الجمارك العالمية/اتحاد النقل الجوي الدولي/منظمة الطيران المدني الدولي في المبادئ التوجيهية بشأن سجل أسماء الركاب (الوثيقة رقم 9944) ونظام المعلومات المسبقة عن الركاب.

[58] دليل تنفيذ رسائل النموذج الموحد لنقل البيانات (PNRGOV) القائمة على قواعد الأمم المتحدة للتبادل الإلكتروني للبيانات لأغراض الإدارة والتجارة والنقل (EDIFACT) ولغة الترميز الموسعة (XML): www.wcoomd.org/en/topics/facilitation/instrument-and-tools/tools/api-pnr.aspx

المرحلة 2: قبل الوصول

2-أ- يتم إنشاء نظام *المعلومات المسبقة عن الركاب* في أنظمة مراقبة المغادرة بشركات الطيران. حيث يتم تجميع المعلومات المسبقة عن الركاب تدريجيًّا عند تسجيل الوصول، ولكن لا يتم إرسالها إلا للوكالات الحكومية لبلد المقصد بعد أن يقوم جميع المسافرين بتسجيل الوصول، والصعود على متن الطائرة، وإغلاق أبواب الطائرة. والأهم من ذلك، يتم استكمال المعلومات المسبقة عن الركاب عند محطات العبور المخصصة لمواصلة الرحلات الجوية الطويلة. ويستخدم نظام المعلومات المسبقة عن الركاب مصدرين للبيانات (1) المعلومات من المنطقة القابلة للقراءة آليًّا بجواز سفر المسافر و(2) تفاصيل الرحلة الجوية ومعلومات تسجيل الوصول، وقد يتضمن ذلك عناصر البيانات القياسية والإضافية على حدٍ سواء مثل الأمتعة المسجلة، وأرقام المقاعد، وعدد الركاب المسافرين، ورقم الرحلة، والتاريخ والوقت والموقع للمغادرة والوصول. ويتيح ذلك للوكالة المستقبِلة إجراء فحص مسبق لجميع الركاب قبل الوصول. إن المعيار المعمول به حاليًا لنقل بيانات نظام المعلومات المسبقة عن الركاب *لم يتضمن بيانات بيومترية، على الرغم من أنه قد يُتاح في المستقبل إمكانية جمع الصورة المتوافقة مع منظمة الإيكاو من الشريحة غير التلامسية من جواز السفر/وثيقة السفر. وسيتطلب ذلك تركيب قارئ لجوازات السفر الإلكترونية عند مكاتب تسجيل الوصول أو المحطات الطرفية، ولا تمتلك جميع البلدان هذه التقنية حاليًا.*

2-ب- النظام التفاعلي للمعلومات المسبقة عن الركاب يمثل هذا النظام نسخة مُحسَّنة من نظام المعلومات المسبقة عن الركاب، نظرًا إلى أنه يعيد توجيه معلومات المسافر إلى وكالة الاستقبال المحددة في وقت تسجيل الوصول الإلكتروني. ويتم إرسالها على نحو فردي وليس دفعة واحدة، كما هو الحال في عملية نظام المعلومات المسبقة عن الركاب. وتسمح عملية النظام التفاعلي للمعلومات المسبقة عن الركاب بإكمال قائمة المراقبة وغيرها من الفحوص قبل صعود المسافر على متن الطائرة، وبناءً على ذلك، توفر مستوى إضافيًّا من الحماية لشركة الطيران، وركابها، وبلد المقصد. *وستكون العناصر البيومترية مشابهة لنظام المعلومات المسبقة عن الركاب في الفقرة 2 أ أعلاه.*

دراسة الحالة 5 – الدخول دون إبراز وثيقة سفر

يجري النظر في مخطط لاستخدام الجيل التالي من نظام بوابات مراقبة الحدود الآلية (ABC) للسفر بين أستراليا ونيوزيلندا. وسيكون من شأنه تعزيز الأنظمة التفاعلية للمعلومات المسبقة عن الركاب القائمة وربط صور الوجه المتاحة من قواعد بيانات التأشيرات وجوازات السفر، لإنشاء قاعدة بيانات ديناميكية للوصول المتوقع لكل مسافر على رحلات الطيران القادمة. وفي هذا التطبيق، يظل جواز السفر الإلكتروني في جيب المسافر وتقارن بوابات مراقبة الحدود الآلية البيومترية صورة وجه المسافر بصورة من قاعدة بيانات الوصول المتوقع، مما يسمح بالدخول فقط في حال تطابق الصورتين. والحل الذي يتم تطويره هو تطبيق للمطابقة البيومترية 1:كثير ذو نطاق صغير.

ويستكمل عدد من الدول عملية فحص قبل الوصول الخاصة بها من خلال موظفي الاتصال، والمسؤولين الحكوميين من دول المقصد، الذين يعملون بالتعاون مع شركات الطيران عند الإقلاع ومطارات العبور للمساعدة على تحديد هوية المسافرين وتقييم المخاطر.

المرحلة 3: الدخول

لا يمكن للراكب السفر إلا بعد اكتمال جميع بروتوكولات قبل الوصول بنجاح. ومع ذلك، بالنسبة إلى معظم الولايات القضائية، فإن إكمال عمليات المرحلة 1 قبل المغادرة وعمليات المرحلة 2 قبل الوصول، لا يضمن الدخول إلى البلد عند الوصول. حيث يتخذ موظف الحدود القرار النهائي عندما يقدم المسافر الوثائق وبيانات الاعتماد اللازمة عند الوصول. ويجب على موظف الهجرة أن يبني قراره على عدد من العوامل، وقد تم تطوير أنظمة معلومات إدارة الحدود للمساعدة على هذه العملية. وتجدر الإشارة مع ذلك، إلى أن بعض نقاط العبور الحدودية الدولية، لا تتمتع بإمكانية الاستفادة من تقنية أنظمة معلومات إدارة الحدود حتى الآن. وتتباين أنظمة معلومات إدارة الحدود إلى حد كبير من حيث تطور وظائفها. ففي الولايات القضائية الأكثر تطورًا، تتزايد عمليات التحقق البيومترية من الهوية. بينما يصبح تطبيق قوائم المراقبة البيومترية أقل شيوعًا. وفيما يلي المتغيرات الرئيسية:

3-أ نظام معلومات إدارة الحدود القياسي تتحكم القوانين والتشريعات الوطنية في عدد الفحوص التي يتم إجراؤها على الحدود وأنواعها، على سبيل المثال ما إذا كان سيتم تسجيل بيانات جميع المسافرين، الذين يدخلون بلدًا أو إجراء عمليات بحث فحسب في قوائم المراقبة أو الجزاءات. وتتطلب تلك البلدان، التي تسجل جميع عمليات وصول المسافرين، شكلًا من أشكال نظام معلومات إدارة الحدود. وقد يتم تسجيل البيانات يدويًا، إلا أن معظم الأنظمة الحديثة تستخدم قارئ جواز السفر لتحميل البيانات من المنطقة القابلة للقراءة آليًّا لوثيقة السفر، وسيُدخِل مسؤول الحدود معلومات إضافية تتعلق بالهوية، وطول مدة الزيارة، وسببها، والعنوان في البلد، وما إلى ذلك. ومن ثمَّ يتم البحث عن البيانات في قوائم المراقبة. ولا يلتقط نظام معلومات إدارة الحدود *القياسي البيانات البيومترية للتحقق الآلي*.

3-ب- نظام معلومات إدارة الحدود الإلكترونية (e-BMS) يستخدم نظام معلومات إدارة الحدود الإلكترونية قارئ جواز السفر الإلكتروني للوصول إلى الشريحة غير التلامسية المُضمنة في وثيقة السفر الإلكترونية المقروءة آليًّا (eMRTD)[59]. وتتضمن هذه الشريحة بيانات المنطقة القابلة للقراءة آليًّا، إضافةً إلى صورة رقمية للوجه وفي كثير من الأحيان بصمتا أصابع أيضًا بما يتوافق مع معايير منظمة الإيكاو. وفي بعض البلدان، لا يمكن الوصول إلى بصمات الأصابع هذه إلا لأغراض التحقق، في حال تضمَّن نظام معلومات إدارة الحدود الإلكترونية شهادة رقمية من البلد المنشأ، تسمح بفتح مجموعة البيانات المحتوية على بصمات الأصابع. ومن أجل التحقق من الهويات من خلال السمات البيومترية المتضمَّنة في الشريحة، يجب توصيل أحد أنظمة معلومات إدارة الحدود الإلكترونية بالنظام البيومتري، وأن يكون قادرًا على التقاط السمات البيومترية من المسافرين باستخدام كاميرا للوجه أو كاميرا بالأشعة تحت الحمراء للحدقة أو ماسح ضوئي لبصمات الأصابع لمقارنتها مع البيانات الموجودة على الشريحة. ويدعم نظام معلومات إدارة الحدود الإلكترونية إجراء الفحوص 1:1 للتحقق البيومتري من الهوية باستخدام الصور ذات الملامح البيومترية المقروءة من جواز السفر الإلكتروني. وقد يتضمن نظام معلومات إدارة الحدود الإلكترونية عملية بحث 1:كثير في قائمة مراقبة بيومترية خاصة بالدول التي قامت بتجميع قواعد بيانات لهذا الغرض.

قد يعتمد الإرهابيون على وثائق سفر زائفة للسفر عبر الحدود دون اكتشاف هويتهم. حيث تختلف الأساليب المستخدمة بين استخدام صورة فوتوغرافية بديلة أو استخدام جواز سفر لشخص بمظهر مشابه، وحتى إنشاء نسخة مزيفة من الوثيقة الكاملة. وهكذا، فإن قارئ جواز السفر الإلكتروني المستقل، والمرتبط بنظام بيومتري متكامل، يمثل أداة ثمينة لفحص الوثائق في مجال مكافحة تزييف جوازات السفر، لا سيَّما عند نقاط العبور الحدودية، التي تفتقر إلى الموارد الكافية للتصدي لهذا النوع من الاحتيال. ويمكن أن يساعد - على نحو كبير - تركيب هذه المعدات في المرافق الثانوية مسؤولي الحدود على التحقيق مع هؤلاء المسافرين، الذين أثارت وثائقهم الشكوك في بداية الأمر عند نقاط العبور الحدودية.

دراسة الحالة 6 – بنية البيانات المنطقية النسخة 2

تمثل النسخة 2 من بنية البيانات المنطقية (LDS) تطورًا جديدًا، قد يسمح بسهولة الوصول إلى السمات البيومترية الإضافية المخزنة في جوازات السفر الإلكترونية. حيث يتم تخزين بنية البيانات المنطقية على شريحة غير تلامسية لجواز السفر الإلكتروني أو وثيقة السفر ويمكن مقارنتها مع "خزانة" تحتوي على 16 درجًا تسمى مجموعات البيانات. وتكون بعض المعلومات المخزنة إلزامية، بينما يكون إدراج معلومات أخرى أمرًا اختياريًّا ويخضع للسلطة التقديرية لكل بلد. ويتعين أن تكون مجموعات البيانات متوافقة مع معايير منظمة الإيكاو – هيكل البنية التحتية للمفاتيح العمومية[60]. ويضمن تحقيق ذلك، أنه قد تم إصدار البيانات الواردة في بنية البيانات المنطقية من جانب سلطة حقيقية ولم يتم تعديلها أو إلغاؤها. وتضيف النسخة 2 من بنية البيانات المنطقية ثلاثة عناصر أخرى إلى هيكل بنية البيانات المنطقية، تتمثل في (1) سجلات السفر وطوابع الدخول والخروج، و(2) سجلات التأشيرات، و(3) السمات البيومترية الإضافية. ويمكن تخزين النسخة 2 من بنية البيانات المنطقية على شريحة غير تلامسية لجواز السفر الإلكتروني، وفقًا لتقدير سلطة الإصدار عند إصدار جوازات سفر إلكترونية جديدة.
هذا يعني أنه يمكن لسلطات مراقبة الحدود والتأشيرات الآن كتابة المعلومات المتعلقة بمجموعات البيانات الثلاث الجديدة، على الشريحة غير التلامسية لبلد آخر. ويمكن عندئذٍ أن تقوم وكالة مراقبة الحدود بتخزين سجلات السفر، وختم جواز السفر على نحو إلكتروني، كما يمكن للسلطات المخصصة إدخال بيانات التأشيرة مباشرة في مجموعة البيانات، ويمكن التحقق من ذلك على نحو إلكتروني عند الوصول إلى أي حدود. ويمكن تخزين القوالب البيومترية ذات الصلة في جوازات السفر الإلكترونية الخاصة بالمسافرين المسجلين في برامج السفر المسجلة، لاستخدامها في بوابات مراقبة الحدود الآلية في البلدان المشاركة.

[59] وثيقة السفر الإلكترونية المقروءة آليًّا - عبارة عن وثيقة سفر مقروءة آليًّا (جواز سفر أو بطاقة) تنطوي على دائرة متكاملة غير تلامسية وتتميز بالقدرة على استخدامها للمطابقة البيومترية لحامل وثيقة السفر المقروءة آليًّا، وفقًا للمعايير المحددة في الجزء ذي الصلة من الوثيقة رقم 9303 الصادرة عن منظمة الإيكاو – وثائق السفر المقروءة آليًّا

[60] تُعرّف منظمة الإيكاو البنية التحتية للمفاتيح العمومية (PKI) بأنها مجموعة من السياسات، والعمليات، والتقنيات المستخدمة للتحقق من مستخدمي أحد التطبيقات الأمنية، وتسجيلهم، واعتمادهم. حيث تستخدم البنية التحتية للمفاتيح العمومية نظام تشفير بالمفتاح العمومي وممارسات التصديق الرئيسية لتأمين الاتصالات.

ملاحظة سيكون الشرط القانوني لكتابة بيانات جديدة على الشريحة غير التلامسية، هو تبادل شهادات البنية التحتية للمفاتيح العمومية لمنظمة الإيكاو بين سلطة إصدار جواز السفر الإلكتروني والبلد الذي يرغب في إضافة البيانات. لا يمكن استخدام النسخة 2 من بنية البيانات المنطقية، ما لم يتم استيفاء هذا الشرط القانوني.

3-ج- نظام معلومات إدارة الحدود الإلكترونية والسمات البيومترية (*e-2BMS*) يُعَد هذا النظام مشابهًا لنظام معلومات إدارة الحدود الإلكترونية، إلا أنه لا يستخدم قارئ جواز السفر الإلكتروني، نظرًا إلى أن السمات البيومترية مسجلة على الحدود، وعبر نظام التأشيرة. وتتمثل ميزة هذا النظام في امتلاك بلد المقصد للعملية البيومترية بأكملها، وذلك يتيح للمسؤولين مراقبة جودة التسجيلات، للحصول على المستوى الأقصى من الأداء في نظام المطابقة باستخدام التحقق البيومتري 1:1. على سبيل المثال، إن تبني الولايات المتحدة لهذا الهيكل يتيح دمج فحوص قوائم المراقبة البيومترية 1:كثير مقابل سجلات قائمة المراقبة الشاملة، التي قامت حكومة الولايات المتحدة بتجميعها لكل حاملي جوازات السفر الأجنبية الوافدين.

3-د- نظام مراقبة الحدود الآلية - أدت الزيادة المتسارعة في أعداد الركاب الدوليين خلال العقود الأخيرة إلى دفع عجلة الابتكار التقني والأتمتة على مستوى الحدود. ومنذ ظهور أول نظام لمراقبة الحدود الآلية في مطار شيفول بهولندا، انتشرت أنظمة مراقبة الحدود الآلية في جميع أنحاء العالم، وتُستخدم الآن على نحو منتظم في العديد من البلدان. وتستخدم الإصدارات الحديثة للنظام مستشعرات عالية السرعة وسمات بيومترية مُخزَّنة في شريحة وثائق السفر الإلكترونية مثل: الوجه، وحدقة العين، وبصمات الأصابع لإكمال عملية التحقق البيومتري 1:1 لتسهيل الدخول التلقائي عبر بوابات الحدود. ويسمح ذلك للجنسيات أو المجموعات ذات الأولوية المؤهلة مسبقًا بالتحرك بسرعة عبر نقاط العبور الحدودية بكميات كبيرة مع أدنى حد من التأخير ويتيح لمسؤولي الحدود إمكانية التركيز على المسافرين الآخرين، الذين قد يحتاجون إلى فحص دقيق. وتقرر السلطات الوطنية أو الإقليمية الجنسيات أو المجموعات، التي يجوز لها استخدام بوابات مراقبة الحدود الآلية الخاصة بها، وفي أي وقت، بناءً على تقييمات المخاطر الحالية والتشريعات المرتبطة بها. وقد تتضمن الحلول الخاصة بمراقبة الحدود الآلية عملية بحث 1:كثير في قائمة مراقبة بيومترية خاصة بالدول التي قامت بتجميع قواعد بيانات لهذا الغرض.

المرحلة 4: الإقامة

تتحمل كل بلد مسؤولية إدارة غير المواطنين ممن يتفضلون بالزيارة فترة وجيزة، أو البقاء فترة أطول، أو الإقامة داخل حدودها. قد تقع هذه المهمة على عاتق مختلف السلطات والوكالات، بناءً على القوانين واللوائح المحلية، ولكن ستكون الأدوار متشابهة، على سبيل المثال، إصدار تصاريح الإقامة والطلاب، ومعالجة مطالبات اللاجئين واللجوء، وطلبات التجنس، إضافةً إلى مهام إنفاذ القانون مثل التعامل مع الأشخاص الذين تجاوزوا فترة الإقامة بشكل غير قانوني، والاتجار بالبشر، وجرائم استغلال العمالة، وما إلى ذلك.

وخير مثال على ذلك على المستوى الإقليمي هو أنظمة الاتحاد الأوروبي الخاصة بالتأشيرات (eu-VIS) والجيل الثاني من نظام شنغن للمعلومات (eu-SIS-II) المذكورة في المرحلة 1-ب أعلاه. تسمح قواعد البيانات هذه لجميع السلطات المختصة في بلدان الاتحاد الأوروبي بإدارة المواطنين الأجانب داخل حدود كلٍ منها. إضافةً إلى ذلك، يوجد النظام الأوروبي لمضاهاة بصمات الأصابع (يوروداك) الذي يُعد قاعدة بيانات مركزية تابعة للاتحاد الأوروبي تقوم بجمع بصمات الأصابع الرقمية لملتمسي اللجوء ومعالجتها. ويستخدمه حاليًا 28 بلدًا أوروبيًّا، إضافةً إلى النرويج، وآيسلندا، وسويسرا، وليختنشتاين. يقوم نظام يوروداك بعملية المعالجة و/أو التخزين و/أو المقارنة لبصمات الأصابع الخاصة برعايا البلدان غير الأوروبية أو الأشخاص عديمي الجنسية الذين لا تقل أعمارهم عن 14 عامًا والذين (1) تقدموا بطلب للحصول على اللجوء في أي بلد مشاركة في نظام يوروداك، أو (2) الذين أُلقي القبض عليهم فيما يتعلق بعمليات عبور الحدود بصفة غير نظامية، أو (3) الذين تم اكتشاف وجودهم بصفة غير قانونية داخل أحد بلدان نظام يوروداك. كما يلعب نظام يوروداك أيضًا دورًا مهمًّا في سبيل تنفيذ لائحة دبلن. يعمل ذلك على تنظيم طلبات ملتمسي اللجوء وتم تصميمه لمنع تقديم طلبات اللجوء المتعددة في مختلف بلدان الاتحاد الأوروبي. ويتمثل الغرض الرئيسي من اللائحة في إسناد المسؤولية عن معالجة طلبات اللجوء إلى دولة واحدة من الدول الأعضاء، وتكون في أغلب الأحيان البلد الذي دخل عبره ملتمس اللجوء أولًا إلى الاتحاد الأوروبي لإجراء المعالجة اللاحقة. منذ تموز/يوليو 2015، كانت سلطات إنفاذ القانون تتمتع بإمكانيات محدودة لاستخدام نظام يوروداك، في ظل ظروف صارمة للغاية، لإجراء عمليات البحث الموجهة عن بصمات الأصابع. حيث استلزم الأمر إجراء عمليات البحث على أساس كل حالة على حدة، وفقط فيما يتعلق بمنع ارتكاب بعض الجرائم الخطيرة والجرائم الإرهابية، والكشف عنها، والتحقيق فيها.

يمكن مشاركة البيانات البيومترية التي جمعتها وكالات ضبط الحدود أثناء المراحل المبكرة من السفر، في سياق جمع معلومات الاستخبارات أو التحقيقات المناسب، مع وكالات إنفاذ القانون والأجهزة الأمنية.

المرحلة 5: الخروج

تتشابه عملية قبل المغادرة مع بروتوكولات قبل الوصول. حيث يحتاج المسافر إلى تسجيل الوصول عبر الإنترنت أو في المطار، وإبراز الوثائق الخاصة به قبل الصعود على متن الطائرة. ويتم استكمال أنظمة مراقبة الحدود الآلية (ABC) من خلال عدد من برامج المسافر الدائم مثل "برنامج المسافر المسجل". وتتطلب هذه البرامج من المسافر التسجيل للحصول على العضوية، وتسجيل بيانات بيومترية، وقد يخضع البعض أيضًا لعملية تدقيق. فالولايات المتحدة الأمريكية، على سبيل المثال، تستخدم برنامج الدخول العالمي (Global Entry Program) الذي يتيح إمكانية منح التصريحات العاجلة للمسافرين الموافق عليهم مسبقًا وقليلي الخطر عند التنقل عبر حدود الولايات المتحدة الأمريكية. حيث يتوجه أعضاء البرنامج نحو الأكشاك المخصصة لبرنامج الدخول العالمي، ويبرزون جواز السفر المقروء آليًّا أو بطاقة الإقامة الدائمة الأمريكية، ويضعون أصابعهم على الماسح الضوئي للتحقق من بصمات الأصابع، ويكملون إقرارًا جمركيًّا. يُصدر الكشك إيصال معاملة للمسافر. ويجب حصول المسافرين على الموافقة المسبقة لبرنامج الدخول العالمي. كما يجب أن يخضع جميع المتقدمين لفحص سوابق صارم وإجراء مقابلة شخصية قبل التسجيل.

على الرغم من عدم قيام جميع البلدان بإجراء مراقبة الخروج من الهجرة في وقت المغادرة، فلا يزال العديد من البلدان تفحص المسافر المغادر للبلد. وعادةً ما يتضمن ذلك فحص أن الاسم الوارد في بطاقة الصعود إلى الطائرة مطابق للاسم الموضح في وثيقة السفر والبحث عنه من خلال قوائم مراقبة السير الذاتية، وأن تفاصيل الرحلة متسقة مع جدول هذا اليوم، وأن المسافر لم يتجاوز فترة الإقامة. إلى جانب هذه الفحوص، تقوم البلدان أيضًا بتقييم المسافرين، بحثًا عن مهربي المخدرات والأموال، والأشخاص الذين يتم الاتجار بهم إلى البلدان الأخرى، وخاصةً المقاتلين الإرهابيين الأجانب، بناءً على وثائق السفر الخاصة بهم، وبطاقة الصعود إلى الطائرة، وغير ذلك من المعايير المحددة.

دراسة الحالة 7 - التحقق البيومتري الخاص بالمغادرة

أحد النماذج الناشئة في الولايات المتحدة الأمريكية مخصص لكي تعمل شركات الطيران، والمطارات، والحكومة بالتعاون معًا من أجل الاستثمار في مبادرات التيسير عند بوابات الصعود إلى الطائرة، مما يقدم آلية بديلة تتيح إمكانية التحقق البيومتري الخاص بالمغادرة. في أوائل عام 2018، شرعت كلٌّ من خطوط طيران لوفتهانزا وخطوط الطيران البريطانية في إجراء تجارب باستخدام برامج التعرف إلى الأشخاص من سمات وجوههم. ويُعد ذلك تطبيقًا إضافيًا لعملية التحقق البيومتري *1:كثير* للمسافرين المعروفين، على غرار الترتيبات التي يتم وضعها في الشراكات بين شركات الطيران والحكومات للسفر بين أستراليا ونيوزيلندا (راجع دراسة الحالة 5).

3-1-2 ضبط الأمن وتطبيقات الإنتربول

عادةً ما تتألف قواعد البيانات البيومترية المستخدمة في عمليات ضبط الأمن من البيانات المرجعية من المعتقلين (صور الوجوه، وبصمات الأصابع، وصور الحمض النووي)، وبيانات مسرح الجريمة، وغير ذلك من البيانات غير المحددة، على سبيل المثال، جراء التحقيقات بشأن الأشخاص المتوفين أو المفقودين أو أنشطة جمع معلومات الاستخبارات. قد تعمل هذه الأنظمة على المستوى المحلي، أو الإقليمي، أو الوطني لاستيفاء الوظائف مثل الاحتفاظ بالسجلات الجنائية، أو التحقيق في الجرائم، أو إصدار نتائج الاستخبارات الجنائية. ويمكن إما إضافة البيانات البيومترية الصادرة عن التحقيقات المتعلقة بالإرهاب إلى هذه الأنظمة وإما تحميلها إلى قواعد بيانات مخصصة بوصفها تدابير أمنية إضافية. وبغض النظر عن تكوين قاعدة البيانات المستخدمة، ستكون هناك حاجة تشغيلية إلى البحث عبر جميع الأنظمة نظرًا إلى الصلة المحتملة بين الإرهاب والإجرام العام، على سبيل المثال، الأفراد الذين يرتكبون جرائم الاحتيال أو السرقة عالية القيمة لتمويل أنشطة الإرهاب على وجه الخصوص، وما شابه ذلك. *ولا شك أنه من المفضل، أن تكون الأنظمة قادرة على العمل بالتوافق مع التطبيقات البيومترية للوكالات الحدودية إذا كان القانون الوطني يسمح بذلك.*

ويمكن للشرطة، على الصعيد الدولي، تبادل البيانات البيومترية من خلال الاتفاقيات الثنائية أو متعددة الأطراف أو الإقليمية، ولكن الطريقة العالمية الرسمية الوحيدة تكون عبر منظمة الشرطة الجنائية الدولية (ICPO أو المعروفة أكثر باسم الإنتربول) التي تعمل على تيسير التعاون الشرطي الدولي. وتجدر الإشارة إلى أن البلدان التي تقدم إسهاماتها من البيانات إلى قواعد بيانات الإنتربول:

1- *تحتفظ بملكية بياناتها* وتكون قادرة على إزالتها من قواعد البيانات في أي وقت (راجع القسم 3-3-2- عمليات البحث أحادية الاتجاه).
2- *تحدد نطاق البيانات التي يتم البحث فيها* أي بيانات البحث، وعدم الكشف عن البيانات المحفوظة أمام البيانات البيومترية من بلدان معينة

يمتلك الإنتربول ثلاث قواعد بيانات بيومترية يمكن استخدامها من جانب البلدان الأعضاء في المنظمة والبالغ عددها 190 بلدًا:

الوجه – توفر تلك القاعدة الوظائف الآتية:

- ☐ التعرف إلى الأشخاص الهاربين والمفقودين
- ☐ التعرف إلى الأشخاص غير المعروفين المثيرين للاهتمام
- ☐ تحديد الأفراد في صور وسائط الإعلام العامة
- ☐ التحقق من "الصور الجنائية التعريفية" (صور حبس السجناء) المتسلَّمة من أي قاعدة بيانات (1:كثير).

بصمات الأصابع – بوابة نظام التعرف الآلي إلى بصمات الأصابع. يتيح هذا النظام لمسؤولي إنفاذ القانون المخوَّلين من البلدان الأعضاء إمكانية استخدام قاعدة البيانات عن بُعد وتلقي استجابة آلية باستخدام شبكة الاتصالات العالمية المأمونة التابعة للإنتربول I-24/7. تتضمن قاعدة البيانات كلًّا من البيانات المرجعية (بصمات الأصابع وراحة اليد) وبيانات مسرح الجريمة (علامات الأصابع وراحة اليد).

الحمض النووي – بوابة الحمض النووي (التي تعمل بطريقة مماثلة لبوابة التعرف الآلي إلى بصمات الأصابع. حيث تمتلك منظمة الإنتربول قواعد بشأن معالجة بيانات الحمض النووي متفق عليها مع جميع البلدان الأعضاء وتتألف قاعدة البيانات من أربعة أقسام:

- مسارح الجرائم غير المحلولة
- مرتكبو الجرائم المعروفون
- الأشخاص المفقودون
- الرفات البشرية مجهولة الهوية

كما يقدم الإنتربول أيضًا خدمات أداته "مطابق الحمض النووي الثنائي" التي توفر منصة خاصة لعمليات البحث والمقارنات للحمض النووي بين بلدين. ويعتمد الإجراء على الثقة المشتركة، واستراتيجية الشرطة، والتشريعات المتوافقة، ومعايير المطابقة المتفق عليها بشكل متبادل، على سبيل المثال، الحد الأدنى لعدد المواقع. حيث يحدد كل بلد صور الحمض النووي ويرسلها بصورة آمنة إلى الإنتربول. ويتم إخطار كلا الشريكين بأي مطابقات تم اكتشافها، ومن ثمَّ تُحذف البيانات من النظام. ويمكن أن تستخدم البلدان هذه الأداة لمقارنات المرة الواحدة أو بوصفها جزءًا من عملياتها للمطابقة المنتظمة.

تتمثل إحدى الوظائف المهمة لقواعد البيانات البيومترية الخاصة بمنظمة الإنتربول في جمع البيانات البيومترية بشأن المقاتلين الإرهابيين الأجانب وغيرهم من الإرهابيين من أجل منع تنقلهم عبر الحدود. ويدعم ذلك مسار العمل العالمي لاستراتيجية مكافحة الإرهاب الخاص بالإنتربول الذي يعطي الأولوية للتعرف إلى أعضاء الجماعات الإرهابية عبر الوطنية المعروفة.

3-1-3 قواعد البيانات البيومترية للإنتربول: الرقابة والحوكمة

تخضع الإدارة الداخلية لقواعد البيانات البيومترية التابعة للإنتربول وتشغيلها لإشراف اللجنة المعنية بمراقبة ملفات الإنتربول (CCF) التي تُعد هيئة مستقلة. وتضطلع بثلاث وظائف:

1- التأكد من أن معالجة البيانات الشخصية من جانب الإنتربول تتوافق مع اللوائح التنظيمية للمنظمة
2- تقديم المشورة إلى الإنتربول بشأن أي مسألة تتعلق بمعالجة البيانات الشخصية
3- معالجة الطلبات التي تتعلق بالمعلومات الواردة في ملفات المنظمة.

أصبحت لجنة مراقبة ملفات الإنتربول هيئة رسمية للمنظمة عندما أجرت الجمعية العامة في دورتها الـ 77 تصويتًا عام 2008 لتعزيز وضعها من خلال تعديل الدستور لضم لجنة مراقبة ملفات الإنتربول إلى هيكلها القانوني الداخلي. وفي تشرين الثاني/نوفمبر 2016، أقرَّت الجمعية العامة للإنتربول مجموعة إصلاحات فيما يتعلق بآليات الإشراف الخاصة بالإنتربول. وشمل ذلك اعتماد القانون الجديد للجنة مراقبة ملفات الإنتربول الذي أدخل إصلاحات جذرية على تشكيلها، وهيكلها، وإجراءاتها. وقد دخل هذا الإطار القانوني الجديد حيز التنفيذ في 11 آذار/مارس 2017 وعزز من المهام الاستشارية والإشرافية المنوطة باللجنة، مع تعزيز قدرتها على تقديم سبل انتصاف فعالة للأفراد فيما يخص البيانات المتعلقة بهم التي قد تتم معالجتها في ملفات الإنتربول.

4-1-3 إدارة البيانات في قائمة المراقبة البيومترية والمتعلقة بالسير الذاتية

إن قوائم المراقبة هي شكل من أشكال نظم التنبيه، اعتمادًا على أنواع البيانات المختلفة، وتعمل على المستوى الوطني وأحيانًا على المستوى الإقليمي. والغرض منها هو تقديم تحذيرات مسبقة وإجراءات فحص للمساعدة على التعرف إلى المجرمين والإرهابيين والبضائع أو المواد المشتبه بها، وتحديد ذلك عند نقاط العبور الحدودية. ثمة أنواع عديدة لقوائم المراقبة تشمل:

- *قوائم المراقبة المتعلقة بالسير الذاتية:* معلومات عن الأشخاص المطلوبين للعدالة أو المفقودين، والأشخاص مثار الشبهات، وحالات حظر الطيران، وما إلى ذلك.
- *قوائم المراقبة البيومترية:* تشمل الأشكال البيومترية المألوفة: بصمات الأصابع، وصور الوجه وحدقة العين (لا يُستخدم الحمض النووي حاليًا على نطاق واسع) ولها وظائف مشابهة لقوائم المراقبة المتعلقة بالسير الذاتية، حيث تضم الأشخاص المطلوبين للعدالة أو المفقودين، والأشخاص مثار الشبهات، والإرهابيين المعروفين أو المشتبه بهم، وما إلى ذلك.
- *قوائم المراقبة التي تتضمن معلومات عن البضائع والوثائق:* المركبات المسروقة، ووثائق السفر المفقودة والمسروقة[61]، والأعمال الفنية المسروقة، وما إلى ذلك.
- *قوائم المراقبة التي تتضمن معلومات عن أسلوب العمل أو التعرف إلى البضائع الخطرة:* الطريقة المعينة المستخدمة لتنفيذ جريمة أو سلسلة من الجرائم، أو الطرق الجديدة للتعرف إلى العملات الورقية أو وثائق السفر المزيفة، والأساليب والمكونات الكيميائية المستخدمة في تصنيع العقاقير غير المشروعة، وما إلى ذلك.

تُستخدم قوائم المراقبة أيضًا من جانب هيئات إنفاذ القانون الإقليمية والدولية مثل الإنتربول[62] ووكالة الاتحاد الأوروبي للتعاون في مجال إنفاذ القانون (اليوروبول).[63] ومن جانب المنظمات غير المعنية بإنفاذ القانون للتطبيقات الأخرى التي ينتج عنها نطاق واسع ومتنوع من المستخدمين:

- *إنفاذ القانون:*
  - على المستوى الدولي[64]؛ الإنتربول[65].
  - على المستوى الإقليمي: اليوروبول[66] وغير ذلك من المنظمات الإقليمية
  - على المستوى الوطني[67]: الشرطة، الهجرة، الجمارك، وما إلى ذلك.
- *المنظمات الدولية*
  - الأمم المتحدة (UN)،[68] وما إلى ذلك.
- *المنظمات العامة،*
  - الجهات المختصة بإصدار جوازات السفر،[69] والجهات المختصة بإصدار رخصة القيادة وما إلى ذلك.
- *المنظمات الخاصة/التجارية،*
  - شركات الطيران، شركات التأمين، شركات تصنيع الأغذية، وما إلى ذلك.

[61] راجع: https://www.interpol.int/INTERPOL-expertise/I-Checkit
[62] راجع: https://www.interpol.int/
[63] راجع: https://www.europol.europa.eu/
[64] راجع: دليل إدارة مراقبة الحدود لبرنامج تحديد هوية الركاب التابع لمنظمة الطيران المدني الدولي (الإيكاو)، الإصدار 1، الفصل: M-5
[65] راجع: https://www.interpol.int/INTERPOL-expertise/Databases
[66] راجع: https://www.europol.europa.eu/activities-services/services-support/information-exchange/europol-information-system
[67] راجع: دليل إدارة مراقبة الحدود لبرنامج تحديد هوية الركاب التابع لمنظمة الطيران المدني الدولي (الإيكاو)، الإصدار 1، الفصل: E-4
[68] راجع: https://www.un.org/sc/ctc/
[69] راجع: https://www.consilium.europa.eu/prado/en/check-document-numbers/check-document-numbers.pdf

تستخدم المنظمات غير المعنية بإنفاذ القانون قوائم المراقبة في المجالات التي تقع داخل نطاق مسؤوليتها أو عملها من أجل حماية منتجاتها وعملياتها ومنع الأعمال الاحتيالية.

2-3 القيود المفروضة على قوائم المراقبة المتعلقة بالسير الذاتية

تستند أغلبية قوائم مراقبة إنفاذ القانون إلى معلومات السير الذاتية للشخص، مثل: الأسماء، وتواريخ الميلاد، وما إلى ذلك. وقد تكون هذه المعلومات غير موثوق بها وعرضة للتغيير أو للخطأ. يرد فيما يلي بعض الأمثلة الشائعة:

- ☐ خطأ إملائي أو ترجمة غير صحيحة للأسماء
- ☐ استخدام اسم أو لقب تم تغييرهما بدلًا من الاسم الرسمي المدرج في وثائق السفر
- ☐ تاريخ ميلاد خاطئ أو تسلسل غير صحيح للأرقام، مثل 12-01-1967 بدلًا من 01-12-1967
- ☐ شخص يحمل جنسيتين
- ☐ قام شخص بتغيير اسمه والحصول على هوية أو وثائق سفر جديدة
- ☐ يقدم شخص وثيقة سفر مزورة، أو مزيفة، أو حصل عليها بطريقة احتيالية تحمل اسمًا (أسماء) آخر
- ☐ يقدم شخص وثيقة سفر أصلية خاصة بشخص آخر من أجل انتحال شخصية حاملها الأصلي
- ☐ يقوم شخص "بمشاركة" وثيقة سفر مع شخص ما باستخدام صورة "مُحولة"، أي صورة مؤلفة من مزج وجهين مختلفين (راجع القسم 2-3-2-)
- ☐ توءم أو ثلاثة توائم يتبادلون الهوية و/أو وثائق السفر

ومن ثمَّ، فإن التحديد الإيجابي للشخص أمر بالغ الأهمية وقد أدى هذا إلى إنشاء قوائم مراقبة بيومترية.

3-3 قوائم المراقبة البيومترية

تلعب قوائم المراقبة البيومترية دورًا إضافيًّا في عمليات التحقق البيومترية 1:1 التي تتم عند الحدود. حيث تُستخدم عمليات الفحص للتحقق 1:1 (راجع القسم 3-1) البيانات البيومترية المخزنة في الرقاقة الموجودة داخل وثيقة السفر الإلكترونية للمصادقة على هوية الشخص الذي يصل إلى الحدود. يمتد مفهوم قائمة المراقبة لما هو أبعد من ذلك ويقدم إمكانية بحث 1:كثير (واحد للكثير) لفحص البيانات البيومترية للمسافر مقابل قاعدة بيانات خاصة بالبيانات البيومترية للأشخاص مثار الشبهات. ويلزم توفر معدات مشابهة لتسجيل البيانات البيومترية لكلا العمليتين ولكن تحتاج قاعدة البيانات إلى برنامج بحث 1:كثير إضافةً إلى برنامج المطابقة 1:1 بحيث يمكنها إجراء إحدى المهمتين أو كلتيهما حسبما يلزم. وسيتطلب ذلك بشكل واضح المزيد من الاستثمار. ستعتمد فعالية البحث 1:كثير في قائمة المراقبة على الآتي:

- ☐ جودة بيانات التسجيل
- ☐ نوع البيانات المخزنة في قاعدة البيانات
- ☐ أداء النظام (راجع القسم 1-1)
- ☐ ضعف النظام أمام هجمات العرض باستخدام التقنيات مثل تحويل الصور أو الانتحال (راجع القسم 2-2)

من الأمثلة على قوائم المراقبة الدولية والإقليمية الكبيرة الآتي:

نظام I-24/7 في الإنتربول - يمكن الوصول إلى جميع قواعد بيانات الإنتربول، باستثناء شبكة الإنتربول للمعلومات الباليستية (IBIN)، في الوقت الفعلي من خلال شبكة I-24/7 التي تربط جميع المكاتب المركزية الوطنية للإنتربول (NCB). فهي مرتبطة بنظام النشرات الخاص بالإنتربول لإصدار التنبيهات الدولية بشأن الهاربين، والمجرمين المشتبه بهم، والأشخاص المرتبطين بالتحقيقات الجنائية الحالية أو محل شك فيها، والأشخاص والهيئات الخاضعة لجزاءات مجلس الأمن بالأمم المتحدة، والتهديدات المحتملة، والأشخاص المفقودين، وجثث الموتى.

نظام معلومات اليوروبول (EUROPOL-EIS) - تتضمن قاعدة البيانات هذه المعلومات الجنائية والاستخباراتية التي تشمل كل مجالات الجريمة المقررة من جانب اليوروبول، بما في ذلك الإرهاب.

دراسة الحالة 8 - نظام معلومات السفر والترخيص الأوروبي

تقترح مفوضية الاتحاد الأوروبي إنشاء نظام معلومات السفر والترخيص الأوروبي (ETIAS)[70] لتعزيز أمن السفر إلى منطقة شنغن بموجب اتفاقيات الإعفاء من التأشيرات. ستتألف قائمة مراقبة نظام معلومات السفر والترخيص الأوروبي (ETIAS)، التي من المقرر إنشاؤها وإدارتها من جانب اليوروبول، من البيانات ذات الصلة بالأشخاص المشتبه في ارتكابهم لجريمة جنائية أو شاركوا في ارتكابها، أو الأشخاص الذين توجد بشأنهم دلائل واقعية أو أسباب وجيهة للاعتقاد بأنهم سيرتكبون جرائم جنائية.
من المقرر إنشاء قائمة المراقبة على أساس:

1) قائمة لجنة الجزاءات التابعة للأمم المتحدة
2) المعلومات ذات الصلة بجرائم الإرهاب أو غيرها من الجرائم الجنائية الخطيرة المقدمة من الدول الأعضاء
3) المعلومات ذات الصلة بجرائم الإرهاب أو غيرها من الجرائم الجنائية الخطيرة التي تم الحصول عليها من خلال التعاون الدولي.

1-3-3 فوائد التطبيقات البيومترية لمكافحة الإرهاب

1-1-3-3 داخل الحدود الوطنية

لقد لعبت قواعد البيانات البيومترية دورًا متزايد الأهمية في تحقيقات الجرائم منذ وضع أول تصنيف لبصمات الأصابع وأنظمة البحث في التسعينيات من القرن التاسع عشر. وأدت الحوسبة وأشكال التقدم العلمية والتكنولوجية في القرن العشرين بشكل كبير إلى زيادة كفاءة مثل هذه الأنظمة وقدرتها على المعالجة، وتوسيع نطاق الأشكال البيومترية المتاحة مثل الوجه والحمض النووي والصوت وما إلى ذلك. فأنظمة البحث البيومترية التي يستخدمها العديد من وكالات إنفاذ القانون اليوم تضم الخوارزميات المتقدمة والمعقدة التي يمكنها تيسير البحث السريع والدقيق في كميات كبيرة من البيانات. ومع ذلك، فإن الميزة الكبرى التي تمتاز بها عملية البحث في قاعدة بيانات كشف الجرائم عن معظم عمليات التحقيق وجمع معلومات الاستخبارات الأخرى هي أنها تقدم مراقبة مستمرة على مدار 24 ساعة يوميًّا طوال أيام السنة ما دامت البيانات مُحتفظًا بها في قاعدة البيانات. وقد يتم العثور على تطابق بمجرد تسجيل البيانات والبحث عنها، بشرط أن تكون بيانات التطابق موجودة بالفعل في قاعدة البيانات، أو ربما يتم حفظها في النظام وإظهار التطابق في وقت لاحق بعد أسابيع، أو شهور، أو أعوام، أو حتى عقود. ومن ثمَّ، يعدّ البحث في قاعدة بيانات كشف الجرائم إحدى المزايا الأكثر فعاليةً من حيث التكلفة ونفعًا على نحو منتظم المتوفرة للمحققين ومحللي الاستخبارات في العصر الحديث. تتيح أيضًا قواعد البيانات المزايا الآتية:

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

1- إمكانية دمجها على الصعيد الوطني لتوفير تغطية فعالة لأي بلد بغض النظر عن حجمه المادي والعدد النسبي لسكانه
2- إمكانية العمل بالتوافق مع الأنظمة البيومترية للوكالات الحدودية
3- إمكانية ربطها بقواعد البيانات البيومترية الدولية أو غيرها من قواعد البيانات ذات الصلة.

التحقيقات الجنائية في الوقت الفعلي

طورت وكالات إنفاذ القانون في العديد من البلدان هذه التقنية البيومترية واستخدمتها لإثبات هوية مرتكبي الجرائم وتأكيد سوابقهم الجنائية، وإثبات تورط المشتبه بهم في أي جريمة أو دحض ذلك، وربط الجرائم. وقد برهنت قواعد البيانات هذه على أنها ذات قيمة، خاصةً في التحقيقات المتعلقة بالإرهاب وتم تعزيز إسهاماتها في السنوات الأخيرة من خلال ظهور "التحقيقات الجنائية في الوقت الفعلي". وتستغل هذه العملية ميزة الإنشاء والاسترداد السريع لبيانات التحقيقات الجنائية القابلة للبحث من مسارح الجرائم مثل صور الوجه المستخرجة من الأجهزة الإلكترونية أو الصور الفوتوغرافية، أو عينات الحمض النووي التي يتم تحليلها بشكل سريع، أو النقل الإلكتروني للصور الرقمية لعلامات الأصابع من مسرح الجريمة مباشرةً إلى بوابة التعرف الآلي إلى بصمات الأصابع (AFIS) لإجراء البحث الفوري. لقد أصبح من الممكن الآن، كما يصبح روتينيًّا بشكل متزايد، البحث عن المواد البيومترية المهمة بوصفها دليلًا والمقارنة فيما بينها بينما لا تزال عمليات فحص مسرح الجريمة جارية. ويتيح هذا الأمر إمكانية إصدار معلومات الاستخبارات الجنائية التي يمكنها تحديد أحد المشتبه بهم على وجه السرعة، أو توجيه المحققين نحو مسارات تحقيق فعالة في المراحل الأولى من التحقيق أو تغيير مسارات التحقيق. ففي التحقيقات المتعلقة بالإرهاب، قد يحدد ذلك البحث المزيد من المشتبه بهم أو المرافقين لهم بعد وقوع أي حادث مباشرةً والمساعدة على منع وقوع المزيد من الهجمات. ومن الواضح أنه يمكن تحسين هذه القدرة على نحو إضافي إذا كانت مجموعة البيانات البيومترية التي يتم البحث فيها في الوقت الفعلي على أوسع نطاق ممكن.

لا شك أن قواعد البيانات مفيدة للغاية عند التعامل مع أعقاب "الهجمات الإرهابية الانتحارية" حيث قد تختلط البقايا الجسدية للمفجر مع رفات الضحايا. ويتحتم في مثل هذه الحالات سرعة تحديد كلٍّ من هوية المفجر، في سبيل التقدم في مسار التحقيق ومحاولة إحباط المزيد من الهجمات، وكذلك تحديد هوية الضحايا بالنيابة عن عائلاتهم. ويمثل كلٌّ من الحمض النووي، وبصمات الأصابع، وعلم الأسنان (طب الأسنان الشرعي) البيانات البيومترية الأساسية المستخدمة بوصفها محددات الهوية الأولية التي تُستغل في تحديد هوية ضحايا الكوارث[71].

3-3-1-2 عبر الحدود الوطنية

كما سبق أن جرى توضيحه، فإن التدخلات البيومترية عند الحدود تندرج تحت فئتين:

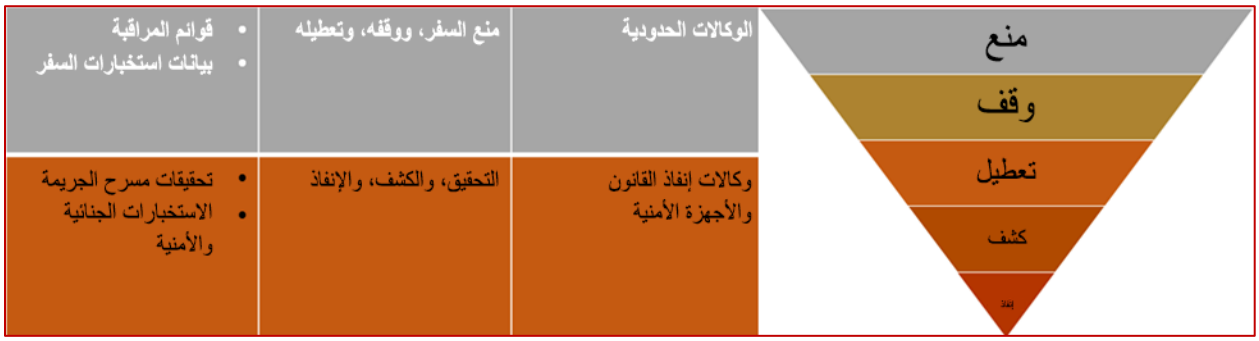
[71] إن تحديد هوية ضحايا الكوارث (DVI) هو إجراء معترف به دوليًّا لاستعادة ضحايا حوادث الوفيات الجماعية وتحديد هوياتهم، ودعم الثكالى أثناء العملية. يتعهد بها موظفو إنفاذ القانون ويُجرَى الاتفاق على العمليات على الصعيد الدولي من خلال عضوية لجان تحديد هوية ضحايا الكوارث التابعة للإنتربول. كما يمكن للإنتربول أيضًا تقديم المساعدة والتنسيق بشكل مباشر في حالة وقوع الحوادث الدولية الكبيرة والمعقدة.

(1) *التحقق البيومتري من الهوية (1:1)* – مقارنة البيانات البيومترية التي تم الحصول عليها من المسافر عند الحدود باستخدام البيانات البيومترية، على سبيل المثال، تلك البيانات المخزنة في وثائق السفر مثل جواز السفر الإلكتروني

(2) *البحث في قوائم المراقبة البيومترية (1:كثير)* – البحث في البيانات البيومترية التي تم الحصول عليها من المسافر عند الحدود أو من جواز السفر الإلكتروني أو وثائق طلب السفر الخاصة به من خلال قائمة مراقبة تتضمن البيانات البيومترية للأشخاص مثار الشبهات مثل أولئك المطلوبين من جانب وكالات إنفاذ القانون، أو الإرهابيين المعروفين أو المشتبه بهم، وما إلى ذلك.

تعمل كل عملية على تحسين تقييم مخاطر المسافرين من خلال إدارة شؤون الهوية.[72] والوضع الأمثل هو تطبيق كلتا العمليتين عبر الحدود. فعملية التحقق من الهوية عند الحدود ستؤكد هوية المسافر مقابل البيانات البيومترية المسجلة والمصدق عليها ولكن قد يكشف البحث في قائمة المراقبة البيومترية أن الهوية المؤكدة قد تكون لشخص مثير للشبهة. ويتطلب هذا النهج زيادة الاستثمار ولكن المستويات الإضافية من الضمان والأمان التي يوفرها عادةً ما تبرر النفقات الإضافية.

الشكل 5 - مقتبس من دليل إدارة مراقبة الحدود لبرنامج تحديد هوية الركاب التابع لمنظمة الطيران المدني الدولي (الإيكاو)، مونتريال (2018)
(بإذن من الإيكاو)



قد تختلف قوائم المراقبة من حيث الحجم والتعقيد في محتواها. حيث تضم بعض قوائم المراقبة البيومترية قواعد بيانات منفصلة للبيانات المرجعية التي تم الحصول عليها من فئات معينة من الأشخاص مثار الشبهات. في حين قد تضيف قوائم المراقبة البيومترية الأخرى بيانات بيومترية محددة من مسرح الجرائم لتوسيع النطاق. ومع ذلك، فإن التفسير الأوسع نطاقًا لمفهوم قائمة المراقبة قد يكون الدمج القانوني لجميع قواعد البيانات البيومترية لوكالات إنفاذ القانون الوطنية (راجع القسم 3-3-2) في شكل "قائمة مراقبة وطنية" على النحو الموضح في الشكل 5. وذلك من شأنه أن يكشف عن المقدار الأمثل من البيانات ذات الصلة في عمليات البحث في قوائم المراقبة ويوفر أقصى قدر من الحماية لجمهور المسافرين والأمن للدولة. ومع ذلك، قد تُفرض قيود قانونية وتنظيمية وطنية تعوق تطبيق مثل هذا الحل.

3-1-3-3 خارج نطاق الحدود الوطنية

قد يمتلك أي بلد ممتلكات خارج حدوده تعد عُرضة للهجمات الإرهابية. وقد تشكل البيانات البيومترية جزءًا أساسيًّا من أي خطة لتخفيف حدة التهديدات. على سبيل المثال، قد يكون من الضروري فحص موظفي البلد المضيف ممن يعملون في المنشآت التي تملكها البلد الأصلي، مثل إحدى السفارات. يقتضي ذلك التعاون بين البلدين، وعلى نحو مثالي، الاتفاق القانوني للبحث في قواعد البيانات البيومترية والمتعلقة بالسير الذاتية الخاصة بكلتا البلدين من أجل إثبات أن الموظفين ليس لديهم سجل إجرامي أو صلة معروفة بالإرهاب في أيٍّ من البلدين. وعلى غرار ذلك، إذا تورط المواطنون من البلد المضيف في أنشطة إرهابية داخل البلد الأصلي، فمن المفيد لكلا البلدين تبادل البيانات البيومترية بينهما والبحث فيها، وذلك أولًا من أجل حماية ممتلكات البلد الأصلي بالخارج، مثل العمليات التجارية، والمباني والأنشطة الدبلوماسية، وما إلى ذلك، وثانيًا لمساعدة البلد المضيف على التعرف إلى أي من مواطنيه المشتبه في قيامهم بأنشطة إرهابية وإدارة عملية إعادتهم. ويرد هذا الشكل من التعاون ثنائي الأطراف وغيره من خيارات تبادل البيانات في القسم 3-3-2.

[72] ارجع إلى دليل إدارة مراقبة الحدود لبرنامج تحديد هوية الركاب التابع لمنظمة الطيران المدني الدولي (الإيكاو)، مونتريال (2018) للحصول على التفاصيل.

3-3-1-4 *البيانات البيومترية المستمدة من مصادر عسكرية*

تستخدم بعض البلدان قواتها العسكرية لمكافحة الإرهاب داخل حدودها الوطنية أو بالخارج. وغالبًا ما تُستخدم البيانات البيومترية في أثناء مثل هذه العمليات العسكرية لعدم السماح بإغفال هوية الإرهابيين ممن يسعون إلى الاختباء والاندماج بين السكان المحليين لتجنب اكتشافهم أو استخدامهم بمنزلة "دروع بشرية". وقد تستخدم القوات العسكرية تقنيات مشابهة لتلك التي تستخدمها وكالات إنفاذ القانون، مثل نشر أجهزة التقاط بيومترية ثابتة أو متحركة للحصول على عينات مرجعية من الإرهابيين المشتبه فيهم أو الفحص الجنائي للعناصر المستردة من المحتجزين أو المواقع المثيرة للشبهات المتصلة بالأنشطة الإرهابية أو أنشطة المتمردين.

قد تمثل كذلك البيانات البيومترية التي تم الحصول عليها من هذه العمليات العسكرية قيمة بالغة الأهمية لوكالات إنفاذ القانون فيما يتعلق بالتحقيقات المتعلقة بالإرهاب، ولكن قد توجد عقبات كبيرة في مشاركة مثل هذه البيانات واستخدامها وسيعتمد ذلك إلى حد كبير على:

- ☐ السلطة القانونية لتبادل هذه البيانات البيومترية بما يتوافق مع القانون الوطني والقانون الدولي لحقوق الإنسان
- ☐ مقبولية البيانات البيومترية العسكرية وغيرها من الأدلة في المحاكم المدنية
- ☐ مدى توافق معايير الجودة للبيانات البيومترية والأدلة الجنائية العسكرية مع تلك المستخدمة من جانب السلطات المدنية في ذلك البلد

بناءً على ذلك، حتى إذا كان تبادل البيانات قد يكون قانونيًّا، فقد لا تصل البيانات إلى المعايير القانونية المطلوبة ليتم قبولها بصفتها دليلًا، رغم أنه بالطبع قد تكون ذات قيمة استخبارية كبيرة (راجع القسم 3-3-3-).

دراسة الحالة 9 - مركز تحليل الأجهزة المتفجرة الإرهابية

يُعد مركز تحليل الأجهزة المتفجرة الإرهابية التابع لمكتب التحقيقات الفيدرالي الأمريكي (TEDAC) مثالًا على هذا النوع من القدرات. يقوم مركز تحليل الأجهزة المتفجرة الإرهابية التابع لمكتب التحقيقات الفيدرالي الأمريكي بتنسيق جهود الحكومة بأكملها، من إنفاذ القانون إلى الاستخبارات وصولًا إلى العمليات العسكرية، وذلك لجمع البيانات الجنائية والاستخباراتية حول الأجهزة والأساليب والتقنيات والإجراءات، ومشاركتها بهدف نزع الأجهزة المتفجرة يدوية الصنع (IED) وتعطيلها، وربطها بصانعيها، والأهم من ذلك، منع وقوع الهجمات في المستقبل. وقد تلقى مركز تحليل الأجهزة المتفجرة الإرهابية التابع لمكتب التحقيقات الفيدرالي الأمريكي حتى الآن ما يزيد عن مئة ألف طلب بشأن الأجهزة المتفجرة يدوية الصنع من أكثر من 50 بلدًا. وتقدم وحدة تحليل البيانات البيومترية (BAU) الدعم لقدرات الحكومة الأمريكية والشركاء الدوليين على الصعيد العالمي لمواجهة تهديد الأجهزة المتفجرة يدوية الصنع والتغلب عليها من خلال فحص البصمات الخفية الجنائية والحمض النووي لمواد الأجهزة المتفجرة يدوية الصنع على نحو يتسم بالجودة العالية وفي الوقت المناسب، مما ينتج عنه معلومات استخباراتية ذات فائدة عملية للاستخدام في التحقيقات.

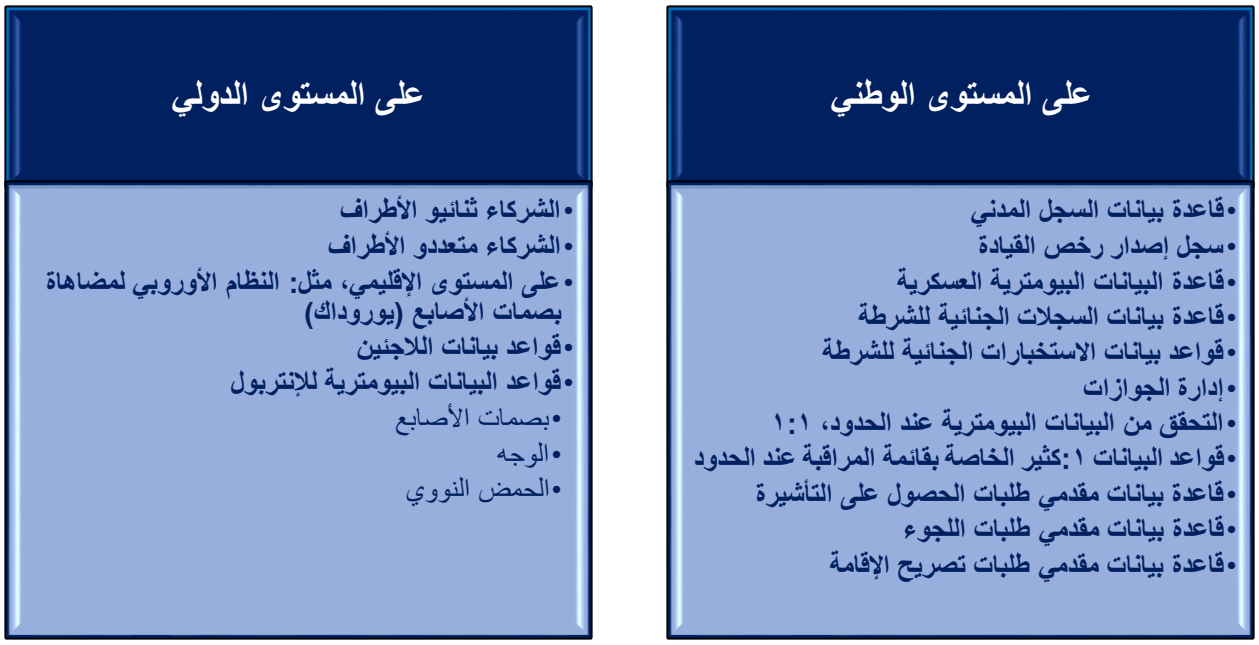
5-1-3-3 الحماية المتبادلة المضمونة

لا يمكن تحقيق فوائد الأنظمة البيومترية في تتبع الإرهابيين والكشف عنهم بشكل كامل إلا في حالة تعاون الدول ومشاركة البيانات. قد يطبق أحد البلدان أنظمة بيومترية وطنية تتسم بالفعالية والشمول داخل حدوده وعبرها، وربما حتى يكون جزءًا من شبكة إقليمية متطورة، ولكن إذا لم يتمكن من الوصول إلى البيانات الإرهابية من البلدان الأخرى الواقعة خارج هذه الشبكة الوطنية والإقليمية، فعندئذٍ، يظل عرضة للخطر. لا شك أن مشاركة البيانات الوطنية، والثنائية، والإقليمية (راجع القسم 3-3-2-) تقدم حلًّا جزئيًّا ولكن من الضروري أن تتم مشاركة البيانات البيومترية الإرهابية على الصعيد الدولي، وعلى نطاق عالمي، وذلك لتوفير حماية متبادلة لجميع الدول. فمن شأن ذلك أيضًا أن يساعد على ردع الإرهابيين وتعطيلهم، ممن يتخذون مقرات لأنفسهم بشكل مؤقت في البلدان ذات القدرات البيومترية الضئيلة أو المعدومة، بحيث يمكنهم اتخاذ هويات جديدة أو الحصول على وثائق سفر تم إصدارها بطريقة احتيالية ثم السفر متخفين إلى وجهات أخرى. يلزم إنشاء نظام قوي وشامل لمشاركة البيانات البيومترية على الصعيد الدولي لمكافحة هذه الأساليب وعدم السماح للإرهابيين بإخفاء هويتهم أو "إيجاد ملاذات آمنة" للعمل من خلالها.

تشكل قواعد البيانات البيومترية التابعة للإنتربول مثالًا جيدًا على هذا النوع من القدرة العالمية. فهي مصممة لاستيفاء هذه المهمة الوقائية والحيوية من خلال السماح للدول بمشاركة البيانات البيومترية المتعلقة بالإرهاب، والأهم من ذلك، أنها تخضع لإجراءات الحوكمة المتفق عليها دوليًّا التي تخضع بدورها لإشراف مستقل.

يوضح الشكل 6 النطاق الواسع لمصادر البيانات البيومترية *المحتملة*، التي تحتفظ بها المنظمات العامة الوطنية والدولية، والتي يمكن الاستفادة منها لأغراض مكافحة الإرهاب. القوائم ليست شاملة، وتخضع بالطبع إمكانية الوصول إلى أي من قواعد البيانات هذه للقيود القانونية والتنظيمية الوطنية. ومع ذلك، فإنها توضح كيف يمكن ربط البيانات البيومترية، نظريًّا؛ لتوفير الحماية المتبادلة من تهديد الإرهاب من حيث الوصول الوطني والإقليمي والعالمي.

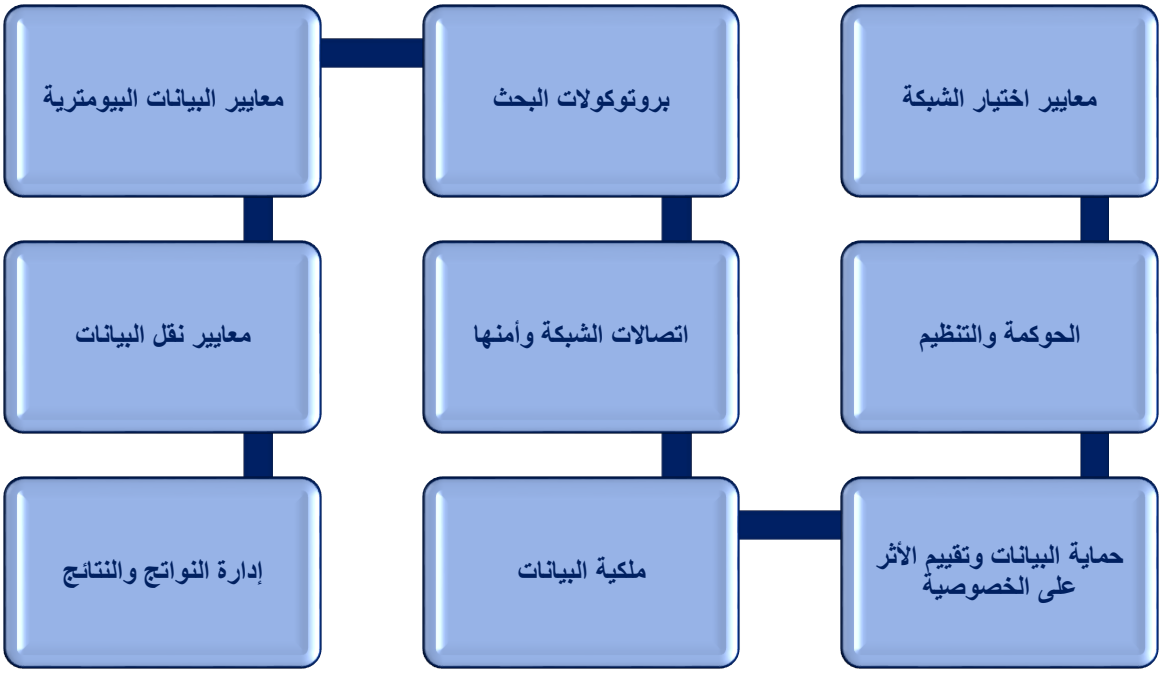
الشكل 6 - مصادر البيانات البيومترية



3-3-2- بروتوكولات مشاركة البيانات والتكامل القانوني لقواعد البيانات

على نحو تقليدي، تعمل قواعد البيانات البيومترية لوكالات إنفاذ القانون بوصفها أنظمة "قائمة بذاتها" نظرًا إلى أن كل تطبيق يخدم حاجة عمل مميزة ومنفصلة، ولم تكن هناك ميزة ملموسة لمشاركة البيانات عبر هذه الأنظمة. وقد صُممت قواعد البيانات هذه على وجه التحديد لأداء مهام الأعمال المرتبطة بضبط الأمن، أو إدارة الحدود، أو السجون. ومع ذلك، فإن التهديد المتزايد للإرهاب العالمي، أثناء العقود الأخيرة، قد أجبر العديد من الحكومات على إعادة النظر في الطريقة التي تُستخدم بها قواعد البيانات الخاصة بها وكيف يمكنها مشاركة البيانات فيما بينها لتوفير حماية معززة لمواطنيها. وقد أدى ذلك إلى تحقيق قدر أكبر من إمكانيات الاتصال والتشغيل المتبادل بين قواعد البيانات على صعيد وطني، وتطوير الشبكات الثنائية ومتعددة الأطراف والإقليمية لقواعد البيانات على صعيد دولي. وبدأ ذلك بتجميع قواعد بيانات متباينة أحادية الوضع، وتطور، في بعض البلدان والمناطق، إلى شبكات بديلة متطورة تضم قواعد بيانات مترابطة متعددة الأوضاع مصممة لخدمة مجموعة من احتياجات الأعمال عبر وكالات إنفاذ القانون، وإدارة الحدود، وغيرها من المهام الحكومية على كلا الصعيدين الوطني والدولي. يرد فيما يلي متطلبات هذا النوع من الاتصال:

الشكل 7 - متطلبات اتصال الشبكة البيومترية



معايير اختيار الشبكة – يجب على مالكي البيانات البيومترية تقييم عضويتهم في أي شبكة من الشبكات البيومترية ليس حسب متطلبات أعمالهم وأهدافهم التشغيلية الخاصة فحسب، مهما كانت أهميتها، ولكن أيضًا من منظور أوسع نطاقًا يأخذ في الاعتبار القيمة الإضافية المحتملة التي تعود على بلدهم أو إقليمهم، وكذلك الشركاء الآخرون في الشبكة. ويُعد هذا النهج ضروريًّا وأساسيًّا في سبيل تطوير قواعد البيانات البيومترية لمكافحة الإرهاب المترابطة شبكيًّا. ومن غير المرجح أيضًا أن يخاطر مالكو البيانات الذين يتطلعون إلى الاشتراك في إحدى الشبكات الدولية بمشاركة بياناتهم مع شركاء مجردين من المبادئ أو غير موثوق بهم، ويلزم إدارة هذه المخاوف بشكل صحيح من خلال أي شبكة لها عضوية دولية كبيرة، على سبيل المثال، راجع القسم 3-1-2- ضبط الأمن وتطبيقات الإنترنبول.

الحوكمة والتنظيم – تحتاج الشبكات البيومترية إلى العمل ضمن إطار قانوني يسمح بنقل البيانات البيومترية وغيرها من البيانات الوصفية ذات الصلة. يجب أن تكون كل قاعدة بيانات موجودة تعمل بالفعل وفقًا للقوانين الوطنية والقانون الدولي لحقوق الإنسان، ولكن قد يستلزم الأمر وضع المزيد من التشريعات لإتاحة البحث بين قواعد البيانات المختلفة داخل أحد البلدان أو على الصعيد الدولي. وفيما يتعلق بالشبكات الدولية، سيتم تحقيق ذلك عادةً من خلال الاتفاقات الرسمية، مثل مذكرات التفاهم، بين الكيانات أو البلدان المشاركة. وقد يقتصر البحث القانوني على عمليات البحث الفردية التي يتم إجراؤها على أساس كل حالة على حدة (على سبيل المثال، الجرائم المحددة) أو التي يتم تطبيقها على نطاق واسع كما هو الحال في عمليات البحث التلقائي في جميع البيانات المسجلة عبر إحدى الشبكات.

يجب أن يوفر أي إطار تنظيمي مراقبة مستقلة للشبكة بالكامل ويولي اهتمامًا خاصًّا لمهام إدارة البيانات والأغراض التي من المقرر أن تستخدم البيانات من أجلها لتجنب أي تمديد للنطاق غير مصرح به، على سبيل المثال، البحث عن مجموعات البيانات سواء داخل الشبكة المحظورة بموجب القانون أو بموجب بروتوكولات التشغيل الحالية، أو خارجها. قامت بعض البلدان بتعيين موظفين يتعهدون بأداء هذه المهام، على سبيل المثال، المنظمين أو المفوضين المعنيّين بالبيانات البيومترية. إضافةً إلى ذلك، يتحمل المنظمون الآخرون - مثل منظم الطب الشرعي في المملكة المتحدة - مسؤولية الإشراف على العمليات العلمية بما في ذلك تلك المستخدمة لإنشاء البيانات البيومترية الجنائية والملفات المستخدمة في قواعد البيانات هذه. مما يعني أن كلًّا من تشغيل قاعدة البيانات والبيانات البيومترية الجنائية الواردة بها يخضع لإشراف وتدقيق مستقلين ويتضمن ذلك عمل اللجان المعنية بالاستعراض الأخلاقي أو ما يماثلها من هيئات. (راجع القسم 2-1-1-)

حماية البيانات وتقييم الأثر على الخصوصية - (راجع القسمين 2-2-3- و2-2-4-).

ملكية البيانات – يجب أن يكون لكل سجل بيومتري مالك بيانات محدد (راجع القسم 2-2-6-) تقع على عاتقه المسؤولية، بموجب القانون، عن تسجيل هذه البيانات، واستخدامها، واستبقائها، وحذفها. يكتسب ذلك الأمر أهمية خاصة عند التعامل مع أي شبكة لقواعد البيانات البيومترية التي تتضمن كميات كبيرة من البيانات من مصادر متنوعة.

اتصالات الشبكة وأمنها – يجب أن يتسم تدفق البيانات البيومترية وغيرها من المعلومات بالكفاءة وحسن التوقيت. يجب أن تكون الشبكة مؤمَّنة نظرًا إلى طبيعة البيانات التي تحتفظ بها وتتمتع بمستويات مناسبة من الأمن لحماية الموظفين والبيئات التشغيلية، بما في ذلك البيانات، والأجهزة، والبرامج، وشبكة الاتصالات. ويُعد من قبيل الممارسة الجيدة الاحتفاظ بالبيانات البيومترية فقط في نظام الشبكة. مع حفظ البيانات الشخصية المتعلقة بالسير الذاتية المرتبطة بالبيانات البيومترية ذات الصلة في نظام منفصل. تحول هذه الاحتياطات دون الوصول إلى المعلومات الشخصية والبيانات البيومترية من تطبيق واحد. لذلك، عادة ما يكون للبيانات البيومترية رقم مرجعي فريد، بحيث يمكن ربطها بالبيانات الموافقة المتعلقة بالسير الذاتية، باستخدام إجراءات تشغيل مؤمَّنة، عندما تستدعي الحاجة.

بروتوكولات البحث – يجب أن تحتوي الشبكة على بروتوكولات لحفظ البيانات وقوائم انتظار للبحث تكون متزامنة ومنهجية تتحكم في توقيت كل عملية بحث وتسلسلها لضمان وصول عملية البحث لمجموعة البيانات الكاملة في كل قاعدة بيانات في الشبكة، أي عدم تفويت أي شيء حتى في أوقات ذروة الطلب (راجع الفقرة التالية - قواعد البيانات المترابطة شبكيًّا: بروتوكولات البحث).

معايير البيانات البيومترية – لا يمكن إجراء عمليات البحث عبر أي شبكة إلا عند قيام الشركاء بحفظ بيانات بيومترية من نوع متوافق. على سبيل المثال، يتم استخدام تركيبات كيميائية مختلفة لتحليل صورة الحمض النووي في جميع أنحاء العالم، على سبيل المثال، في حالة أستراليا، وأوروبا، والولايات المتحدة الأمريكية. فكلٌّ من التركيبات الكيميائية الخاصة بهم استخدمت مواضع فريدة للتكرارات المترادفة القصيرة، إضافةً إلى موضع التكرارات المترادفة القصيرة الذي كان مشتركًا للجميع. ومع ذلك، عند توفير عدد كافٍ من المواضع المشتركة، أمكن البحث في صور التحليل المستخرجة من هذه التركيبات الكيميائية المختلفة في أيٍّ من قواعد بيانات الحمض النووي الخاصة بهم. تستخدم أحدث التركيبات الكيميائية لتحليل الصور عددًا أكبر من مواضع التكرارات المترادفة القصيرة، لذلك ثمة مواضع أكثر نسبيًّا مشتركة بين جميع الشركاء.

يجب أن تدعم المعايير التقنية والعلمية (مثل ISO 17025) الواردة في القسم 2-4 جميع الميزات التشغيلية للشبكة.

معايير نقل البيانات – يمكن أن تُعرّض جودة الصورة دون المستوى القياسي الشبكة البيومترية لمخاطر جسيمة وغير ضرورية، مثل: زيادة عدد حالات الرفض الزائفة أو حتى تحديد الهوية بشكل خاطئ. ولضمان عدم تدهور جودة الصور، مثل الوجه أو بصمات الأصابع، أثناء النقل عبر الشبكة، يجب تطبيق المعايير[73] التي تلبي متطلبات دقة الصورة. مما يعني أن الصورة ستحتفظ بنفس الوضوح والمواصفات بغض النظر عن مكان عرضها على الشبكة.

[73] على سبيل المثال المنشور الخاص من المعهد الوطني للمواصفات القياسية والتكنولوجيا رقم 1152 "مواصفات النقل لقابلية التشغيل المتبادل للطبعات الخفية" www.nist.gov

إدارة النواتج والنتائج – يلزم إدارة المطابقات بين البيانات البيومترية الناتجة عن شبكة البحث (النواتج) والإجراءات المتخذة نتيجة لتلك المطابقات (النتائج) بعناية وبما يتوافق مع المتطلبات القانونية، والمعايير العلمية القوية، والبروتوكولات التنظيمية الصارمة (راجع القسم 3-3-3-). يجب أن تخضع مطابقات البيانات البيومترية لاستعراض الأقران، بوصفه جزءًا من نظام إدارة الجودة، من جانب خبير آخر أو بفضل خبيرين قبل إعلان النتائج. فمن شأن ذلك منع خطر قيام شخص واحد بمطابقة غير صحيحة.

قواعد البيانات البيومترية المترابطة شبكيًّا: بروتوكولات البحث - ثمة طريقتان أساسيتان لمزامنة عمليات البحث بين قواعد البيانات:

البحث أحادي الاتجاه – يتم تسجيل البيانات البيومترية (أ) والبحث فيها على قاعدة البيانات 1. في حالة عدم العثور على مطابقات، يتم عندئذٍ حفظ البيانات في قاعدة البيانات 1 وإرسالها إلى قاعدة البيانات 2 لإجراء البحث، ومرة أخرى في حالة عدم العثور على تطابق، يتم حفظها في قاعدة البيانات 2.

ملاحظة يمكن تفويت حالات المطابقة المحتملة إذا تم البحث في البيانات (أ) *فقط ولم يتم* حفظها على قاعدة البيانات 2 لأن نتيجة البحث ستقتصر على الوقت المحدد للبحث. على سبيل المثال، في حالة تسجيل المزيد من بيانات البحث (ب)، التي تطابق البيانات البيومترية (أ) والبحث فيها على قاعدة البيانات 2 *بعد* الوقت المحدد للبحث في البيانات (أ)، فلن يتم الحصول على أي تطابق؛ لأنه لم يتم حفظ البيانات (أ) ومن ثمَّ لم تصل إليها عملية البحث في البيانات (ب). لذلك، في عمليات نقل البيانات أحادية الاتجاه بين اثنين أو أكثر من قواعد البيانات، من الأهمية بمكان أن تقوم كل قاعدة بيانات بحفظ البيانات بعد البحث لضمان ظهورها في عمليات البحث اللاحقة ومن ثمَّ الحفاظ على التغطية المستمرة.

يمكن أن تمثل إدارة البيانات أيضًا مشكلة مع عمليات النقل أحادية الاتجاه، خاصةً إذا كانت قواعد البيانات تابعة لولايات قضائية أو بلدان مختلفة. حيث يجب أن يتوصل كل مالك للبيانات إلى اتفاق رسمي مع الشركاء الآخرين فيما يتعلق بسياسة الحذف ووقت استبقاء البيانات التي تتم مشاركتها. وفي حالة عدم التوصل إلى مثل هذا الاتفاق، فلن يضطر مالكو قواعد البيانات الأخرى، الذين لا يخضعون لنفس القوانين الخاصة بقاعدة البيانات المضيفة، إلى الامتثال لذلك. كما قد يُحجمون عن إجراء عمليات الحذف المطلوبة لأسباب أخرى مثل القيود المفروضة على الشؤون المالية، أو الموارد، أو الوقت.

البحث المتبادل ثنائي الاتجاه – يتم تسجيل البيانات البيومترية (أ) والبحث فيها على قاعدة البيانات 1. في حالة عدم العثور على مطابقات، يتم عندئذٍ حفظ البيانات في قاعدة البيانات 1 وإرسالها إلى قاعدة البيانات 2 لإجراء البحث، ولكن لا يتم الاحتفاظ بالبيانات (أ) في قاعدة البيانات 2. وبالطريقة نفسها، إذا تم تسجيل البيانات البيومترية (ب) والبحث عنها على قاعدة البيانات 2 ثم إرسالها إلى قاعدة البيانات 1 لإجراء البحث، فلن تحتفظ قاعدة البيانات 1 بها. يتم تكرار هذه الطريقة لأي عدد من قواعد البيانات في الشبكة حيث تبحث كل قاعدة بيانات في عمليات تسجيل البيانات الجديدة لديها من خلال قواعد البيانات الأخرى. ويتم تجنب خطر تفويت المطابقات المحتملة (كما هو الحال في عمليات البحث أحادية الاتجاه) من خلال حفظ البيانات على قاعدة البيانات المضيفة *قبل* البحث فيها عبر الشبكة من أجل منع حدوث فجوات في التوقيت، التي بخلاف ذلك قد تسمح لعمليات البحث في الشبكة الواردة المتزامنة بتفويت بعضها.

ملاحظة غالبًا ما تتم الإشارة إلى هذا النظام باسم "تسجيل فردي لبحث متعدد" أو "إدخال مرة والبحث عدة مرات". تقوم قاعدة البيانات التي تمتلك البيانات بحفظها بعد إجراء البحث فيها ولكن قواعد البيانات الأخرى تقوم بالبحث فقط. يعمل ذلك على تبسيط عملية إدارة البيانات نظرًا إلى أنه يتم تخزين بيانات المالك فقط في قاعدة البيانات الخاصة به، كما يقلل ذلك أيضًا كمية البيانات المحفوظة عبر الشبكة. يجب إدارة تسلسل عمليات البحث بين قواعد البيانات بعناية وتحديدًا عند قيام العديد من قواعد البيانات التابعة لإحدى الولايات القضائية بالتغذية في قاعدة بيانات تابعة لولاية قضائية أخرى. على سبيل المثال، يجب استنفاد تبديلات البحث بين قواعد البيانات في الولاية القضائية (1) بالكامل قبل أن يرسل أيٌّ منها عمليات البحث إلى الولاية القضائية (2)، وإلا فقد يتم الإفصاح عن المطابقات في الولاية القضائية (2) التي كان ينبغي العثور عليها بالفعل في الولاية القضائية (1). يمكن منع ذلك من خلال إرسال عمليات البحث من الولاية القضائية (1) إلى الولاية القضائية (2) عبر قناة واحدة مُدارة.

3-2-3-1 *البيانات البيومترية التنبؤية: الاستخدام الاستباقي لشبكات قواعد البيانات البيومترية لمنع الهجمات الإرهابية*

إن تكامل قواعد البيانات البيومترية عبر المنظور الواسع لوكالات إنفاذ القانون وإدارة الحدود (والبيانات البيومترية العسكرية إذا كانت متوفرة) تتيح إمكانية تحليل النواتج المجمعة للشبكة، ليس فقط من منظور احتياجات العمل المميزة، على سبيل المثال، الكشف عن الجرائم أو فحوص تحديد الهوية عند الحدود، وما إلى ذلك، ولكن أيضًا بوصفها سلسلة أو نمطًا أوسع من "الأحداث البيومترية" في حد ذاتها. فيما يتعلق بالتهديد الإرهابي، قد يكون لكل حدث صلة مباشرة أو غير مباشرة أو ربما يبدو غير ضار بشكل كامل وليس له قيمة ظاهرة، ولكن عند وضعه في سياق المعلومات أو الأحداث البيومترية الأخرى، فقد يُسهم ذلك بشكل واضح في صورة المعلومات الاستخباراتية الأكبر للحركات والأنشطة الإرهابية. وقد تكون بعض هذه النواتج صريحة إلى حد ما مثل الكشف عن ترتيبات السفر المشبوهة أو إيجاد روابط بالجرائم الإرهابية، في حين قد تكون الأخرى أبسط وأوضح ولكن لا تزال تقدم مؤشرات ذات قيمة عند أخذها في الاعتبار مع المواد الأخرى ذات الصلة. تعتمد هذه الطريقة، الموضحة أدناه في الشكل 8، على الاستخدام التقليدي والتفاعلي والسلبي إلى حد كبير لقواعد البيانات البيومترية لأغراض التحقيق ومحاولات إنقاذ الأرواح من خلال منع الهجمات الإرهابية قبل حدوثها باستخدام البيانات البيومترية من المجموعة الأوسع من المصادر المجمعة بشكل استباقي مع تقارير الاستخبارات الأخرى.

الشكل 8 - نموذج البيانات البيومترية التنبؤية

صُممت قواعد البيانات البيومترية التقليدية (الواردة في القسم 1) لتكون تفاعلية وتطرح أسئلة استقصائية قائمة على الهوية والنشاط *الحالي* أو *السابق* مثل *"هل أنت معروف لدينا، ومَنْ المرافقين لك، وماذا فعلت؟"* ويمكن بوضوح لقواعد البيانات البيومترية المتكاملة الإجابة عن نفس الأسئلة ولكن يمكن استخدامها أيضًا بشكل استباقي للاستدلال والتنبؤ بالإجراءات والتنظيمات المستقبلية المحتملة، أي *ما الذي تخطط له أنت ومَنْ يرافقك، أو مَا المرجح أن تقوم به ومتى وأين؟"* ولذلك، يُعد إجراء تحليل شامل ودقيق لجميع النواتج عبر الشبكة أمرًا ضروريًا ويمكن أن يشكل عامل نجاح حاسمًا في تقييم النشاط الإرهابي وتوقعه عند اقترانه بالمعلومات الاستخباراتية الأخرى. وينطبق ذلك بنفس القدر أيضًا على إدارة النواتج اللاحقة.

3-3-3- إدارة النواتج

3-3-3-1 التقييم السياقي للنواتج

في الأنظمة البيومترية المستقلة، يمكن أن تكون النواتج عملية آلية إلى حد كبير مع تدخل بشري ضئيل (راجع القسم 1) ولكن عند تكامل البيانات الواردة في هذه الأنظمة في شبكة من قواعد البيانات البيومترية متعددة الوظائف والبحث فيما بينها، فمن الأهمية بمكان استعراض النواتج وفهمها جيدًا قبل اتخاذ أي إجراء. ويجب أن يأخذ التقييم السياقي لهذه النواتج وأولئك الذين يديرون النتائج الصادرة عن ذلك بعين الاعتبار العوامل الآتية:

ضمان الاستجابة القانونية المتناسبة وإدارة المطابقات غير الصحيحة أو غير المهمة – من الطبيعي لأولئك الذين يتلقون النتائج من أي نوع من قواعد البيانات البيومترية ويتعاملون معها، وعلى وجه الخصوص، قاعدة البيانات المرتبطة بالإرهاب، تشكيل وجهات نظر ازدرائية وافتراض أن أي شخص يتعرف إليه النظام يجب أن يكون إرهابيًّا. ولكن، ذلك ليس الحال دومًا للأسباب الآتية:

1- قد يتسبب خطأ بشري أو خطأ في النظام في تحديد هوية أحد الأفراد على نحو خاطئ، وعلى الرغم من أن ذلك نادر الحدوث، فإنه يجب أن يشكل جزءًا لا يتجزأ من أي بروتوكول استعراض وخصوصًا في حالة ظهور البيانات أو الأدلة الأخرى للتشكيك في النتيجة.
2- قد ترغب الحكومات أو الأطراف الأخرى في إساءة استخدام النواتج البيومترية من خلال إطلاق ادعاءات كاذبة حول الأنشطة الإرهابية من أجل عرقلة معارضتها، أو الأنشطة السياسية، أو النشطاء في مجال حقوق الإنسان (راجع القسم 2-2-5-)
3- قد يكون الشخص الذي تعرف إليه النظام غير متورط بأي شكل في الإرهاب. ولهذا السبب، يجب تقييم القيمة السياقية والنسبية لأي نتيجة بشكل صحيح *قبل* اتخاذ أي إجراء.

على سبيل المثال، قد يتعرض موقع أو عنصر أساسي في أحد التحقيقات المتعلقة بالإرهاب للتلوث عن غير قصد على يد شخص ما غير متورط في أي نشاط إرهابي أو بواسطة موظف مهمل من موظفي إنفاذ القانون. ومن ثمَّ، يقوم المحققون وعلماء الأدلة الجنائية باستخلاص المواد الجنائية وتسجيلها في شبكة قاعدة البيانات المناسبة. وعندئذٍ، قد تستجيب هذه البيانات الجنائية "غير المهمة" لعمليات البحث عبر الشبكة وتُصدر تطابقًا، على سبيل المثال، عندما يقدم الفرد لاحقًا إحدى البيانات البيومترية لعبور الحدود. لذا، يجب أن تكون الإجراءات التي تتخذها السلطات الحدودية مستندة إلى السياق الكامل لأي تطابق بيومتري وليس إلى افتراض آلي بأن الشخص إرهابي لمجرد وجود تطابق بيومتري. ينبغي أن تكون الاستجابة من جانب وكالات إنفاذ القانون مدروسة ومتناسبة بما يتوافق مع القانون الدولي لحقوق الإنسان. ويجب أن تخضع إجراءات التقييم السياقية هذه للإشراف المستقل القوي لمنع أي اعتقال ظالم محتمل أو إخفاق محتمل في تطبيق العدالة.

استراتيجية الاتصال – من أجل ضمان تطبيق التقييمات السياقية على نحو متسق وفعال في إدارة النواتج، يجب على السلطات وضع خطوط اتصال تتسم بالوضوح والتأمين والاستمرارية بين أولئك المعنيين بتقييم النواتج البيومترية والموظفين التنفيذيين على أعلى مستوى وصناع القرار الذين يجب أن يتصرفوا بناءً على المعلومات. سيشمل ذلك تسهيل الحوار العاجل بين مالكي بيانات مسرح الجريمة (إحدى وكالات إنفاذ القانون) والمسؤولين الذين يتعاملون مع أي شخص محتجز بسبب وجود تطابق مع بيانات مسرح الجريمة. ويحدث تبادل هذه المعلومات والأنواع الأخرى من المعلومات بانتظام إلى حدٍ ما وعادةً ما يكون إجراءً تشغيليًّا موحدًا في دوائر إنفاذ القانون الوطنية والدولية. وسيتعين على شبكة الاتصالات أيضًا ترتيب أولويات نتائج قاعدة البيانات والعمل ضمن نطاق زمني متفق عليه، خاصةً عند القبض على أشخاص أو احتجازهم بسبب وجود تطابق بيومتري. كما يجب أن تحدد استراتيجية الاتصال أيضًا القائمة الكاملة لمتسلِّمي النواتج البيومترية من الشبكة مع تطبيق معايير لحل النزاعات لمنع حدوث الخلافات أو حلها بين اثنين من المتسلِّمين فيما يخص مسائل مثل الأولوية القضائية أو أولويات التحقيق.

الأشكال البيومترية، ومعايير إعداد تقارير بيانات الاستخبارات الجنائية، والتفسير العلمي – قد تستخدم بعض شبكات قواعد البيانات البيومترية شكلًا بيومتريًّا واحدًا فقط، ولكن الأكثر اعتيادية وفعالية وجود مجموعة من الأشكال البيومترية التي تعمل بشكل متوازٍ عبر أي شبكة بيومترية، على سبيل المثال، بصمات الأصابع، والحمض النووي، والوجه. إن النواتج من الأنظمة متعددة الأشكال ستقدم نظرة أوسع نطاقًا للنشاط عند جمعها مع الأنظمة متعددة الوظائف التي ستتضمن بيانات استخباراتية جنائية من مسارح الجرائم، إضافةً إلى البيانات المرجعية من مجموعة متنوعة من المصادر. قد لا توفر دائمًا المواد الجنائية المستخلصة من أحد مسارح الجرائم تطابقًا "كاملًا" مع البيانات المرجعية، وذلك بسبب العوامل الواردة في القسم 1 ولكنها لا تزال ذات قيمة هائلة للتحقيق بصفتها دليلًا. يجب أن يحظى هذان المكونان بكامل التقدير والفهم من جانب أولئك المعنيين بتجميع نواتج قواعد البيانات. حيث يجب تصنيف القوة النسبية للتطابق وقيمته الإثباتية أو التحقيقية المحتملة، إضافةً إلى أي معلومات أخرى ذات صلة تم الحصول عليها أثناء التقييم القياسي وإبلاغها إلى الموظف أو المحقق أو المحلل المعني بحيث يمكن اتخاذ الإجراء المناسب والمتناسب. ولذلك، فإنه من قبيل الممارسة الجيدة تسجيل البيانات فقط التي يمكن تقديمها بوصفها دليلًا في المحاكم. مما يتيح استخدام جميع المطابقات بالكامل في أي تحقيق والكشف عنها أو تقديمها في المحكمة.

دراسة الحالة 10 - إجراءات حوكمة النشرات الخاصة بالإنتربول

مثال عملي على إدارة تبادل البيانات الدولية

على الرغم من أن نظام النشرة الحمراء الخاص بالإنتربول لا يتعامل مع النتائج البيومترية، إلا أن له أوجه تماثل كبيرة مع عمليات التقييم المذكورة في القسم 3-3-3-1 ويوفر نموذجًا سليمًا لإدارة البيانات على صعيد عالمي. كما أنه ملزم بالعمل بما يتوافق مع سيادة القانون على الصعيد الدولي وقواعد المنظمة، وضمان تيسير الاتصال الفعال بين الأطراف الرئيسية ووجود نظام معمول به للتعامل بشكل مستقل وقوي مع الشكاوى والطعون المُقدمة من أولئك الخاضعين لإجراءات النشرة الحمراء.

النشرة الحمراء هي طلب لإلقاء القبض بشكل مؤقت على فرد بانتظار عملية التسليم بأمر صادر عن الأمانة العامة بناءً على طلب من أحد البلدان الأعضاء استنادًا إلى أمر قبض وطني صالح. وقد تصدر النشرات الحمراء أيضًا بناءً على طلب من المحاكم الدولية.

إضافةً إلى النشرات الحمراء، يُصدر الإنتربول أنواعًا أخرى من النشرات، على سبيل المثال، النشرة الزرقاء التي يتم إصدارها بناءً على طلب من أحد البلدان الأعضاء بغرض الحصول على معلومات في سياق أي تحقيق جنائي. ويجوز كذلك للبلدان الأعضاء إصدار تعميمات، وهي طلبات للتعاون يتم تعميمها مباشرةً فيما بين البلدان الأعضاء.
لا يحق للإنتربول الإصرار على قيام أي بلد عضو بالقبض على فرد صادر بشأنه نشرة حمراء، أو إجباره على القيام بذلك. ولا يمكن للإنتربول أن يطلب من أي بلد عضو اتخاذ إجراء استجابةً لطلب بلد عضو آخر. فكل بلد عضو في الإنتربول يقرر بنفسه حجم القيمة القانونية التي يمنحها للنشرة الحمراء داخل حدوده. وعند اتخاذ قرار للتصرف بناءً على أي نشرة أو أي طلب آخر، يتحمل البلد المسؤولية الكاملة عن هذا القرار. تعتمد الفعالية التشغيلية لترتيبات النشرة الحمراء على إمكانية إدارة الإحالات بين المكاتب المركزية الوطنية (NCB) على مدار اليوم طوال أيام الأسبوع طوال العام.

يجب أن تستوفي جميع النشرات والتعميمات القواعد واللوائح التنظيمية الخاصة بالإنتربول. ويشمل ذلك المادة 2 من دستور الإنتربول، التي تشير صراحةً إلى روح الإعلان العالمي لحقوق الإنسان، والمادة 3 من دستور الإنتربول، التي تفيد بأنه "يحظر على المنظمة حظرًا باتًّا أن تنشط أو تتدخل في مسائل أو شؤون ذات طابع سياسي أو عسكري أو ديني أو عنصري". وتنص قواعد الإنتربول بشأن معالجة البيانات على معايير إضافية لإصدار كل نوع من أنواع النشرات، وتوزيع المسؤوليات بين مختلف الكيانات، أي البلد مقدم الطلب، والأمانة العامة، والبلدان المستقبلة، وما إلى ذلك.

الإشراف التنظيمي - ثمة عدة مستويات للمراقبة لضمان الامتثال للوائح التنظيمية الخاصة بالإنتربول. المستوى الأول هو المكاتب المركزية الوطنية التي ترسل طلبًا للحصول على تعاون الشرطة (على سبيل المثال، طلب النشرة الحمراء). وتتحمل المسؤولية الكاملة عن أي معلومات تقدمها إلى قواعد بيانات الإنتربول أو تعممها باستخدام نظام المعلومات الخاص بالإنتربول. ويجب أن تضمن المكاتب أن المعلومات دقيقة، وذات صلة، ومحدثة، وأن معالجتها تتم وفقًا لدستور المنظمة وكذلك وفقًا للتشريعات الوطنية الخاصة بها.
والمستوى الثاني هو مقرات الأمانة العامة للإنتربول. أنشأت الأمانة العامة في تشرين الثاني/نوفمبر 2016 فرقة عمل مخصصة تتألف من وحدة متعددة الاختصاصات، تشمل محامين، وضباط شرطة، ومحللين، واختصاصيّي عمليات لاستعراض جميع مستويات معالجة البيانات، بما في ذلك ما يتعلق بالنشرات الحمراء والتعميمات. حيث تُفحص جميع الطلبات بعناية من جانب فرقة العمل لضمان امتثالها لدستور الإنتربول أو قواعده. وربما تُطلب معلومات إضافية من جميع المصادر ذات الصلة، باعتبار ذلك جزءًا من الاستعراض الذي تقوم به فرقة العمل، من أجل اتخاذ قرار بشأن ما إن كان يلزم إصدار نشرة أم لا. علاوةً على ذلك، قد يثير بلد عضو مخاوف بشأن المعلومات التي تتم معالجتها من جانب بلد عضو آخر، بما في ذلك إصدار نشرة حمراء، إذا عدّ ذلك لم يتم وفقًا لقواعد الإنتربول.

إدارة شؤون اللاجئين - منذ حزيران/يونيو 2014، قام الإنتربول بتطبيق سياسة جديدة فيما يتعلق بالقضايا التي تخص اللاجئين. يتيح ذلك للإنتربول دعم البلدان الأعضاء في منع المجرمين من إساءة استخدام حالة اللاجئ، مع توفير الضمانات الكافية والفعالة لحماية حقوق اللاجئين. ويخضع كل طلب من طلبات النشرة الحمراء والتعميم ضد أحد اللاجئين للتقييم بواسطة الأمانة العامة، أو عند الاقتضاء، من جانب اللجنة المعنية بمراقبة ملفات الإنتربول (راجع القسم 3-1-2-)، على أساس كل حالة على حدة. وبشكل عام، لن يتم السماح بمعالجة طلبات النشرة الحمراء والتعميمات ضد اللاجئين إذا تم تأكيد وضع اللاجئ أو ملتمس اللجوء، وكان طلب النشرة/التعميم مقدمًا من البلد الذي يخشى فيه الفرد التعرض للاضطهاد.

حقوق الأفراد الصادر بشأنهم نشرة/تعميم - إن اتخاذ قرار بشأن إصدار نشرة أو تسجيل معلومات في قواعد بيانات الإنتربول لا يؤثر في حقوق الأفراد، بما في ذلك حقه في افتراض براءته، أو حقه في الطعن أمام السلطات المعنية بالبلد الذي أصدر أمر القبض والتمس مساعدة الإنتربول، أو حقه في الطعن أمام السلطات الوطنية التي تنظر في طلب التسليم.

ويتمتع أي فرد على الأقل بالخيارات الثلاثة الآتية التي يمكنه من خلالها الطعن على أي نشرة أو تعميم:

- ☐ الترافع في قضيته أمام السلطات الوطنية بالبلد مُقدم الطلب، سواء بطريقة مباشرة أو من خلال الاستعانة بالتمثيل القانوني. ونظرًا إلى أن أي نشرة حمراء تستند إلى أمر قبض صحيح، ففي حالة سحب السلطات الوطنية المختصة لأمر القبض، ستُحذف النشرة الحمراء.
- ☐ الاتصال باللجنة المعنية بمراقبة ملفات الإنتربول
- ☐ الطلب من بلده أن يتولى القضية بنفسه والاحتجاج على النشرة الحمراء.

عند إلغاء نشرة حمراء أو تعميم، لأي سبب كان، تُرسل رسالة إلى جميع البلدان الأعضاء تخطرهم بالقرار ويُطلب منهم حذف أي معلومات ذات صلة من قواعد البيانات الوطنية لديهم.

تضمن هذه الاحتياطات تحقيق عملية تتسم بالشفافية والتنظيم لمعالجة مثل هذه المسائل وحلها وتجنب إساءة الاستخدام المحتملة للنشرات الحمراء.

2-3-3-3 الأهداف الاستراتيجية والمبادئ التوجيهية للمحققين

يجب أن تعكس استراتيجيات مكافحة الإرهاب الوطنية والإقليمية أهمية الأدلة الجنائية والأنظمة البيومترية. كما يجب أن تدعم وكالات إنفاذ القانون وإدارة الحدود هذه الاستراتيجيات بفعالية من خلال توظيف كل الموارد الجنائية والبيومترية المتاحة لهم والاحتفاظ بقواعد بيانات فعالة.

يمكن أيضًا وضع استراتيجيات جنائية وبيومترية على مستوى التحقيقات ويجب التشجيع على هذه الممارسة من خلال التدريب ومبدأ العمليات. يجب أن يتولى كبير ضباط التحقيق المسؤول عن أي تحقيق متعلق بالإرهاب مهمة تحديد الأهداف الجنائية والبيومترية الأساسية في بداية التحريات ويجب أن تتضمن الملامح البيومترية بشكل روتيني الآتي:

- ☐ جميع العينات البيومترية المرجعية للمعتقلين، التي تم الحصول عليها أثناء التحقيق، يجب أن تكون بجودة مثالية
- ☐ جميع مسارح الجرائم – يجب أن تخضع للفحوص الجنائية الشاملة والمتسلسلة بالكامل لتحقيق أقصى قدر ممكن من نتائج الحمض النووي وبصمات الأصابع لإيجاد الروابط الإرهابية الأوسع نطاقًا، إضافةً إلى المتطلبات الجنائية المحددة للتحقيق
- ☐ يجب تسجيل جميع البيانات البيومترية المناسبة، التي تم استخلاصها أثناء التحقيق، و/أو البحث فيها على جميع قواعد البيانات الوطنية والدولية ذات الصلة.

تتناول عناصر الاستراتيجية البيومترية الثلاثة هذه الآتي:

1- *احتياجات التحقيق* أي البيانات المرجعية البيومترية عالية الجودة للمقارنة الفعالة 1:1 مع مواد مسرح الجريمة، وتسجيل قواعد البيانات والبحث فيها لإحراز تقدم في التحقيقات،
2- *متطلبات التحقيقات الأخرى المتعلقة بالإرهاب والعمليات الاستخباراتية* من خلال إلقاء نظرة أوسع على مسارح الجرائم وجمع المواد البيومترية التي قد لا تكون بالضرورة ذات صلة بالتحقيق الأساسي ولكن يمكن أن تكشف عن شركاء، أو خلايا، أو شبكات غير معروفة مسبقًا،
3- قد لا تقتصر مساعدة البيانات البيومترية المجمعة من تحقيق واحد على حل التحقيقات الأخرى أو إيجاد روابط بتلك التحقيقات فحسب، ولكن من المحتمل أيضًا أن *تمنع وقوع الهجمات الإرهابية في المستقبل* ومن خلال القيام بذلك، تُسهم في إنقاذ العديد من الأرواح.

4-3 الممارسات الموصى بها

أ) ينبغي على الدول أن تكافح التهديد الذي يفرضه استمرار حركة الإرهابيين عبر الحدود الدولية من خلال الاستعانة بالأنظمة البيومترية لحماية حدودها وممتلكاتها الوطنية ومن خلال مشاركة البيانات البيومترية بشكل قانوني مع الشركاء الدوليين.

ب) يمكن إدارة أمن الحدود بشكل أكثر فاعلية من خلال استخدام تقنيات التحقق البيومتري 1:1 بالاشتراك مع فحوص قائمة المراقبة البيومترية 1:كثير لتتبع الإرهابيين وشركائهم، والكشف عنهم. يمكن إنشاء قوائم المراقبة البيومترية بأي حجم بداية من المجموعات المرجعية الصغيرة ووصولًا إلى الاتصال الكامل مع قواعد بيانات كشف الجرائم وإدارة الهوية بوكالات إنفاذ القانون، وفقًا للقانون الوطني، والقيود التنظيمية، والقانون الدولي لحقوق الإنسان.

ج) توصي الدول بشدة بتحقيق أقصى استفادة من استخدامها لقواعد البيانات البيومترية للإنتربول (الوجه، وبصمات الأصابع، والحمض النووي) من أجل مواجهة تهديد الإرهاب والمقاتلين الإرهابيين الأجانب.

د) تُعد مشاركة البيانات البيومترية على المستوى الدولي أداة حيوية في سبيل مواجهة الإرهاب ولكن يجب تنفيذها بما يتوافق مع القانون الدولي لحقوق الإنسان. يجب أن تتأكد الحكومات أنه من خلال مشاركة البيانات البيومترية، لن تُسهّل عمليات القبض التي من شأنها أن تؤدي إلى التعذيب أو فرض عقوبة الإعدام.

هـ) من الضروري إجراء بحث شامل عن السياق الكامل لجميع المطابقات البيومترية قبل اتخاذ أي إجراء، مما يضمن الامتثال الكامل للقانون الدولي لحقوق الإنسان.

و) يجب أن تعكس استراتيجيات مكافحة الإرهاب الوطنية والإقليمية أهمية الأدلة الجنائية والأنظمة البيومترية من خلال وضع المسؤولية على وكالات إنفاذ القانون وإدارة الحدود لزيادة عملياتها من الجمع والاستخدام القانوني للمواد الجنائية أو البيومترية والاحتفاظ بقواعد بيانات فعالة وبروتوكولات مشاركة البيانات.

1-4-3 الوثائق المرجعية

دليل إدارة مراقبة الحدود لبرنامج تحديد هوية الركاب التابع لمنظمة الطيران المدني الدولي (الإيكاو)، مونتريال (2018)

دليل تنفيذ رسائل PNRGOV EDIFACT و XML:
www.wcoomd.org/en/topics/facilitation/instrument-and-tools/tools/api-pnr.aspx

المبادئ التوجيهية لمنظمة الجمارك العالمية/اتحاد النقل الجوي الدولي/منظمة الطيران المدني الدولي (الإيكاو) بشأن سجل أسماء الركاب (الوثيقة 9944)

وثيقة الإيكاو 9303 – وثائق السفر المقروءة آليًا

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

www.interpol.int/INTERPOL-expertise/Databases

بوابة الحمض النووي التابعة للإنتربول - المنشور الرسمي شباط/فبراير 2017

دليل الإنتربول بشأن أفضل ممارسات صور الوجه، تشرين الأول/أكتوبر 2015 وصحيفة وقائع التعرف إلى الوجه

إرشادات الإنتربول بشأن نقل بصمات الأصابع 2012

قواعد الإنتربول بشأن معالجة المعلومات لأغراض التعاون الشرطي الدولي

نظام معلومات السفر والترخيص الأوروبي (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

المنشور الخاص من المعهد الوطني للمواصفات القياسية والتكنولوجيا رقم 1152 "مواصفات النقل لقابلية التشغيل المتبادل للطبعات الخفية"
www.nist.gov

4- الملاحق

4-1 الاختصارات

ABC	نظام مراقبة الحدود الآلية
AFIS	نظام التعرف الآلي إلى بصمات الأصابع
API	نظام المعلومات المسبقة عن الركاب
BCP	نقطة العبور الحدودية
BMS	نظام معلومات إدارة الحدود
CCF	اللجنة المعنية بمراقبة ملفات الإنتربول
CCTV	الدوائر التلفزيونية المغلقة
eBMS	نظام المعلومات الإلكتروني لإدارة الحدود
EER	معدل الخطأ المتساوي
ETS	أنظمة السفر الإلكترونية
FAR	معدل القبول الخاطئ
FAR	معدل الرفض الخاطئ
FTA	معدل فشل الحيازة
FTF	المقاتلون الإرهابيون الأجانب
IEC	اللجنة الدولية للتقنيات الكهربائية
ICAO	منظمة الطيران المدني الدولي
iAPI	النظام التفاعلي للمعلومات المسبقة عن الركاب
ISO	المنظمة الدولية لتوحيد المقاييس
LDS	بنية البيانات المنطقية
MRZ	المنطقة القابلة للقراءة آليًّا
PKI	بنية تحتية للمفاتيح العمومية
PNR	سجل أسماء الركاب
QMS	نظام إدارة الجودة
SIS	نظام شنغن للمعلومات
STR	التكرار المترادف القصير
TAR	معدل القبول الصحيح
TRR	عدل الرفض الصحيح
VIS	نظام المعلومات عن التأشيرات

2-4 مسرد المصطلحات البيومترية

الاعتماد – تُعرّف منظمة الأيزو الاعتماد بأنه "اعتراف رسمي من هيئة مستقلة، تُعرف بشكل عام بأنها هيئة اعتماد، بأن أي هيئة مصادقة تعمل وفقًا للمعايير الدولية."

الانتحال – (يُعرف كذلك باسم هجوم عرض) هي عرض سمات بيومترية زائفة (مثل: قناع وجه مطاطي، أو صورة فوتوغرافية، أو إصبع زائف، أو تسجيل صوتي زائف) لمستخدم قانوني مُسجل للتمكن من الوصول غير المصرح به إلى أي نظام للتعرف إلى السمات البيومترية.

البيانات المرجعية – المستخلصة في ظل ظروف خاضعة للرقابة من المقبوض عليهم في جرائم أو مشتبه فيهم لارتكابها، مثل بصمات الأصابع العشرة لكلتا اليدين والتي يتم أخذها إلكترونيًا بواسطة ماسح ضوئي أو بواسطة الطرق التقليدية باستخدام الحبر والورق؛ ومسحات اللعاب التي يتم أخذها من داخل فم المقبوض عليه أو عينات الشعر أو الدم التي تتم معالجتها لإنشاء صورة حمض نووي كاملة والصور الفوتوغرافية الرقمية للوجه وغيره.

التحقق – (تعرف كذلك باسم مقارنة واحد لواحد أو 1:1). يستخدم هذا النموذج هوية مقترحة لتحديد قالب واحد فقط من قاعدة البيانات للمقارنة مع القالب محل البحث. بشكل أساسي، إنها عملية مصادقة تقارن القالب محل البحث بقالب قاعدة البيانات وإما تؤكد نشأة كلا القالبين من نفس الشخص وإما تنفي ذلك.

التوثيق – تُعرّف الأيزو التوثيق بأنه "قيام هيئة مستقلة بتقديم ضمان خطي (شهادة) بأن المنتج، أو الخدمة، أو النظام المعني يلبي المتطلبات المحددة."

الحد الأساسي - إعداد قابل للتعديل للأنظمة البيومترية. ينظم التوازن بين القبول والرفض لأي تطبيق محدد.

الشكل البيومتري – نوع البيانات البيومترية المستخدمة في أي نظام أو سياق تشغيلي مثل: بصمات الأصابع، والوجه، والحدقة، وما إلى ذلك.

المطابقة – (تعرف كذلك باسم واحد للكثير أو 1:كثير) هذه وظيفة بحث لا تعتمد على هوية مقترحة، ولذلك تبحث في قاعدة البيانات بالكامل للعثور على تطابق محتمل.

بحث إدارة الهوية – يحدد ما إذا تم تسجيل شخص سابقًا في قاعدة بيانات من خلال البحث في البيانات المرجعية البيومترية الخاصة بالشخص من خلال البيانات المرجعية المحفوظة في النظام

بحث الجرائم/الأحداث المتسلسلة – البحث في بيانات مسرح الجريمة البيومترية أو الجنائية من خلال قاعدة بيانات لبيانات مسرح جريمة مشابه لتحديد أي مطابقات ومن ثمَّ إيجاد روابط بين الجرائم أو روابط بين الأحداث في تحقيق واحد.

بحث كشف الجرائم – بروتوكول بحث ثنائي الاتجاه يبحث في (1) البيانات المرجعية مقابل بيانات مسرح الجريمة و(2) بيانات مسرح الجريمة مقابل البيانات المرجعية

بيانات مسرح الجريمة – صادرة عن العينات والعناصر المستخلصة من مسارح الجرائم.

تحويل الصور – العينات البيومترية (مثل صور الوجه) المأخوذة من اثنين أو أكثر من الواهبين، التي يتم دمجها للسماح بالتحقق الناجح من أيٍّ من الأشخاص الواهبين مقابل الهوية المُحوَّلة.

تقييم الامتثال – تضع اللجنة الدولية للتقنيات الكهربائية تعريفًا لتقييم الامتثال بأنه "إثبات باستيفاء المتطلبات المحددة ذات الصلة بمنتج، أو عملية، أو نظام، أو شخص، أو هيئة."

معالجة الاستثناءات – تدابير الطوارئ التي تُتخذ في حالة إخفاق أي نظام بيومتري، على سبيل المثال، التدخل البشري، والأنظمة الاحتياطية، وما إلى ذلك.

معدل الإنتاجية – عدد الأشخاص الذين يستخدمون أي نظام بيومتري ضمن إطار زمني محدد.

معدل الخطأ المتساوي (EER) يشير إلى إعداد الحد الأساسي المعين حيث يتساوى معدل القبول الخاطئ ومعدل الرفض الخاطئ.

معدل الرفض الخاطئ (FRR) – عدد حالات الرفض الخاطئة في صورة نسبة من العدد الإجمالي للاستعلامات البيومترية التي كان يجب قبولها، أي عدد حالات التطابق *التي أصدرها النظام وقدمها على أنها حالات عدم تطابق* في شكل نسبة من حالات التطابق الأصلية

معدل الرفض الصحيح (TRR) – مقياس عدد الحالات التي تكون فيها سمة تحديد الهوية البيومترية لأحد الأشخاص غير مطابقة على نحو صحيح لسمات تحديد الهوية البيومترية للآخرين في قاعدة البيانات، أي عدد حالات عدم التطابق الصحيحة.

معدل القبول الخاطئ (FAR) – عدد حالات القبول الخاطئة في صورة نسبة من العدد الإجمالي للاستعلامات البيومترية التي كان يجب رفضها، أي عدد حالات عدم التطابق *التي أصدرها النظام وقدمها على أنها حالات تطابق* في شكل نسبة من حالات عدم التطابق الأصلية

معدل القبول الصحيح (TAR) – مقياس قدرة النظام على المطابقة الصحيحة لسمات تحديد الهوية البيومترية من نفس الشخص.

معدل فشل الحيازة (FTA) هو نسبة جميع المعاملات المسجلة التي يتعذر إكمالها بسبب حالات الإخفاق عند مراحل العرض (لم يتم التقاط صورة)، أو استخلاص الملامح، أو مراقبة الجودة.

نظام إدارة الجودة – بروتوكول رسمي يحدد العمليات، والإجراءات، والمسؤوليات ويوثقها لاستيفاء أهداف الجودة. فالنظام مصمم لتنسيق أنشطة المنظمة وتوجيهها لتلبية متطلبات العميل والجهة التنظيمية، ومعالجة حالات عدم الامتثال، وإيجاد ثقافة للتحسين المستمر.

نظام التعرف الآلي إلى بصمات الأصابع – نظام إلكتروني مصمم لتخزين كميات كبيرة من (1) المجموعات المرجعية لبصمات الأصابع وراحة اليد و(2) علامات الإصبع وراحة اليد من مسارح الجرائم، والبحث فيها. عادةً ما ينتج عن عمليات البحث في إدارة الهوية استجابة واحدة فقط أو تظهر نتيجة عدم وجود أثر. وتُعرض النتائج الخاصة ببحث كشف الجرائم في صورة قائمة استجابة للمطابقات المحتملة. حيث يُجرى استعراض للاستجابات من جانب فاحص بصمات الأصابع الذي يؤكد أي مطابقات أصدرها النظام.

3-4 دليل المنظمات الدولية

معهد القياسات الحيوية www.biometricsinstitute.org

منظمة الطيران المدني الدولي www.icao.int

لجنة الصليب الأحمر الدولية www.icrc.org

المنظمة الدولية للشرطة الجنائية (الإنتربول) www.interpol.int

اللجنة الدولية للتقنيات الكهربائية www.iec.ch

المنظمة الدولية لتوحيد المقاييس www.iso.org

4-4 مكتب الأمم المتحدة المعني بمكافحة الإرهاب (UNOCT)

تُسهم الأمانة العامة للأمم المتحدة، والوكالات، والصناديق والبرامج، والمنظمات التابعة لها في تنفيذ استراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب من خلال كلٍّ من ولاياتها الفردية وعضويتها في فرقة العمل المعنية باتفاق الأمم المتحدة العالمي لتنسيق مكافحة الإرهاب (GCTCCTF).

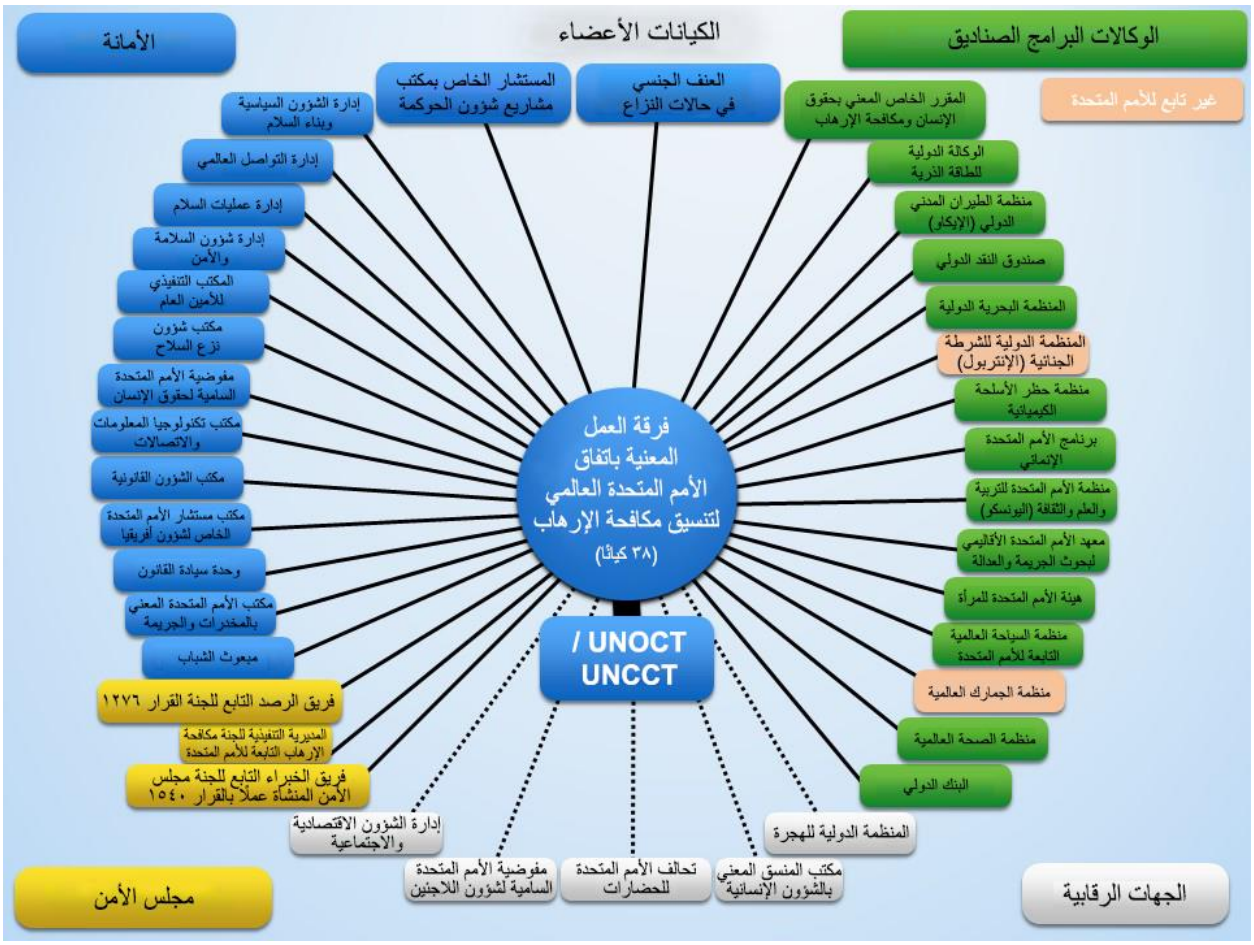
تتألف فرقة العمل من 38 كيانًا دوليًّا ومنظمة الإنتربول التي بحكم عملها تشارك في الجهود متعددة الأطراف لمكافحة الإرهاب. ويُقدم كل كيان إسهامات تتسق مع ولايته الخاصة. يضم أعضاء فرقة العمل مكتب الأمم المتحدة المعني بمكافحة الإرهاب والكيانات التالية:

1- فريق الرصد المعني بتنظيم القاعدة وحركة طالبان
2- المديرية التنفيذية للجنة مكافحة الإرهاب (CTED)
3- إدارة عمليات السلام (DPO)
4- إدارة الشؤون السياسية وبناء السلام (DPPA)
5- إدارة التواصل العالمي (DGC)
6- إدارة شؤون السلامة والأمن (DSS)
7- فريق الخبراء التابع للجنة مجلس الأمن المنشأة عملًا بالقرار 1540
8- الوكالة الدولية للطاقة الذرية (IAEA)
9- منظمة الطيران المدني الدولي (الإيكاو)
10- المنظمة البحرية الدولية (IMO)
11- صندوق النقد الدولي (IMF)
12- المنظمة الدولية للشرطة الجنائية (الإنتربول)
13- مكتب شؤون نزع السلاح (ODA)
14- مفوضية الأمم المتحدة السامية لحقوق الإنسان (OHCHR)
15- مكتب الشؤون القانونية (OLA)
16- مكتب الأمين العام (OSG)

17- مكتب المستشار الخاص المعني بمنع الإبادة الجماعية
18- مكتب الممثل الخاص للأمين العام المعني بالأطفال والنزاع المسلح (CAAC)
19- مكتب الممثلة الخاصة للأمين العام المعنية بالعنف الجنسي في حالات النزاع (SVC)
20- مكتب مبعوث الأمين العام المعني بالشباب
21- منظمة حظر الأسلحة الكيميائية (OPCW)
22- المقررة الخاصة المعنية بتعزيز وحماية حقوق الإنسان في سياق مكافحة الإرهاب
23- برنامج الأمم المتحدة الإنمائي (UNDP)
24- منظمة الأمم المتحدة للتربية والعلم والثقافة (اليونسكو)
25- معهد الأمم المتحدة الأقاليمي لبحوث الجريمة والعدالة (UNICRI)
26- مكتب الأمم المتحدة المعني بالمخدرات والجريمة (UNODC)
27- مكتب مستشار الأمم المتحدة الخاص لشؤون أفريقيا (OSAA)
28- وحدة سيادة القانون التابعة للأمم المتحدة
29- هيئة الأمم المتحدة للمرأة
30- منظمة السياحة العالمية التابعة للأمم المتحدة (UNWTO)
31- منظمة الجمارك العالمية (WCO)
32- البنك الدولي
33- منظمة الصحة العالمية (WHO)

الجهات الرقابية

34- المنظمة الدولية للهجرة (IOM)
35- مكتب المنسق المعني بالشؤون الإنسانية (OCHA)
36- إدارة الشؤون الاقتصادية والاجتماعية بالأمم المتحدة (DESA)
37- مفوضية الأمم المتحدة السامية لشؤون اللاجئين (UNHCR)
38- تحالف الأمم المتحدة للحضارات (UNAOC)



5-4 الفريق العامل التابع لمكتب الأمم المتحدة المعني بإدارة الحدود وإنفاذ القانون فيما يتعلق بمكافحة الإرهاب

يهدف فريق الأمم المتحدة العامل المشترك بين الوكالات هذا إلى تقديم الإرشادات إلى الدول الأعضاء بشأن تنفيذ التدابير اللازمة القانونية والمؤسسية والعملية لمراقبة الحدود فيما يتعلق بمكافحة الإرهاب. ويركز تحديدًا على المجالات الآتية: تنقل الإرهابيين؛ وسلامة وثائق السفر وأمنها؛ والحركة غير المشروعة للنقود والصكوك لحاملها القابلة للتداول؛ وحركة البضائع والعمليات الخاصة بها؛ والنقل غير المشروع للأسلحة الصغيرة، والأسلحة الخفيفة، والذخيرة، والمتفجرات، وأسلحة الدمار الشامل؛ والأمن البحري وأمن الطيران؛ ونظم الإنذار المبكر والتحذير؛ ومراقبة الحدود المفتوحة.

الولاية

تم إنشاء الفريق العامل لمساعدة الدول الأعضاء على تعزيز أنظمتها الخاصة بإدارة الحدود ومراقبة الحدود على النحو المنصوص عليه في العنصر الثاني، الفقرات 4 و5 و7 و8 و13 إلى 16، والعنصر الثالث، الفقرات 2 و4 و11 إلى 13 من استراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب (A/RES/60/288).

وُضعت الاختصاصات للفريق العامل المعني بإدارة قضايا الحدود المتصلة بمكافحة الإرهاب.

الوضع

يقوم الفريق العامل حاليًا بتنفيذ مشروع بشأن إدارة الحدود المنسقة، حيث يقوم بتجميع كل المعاهدات والمعايير وأفضل الممارسات الدولية ذات الصلة في تنسيق قابل للتنفيذ وسهل الاستخدام لمساعدة الدول المهتمة على بناء الآليات المؤسسية والإجرائية اللازمة لتحقيق نظام فعال لإدارة الحدود. وقد أنهى الفريق العامل إعداد قالب عمل بشأن إدارة الحدود المنسقة. وستستمر عملية تحسين هذا القالب من خلال إقامة الحوار والمشاورات المستمرة مع الدول الأعضاء والمنظمات الدولية.

الكيانات

الرؤساء المشاركون:

- المديرية التنفيذية للجنة مكافحة الإرهاب (CTED) (القائد)
- منظمة الجمارك العالمية (WCO)
- المنظمة الدولية للشرطة الجنائية (الإنتربول)

الكيانات الرئيسية:

- مكتب الأمم المتحدة المعني بمكافحة الإرهاب (UNOCT)
- فرقة العمل المعنية باتفاق الأمم المتحدة العالمي لتنسيق مكافحة الإرهاب (GCTCCTF)
- منظمة الطيران المدني الدولي (الإيكاو)
- المنظمة البحرية الدولية (IMO)
- مكتب الأمم المتحدة المعني بالمخدرات والجريمة (UNODC)
- المنظمة الدولية للهجرة (IOM)
- مفوضية الأمم المتحدة السامية لحقوق الإنسان (OHCHR)
- معهد الأمم المتحدة الأقاليمي لبحوث الجريمة والعدالة (UNICRI)
- مكتب شؤون نزع السلاح (ODA)
- فريق الرصد التابع للجنة القرار 1276
- فريق الخبراء التابع للجنة مجلس الأمن المنشأة عملًا بالقرار 1540
- مفوضية الأمم المتحدة السامية لشؤون اللاجئين (UNHCR)

الكيانات الأعضاء الأخرى:

- إدارة عمليات السلام (DPO)
- منظمة حظر الأسلحة الكيميائية (OPCW)
- برنامج الأمم المتحدة الإنمائي (UNDP)
- منظمة الصحة العالمية (WHO)
- إدارة الشؤون الاقتصادية والاجتماعية (DESA)

يوجه الفريق العامل أنشطته عبر عدد من الموضوعات الرئيسية:

- تنقل الأشخاص والتجهيزات الخاصة بذلك
- سلامة عملية إصدار الوثائق وأمنها
- حركة النقود وغيرها من الصكوك لحاملها القابلة للتداول

- نقل البضائع والتجهيزات الخاصة بذلك
- نقل الأسلحة الصغيرة، والأسلحة الخفيفة، والذخيرة، والمتفجرات، والمواد الكيميائية والبيولوجية والإشعاعية والنووية
- الأمن البحري
- أمن الطيران
- نظم الإنذار المبكر والتحذير
- مراقبة الحدود المفتوحة
- الحاجة الملحة إلى احترام حقوق الإنسان

تنقل الأشخاص والتجهيزات الخاصة بذلك

من النتائج المهمة المترتبة على الهجمات الإرهابية المنفذة في جميع أنحاء العالم على مدار السنوات الأخيرة زيادة الربط بين حركة الأشخاص عبر الحدود والتدابير المتخذة لحماية الأمن الوطني. ونظرًا إلى أن الإرهابيين يستغلون العمليات نفسها التي تيسر السفر وعمليات التبادل الاقتصادي والثقافي، أصبحت التدابير الرامية إلى منع الإرهاب ترتبط بوضوح بإدارة التنقل عبر الحدود وتنظيمه. وتشمل هذه التدابير تنفيذ نظم إدارة الحدود المتكاملة للمسافرين، وإصدار وثائق سفر مؤمنة، وتعزيز تبادل المعلومات بين أصحاب المصلحة، والتدريب، وبناء القدرات. ومن شأن إدخال التحسينات على هذه المجالات المساعدة على تعزيز أنظمة الهجرة والأمن بينما تيسر أيضًا حركة الأشخاص عبر الحدود. بعض هذه التدابير معقدة من الناحية التكنولوجية ومبتكرة للغاية، ولكن يمكن تنفيذ عدد من التدابير الأكثر بساطة في المجالات التقليدية لإدارة الهجرة بهدف تحسين القدرة الإجمالية. ويجب دائمًا أن تكون هذه التدابير مبررة حسب مستوى التهديد الذي تتم مواجهته، ولا سيما أن زيادة الأمن قد تؤدي بدورها إلى زيادة العراقيل والتدخل المحتمل في الخصوصية والحقوق المدنية.

سلامة عملية إصدار الوثائق وأمنها

إن أمن وثائق السفر وإدارة الهوية أدوات مهمة في سبيل منع تنقل الإرهابيين ومكافحة الجرائم عبر الحدود. فوجود وثائق سفر مزورة في أيدي الإرهابيين لا يقل خطورة عن السلاح. ولأن جوازات السفر الحديثة أصبحت أكثر أمانًا وتزيد صعوبة تزويرها، يحاول المجرمون والإرهابيون بشكل متزايد تزوير وثائق داعمة (مثل شهادات الميلاد، وبطاقات الهوية القومية، وما إلى ذلك) أو التقدم بطلب للحصول على جوازات سفر "صادرة رسميًّا". ومن ثمَّ، فإنه لأمر أساسي أن تضع الدول مواصفات عالمية لإدارة الهوية وأمن وثائق السفر (بما في ذلك في عملية الإصدار) وتطبقها، وذلك من أجل معالجة مواطن الضعف هذه.

حركة النقود وغيرها من الصكوك لحاملها القابلة للتداول

إن تهريب النقود و/أو الصكوك القابلة للتداول لحاملها (BNI) عبر الحدود تُعد من بين الوسائل المفضلة التي يستخدمها الإرهابيون لنقل الأموال عبر الحدود الدولية، سواء بغرض تمويل الإرهاب أو من أجل غسل عائدات الأنشطة غير المشروعة. وتعهد الحكومات إلى دوائرها الجمركية بتنفيذ تدابير مراقبة الحدود التي تمتثل للمعايير الدولية، بوصفها وسيلة للكشف عن الحركة غير المشروعة للنقود والصكوك لحاملها القابلة للتداول (BNI) ومنعها. ومن شأن الامتثال الصارم لهذه المعايير أن يُحسِّن من فعالية مراقبة الحدود في هذا المجال. ولا شك أن مكافحة تمويل الإرهاب هو جزء لا يتجزأ من نهج الأمم المتحدة لمكافحة الإرهاب، كما يتضح في العديد من قراراتها واتفاقياتها.

نقل البضائع والتجهيزات الخاصة بذلك

إن التجارة العالمية وسلسلة التوريد الدولية معرضة بوجه خاص لاستغلال الإرهابيين. ومن أجل تقليل وجه الضعف هذا إلى أدنى حد ممكن، ينبغي اتخاذ مجموعة من التدابير، بما في ذلك ضمان تسلُّم معلومات مسبقة عن البضائع الإلكترونية بشأن الشحنات الصادرة والواردة والعابرة، والاستعانة بنهج متسق لإدارة المخاطر للتصدي للتهديدات بشأن أمن البضائع، واستخدام معدات كشف غير تدخلية، وتعزيز التعاون بين إدارات الجمارك (على سبيل المثال، من خلال إجراء الفحص الصادر للحاويات والشحنات عالية المخاطر)، وإقامة شراكات مع القطاع الخاص لتنفيذ الممارسات الأمنية عند كل مرحلة من مراحل سلسلة التوريد، من خلال برامج المشغلين الاقتصاديين المعتمدين (AEO). ولا شك أن تنفيذ مثل هذه التدابير والتدابير ذات الصلة أمر أساسي من أجل زيادة أمن التجارة العالمية وتيسير تدفق البضائع عبر الحدود الدولية.

نقل الأسلحة الصغيرة، والأسلحة الخفيفة، والذخيرة، والمتفجرات، والمواد الكيميائية والبيولوجية والإشعاعية والنووية

إن الاتجار والنقل غير المشروعين للأسلحة الصغيرة، والأسلحة الخفيفة، والذخيرة والمتفجرات، وكذلك المواد الكيميائية والبيولوجية والإشعاعية والنووية، والسلع مزدوجة الاستخدام، مع استخدام الأنماط المتغيرة فى تجارة الأسلحة وتورط العناصر الفاعلة غير التجارية، يمثل مشاكل كبيرة يجب أن تتصدى لها الجهود العالمية المعنية بمكافحة الإرهاب. وعند وقوع هذه الذخائر والمواد فى أيدي الإرهابيين تصبح العناصر المكونة للهجمات الإرهابية. ولكن التنظيم الفعال، وضوابط التصدير، وإدارة الحدود، بما في ذلك التدابير التشريعية والتنفيذية، يمكنها التقليل من الخطر الذي يمكن أن تمثله مثل هذه العناصر، إما التي تحول مسارها إلى جهات غير الدول وإما التي تحصل عليها الجهات غير الدول بشكل غير مشروع. وينبغي أن تحترم هذه التدابير الحاجة إلى الحفاظ على التوازن الصحيح بين ضوابط التصدير وتيسير التجارة المشروعة.

الأمن البحري

يتم نقل ما يزيد عن 90 في المئة من إجمالي البضائع المُتاجر فيها دوليًّا من المصدر إلى الوجهة عبر طرق التجارة البحرية العالمية الرئيسية في جميع أنحاء العالم. ومن ثمَّ، فإن أمن المجال البحري مسألة ذات أهمية عالمية. وتتمثل أهداف الأمن البحري في الكشف عن المخاطر الأمنية وقمعها، واتخاذ التدابير الوقائية ضد الحوادث الأمنية التي تؤثر في السفن أو مرافق الموانئ، وحماية الركاب وأطقم العمل والسفن وحمولاتها، ومرافق الموانئ والأشخاص العاملين في مناطق الموانئ والقاطنين في تلك المناطق، مع الاستمرار في السماح بالحركة الآمنة والفعالة للتجارة البحرية. ومن الضروري التنفيذ الفعال للتدابير الأمنية التشريعية والعملية ذات الصلة من أجل منع ارتكاب الأعمال غير القانونية ضد الركاب وأطقم السفن المشتركة في الرحلات العالمية وضد مرافق الموانئ التي تخدمهم.

أمن الطيران

تظل أعمال الإرهاب تشكل تهديدات خطيرة ومستمرة على الطيران المدني الدولي. ويتطلب التصدي لهذه التهديدات وضع سياسات وتدابير أمنية تتسم بالشمولية والمسؤولية ترمي بدورها إلى ضمان الأمن المادي للطائرات والمطارات. ولا شك أن تبني أحكام تشريعية لتجريم أعمال التدخل غير القانوني ضد الطيران المدني، وفعالية تنفيذ معايير أمن الطيران ذات الصلة وإنفاذها، سيعزز قدرة الدول على التصدي لهذه التهديدات بشكل ملحوظ.

نظم الإنذار المبكر والتحذير

إن أمن الحدود عملية ديناميكية ومتطورة. ونظرًا إلى أن التنقل غير المشروع للأشخاص عبر الحدود لا يؤثر سلبًا في الأمن فحسب، بل يؤثر أيضًا في رفاهة الدول من الناحية السياسية والاقتصادية والاجتماعية، فإن الحكومات تركز حاليًا على الجهود الأمنية التعاونية، انطلاقًا من مفهوم أن الإجراءات الانفرادية لم تعد مُجدية. ولذلك، فإن نظم الإنذار المبكر والتحذير الشاملة هي مكونات رئيسية لنظم إدارة الحدود الفعالة. حيث تعزز القدرة الإجمالية للدول على الكشف عن الإرهاب ومنعه ومكافحته، من خلال تيسير التعاون بين الوكالات، وتبادل المعلومات الموثوق بها ذات الصلة ومشاركتها في الوقت المناسب، ومن ثمَّ إتاحة اتخاذ القرارات الحاسمة بأسلوب مسؤول.

تستفيد العديد من المنظمات الدولية ذات الولاية المتعلقة بمراقبة الحدود من نظم الإنذار المبكر والتحذير أو تشجع على استخدامها، سواء من خلال الأدوات التي طورتها المنظمة الفردية أو من خلال الأدوات التي طُورت ليستخدمها المجتمع الدولي. وتتضمن هذه الأدوات شبكات مكتب الاتصال الإقليمي للاستخبارات الجمركية (RILO) وشبكة الإنفاذ الجمركي (CEN) التابعة لمنظمة الجمارك العالمية (WCO)؛ والاتفاقية الدولية لسلامة الأرواح في البحار (SOLAS) ونظام تحديد الهوية والتتبع عن بعد (LRIT) والنظام الآلي لتحديد الهوية (AIS) التابعة للمنظمة البحرية الدولية (IMO)؛ والقوائم الموحدة للجان "الجزاءات" بمجلس الأمن، ونظام الاتصالات العالمي المؤمن "I-24/7"، وقاعدة بيانات الإنتربول المتعلقة بوثائق السفر الضائعة أو المسروقة ونظام الإشعارات خاصة المنظمة الدولية للشرطة الجنائية (الإنتربول).

مراقبة الحدود المفتوحة

لا تزال الحدود المفتوحة (الحدود بين نقاط التفتيش البرية والموانئ البحرية الرسمية) تُسهّل عملية التنقل غير القانوني للأشخاص عبر الحدود، بما في ذلك الإرهابيون والمجرمون، ونقل البضائع (بما في ذلك الأسلحة الصغيرة، والأسلحة الخفيفة، والذخيرة والمتفجرات، والمواد الكيميائية والبيولوجية والإشعاعية والنووية). تدرك الحكومات أهمية تأمين الحدود المفتوحة وتحاول القيام بذلك من خلال مجموعة متنوعة من التدابير، بما في ذلك الإشراف، والدوريات، والحواجز المادية، وعمليات المراقبة والدوريات المشتركة، وتبادل المعلومات، وتقييمات المعلومات الاستخباراتية، والاشتراك مع المجتمعات الحدودية بشأن المسائل المتعلقة بالمراقبة وضبط الأمن. ويلزم تضافر جهود المراقبة من جانب السلطات ذات الصلة من أجل التصدي بفعالية للمخاطر التي تمثلها الحدود المفتوحة.

الحاجة الملحة إلى احترام حقوق الإنسان

تعكس استراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب تأكيدًا واضحًا، من جانب الدول الأعضاء، على أن التدابير الفعالة لمكافحة الإرهاب وحماية حقوق الإنسان غير متضاربة، بل هي أهداف تكميلية وتعزز من بعضها، وأن حقوق الإنسان ووحدة سيادة القانون تشكل الأساس الجوهري للجهود العالمية لمكافحة الإرهاب. ومن خلال تبني الاستراتيجية العالمية وخطة عملها، عقدت الدول الأعضاء العزم على "التسليم بأن التعاون الدولي وأي تدابير نضطلع بها من أجل منع الإرهاب ومكافحته يجب أن تتماشى مع الالتزامات المنوطة بنا بموجب القانون الدولي، بما في ذلك ميثاق الأمم المتحدة والاتفاقيات والبروتوكولات ذات الصلة، وبخاصة قانون حقوق الإنسان وقانون اللاجئين والقانون الإنساني الدولي" (قرار الجمعية العامة 288/60، المرفق، فقرة الديباجة 3، التي أعيد التأكيد عليها في قرار الجمعية العامة 297/64). وشددت الجمعية العامة أيضًا على الحاجة الملحة إلى ضمان احترام حقوق الإنسان في الجهود المبذولة لمكافحة الإرهاب في أكثر من 60 قرارًا بشأن الإرهاب الدولي. وفيما يتعلق بصفة خاصة بمراقبة الحدود، دعت الجمعية الدول الأعضاء إلى "كفالة توخي الوضوح والاحترام التام لالتزاماتها بموجب القانون الدولي، وبخاصة قانون اللاجئين وقانون حقوق الإنسان، في المبادئ التوجيهية والممارسات المتعلقة بجميع عمليات مراقبة الحدود وغيرها من الآليات السابقة للدخول إزاء الأشخاص الذين يلتمسون الحماية الدولية" (قرار الجمعية العامة 159/62، الفقرة 8، التي أعيد التأكيد عليها في قرار الجمعية العامة 221/64).